T.R.
ISTANBUL SABAHATTIN ZAIM UNIVERSITY
GRADUATE EDUCATION INSTITUTE
DEPARTMENT OF ISLAMIC ECONOMICS AND FINANCE

A PROPOSED CONTEMPORARY *FIQH* FRAMEWORK FOR ANALYZING ISSUES IN CRYPTOCURRENCIES

Ph.D. THESIS

Ayman BEKİROĞLU

Istanbul
February-2024

T.R.
ISTANBUL SABAHATTIN ZAIM UNIVERSITY
GRADUATE EDUCATION INSTITUTE
DEPARTMENT OF ISLAMIC ECONOMICS AND FINANCE

A PROPOSED CONTEMPORARY *FIQH* FRAMEWORK FOR ANALYZING ISSUES IN CRYPTOCURRENCIES

Ph.D. THESIS

Ayman BEKİROĞLU

Supervisor
Asst. Prof. Dr. Mohamed Cherif El AMRI
Co-supervisor
Assoc. Prof. Dr. Mustafa Omar MOHAMMED

Istanbul
February-2024

THESIS APPROVAL

This study has been approved in partial fulfillment of the requirements for Ph.D. Degree in Islamic Economics and Finance.

Advisor Asst. Prof. Dr. Mohamed Cherif El AMRI ----------

Co-advisor Assoc. Prof. Dr. Mustafa Omar MOHAMMED ----------

Member of jury Asst. Prof. Dr. Abdelkader CHACHI ----------

Member of jury Asst. Prof. Dr. Ensari YÜCEL ----------

Member of jury Asst. Prof. Dr. Omar KACHKAR ----------

Member of jury Asst. Prof. Dr. Tawfiq AZRAK ----------

Approval by

Graduate Education Institute

Prof. Dr. Erhan İÇENER

Director, Graduate Education Institute

DECLARATION OF SCIENTIFIC ETHICS AND ORIGINALITY

This is to certify that this PhD dissertation titled "A Proposed Contemporary *Fiqh* Framework for Analyzing Issues in Cryptocurrencies" is my own work and I have acted according to scientific ethics and academic rules while producing it. I have collected and used all information and data according to scientific ethics and guidelines on thesis writing of Sabahattin Zaim University. I have fully referenced, in both the text and bibliography, all direct and indirect quotations and all sources I have used in this work.

Ayman BEKİROĞLU

February-2024

ACKNOWLEDGEMENT

In the name of **Allah**, the **Most Gracious**, the **Most Merciful**.

All praise is due to **Allah**, the **Lord** of all the worlds, and peace and blessings be upon the **Messenger** of **Allah**, who was sent as a mercy to all. Commencing this acknowledgment, I extend my profound gratitude to **Allah** for bestowing upon me the strength and guidance necessary for navigating the intricate path of my doctoral journey. I earnestly pray that the knowledge granted to me becomes a source of benefit, and I implore **Allah** to extend these benefits to the broader ummah. May the insights gained contribute positively to the collective understanding and welfare of the community.

My heartfelt thanks extend to my parents, whose constant prayers, benevolent emotions, and enduring patience have played a pivotal role in witnessing the fruition of my academic journey. Despite their advanced age, they still provide the care and generosity that know no bounds. I find them to be a source of immeasurable strength. Truly, reciprocation is possible for everyone except for a mother and father.

Special appreciation goes to my supervisor, Mohammed Cherif El Amri, for going above and beyond in providing invaluable support, making the complexities of this task more manageable. His commitment extended beyond mere guidance – his efforts were directed to enhance my academic profile and open doors for professional advancement.

Prof. Mustafa Omar Mohammed deserves special acknowledgment for his insightful ideas, transformative feedback that opened new horizons, assistance in maintaining the structure and quality, and for generously sharing his precious time. His contributions have been a catalyst for academic growth as they were instrumental in shaping and refining my research skills, significantly elevating my methodological rigor.

I am deeply grateful to my wife for her remarkable patience, sacrificial commitment of quality time, steadfast support, and endless encouragement throughout the challenging journey of completing my PhD. Her cherishing soul added an extra layer

of comfort and encouragement, turning this academic pursuit into a shared endeavor filled with warmth and understanding. My children's understanding and sacrifice of valuable time, allowing me the peace of mind to focus on my research, have been irreplaceable. For that, their sacrifice will not go unnoticed.

I am also indebted to all colleagues and friends with whom I have engaged in discussions on the topic of cryptocurrencies, and to the experts whom I have interviewed for their invaluable insights. Their contributions have enriched my understanding and perspective on this complex subject matter.

Lastly, but not least, in dedicating this work, I also honor the brave souls in Palestine, particularly those enduring hardship and loss in Gaza. My thoughts are with the heroes, children, and families facing the harsh realities of occupation. May their resilience and patience be rewarded by **Allah**.

Ayman BEKİROĞLU

ABSTRACT

A PROPOSED CONTEMPORARY *FIQH* FRAMEWORK FOR ANALYZING ISSUES IN CRYPTOCURRENCIES

Ayman BEKİROĞLU

Ph.D. Dissertation, Islamic Economics and Finance

Supervisor: Asst. Prof. Dr. Mohamed Cherif EL AMRI

February-2024, 172 + xvii Pages

Cryptocurrencies have significantly disrupted traditional financial systems since their inception, highlighted by their innovative features and original decentralization. This has led to widespread confusion and debate among scholars and researchers. This study assesses the complexities and disputes cryptocurrencies introduce and evaluates the current juristic frameworks' ability to address these challenges. It proposes a new jurisprudential framework for analysis of such issues.

Employing qualitative methods, this research involves in-depth semi-structured interviews with experts having academic rigor and possessing jurisprudential knowledge or equivalent Sharī'ah expertise, actively engaged in cryptocurrency research. To extract key insights, this thesis employs thematic analysis.

The analysis reveals critical challenges, including traditional precedent paradox and scholarly disagreements over definitions, and highlights the superficial depth of current investigations. The findings validate and optimize the proposed framework, resulting in a clear demarcation between the jurisprudential and *Sharī'ah* objectives. The study underscores the need for effective risk management in cryptocurrency regulation and the establishment of standards in the digital currency realm. Consequently, it offers recommendations for jurists, institutions, regulatory bodies, and policymakers.

Keywords: Cryptocurrency, *Fiqh* framework, Risk management, Juristic paradigms, Thematic analysis, Crypto *Sharī'ah* standards, *Maqāṣidi* component.

ÖZET

KRİPTO PARALARA İLİŞKİN SORUNLARIN ANALİZİNDE ÇAĞDAŞ BİR FIKHİ ÇERÇEVE ÖNERİSİ

Ayman BEKİROĞLU

Doktora Tezi, İslam Ekonomisi ve Finans

Danışman: Dr. Öğr. Üyesi Mohamed Cherif EL AMRI

Şubat-2024, 172 + xvii Sayfa

Kripto paralar, ortaya çıktıkları andan itibaren yenilikçi özellikleri ve orijinal merkeziyetsizlikleriyle geleneksel finans sistemlerini önemli ölçüde sarsmıştır. Bu, akademisyenler ve araştırmacılar arasında yaygın bir kafa karışıklığına ve tartışmaya yol açmıştır. Bu çalışma, kripto paraların getirdiği karmaşıklıkları ve tartışmaları değerlendirerek mevcut yargı çerçevelerinin bu zorlukları ele alma kapasitesini incelemektedir. Böylece sorunların analizi için yeni bir yargısal çerçeve önermektedir.

Nitel yöntemler kullanarak, bu araştırma akademik titizliğe sahip ve yargısal bilgiye veya eşdeğer Şeriat uzmanlığına sahip, kripto para araştırmalarında aktif olarak yer alan uzmanlarla derinlemesine yarı yapılandırılmış mülakatlar içermektedir. Temel içgörüleri çıkarmak için bu tez tematik analiz yöntemini kullanmaktadır.

Analiz, geleneksel öncül paradoksu ve tanımlar üzerine bilimsel anlaşmazlıklar da dahil olmak üzere kritik zorlukları ortaya çıkarmakta ve mevcut incelemelerin yüzeysel derinliğini vurgulamaktadır. Bulgular, önerilen çerçeveyi doğrulayıp optimize ederek, yargısal ve Şeriat hedefleri arasında net bir ayrım sağlamaktadır. Çalışma, kripto para düzenlemesinde etkili risk yönetiminin gerekliliğini ve dijital para alanında standartların oluşturulmasını vurgulamaktadır. Sonuç olarak, yargıçlar, kurumlar, düzenleyici organlar ve politika yapıcılar için öneriler sunmaktadır.

Anahtar kalimeler: Kripto para, Fıkıh çerçevesi, Risk yönetimi, Hukuki paradigmalar, Tematik analiz, Kripto *Sharī'ah* standartları, *Maqāṣidi* bileşen.

TABLE OF CONTENTS

CHAPTER IV

CHAPTER V

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AAOIFI	:	Accounting and Auditing Organization for Islamic Financial Institutions
Altcoin	:	Alternative Coin
ATM	:	Automated Teller Machine
ATO	:	Australian Tax Office
AUSCIF	:	Australian Center for Islamic Finance
BLK	:	BlackCoin
BNB Chain	:	Binance Smart Chain
BTC	:	Bitcoin
BTG	:	Bitcoin Gold
CAD-coin	:	Central Bank of Canada's stablecoin
CIIF	:	Chartered Institute of Islamic Finance Professionals
COVID-19	:	Corona Virus pandemic – 2019
CRA	:	Canadian Revenue Agency
Crypto	:	Crypto Asset / Cryptocurrency
DAI	:	Development Alternatives Incorporation's employee stablecoin
DAO	:	Decentralized Autonomous Organization
DGX	:	Digix Gold
DOGE	:	Dogecoin
ERC-20	:	Ethereum-Compatible tokens
ETH	:	Ethereum
EUR	:	European Union currency
Eurocoin	:	European Central Bank's Stablecoin

EXP : Expanse Coin

Fedcoin : Federal Reserve's Stablecoin

FinCEN : Financial Crime Enforcement Network

FinTech : Financial Technology

FRB : Fractional Reserve Banking

FRC : Freicoin

FTX : Futures Exchange

GBP : Great Britain Pound

HANA : Hanacoin

IFIN : Islamic Finance Institution Network

IIFA : International Islamic *Fiqh* Academy

IMF : International Monetary Fund

INCEIF : International Center for Education in Islamic Finance

IRS : Internal Revenue Service

ISRA : International *Sharī'ah* Research Academy

LBXPeg : London Block Exchange pound-Pegged stablecoin

LCC : Litecoin Cash

LTC : Litecoin

M-Pesa : Mobile phone-based Pesa (money) transfer service in Kenya

MultiSig : Multiple Signatures

NFT : Non-Fungible Token

NMC : Namecoin

NXT : BCNeXT crypto

OIC : Organization of Islamic Cooperation

P2P : Peer-to-Peer

PoS : Proof of Stake

PoW	:	Proof of Work
QR	:	Quick Response
SEC	:	Securities and Exchange Commission
SHA256d	:	Secure Hash Algorithm - 256-bit - Double hashing
SRC	:	Swiss Real Coin
SRR	:	Statutory Reserve Requirement
TCX	:	Tiberius Coin
TRY	:	Turkish Lira
USD	:	United States Dollar
USDC	:	USD-pegged Circle’s stablecoin
USDT	:	USD-pegged Tether’s stablecoin
UTXO	:	Unspent Transaction Output
VR	:	Virtual Reality
VRC	:	VeriCoin
VTC	:	Vertcoin
XTZ	:	Tezos Token
XVG	:	Verge Coin

CHAPTER I

INTRODUCTION

1.1. Background

Cryptocurrencies (cryptos), including Bitcoin, alternative coins (altcoins)[1] (Ammous, 2018; Bonneau et al., 2015), and other crypto types, represent a new innovation in money that has captured the attention of investors, technologists, and economists alike. These new forms of currency offer a dazzling array of features and benefits that promise to revolutionize digital transactions and the digital world. From the barter system to fiat money, money has seen numerous transformations throughout history in response to the need for faster, more reliable, and secure transactions.

In this context, cryptocurrencies offer an exciting new possibility for transferring funds without the need for traditional third parties such as banks, credit cards, and payment gateways (Maghdeed, 2020a). They also feature blockchain technology, which provides robust encryption and the potential to tokenize financial securities, creating trading platforms without the need for intermediaries (Maghdeed, 2020b). In the wake of the 2007 financial crisis and the ongoing COVID-19 pandemic, the interest in and adoption of cryptocurrencies has continued to rise and has seen more adoption from several governmental bodies.

For instance, the US Department of Treasury's Financial Crime Enforcement Network (FinCEN) has issued a guidance report in 2013 that considers "convertible" virtual currencies having a value equivalent to a real currency or is a substitute to a real currency (FinCEN, 2013). The Internal Revenue Service (IRS), also in the US, now recognizes virtual currencies as taxable properties (IRS, 2014). Similarly, the Canadian Revenue Agency (CRA) issued a guide that requests businesses to report any revenues generated from the disposition of virtual currencies (Canada Revenue Agency, n.d.). The Australian Tax Office (ATO) has followed similar path and

[1] Altcoins refer to cryptocurrencies that are alternative (hence the prefix 'alt') to the Bitcoin.

considers cryptocurrencies taxable if a capital gains tax event is initiated from actions such as exchanging, swapping, trading, buying, selling, or gifting (ATO, n.d.).

In addition to their superior features such as faster fund transfers, stronger encryption, enhanced privacy and control, and the removal of financial intermediaries, cryptocurrencies have given rise to new innovative use cases. For instance, smart contracts enable distributed computation, allowing for applications in diverse fields such as supply chain management, real estate transactions, and voting systems. Smart contracts also opened the possibility for innovative document hashing that can be used for tracking intellectual property rights and verifying authenticity of digital assets. Another promising application is the use of cryptocurrencies in charitable donations, where transparency and accountability can be ensured through blockchain technology. Cryptocurrencies have also introduced non-fungible tokens, which were initially designed for providing unique signatures for art, music, and video works. However, these tokens also have the potential to provide an easier approach for the verification of ḥalāl licenses or certificates.

Despite the superiority in their features, use cases, and the role they play in enhancing and securing transactions, cryptocurrencies are not void of issues. Some of these issues are exogeneous and relate to how different categories of people perceive and value the concept of cryptocurrency. Other issues, which are endogenous, relate to some of the features and the model upon which cryptocurrencies are based. Five of the most important issues discussed in the literature are: inconsistencies in the definition and understanding of cryptocurrencies, misconception about their underlying technology, misconceptions that all altcoins are synonymous to Bitcoin (BTC), disputes about the effect of cryptocurrencies on the economy due to insignificant empirical studies, and absence of viable *Fiqh* studies on these issues and other related issues.

1.2. Problem of the Study

Cryptocurrencies is one form of many forms of innovations that emerge today. Technology is at the forefront of playing a major role in enabling these innovations and allowing them to see the light. Like any innovation that arises, there are bound to be issues of misconceptions of the definition of these innovations, misconceptions of the underpinning technologies, and lack of understanding of their socio-economic impact. *Fiqh* studies have widely discussed some of these issues associated with

cryptocurrencies and revealed other issues as well. For example, in relation to determining the definition of cryptocurrency, Abu-Bakar (2017) asserts that the understanding of cryptocurrency and its technology is evolving, and that jurists' opinion should become more informed as they become more understood. On the other hand, the difficulty to model a cryptocurrency system resulted in many several issues. For instance, the literature shows a commonly cited issue whereby cryptocurrencies are thought to be generated by people with unknown identities and are being exchanged via imaginary nicknames (Abu Layl, 2019). This is related to the *Fiqhi* (jurisprudential) issue of *Jahālah* (ignorance) of the issuing entity. On the contrary to that belief, cryptocurrencies are mainly issued through a deterministic code set by its protocol. In contrast, another important issue is that cryptocurrencies are widely thought to have negative impact on economies (Abu Layl, 2019; Al-Yahya, 2019). These disputes are just a manifestation of the lack of significant empirical studies on the matter.

An extensive and intensive analysis of the *Fiqh* discussion on these issues reveals that there are misconceptions about the underlying technology of these cryptocurrencies and misconceptions that all altcoins are synonymous to Bitcoin. Most of these *Fiqh* discussions are normative devoid of any adequate research framework upon which objective analysis of these issues could be done. These observations are considered gaps in the extant *Fiqh* literature related to cryptocurrencies. The present study aspires to address these gaps via developing a contemporary systematic *Fiqh* framework for analyzing the issues of cryptocurrencies.

1.3. Research Objectives

The following are the research objectives of the study:

1. Examine the following four main issues, unified by the overarching theme that an incomplete comprehension can detrimentally influence the legal rulings associated with cryptocurrencies from a *Fiqh* (jurisprudence) perspective:
    1.1. Contention on the definitions of cryptocurrency. There are diverse opinions on what they are.
    1.2. Limited understanding of the technical aspects of cryptocurrency. It is difficult to model cryptocurrencies and understand how they operate technically.

1.3. Misconceptions of equating altcoins to Bitcoin. The differences among cryptocurrencies and their types are often overlooked.
1.4. Cryptocurrency risks. The risks of cryptos are not properly studied and often risks are conflated with *Gharar* (uncertainty).

2. Examine the extent to which the existing *Fiqh* framework has addressed the four main issues of cryptocurrencies stated in **research objective 1** above.
3. Propose a contemporary *Fiqh* framework for analyzing the stated four main issues of cryptocurrencies and validate the viability of the proposed framework.
4. Use the proposed *Fiqh* framework in **research objective 3** to analyze the four main issues of cryptocurrencies.

1.4. Research Questions

The following are the research questions of the study:

1. To what extent are the following four main issues related to cryptocurrencies considered issues from a *Fiqh* perspective?
   1.1. Contention on the definitions of cryptocurrency
   1.2. Limited understanding of the technical aspects of cryptocurrency
   1.3. Misconceptions of equating altcoins to Bitcoin
   1.4. Cryptocurrency risks
2. To what extent has the existing *Fiqh* framework addressed the four main issues of cryptocurrencies stated in **research question 1** above?
3. Is it feasible to propose a contemporary *Fiqh* framework for analyzing the stated four main issues of cryptocurrencies and validate the viability of the proposed framework?
4. How can the proposed *Fiqh* framework in **research question 3** above be used to analyze the four main issues of cryptocurrencies?

1.5. Significance of the Study

The ability of this endeavor to serve the stakeholders of this topic and address their concerns conveys the significance of the thesis. The stakeholders of this topic are no longer confined to Muslims who are closely monitoring the latest *Fiqh* opinions, dealers in crypto markets, and interested individuals and investors. The base of the stakeholders has grown to also include interested researchers, developers of cryptocurrency exchange platforms and service providers, financial technology

(FinTech) companies, regulators and policymakers, and *Sharī'ah* jurists. The very essence of this growing base imparts the significance on the thesis.

Muslim crypto dealers, whether individuals or organizations, and Muslim users of cryptocurrencies who closely follow the latest *Fiqh* (jurisprudence) scholarship can benefit from this thesis by gaining a better understanding of the *Fiqh* implications of using cryptocurrencies and avoiding violations of Islamic ethical principles, such as *Gharar* (uncertainty) and *Ribā* (usury). Specifically, this study can shed light on how cryptocurrencies may introduce *Gharar* and *Ribā* in financial transactions, which can help individuals and organizations make informed decisions that ensure compliance with *Sharī'ah* (Islamic Law) standards.

On the other hand, this study will provide researchers with a wealth of knowledge in the area of cryptocurrencies. In essence, it will offer a comprehensive and structured approach to studying the *Fiqh* implications of cryptocurrencies. The framework to be developed will guide researchers in identifying research gaps and questions related to the *Fiqh* of cryptocurrencies, understanding the existing literature on the topic, and developing new research methodologies that are consistent with Islamic ethical principles. The benefits to researchers are not limited, as the framework can also help them communicate their findings to a wider audience, including policymakers, regulators, and the general public, in an accessible and meaningful way. This is because the study's framework provides a methodical way of perceiving cryptocurrencies and understanding all of their main *Fiqh* issues. This could raise awareness about the importance of incorporating Islamic ethical principles into the regulation and use of cryptocurrencies, potentially leading to the development of more informed and responsible practices in this area.

In light of the comprehensive and structured approach to studying the *Fiqh* implications of cryptocurrencies outlined in this study, regulators and policymakers can greatly benefit from the clear guidance provided by this research in developing regulatory and policy frameworks. The framework developed in this thesis offers a systematic view of the conceptual and operational models of cryptocurrencies and provides a register of *Fiqh* issues that can be instrumental in identifying areas where consumers may be at risk. Consequently, this research can inform the development of regulations and policies that protect consumers and promote the adoption of responsible practices in the use of cryptocurrencies.

Moreover, the outcomes of this study provide valuable insights for developers of cryptocurrency exchange platforms, service providers, and FinTech companies seeking to ensure compliance with Islamic ethical principles. The issue registers developed in this research offer a broad and organized approach to identifying areas for improvement and inspiring the development of new products and services tailored to the needs of Muslim clients while maintaining the utmost level of security. FinTech companies can study the implications of the *Fiqh* issues on cryptocurrencies and identify areas of demand for Islamic-compliant financial products and services related to cryptocurrencies and develop innovative solutions to meet those needs. Such financial products and services related to cryptocurrencies can promote financial inclusion by enhancing access to financial services for Muslims who may have been excluded from traditional financial services, contributing to the growth and development of the industry as a whole.

Most importantly, the deliverables of this thesis will be of great value to *Sharī'ah* jurists who play a critical role in ensuring compliance with Islamic ethical principles in financial transactions. Again, the models developed in this study will serve as a valuable resource for jurists seeking to understand the underlying technologies of cryptocurrencies. The framework will also notably help jurists to analyze the *Fiqh* implications from the legal and ethical dimensions of these cryptocurrencies via a complete and a holistic view of the system. In particular, it will enable jurists to identify potential areas of risk to Islamic ethical principles in the use of cryptocurrencies, and as a result, the framework can assist in the development of guidance and recommendations to promote compliance. Therefore, the insights gained from this study can also facilitate the development of innovative and *Sharī'ah*-compliant financial products and services related to cryptocurrencies. Additionally, the framework can dispel misconceptions and direct jurists' attention to more pressing issues related to the use of cryptocurrencies. The most significant contribution of this thesis can therefore be seen in the advancement it can make in the field of Islamic finance and the expansion of financial inclusion for Muslim communities.

1.6. Design and Organization of the Research

This thesis adheres to a slightly modified IMRaD[2] study structure. Notably, this study first attempts to identify gaps in the literature in order to build a conceptual framework that will address the issues of cryptocurrencies. To validate this conceptual framework, the study then undertakes qualitative research through semi-structured interviews with experts in the field. Subsequently, thematic analysis is employed to extract valuable insights into the strengths and weaknesses of the proposed framework from the collected data. In essence, the adoption of this structured approach is crucial for aligning with the core objectives of the study. To comprehensively cover these research components, the study is organized into the following six chapters.

Chapter I addresses the importance of the topic by providing a brief description of the unique features of cryptocurrencies and what have started the contentious debate among scholars and researchers. This chapter also discusses the problem of the study, sets the objectives, and explicates the significance of this research in addressing its stakeholders.

Chapter II lays the groundwork for the literature and delineates research gaps concerning cryptocurrency-related issues. It is organized into three primary sections. The initial section delves into the historical context of money, exploring its concept through the lenses of traditional conventional economists (here forth will be called mainstream economists), the *Qur'ān* and *Sunnah*, early jurists, and late jurists. The second section scrutinizes contemporary *Fiqh* perspectives on cryptocurrency issues. Subsequently, the outcome is integrated into the concluding section to assess the existing framework's analysis of cryptocurrency-related issues.

Chapter III details the methodology used to propose a contemporary framework and the meticulous approach to validate it. In other words, it discusses the identification of gaps from literature, research design, sample size and sampling technique, the method used for collecting data, precautions taken, theoretical explanation behind choosing thematic analysis as a data analysis technique, ethical considerations, and limitations.

---

[2] IMRaD: an abbreviation for a study format that stands for Introduction, Method, Results, and Discussion

Chapter IV is dedicated to operationalizing the identified gaps by constructing a framework rooted in an in-depth conceptual and operational comprehension of the first cryptocurrency ever. The chapter establishes the prominent need for the convergence of terminologies and the creation of a universal definition of cryptocurrencies. The argument develops to classify the cryptos into six distinct categories. Based on these varied categories, the chapter discusses the synthesis of the information to develop a coherent and comprehensive *Fiqh* framework for analyzing cryptocurrencies.

Chapter V presents and examines the collective findings from the qualitative data while ensuring that the primary study objectives were being addressed. These objectives include an investigation into the main issues and complexities introduced by the concept of cryptocurrencies, an evaluation of the effectiveness of current juristic approaches in addressing these concerns, and an assessment of the proposed framework's validity for analyzing these issues. The significance of this chapter is highlighted by its provision of an optimized framework.

Lastly, Chapter VI is the conclusion of the study, summarizing the whole process of the thesis. The discussion delves into the original contributions made within the research, highlighting distinctive features that contribute to the existing body of knowledge in the field. The conclusion also addresses the possible challenges that might be faced by implementing the framework and the potential prospects and implications of the proposed framework. Subsequently it thoughtfully examines the limitations followed by a discussion on the way forward for future research endeavors. Finally, the chapter extends the discussion to present key recommendations and suggestions for stakeholders involved.

CHAPTER II

LITERATURE REVIEW

2.1. Introduction

This chapter aims to achieve the first two research objectives of this study which are:

1. Examine the following four main issues, unified by the overarching theme that an incomplete comprehension can detrimentally influence the legal rulings associated with cryptocurrencies from a *Fiqh* perspective:
   1.1. Contention on the definitions of cryptocurrency
   1.2. Limited understanding of the technical aspects of cryptocurrency
   1.3. Misconceptions of equating altcoins to Bitcoin
   1.4. Cryptocurrency risks
2. Examine the extent to which the existing *Fiqh* framework has addressed the four main issues of cryptocurrencies stated in **research objective 1** above.

In pursuit of these objectives, this chapter establishes a foundation for the literature and identifies research gaps related to issues surrounding cryptocurrencies. The chapter is divided into four main sections. The first section presents the historical context of money and examines its concept from the perspectives of mainstream economists, *Qur'ān* and *Sunnah*, early jurists, and late jurists. The second section inspects the definition of cryptocurrencies and their characterization. The third section analyzes the contemporary *Fiqh*'s perspectives on the issues of cryptocurrencies, contributing to the achievement of **research objective 1**. The final section evaluates the current framework's analysis of the issues related to cryptocurrencies, thus aiding in achieving **research objective 2**.

2.2. Concept of Money

In the most basic societies, people exchanged there needs through what is known as the barter system. That system is built upon the coincidence of wants among the transacting parties. However, due to the low probability of double coincidence of wants in a highly specialized society, the barter system proves to be an impractical solution for people to carry out their transactions and trade operations. In big societies, what one person needs from another will hardly be fulfilled as the other might not need

what the first owns. The issue is impressively analyzed by Ammous (2018) via three dimensions: coincidence of scales, coincidence of time frames, and coincidence of locations. The first discusses the issue whereby in certain cases it would be impractical to divide a product into smaller units to complete the transaction. As an example, the author quotes a shoemaker who wants to buy a house – it is impossible to buy smaller units of the house proportionate to the value of the shoes while, on the other hand, the owner of the house will most probably not want to trade his house for a large number of shoe pairs. The coincidence of time frames refers to the dilemma posed by exchanging perishable goods with more valuable durable goods. By the time an owner of an apple field collects apples enough to exchange for a house, some apples would have rotten. The last dimension, coincidence of locations, delineates the difficulty/impossibility of transporting certain goods. The author depicts this issue with the example of a house owner who wants to sell his house to buy another house in another location, yet it is known to everyone that houses are not transportable. Furthermore, in such a system, there will be challenges in pricing (Abdullah et al., 2018) the items exchanged and how each will be valued in terms of the other. The problem boils down to the question of "How to move economic value across time and space" (Ammous, 2018). Therefore, there was a need to introduce a medium of exchange that could overcome the shortcomings of the barter system. This medium of exchange is what is called money.

Historically, it was reported that ancient societies used salt, rocks, shells, glass beads, or leather as money. These forms of money are classified as commodity money. As societies developed, so did the means of the production of these forms of money. The ease of their production or extraction was in certain cases detrimental to the value of the money, simply because a sudden deluge of the money in the market meant the money debauched and its value went through a free fall. Eventually, these forms of money were replaced by commodities that had superior characteristics, namely precious metals. Metal commodity money like gold and silver were used as money for more than a millennium. Since the 16th century, gold was deposited with gold-smith bankers and the latter introduced receipts for cash called "Running cash notes" (*Banknotes: A Short History*, n.d.) – receipts certifying that its bearer is entitled for the said amount of gold. These papers were convertible to gold on demand. In the 18th century, these receipts developed into fixed denomination banknotes (*Banknotes: A*

Short History, n.d.) that formed a paper system which is fully backed by gold. Then, in the 20th century, in 1971 specifically, people witnessed a move from the gold standard, giving birth to the current fiat[3] money that is not covered by gold anymore. Although laypersons might have a common picture of what money is, some dissimilarities exist in conceptualizing money among the mainstream economists on the one hand, and the early and contemporary Islamic *Fiqh* jurists on the other hand.

2.2.1. Money from the Viewpoint of Mainstream Economists

Mainstream economists "Define money… as anything that is generally accepted as payment for goods or services or in the repayment of debts" (Mishkin, 2022). This is a broad definition that not only includes currencies, but also encompasses other forms like checks, checking account deposits, debit cards, prepaid cards, and electronic payments through FinTech-based payment systems. The latter is one of the most recent inclusions to this definition. While all other forms (except coins and currencies in the hands of people) involve financial institutions as intermediaries, FinTech-based payment systems eliminate these traditional intermediaries and, instead, utilize technology to fulfill monetary transactions and payments – examples: M-Pesa in Kenya and Orange Money available in 13 African countries, both of which utilize mobile services for the purpose of financial transactions (El Amri et al., 2021).

In contrast to economists, when people talk about money, they usually refer to currency. Currency is one type of money which includes fiat money (like dollar and lira bills) and coins. It is the notes and coins in the hands of people, that is in circulation. Before the existence of central banks, currency forms also included running cash notes and banknotes. Confining money to only currency is utterly incorrect as one will miss other types of money in the form of checks, checking account deposits, electronic payment, and electronic money to name a few. Economists do not have one clear-cut classification for the types of money. Some would classify them in terms of the evolution of the method of payment, like Mishkin (2022), others would classify them according to their debut in history with a general naming that encompasses their specific characteristics which set them apart, like Abdullah et al.

[3] Fiat refers to an authoritative or king's decree. Since the paper money took the form of a legal tender, hence it got its name as fiat money.

(2018). Using the latter classification, Figure 2.1 summarizes the different types of money.

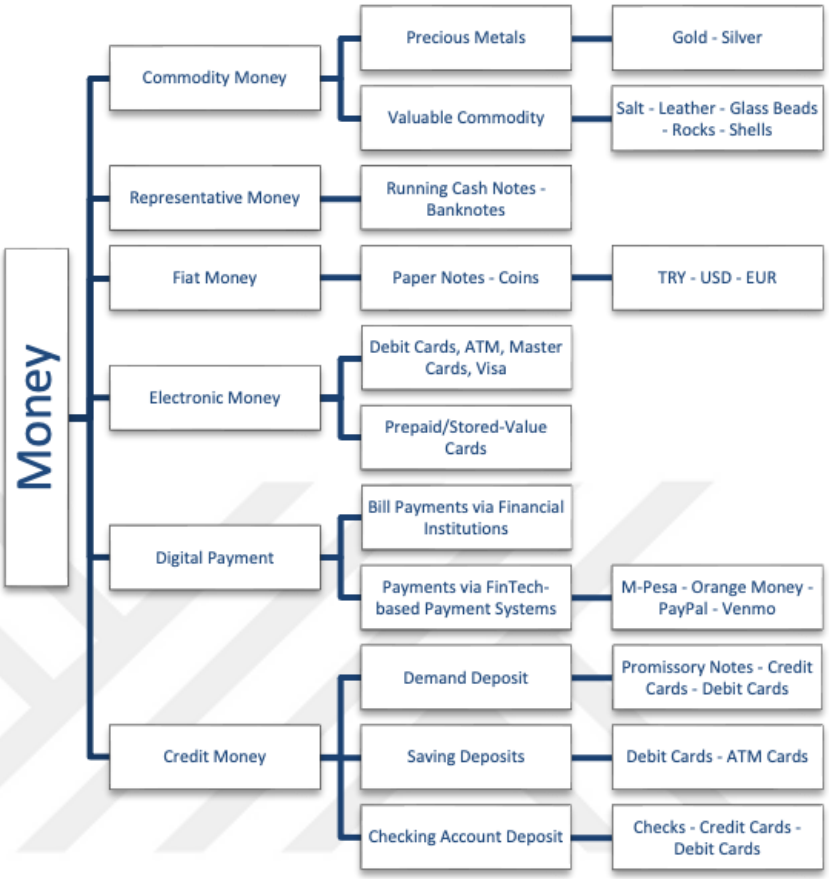

Figure 2.1: Types of Money

Source: Author

In the figure above, we can see the main categories of money according to their appearance throughout history. The first of these is commodity money which involves two sub-categories: valuable commodity (e.g., salt and shells) and precious metals (e.g., gold and silver). The second main category as it appeared in history is representative money which involved certificates that are claims on certain assets usually gold (e.g., running cash notes and banknotes). The rise of the fiat standard made the third main category which concerned printed papers that are not claims on any asset and do not entitle their bearers for their equivalent of gold or silver (e.g., US dollar (USD), Turkish lira (TRY), euro (EUR), etc.… and all their accompanying metal coins). The advent of the internet and outburst of e-commerce introduced the electronic money as a fourth main category (e.g., debit cards, automated teller machine (ATM) cards, visa, and prepaid cards). The development of the financial institutions

and advancement of technology allowed for the age of digital money as a fifth main category which provided people the means for payments digitally (e.g., bill payments and payments via FinTech like M-Pesa). The last category is related to credit money. Although one can argue that this type of category which involved loans has been there long before electronic and digital money, nonetheless this category is very important as it makes the basis for the instruments of monetary policies set forth by the central banks. These central bank instruments will be discussed in section 2.2.1.2 following the discussion of the functions and attributes of money as seen by the Mainstream economists.

2.2.1.1. Functions and Attributes of Money

To function as money, an object "Must be universally acceptable… An object that clearly has value to everyone is a likely candidate to serve as money" (Mishkin, 2022). This indeed indicates that from the mainstream perspective there is no limit for what can be considered money as long as that thing observes the functions of money. There are three main generally accepted functions of money: medium of exchange, unit of account, and store of value. Of the three, medium of exchange is the primary function. It relates to being widely accepted in exchange for goods and services. Unit of account is a standard numerical unit that measures the values of things. In a barter system, comparing the worth of one product in terms of the other is easy because one would have to remember only one exchange rate. With three products, comparing each to the other, one will have to remember three exchange rates. However, with ten products, it becomes impracticable and very difficult to remember because there will be $(9 + 8 + 7 + 6 + 5 + 4 + 3 + 2 + 1) = 45$ exchange rates! The number of exchange rates can be generalized to N products:

$$\frac{N(N-1)}{2}$$

But having a unit of account, eliminates the above complication and the price of all products will be compared to it. Therefore, with N products, one would only need to know N exchange rates. The last function, store of value, refers to the money's resistance to volatility and its ability to remain stable. If it cannot remain stable over the long term, it cannot be accepted as a means for paying debts. Strict it may seem; it is observed though that mainstream economists are lax on this function when it comes to paper money. The fiat money, since 1971 when paper money no longer was backed

by gold or any other asset, hardly can satisfy this function, yet it is accepted by the economists as currency money.

On the other hand, mainstream economists (traditional conventional economists) have suggested six main attributes of money: durability, portability, divisibility, homogeneity, fungibility, and counterfeit resistance (Abdullah et al., 2018). Firstly, durability means money has to last for a long time intact from wear and tear. That's why perishable commodities like apples cannot and were not taken as money in the ancient days. Secondly, portability means the ease of carrying money around which has prominent effect on the efficiency of transacting. According to the Mainstream economists, this attribute is one of the factors that carried people to move away from using gold and silver. The precious metals are heavy to carry around. On the authority of Mishkin (2022), for a large purchase such as a house, one would have to rent a truck to transport the money coins (gold or silver)! Noticeably, this is very exaggerated. As of 11th July 2023, an ounce of 24K gold is priced at about USD 1,937.09. Thus, a \$200,000 house will need $\frac{200{,}000}{1937.09}$ ounces of gold. This means you will need short of 104 ounces of 24K gold. An ounce of gold is less than 29 grams. It follows then that a \$200,000 house will not cost more than 3 kilograms of gold. Evidently, carrying such a weight is very much manageable, though inconvenient, and a truck is definitely not needed. Thirdly, money must be divisible in order to conduct transactions for the trivial things and cheap products (Abdullah et al., 2018). Fourthly, money has to be homogeneous; its units must be standardized and homogeneous (Abdullah et al., 2018). This attribute allows it to determine its value and helps fulfill the fifth attribute. Fifthly, money has to be fungible; all its units must be identical and of equivalent values and therefore each unit is easily replaceable by the other (Abdullah et al., 2018). Sixthly, money should be counterfeit-resistant; faking its units should be almost impossible or extremely difficult (Abdullah et al., 2018). Any attempt to lower the caliber of the money should be easily detectable.

The openness of mainstream economists to embrace anything as money, provided it gets universally accepted, with no reservations has profound implications on any future development to money. The embracement of new forms of money is comparatively faster than in its Islamic counterpart. However, this openness has implications on the fractional reserve banking (FRB) system. The existence and conception of FRB system have very eminent and serious repercussions on shaping the economic monetary

policies and their instruments and on the establishment of new forms of money. In section 2.2.1.2 the FRB system will be defined and explained followed by exposing one of its main byproducts which is the partial creation of money. Subsequently, within the same section, a critical examination of the impacts of the FRB system on the economy will be undertaken, substantiated by research.

2.2.1.2. The Fractional Reserve Banking System

The birth of central banks to control and regulate the financial and economic stance of a country gave rise to the FRB system. In order to manage liquidity and curb the possibility of solvency of banks, the system stipulates that commercial banks should have a ratio of their liabilities (deposits made by their clients) as reserves in the central bank. The remaining can be loaned to their clients. Being one of the monetary policy instruments, the ratio, which is called statutory reserve requirement (SRR), is determined by the central bank to control the money supply in the market. It follows then that not only central banks can create money through the printing of currencies, but also the retail banks contribute to the making of money via interest on loans. Two main models in the mainstream economics are used to describe the money creation process in retail banks.

According to the money multiplier theory, retail banks are passive in the sense that loans will only be provisioned on the condition that clients approach the banks to open deposit accounts. Once there are deposits, retail banks will be able to loan out each deposit fully less the SRR. For every loan issued, with that model, there is a deposit counterpart created into the borrower's account. That deposit is now ready to be fully used, except for the reserve, by the bank for loans. This cycle can go further down producing more and more new credit money out of thin air. However, in their article published in the Bank of England Quarterly Bulletin, Mcleay, Radia, & Thomas (2014) describe the money multiplier model as a misconception. They explain that rather than banks receiving deposits from household savings and then lending them out, it is actually lending that creates deposits.

Conversely, this brings the discussion to the other model that explains the creation of money by commercial banks. This model is the post Keynesian endogenous money theory. In this model, banks actively provision loans at will regardless whether they have the deposits or not because they can always later acquire the money they have to

loan from the market or the central bank (Etzrodt, 2018). As such, central banks have very limited means to control commercial banks' creation of money. The determination of money supply, therefore, transfers from the hands of the central bank and the issue becomes "That banks are responsible for creating the nation's money supply" (Jackson & Dyson, 2012). Although Mcleay et al. (2014) believe the contrary and that the central bank still owns the instruments (mainly the interest rate) to control the supply of money, it is interesting to note that central bankers like Mervyn King, Governor of the Bank of England, VítorConstâncio, Vice President of the European Central Bank, and PitiDistayat, Bank for International Settlements, admit to the accuracy of the endogenous money theory (Etzrodt, 2018).

In reality, the financial system is structured in order to make maximum profits. The lower the reserve rate, the more banks are free to loan out the money and the higher are their profits. Should the banks loan out money without consideration to the availability of customers' deposits, the profits will even be higher. Commercial banks therefore tend to opt for high-risk endeavors that are not compatible with their task to ensure low risk functions for their customers. Therefore, commercial banks tend to play at the verge of the realm of failure. A failure of one bank has profound effect on others which can carry the whole system into a domino effect of disasters. Failure of private banks can lead to a long lasting depression (Etzrodt, 2018).

The cry about the consequences of the FRB system has been outlined by many researchers and economists, and many have called for reforms, of which some examples follow. Merkel (2020), for instance, described the inherent instability of a banking system based on money-creating fractional reserve banks because they undermine the mechanism by which the roles of money act as stabilizing forces. Moreover, using a multi-agent-based computational model, Monett & Navarro-Barrientos (2016) showed that the minimum reserve rate is one of two contributors to the insolvency of a bank, suggesting it as a likely destabilizing economic force. In order to combat the instability instilled by the FRB system, many sets of plans have been devised to transition to a full reserve banking. For example, the 1930s Chicago Plan recently revisited by Michael & Jaromir (2012), the Positive Money plan for monetary reform (Jackson & Dyson, 2012), Kay's (2009) Narrow Banking plan, and Limited Purpose Banking plan (Kotlikoff & Goodman, 2009). What all these plans have in common:

> *Is the fundamental point that banks will no longer be able to create money through credit and not face the associated risks… the focus of all the plans is on the supply of money and ensuring that imprudent banks fail without threatening the rest of the banking system or the public purse* (Dow et al., 2015).

In summary, in their texts, mainstream economists are open to what can be considered money as long as it satisfies the three functions – medium of exchange, unit of account, and store of value – and as long as it is generally accepted for the payment of goods or services or the repayment of debt. Currency is one category of money which relates to the physical representation of money in circulation and in the hands of people like paper money and coins (currently the fiat money). Yet, if we evaluate the fiat money over the functions of money, we find that it hardly can satisfy the 'store of value' function. Mainstream economists are silent about this issue, and, despite this fact, they still consider fiat currencies as money.

The move away from the gold standard gave space to non-backed currency money and gave rise to central banking and the FRB system. The whole system is built on the capitalist view of money that it can be a commodity which can grow and earn return in the form of interest rates. While the central banks are presumably the authority for the money supply (they do print currencies), they however have left the creation of the bulk of money in the form of loans to commercial banks. The partial supply of money by the commercial banks in the FRB system is heavily believed to be the cause for periodical financial instabilities. In fact, private banks can enhance profits, yet elevate risks for the broader society via fueling bubbles through FRB and securitization (Etzrodt, 2018).

2.2.2. The Concept of Money in the *Qur'ān* and *Sunnah*

A key difference between the *Sharī'ah* perspective of money and the mainstream view is the return on money. "Unlike in mainstream economics, money cannot be considered a commodity on its own in Islam and thus, cannot be entitled to any return when traded or loaned" (Abdullah et al., 2018). A clear and thorough study on the *Sharī'ah* perspective of the functions of money and its *Sharī'ah* implications will lead to profound conclusions on defining cryptocurrencies.

In *Qur'ān* and *Sunnah*, we have a few texts that discuss matters of pricing, monopoly, *Ḥisbah* (Market Ombudsman) (Kahf, 2014), and a few that address money and currencies. Actually, the primary Islamic texts do not directly either mention the characteristics and functions of money and currency. In fact, the distinction between money and currency is not evident in the *Qur'ān* or *Sunnah* and that's because almost all money was in the hands of people when no financial institutions existed at the time. Therefore, there is no mention for a word equivalent to currency. Historically, at the time of the Prophet (ﷺ) the people had no other forms of money other than gold and silver (in addition to the barter system) and thus the distinction between money and currency seems to be meaningless. To make a significant contribution through the examination of the texts, one can project today's agreed characteristics and functions of money on the primary Islamic texts in an attempt to check whether all or some of these functions of money are approved. Through objective analysis, subject to the exegesis set forth by our early and current scholars, one can make valuable conclusions.

2.2.2.1. Concept of Money in the *Qur'ān*

The Arabic equivalents of gold, silver, price, buy, sell, their synonyms, and derivatives were used to examine the *Qur'ānic* text for any mentions of money. It is worth noting that the Holy *Qur'ān* does not use the Arabic word *Nuqūd* for money, but points to it explicitly in exactly three places. The first is in *Sūrah* 'āl-'Imrān:

> *Among the people of the Book there is one who, if you entrust him with a heap (of gold or silver), will give it back to you; and among them there is one who, if you entrust him with a single Dīnār (a coin of gold), he will not give it back to you, unless you keep standing over him…* [*Qur'ān* 3:75].

Dīnār is a minted coin of gold used as money since the pre-Islamic era and its use lasted after Islam, albeit went into many transformations in shape, size, weight, and quality. Gold is one of two main precious metals from which monetary coins were made. Second to gold, silver is the other precious metal from which monetary coins were made and it makes the content for the second explicit mention of money in *Qur'ān*, "And they sold him for a paltry price, for a few countable *Dirhams*, and they had not much interest in him" [*Qur'ān* 12:20]. *Dirham* is a minted coin of silver. We can see that *Dirham,* and by analogy *Dīnār,* is a coin that has been known at least as

far back in history as the times of the Prophet Yūsuf (ﷺ). A couple of things can be deduced at this stage. First, this verse clearly shows the function of money as a medium of exchange since the brothers of the Prophet Yūsuf (ﷺ) sold him to the wayfarers (Al-Qurṭubī, 1964a, p. 155; Al-Ṭabarī, 2001a, p. 50) in return for a few silver coins. Second, it is worth noting that this verse points to an in-kind exchange, that is the price was declared in quantity of the coins and not by weight[4]. An implication of this is that these silver coins were used as a unit of account where things were priced according to the coins, hence the other function of money. The latter is very evident with the *Qur'ānic* description "Paltry price". The third explicit mention of money is in *Sūrah* al-Kahf:

> *In this way We raised them up until they asked each other. One of them said, 'How long have you tarried (asleep)?' They said, 'A Day, or part of a day.' They said, 'Your Lord knows best how long you have tarried. So, send one of you with this silver (coins) of yours to the city and let him find which food is the purest, and then bring provisions from it. And he must act in polite manner, and do not let him give you away'* [*Qur'ān* 18:19].

Despite consisting of a few lines, the above verse remarkably allows us to make endless interpretations. Perhaps all of the functions of money known today are most prominent here. To put things into context, the word 'silver' in that verse needs further interpretation. In the original Arabic revelation, the word is 'بِوَرِقِكُم' (read *Biwariqikum*), which if stripped from the extra letters while keeping the primal ones becomes 'وَرق' (read *Wariq*). Literally, the word means both raw and minted silver ("Ta'rīf Wa Ma'nā Wariq Fi Qāmūs Al-Kul - Qāmūs 'Arabī 'Arabī," n.d.) where both meanings are equally likely. However, from the exegesis of the *Qur'ān* we know that this verse alludes silver to minted coins. This is evident from the story of the young man, elected by the group of the people of the cave, who went back to his city, under cover, to buy them some food. The silver coins he took with him to exchange for food exposed him because they were minted currencies that had the face of the old infidel king Daqnayus inscribed in them (Al-Ṭabarī, 2001b, pp. 196–199). Evidently then, the

[4] Texts show us that both in weight and in kind were used for exchange during the time of the Prophet Muḥammad (ﷺ).

word *Biwariqikum* denoted minted silver coins. Consequently, the money was used as a medium of exchange since the young man was paying it in return for food. The reaction of the sellers and people in the market was unexpected by the youth because the coin presented was unfamiliar to them, triggering the thought that the youth has found a treasure! So, they terrified him while dragging him to the authorities with the intention that he shows them where the silver was hidden. A couple of inferences can be made out of this incident. First, the people in the market demanded for more out of their greed to acquire a share of the so-thought treasure and not because the payment was not sufficient. That indicates that the few coins presented were in par with the food requested; hence the coins were used as units of account. Second, the people's zeal for more suggests the great value they entrusted to the unfamiliar coins where the trust stemmed from the fact that they were made of silver. It is worth noting that these coins have lived at least 309 years, the period for which the people of the cave have tarried. This is just but a clear evidence from *Qur'ān* that silver coins function as stores of value. Of course, since this is the case with the less valuable of the two precious metals, it follows that gold will function as a store of value as well.

Besides the explicit mentions, *Qur'ān* provides several tacit references to money. In its implicit form, the *Qur'ān* reveals the importance of the two precious metals, gold and silver, to people. For example:

> *It has been made attractive for the people to love the desired things: women, children, heaps of gold and silver, branded horses, cattle, and tillage. That is an enjoyment of the worldly life; but with Allah is the finest destination* [*Qur'ān* 3:14].

In the above verse, people disagreed on who made the worldly desires attractive; some (like 'Umar bin al-Khaṭṭāb as narrated by al-Bukhārī) said that Allah made it attractive, while others (like al-Ḥasan) said that it is the work of satan (Al-Qurṭubī, 1964b, p. 28). Nevertheless, the attractiveness to these desires, including gold and silver, is a fact since the inception of life in this world. The importance of gold and silver stems from their attributes that make them the best choice for fulfilling the needs of people. *Qur'ān* indicates some of these needs in several verses. Table 2.1 below enumerates some of these verses and delineates the needs fulfilled by gold and silver as indicated by *Qur'ān*. As can be seen from these verses, the use of gold and silver ranges from using them as adornments, as a means for payment, and as an indication of authority. An

implication of these *Qur'ānic* verses is the attributes of gold and silver that make them suitable for these usages. What was definitely clear to the people at the time is gold and silver's durability, portability, shininess (thus attractiveness for adornments), and homogeneity. These are obviously the same reasons why people today still use them for the same purposes and needs.

Table 2.1: *Qur'ānic* Indications of People's Needs Fulfilled by Gold and Silver

Verse in the *Qur'ān*	Needs Fulfilled
"So why were the bracelets of gold not sent down to him…" [*Qur'ān* 43:53].	▪ Bracelets of gold indicate authority ▪ Gold is used as adornment
"Indeed, those who disbelieve and die as disbelievers, even an Earth-full of gold shall never be accepted from any of them, even if one were to offer it as ransom…" [*Qur'ān* 3:91].	▪ Gold is used for payment (ransom payment)
"… and they will be adorned by bracelets of silver…" [*Qur'ān* 76:21].	▪ Silver is used as adornment

Source: Author

The significance of gold and silver for people will last forever, this is why they (especially gold) are still considered by people as safe-haven and this is why they are the constituents from which vessels, adornments, bracelets, and cups are made for the believers in paradise.

2.2.2.2. Concept of Money in the *Sunnah*

From *Sunnah* it suffices to mention three important *Ḥadīths*. The remaining *Ḥadīths* on the topic will be the subject of the next subsection since the early scholars heavily depended on them to shape their thoughts on the issue of money. The first of the three *Ḥadīths* that will be discussed here demonstrates the significance of money in Islam. The second one sets apart the Islamic concept of money from mainstream's concept. The third *Ḥadīth* has profound implications on the functions of money.

The first *Ḥadīth*, narrated from 'Alqamah bin 'Abdullah from his father, states: "The Messenger of Allah (ﷺ) forbade breaking the coins of the Muslims that are in circulation among them, without any necessary reason" [*Ḥadīth* 2263] (Ibn Mājah, n.d., p. 761). Although the degree of this *Ḥadīth* is weak, yet it aligns with the saying

of Sa'īd bin al-Musayyib[5] (*Ḥadīth* 37): "Breaking[6] gold and silver is part of working corruption in the land" (Al-Aṣbaḥī, 1985, p. 635). Kahf (2014) argues that an implication of this is to provide sufficient liquidity in the market. The reason for that is because breaking the coins causes them to become invalid and eventually leads to deterring them from circulation. Another important implication is to prevent any means for cheating. Some were breaking the coins in order to purchase things, presumably with the requested quantity of coins as a value for that thing, however with less weight; since people were buying in-kind and in-weight, this had the effect of buying things with less weighted coins (an act of deception and fraud) while keeping what has been broken for future purchases or to make them into adornments and jewelry. While this *Ḥadīth* makes the foundation for the argument for state's sole control on money and currency, we can look at it from the lens of attributes that money should possess. This *Ḥadīth* implicates that an essential attribute of money is its homogeneity which helps in avoiding any attempts of cheating or imbalanced sales. Also, durability can be deduced because non-lasting perishable things cannot keep in circulation and cause the breaking of the currency.

The second *Ḥadīth* is the one reported by 'Ubādah ibn Al- Ṣāmit as narrated by Muslim (No. 1587) that Allah's Messenger (ﷺ) said:

> *Gold (is to be paid for) by gold, silver by silver, wheat by wheat, barley by barley, dates by dates, and salt by salt, like for like and equal for equal, payment being made on the spot. If these classes differ, sell as you wish if payment is made on the spot* (Al-Ḥajjāj, 1955, p. 1211).

This *Ḥadīth* specifies money, depicted by gold and silver, as two of the six *Ribawī* (If rules aren't followed carefully, then the transaction can lead to usury) items. This

---

[5] Sa'īd bin al-Musayyib is one of the followers who lived among the companions of the Prophet (ﷺ), having the chance to see some of them and hear from others. He is considered the master of the followers at his time due to his great knowledge and is considered one of the seven jurists.

[6] Some people used to cut a small piece of the coin which allowed them to have the advantage of buying the same amount of a product as a full coin and also benefit from the additional silver or gold they cut.

means that when exchanged with the same genus (like gold by gold or silver by silver), money has to be equal in amount (forbidding the increase of one over the other, so eliminating *Ribā al-Faḍl*) and must be paid on the spot during the exchange session (forbidding the delay of one paying one of the items exchanged, so eliminating *Ribā al-Nasā'*). However, if the genus differ (like gold by silver), equality becomes unnecessary and only the condition of payment on spot holds. In contrast to the mainstream economists' concept of money, Islam does not only suffice with the condition that money has to be generally accepted as a means for payment of goods and service or repayment of debt, but also imposes strict rules on its exchange. As such, the conventional thought of the time value of money does not hold in Islam. Money cannot be treated as a commodity and therefore is not entitled for return. Consequently, what Islam achieves is the balance in transactions among the parties in which there is no winner on the expense of the other. This is further demonstrated by the third *Ḥadīth* narrated by both al-Bukhārī (No. 2188) and Muslim (No. 1594) where Abū Sa'īd al-Khudrī reported:

> *Once Bilal brought Barnī dates (spherical yellow dates of high quality) to the Prophet (ﷺ) and the Prophet (ﷺ) asked him, 'From where have you brought these?' Bilal replied, 'I had some inferior dates and exchanged two Sa's of it for one Sa' of Barnī dates in order to give it to the Prophet; to eat.' Thereupon the Prophet (ﷺ) said, 'Beware! Beware! This is definitely Ribā (usury)! This is definitely Ribā! Don't do so, but if you want to buy, sell the inferior dates for money and then buy the superior kind of dates with that money'* (Al-Bukhārī, 1993, p. 813; Al-Ḥajjāj, 1955, pp. 1215–1216).

While this *Ḥadīth* is used as the basis, among others, for forbidding *Ribā al-Faḍl*, we can look at it from another perspective related to money. One has to note that there is no known fair way to valuate a commodity with another given the tons of commodities available that one can exchange with each other. This results in an imbalance in the transaction where one party gains while the other loses. In Islam, balanced transactions where none lose are very important. Therefore, exchanging with the same genus from one of the *Ribawī* items should be in equal weight. The Prophet (ﷺ), therefore, asked Bilāl to sell the inferior dates in another transaction with some other genus or money and then buy with those the high-quality dates. This has the effect of valuating each product correctly, accurately, and fairly. An elemental inference here is the function

of money as a unit of account for which others can be priced and valuated correctly. On the other hand, the function of money as a medium of exchange is crystal clear from this text. While not as clear, the function of money as a store of value can indirectly be recognized: since price stability is quintessential, money will not be able to serve this purpose if it was not a store of value.

In summary, although there are a few texts on money, its functions, and attributes, nonetheless, *Qur'ān* and *Sunnah* provided strong grounds from which Islamic jurists were able to identify what money is, its functions, and attributes. Analyzing the texts in the light of the interpretations and exegesis transmitted to us can help us extract insightful conclusions about money and its characteristics from the worldview of Islam.

2.2.3. Concept of Money in the Views of Early Jurists

The concept of money and its *Sharī'ah* implications has been the subject of interest for the early jurists from which one can find a plethora of such texts. The diversity of the gold and silver coins since the time of the Prophet (ﷺ) led the jurists to exert effort to come up with rulings that comply with the *Sunnah* while observing the rules of *Zakāh* (alms), inheritance, or blood money. As such, most of these writings have taken a jurisprudential dimension. As a matter of fact, the topic has primarily been but discussed in the jurisprudential, *Fiqh*, books. One can usually find these discussions under the book of *Zakāh* from each of these *Fiqh* books and, to a lesser extent, under the book of sales and book of exchange.

Unlike in the mainstream thought, what makes money from the Islamic perception was not discussed from the perspective of the functions and attributes of money. Rather, the focal point of their arguments emerged from a *Fiqhi* standpoint. Mainly, the early scholars debated whether the monetary *Ribawī* items could be extended to different forms of money not mentioned in the Prophet's (ﷺ) *Ḥadīths*. However, according to al-Sarakhsī (1989), the jurists of the metropolises, except for Dawūd from the late jurists and 'Uthmān al-Battī from the early jurists, agreed that the rule of *Ribā* is not confined to the six *Ribawī* items, but it extends to other items. Besides that, the early jurists had their say on who owns the right of producing these coins. Nonetheless, a remarkable account of the functions of money and the issues of the barter system, indeed, was found in the Islamic literature five centuries before Adam Smith

mentioned them. Al-Dimashqī (1900) provides an in-depth explanation of the difficulties faced by the barter system that hinder the double coincidence of wants. He notes the high possibility of the absence of double coincidence of time and absence of double coincidence of scales, the need to know the value of things and be a price for others that can be used for exchange, the rotting characteristic of plants and animals being the reason for not taking them as money, and the rapid rusting of iron and copper that makes them unsuitable for being the source of money. Clearly, his above argument touches upon all the functions of money: medium of exchange, unit of account, and store of value, though not directly clear. The above discussion also outlines two of the main attributes of money, namely being durable and divisible. Furthermore, on discussing the virtues of gold and silver, Al-Dimashqī (1900) exposes one of the most critical attributes of money, namely being counterfeit-resistant. He articulates that both of these metals accept marks that preserve them and possess features that safeguards them from adulteration and fraud.

Coming to the key points of their discussions, a considerable number of the early jurists from different sects confined money to gold and silver. For example, this is generally the thought of Ḥanafīs as can be found in article 130 in the civil code of the Ottoman Empire that states that *Nuqūd*, plural of *Naqd* (which is the Arabic word for money), is gold and silver (Pasha, n.d.). Conversely, Shāfi'īs state that, unlike gold and silver, *Fulūs*[7] do not require *Zakāh* nor do they act as values/prices for things (Al-Shafi'ī, 1990). Similarly, Al-Maqrīzī (1609), a Shafi'ī jurist and historian, upheld that *Fulūs* were never considered money; he only approved of gold and silver as forms of money. Similar to this opinion, Al-Nawawī (1991), another Shafi'ī jurist, disapproved *Fulūs* as a form of money. In the Ḥanbalī sect we find Al-Bahūtī (1968) maintained that *Fulūs* are like traded commodities: *Fulūs* are subject to *Zakāh* and it is not permissible to pay it from them. The majority of jurists are of the opinion that *Zakāh* of traded commodities should exclusively be paid using money. This Ḥanbalī opinion aligns with the other aforementioned opinions where *Fulūs* can't be considered money. Also, Al-Dimashqī (1900) argued that only a mute property, yet not all, can take the

[7] *Fulūs* are coins minted from copper and used for the purchases of the cheap fractional products that cannot be bought by gold or silver (Al-Maqrīzī, 1609).

form of money. He confined this to precious metals like gold and silver and explained why they are preferred over others.

In contrast, there is a group of other scholars from various sects who accepted other forms of money. For example, Mālik bin Anas stated, "Should the people have accepted leather as coins and corpus among them, I would have reprehended its sale with gold and silver on deferred payment" (Al-Aṣbaḥī, 1994). This is a clear consent that he would not object about a form of money different from gold and silver and that has general acceptance among the people.

Likewise, when the Muslims suffered from the lack of gold and silver at the time of the caliph Umar, he was about to mint coins from the skin of camels (Al-Balādhurī, 1988). But he retracted his opinion when his companions foresaw the negative effect of it which will eventually lead to the extinction of camels. This means that caliph Umar had no legal reservations on introducing a new form of money alternative to gold and silver.

This view is also held by one of the most prolific writers on the topic: Ibn Taymiyyah who is a prominent Ḥanbalī jurist. He observed that there were no limits on the *Dirham* or *Dīnār* during the Prophet's (ﷺ) time, nor it was minted – instead it was brought readily minted from the infidel's lands, add to it that people were using a mix of different sizes (big and small) and different weights (8, 6, and 4 Dāniq[8]) for the coins and that the people at the time of the Prophet (ﷺ) sometimes dealt with them in kind and sometimes in weight (Ibn Taymiyyah, 2004a). Therefore, he said that in the standards of *Dirham* and *Dīnār*, the people use what is customary among themselves; so what they have accepted to be a *Dirham* then a *Dirham* it is and what they have accepted to be a *Dīnār* then a *Dīnār* it is, regardless whether they were of one minting kind or more or whether they were unadulterated or not (Ibn Taymiyyah, 2004a). Besides gold and silver, Ibn Taymiyyah did not have any reservations on the use of minted copper as money among people. He argued that the sultan should mint *Fulūs* that has a fair value for people's transactions without causing injustice to them (Ibn Taymiyyah, 2004b). So, the sultan should not trade with *Fulūs* nor should he cancel

[8] *Dāniq* is a weight measure that is equal to the weight of 8.4 unpeeled medium-sized barley grains that have their extended ends cut (Al-Maqrīzī, 1609).

what is in their hands to replace it with other minted *Fulūs*, instead he should mint while keeping the same value without any profits (Ibn Taymiyyah, 2004b). Otherwise, Ibn Taymiyyah believed that the latter fitted the description of the *Ḥadīth* narrated by Abū Dāwūd that the Prophet (ﷺ) forbid breaking Muslim coins unless there is a problem (Ibn Taymiyyah, 2004c).

On the other hand, other early jurists emphasized the importance of who owns the right of producing money. Some have delineated that minting money is the responsibility of the state. For example, al-Nawawī, a Shāfi'ī jurist, restricted the production of money to one source only. According to him, it is reprehensible for the *Imām* (head of state) to mint impure coins (*Dirham*), as well as it is reprehensible for people to mint coins even if they were pure because it is the responsibility of the *Imām* (Al-Nawawī, 2003). It is worth noting, though, that he considered minting of coins by an entity other than the state reprehensible rather than forbidden.

2.2.3.1. Variation of Early Jurists' Opinions on the Concept of Money

A bit of a historic context will help to understand the differences among the early jurists' thoughts about the concept of money. At the time of Quraysh, *Dirham* and *Dīnār* were both weighed and used in kind. Figure 2.2 is a graph that depicts some of the various weights used.

When the Prophet (ﷺ) came, he approved these weights. He imposed *Zakāh* such that for every 5 *Ūqiyyah* (each *Ūqiyyah* is an ounce or equivalent to 40 *Dirhams*) of pure unadulterated silver, 5 *Dirhams* are given and for every 20 *Dīnār*, half a *Dīnār* is given for *Zakāh* (Al-Maqrīzī, 1609). The coins remained as is until the caliph Umar ordered special coins to be minted in his eighth year of ruling (Al-Maqrīzī, 1609). However, historians agree that these were not minted by Muslims, rather they were adulterated silver coins with high percentages of copper minted for Muslims on their request. Since then, the coins minted for Muslims went into several development where their weights and sizes changed with every ruler until the reign of 'Abd al-Malik bin Marwān. By his time, there existed big and small silver coins with various weights which caused an imbalanced impact on *Zakāh*. People were calculating their *Zakāh* half from the big coins and half from the smaller ones (Al-Maqrīzī, 1609). Therefore, 'Abd al-Malik took the decision to standardize the coins and unite their weights and sizes. His *Dirham*, the first Islamic coin as considered by historians, was mid-sized between the

big and small coins and its weight was designed to be 6 *Dāniq* (the big coin's weight was 8 *Dāniq* and the small coin's weight was 4 *Dāniq*).

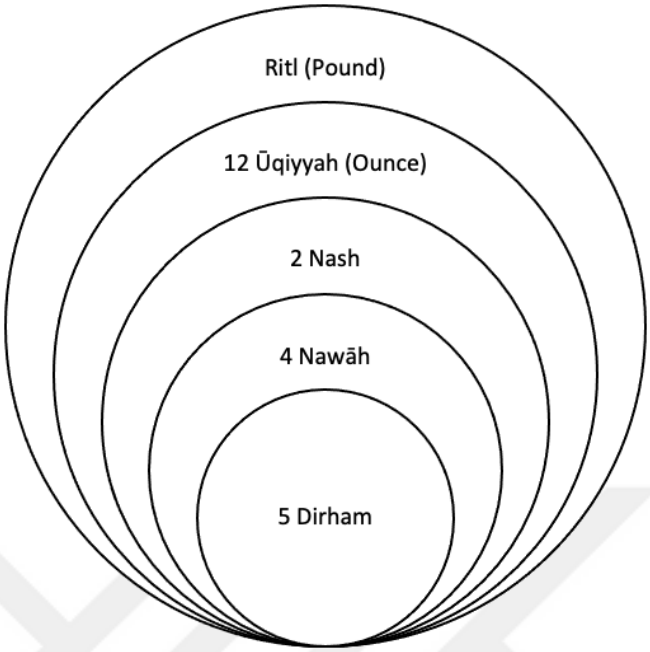

Figure 2.2: Pre-Islamic Weights[9]

Source: Author's illustration adapted from Al-Maqrīzī, 1609

In the design of his *Dirham*, 'Abd al-Malik maintained the *Sunnah* of the Prophet with respect to *Zakāh* (Al-Maqrīzī, 1609). Almost all subsequent rulers sought their glory by minting their own *Dirham* while giving them suffix names that either contained their names or the region where they were minted. Ever since then, the silver coins experienced constant adulteration which led to corruption that creeped into the royal courts. Interestingly, al-Maqrīzī witnessed the economic crisis suffered by the Egyptians. He alluded this crisis to the minting of non-gold non-silver coins.

From this historical account, we can deduce the reasons for the differences between the jurists. Considering *Dirhams* and *Dīnārs*, Ibn Qayyim al-Jawziyyah (1991) stated that a group of jurists said that the cause (for being *Ribawī* items) is due to the fact that they are weights, and this is the madhab of Ahmed bin Ḥanbal in one of the two narrations about him, as well as the madhab of Abū Ḥanīfah. The other group said that

[9] Each *Ritl* = 12 *Ūqiyyah*, each *Ūqiyyah* = 2 *Nash*, each *Nash* = 4 *Nawāh*, and each *Nawāh* = 5 *Dirham*. So, one *Ritl* = 480 *Dirham*

the cause is due to being values (prices), and this is the opinion of Shafi'ī, Mālik, and Ahmed in the other narration about him. While Al-Maqdisī (1997) maintained that the former narration of the opinion in the madhab of Ahmed bin Ḥanbal is the most famous, on the other hand Ibn Qayyim al-Jawziyyah (1991) articulated that the latter was the correct one. The jurists further disagreed on the second cause, which is related to valuation and pricing. While some were of the opinion that the cause was absolute pricing, the majority were of the opinion that the cause was price predominance. Absolute pricing means that only when something is used as a medium of exchange, it will be considered money. So, gold or silver are considered prices when they are minted and used for exchanges; but as jewelry they are no longer considered prices. Price predominance, on the other hand, means that a thing can sometimes take the form of commodities like jewelry and cups, but what is predominant about their use is the fact that they are used as prices and medium of exchange.

As explained, this second opinion of the cause of pricing is the one undertaken by the majority of the jurists. Therefore, according to Al-Maqrīzī (1609), only gold and silver should be accepted as money because only these can be prices for sales and values for any work. The reason for this thought is partly built upon his experience of the ill-effects of minting coins which are not gold or silver. And partly because he was of the opinion that gold and silver were prices by nature. Per se, *Fulūs* gets excluded from this definition because they are not prices by nature. On the Mālikī *Fiqh*, Al-'Adawī (1994) states that should the price predominance be considered the cause, then the new *Fulūs* are excluded and therefore will not be considered *Ribawī*. This is shared by many jurists as well. Moreover, the implications of money on *Sharī'ah* rulings related to *Zakāh*, blood money, the punishment codes like stealing limits for amputating the hand, and inheritance cast their shadows as well. Almost all of these legal rulings have been set by the *Dirham* in the Islamic primary texts. This forms a strong reason for why this group of jurists will not approve any form of money other than gold or silver.

In contrast, considering the 'absolute pricing' cause makes *Fulūs* (and any other minted metal or thing used as prices and medium of exchange) fall under the definition of *Ribawī* items. Also, some jurists in this group noted that there was no minting at the time of the Prophet (ﷺ) and that money is what the people have generally accepted. What makes gold and silver prices and values for other items is people's convention (Al-Jaṣṣaṣ, 1994). *Fulūs* were widely used at the time of the Prophet (ﷺ) and after him

and people were using them as exchange for goods. Therefore, like gold and silver, *Fulūs* is subject to *Zakāh* and all related *Sharī'ah* ruling implications. In addition, the intention of the caliph Umar to make the skin of camel money is taken as an evidence that money can be what people generally accept and is not confined only to gold and silver.

2.2.4. Money in the Views of Contemporary Jurists

From the perspective of current scholars and jurists, the definition of money in terms of functions is more or less the same as the early jurists and the mainstream economists. Though approved, not all the functions had an explicit mention in some of these definitions. Some of these definitions would explicitly mention only one of these functions, others have an explicit mention of two, while another group explicitly mention all three. Al-Shaykh (2019) enumerates most of these definitions. Including these functions in the definition shows the state of agreement the current jurists have with the mainstream economists. However, most of the contemporary jurists are more attached to the jurisprudential rules that bind the current fiat system together.

Again, a historical context in this discussion would add insights to the thought of contemporary jurists. Since gold and silver were the two main coins that played the role of money for many centuries, it was very difficult to understand how the alternatives (banknotes, running cash notes, and fiat money), which only have been there for no more than three centuries, should be classified in *Fiqh*. The issue exacerbated when gold backing of fiat money was terminated in 1971. *Fiqh* jurists went into a complicated dilemma of entangled issues of what rulings fiat money should undertake. The discussions of the jurists, enumerated in Table 2.2, uncovered eight main opinions on the *Fiqh* adaptation of paper money (Al-Mosleh, n.d.).

The **first** opinion notes that paper money is a debt instrument represented by the number written on it where the issuing body is committed to paying its equivalent of gold or silver (Maneei, 1984). This opinion departs from truth in that the issuing body is not committed to paying the equivalent of the value written on the paper money note especially that these new forms of money are no longer backed by gold or silver. The **second** opinion states that paper money is a special form of money that doesn't fully resemble gold, silver, or *Fulūs*; and therefore, the implication of this opinion is that

paper money takes its own rulings composed from a mix of gold and silver rulings, on the one hand, and *Fulūs* rulings, on the other hand (Al-Mosleh, n.d.).

Table 2.2: Jurisprudential Adaptation of Paper Money

	***Fiqh*i Opinions Defining Paper Money**	
	Definition	**Remarks**
1	Paper money is a debt instrument	Refuted because the issuing body is not committed to paying the equivalent value written
2	Paper money is a special form of money	This doesn't necessarily impose all the rulings of what it has been associated to
3	Paper money replaced gold and silver	Being backed by gold or silver is no longer valid and this opinion doesn't withstand
4	Paper money is a traded commodity item	Traded commodities are intended for profit; this isn't the case with paper money
5	Paper money is a special debt bond	This considers it a special debt that can grow, and its owner can benefit from
6	Paper money is a deposit document	Refuted because backing of gold and silver has been stopped since a long time
7	Paper money resembles *Fulūs*	Fiat and *Fulūs* are money by convention Believed by some to be the closest adaptation
8	Paper money is an independent form of money similar to gold and silver	Every type is an independent genus Opinion of the majority of the scholars Decision taken by the Islamic *Fiqh* Council in its favor and is currently the approved definition

Source: Al-Mosleh, n.d.

Although paper money resembles gold and silver in being prices and values for things but departs in many other ways, and although it resembles *Fulūs* in that it doesn't have intrinsic values but departs also in many other ways, it must have been compared to the most similar of both forms; such a comparison doesn't necessarily impose on it all the rulings of what it has been associated to (Al-Mosleh, n.d.). The **third** opinion believes that paper money replaced gold and silver because it is covered by gold or silver and therefore takes their rulings (Maneei, 1984). Again, being backed by gold or silver is no longer valid and this opinion doesn't withstand. Moreover, the implication of this opinion is that different currencies backed by the same precious metal (gold or silver) would have to be exchanged equally with no difference, otherwise one would commit *Ribā al-Faḍl*. Clearly, this would cause hardship as it won't be logical or fair to exchange for example a Turkish lira with a Syrian lira in equal amounts. The **fourth** opinion considers paper money as a traded commodity since it is neither gold or silver and it cannot be measured or weighed (Al-Mosleh,

n.d.; Maneei, 1984). As such, according to this opinion, it is not subject to usury and can't be capital for muḍārabah. However, paper money is a price and value by convention, which therefore associates it to gold and silver since they are prices. Moreover, traded commodities are intended for profit which is not the case with paper money. The **fifth** opinion is similar to the first opinion except that this kind of debt is special where it is not subject to the restrictions of the jurists which imposes that a debt cannot grow as long as the debtor is liable of it. That is to say, this type of special debt related to paper money can grow and its owner can benefit from it (Al-Qaradawi, 1973). The **sixth** opinion states that paper money is a deposit document based on the belief that the backing of this money from gold or silver is deposited with the issuing body (Al-Mosleh, n.d.). As explained before, this thought is refuted with the knowledge that gold and silver backing has been stopped since a long time. The **seventh** opinion considers that paper money resembles *Fulūs* (Al-Zarqa, 1989; Maneei, 1984). In essence, this opinion states that paper money is a popular currency by which commodities and services are priced. It resembles *Fulūs* to a great degree because both are money by convention. Researchers who refuted this opinion based their view on that *Fulūs* were used for cheap products only (Al-Sarakhsī, 1989), or considered *Fulūs* the most inferior of all properties (Al-Maqdisī, 1997). On the contrary, it has been reported that *Fulūs* has been used to buy valuable products and where the only money used in certain regions in history in different periods of time, see (Al-Maqrīzī, 1609). As such, the researcher of this thesis, among others (Al-Mosleh, n.d.), finds this opinion the closest adaptation for paper money for reasons that will follow the discussion of the next and last opinion. The **eighth** opinion perceives that paper money is an independent form of money that takes the rulings of gold and silver (Afanah, 2009; Maneei, 1984). Every type of it is an independent genus depending on its issuer. So, a Turkish lira is a different genus from the US dollar. The reason for this perception is because paper money performs the functions of gold and silver in that all of them are considered prices for things and that the pricing attribute of gold and silver is not confined to them but can be extended to any form accepted by people to perform the functions of money. Yet, there are many differences that can be found between paper money on the one hand, and gold and silver on the other. For example, the value of paper money is by convention acquired by its legal tender, whereas the value of gold and silver is intrinsic to them.

Further, the value of paper money is not as stable as gold and silver; the former's value can rise and recess according to the performance of governments and sometimes can even collapse as happened to Zimbabwe dollar in 2008. Moreover, paper money's acceptance and popularity are variable over time and space. For these reasons, the author of this thesis believes that paper money resembles *Fulūs* more than it does for gold and silver and therefore should have been attached to the rulings of *Fulūs*. However, the majority of contemporary scholars and jurists accepted the eighth opinion likening paper money to gold and silver and, in fact, a decision has been taken by the Islamic *Fiqh* Council, an affiliate of the Muslim World League, in favor of it (Al-Mosleh, n.d.; Al-Yahya, 2019).

The above analysis makes the ground for the contemporary jurists in discussing the permissibility of cryptocurrencies. Now that it has been so crucial for a non-gold non-silver paper money to survive, the notion of a legal tender solely issued by the state became a key criteria in accepting or rejecting cryptocurrencies. It is the eighth opinion rather than the seventh one which caused this stiffness in dealing with the topic: legal tender and being state-issued. It is worth noting though that Islamic minting as an official function of the Sultan only took its official framework during the reign of 'Abd al-Malik bin Marwān; prior to that, coin minting was not the work of the government, but was a profession for people (Al-Ḥarīrī, 1993).

2.3. Cryptocurrencies: Definition and Characterization

Despite being in existence for more than a decade by now, there is no general agreement on how cryptocurrencies should be defined or characterized. Even the terminology used to refer to cryptocurrencies has been very loose and lacked tuning. The divergence of terms when referring to cryptocurrencies only further added unnecessary confusion.

For example, although cryptocurrencies are digital in nature, using the term 'digital currency' or 'digital money' to describe a cryptocurrency is problematic. Abu Husein (2019) raised this issue as he explained that 'digital' is anything concerned with computers and, as a result, the term is widely vague where it can incorporate anything including cryptocurrencies and electronic money. Researchers and practitioners have to bear in mind that prior to the birth of the first cryptocurrency, the Bitcoin, digital transactions via e-commerce were already in place where digital money was used in

the form of credit or debit money. The key difference from cryptocurrencies is that this type of money is associated with one or more financial institutions like Visa and commercial banks.

On the other hand, Abu Husein (2019) reports another term that should not be used as an alternative to cryptocurrency, namely ‘electronic’ money. This again is problematic because ‘electronic’ money has been used at one time as special pre-topped debit cards. That is to say, these cards are associated with one of the paper money issued as a legal tender. The whole purpose of these cards is to use them in their electronic transactions, like for example to pay for e-government service fees. In both of these cases, ‘digital’ and ‘electronic’ money are related to digital transactions, like e-commerce and e-government service payments, but where in both of the cases they are associated with the fiat paper money.

In contrast, although cryptocurrency transactions are completely carried out digitally over the internet, these transactions are sealed with the transfer of the cryptocurrency coin from the buyer to the seller and is being recorded as part of the history of transactions on the decentralized ledger, the blockchain. No reference is made to any intermediary financial institution whatsoever and no legal tender fiat paper money gets involved in the process. Abu Husein (2019) suggests that if it would be necessary to use the terms ‘digital’ and ‘electronic’ for cryptocurrencies then they should be coupled with the term ‘encrypted’ or ‘virtual’. However, the author of this thesis argues that doing so does not produce any added value and, on the contrary, only elongates the terms describing cryptocurrencies and increases the nomenclature with unnecessary phrases. The current terms within the terminology are sufficient to make it clear for people to refer to these cryptocurrencies.

For example, cryptocurrency is widely used alongside the term ‘virtual currency’. The latter describes the virtual nature of the money in the way it is produced and transferred over the internet in the virtual world without direct reference to the real world. Also, the term ‘altcoin’ is widely used, and this refers to a cryptocurrency alternative to Bitcoin.

Yet, it has to be noted that the term ‘cryptocurrency’ can be confusing itself since it has the connotation of a currency while not all cryptos are monetary in nature, see section 4.4. Alternatively, ‘crypto’ is a less confusing shorthand for cryptocurrency

and is sometimes used as well and is understood to refer to these virtual currencies. Currently, there is a gradual shift to converge using the word 'crypto asset' instead to incorporate all the different types of cryptos. The author acknowledges the term 'crypto asset', however, sticks to 'cryptos' and 'cryptocurrencies' for reasons explained in subsection 5.4.1.

2.3.1. Commodity Versus Money Discussion

Taking the case of the Bitcoin, the great degree of its adoption as a currency is highly evident. Projecting it on the mainstream economists' definition of money, we can see that it indeed has gained general acceptance by the public and is in fact used in payments for goods, services, and repayment of debts. Considering it a commodity is not a problem either in the conventional perspective because, for them, money can earn returns.

On the attributes part, Bitcoin is durable, portable, divisible, homogeneous, fungible, and counterfeit resistant. On the functions part, Bitcoin has already proven to be a medium of exchange and can easily assume the role of unit of account. Mishkin (2022) will not agree with the latter on the basis that no commodity is seen priced via Bitcoin. But the fact that you can see no commodity is priced in Bitcoin, doesn't necessarily mean that it cannot assume the unit of account role.

The problematic function is the 'store of value'. Due to Bitcoin's volatility, mainstream economists are not able to consider it money. Though we have already seen how lenient economists are when evaluating fiat money on this third function. Also, it has to be noted that the short-term stability issues occur because Bitcoin is treated as a commodity through using it in short or long selling speculations. Otherwise, it can be considered money in the conventional perspective.

Now we project the previous discussion on *Sharī'ah* perspective. First, as explained previously, in Islam money cannot be regarded a commodity because it is not entitled for a return. The fact that cryptocurrencies are being bought and sold for no purpose other than gaining profits, which accrue from these dealings, has important legal consequences.

Being sold and bought not for the sake of itself raises *Sharī'ah* compliance issues. This clearly shows that Bitcoin has no intrinsic utility and therefore cannot be considered commodity, even though this might follow from the fact that it is subject to

speculations, trading, and short and long selling. Just as trading currencies doesn't make them commodities from the perspective of *Sharī'ah*, by analogy Bitcoin should not be considered a commodity. Moreover, jurists have forbidden forex and similar trading platforms due to the excessive violations to *Sharī'ah* rules.

Therefore, if the short and long sell speculative trading of Bitcoin is dismissed (at least mentally because we know as Muslims these shouldn't be traded legally), the author is of the opinion that we eventually come to the safe conclusion that Bitcoin and similar payment cryptocurrencies are not commodities.

The discussion of stability in the previous paragraph follows here too. Should these points become crystal clear, a preliminary definition can be sought with two reservations. First, we refrain from describing payment-type cryptocurrencies as commodities. Second, the whole system is *Sharī'ah* compliant.

The above discussion applies to payment-type cryptocurrencies. Yet, there are other types of crypto assets that were not intended for transaction payments. An example of these are non-fungible tokens. In this case, some of these types can be considered commodities rather than money. Details of these and other types will be discussed in section 4.4.

2.3.2. Cryptocurrency as a System

A common thing among all cryptos is that they are not just what one owns as a representation of money or commodity, rather they are a whole network system underpinned by the technology behind it and governed by the protocol it obeys. In the extant literature, the first thing that is discussed when it comes to the underpinning technologies is the blockchain. This is considered natural because of the profound effects this technology has implicated on Bitcoin and other cryptocurrencies.

But, although the blockchain is very important, needless to say, the backbone of the whole system is not limited to it but extends to the internet and individual nodes' computers. The software (trading platform, altcoin wallet, altcoin protocol, decentralized distributed ledger - blockchain), the hardware (mining pools, individual nodes' computers and electronic devices, communication hardware), and the internet altogether form the underpinning technologies that support the network of the crypto.

2.4. Analysis of the *Fiqh* Discussions of the Main Issues Related to Cryptos

In the previous subsections, the study showed a good degree of agreement on the functions of money. However, it deliberated issues on variations on the understanding of currencies, the concept of money, and its definition. These issues are also extended to the discussion on cryptocurrencies in almost the same way. For example, the definition of cryptocurrency remains contentious. Therefore, an important step that this study undertakes is to traverse the literature to extract the main discussions made about the Islamic stance of cryptocurrencies.

From the analysis of these discussions one can elicit the main issues in the topic and elaborate on the gaps that will act as the fundamental building blocks for this thesis. The review revealed several important outcomes that need to be addressed. Foremost, when one talks generally about cryptocurrencies, people's understanding of the concept seems to be aligned. As soon as one digs deeper into the topic, this artificial alignment starts to fade away. The resultant illusion is just a manifestation of the disagreement among researchers on how to define cryptocurrencies and their characteristics as money. Second, the misconception and misunderstanding of the underlying technology is so great to the extent that it plays a major role in causing the lack of consensus on the definition of cryptocurrencies. This has just led to legal rulings based on unsound reasoning and flawed assumptions.

The literature has also revealed a very interesting consequence of these issues: notwithstanding the various diverse cryptocurrencies out there, all of these altcoins seemed to be synonymous to Bitcoin for many researchers – this makes the third gap. Fourth, despite treating all altcoins as if they were all identical, a cursory trend analysis of the literature shows that after 2019, some researchers in the field of Islamic economics and finance started to appreciate the differences between the diverse cryptocurrencies. However, their view remains short of the proper systematic synthesis of the topic. A very highly quoted consequence of cryptocurrencies is their negative effect on the economy. This seems to be a direct manifestation of the influence of stability issues associated with cryptocurrencies on the researchers. However, there is a negligible number of papers that studied their effect on the economy, and even those few that did lacked the proper methodology; nonetheless, this issue is beyond the scope of this thesis.

2.4.1. Contention on the Definition and Attributes of Cryptocurrencies

There is a clear inconsistency in the terminological usage of cryptocurrencies. Inconsistencies included using terminologies such as 'digital currency', 'digital money', and 'electronic money' (Abu Layl, 2019; O. A. A. Al-Jumayli, 2019; Bu Abdaly & Saeed, 2019; Dahshan, 2019; Smiran, 2019). These terminologies are widely used to represent digital financial currencies other than cryptocurrencies (or virtual currencies). Moreover, there is a lack of consensus on the definition of cryptocurrency. There is no agreement on its legal representation or characteristics and whether it can be considered money or not. For example, in its resolution no. 237 (24/8), the International Islamic *Fiqh* Academy (IIFA) of the Organization of Islamic Cooperation (OIC) called for further research and studies on issues that affect the *Sharī'ah* rulings on crypto-currencies, the most important of which include: the definition of cryptocurrencies, reality of Bitcoin, and the characterization of cryptocurrencies in terms of whether it is a commodity or benefit, or being a real-valued property and a tradable item ("Closing Statement of Digital Crypto-Currencies Symposium," 2021). Similarly, the European Banking Authority realized the difficulty of determining the legal entity of cryptocurrencies and therefore called for the adoption of a gradual special organization (Al-Maknouzi, 2019). Abu-Bakar (2017), therefore, asserts that the understanding of cryptocurrency and its technology is evolving, and that jurists' opinion should become more informed as cryptocurrency becomes more understood. Yet, the contention surpasses the jurists to include economists, bankers, and researchers as can be derived from the literature. For example, China doesn't consider Bitcoin as fiat currency on the basis that it is non-sovereign cryptocurrency (El Islamy, 2021). Also, the governor of the Bank of England considers cryptocurrencies having no intrinsic value (Morris, 2021). On the contrary to this idea, El Islamy (2021) believes that the Bitcoin does have intrinsic value. She sees the cryptocurrency closely resembling the early Shariah currency since it has the characteristic of being an asset (commodity) and a medium of exchange just like gold and silver used to be.

Many jurists, though, do not share the latter view. For instance, some argue that the controls and functions of money, including being a medium of exchange, are not satisfied by the virtual currencies; of this view are I. A. A. Al-Jumayli (2019); O. A. A. Al-Jumayli (2019); Al-Shummari (2019); Mabout (2019); Oudah (2019); Samai

(2019). Others even went to define controls for *Sharī'ah* compliance, each according to his opinion; for instance Abu Ain (2019); Al-Samirrai (2019). Their reasons range from volatility issues to popularity issues, non-existence of issuing body, risks involved, and inability of acting as a unit of accounting, just to mention a few. While he agrees with some of the aforementioned issues, Al-Yahya (2019) is of the opposing view that the volatility or instability of a virtual currency does not negate its function as a price, unit of accounting, for commodities. Abū Ghuddah (2018), on the other hand, does not consider a cryptocurrency as a unit of accounting. Such discrepancies as outlined by the literature necessitates a deeper look into the concept of money, a clear understanding of its characteristics, a *Fiqhi* understanding of the concept of money, and how cryptocurrencies can be harmonized with these characteristics and attributes.

2.4.2. Limited Understanding of Cryptocurrency Technicalities

From literature, it becomes very clear that technology has played a major role in creating a state of dichotomy, whereby people, governments, and even states disagreed on the characteristics of the cryptocurrencies. Daghi (2019) recognizes the importance and rapid advancement of technology and asserts the need to prepare [from a *Fiqh* perspective] for the future. Despite such acknowledgement, many researchers sufficed to have a very basic and simplistic description of the virtual currencies. Even with the case of Bitcoin, researchers are found to have obscure ideas. As such, many researchers demonstrated traces of inaccuracies and confusion related to some technical aspects. The consequence of these misconceptions can be as severe as coming up with unsound and invalid rulings like declaring a cryptocurrency is impermissible on the basis that the transacting parties are unknown, the case of which is a clear misconception. Also, we find rulings of impermissibility taken on the grounds that cryptocurrencies are based on gambling, speculation, and *Gharar* (Smiran, 2019). Moreover, most of the rulings were derived using the *Fiqh* rules of paper money based on the unsubstantiated assumption that cryptocurrencies have to be compared with fiat currency. For instance, should there be key differences in the functions of cryptocurrencies and fiat money, their issuance, and characteristics, then Al-Shaykh (2019) argues that the ruling has to be the prohibition of those virtual currencies. From a *Fiqh* perspective, the latter seems to be due to the influence of early scholars' opinion on today's scholars' opinion related to the requirement of control and regulations. Nonetheless, the literature hardly

speaks about the validity of projecting early regulation requirements on today's innovations. It is worth noting that the peer-to-peer network (Maghdeed, 2020a) of the blockchain that underpins major cryptocurrencies differs from the brick-and-mortar infrastructure of the current banking system.

The whole concept on which bitcoin was initiated revolves around trust provided by the peers while completely moving away from any central control which is completely different from the form of currencies having legal tender. Hence, following is a quick examination of the problems stemming from technical incompetence. First some researchers lacked the understanding of the mechanism of cryptocurrencies. For example, Abu Layl (2019) believes that cryptocurrencies are issued by people with unknown identities and are being exchanged via imaginary nicknames. On the contrary to this thought, cryptocurrencies are not issued by people, but by a deterministic code dictated by the protocol of the system. The hidden addresses and 'nicknames' of end users are necessary to ensure the security of their funds and that only owners of funds authorize their own transactions. But this doesn't imply that the transacting parties do not know one another. As a matter of fact, a transacting party knows exactly to whom he is sending his funds to.

Other researchers have erred when analyzing the technology; a discussion of some of them will follow. Terminological inaccuracies, incorrect conclusions, and technical mistakes were common. For instance, Al-Jumayli (2019) and Oudah (2019) fell into terminological inaccuracy when using the general word 'algorithm' for labeling the mining crypto puzzle. These researchers also reached to incorrect conclusions stating that blockchain requires giant network of computers, internet, and programs to operate and store the information. Interestingly enough, both these researchers used the same exact sentence, which most probably implies that both have extracted it from the same source. In his research, Mabout (2019) uses uncredible websites that led him to wrong conclusions. For example, he is under the impression that a malicious miner can simply win a new Bitcoin token by fraudulently adding an imaginary block to the blockchain. On the other hand, many researchers committed technical mistakes like stating that 50 tokens are generated when solving the puzzle (Oudah, 2019), or believing that no one knows accurately what equations the computer tries to solve (Al-Yahya, 2019), or stating that miners are unknown and therefore the ignorance of the identity of a party in dealing or trading results in its invalidity (Al-Samirrai, 2019). The misconception

of the underlying technology calls for the need to harmonize technology with *Sharī'ah* requirements.

2.4.3. Misconception of Equating Cryptocurrencies to Bitcoin

The widespread and popularity of Bitcoin influenced the interest of academics. The efforts were mostly exerted to study Bitcoin and its underlying technology, the blockchain. Comparatively, little was employed to understand other cryptocurrencies. In the majority of the studies related to Islamic economics, researchers viewed cryptocurrencies synonymous to Bitcoin. Al-Shaykh (2019) argues that the study of Bitcoin and its *Sharī'ah* ruling is, in fact, a study for the remaining alternative cryptocurrencies because, in essence, they are the same except for a few technical matter that doesn't affect the ruling.

This stance, whether implicitly or explicitly, was embraced by many researchers, for example see (Al-Yahya, 2019). They studied the characteristics of Bitcoin and, assuming they are similar, generalized the rulings to all of the other cryptocurrencies. This view fails to realize the diversity among all cryptocurrencies and the existing differences in terms of the purpose of their initiation, structure, operation, and consequences. For example, unlike Ethereum, Bitcoin doesn't fully support smart contract features and, instead, facilitates a small pose of it (Maghdeed, 2020b). Evaluating all cryptocurrencies using Bitcoin will result in incorrect inferences because each has its own purpose and characteristics; instead, white papers need to be examined first for each of these currencies (Selcuk & Kaya, 2021). Abu Husein (2019) reinforces this viewpoint by saying that they have to be examined on a one-by-one basis. However, these researchers do not contribute to that direction either. Consequently, there seems to be an unrelenting need for categorizing these cryptocurrencies and modeling them to aid in understanding their technology.

2.4.4. Risks of Cryptocurrencies

The high risks surrounding the use of cryptocurrencies have been highly cited by the majority of researchers as reasons for rejecting them especially from a *Sharī'ah* perspective. The discussion of risks in literature has been mainly scattered and lacked a systematic and thorough study of risk analysis and management. The highest cited risk is related to lack of regulations and regulatory bodies (Abu Layl, 2019; I. A. A. Al-Jumayli, 2019; Al-Shummari, 2019; Samai, 2019). While this is still raised by

Muslim researchers as a major concern, it is worth noting that the European Banking Authority eventually called for the adoption of a gradual special organization for these cryptocurrencies and the legal debate transformed from one that questions their legal legitimacy and risks to a one that is limited to their legal nature, i.e. one that only discusses how should they be defined from a legal perspective (Al-Maknouzi, 2019).

Another risk that emerges greatly in literature is the lack of issuing authority (usually the state) or the lack of association with any financial institution (Al-Shummari, 2019; Oudah, 2019; Samai, 2019). This risk is based on the *Fiqh*i ruling that the issuance of money should be the sole right of the state.

On the other hand, other cited risks include stability and price fluctuations (O. A. A. Al-Jumayli, 2019; Mabout, 2019; Samai, 2019), *Gharar* (O. A. A. Al-Jumayli, 2019; Al-Shummari, 2019), resemblance of gambling (O. A. A. Al-Jumayli, 2019), and speculative investments (Samai, 2019). These four types of risks have been very interrelated in literature and occasionally they were referred by some researchers to have the same meaning. For instance, according to Smiran (2019) cryptocurrencies are based on gambling, speculation, and *Gharar*. Also, according to Al-Yahya (2019) gambling is related to mining, stability, and speculative investments. Another cited risk very related to these four risks is *Jahālah* (ignorance). Al-Samirrai (2019) argues that there is *Jahālah* in the miners because they are unknown and therefore the ignorance of the identity of a party in dealing or trading results in its invalidity. Contrary to these thoughts, Abu Husein (2019) refutes both *Jahālah* and *Gharar* related to speculative investment. Besides, there is a fallacy in the latter point because miners are not part of a transaction, they are just ledger bookkeepers. Other risks like not being backed by any asset (Abu Layl, 2019; Samai, 2019), being virtual and having no physical existence (Samai, 2019), and lacking intrinsic value and not being legal tenders (I. A. A. Al-Jumayli, 2019) are not based on thorough research and therefore are very subjective and debatable. Perhaps one of the fundamental questions raised by El Islamy (2021) is the risk associated with inheritance issues and loss of passwords in the context of cryptocurrency, which has significant implications for *Sharī'ah* compliance.

A holistic study of the risks of cryptocurrencies is barely evident in literature. A scanty discussion of a holistic view of risks is found in Al Yahya's (2019) study where he had a light mention of cryptocurrency economical, technical, and legal risks. Yet, such a

study again was marginal and lacked the required depth and systematic approach. Specifically, when discussing the technical risks, researchers fell into many fallacies. For example, Al Yahya (2019) states that although the trust is extracted from technology, the unknown issuer of the altcoin is necessarily the controller of it even if it claimed that its system denies anybody to control or manipulate it. Another such problem is claiming malicious miners can add imaginary blocks to the blockchain in order to get new bitcoin tokens by fraud (Mabout, 2019). Also, when discussing the economic risk, the negative associations made are not substantiated by any statistically significant study. In contrast, cryptocurrencies' role in the economics of the countries is marginal compared to the legal money issued by the central banks; by April 2018, their market value reached 300 billion dollars whereas the wide money supply of US was in excess of 114 trillion dollars by the end of the year 2017 (Abdelhamid & Ahmad, 2019). As of the writing of his study in 2019, Dahshan (2019) believes that the virtual currencies have no tangible effect, whether positive or negative, on the ability of the central banks to execute their monetary policies. Also, he believes that they have no effect on the international trade. In summary, the risks raised by the majority of the studies are limited in the sense that they were enumerated without proper analysis of these risks.

2.5. The Existing *Fiqh* Framework on the Issues of Cryptocurrencies

The majority of researchers focusing on the study of cryptocurrencies from a *Fiqh* perspective, many of whom were discussed in the preceding subsections, adhered to the analytical inductive method established long ago by early jurists. Such a methodology is very rigorous and has proven to have preserved the transmission of our teachings. Yet these studies concentrated their effort on the *Fiqh* side and neglected the proper examination of the technical side. Figure 2.3 portrays the prevailing framework employed by contemporary scholars to examine the intricacies of cryptocurrencies. Notably, a thorough exploration of the technical aspects of cryptocurrencies has been generally absent from scholarly analysis.

It is intriguing to observe that a significant number of scholars have developed their perspectives and paradigms on cryptocurrencies by juxtaposing them against fiat currency, guided by a ruling pronounced by earlier jurists based on public interest.

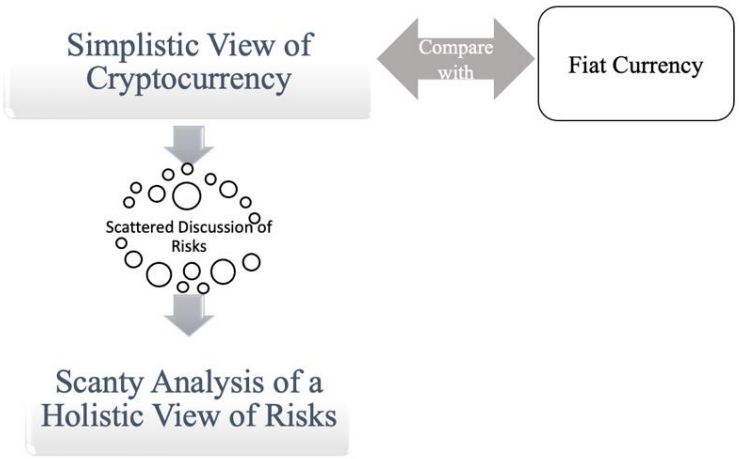

Figure 2.3: Current Juristic Paradigm for Analyzing Cryptocurrencies

Source: Author's view based on extant literature

This perspective is problematic for several reasons. Firstly, the fiat currency is a product of a Central Bank, which is more or less related to a central government, whereas cryptocurrencies are, in large, independent of governments. Therefore, the models that govern them are completely different. Secondly, fiat currencies were themselves problematic and jurists disagreed on their adaptation with eight main opinions as discussed previously in section 2.2.4. The majority then agreed on one of the opinions after meticulous discussions, thorough examination, and careful comparison with the original money: gold and silver. As such, it would be more adequate to compare cryptocurrencies with gold and silver rather than comparing them with fiat currencies. Thirdly, fiat currencies represent the money in circulation which requires a large network of financial institutions and intermediaries for it to function. However, the view that makes cryptos comparable to fiat currencies fails to recognize that cryptos are not mere money or currencies, but rather they are complete financial systems.

Additionally, it is noteworthy that the discourse on risks associated with cryptocurrencies remains fragmented, lacking a comprehensive analysis that considers risks holistically. The discussion of risks in literature hardly could segregate technical risks from investment risks. While the latter risks are considered part of the entitlement for profit, and thus are completely acceptable from a *Fiqh* viewpoint, the technical risks cannot be tolerated in *Fiqh*. This often led jurists to conflate risks with *Gharar*.

However, through a cursory trend analysis, the most recent research in the area reveals that some Islamic economic researchers indeed started to have a better understanding of Bitcoin and a remarked appreciation of the existing differences between it and other cryptocurrencies. Nonetheless, such an understanding is still built upon a nonsystematic high-level abstraction of the system which may easily result in misconception, misapprehension, misinterpretation, and unsubstantiated claims. Mashal (2022) argues that research and discussion in a category of cryptocurrencies have not gained traction yet in a systematic way by the Muslim jurist assemblies, forums, and conferences. He explains that such issues have accelerated since the inception of Bitcoin, blockchain, and the smart contracts; this includes mining through the Proof-of-Stake (PoS) system, agency mining, and NFTs. The contemporary jurists have not addressed these issues adequately. In part the topic is very complicated with varying technical aspects. Yet, it seems very clear that the jurists lack a proper contemporary framework that helps them to analyze the issues of cryptocurrencies from a *Fiqh* perspective.

CHAPTER III

METHODOLOGY

3.1. Introduction

This chapter outlines the meticulous methodology employed to propose and validate the contemporary *Fiqh* framework for analyzing the issues in cryptocurrencies. While the proposal presents a more robust Fiqh paradigm, surpassing the existing framework for examining and analyzing cryptocurrency issues and exploring their Sharī'ah implications, the validation process aims to fortify the scholarly integrity of the proposed framework. Thus, it seeks to enhance its contribution to the ongoing scholarly discourse on contemporary Fiqh issues in cryptocurrencies. As such, the methodology is divided into two phases as depicted in Figure 3.1.

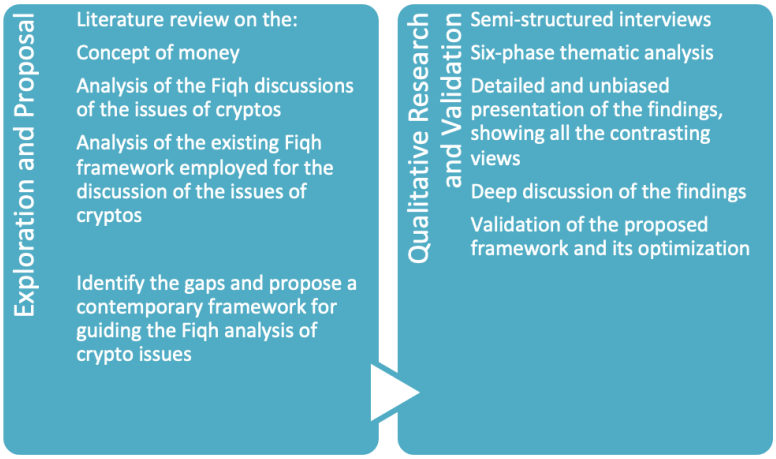

Figure 3.1: Two-Phase Methodology

Source: Author

In the first phase, the gaps identified from the literature review are used to develop a contemporary *Fiqh* framework for the analysis of cryptocurrency issues. In the second phase, qualitative research is employed to validate that framework. The following sections elaborate the two phases.

3.2. Phase 1: Exploration and Proposal

This phase makes use of the literature review on the concept of money, analysis of the *Fiqh* discussions of the issues of cryptos, and the adequacy of the currently existing

Fiqh framework. The aim of this exploration, which was conducted in chapter II, is to identify the gaps in the paradigms of the existing *Fiqh* views on the topic and examine their adequacy. These gaps will then be used by chapter IV to propose a better-equipped and more adequate contemporary *Fiqh* framework.

3.3. Phase 2: Qualitative Research and Validation

This phase of the methodology adopts qualitative research to obtain expert insights and recommendations in order to ensure the proposed framework's robustness and suitability. The findings of this qualitative research will be presented and discussed in chapter V of this thesis. The following subsections describe the research design, the researcher's role, sampling strategy, data collection methods, data analysis approach, and ethical considerations and limitations.

3.3.1. Research Design

This thesis conducted semi-structured interviews to delve into the fundamental subject matter and its associated issues in a qualitative research context. Consistent with the recommendation of Miles and Huberman (1994), qualitative research is widely recognized as the most effective method for discovering and exploring novel areas of inquiry. The selection of semi-structured interviews allows the research to develop into conversational sessions, thus, enabling participants to freely articulate their viewpoints and explore significant facets of the subject matter (Longhurst, 2016). Consequently, the thesis lends itself to a qualitative exploratory study due to the absence of a well-structured *Fiqh* framework in the existing literature that can adequately analyze the issues of cryptocurrencies. This is consistent with Neuman's (2014) depiction of exploratory research which seeks to investigate areas or phenomena that are not well understood with the objective of generating initial insights and formulating preliminary concepts regarding them. Such a qualitative design is well-suited for this exploratory research as qualitative approaches foster innovation, creativity, and the exploration of researcher-designed frameworks (Creswell, 2009). Moreover, exploratory research offers flexibility in terms of data collection techniques, encompassing formal approaches like in-depth interviews and informal approaches such as informal discussions.

3.3.2. The Researcher's Role

As the primary individual for collecting data, it is quintessential that the researcher identifies his personal values, perceptions, and biases on the onset of the qualitative research. "Good qualitative research contains comments by the researchers about how their interpretation of the findings is shaped by their background" (Creswell, 2014). From March 2003 to January 2019, I served as an Information Technology (IT) analyst in a large financial institution. My role as a technical analyst, supporting tens of financial applications and FinTech products, helped shape my perceptions about financing and monetary aspects, financial issues, and the technical intricacies and complexities of financial settings. Particularly, my interest in cryptocurrencies, since the inception of the Bitcoin, and their issues gradually grew over the years from two dimensions. The first is understanding the *Fiqh* worldview of these new innovations, while the second dimension relates to understanding, and seeking ways of simplifying the comprehension of, the technology behind the crypto systems.

Due to previous experiences in the technical realm and ample exposure of the *Fiqh* viewpoint on cryptocurrencies, I bring certain biases to this thesis. Every effort will be made to ensure objectivity of the study; however, these biases may shape the way I examine the collected data and how I interpret my experiences. I start this study with the belief that contemporary jurists do not possess an adequate guideline and framework to investigate a relatively new innovation, the cryptocurrencies. I question the adequacy of employing the classical 20th century method of inspecting money in examining these new digital innovations. Further to that, I acknowledge the difficulty the jurists face in developing a comprehensive understanding of their technologies.

3.3.3. Sampling Strategy

Graneheim, Lindgren, and Lundman (2017) underscore the importance of ensuring credibility by involving study participants who possess relevant experience and knowledge pertaining to the phenomenon being investigated. Accordingly, experts who possess profound expertise in the field of Islamic jurisprudence (*Fiqh*) pertaining to commercial transactions and have had an in-depth exposure to the issues of cryptocurrencies were purposefully identified and selected based on their "Substantive area expertise… by virtue of their command of a field of knowledge" (Sandelowski, 1998). The inclusion of participants with such expertise is critical for member

checking or member validation, whereby their insights are sought to corroborate the accuracy of the data and interpretations (Sandelowski, 1998).

To ensure comprehensive and representative validation, a purposive sampling strategy was adopted supplemented with a form of snowball sampling. Purposive sampling is particularly appropriate for unique circumstances and exploratory research endeavors (Neuman, 2014). This sampling technique allows for the deliberate selection of informative cases that merit thorough examination which enables a more profound comprehension of the subject matter (Neuman, 2014). In the current context, snowball sampling played a valuable role by facilitating the identification of experts within a tightly interconnected network. This approach proved especially beneficial in identifying experts based on their demonstrated knowledge and experience in both traditional *Fiqh* and contemporary issues, particularly those pertaining to cryptocurrencies. Nineteen such experts were identified through Islamic Economics Forum (IEF) or through referrals from them. Out of the nineteen experts, ten responded and agreed to participate. However, due to unforeseen circumstances, one of the experts apologized at the last minute. Therefore, the final sample consisted of nine participants. From the review of many qualitative research studies, the sample size of phenomenology research has been found to typically range from three to ten (Creswell, 2014). The data analysis in this thesis lends itself to thematic analysis as will be delineated in section 3.3.5, where it is very relevant to phenomenology studies. Guest, MacQueen, & Namey (2012) were cited to express the relevance of thematic analysis "to phenomenology since it stresses subjects' perceptions, feelings, and experiences subjectively" (Chang & Wang, 2021). As such, nine is a number that is considered sufficient for data saturation and enough for ensuring a thorough exploration of the research topic, and therefore the chosen sample size is deemed appropriate for the objectives of this study. This aligns with the emphasis of qualitative research on achieving a deep understanding rather than focusing on a large sample size (Boddy, 2016). It is worth noting that in-depth qualitative research has the potential to yield valuable insights, even from a single participant, underscoring the significance of sample sizes as small as one (Boddy, 2016). This sampling strategy ensured that the panel of experts comprised individuals capable of critically evaluating the proposed framework from multiple perspectives.

3.3.4. Data Collection

Data collection was conducted through individual semi-structured interviews that allowed for in-depth discussions and the elicitation of nuanced insights. Semi-structured interview guides were prepared in advance to ensure consistency and focus during data collection sessions. These preliminary guides also played a significant role in preparing the experts before the interviews and making them familiar with the proposed framework. The interview process was facilitated either face-to-face or through virtual mediums, such as video conferences, ensuring flexibility and accessibility for the participating experts. The former interviews were audio recorded, while the latter were both audio and video recorded. This helped in increasing the participation rate and accommodating geographic limitations.

Initially the experts were approached via WhatsApp messages with the explanation of the study, a guide that briefly described the framework and its processes, and the set of questions. This approach acted as an ice-breaker and set the ground for the nature of the study, its significance, and what to be expected. The message was followed to arrange the time and location of the interviews. Each interview lasted on average 1 hour and 43 minutes amounting to a total of 15 hours and 24 minutes of interviewing time. The first 5 minutes of each interview were utilized by the interviewer to welcome the participants and briefly explain the proposed framework. During the interviews, the experts were encouraged to provide constructive feedback, suggestions, and critical observations with the aim to identify potential areas for the framework's refinement and improvement. The process encouraged an open and rigorous dialogue to extract diverse viewpoints and foster ideas that help validate the framework. Interference during the conversation was made to a minimum so that any type of leading and guiding bias was minimized. This also has the effect of letting the participants' thoughts to flow smoothly and seemingly. When necessary, a session was dedicated with the experts to explain and delineate the intricacies of the proposed framework so as to eliminate any misunderstandings that might have developed. This was the case with two of the participating experts who preferred to provide the answers in typing after these sessions. The remaining interviews were either audio or video recorded.

The interview questionnaire consisted only of open-ended questions. This type of questions offer the participants with the freedom to give any answer they wish to the

questions (Neuman, 2014). The questions in the questionnaire discussed issues related to technical confusion and contention about cryptocurrencies, adequacy of the existing *Fiqh* framework, the validity of the proposed framework, the challenges of implementing it, and its prospects. Presented in APPENDIX B, these questions were validated by two esteemed professors specialized in Islamic economics and finance, each possessing extensive experience in developing questions that precisely align with the research objectives. Such validation goes hand in hand with the description of Sandelowski (1998) "Outsider-experts can help researchers ask better questions of their data, lead them to new ways of analyzing data".

3.3.5. Data Analysis

Nowell, Norris, White, & Moules (2017) quoted that thematic analysis is a highly flexible approach providing a rich and detailed, yet complex account of data. The objective of this analysis is to traverse the different perspectives of the participants and gain insights. Thematic analysis proves to be a valuable approach for scrutinizing the viewpoints of diverse participants, elucidating both commonalities and distinctions, and uncovering unexpected insights, all the while summarizing essential features within an extensive dataset (Nowell et al., 2017). Therefore, the collected data was analyzed by employing a thematic analysis approach. Due to the exploratory nature of the study, the coding and thematic development unfolded from the data content itself. Thematic development followed the six phases of thematic analysis proposed by Braun and Clarke (2006). The first phase discusses the notion of becoming familiar with the data. In order to do this, the audio/video recordings were transcribed using a tool powered by artificial intelligence (AI) from Riverside[10]. These transcripts were meticulously reviewed against the recordings, line by line and word by word, and the errors were corrected to ensure reliability and accuracy in line with the proofreading checks suggested by McLellan, MaCqueen, & Neidig (2003). In the interim, the researcher took notes of interesting data and emphasis made by the participants. It is worth noting that there exist two primary methods for transcribing data: naturalism, which entails capturing every utterance in meticulous detail, and denaturalism, which

[10] https://riverside.fm/transcription

involves correcting grammar, eliminating interview noise such as pauses and stutters, and standardizing non-majority accents (Oliver et al., 2005).

Naturalism approach is often used by researchers who are interested in conversational studies where every detail is deemed valuable. However, Oliver et al. (2005) proposes an approach to transcription that is denaturalized, catering to researchers who prioritize the informational content of speech. This study is interested in the experiences and opinions of the participants and in the informational content provided by them more than the intricacies of their language and linguistics. As such, this study was more inclined to a denatural approach and, therefore, on reviewing the transcripts this was taken into consideration.

The second phase of thematic analysis is to generate the initial codes. This study partially followed the recommendation by Guest et al. (2012) to "winnow" the data before coding. Therefore, the transcripts were reduced to only code the relevant data while the highly irrelevant were disregarded. Some non-conspicuous irrelevant data became only notable after the theme development phase, at which stage they were omitted. This approach also followed from the denaturalism mode employed in transcription. NVivo software was used to carry out the coding, organizing, and thematizing of the data.

In the third phase, the researcher searched for key themes and patterns using the software and noted these down. The fourth phase involved reviewing these themes and refining them while looking at further interconnections among the codes. The themes were then defined in the fifth phase followed by writing them up and presenting them in the sixth phase.

To ensure validity and reliability of the findings the following strategies were undertaken. For verifying and validating the findings, Creswell (2014) recommended the use of multiple approaches including clarifying "The *bias* the researcher brings to the study", "Use a *rich, thick description* to convey the findings", and "Present *negative* or *discrepant information* that runs counter to the themes". In this study, self-reflection was provided by the author in section 3.3.2 'The Researcher's Role'. That section clearly delineated, on the onset, any biases the researcher might have brought to the study. Second, the analysis offered many perspectives about the themes to give

a rich, thick description of the findings. Third, information that contradicts the general perspective of some themes besides evidence of other themes were demonstrated.

To ensure reliability of the findings, transcripts were carefully and thoroughly checked to eliminate any mistakes. For every 10 minute of audio/video recording, an average of one hour was spent to ensure accuracy. Moreover, the data was constantly compared with the codes and their definitions to eliminate any shift in the meaning of the codes during the coding process. These approaches go in line with "Check transcripts to make sure that they do not contain obvious mistakes" and "There is not a drift in the definition of codes" approaches listed by Creswell (2014) to ensure consistency and reliability.

3.3.6. Ethical Considerations and Limitations

In most of the discourses on qualitative research, authors discuss the vitality of ethical considerations (Creswell, 2014; Neuman, 2014). Particularly, these issues are more prevalent in anthropological ethnographic type of studies. As the subject of this thesis study is related to *Fiqh* analysis of cryptocurrency issues, no revealing of sensitive participant data or violation of rights are anticipated. Nonetheless, this research adhered to ethical guidelines and ensured the protection of participants' rights and confidentiality. The following safeguards were employed to address these ethical issues.

First, the thesis had no conflict of interest. There was no intention at all to use the research for personal reasons, nor were there any vested interest in the outcome of the data. Additionally, this study received no payment. Second, since this study is non-anthropological in nature, there were no harmful data collected which might affect the privacy of the participants. Although the interviewees are human, but they were not the subjects of this research. Rather, their part was the role of experts who provided valuable information where the subject was about cryptocurrencies and their *Fiqh* view. Third, informed consent was obtained from all participating experts, who were fully informed about the purpose, scope, and expected outcomes of the validation process. The research objectives were at least articulated in writing and during the interviews were outlined verbally to ensure clarity. Also, during the study, leading questions were completely avoided. Fourth, verbatim transcriptions and written interpretations will be made available to the participants on their request. Fifth, in the

data analysis phase, to avoid standing by a certain viewpoint, multiple perspectives were reported. Furthermore, to reveal all aspects of the study, contrary findings were also reported.

CHAPTER IV

THE PROPOSED *FIQH* FRAMEWORK

4.1. Introduction

This chapter aims at achieving **research objective 3** which is to propose a contemporary *Fiqh* framework for analyzing the stated issues of cryptocurrencies and validate the viability of that framework. It aims to fill the gaps in the previous literature by proposing a contemporary *Fiqh* framework for constructive analysis of cryptocurrencies. The framework is built upon an in-depth conceptual and operational understanding of the most common cryptocurrency, Bitcoin. The chapter makes another valuable contribution to the field by proposing a comprehensive definition of cryptocurrencies based on widely accepted terminologies.

To achieve these objectives, this chapter is organized into five sections. The first section proposes convergence of terminologies and a universal definition of cryptocurrencies, which establishes a common understanding for the subsequent analysis. The second section presents two models, conceptual and operational, that explain the modus operandi of Bitcoin in detail. The third section categorizes cryptocurrencies into six distinct categories and explains the differences among them. The fourth section provides a thorough risk analysis of cryptocurrencies, taking into consideration the different categories and the unique risks associated with each. The fifth section integrates the information presented in the previous sections to develop a coherent and comprehensive *Fiqh* framework for analyzing cryptocurrencies.

The proposed framework emphasizes the importance of understanding the technical aspects of cryptocurrencies and their potential implications. It also highlights the need for a systematic and comprehensive risk analysis to inform *Fiqh* ruling processes related to cryptocurrencies. This research contributes to the academic literature by offering a rigorous and structured approach to analyzing cryptocurrencies, which has practical implications for jurists, policymakers, investors, and regulators alike.

4.2. Towards Convergence of Terminology and Definition

The presence of imprecision in the terminology and the conflation of cryptocurrencies with other forms of digital currency underscores the need for a precise and widely accepted definition of cryptos. Such a definition would facilitate unambiguous communication among researchers, ensuring that the objects of their analysis are clearly demarcated and accurately delineated. But, just as noted by technical experts, "Bitcoin is not easy to model" (Bonneau et al., 2015). This equally well applies to other cryptocurrencies.

The complexity of conceptualizing Bitcoin and other cryptocurrencies demands that researchers reevaluate the situation from a holistic point of view. The difficulty to model them is perhaps the reason why there is a lack of consensus on the definition of cryptos. Economists and financial experts, Muslims and non-Muslims equally well, dispute whether they are commodities, currencies, both, or none. An important reason for this ambiguity is perhaps because most of them are mainly studying the case of the Bitcoin and generalizing to other altcoins. Since they are unable to clearly define and categorize the crypto assets, they are also unable to have a unanimous decision on their legality or permissibility; often treating the various types of cryptos in the same manner; see the closing statement by IIFA ("Closing Statement of Digital Crypto-Currencies Symposium," 2021).

Almost all of the definitions devised are either a long explanation of the virtual currencies as noted by Abu Hussein (2019) or they lack essential parts that are necessary to describe a cryptocurrency (crypto asset). In his definition, Abu Hussein (2019) states that virtual currencies are encrypted mathematical data with a value acquired from the custom and trust of its users and that is being transacted in a virtual computer environment without intermediary. This definition, however, can encompass other things besides a cryptocurrency. For instance, ciphered text can fall under that definition. Therefore, even in his definition he misses out key components that sets cryptos apart from other things.

As will be explained in the subsequent sections, there are many types of cryptocurrencies of which only some that function as payments. In addition to that, the next section will show that a cryptocurrency is in no way a single coin that gets transferred, but instead is a complete system that ensures these coins and tokens change

ownership without any hassle. It is very important that the definition includes the key word ‘token’ next to the word ‘coin’ because not all cryptocurrencies serve the purpose of being a payment system. Hence, ‘token’ describes the situation for other purposes. Also, a key aspect that distinctly distinguishes cryptos from other things is the fact that the system ‘seeks’ decentralization (being recorded on the blockchain where every node keeps a copy of) as far as practicable (since many cryptos exist that are more centralized than decentralized), and transfers are done securely between peers without intermediaries. As such the author suggests the following for the definition of a cryptocurrency (actually crypto asset): “Aspiring to be decentralized, it is a system that ensures coins or tokens are transferred securely and directly between peers without intermediaries” (Author’s definition).

4.3. Modus Operandi of the Underlying Technology

The extant review of literature in the present study reveals that the lack of understanding of the technical part of cryptocurrencies led to some, the least that can be said about, inaccurate rulings. Since the basic form of the underpinning technology of almost all cryptocurrencies is derived from that of the Bitcoin’s, the latter will be taken as an example to discuss the modus operandi. The significance of this approach is that it will help simplify understanding the concept of cryptocurrencies, model their systems, and as a result identify key elements for developing the framework which will help to analyze the *Fiqh* issues of cryptocurrencies. In this subsection, the implications of the motives for establishing the first cryptocurrency will be discussed. Doing so will set the grounds for conceptualizing how the system is built from the grounds up. This will be followed by operationalizing the system via linking all the individual components together.

4.3.1. Implications of the Motives for Establishing the Bitcoin

In the normal classical day-to-day sale transaction, there is a physical face-to-face meeting between the seller and the buyer. In this type of transaction, payment is done directly without the involvement of a third party or a middleman. In contrast, modern transactions can also happen over a communications channel like the internet. Examples of these include e-commerce and money transfers. In these types of transactions, payment is indirect and involves trusted third party intermediaries. These

intermediaries are financial institutions that validate the transaction by ensuring the buyer has the payable amount and also verifying the overall integrity of the process.

The inventor of Bitcoin, Satoshi Nakamoto, resented the second form of payment and believed that the existence of trusted third parties caused several issues. First, these kinds of transactions are not completely non-reversible (Nakamoto, 2008). In his opinion, once fulfilled, a transaction should not be reversed. In the current online transactions, the possibility that any of the parties involved can reverse the operation jeopardizes the integrity of the buy/sell process and causes inflictions on one of the two parties. The second issue lies in the fact that the current online transactions involve mediating costs and, therefore, limit the minimum practical transaction size. This also meant cutting off the possibility for small casual transactions.

In order to replicate the mechanism of the first form of payment, which is the direct peer-to-peer payment, in a form that encompasses a communications channel like internet but without the need for a trusted third party, Satoshi Nakamoto needed to devise a way to ensure the integrity and avoid any fraud (which is known as double spend). As a consequence, Nakamoto created a software system that comprises a network of participants (nodes) governed by a protocol that enables them to transact directly together while validating the integrity of the transaction via solving a mathematical puzzle. The solution of the encrypted mathematical puzzle is called cryptographic proof (Nakamoto, 2008), or proof-of-work (PoW). This gave rise to a whole system which Nakamoto called Bitcoin.

4.3.2. Modeling the Bitcoin: Conceptualizing the System

As discussed earlier, Bitcoin is a system that consists of the communication channel like internet, the individual participants represented by their devices called the nodes, the software platforms which include the wallet and trading platforms, and the software represented by the ‘accounting’ ledger (blockchain). The whole framework is governed by a set of rules, a protocol, that ensures the whole system is operating in coherence.

A key factor to model the Bitcoin is to understand what the system is trying to achieve. The whole purpose of the system is to eliminate the intermediaries, consisting of the financial institutions, and strip the transactions from the involvement of third parties. In other words, the transaction should occur between the two contracting parties

directly, peer-to-peer, similar to the face-to-face transactions of the real world. But, with the real world's face-to-face transactions, the receiver can directly ensure that the transferer of money actually does have the amount required readily available. Also, being face-to-face implicates that the receiver can verify the true identity of the other contracting party. Otherwise, the transaction can be easily cancelled before it takes place. This answers the question what the system is trying to achieve. Therefore, the verification of the identity and the availability of the required amount need to be offloaded to the Bitcoin system. On the other hand, the documented paper/receipt makes the backbone for the proof that a transaction happened in the traditional real-world application. In other words, the Bitcoin system needs to verify the transactions and record the history of their occurrences in the blockchain, the ledger explained before. With that being said, the author proposes a high-level model, illustrated in Figure 4.1, that explains how the hardware technology layers and software or application layer talk to each other in the Bitcoin system and how they are governed by the Bitcoin protocol.

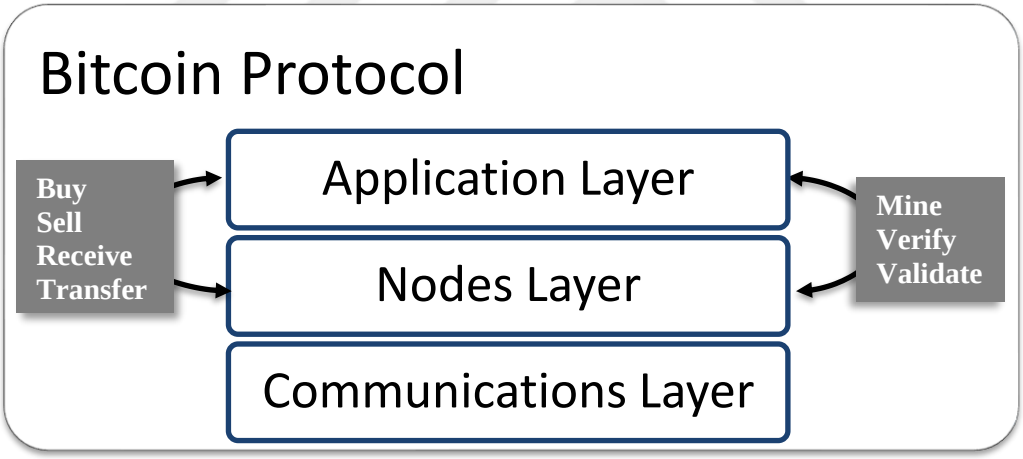

Figure 4.1: Conceptual Model of Bitcoin

Source: Author

The above figure displays three layers for the Bitcoin system. The lowest layer is the communications channel on top of which the other two layers can operate. The communications layer is the backbone, without which the whole system cannot be established. This layer is mainly the internet and all the physical devices involved like routers, gateways, and cables. Above that layer are the nodes represented by the devices of the individual participants in the system. These devices are computers, tablets, mobile phones, etc. These devices represent the physical interface for the

actions taken by the participants. On top of this layer, is the application layer which provides the nodes layer the means to carry out their transactions: buying, selling, transferring, receiving, mining, and validating.

Similarly, this layer represents the software interface for the actions decided by the participants. All the three layers sit on top of the Bitcoin protocol which is a set of rules that govern the whole framework. The rules address questions like how is the blockchain ledger distributed or updated, what is the maximum size of daily transactions, how is the cryptographic puzzle determined, what happens should a conflict occur in the blockchain, and who can add a block to the blockchain[11].

The application layer and nodes layer talk to each other on either of two main fronts. This segregation indicates that there are two different broad types of users to the system: buyers/sellers/transferers/receivers, and miners/validators. The first front occurs when one user wants to buy a commodity from a seller (or transfer bitcoins to another), or conversely wants to buy/sell bitcoins. In the former case, the user sends the bitcoins to the other party using the bitcoin wallet software. In the latter, the exchange platform provides the desired exchange rate. These two cases trigger another set of application-node layer communication which forms the second front. This time the transaction is broadcasted seeking a 'miner' whose whole task is to add a new block to the blockchain, recording the transaction's information. Because this action is rewarded with the production of new bitcoins, there will be a competition among the miners as to who will win the right of adding the block. Miners expend CPU power to solve the cryptographic puzzle. The miner who solves it first will be able to add the block and broadcast the new blockchain. The mining process is then followed by a validation process. To ensure that there are no cooperating group of attackers or fraud action, all other nodes in the network will have to validate the newly added block.

4.3.3. Modeling the Bitcoin: Operationalizing the System

In a direct one-to-one transaction, security is guaranteed by the difficulty to counterfeit fiat currency. In the current traditional digital transaction over a communications

[11] To record a new transaction in the ledger, a participant will insert this information in a special form called a block which in turn is appended to the end of the existing blockchain.

channel, like e-commerce, security is guaranteed by a third-party financial institution. The latter ensures that funds exist, legitimate owners of the funds are indeed those who carried out the transaction order, and money transfers are carried out smoothly between the intended parties. Essentially, a financial institution provides three main services during a transaction. Firstly, it provides account management, secondly, legitimacy is ensured through authentication to safeguard against any possible impersonation, and thirdly, the financial institution updates the balance and keeps track of all transactions (Savla, 2023c). However, in a peer-to-peer model, the absence of such a third-party guarantor raises several challenges. A virtual currency represented by code can be theoretically copied. Besides that, a malicious participant can choose to use the same funds in two or more transactions, the act of which is called double spending. As noted before, Satoshi's Bitcoin overcame these challenges by having all nodes (participating devices in the network) maintain the same copy of blockchain and through the validation consensus conducted by all nodes on the PoW (Savla, 2023c).

4.3.3.1. Node Types: Roles and Functions

While all nodes in the Bitcoin network are equal, they still can assume different roles depending on the functionality they support (Antonopoulos, 2014). Figure 4.2 details the various roles that a node can assume in a Bitcoin network and what functions characterize each role. Collectively, these functions are: routing, maintaining the blockchain ledger, mining, and conducting wallet functionality (Antonopoulos, 2014). What can be observed from Figure 4.2 is that all nodes perform the network routing function. In other words, all nodes validate and propagate transactions and blocks, and discover and maintain connectivity with other peer nodes (Antonopoulos, 2014). To be a full blockchain node, a node has to additionally host a complete copy of the latest blockchain database. Due to the latter fact, a full node can autonomously and authoritatively verify any transaction without external reference (Antonopoulos, 2014). A full node can also host the wallet client application like in the case of the 'Reference Client (Bitcoin Core)'.

The wallet is the graphical interface for users to create transactions by sending funds to others or exchanging or creating payment requests to receive funds from others, the details of which will be explained shortly in subsection 4.3.3.3 when describing the whole process from initiating a transaction to recording it on the blockchain. On the other hand, a node can be a solo miner in which case it opts for not having a wallet

client application. So, it will only conduct routing, mining (which will also shortly be discussed in subsections 4.3.3.2 and 4.3.3.3) and maintaining a full copy of the blockchain. However, hosting the up to date blockchain database is storage intensive.

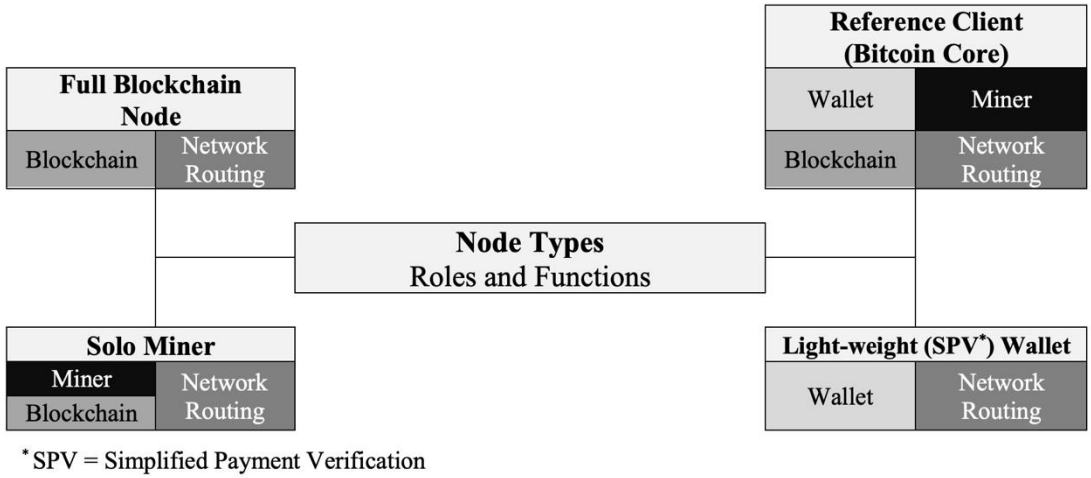

Figure 4.2: Node Types

Source: Author, adapted from Antonopoulos, 2014

As of 13th February 2023, the blockchain size almost reached to 455 Gigabyte which is almost half the size of today's hard disks (*Blockchain Size (MB)*, 2023). Some devices like smart phones are resource-constrained and, therefore, can't host the full blockchain database. Instead, these devices host and maintain a subset of this database and verify transactions using a method called 'Simplified Payment Verification' (SPV) (Antonopoulos, 2014). This forms the fourth role portrayed in Figure 4.2, namely the lightweight (SPV) wallet node. These nodes only host the wallet and carry out routing using SPV.

4.3.3.2. Node Routing

Since routing is executed by all nodes regardless of the role each will assume, this functionality is critical for the Bitcoin network which is built on communication among the network members. Hence, it is very important that the protocol holding them together should be resilient and reliable. Examining how a node handles conflicting or invalid data is key to determining this aspect. Figure 4.3 summarizes the output decisions of a node when receiving full content of block or transactions. The figure describes how a node contributes to the performance optimization of the whole network by observing a set of rules. These rules ensure to limit the data by avoiding invalid or conflicting data sent by non-compliant nodes. For instance, a node will only

relay incoming transactions and blocks that are valid. Invalid ones will not pass through. Another example is the reaction to forks. A fork happens when two or more different miners/nodes each send a different new block to be added to the existing blockchain. Which of these blocks should be added at a fork? The node will only relay the first block it hears of. The rules also ensure to eliminate infinite propagations. For example, a node will forward new transactions only once.

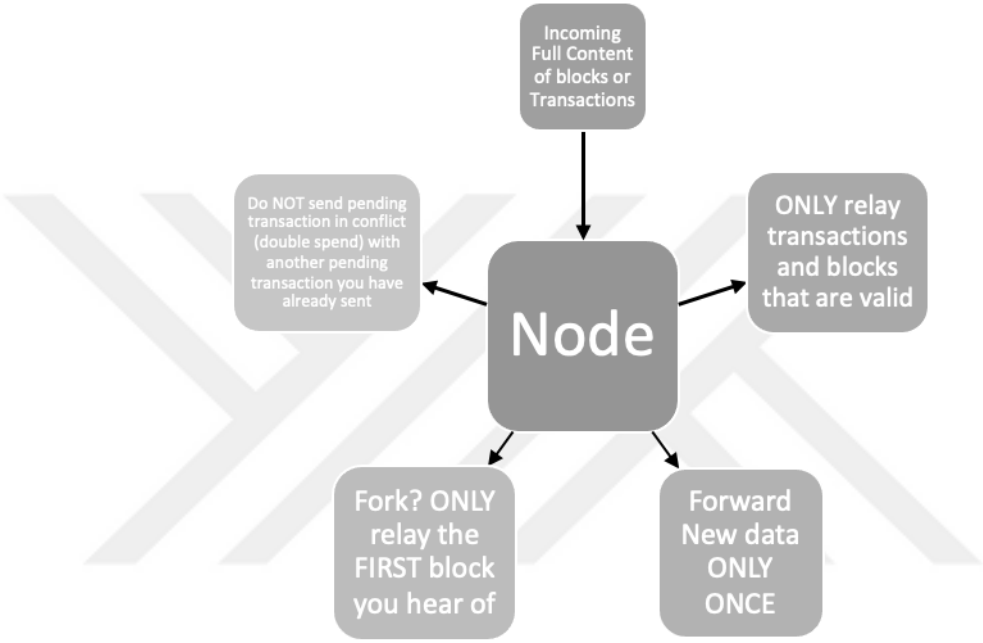

Figure 4.3: Communication Protocol with Optimized Performance

Source: Author

4.3.3.3. Operational Steps

After looking at the operational aspects of the types of nodes, their roles and functions, and studying how nodes route information, we now need to visit each step involved from the initiation of the transaction to recording it on the blockchain. This means moving through the whole process involved from a user's perspective as his bitcoin/s leave/s his wallet to another user's wallet. Figure 4.4 depicts this process and puts all the aforementioned explanations in this section together. The first step in the process is the desire for a payment or transfer of funds. It is the process of initiating a transaction. At this stage, the user will open his secure wallet (usually a light-weight client application of Bitcoin) and create a send (transfer of funds), exchange (exchange bitcoins with fiat currency), or swap (exchange between two different

cryptocurrencies) request. Conversely, a seller can create a payment request from his wallet which creates a quick response (QR) code that the user can scan from his wallet to make the payment (Antonopoulos, 2014). Upon the request, next the wallet starts the second step which is the process of creating a new transaction. To ensure legitimacy and availability of funds, Bitcoin adopts digital signatures by using private-public key cryptography. The randomly generated private keys provide the identity in Bitcoin (Savla, 2023b) and is only known by its owner. It is used by the owner of the funds to encrypt, that is, digitally sign, the message for transferring the funds.

The public key is generated from the private key (*Wallets*, n.d.) forming, as such, corresponding pairs. This public key is essentially the key distributed to the public that allows others to verify the true identity of the sender. This cryptographic technology allows Bitcoin to maintain a tamper-evident transactions (Savla, 2023b). Tamper-evident means if the transactions are manipulated by a malicious entity, that modification will be obvious for the entire network and thus will be rejected. Almost all wallets keep track of all private keys of the owner that can unlock his corresponding funds which are preserved in the "unspent transaction outputs" of other transactions; otherwise, the Bitcoin network is queried to retrieve this information (Antonopoulos, 2014). Depending on its algorithm, the wallet will use one or more of those unspent transaction outputs to feed as input/s to the new transaction. In order to do so the chosen unspent transaction outputs need to be unlocked with their corresponding signatures (private keys) until funds are sufficient for the intended transfer/payment. This is what is referred to as signing the transaction. As the required inputs are found, the wallet will create the first output for that new transaction locking it with the address (public key) of the recipient. In most cases a change remains, so, a second output is created which contains the amount to be returned to the sender. Of course that output is locked with the address (public key) of the sender (Antonopoulos, 2014). The wallet now is ready for the third step which is the process of transmitting this new transaction.

The wallet sends this new transaction to any neighboring node it is connected to (Antonopoulos, 2014). When a Bitcoin node receives a valid transaction that it hasn't encountered before, it promptly disseminates it to all connected nodes, see Figure 4.3, a process commonly referred to as flooding (Antonopoulos, 2014) allowing the whole network to see that transaction. As such, each node will store a copy of the valid transaction in its own pool of unverified transactions (Antonopoulos, 2014).

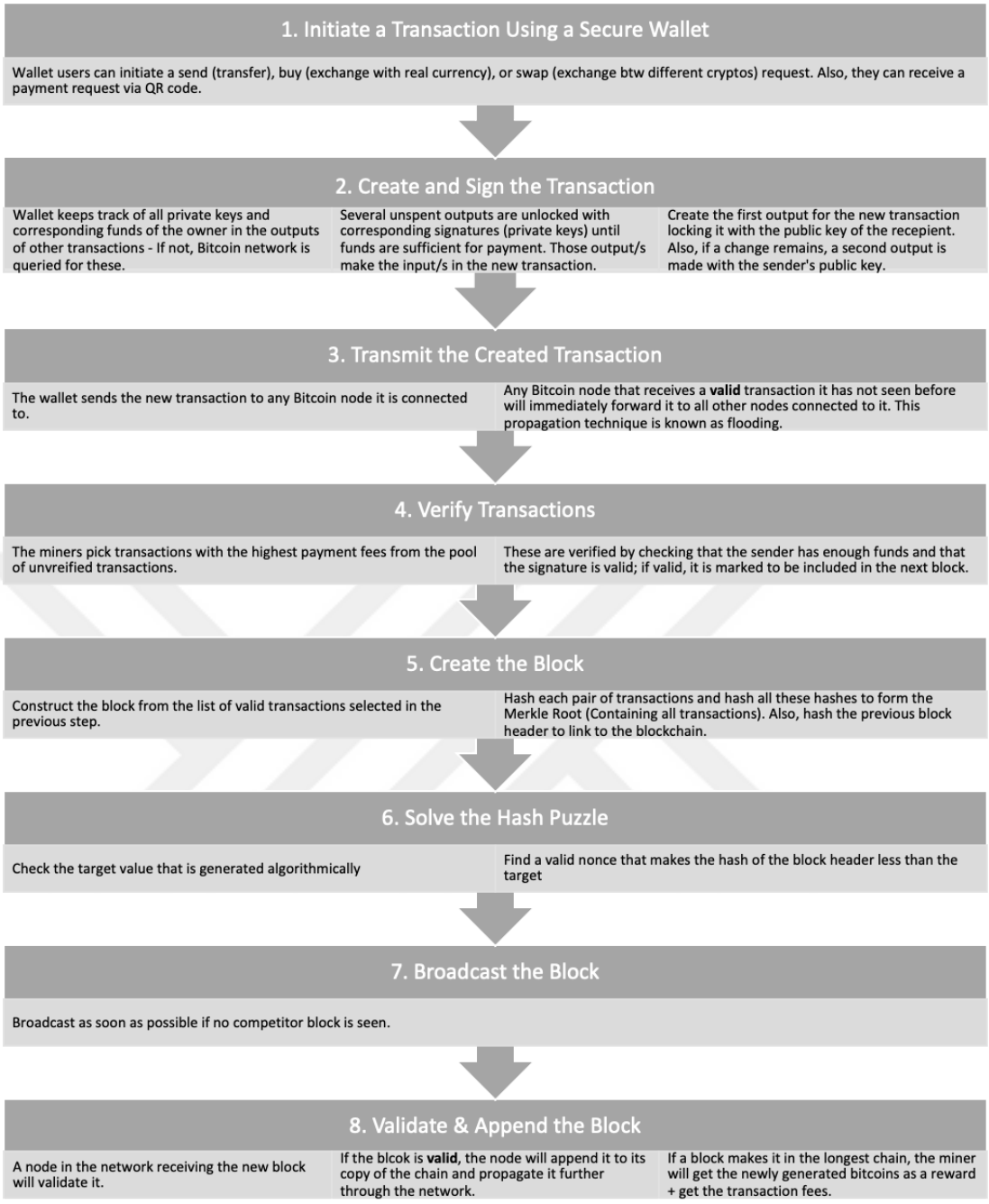

Figure 4.4: The Operational Model of Bitcoin

Source: Author

The fourth step will be the boundary which marks the start of the other front of the model which is mining. In this process, miners will pick up the transactions with the highest fee payment from the pool of unverified transactions, verify that they are valid, and if so mark them to be processed for the next block in the blockchain (Savla, 2023a). Step five involves the process of creating the block. All the selected valid transactions from the previous step will be used to construct the block data. This is done by using

cryptographic hashing to hash each pair of transactions and then hashing all these hashes to form what is called the Merkle Root (Savla, 2023a). In this step, the previous block's header is also hashed to provide for linking to the previous block in the blockchain. In step six, the miner will try to solve the hash puzzle. This is done by finding a valid value called the nonce that makes the hash of the block header less than the target value generated by the Bitcoin algorithm (Savla, 2023a). Essentially by doing so, the miner would have solved the PoW (Savla, 2023b). The seventh step involves broadcasting the new block. The miner will carry out this step as soon as possible, provided it hasn't seen any competitor blocks (Savla, 2023a). In the last step, step eight, any node receiving the block will validate it. In case the block is verified to be valid, the node will append it to its copy of the chain and further propagate it (the block) to others in the network (Antonopoulos, 2014). If the block makes it in the longest chain, the miner who created the block and solved the puzzle will receive the newly generated bitcoins in addition to the transaction fees (Savla, 2023a).

4.4. Differences Among Cryptos

Antonopoulos (2014) argues that there are three areas where altcoins differentiate from Bitcoin. This aspect clearly conveys that all cryptos and Bitcoin are not synonymous, despite being similar in certain features and structures. The diversity among all cryptocurrencies and the existing differences between them in terms of the purpose of their initiation, consensus mechanism, rules and policies, and consequences need to be realized. For example, in terms of the consensus mechanism, Bitcoin uses the 256-bit Secure Hash Algorithm (SHA256d) PoW with double hashing, while some altcoins such as BlackCoin (BLK), VeriCoin (VRC), and NXT (Antonopoulos, 2014) use proof-of-stake (PoS) or other mechanisms. Additionally, altcoins vary in terms of their purpose and objectives. For instance, some altcoins are designed to offer greater privacy, while others aim to improve transaction speeds such as Litecoin (LTC) and Dogecoin (DOGE) (Antonopoulos, 2014). Understanding these distinctions is crucial in evaluating each cryptocurrency, gaining a more comprehensive understanding of their ecosystem, and developing effective strategies for managing their challenges. This is key to developing a framework that will help analyze their issues.

Since the introduction of the first cryptocurrency in 2009, the number of new cryptocurrencies has grown exponentially. According to CoinMarketCap's report in 2022, there were around 21,910 cryptocurrencies, which had a total market

capitalization of $850 billion (Hicks, 2022). As of 2023, just two months later, this number has increased to 22,644 cryptocurrencies, a rise of 734, with a total market capitalization of roughly $1.085 trillion (*All Cryptocurrencies*, 2023). The substantial quantity of cryptocurrencies presents a significant challenge when attempting to analyze them. However, Antonopoulos (2014) maintains that most of the alt-coins differ very slightly from Bitcoin, yet there are some notable exceptions and very important innovations. Therefore, cryptocurrencies can be broadly classified into several categories based on their unique features and characteristics. One classification system groups cryptocurrencies as either payment-focused or asset-focused. Payment-focused cryptocurrencies, such as Bitcoin, are primarily used as a medium of exchange, while asset-focused cryptocurrencies, such as Ethereum (ETH), are designed to support decentralized applications and smart contracts. Another classification system is based on the consensus mechanism used by the cryptocurrency. For example, PoW-based cryptocurrencies rely on computational power to validate transactions, while PoS-based cryptocurrencies rely on the stake held by users in the network. Other consensus mechanisms, such as delegated PoS and a combination of several different hashing techniques PoW, have also been implemented in various cryptocurrencies. In addition to these classifications, cryptocurrencies can also be distinguished based on their governance structures, with some cryptocurrencies being more decentralized than others. This study utilizes a modified version of the classification system developed by Härdle, Harvey, & Reule's (2020) to categorize cryptocurrencies based on their intended purposes. This classification system is particularly suitable because it covers a wide range of general purposes for which cryptocurrencies have been created. Specifically, it groups cryptocurrencies into six broad classes, including peer-to-peer (P2P) money transaction, distributed computation, non-fungible token (NFT), utility token, security token, and stablecoin. In the following subsections, each of these classes will be further elucidated.

4.4.1. P2P Money Transaction

Bitcoin belongs to this class of cryptocurrencies because it was intended as a medium of exchange to carry out P2P money transactions. It has been detailed in the preceding section, which explained its underlying mechanisms in depth. Several cryptocurrencies share similar features with BTC either by being forked from it or by utilizing the BTC open-source code as a basis for their development. These altcoins fit within the same

broad class as BTC but differ in their monetary policies and their implementation of the PoW hashing techniques; see APPENDIX A for more about hashrates. Notable examples of altcoins that belong to this class include LTC, DOGE, and Freicoin (FRC) (Antonopoulos, 2014; Härdle et al., 2020).

4.4.2. Distributed Computation

Cryptocurrencies that fall under the category of distributed computation utilize blockchain ledgers to process smart contracts, which are essentially small programs capable of executing specific functions such as domain name registrations (Antonopoulos, 2014). The network in this class can be visualized as an internet-based computer, where smart contracts are executed on each node, functioning as the network's distributed computational power (Härdle et al., 2020).

Before the inception of the first cryptocurrency, cloud computing was the latest technological advancement enabling reliable execution of programs on centralized servers. The distributed computation cryptocurrency class can be thought of as providing similar functionality to some extent. However, rather than depending on centralized servers, these cryptocurrency systems distribute computations on every node of their network. As part of the block verification process, every node executes the low-level code of the smart contract, which can be perceived as the transition state that moves the blockchain from the current state to the new state (Savla, 2023d).

To facilitate payment for executing these contracts, the cryptocurrency system offers its own payment tokens. For example, Ethereum, the first cryptocurrency in this category, has its own built-in currency called ether that serves as payment for executing its smart contracts (Antonopoulos, 2014). In addition to Ethereum, a few examples that fall in this category are Tezos (XTZ), EOS, and DFinity (Härdle et al., 2020).

The differences between the P2P money transaction category and the distributed computation can be delineated by comparing the highest market capitalization and most popular in each category: Bitcoin and Ethereum. In fact, with a market capitalization of $640 billion (*All Cryptocurrencies*, 2023), among all cryptocurrencies, both of Bitcoin and Ethereum rank the first and second respectively. Some of the most notable differences existing between these two include the main purpose and functionality, the complexity of the system, account management, the

consensus mechanism (PoW or PoS), and scripting language for verification and running the system. Table 4.1 details these differences. Continuing with the example of Ethereum, its architecture is designed to enable distributed and trustless computation rather than optimizing computational efficiency. This implies that every node in the network has to run the same computation, resulting in redundantly parallel execution (Savla, 2023d). However, since the execution is run on all nodes, it is expensive, making it unsuitable for running training sets for machine learning on the blockchain. Moreover, while building smart contracts is easy, securing them is challenging.

Table 4.1: Main Differences Between BTC and ETH Networks

Bitcoin	Ethereum
'Gold Standard' Transaction Blockchain	Smart Contract Blockchain Platform
Simple and Robust	Complex and Feature-Rich
Primitive Scripting Language (not Turing-Complete)	Turing-Complete Scripting Language
No Accounts – Depends on Unspent Transaction Outputs (UTXO)	Account-Based
Consensus Mechanism: PoW	Consensus Mechanism: was PoW but recently moved to PoS

Source: Savla, 2023d

Despite these limitations, the Ethereum blockchain has numerous applications, including the creation of smart assets such as new tokens and currencies, and the implementation of wallet control by multiple addresses through m-of-n multiple signatures (MultiSig). It can also be used for proof-of-existence, where a hashed document can be recorded at a specific point and later revealed, as well as for title deed ownership in corrupt underdeveloped countries, where ownership of documents can be associated with addresses on the blockchain.

The Ethereum blockchain can also be utilized for prediction markets, including hedging, insurance, and voting, as well as for diamond trail tracking in supply chain management to ensure the origin of goods. In addition, it can facilitate the creation of smart contracts through a build service, allowing untrusting parties to donate money to a contractor who will build the infrastructure for them, as is the case with smart

grids. Finally, the Ethereum blockchain can be used to tokenize stocks and enable after-hours trading.

4.4.3. Non-Fungible Token – NFT

The essence of NFT is to create a unique representation of something so that it cannot be replicated. It is a digital signature of an artwork or collectible (songs, music, pictures, videos, or video games) that is stored on a blockchain. The artwork or collectible is mainly digital, but could also be physical (*How to Create an NFT*, 2023). Since it is stored on the blockchain, hence, it is a type of cryptocurrency. While the underlying work or collectible can be copied or replicated, the digital signature of that specific work makes it unique. The two most common blockchain networks for creating NFTs supported by most crypto wallets available nowadays are Ethereum and Binance Smart Chain (BNB Chain), but the list also includes Polkadot[12], TRON[13], Tezos[14], and many more (*How to Create an NFT*, 2023). Figure 4.5 shows the process of creating an NFT.

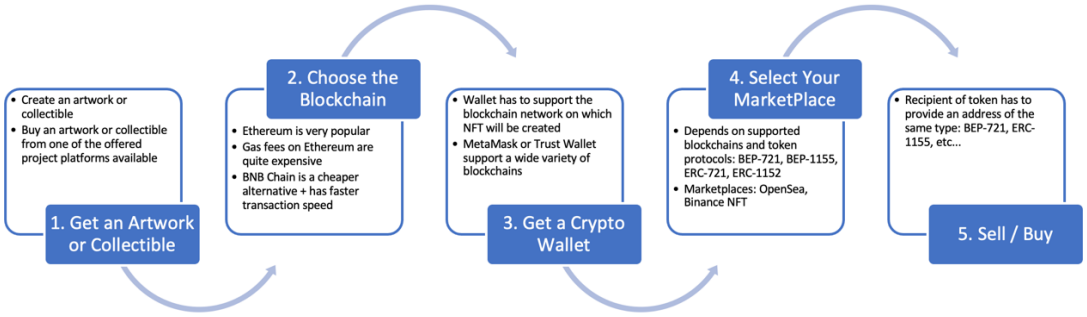

Figure 4.5: Process of Creating an NFT

Source: Author

[12] Polkadot: a platform for Web3 to create and connect decentralized apps, services, and institutions (*About Polkadot, a Platform for Web3*, n.d.)

[13] TRON: a decentralized autonomous organization (DAO) and a platform for smart contract functionality (Sun, n.d.)

[14] Tezos: an open-source blockchain that can execute P2P transactions and serve as a platform for deploying smart contracts (*Home | Tezos*, n.d.)

As can be seen from the figure, part of an NFT system is having a marketplace platform to buy and sell NFTs. Besides one's own artwork, there are other platforms carrying out projects that produce NFTs and offer them for minting by the community. The person to mint any of these offered works will have the chance to sell it on the marketplace. The minting process incurs transaction fees, called gas fees, which are determined by the amount of computational work required. So, demanding tasks will have a higher gas cost than less demanding ones (Ifegwu, n.d.). Similar to how physical artworks are valued, there are many factors that determine the value of an NFT, among which are the specific use cases, aesthetic qualities, exclusive community access, and the project's founding team or creator's reputation (*A Guide to NFT Rarity*, 2022). While the previous are very important in valuing NFTs, some platforms and marketplaces calculate and rank NFTs based on their rarity by using a rarity index in order to guide sellers and buyers about their prices. Rarity index is calculated by these tools by accessing blockchain explorers and other data sources to estimate an NFT's rarity (*A Guide to NFT Rarity*, 2022). The higher the rarity index, the more unique and usually more desirable is the NFT.

Although considered a cryptocurrency due to the fact that it is stored on a blockchain, an NFT acts more like a commodity than money. Money in the form of other crypto is paid in exchange for a certain NFT. The added value in producing rare pictures or digital signatures to make a collectible unique might be questionable from a *Sharī'ah* perspective. Of course, NFTs of impermissible representations like nakedness are not even considered. Another question that might be coming to mind is why would anyone want a uniquely digitally signed artwork while the underlying asset itself can be easily replicated? A person surfing these marketplaces can easily realize how the illusion of rarity seems to drive the market demand for the NFT. But, to understand these desires we can take Mont Blanc watches and pens as an analogy of an NFT. Although technology makes it easy nowadays to create replicas of these products with close to original quality, some people are more willing to pay hefty prices to get those Mont Blanc watches and pens produced by the original company because of their uniqueness and prestige. Therefore, the NFT replicas are "Just not the same in the mind of a collector" (*How to Create an NFT*, 2023). On the other hand, applications for *Sharī'ah* using these NFTs have started to emerge. Some researchers have thought of the use of NFTs to provide an easier approach for the verification of ḥalāl licenses or certificates.

Other applications see the tokenization of sensitive customer data like passport and driving license information into NFTs.

4.4.4. Utility Tokens

Utility tokens are cryptocurrency tokens on a smart contract blockchain issued within their own use cases on a Web3[15] project. Unlike Bitcoin, they are not designed to be medium of exchange because they are not meant to store value in the long term or act as hedges for inflation, hence why the definition has been restricted to 'their own use cases'. Such tokens are not mined like in the previous types of cryptocurrencies, instead they are 'pre-mined' by the project leaders and sent to members, investors, and the general public (*What Is a Utility Token?*, 2022). Governance tokens are one of the most common utility tokens. The owners of these tokens will have the right to vote on upcoming improvements, updates, or upgrades to a decentralized application. Typically, one token represents one vote. The more tokens one own, the more votes he will be entitled to. Another example of utility tokens is those given by the developers of a blockchain game to their game players. The players can use the tokens to purchase in-game items or upgrade their playing characters.

A third example is the provision of discounts and rewards. Binance allows its users to earn reward tokens from their crypto holdings (*How to Earn Rewards On Your Crypto Holdings*, 2022; *What Is a Utility Token?*, 2022). A fourth way where utility tokens are used is rewarding content creators through a decentralized application's tipping mechanism. This function may influence the ranking of comments or videos on a decentralized social media application (*What Is a Utility Token?*, 2022). Another way utility tokens can be used is in the case of a smart contract on a blockchain that will not accept paying transaction fees except in its own native tokens. Because of all the

[15] Web3 refers to the third generation of the web after Web1 and Web2. Web1 is the first wave of the web that did not provide its users more than a mere of static pages to read from. Web2 was a great jump from Web1 where users were allowed to interact, comment, perform tasks with web applications; this wave included the burst of the social media. Web3 is the third wave that moves away from having data and control on giant centralized servers, like Facebook and Google, to have data and control decentralized over blockchain networks.

examples aforementioned, utility tokens have no legal restrictions, and, in fact, these utility tokens do not need the US Securities and Exchange Commission's (SEC) approval to be listed on crypto exchanges. This is unlike a security token which involves a share in a company, and which requires the approval of SEC to be listed on exchanges in the US (Majaski, 2022; *What Is a Utility Token?*, 2022). Therefore, a "cryptocurrency must provide a viable use case beyond mere speculation to qualify as a utility token" (*What Is a Utility Token?*, 2022).

4.4.5. Security Tokens

A security token is another type of cryptocurrency. Stored on the blockchain, it is a digital representation of an investment asset like a stock, bond, option, or future. A security token is created through a process called tokenization. This is similar to when a company, for example, wants to raise funds through selling some of its stocks on a security exchange. However, the only difference is that these assets to be tokenized are assigned a randomized number, the token, on a blockchain and then it gets offered in an exchange for investors. The ownership would then be recorded on the blockchain (Majaski, 2022).

Companies tokenizing their securities most commonly choose to do so using ERC-20 tokens, which are Ethereum-compatible tokens that can run on the Ethereum blockchain (*Security Token*, n.d.). The intended purpose, therefore, for these tokens is investment. Holders of these investments will be able to see their ownership, value, and any dividend through their wallets (Majaski, 2022).

Although their purpose was not intended as securities, but as payment transactions, Bitcoin and Ethereum have been used by investors and traders on cryptocurrency exchanges where it was thought they could reap a lot of return. Nonetheless, SEC doesn't view Bitcoin and Ethereum as securities (Hinman, 2018).

4.4.6. Stablecoins

Stablecoins are cryptocurrencies that drive their values from the underlying asset they are pegged to. The whole purpose of introducing stablecoins is to avoid the price instability of traditional cryptocurrencies like the Bitcoin. There are four main categories of stablecoins according to what they are collateralized by. The first category involves stablecoins collateralized with fiat currency. Examples include those that are designed to be fully collateralized by US dollar deposits (such as tether USDT

and Circle's USDC), and those collateralized by the GBP, pound sterling (such as London Block Exchange Pound-Pegged, LBXPeg) (Härdle et al., 2020). Also included in this category are the coins investigated by central banks like US Federal Reserve's Fedcoin, European Central Bank's Eurocoin, and Bank of Canada's CAD-coin (Härdle et al., 2020). These fiat-backed stablecoins keep a fiat currency, such as USD and GBP, in reserves and any drift in the price of the token from its underlying fiat will be brought back to its fixed rate by arbitrageurs (*What Is a Stablecoin?*, 2023).

The second category are stablecoins that are pegged to real assets like precious metals or real estate. Examples include Digix Gold (DGX) that is collateralized by gold, Tiberius coin (TCX) that is collateralized by a basket of seven precious metals in technology, and Swiss Real Coin (SRC) that is collateralized by Swiss real estate (Härdle et al., 2020).

The third category are the stablecoins that are pegged to a reserve of cryptocurrencies. Given the high volatility of the cryptocurrency market, stablecoins backed by crypto assets adopt a strategy of over-collateralizing reserves to mitigate the impact of price fluctuations (*What Is a Stablecoin?,* 2023). An example of this category is DAI coin offered by market Decentralized Autonomous Organization (DAO) (Härdle et al., 2020).

The fourth category, unlike the other three categories, removes the need of reserves and instead algorithms and smart contracts manage the supply of the stablecoin tokens. If the stablecoin's price fall below the value of the fiat it tracks, the algorithm will reduce the token's supply by locked staking, burning tokens, or buy-backs (*What Is a Stablecoin?*, 2023). If the price increases beyond its fiat currency, the algorithm will issue new tokens into circulation.

The fact that stablecoins are pegged to something, implies a constant use of monetary policies in order to maintain the value of the peg. Many stablecoin projects have failed in doing so; when a stablecoin has constant issues in maintaining its peg, it can dramatically lose its value (*What Is a Stablecoin?*, 2023). Therefore, stablecoins aren't guaranteed to maintain their peg.

One of the risks users of stablecoins should bear is the lack of transparency. Not all issuers of stablecoins release full public audits (*What Is a Stablecoin?*, 2023). Also, issuers of stablecoins centrally hold the collateral giving them significant control over

the coin. Users of these coins will have to trust that these central entities have the reserves they claim.

4.5. *Sharī'ah* Compliance Risk Analysis

Table 4.2 presents a summary of the problematic issues that have been identified in extant literature and deliberated upon by contemporary jurists. These issues give rise to risks pertaining to compliance with the *Sharī'ah*. The identification of issues in Table 4.2 primarily stemmed from the contemporary researchers' examination of the Bitcoin, with limited consideration given to other cryptocurrencies. Specifically, the first three issues pertain to the lack of authority and oversight, which arises as a result of decentralization, a pervasive attribute observed in the majority of cryptocurrencies, albeit with variable degrees.

Nonetheless, such an observation does not apply universally to all cryptocurrencies. For instance, Ripple functions as an alternative to SWIFT and is built and utilized by financial institutions, thereby refuting issue number 3 in the table. Another example is Ethereum, whose organizational and community leaders are well-known figures, such as Vitalik Buterin, the founder of Ethereum, Gavin Wood, the Chief Technology Officer (CTO), and Nick Szabo, one of its researchers. Thus, the first issue scarcely applies to Ethereum, while the issuer is recognizable, rendering issue 14 irrelevant. In contrast, issue 2 does not hold for stablecoins that the central banks of a state issue. For a non-state issued cryptocurrency, the ramifications of issue 2 could become inconsequential if the state permits its usage. Notably, in the United States, physical Bitcoin ATMs are available with the purpose of facilitating the exchange of Bitcoin (both buying and selling) for cash. It follows that the first three issues demand meticulous scrutiny within the context of the cryptocurrency being examined to avoid hasty and premature generalizations.

Issues 4 through 7 are related to the volatility and speculative nature of cryptocurrencies. Similar to the previous discussion, issue 4 which is related to stability and price fluctuations does not hold for all types of cryptocurrencies. For instance, being backed by sovereign currencies, stablecoins are relatively stable. However, cryptocurrencies that are characterized by high volatility warrant further examination. As known, volatility at certain times can also affect other types of money

like fiat money despite being a legal tender. Yet, fiat money is still trusted to hold one's wealth.

Table 4.2: Issues Identified from Extant Literature

Issues – Extant Literature
1. Lack of regulations and regulatory bodies
2. Lack of issuing authority (usually the state)
3. Lack of association with any financial institution
4. Stability and price fluctuations
5. *Gharar*
6. Resemblance of gambling (on Mining, Stability, Speculative Investment)
7. Speculative investments
8. *Jahālah* (of Miners)
9. Inheritance Issues
10. Loss of Password
11. Not backed by any asset
12. Virtual and having no physical existence
13. Lacking intrinsic value and are not legal tenders
14. The unknown issuer of the altcoin is necessarily the controller of it
15. Adding imaginary blocks to the blockchain (Malicious Attack)

Source: Author

Whether volatility is caused by a temporary external factor (market forces, speculation, explosion of adoption) or is intrinsic to the subject, might be key to studying the *Fiqh* issue of cryptocurrency. For example, the sudden and significant price fluctuations of Bitcoin, Ethereum, and many other cryptocurrencies happened synchronously between the beginning of 2021 and end of 2022. This calls for a real statistical study to ascertain the extent to which such fluctuations are temporary or enduring.

Issue 5, which pertains to the preservation of people's wealth, is a general concern that warrants careful attention to every aspect of the cryptocurrency system. To simply

claim the existence of *Gharar*, or excessive uncertainty, is insufficient. It is crucial to identify where *Gharar* exists within the system.

Issue 6, which relates to the resemblance of cryptocurrency mining to gambling, is a matter that demands further scrutiny. While mining entails competition among miners, the winner does not claim the rights of others. Rather, the winning miner receives crypto tokens from the cryptocurrency system, and no other miner's rights are affected. Mining is thus more akin to a race competition than to gambling. The loss of efforts that inevitably accompanies competitions, such as the loss incurred by a losing racer, does not amount to gambling. Moreover, stability issues, which may give rise to concerns about gambling, can be addressed by the aforementioned discussion of stability and price fluctuations.

As for issue 7, which concerns speculative investment, it is a matter that is external to cryptocurrencies and must be subject to the rules of trading and to the scrutiny of the platform on which the speculation occurs. Any rulings arising from issues related to this issue should affect only the conduct and the parties responsible for that conduct, rather than the cryptocurrency itself. Issue 8, which pertains to the ignorance (*Jahālah*) of the miner, has been called into question due to a flawed assumption that miners are active parties in trading transactions. This flawed perspective undermines the validity of the issue, as it fails to recognize that miners merely function as bookkeepers within the context of cryptocurrency transactions.

Issues 9 and 10, which relate to the wealth of people, are of paramount importance from a *Sharī'ah* perspective. Inheritance, which forms one avenue for the circulation of wealth, and the security of one's wealth, which is integral to the preservation of property rights, are both essential considerations that must not be overlooked. It is noteworthy that both of these issues fall under the purview of wallet management within the cryptocurrency system.

The formulation of Issues 11 through 15 appears to be lacking solid grounds. Issues 11 and 13 are closely related, both raising concerns about the lack of assets or entities to back the value of non-stablecoin cryptocurrencies. However, many countries now recognize cryptocurrencies like Bitcoin and Ethereum, and their value is derived from trust in their networks, as well as market forces and state approval. Failing to

acknowledge these factors could invalidate all non-stablecoin cryptocurrencies, including ones like Bitcoin, which continue to grow in value.

Issue 12, which asserts that cryptocurrencies are non-physical and virtual, has been refuted previously. *Sharī'ah* acknowledges non-physical properties and rights such as copyright, patents, and software. Therefore, the non-physical nature of cryptocurrencies does not inherently pose a problem from a *Sharī'ah* perspective.

Issue 14 claims that the issuer of a cryptocurrency necessarily controls it, but this is a technical fallacy. Altcoins that derive their blockchain from Bitcoin, including Islamic altcoins, use the open-source code of Bitcoin which can be read and verified by anyone. The issuer of a cryptocurrency is not necessarily the controller of it, as the technical code is open to anyone for verification.

Issue 15 is a technical issue that can lead to *Gharar*. However, the formulation of this issue contains technical inaccuracies that give the illusion that imaginary blocks can be added when needed. This is not the case, and the issue needs to be revised to capture the actual technical issue that could lead to *Sharī'ah* compliance risk. Nonetheless, it is important to consider the technical aspects of cryptocurrencies when evaluating their compatibility with *Sharī'ah* principles.

Based on the aforementioned analysis, several observations can be deduced. Although the prevailing literature raises valid concerns regarding the violation of *Sharī'ah* principles, some issues are sufficiently weak to warrant exclusion from further consideration. Specifically, issues 6 (resemblance of gambling), 8 (*Jahālah* of the miner), 12 (virtual and no physical existence), and 14 (the unknown issuer is necessarily the controller) are deemed to be of negligible significance. The justifications for refuting these issues have been previously articulated, and therefore, repetition is deemed unnecessary. In contrast, issue 5 (*Gharar*) is a valid *Sharī'ah* concern; however, its specificity must be contextualized. Consequently, issue 5 will be removed from the present list but will be referred to when relevant. The remaining issues can be categorized into four primary themes, namely regulatory concerns, financial considerations, security concerns, and value concerns.

Table 4.3 presents an overview of pertinent information related to each issue and how it pertains to each theme. Of the ten remaining issues, six are specific to certain types of cryptocurrencies. These six issues, which are dependent on the type of

cryptocurrency, include issue 1 (lack of regulations and regulatory bodies), issue 2 (lack of issuing authority), issue 3 (lack of association with any financial institution), issue 4 (stability and price fluctuations), issue 11 (not backed by any asset), and issue 13 (lack of intrinsic value and not being a legal tender). It is noteworthy that issue 3 appears to be redundant with issue 2. Furthermore, issue 4, which concerns stability and price fluctuations, is subject to endogenous and exogenous factors. The exogenous factor, mainly speculative investment and speculation, itself constitutes an issue raised by the existing literature (issue 7).

Since cryptocurrencies form part of one's wealth, discussion of the implications of the system is critical and thus inevitable from a worldly perspective in general and from the *Sharī'ah* perspective in particular. If the whole system cannot be held in coherence or the integrity cannot be guaranteed, then rights cannot be preserved either. Therefore, it is of utmost importance that issues are kept to the minimum and the system's reaction to conflicts in the transactions is such that the whole network remains stable. However, upon conducting the above analysis on the issues derived from extant literature, it is apparent that these issues touched upon only a part of the cryptocurrency system, namely the trading platform and wallet management. Notwithstanding, it is evident that these issues are not exhaustive, and a thorough investigation is essential to assess their full impact. The detailed study of the main types of cryptocurrencies in the previous sections also reveals that indeed there are additional issues beyond what has been outlined. Besides the issues pertaining to the trading platform and wallet management, there are other issues as well which concern the monetary policy, the mining process, the network's node routing, and the protocol development (rule changes).

In particular, every cryptocurrency has a monetary policy that specifies its maximum supply, frequency of mining, number of tokens released in each mining activity, and unit divisibility. For instance, the Bitcoin network has a maximum supply of 21 million tokens that are gradually discovered, with each bitcoin token divisible into 100 million satoshis. Mining frequency is designed to be approximately every 10 minutes, with block rewards halved every 210,000 blocks or every four years (*Bitcoin (BTC): A Peer-to-Peer Electronic Cash System*, 2020; Hayes, 2022). Initially, the first block released 50 tokens of reward to miners. As of May 12th 2020, the block mining rewards

were at 6.25 bitcoin tokens (BTC) per block (*Bitcoin (BTC): A Peer-to-Peer Electronic Cash System*, 2020).

Table 4.3: Extant Literature Issues Thematized

Issues – Extant Literature	Remarks
1. Lack of regulations and regulatory bodies	▪ **Theme**: Regulatory concerns ▪ Crypto type-dependent
2. Lack of issuing authority (usually the state)	▪ **Theme**: Regulatory concerns ▪ *Sharī'ah* requirement (with conditions) ▪ Crypto type-dependent ▪ Not an issue if authority is indifferent
3. Lack of association with any financial institution	▪ **Theme**: Regulatory concerns ▪ Crypto type-dependent ▪ Redundant with the above
4. Stability and price fluctuations	▪ **Theme**: Financial considerations ▪ Crypto type-dependent ▪ Affected by endogenous factors: market forces (supply/demand), monetary policy ▪ Affected by exogenous factor: speculation
7. Speculative investments	▪ **Theme**: Financial considerations ▪ It is itself an exogenous factor ▪ Provisioned by trading platforms
9. Inheritance Issues	▪ **Theme**: Financial considerations ▪ Wallet management-related
10. Loss of Password	▪ **Theme**: Security concerns ▪ Wallet management-related
11. Not backed by any asset	▪ **Theme**: Value concerns ▪ Crypto type-dependent ▪ Fiat currency is not backed by any asset, yet has value
13. Lacking intrinsic value and are not legal tenders	▪ **Theme**: Value concerns ▪ Crypto type-dependent ▪ Value is derived from the network and market forces
15. Adding imaginary blocks to the blockchain (Malicious Attack)	▪ **Theme**: Security concerns ▪ Security risk caused by technology ▪ Consensus mechanism-related

Source: Author

As of January 2022, approximately 18.9 million BTC have been mined, with about 2.1 million tokens yet to be released (Hayes, 2022). This information is critical for assessing the long-term viability and sustainability of the cryptocurrency system. Some issues may arise from the monetary policy. For example, transaction recording and confirmation time, block time, can have certain important consequences. Shorter times can add transactions to the blockchain faster thereby achieving *Sharī'ah* constructive payment receipt (al-Qabḍ al-ḥukmī) faster. However, a cryptocurrency featuring a shorter block time requires a higher number of blocks to attain a security level equivalent to that of a slower blockchain upon the creation of a new block (*What Is Block Time?*, 2022).

Due to its limitation and in order to scale, developers of slow block time cryptocurrencies such as Bitcoin allow platforms to offload transaction recording from the blockchain to be added later. Yet, such solutions, called layer 2 solutions, have been shown to be disastrous when exchanges crashed and announced bankruptcy. For instance, the recent collapse of the leading cryptocurrency exchange platform, Futures Exchange (FTX) has left an estimated 9 million customers and other investors facing total losses in the billions of dollars (Illien et al., 2023).

Another issue related to trading platforms is the risk of committing *Ribā*. For example, some platforms offer their clients loans in the name of free rewards with the purpose of receiving commission returns from their clients' profits. Others would loan on a short sell and get the returns when their clients gain profits after they sell their currencies. Such applications are clear *Ribā* practices.

One of the significant risks associated with cryptocurrencies is their vulnerability if a malicious party can control 51 percent or more of the network's processing power. This party can effectively then collude and destroy the system in what is known as Goldfinger attack. Yet, the stability is unknown if miners collude to control 51 percent of the network or more. Practically, in July 2014, GHash.IO, a Bitcoin mining pool, momentarily surpassed 50 percent of the network's computational capacity, prompting a public commitment to restrict their capacity in subsequent instances to prevent undermining confidence in the system (Bonneau et al., 2015). Nonetheless, the Bitcoin network has experienced no evidence of a malicious mining attack (Bonneau et al., 2015). This issue has already been noted in the literature, specifically issue 15 in Table 4.4, although the description here is more accurate.

Another issue relates to the importance of the randomization nature of the puzzle, without which the most powerful individual miner could be expected to generate all the blocks. With randomization, each miner will have a probability of finding the next block equivalent to his share of competing computational power (Bonneau et al., 2015). However, although each node is supposed to have roughly the same weight of mining power, random connections, and look fairly uniform, there is a huge difference in mining power node to node as mining pools and farms started to form. In other words, some nodes are more influential than others where we have uneven distribution of hash power.

Another issue that might arise with respect to the cap on the monetary supply is the consequences post discovering the last token. For instance, as most of the bitcoins have been mined so far, the 'new bitcoin' incentive part will eventually phase out. The last BTC is expected to be generated in 2140 (Hayes, 2022). The repercussion of this is that miners will no longer be able to receive 'new' BTC incentives and therefore they become only bookkeepers who write to the ledger (blockchain) with the only possible income to be the transaction fee. The only drawback is the possibility that mining income becomes insufficient, and some miners might have the selfish desire to control the whole network. For example, Goldfinger attack has been observed on CoiledCoin, an altcoin destroyed by a significant attack from a Bitcoin mining pool named Eligius (Bonneau et al., 2015).

Arguably these attacks have been observed through altcoin infanticide and as explained before, there has been no evidence for a selfish network attack. Moreover, this issue becomes likely improbable as the network grows and as the blockchain grows several hundred blocks in depth. According to Antonopoulos (2014), the first six blocks in the blockchain are likened to a thin layer of topsoil, however, as one delves deeper beyond six blocks, the likelihood of changes in blocks diminishes, and after reaching 100 blocks, a significant level of stability is established. The latter also minimizes the racing attack which causes double spend.

On the other hand, to maintain creating a block within the block time limit, PoW-based cryptocurrencies have the difficulty of the puzzle adjusted every certain period of time. The difficulty level in Bitcoin is modified approximately every fortnight, determined by a function involving the timestamps from the prior 2016 blocks (*Bitcoin (BTC): A Peer-to-Peer Electronic Cash System*, 2020; Bonneau et al., 2015). As the

difficulty of the puzzle and thus PoW have increased exponentially, normal personal computers are no more able to compete. As a consequence, the system's behavior tended towards producing mining pools that are capable of handling the processing power required to solve such difficult problems. A few giants with enormously powerful central processing units (CPU) thus emerged to form mining pools and steer the lead of mining. Some mining pools are thought to represent over 30 percent of the total mining capacity (Kroll et al., 2013). The system hence moved towards a governance structure that can immediately affect the network. In their 2013 article, Kroll et al. (2013) predicted these governance structures albeit more about to be in the hands of leading developers. An issue that may arise with respect to this consensus mechanism is that this might lead to the emergence of mining cartels that are capable of censoring certain transactions (Kroll et al., 2013).

From the lens of protocol development, the need for changing some rules means some form of governance is essentially required (Bonneau et al., 2015). The absence of a clear process for changes in transaction validation rules, for example, can cause issues such as permanently forking the system (producing two blockchains) due to lack of unanimity. This should not be mistaken with the security of transactions. Cryptocurrencies are known to use strong hashing algorithms which gives high confidence about the integrity of these transactions.

As for the wallet management, an issue that has not been tapped is the use of Type-0 non-deterministic wallets. These wallets are cumbersome to manage as they require frequent backups for each key which makes them prone to irrevocably loss of funds (Antonopoulos, 2014).

Moreover, any user error mistakes can result in permanent loss of cryptocurrency tokens, not only from the user's wallet, but also, from the cryptocurrency economy overall, for instance losing the private key due to hard drive crashes or insufficient backups. This implies that users of cryptocurrencies have to be fully aware of the different types of wallets and which are more secure and less prone to loss of funds.

Cryptocurrencies that offer distributed computation face a great challenge. Since their underlying scripting technology is Turing-complete, this implies that they have full-fledged coding statements including loops. Such capabilities make weak points from which malicious entities can hack the system and cause damages. Securing smart

contracts is therefore a challenge. On the other hand, cryptocurrencies of the NFT type demonstrate no added value. The illusion of rarity is more likened to squander. Unless otherwise finding an application of value, NFTs from *Sharī'ah* perspective can hardly be accepted. As for stablecoins, while they seem the most viable for a *Sharī'ah*-based cryptocurrency, it has to be noted that many stablecoin projects have failed in maintaining their peg which led to having its value debauched. Therefore, stablecoins aren't guaranteed to maintain their peg. Moreover, one of the risks users of stablecoins should bear is the lack of transparency. Not all issuers of stablecoins release full public audits. Also, issuers of stablecoins centrally hold the collateral giving them significant control over the coin. Users of these coins will have to trust that these central entities have the reserves they claim.

Table 4.4 provides a modified version of Table 4.3 by listing an improved form of its issues and adding the issues identified in the previous discussion. The table also elaborates on the possible violations to *Sharī'ah*. Where a potential for addressing *Sharī'ah*-compliance is found, the nature of that compliance is explained. Also, each issue is classified using the themes discovered and what component of the cryptocurrency system it is related to.

Several points in Table 4.4 owe further delineation. The issue that has been identified as *Gharar* without further explanation or specification by the literature, now itself appears in the table as a potential violation to *Sharī'ah* committed by several specific issues. Additionally, the 'm of n multi-sig' property has been identified as a potential temporary solution to the case of inheritance and the threat of loss of wealth on death. The property means that no funds can be transferred or acted upon without the signature of 'm' number of people out of 'n' number of people. That is, if '2 of 3 multi-sig' is specified, any 2 of the 3 people authorized have to sign in order to transfer funds.

Table 4.4: Issue Register 1: Issues and *Sharī'ah*-Compliance Classifications

Issue	*Sharī'ah* Violations	Potential for *Sharī'ah* Compliance	Remarks
1. Lack of regulations and regulatory bodies	*Gharar*, Imbalance, Risk of deception		▪ **Theme**: Regulatory Concern ▪ Trading Platforms and Wallet Management providers are regulated in their own countries ▪ Crypto-dependent

2. The extent to which authorities are concerned or non-supporting	Infringement upon the Sultan's right to issue money		▪ **Theme**: Regulatory Concern ▪ This can be flexible: - Non-state issuance is reprehensible - State is indifferent - State allows/uses it ▪ Crypto-dependent
3. Lack of association with any financial institution	*Gharar*		▪ **Theme**: Regulatory Concern ▪ Crypto-dependent ▪ Redundant with the previous issue
4. Stability and price fluctuations	Erosion of property and wealth, Violation of 'store of value'		▪ **Theme**: Financial consideration ▪ Crypto type-dependent ▪ Affected by endogenous factors: market forces (supply/demand), monetary policy ▪ Affected by exogenous factor: speculation
5. Speculative investments	*Gharar, Ribā*		▪ **Theme**: Financial consideration ▪ It is itself an exogenous factor ▪ Provisioned by trading platforms
6. Inheritance Issues	Wealth is lost on death		▪ **Theme**: Financial consideration ▪ Wallet management-related
7. Loss of Password	Loss of property and wealth		▪ **Theme**: Financial consideration ▪ Wallet management-related
8. Not backed by any asset	*Gharar*		▪ **Theme**: Value concern ▪ Crypto type-dependent ▪ Fiat currency is not backed by any asset, yet has value
9. Lacking intrinsic value and are not legal tenders	*Gharar*		▪ **Theme**: Value concern ▪ Crypto type-dependent ▪ Value is derived from the network and market forces
10. Possibility of miner controlling more than 50% of the network / Altcoin is at the infanticide stage	*Gharar*		▪ **Theme**: Security concern ▪ Security risk caused by technology ▪ Network routing-related ▪ On growth of the blockchain several blocks deep, it becomes **improbable**
11. Short block times need more blocks to reach the desired level of security	*Gharar*		▪ **Theme**: Security concern ▪ Monetary policy-related ▪ The issue is not that it is insecure, it is only that it requires more blocks to reach the desired level of security.
12. Offload recording	*Gharar*	Dispute resolution	▪ **Theme**: Financial consideration ▪ Trading Platform-related

transactions from the blockchain	Constructive payment receipt might be questionable		▪ The *Gharar* is in case the trading platform collapses ▪ Potential solution for dispute resolution used within wallets
13. Trading platform rewards in exchange for nominal percentage of the returns	*Ribā*		▪ **Theme**: Financial consideration ▪ Trading platform-related
14. Lack of proper randomization of the puzzle	Imbalance between mining participants		▪ **Theme**: Operational Efficiency of Mining ▪ Mining-related
15. Mining pools and farms make the influence in the hands of few	*Gharar*		▪ **Theme**: Security concern ▪ Mining-related ▪ Could lead to issue **10**
16. Consequences of insufficient mining income	*Gharar*		▪ **Theme**: Security concern, Mining Operational Efficiency ▪ Monetary-policy ▪ Could lead to issue **10** or **18** ▪ This is a future anticipation that needs to be researched related to end of tokens supply
17. Racing attack causing double-spending	*Gharar*, Loss of property and wealth		▪ **Theme**: Security concern ▪ Network routing-related ▪ With a few blocks confirmation technique this becomes improbable
18. Emergence of mining cartels capable of censoring transactions	Preservation of property is violated		▪ **Theme**: Operational Efficiency of Mining ▪ Mining-related
19. Lack of a clear process for changing transaction validation rules	*Gharar* Loss of property and wealth		▪ **Theme**: Security concern, Value concern ▪ Protocol development-related ▪ May lead to forks which might lead to loss of tokens ▪ Low probability for well-established and well-maintained blockchains
20. Wallet is a Type-0 non-deterministic one	Loss of property and wealth		▪ **Theme**: Financial consideration ▪ Wallet management-related ▪ More secure types of wallets exist
21. Multi-sig enablement for inheritance		m of n multi-sig property can be used	▪ **Theme**: Financial consideration ▪ Wallet management-related

		for heirs' wealth	
22. Security of smart contracts	*Gharar*		▪ **Theme**: Security concern ▪ Crypto type-dependent
23. Application of NFT is not of value	Squander		▪ **Theme**: Value concern ▪ Crypto type-dependent
24. Inability of a stablecoin to maintain its peg	Erosion of property and wealth, Violation of 'store of value'		▪ **Theme**: Financial consideration ▪ Monetary policy-related
25. The extent a stablecoin issuer releases full public audits	*Gharar*		▪ **Theme**: Financial consideration
26. The extent to which an issuer of a stablecoin can be trusted to have the reserves they claim	*Gharar*		▪ **Theme**: Value concern

Source: Author

In order to be more practical and have the owner practice his full right of utilizing his wealth as he wishes, the property should be set at '1 of n multi-sig'. This means only his signature out of 'n' authorized signatures is required. In case of his death, any of the remaining 'n' people can access the funds and distribute it according to *Sharī'ah* laws of inheritance. This solution is temporary because it raises a security issue whereby any of the other 'n' authorized signatories will also have the right of utilizing the funds even while the owner is alive. Therefore, when setting this property, trustworthy people should be elected to represent the other signatories while at the same time look for a new development of a wallet that will have a feature for transferring funds to heirs in case of the owner's death without breaching the security of his funds during his life. Another potential solution identified is developing a wallet that can offload transactions from the blockchain. This can further be discussed with technology experts. Lastly, a new theme emerged, 'operational efficiency of mining', next to the four that were already identified in the previous table.

To guide the decision of the extent of risk each issue is exerting, the author suggests borrowing the concept of a risk matrix from the field of risk management. The risk matrix can be adaptable by jurists according to their opinions and sects (madhab). This will help demonstrate the extent of *Gharar* for example in a certain issue and whether the conditions for a prohibited *Gharar* are realized.

Table 4.5 demonstrates a risk severity matrix where any risk is considered a combination of its impact and the likelihood for its occurrence. In this example, the author chose five levels for each of the impact (negligible, minor, marginal, significant, and critical) and the probability (highly improbable, improbable, possible, probable, and certain).

Table 4.5: Risk Severity Matrix

		Impact				
		Negligible (1)	**Minor (2)**	**Marginal (3)**	**Significant (4)**	**Critical (5)**
Probability	**Certain (5)**	Low	Medium	High	Very High	Very High
	Probable (4)	Low	Medium	High	High	Very High
	Possible (3)	Low	Medium	Medium	High	High
	Improbable (2)	Low	Low	Medium	Medium	Medium
	Highly Improbable (1)	Low	Low	Low	Low	Low

Source: Author

The numbers appended to each of these levels represent the weight. The following equation determines the severity of the risk:

$$\textit{Severity of the risk} = \textit{Weight of its impact} \times \textit{Weight of its probability} \qquad (1)$$

For example, a risk that has a significant impact but that is highly improbable will have a severity of $4 \times 1 = 4$. The severity can be described with 3 or more levels; the table above has four levels (low, medium, high, and very high). The severity range for each level is depicted in Table 4.6. The severity range is again the choice of the author and is not an exact science, but one that guides to give a clue for analyzing the issues. Therefore, it can be adjusted according to needs.

Finally, the issues can be reorganized using a 7x5 matrix to display which theme and system component each issue belongs to. This approach offers the advantage of

presenting all issues within a particular theme and system component. Please refer to Table 4.7, issue register 2, for an illustration of this matrix.

Table 4.6: Risk Levels and Their Corresponding Severity Ranges

Level	Severity Range
Low	Level < 6
Medium	$6 \leq$ level < 12
High	$12 \leq$ level < 18
Very High	Level ≥ 18

Source: Author

Additionally, after analyzing the risk severity of each issue associated with a particular cryptocurrency using the above risk severity matrix, a color code can be added to the cell of the relevant issue in issue register 2 table. This approach enhances readability and facilitates referencing.

Table 4.7: Issue Register 2

	Regulatory Concern	**Financial Concern**	**Security Concern**	**Value Concern**	**Mining Operational Efficiency**
Mining Process			**15.** Mining pools and farms make the influence in few hands		**14.** Lack of proper puzzle randomization
					18. Rise of cartels that can censor transactions
Monetary Policy		**24.** Inability of a stablecoin to maintain its peg	**11.** Short block times need more blocks for the desired security level	**8.** Not backed by any asset	**16.** Consequences of insufficient mining income
			16. Consequence of insufficient	**9.** Lack intrinsic value - not	

			mining return	legal tenders	
Node Routing			**10.** Possibility of miner controlling > 50% of the network /infanticide stage		
			17. Racing attack causing double-spending		
Overall Crypto System	**1.** Lack of regulations and regulatory bodies	**4.** Stability and price fluctuation	**22.** Security of smart contracts	**23.** NFT Application is not of value	
	2. The extent to which authorities are non-supporting	**25.** The extent an issuer of a stablecoin releases full public audits		**26**. The extent to which an issuer of a stablecoin can be trusted to have the reserves they claim	
	3. Lacks association with any financial institution				
Protocol Development			**19.** Lack of a clear process for changing transaction validation rules	**19.** Lack of a clear process of changing transaction validation rules	
Trading Platform		**5.** Speculative investment			

		12. Offload transaction from the blockchain			
		13. Trading platform reward in exchange for a % of returns			
Wallet Management		**6.** Inheritance Issues			
		7. Loss of Password			
		20. A Type-0 non-deterministic wallet			
		21. multi-sig as a solution for inheritance			

Source: Author

4.6. The Framework: Putting it All Together

The preceding section established two issue registers and a framework to assess their risks using a risk severity matrix. The evaluation was conducted with regard to the cryptocurrency system component involved and the theme of the issue. Moreover, the study examined the type of cryptocurrency and its developmental stage. Figure 4.6 provides a summary of these findings and lays out a topology for the risk analysis process. As can be seen from the figure, tokens play a very minor role as rewards, and in fact they are just a byproduct of the overall cryptocurrency system's operation.

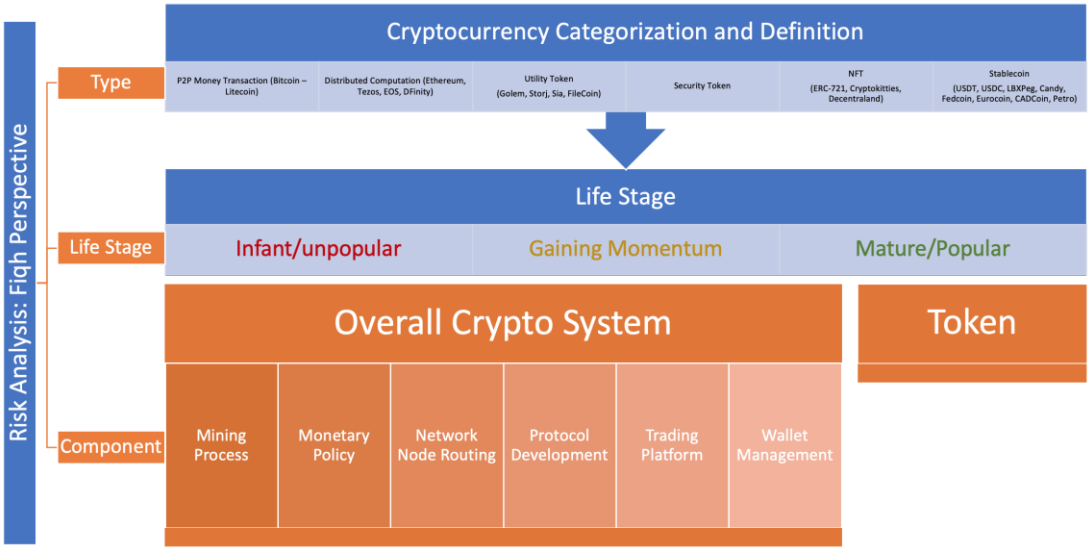

Figure 4.6: Topology for the Risk Analysis Process

Source: Author

The analysis of issue registers has revealed a critical risk related to the control of certain miners, who take over 50 percent of the network. Such control grants them the ability to launch attacks that can harm the system. However, the likelihood of such an event decreases as the cryptocurrency matures. Therefore, before analyzing the overall issues, it is crucial to determine whether the system has reached a mature developmental stage. If it has not, there is no point in continuing with the analysis. The topology in the figure clearly illustrates this point, indicating that the determination of the cryptocurrency type must be followed by an understanding of its developmental life stage. The discussion leads to the final framework which is depicted in Figure 4.7.

In a thorough analysis of a cryptocurrency, and as demonstrated by Figure 4.7, two distinct parts are encountered. The first involves an examination of every endogenous factor of the virtual system, including the mining process, monetary policy, network node routing, overall crypto system, and protocol development. While the latter may not be entirely endogenous to the crypto system, it provides a good indication of the health of its development.

The second part of the analysis pertains to the exogenous components. The analysis of these components does not affect the crypto system itself, and any *Sharī'ah* consequences apply only to them and not to the system. These exogenous components include wallet management and trading platforms.

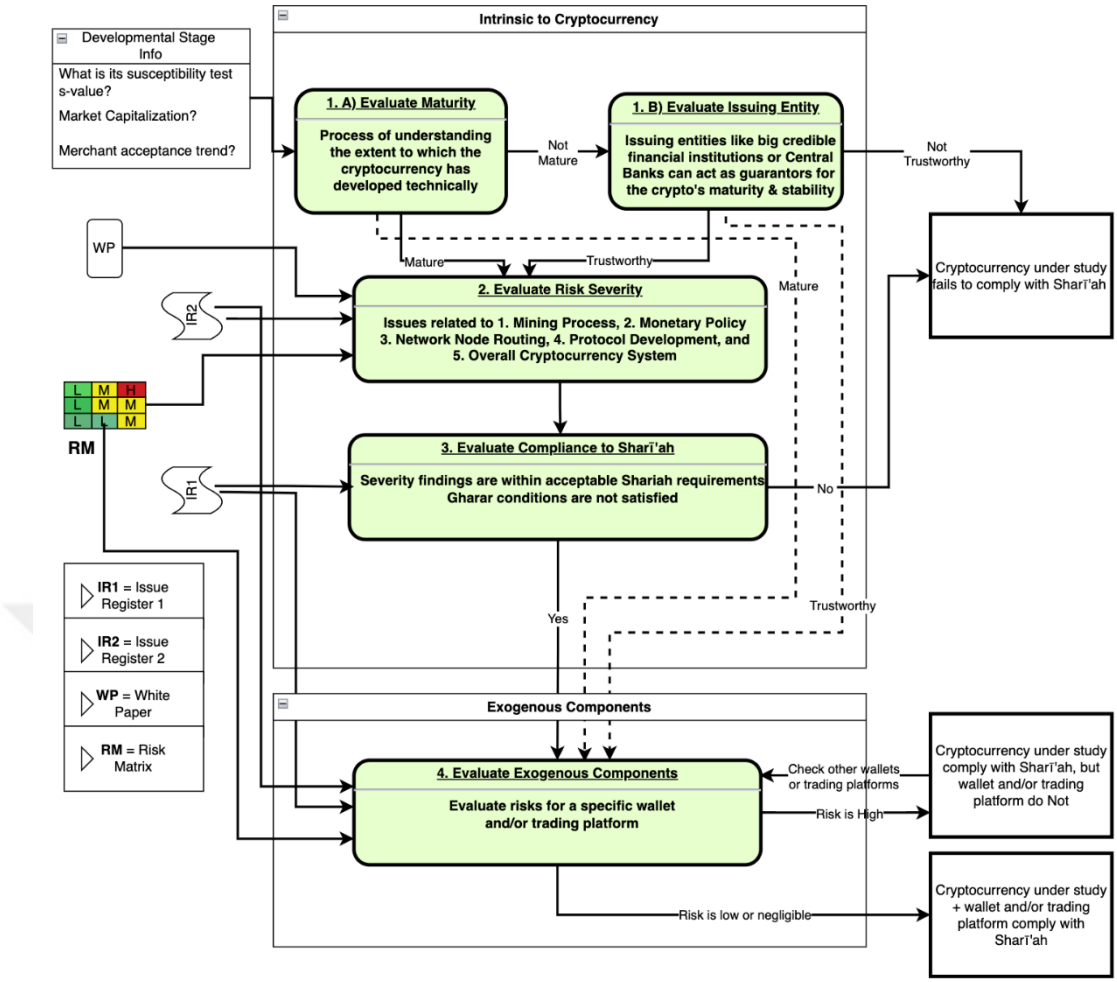

Figure 4.7: *Fiqh* Framework for Analyzing the Issues of Cryptocurrencies

Source: Author

In the next subsections, the framework in **Hata! Başvuru kaynağı bulunamadı.** is detailed and benchmarks are provided for each section in order to guide the *Fiqh* ruling/decision about the cryptocurrency under study.

4.6.1. Evaluate Maturity and Issuing Entity (Process 1)

This involves two subprocesses: Evaluate Maturity (Process 1.A) and Evaluate Issuing Entity (Process 1.B).

4.6.1.1. Evaluate Maturity (Process 1.A)

To evaluate the maturity of the cryptocurrency, a criteria will be required. That criteria must address the requirements of the first layer of the topology in Figure 4.6. In other words, the criteria should differ with the type of cryptocurrency. Nonetheless, there are certain criteria which will be common among all. In this section, first the common criteria will be discussed which involves market capitalization and the trend of

merchant acceptance. Then that will be followed by discussing the criteria pertaining to each category of the cryptocurrencies.

In his book, Antonopoulos (2014) discusses several questions, shown in Table 4.8, to be asked that helps to evaluate cryptocurrencies, the altcoins in particular, from the market perspective. Except for the first question, these questions are common to all categories and, thus, can be asked to evaluate any cryptocurrency. However, Antonopoulos does not show what measures for each question would make a mature cryptocurrency. For example, it is not clear how many merchants and wallets would make a strong cryptocurrency. It becomes clear that certain benchmarks are required.

Table 4.8: Questions to Evaluate Altcoins

Questions
Can the altcoin attract enough miners to be secured against consensus attacks?
What is the total market capitalization of the altcoin?
How many merchants accept payment using the altcoin?
What is the volume of transactions executed on the altcoin?
What is the volume and value of daily transactions?
How many estimated wallets does the altcoin have?
Are there highly secured wallets?

Source: Antonopoulos, 2014

Notably, one of the questions asked is related to the market capitalization (or shortly market cap) of the cryptocurrency. This criterion is heavily discussed in the crypto market as a measure of crypto performance. Market capitalization is a crucial metric used by market analysts to evaluate the performance of both stocks and cryptocurrencies, and to guide investors' decision-making. While the market cap for stocks is the total value of a company's outstanding shares, for cryptocurrencies, it is the product of the number of coins mined and the market price per coin (*What Is Market Cap?*, 2020).

Studies have supported the use of traditional market measures for cryptocurrencies as well. For instance, in a recent study by Leirvik (2022), the relationship between market liquidity volatility and the returns of the top five cryptocurrencies by market capitalization was analyzed. The study found that when liquidity is low, expected

returns are high, which is consistent with findings from other financial markets. Therefore, market cap can be considered "A rough gauge of an asset's stability" (*What Is Market Cap?*, 2020).

While there is no formal categorization, market caps over $50 billion (or shortly $50b) are typically referred to as mega-caps, those over $10b as large (big) caps, and $1b ($2b for stock markets) to $10b as mid-caps, while under $1b ($2b for stocks) are small-caps (The Investopedia Team, 2022; *What's Crypto Market Cap? Why Does It Matter?*, 2022). Mega and large market caps are usually associated with low risk and stability, while medium caps are linked to high risk, and small caps are considered the most risky (*What's Crypto Market Cap? Why Does It Matter?*, 2022).

Despite the volatility associated with cryptocurrencies, large-cap cryptocurrencies have a demonstrated track record of growth and higher liquidity, making them more resilient to market volatility and high volumes of cashing, while small-cap cryptocurrencies are susceptible to dramatic swings based on market sentiment (*What Is Market Cap?*, 2020). The risk diffusion in the cryptocurrency market, as indicated by Yang, Wu, & Wu's (2022) study, is influenced by cryptocurrencies with large market capitalization and those experiencing price declines or low turnover.

With respect to number of merchants accepting cryptocurrencies as payment, in a survey conducted by Zogby Analytics in 2020, it has been found that 36 percent of the small and mid-sized businesses accepted cryptocurrency as payment for goods and services (*HSB Survey Finds One-Third of Small Businesses Accept Cryptocurrency*, 2020). Furthermore, according to a survey conducted by Deloitte, 75 percent of retailers are intending to incorporate either cryptocurrency or stablecoin payments into their accepted modes within the upcoming two years (DeVon, 2022). The survey's sample was senior executives of retail organizations across the US (Deloitte, 2022).

Although similar statistical studies are required in other parts of the world to see the extent of adoption, there is a common belief that there is an uprise trend in accepting cryptocurrencies as payments. Yet, a number threshold to determine whether a crypto has a general public acceptance is not clear, but the author believes that a look to see an uprise trend in accepting a crypto as a payment should suffice to tell whether the crypto is going to have a general public acceptance.

Next we discuss the maturity from some criteria that is specific to each category of cryptocurrency. These categories were discussed in the previous section and are enumerated in Figure 4.6. This includes P2P Money Transaction (cryptos that are usually mined and operate using PoW algorithms), Distributed Computation (which are mostly common to use PoS algorithms and have smart contracts), Utility Tokens, Security Tokens, NFTs, and Stablecoins. Two important points are worth mentioning at this point.

First, the consensus mechanisms and algorithms, like PoW and PoS, used for the operation of issuing cryptos do not directly relate to either the P2P money transaction or distributed computation crypto types. Many P2P money transaction cryptos operate using PoW, like BTC, LTC, DOGE, and Namecoin (NMC), while others might operate using PoS, like BLK. Similarly, a few of the distributed computation cryptos operate using PoW, like Ethereum prior to September 2022 and R3's Corda[16], while many operate using PoS, like ETH, Polkadot, Cardano[17], Tezos, and TRON. Since the maturity is based on the mechanism on which the crypto operates, and since PoW and PoS combined dominate about 78 percent of the crypto market (*CryptoSlate*, 2023), it would be wise to consider criteria based on these two mechanisms. This is in addition to developing a criteria for the maturity of smart contracts within a distributed computation crypto network.

Second, NFT, utility tokens, and security tokens are cryptocurrencies built on other decentralized blockchains characterized by hosting smart contracts and other codes. In other words, they are hosted on distributed computation networks. As such, studying the maturity of the underlying distributed computation network suffices for understanding the maturity of those hosted cryptocurrencies.

---

[16] Corda: a tokenization platform powering regulated digital finance (*Open, Permissioned Distributed Platform: Capitalize on the New Digital Economy—Transact Openly and Securely, at Scale and Across Networks*, n.d.).

[17] Cardano: a decentralized development platform with verifiable smart contracts (Conway, 2023).

The way PoW work, in principle, makes them vulnerable to various attacks. Such attacks threaten to reorganize the blocks and cause double-spends and in certain cases might demolish the whole system. This fact conflicts with the *Sharī'ah* principle that private property and wealth should be preserved. However, not all such cryptos have the same vulnerability as they are seen to be exposed to various degrees of susceptibilities while some are even resilient.

In his study, Bakr (2023) developed a mathematical formula supported by statistical rigor to model the susceptibility of a PoW cryptocurrency. He devised that cryptos with a susceptibility test value less than 0.532 are resilient. On the other hand, cryptos with susceptibility test values falling between 0.532 inclusive and 0.826 are those that experience moderate resilience. Anything beyond that would be considered vulnerable and thus immature enough to be considered for further scrutiny.

PoS cryptocurrencies are also prone to attacks, but the risks encountered are less severe than that faced in PoW cryptos. In their study, Nguyen et al. (2019) suggested to maintain the ratio of block rewards to the total stakes in the network in order to preserve the decentralization of the PoS system. However, they are silent on what that ratio should be.

Yet, we suggest a simple criterion to avoid collusion on the system. The criterion is that the network should not have a single stake owning 50 percent or more of the total stakes. In other words, the farther the largest stake in the network is below 50 percent the less the PoS will be prone to collusion and other attacks.

On the other hand, in distributed computation cryptos, smart contracts need to be secure. Otherwise, the smart contract will be prone to major *Gharar*. If a jurist is also evaluating a specific smart contract then we suggest that it observes the following four controls.

First, it should possess access control and role-based controls. This is necessary so that each role within the contract should not get access more than it requires for its role. Second, the smart contract should implement internal safeguards against problematic interactions. This can be verified by confirming that the code contains 'require()', 'assert()', and 'revert()' statements.

Third, the smart contract should undergo formal verification. There are many tools and websites that can carry out the verification of the correctness of the code and discover any vulnerabilities. This includes Certora Prover[18], Solidity[19] SMTChecker[20], and Mythril[21]. Fourth, the jurist needs to request that the smart contract is subjected to an external auditor for further reviews. A few examples of these auditors include Consensys Diligence[22], Certik[23], OpenZeppelin[24], and Quantstamp[25].

There are many other guidelines and recommendations for developers when coding smart contracts as can be seen in (Busch, 2023). Nonetheless, from a jurist's perspective ensuring the aforementioned controls should suffice as a criteria for accepting the smart contract from a *Sharī'ah* point of view. The jurist can also be more flexible by just requesting the last two controls to be presented or even only request that the smart contract be certified by an external auditor.

In contrast, for stablecoins to be accepted for further scrutiny within the framework, it has to have a good deal of transparency in order to avoid *Jahālah*. In other words, the stablecoin need to have full public audits.

Stablecoins should, also, have a track-record of maintaining their peg against the asset they represent. Lastly, the central entities behind the stablecoin should be trusted to have the reserves they claim. All the aforementioned benchmarks are summarized in Table 4.9.

---

[18] Certora's website: https://www.certora.com/

[19] Solidity: an object-oriented programming language for implementing smart contracts

[20] SMTChecker: a tool that performs formal verification for the code of smart contracts (Owleksiy, 2021)

[21] Mythril: a security analysis tool for detecting vulnerabilities in smart contracts (*About | Consensys/Mythril*, n.d.)

[22] Consensys Diligence's website: https://consensys.net/diligence/

[23] Certik's website: https://www.certik.com/

[24] OpenZeppelin's website: https://www.openzeppelin.com/security-audits

[25] Quantstamp's website: https://quantstamp.com/

Table 4.9: Benchmarks for Cryptocurrency Maturity

		Mature	**Further Scrutiny**	**Rejected**
PoW	Market Cap	≥ $10 b	≥ $1 b and < $10 b	< $1 b
	S-value *	< 0.532	≥ 0.532 and < 0.826	≥ 0.826
	Merchant Acceptance Trend	Increasing	Increase is not obvious	Acceptance not established
PoS	Market Cap	≥ $10 b	≥ $1 b and < $10 b	< $1 b
	Largest Stake	≪ 50 %	≈< 50 %	≥ 50 %
	Merchant Acceptance Trend	Increasing	Increase is not obvious	Acceptance not established
Smart Contracts	PoS Criteria Satisfied	Yes	See PoS	None is Satisfied
	Access Controls	Recommended	Satisfied	
	Require(), assert(), revert()	Recommended	Satisfied	
	Formal Verification	Recommended	Maybe	
	External Audit	Must	Not Satisfied	
Stablecoin	Market Cap	≥ $10 b	≥ $1 b and < $10 b	< $1 b
	Full Public Audits	Satisfied	Partial	No
	Track-record of peg stability	Yes	No	No
	Reserves are established	Yes	Not clear	No
	Merchant Acceptance Trend	Increasing	Increase is not obvious	Acceptance not established

* S-value = Susceptibility test value

Source: Author

4.6.1.2. Evaluate Issuing Entity (Process 1.B)

In case the evaluation of the cryptocurrency's maturity resulted in the need for further scrutiny, depicted in the column 'Further Scrutiny' of Table 4.9, then the jurist needs

to evaluate the entity issuing that cryptocurrency. A critical *Sharī'ah* aspect that needs to be observed is the preservation of private ownership and wealth. This means that the characteristics of the entity behind the crypto should be such that it avoids negligence and fraudulence. Moreover, transparency is critical to avoid any form of *Jahālah*. Therefore, that entity should be either a central bank, or a governmental body, or a big credible financial institution known for its trustworthiness. Otherwise, the entity should be a truthful, trustworthy, and experienced body with proven-track record of due diligence and transparency.

4.6.2. Evaluate Risk Severity

At this stage of evaluation, most of the risks have already been mitigated due to the acceptance of mature cryptocurrencies, or at the very least, those backed by credible and trustworthy entities. Nevertheless, it might be essential to examine specific issues outlined in issue register 2 i.e., Table 4.7, and any additional concerns derived from the crypto's white paper. It should be noted that some issues mentioned in issue register 2 pertain exclusively to certain categories of cryptocurrencies and do not apply universally. Consequently, if an issue does not apply to a particular crypto, its severity rating will be grayed out in the final risk assessment output. Moreover, within issue register 2, only issues related to the 'Mining Process', 'Monetary Policy', 'Node Routing', 'Overall Crypto System', and 'Protocol Development' components of the crypto system will be considered. Issues related to 'Trading Platform' and 'Wallet Management' are exogeneous to the crypto system and therefore will be evaluated in subsection 4.6.4.

To determine the severity of each issue, the jurist must employ equation 1. For instance, Issue '**1.** Lack of regulations and regulatory bodies' pertains to the overall crypto system. This encompasses not only regulations concerning the crypto itself but also regulations governing exchange platforms and wallet providers. The extent of regulations varies depending on the specific crypto. For example, while Bitcoin lacks a direct regulatory body due to its decentralized nature, Ethereum operates under the governance of its known issuer and the country where it operates. Nonetheless, the platforms and wallets supporting Bitcoin are subject to regulations in their respective countries. Also, Bitcoin is governed by the developers of its protocol which gives it an extent of regulations. Consequently, the risk level for Bitcoin is categorized as possible with a minor impact. Table 4.10 can help in determining the risk level as it provides

the interpretation of each level of impact and probability. Using Table 4.5, a possible probability has a value of 3, and a minor impact has a value of 2. Applying equation 1, the risk severity is calculated as $2 \times 3 = 6$. Referring to Table 4.6, this results in a medium-risk level, which can be denoted by a yellow color code. Similarly, for Ethereum, the probability of the risk is considered improbable (a value of 2), and the impact is minor (a value of 2). This yields a risk severity of 4, which is classified as low, which can be denoted by a green color code. This process is repeated for all issues within register 2 related to the specific crypto under study. We recommend approving cryptos with low and medium-level risks, while those with higher risk levels should probably be rejected, however after analyzing the *Sharī'ah* violations that will be conducted in subsection 4.6.3. Table C.2 in APPENDIX C shows a sample output of issue register 2 after evaluating Bitcoin with the severity color codes. Also, under each issue the weights of the impact and probability with the resultant severity are recorded.

Table 4.10: Risk Impact and Probability Level Interpretations

Impact		
Level	**Weight**	**Interpretation**
Negligible	1	No real effects.
Minor	2	Minor frustration exists with access & transactions.
Marginal	3	Minor loss of wealth and/or difficulty of transacting is causing inconvenience.
Significant	4	Considerable loss of wealth and/or barely able to transact.
Critical	5	Significant loss of wealth and/or significant loss of access and transacting.
Probability		
Level	**Weight**	**Interpretation**
Highly Improbable	1	Probability is significantly negligible, impossible, or highly unlikely.
Improbable	2	Very unlikely but may happen occasionally.
Possible	3	50-50 chance to happen. Can sometimes happen.
Probable	4	Very likely to happen. Happens frequently.
Certain	5	Highly likely to happen. Almost always happens.

Source: Author

It is crucial to recognize that a certain degree of subjectivity and flexibility exists within the evaluation process. Firstly, the jurist has the autonomy to adopt a distinct

risk matrix with varying numbers of risk levels, allowing for greater customization. Furthermore, the jurist can assign different value ranges to each level. However, the jurist should make diligent efforts to be as objective as possible when evaluating the probability and impact of risks. While objectivity should be pursued to the greatest extent possible, it is necessary to acknowledge that complete objectivity may not be attainable. Therefore, examining the remarks of issue register 1 in Table 4.4, and consulting with market and technical experts can provide valuable insights and contribute to a more comprehensive understanding of the risk landscape. Furthermore, we strongly advise the jurist to assess the weight of the impact associated with each issue independently before evaluating the probabilities. This will have the effect of mitigating the influence of bias. It is crucial, also, to consult Table 4.10 throughout this process to ensure objectivity and consistency.

Secondly, it is essential to be cautious regarding the probability levels assigned to certain issues. For instance, while Bitcoin is renowned for its lack of regulations and regulatory bodies in its crypto mechanism, formal regulations do exist to some extent in protocol development and exchange platforms. This might lead to misconceptions regarding the risk probability being 'certain.' However, in this context, 'certain' implies the complete absence of regulations at any level within the crypto system. Hence, the jurist must exercise care when assigning risk probabilities. Thirdly, the jurist has the flexibility to employ a strict approach, accepting only low severity risks, or can be more lenient, considering medium severity levels as well, or even a combination of both based on the specific issue at hand, but only after analyzing the *Sharī'ah* violations of these issues which will follow in the next subsection.

4.6.3. Evaluate Compliance to *Sharī'ah*

This stage of evaluation refers to issue register 1 where the risk levels achieved in the previous subsection highlight which *Sharī'ah* concept might be violated. Continuing with the same sample output of Table C.2 in APPENDIX C, we can now view the *Sharī'ah* compliance of Bitcoin in issue register 1, shown in Table C.1 in APPENDIX C.

Notice that the issues related to exogenous components, trading platform and wallet management, have been removed as these will be the subject of discussion in the next subsection. A green-colored issue demonstrates that the risk is minimum and, as such,

there is no fear of violating the *Sharī'ah* concepts listed to the right of it. For example, issue '**8.** Not backed by any asset' is green and thus demonstrates that for Bitcoin there is no element of *Gharar* caused by that issue as its system is well-established. A yellow-colored issue expresses a nominal degree of risk for violating *Sharī'ah* rules. This can be accepted since determining the impact and probability of the issue was the exercise of the previous subsection. Otherwise, further analysis can still be conducted. For example, in issue '**2.** The extent to which authorities are concerned or non-supporting', there is a nominal degree of risk of infringing upon the sultan's right to issue money. With further analysis and using the remarks in the same row of the issue, the violation might not be a problem if the state is indifferent about it, the state allows it, or even the state transacts with that crypto. Also, in issue '**4.** Stability and price fluctuations' there is a nominal degree of risk of loss of wealth and violating the concept of 'store of value'. However, in the previous subsection's exercise, for Bitcoin it was determined that the impact was marginal in this case which meant there might be a minor loss of wealth which is tolerable. This is because Bitcoin has a high market cap and is resilient against market fluctuations. Moreover, this is similar to fiat currency valuations affected by the market.

Notably, out of the 26 *Sharī'ah* violations, *Gharar* is mentioned the most with 13 occurrences forming 50 percent of all the issues. Therefore, it is imperative that we give special attention to it. Besides the aforementioned analysis, *Gharar* should not be viewed as an immediate reason for declaring impermissibility without fulfillment of the conditions it is confined to. According to fatwa 23724, there are four conditions for prohibiting *Gharar* (*Al-Gharar.. Ma'nāhu Wa Ḍawābiṭuhu*, 2002). These are: *Gharar* is a lot to the extent that it predominates the contract, avoiding *Gharar* should not lead to inflictions and hardship, what is causing *Gharar* is not a general need, and should be confined to exchange-based contracts or anything that is offsetting of exchange. The jurist needs to observe these four conditions when evaluating the issues related to *Gharar*.

4.6.4. Evaluate Exogeneous Components

Exogeneous components include the trading platform and wallet management. These components are not directly related to the operation of the crypto, but rather they only have a 'window' to the system. This means that any issues within the exogeneous components causing *Sharī'ah* violations, will not in essence have any effect on the

ruling of the crypto system. Rather, the violations will only affect the ruling on a certain contract of the component or all of the component itself. So, if there is an issue within a contract provided by a trading platform causing *Sharī'ah* violations, then only that contract will be ruled impermissible, while all other transactions and contracts of the trading platform should be evaluated separately. In case the majority or all of the trading platform's contracts have *Sharī'ah* violations, then that platform should be ruled impermissible as a whole.

This stage takes the remaining issues of issue register 2 because these are the issues related to the trading platform and wallet management. To facilitate looking at the issues from a theme perspective as well as view the related potential *Sharī'ah* violations, Table 4.11 shows an adapted version of both issue register 1 and issue register 2.

Table 4.11: Exogeneous Issues and Potential *Sharī'ah* Violations.

	Issue	Potential *Sharī'ah* Violation	Theme – Financial Consideration
Trading Platform	**5.** Speculative Investments	*Gharar*, *Ribā*	- Exogeneous factor for issue '**4**. Stability & Price Fluctuations'
	12. Offload Transactions from the Blockchain	*Gharar*, Constructive payment receipt might be questionable	- *Gharar* is caused if the trading platform collapses - Could be used as a potential solution for conflict resolution
	13. Trading platform rewards in exchange for a nominal percentage of the returns	*Ribā*	
Wallet Management	**6.** Inheritance Issues	Wealth is lost on death	
	7. Loss of Password	Loss of property & wealth	
	20. Type-0 non-deterministic	Loss of property & wealth	- More secure types of wallets exist
	21. multi-sig as a solution for inheritance[1]		

[1] This is not an issue. It is, in fact, an opportunity for a solution to issue '**6**. Inheritance Issues'.

Source: Author

Table 4.11 presents a lucid depiction of the essential factors that demand consideration by a jurist when assessing each of the exogenous components. Regarding the trading platform, a comprehensive evaluation must be conducted, both holistically and on an

individual contract basis. Notably, issue '**13**. Trading platform rewards in exchange for a nominal percentage of the returns' presents a great challenge. This arises from the *Fiqh* axiom asserting that 'Every loan that entails a benefit is usury,' consequently leading to *Ribā*. To redress this matter, the trading organization ought to refrain from making the use of its platform a prerequisite for receiving rewards or cease providing the rewards entirely. Similarly, issue '**5**. Speculative investments' carries the potential to engender *Gharar* and *Ribā*. Contracts must be devoid of short sells, and forex-type speculations, which contravene various *Sharī'ah* principles, must be prevented. One such violation manifests in issue '**4**. Stability and price fluctuations'. These speculative investments further yield *Ribā* due to the combination of loans and exchanges within a single contract, a practice prohibited by our revered prophet (ﷺ). Moreover, *Ribā al-Nasī'ah* emerges due to the absence of actual or constructive reception of either compensation (*Ḥukm Al-Ta'āmul Bi Al-Forex Al-Islāmī!*, 2009). Conversely, issue '**12**. Offload transactions from the blockchain' poses the risk of *Sharī'ah* transgressions, primarily due to the questionable nature of constructive payment receipts, which can only be realized within the confines of the blockchain. Such circumstances may precipitate *Gharar*. However, offloading transactions from the blockchain may serve as a potential conflict resolution mechanism, whereby funds can be returned to one of the parties prior to permanent recording on the blockchain. To implement such offloading layer 2 solutions, a jurist may require clear contractual provisions stipulating the recording of offloads as credit liabilities on the platform's part, with the platform assuming full responsibility for ensuring their transfer back to the customer.

Likewise, several considerations arise when evaluating the wallet management component. Firstly, the jurist must insist on the utilization of non-Type-0 wallets. Type-0 wallets, being non-deterministic and generating random private keys for transactions, prove arduous to manage and necessitate constant backup. Their usage is ill-advised, as the recovery of such keys becomes increasingly challenging over time, thereby risking potential wealth loss. This relates to issue '**20**. Type-0 non-deterministic'. The Bitcoin development community discourages the use of the Bitcoin core client as a wallet due to its Type-0 nature, advocating instead for more secure wallet management software solutions that abound. Secondly, the overlooked yet paramount issue '**6**. Inheritance issues' demands attention. This issue leads to the

squandering of heirs' assets and consequent wealth loss upon the demise of the owner. Until a wallet solution specifically addressing this concern emerges, we propose considering the adoption of '**21**. Multi-sig as a solution for inheritance'. The jurist should mandate the presence of this feature within the cryptocurrency for it to be deemed viable. The multi-sig functionality empowers transacting individuals or entities to configure an m-of-n multi-signature scheme, requiring 'm' out of 'n' total signatures for a transaction to be authorized. For inheritance purposes, individuals can employ a 1-of-n multi-sig configuration, necessitating only one signature out of 'n' to process transactions. This solution, albeit temporary, does introduce a security consideration, as other signatories can execute transactions on behalf of the account holder at any time. Hence, it is crucial to designate only a select few trustworthy individuals as signatories. Furthermore, issue '**7**. Loss of password', although related to wallet management, falls under the purview of the owner's responsibility, akin to losing a password granting access to funds in a conventional setting.

CHAPTER V

FINDING AND ANALYSIS

5.1. Introduction

The previous chapter built on the gaps extracted from the extant literature to propose a framework for guiding the *Fiqh* analysis of the issues in cryptos. This chapter, on the other hand, presents and analyzes the overall findings from the qualitative data, collected for exploring the main objectives of the study which are the main issues and the confusion that the concept of cryptocurrencies introduced, the extent of adequacy of the approaches followed by the current jurists to address these issues, and the validity of the proposed framework to analyze these issues. The most significant contribution of this chapter is optimizing the framework that was proposed from the previous chapter in section 4.6.

Besides this introduction, there are four other sections. The first shows the profiles of the interviewed participating experts. The second section presents the qualitative data findings from the interviews with those experts, the third discusses and analyzes these findings, and the fourth employs the optimized and validated proposed framework to test a randomly selected crypto on a selected issue.

5.2. Participants Profile

Table 5.1 depicts the profiles of the interviewees by qualification, profession, and institution. The participants have been coded with ‘E’ for Expert followed by a number. In other words, the first Expert would be coded E1, the second E2, and so on until the ninth Expert who will be coded E9.

All respondents were males, reflecting a gender bias. This is rooted in the predominance of male scholars in *Fiqh* treatises on cryptocurrencies and related issues. Eight out of the nine participants are holders of a PhD degree – three in Islamic Finance, two in Islamic Jurisprudence (including comparative Jurisprudence and principles of Jurisprudence), one in Islamic Law, one in monetary economics, and one in business administration. The remaining expert is a holder of a master’s degree in Islamic Banking and Finance.

Table 5.1: Participant Profile

Code	Expert	Qualification	Profession	Institution
E1	Mohammad Abo Jazar	**PhD**, *Fiqh* (Comparative)	Founder & CEO	Crypto Halal
E2	Moutaz Abojeib	**PhD**, Islamic Finance	Senior Advisor	Islamic Finance Initiation Network (IFIN) Services
			Director, Operations	Islamic Finance Advisory and Assurance Services
E3	Almir Colan	**Master's**, Islamic Banking & Finance	CEO	Olive Investments
			Director	Australian Center for Islamic Finance (AUSCIF)
			Member of Working Group	Accounting & Auditing Org. for Islamic Financial Institutions (AAOIFI)
E4	Shabeer Khan	**PhD**, Islamic Finance	Assistant Professor	Sakarya University
			Editor	Hamdard Islamicus
			Sharī'ah Board Member	Tayyib Advisory
			Consultant	iFINTELL Ltd.
E5	Farrukh Habib	**PhD**, Islamic Finance	Cofounder	Alif Technologies
			Strategic Advisor	VePay
			International Chapter Committee Member	Chartered Institute of Islamic Finance (CIIF)
E6	Othman Hamad	**PhD**, Business Administration	Assistant Professor (Part-time)	The Arab Academy for Management, Banking, & Financial Sciences
			Member of National Authority for *Sharī'ah* Control	Central Bank of Djibouti
E7	Ahmed Stitou	**PhD** Monetary Economics	Energy Trading & Senior Business Analyst	STX Group
E8	Majdi Qwaider	**PhD**, *Fiqh* and Principles of *Fiqh*	Member	Association of Palestinian Scholars
			Editorial Manager	Mirqah (Journal)
			Former Imam & Preacher	Gaza Ministry of Religious Affairs
E9	Said Bouheraoua	**PhD**, Islamic Law	Associate Professor	INCEIF University
			Director of Research Development and Innovation	International Shari'ah Research Academy (ISRA)
			Independent Board Member	Affin Islamic Bank
			Sharī'ah Member	Central Bank of Oman

Source: Author

From these results, more than 30 percent of the participants hold academic positions in universities and at least 20 percent are involved in lecturing and training. This amounts to more than 50 percent being involved in academic-related work. Notably, two out of nine, which makes more than 20 percent, are *Sharī'ah* board members in two central banks, Central Bank of Djibouti and Central Bank of Oman.

Additionally, more than 50 percent are board or working group members in banks, organizations, and standard setting institutions like the Accounting and Auditing Organization for Islamic Financial Institutions (AAOIFI). Also, more than 50 percent hold at least one senior position (Director, Cofounder, Founder, and CEO) at prominent institutions (such as ISRA) out of which two hold a CEO position. Moreover, two of the experts are active in peer-reviewed journal editorial positions. Above all, 100 percent of the participants were involved, in various degrees, with cryptocurrencies and their issues whether in research, study-based fatwa, Islamic economic forums discussions, practical work and consultancy, or a blend of them.

The backgrounds of the participants show that they are suitable and relevant for this thesis. The composition of the interview participant sample exhibits a commendable level of related expertise and diversity. Their qualifications demonstrate a robust distribution across disciplines, including Islamic Finance, Islamic Jurisprudence, Islamic Law, monetary economics, and business administration. This diverse academic background enriches the study by bringing in a comprehensive perspective.

Noteworthy is the substantial representation of participants with academic affiliations, exceeding 50 percent. This is complemented by the active involvement of experts in editorial positions for peer-reviewed journals, underscoring their dedication to academic rigor. Such a situation significantly enhances the scholarly depth of the study. In contrast, the active engagement of over 20 percent of participants in *Sharī'ah* board memberships in central banks introduces a practical dimension to their insights. Moreover, the inclusion of *Sharī'ah* board members from central banks, individuals occupying key committee and board memberships in banks and standard-setting institutions, and those holding senior roles at prominent institutions further highlights the study's credibility. Hence, the expert participants were able to provide valuable, credible, accurate, and rich information on the subject during the interview sessions. Such backgrounds are very important for the validity of the data, and the trustworthiness of the research conducted (Graneheim et al., 2017).

5.3. Data Findings

The thematic analysis of the interview extracts resulted in five main themes: Sources of and Reasons for Confusion, Current Juristic Frameworks and Paradigms: Extent of Adequacy, Viability and Validity of the Proposed Framework, Implementation Dynamics: Challenges and Prospects, and Optimizing the Proposed Framework: *Fiqh* and Strategic Recommendations. Table 5.2 shows the themes with their corresponding research objectives. The analyses in the subsequent subsections [5.3.1 – 5.3.5] are conducted based on these five themes.

Table 5.2: Theme-Research Objective Mapping

Theme	Research Objective
Sources of and Reasons for Confusion	1. Examine the following four main issues, unified by the overarching theme that an incomplete comprehension can detrimentally influence the legal rulings associated with cryptocurrencies from a *Fiqh* perspective: 1.1. Contention on the definitions of cryptocurrency 1.2. Limited understanding of the technical aspects of cryptocurrency 1.3. Misconceptions of equating altcoins to Bitcoin 1.4. Cryptocurrency risks
Current Juristic Frameworks and Paradigms: Extent of Adequacy	2. Examine the extent to which the existing *Fiqh* framework has addressed the four main issues of cryptocurrencies stated in research objective 1 above.
Viability and Validity of the Proposed Framework	3. Propose a contemporary *Fiqh* framework for analyzing the stated four main issues of cryptocurrencies and validate the viability of the proposed framework.
Implementation Dynamics: Challenges and Prospects	3. Propose a contemporary *Fiqh* framework for analyzing the stated four main issues of cryptocurrencies and validate the viability of the proposed framework.
Optimizing the Proposed Framework: *Fiqh* and Strategic Recommendations	3. Propose a contemporary *Fiqh* framework for analyzing the stated four main issues of cryptocurrencies and validate the viability of the proposed framework.

Source: Author

5.3.1. Sources of and Reasons for Confusion

This theme relates to the sources of misconception and reasons underlying the confusion that occurred when analyzing the issues of cryptocurrencies. The experts extracts unfolded to show 7 main sources and reasons for the state of confusion – rapid changes; failure to acknowledge crypto diversity; divergent stakeholder agendas and backgrounds; complex concept and phenomena; terminological inconsistencies; lack of expertise and access to information; and influences in rulings in crypto discourse. The fourth (complex concept and phenomena) and the seventh (influences in rulings in crypto discourse) further formed two sub-themes. These will be detailed further in the following subsections. Figure 5.1 portrays this theme and its subthemes.

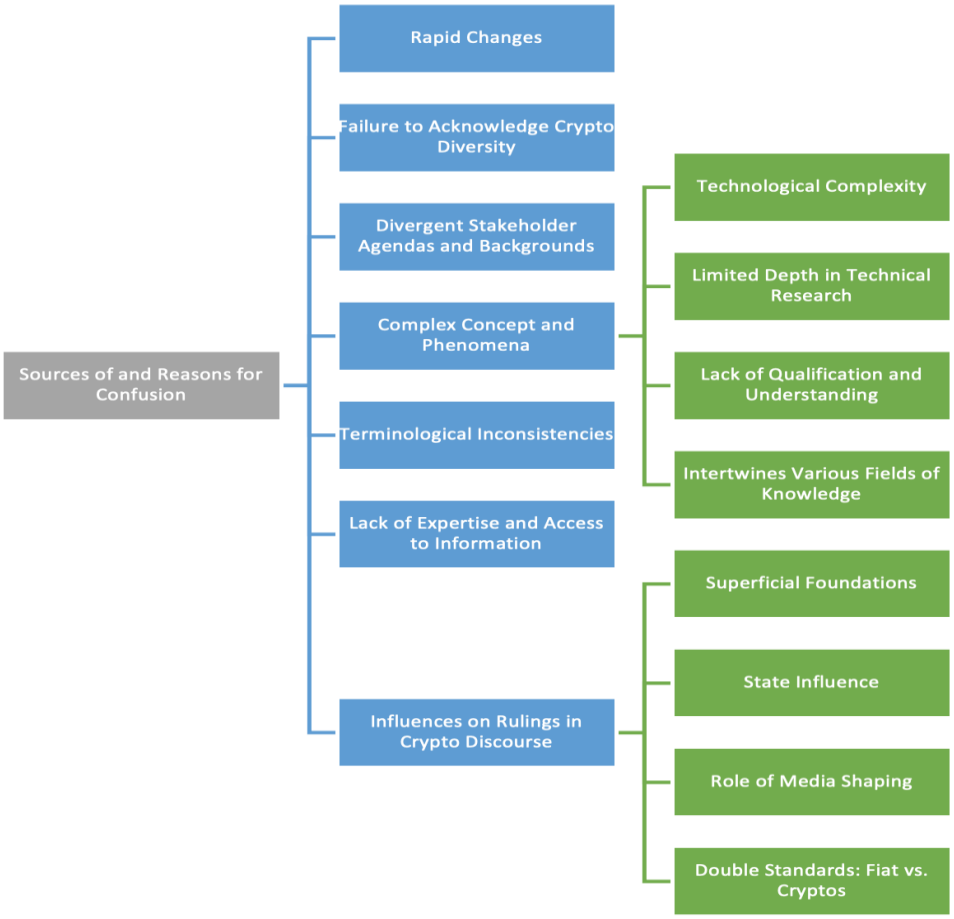

Figure 5.1: Sources of and Reasons for Confusion

Source: Author

5.3.1.1. Rapid Changes

This concept has been mentioned by two experts (E4 and E6). Both experts highlighted the fast evolution of technology outpacing the juristic scrutiny of current

cryptocurrencies. E6 contended that “Conditions evolve... a new cryptocurrency emerges before the ruling on the existing cryptocurrency stabilizes, presenting new features”. In parallel, E4 emphasized that “Change is happening very rapidly” impacting researchers' capacity to standardize and classify these financial entities.

5.3.1.2. Failure to Acknowledge Crypto Diversity

This made a common reason for confusion described by more than 50 percent of the experts. E1 criticized researchers for indiscriminately grouping all digital currencies into one basket. E7 accentuated this concern, highlighting the incongruity of bundling performance-oriented currencies with the second-generation designed for smart contracts. E1 reiterated, “Today, smart contracts… these days, are issued to you in various forms”. On the other hand, E5 shed light on the common perception that all cryptocurrencies mirror Bitcoin, emphasizing the absence of proper categorization. Notably, this was also acknowledged by E6, “It's not just one currency true; but they are looked upon as one type”.

5.3.1.3. Divergent Stakeholder Agendas and Backgrounds

This reason delineated the effect of each stakeholder, shaped by his prejudices and requirements, on the state of confusion. This has been collectively articulated by E2, E3, and E5.

> *Different stakeholders with different agenda… not all of them are coming from the same background. Some of them are coming from purely technical background, some from finance background, and some are mixed… people are not also free from their biasness… all of this contribute to huge confusion* (E2).

> *I think people have a different varying understanding of economics of money in particular. And so, I think it is also context in which this discussion is taking place. Background, larger trends in economy are causing different people to conclude different things* (E3).

> *I think there is a confusion for all the experts in each field. For example, it is not only a confusion from the Sharia perspective, but there is a confusion from the regulatory perspective, political perspective, academicians, bankers, financial experts, economists, [and] technology even* (E5).

E2 observed that distinct stakeholder backgrounds and agendas contributed to considerable confusion. E3 extended this perspective, linking diverse economic trends to disparate conclusions. E5 expanded the purview, acknowledging confusion not only from a *Sharī'ah* and regulatory standpoint but also among academicians, bankers, financial experts, economists, and technologists. This multiplicity of perspectives highlighted the complexity inherent in cryptocurrency discourse, complicating efforts to establish a unified understanding.

5.3.1.4. Complex Concept and Phenomena

A very interesting source of confusion that had a unanimous agreement among all participants is 'complex concept and phenomena'. E7 encapsulated this sentiment, stating, "The subject of cryptocurrencies and the associated blockchain technology is inherently complex". E2 questioned why cryptocurrency should be taken lightly, highlighting the intricate nature of the topic. The underlying factors that played a role in adding to the complexity is 'technological complexity', 'limited depth in technical research', 'lack of qualification and understanding', and 'intertwines with various fields of knowledge'.

E3 acknowledged the complex nature of cryptocurrency technology, the first factor, highlighting the prevalent curiosity surrounding its operational mechanisms. In contrast, E8 expanded on the second factor, lack of in-depth research, attributing it to the insufficient scrutiny by *Sharī'ah* scholars. According to E8, their shortfall lied in the inadequate examination of the fundamental aspects of each cryptocurrency, encompassing their trading dynamics, investment scope, and associated risks. Of significance is E1's assertion that, "They approach the issue technically and delve into it with very superficial depth". This represented the prevailing response among participating experts – a semi-consensus highlighted by E7, conveying a collective "Lack of qualification to delve into these issues". Diverging from this prevailing view, E6 posited an alternative perspective, arguing that proponents of cryptocurrencies have failed to furnish lucid research demonstrating the methods and mechanisms deployed to mitigate risks.

Addressing the third factor, concerning a deficiency in qualification and understanding, E3 astutely observed a predominant tendency to treat cryptocurrencies not as economic entities but rather as technological artifacts. This observation aligned

with E8's contention that technology should be perceived as a means to an end, rather than an end in itself.

Regarding the final factor, 'intertwines with various fields of knowledge', E7 elucidated the expansive multi-disciplinary nature of cryptocurrencies that spanned domains such as programming, encryption, mathematics, economics, and finance. This interdisciplinary involvement, according to E7, amplifies the complexity of the environment.

5.3.1.5. Terminological Inconsistencies

The notion of this concept describes the confusion that resulted from using an inconsistent terminology to describe the crypto space. E2 and E5 both agreed to shift from using the word 'cryptocurrency', in describing the whole spectrum of different types of cryptos, to using the word 'crypto asset'. E5 sustained that the "World Economic Forum, [International Monetary Fund] IMF, World Bank, and all the regulatory bodies… are categorizing this phenomena as crypto assets". E2 extended this terminological inconsistency to other aspects articulating the importance of "Differentiating and defining every and each term… Like what is your definition [of] risk? What is the definition of exogenous factors?… endogenous"?

5.3.1.6. Lack of Expertise and Access to Information

One of the most prominent clarifications of this issue came from E9, who highlighted a conspicuous gap: Arabic-speaking jurists confront limited access to a substantial portion of available cryptocurrency presentations. E9 substantiated this assertion by pointing to the noteworthy postponement of the OIC's IIFA resolution on cryptocurrencies as an illustrative example of the dearth of accessible information. In parallel, E6 attributed the deficiency in expertise to the absence of exchanges in the local markets.

5.3.1.7. Influences on Rulings in Crypto Discourse

This sub-theme elucidates the multifaceted factors contributing to the confusion surrounding unsound rulings in the realm of cryptocurrency. The identified factors encompass 'superficial foundations', 'state influence', 'the role of media shaping', and 'double standards: fiat vs. crypto'. Each participant contributed insights on at least one of these factors.

To explicate the first factor, ‘superficial foundations’, quotes encapsulating the expressed ideas are enlisted below:

> *This superficiality necessarily leads to a deviation in the Sharia ruling. Yet, judgments are made on this basis!… They say to you, “I am hearing this for the first time!” Well, on what basis do you issue the ruling? So, in the end, this is a question posed by someone who was lacking in research!* (E1).

> *As a researcher, [you] have surely encountered some of those scholars who say that this type of currency violates Sharia guidelines and is therefore not allowed at all, [they do so] without going into details. They say, as long as the issuing authority does not guarantee it and risks exist, they generally abstain, meaning they don't delve into these details* (E6).

The second factor, ‘state influence’, is distinctly articulated by E7, revealing that inhibiting opinions may reconsider their stance once countries embrace decentralized cryptocurrencies and thus confirming that the concern was not rooted in sound reasoning but rather in fear of the consequences of having jurisprudential opinions diverging from the official direction. E1 underscored this by questioning the validity of seeking judgment from a staunch Bitcoin opponent and then adopting that judgment.

The third factor, ‘the role of media shaping’, is raised by E4 and E5. Both experts stressed the dangerous influence of media hype and journalism on shaping rulings grounded in unsound reasoning.

The contentious fourth factor, ‘double standards: fiat vs. crypto’, triggered heated debate. While opponents of cryptocurrencies attributed impermissibility to price fluctuations which cause *Gharar*, E8 contended that this risk parallels traditional fiat currencies which are widely accepted. On that basis, E7 argued against exempting cryptocurrencies from sales and *Gharar* rules dictated by Islamic jurisprudence. Comparatively, E5 and E2 drew attention to hyperinflation in countries, emphasizing the disparate standards applied to crypto despite similar challenges in traditional currencies.

According to E5 and E7, the exogenous factor is determined by demand and supply dynamics. Significantly, this factor is also discussed in terms of considering constructive payment receipt. E1 posited that constructive receipt is achieved even if

the transaction is offloaded from the blockchain. Interestingly, E7 challenged this notion, asserting that constructive receipt was allowed for fiat due to a general affliction not reaching the same level in cryptos. Therefore, E7 supported the argument that possession only occurs on the blockchain.

5.3.2. Current Juristic Frameworks and Paradigms: Extent of Adequacy

Figure 5.2 depicts the theme related to the extent of adequacy of the current juristic frameworks and paradigms. The thematic analysis revealed seven factors that influenced the extent of adequacy of the existing juristic paradigms towards cryptocurrency analysis – traditional precedent paradox; superficial screening: regulatory and financial naivety; scholarly disagreement - technical complexity of the concept; verification challenges - absence of regulatory bodies; sensitivity, state influence, and existing framework limitations; divergent views on adequacy; framework challenge - unsettled criteria for cryptocurrency stability.

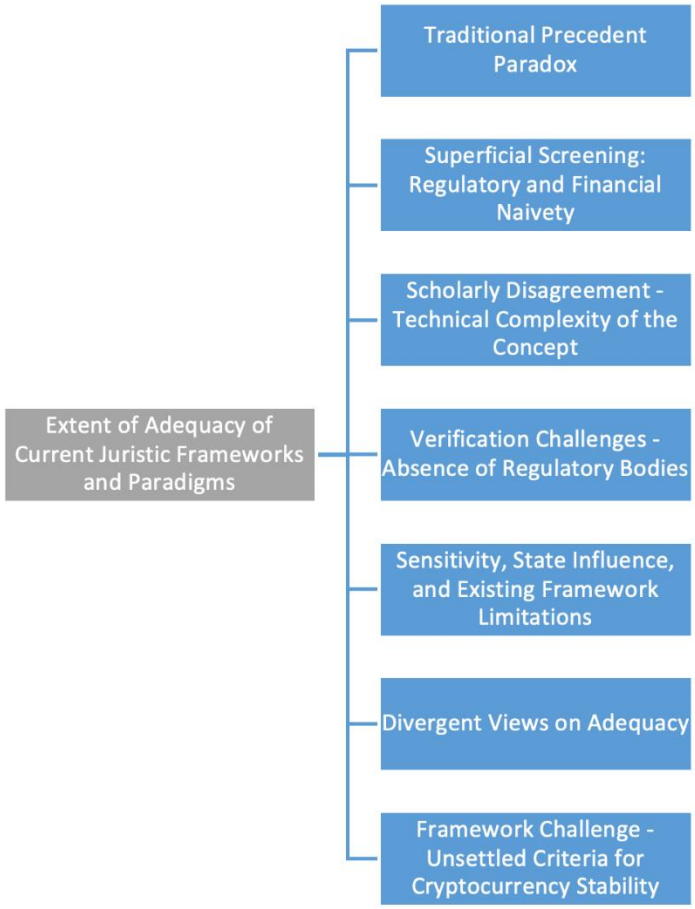

Figure 5.2: Extent of Adequacy of Current Juristic Frameworks and Paradigms
Source: Author

‘Traditional precedent paradox’ has been discussed by one expert only. E8 explicated the complete reliance of the current jurists on the opinions of scholars from various schools of thought regarding the conditions of money in the past and applying these conditions to cryptocurrencies. The second factor, ‘superficial screening: regulatory and financial naivety’, has been brought up by E3 who noted that many scholars on the advisory boards of some cryptocurrencies take the evaluation of the crypto lightly with naivety. Perhaps this forms what was discussed in subsection 5.3.1 as ‘limited depth in technical research’ and rulings based on ‘superficial foundations’. However, what E3 pointed out here is related to the proponents side who are very lenient in their decisions without sufficient scrutiny.

The third factor, ‘scholarly disagreement – technical complexity of the concept’, which links to the sub-theme ‘complex concept and phenomena’ in subsection 5.3.1, has been considered by experts E2 and E4. E2 argued that the technical complexity in a fast-developing environment “added to the issue and challenge of having this kind of framework”. Similarly, E4 affirmed that “it’s too much technical” that those who attempted to develop a [proper] framework struggled to address the contemporary cryptocurrency issues.

The fourth factor ‘verification challenges – absence of regulatory bodies’ has been mentioned by two experts also, E4 and E9. While E4 questioned why known bodies like AAOIFI haven’t taken the initiative for an adequate framework, E9 reasoned that this might be because certain aspects of the cryptocurrencies cannot be easily verified or validated. Perhaps the fifth factor ‘sensitivity, state influence, and existing framework limitation’ is the most prevalent on the extent of adequacy of current views and paradigms which directly links to the ‘state influence’ factor discussed in the previous subsection 5.3.1. This factor has been discussed by almost 50 percent of the participants. Interestingly, E1 indicated that many of the current examinations of cryptocurrencies have not been based on *Fiqh* rules – “Their speech is not related to the legal *Fiqh* rules”. E2 also discussed similar discourse by many scholars where in most of the cases they have been influenced by the political context. E7 described this situation as “A branch of the weakness in theorizing and properly justifying the restriction of issuance in the hands of the governing authority”. Comparatively, E5 questioned the legitimacy of such framework to address the contemporary issues of cryptocurrencies.

The sixth factor 'divergent views on adequacy' is related to the response of the participants towards their opinion on why they think that the current *Fiqh* framework (if exists) is inadequate. Remarkably, the experts split into two groups. E7, E8, and E9 believed that there is no clear and defined framework for contemporary rulings regarding cryptocurrencies. On the other hand, E1, E5, E6 disagreed with this question noting that *Fiqh* framework is flawless and has been working since its inception. Instead, they believed that the problem lies in the implementation of those *Fiqh* rules.

In the last factor, 'framework challenge – unsettled criteria for cryptocurrency stability', E2 indirectly criticized scholars who used the stability of prices as a reason for *Gharar*. Specifically, E2 questioned the lack of standardized criteria for evaluating the acceptability of [fiat] currency fluctuations in financial contracts.

5.3.3. Viability and Validity of the Proposed Framework

The thematic exploration has crystallized into key components that collectively contribute to the overarching theme of 'viability and validity of the proposed framework'. The key components are – 'overall view on the sufficiency of the indicators'; 'validating the developmental stage and cybersecurity indicators'; 'validating the issuing entity criteria'; 'validating the wallet management and platform criteria'; 'regulation role and dual impact of risk methods'. This is depicted in Figure 5.3. We aim to dissect and contextualize the implications of each subtheme within the broader framework discussion.

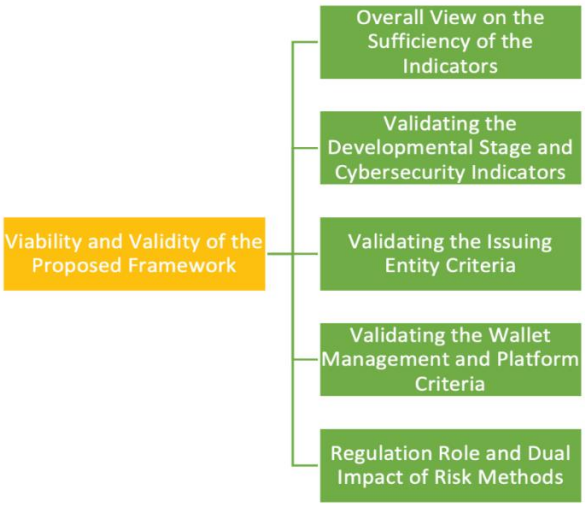

Figure 5.3: Viability and Validity of the Proposed Framework

Source: Author

5.3.3.1. Overall View on the Sufficiency of the Indicators

This component reflects on the extent of overall acceptance of the proposed framework's indicators among the experts. E9 expressed his confidence in them describing them as rational based on justified explanation. Equally, E8 communicated the significant impact the indicators possess "On judging the currency, as they contribute to the stability, acceptance, popularity, and risk reduction". On the contrary to these views, E4 believed that while the current indicators captured technical maturity to a certain extent, he advocated the need for additional ones.

5.3.3.2. Validating Developmental Stage and Cybersecurity Indicators

This has been delineated by E1, E2, E3, E5, E7, E8, and E9, forming more than 75 percent of the participants. On the onset, E3, E9, and E5 conveyed their concerns about the developmental stage criteria and indicators. E5 articulated that the indicators are strict for a new startup project and foretells that such projects will fall prematurely on such benchmarks. Instead, he suggested employing market standards by performing audits. Reinforcing this opinion, E9 advocated relaxed conditions for the infancy stage on the basis that "Even *Fiqh* perspective gives some leniency into the infancy stage". With a completely opposite view, E3 considered the developmental stage unimportant because according to him it is easily fakable. Notwithstanding, the experts discussed the validity of indicators such as merchant acceptance trend, s-test value, market cap, largest stake, smart contract indicators, and stablecoin indicators.

On the s-test value, E7 asserted that it "Undoubtedly reflects the maturity of the currency and its level of security progress". However, E3 emphasized that the s-test value or any similar tests, that might be available for testing the resilience of a crypto against cyber-attacks, only do so on the presumption that the attacks are economic in nature. As such, there has to be a way to test vulnerabilities against attacks based on non-economic motivation such as sabotage intentions. As for the merchant acceptance trend, while E5 expressed his concern that the indicator is very difficult to gauge, E7 argued that the degree of currency adoption based on the increasing number of addresses owned may be used to measure merchant acceptance trend. Nonetheless, E7 alerted that the merchant acceptance trend only makes sense for payment-based cryptos. On the other hand, E8 advised to segregate technical indicators from market efficiency ones since the former are intrinsic and affect *Fiqh* rulings, while the latter

are considered extrinsic and the look at them will only be from a *Maqāṣidi* (objectives of *Sharī'ah*) perspective. In this case, merchant acceptance trend might not make sense at all.

The market cap elicited divergent opinions among the experts. While E7 and E8 considered it important for the determination of market stability, E2, E3, E5, and E1 expressed their reservations deeming it a bad indicator. According to E5, market cap benchmarks are difficult to determine, while E2, E3, and E1 articulated that it is easily manipulated. However, E1 suggested a periodical announcement of a varying benchmark depending on current market conditions to be carried out by an institution.

As for the largest stake indicator in a PoS setting, E2 demonstrated his general contentment for it, however he explained that more can be added to gauge control. In contrast, E1 discussed that the benchmark has to be greatly decreased to "a single digit as an upper limit in the hand of a single entity" in order to achieve a great reduction in risk. Additionally for a crypto "Coin, the percentage we're talking about, meaning fractions of one percent, should be distributed in this way among thousands of people in distributed locations worldwide".

For stablecoins, E2 implicitly advised to evaluate them differently according to the nature of their pegs, while E3 asserted that the audits should be carried out by legitimate entities. In contrast E5, questioned the need for that when they are already centralized cryptos and the issuing entity are already being evaluated. As for smart contracts, E5 acknowledged the suitability of the chosen criteria, but guided to incorporate substrate chains into it.

5.3.3.3. Validating the Issuing Entity Criteria

On the onset, E1 and E5 expressed that the criteria used are fine from a risk management perspective which is one of the components of *Sharī'ah*. However, E2 cautioned that this criteria is meaningless for a decentralized crypto and therefore should be explicitly mentioned. In contrast, other experts advocated to add more conditions to the criteria such as guarantor (E6), verifying business legitimacy (E8), technical and managerial capability (E8), and audits (E7) with reliable disclosures (E3).

E8 articulated that the technical and managerial capabilities can be gauged through individual's operational history. While E1, E3, E4, and E9 raised a flag on the boldness

of terms like trustworthy and truthful, E9 prescribed that trustworthiness can be gauged through track records. In contrast, E3 advocated not to rely on past track records, but instead to take trust by verification through transparency, checking the balances, and audits.

5.3.3.4. Validating the Wallet Management and Platform Criteria

In this component, experts discussed the criteria related to both the exogenous crypto components: platform and wallet management. E2 advised to remove the inheritance criteria as he believed should be part of the awareness of people rather than something that a jurist should rely on for his ruling. As for the platform, E1 emphasized that only spot trading should be allowed and advised to stay "Away…[from] Ethereum network... some matters also remain, such as avoiding derivatives, loans, financial leverage, margins, and the like." Similarly, E8, E4, and E6 stressed to clearly emphasize staying away from usury. As a control in the criteria, E5 added to avoid "Insider trading" as well.

5.3.3.5. Regulation Role and Dual Impact of Risk Methods

More than 66 percent of the participants, namely E1, E2, E4, E6, E8, and E9, expressed the importance of integrating risk management in enhancing the objectivity of *Sharī'ah*. Following are some of the evidence demonstrating this claim:

> *The idea of considering the impact and probability is commendable, I would say. However, I'm not sure again from Shariah perspective, if we can apply it. For me, that could be used when you are applying siyasah Sharī'ah… To measure the Gharar… I believe it may not be the right formula* (E2).

> *Through the integration of methods and risk management, a jurist gains a genuine understanding of the risks and how to mitigate them, contributing to the comprehension of the nature of the currency and subsequently issuing a ruling. This is because the ruling on something is part of its conception* (E8).

E2, E3, E4, and E9 agreed that different cryptos can take on different risk levels on a certain issue. The opinions on the risk levels are as follows. E1, E4, E8, and E9 agreed that low and medium risk can be acceptable risk levels for non-prohibited activities. In parallel, E1 and E9 agreed that issues with high risk level or higher become suspicious. However, E1 and E2 noted that risk level decisions are based on personal assessment, while E6 noted that what is considered high risk for someone, might be a

low risk for another. The same stance has been expressed by E7. Remarkably, E8 summarized the whole thing as, “In Sharia, there is no clear standard or measure that determines the acceptable or unacceptable level of risk”. E2, though, warns that “The implications on the *Fiqh* opinion are pretty much different and higher on the endogenous factors” than on the exogenous ones. So, there should be a differentiation on this part.

As for Table 4.10, which mapped the impact and probability of risk levels and weights with their interpretations, E5 deemed it fine and good to have sharing the same opinion with E9 who said that the interpretations in the table look reasonable and rational, however he emphasized that this falls within the domain of ijtihad. Contrastingly, E7 warned “Not to conflate the risk assessment test with the legal ruling of permissibility or prohibition”.

5.3.4. Implementation Dynamics: Challenges and Prospects

In this theme, the experts discussed the implementation dynamics in terms of the challenges faced by stakeholders in implementing the proposed framework and its prospects towards these stakeholders.

5.3.4.1. Challenges

One of the biggest challenges outlined by a cohort of the experts is the requirement of a complex team to implement it. E1, E2, E4, E5, and E7 pointed out that such an endeavor requires the collaboration of a diverse team and an institution to adopt and sponsor it. Consequently, E5 shed the light on one of the challenges facing the framework which is the capacity to address the different stakeholders with their diverse expertise and backgrounds.

E2 explored another challenge as he highlighted the profound difficulty in measuring speculation. He elucidated that despite conducting a comprehensive research effort to establish measurements for speculation, tangible results have proven elusive. E4 contributed to this narrative, stating that contending with divergent interpretations and opinions among scholars poses a significant challenge.

On the other hand, E1 argued that a challenge for implementing the rules of the proposed framework is to visualize the practical issue. Nevertheless, he articulated that this challenge will uncloud with the entrance to the markets and interacting with traders, project owners, and platform operators themselves daily for a year or two. In

contrast, E4 explored the "Lack of *Sharī'ah* standard" and regulatory standard-setting bodies for cryptocurrencies, akin to AAOIFI, which posed a challenge for the proposed framework.

A significant challenge was raised by E8 who maintained that the calculation of risk ratios is a matter of juristic reasoning, ijtihad. Therefore, both E8 and E7 challenged the proposed framework's "Claim that there is a regulated threshold for *Sharī'ah*-compliant risk". Consequently, E8, E7, E2, and E5 recommended treating the risk thresholds as advice and guidance for scholars and jurists, rather than discussing the *Fiqh* legality of the matter. Realizing the hidden aspects of *Fiqh* in the framework, E1, E5, and E9 collectively emphasized that the proposed framework falls short of capturing the pure *Fiqh* aspect.

5.3.4.2. Prospects

The prospects of the proposed framework, as articulated by a cohort of experts, reveal its potential to serve as a crucial standard for *Sharī'ah* guidance. E1 and E5 specifically highlighted its capacity to establish a normative reference for *Sharī'ah* scholars. E1 further highlighted the pressing need for regulation in the digital currency markets where he positioned the proposed framework as an essential tool for achieving this regulatory imperative. This sentiment was echoed by E3 where he argued that the implementation of the proposed framework is aspired to safeguard people's wealth and prevent harm in the evolving landscape of Web3, metaverse, and virtual reality (VR). This is also evident in:

> *So, in the Fiqh aspect, we need regulation in some respects and significant risk management more than other issues discussed today… It [proposed framework] is a step in the right direction… Everyone agrees that this market, especially in terms of platforms, markets, and transactions, and not only that, needs regulation* (E1).

> *I would say that it will be a great contribution towards having a tool, for example, or a criteria for Sharia scholars to understand more about cryptos and this market. And so that like we will have some sort of standard opinion about Sharia* (E5).

I can say that in terms of framework proposed, it has a combination of good elements… it will give them first of all a comprehensive approach in assessing the implementation of the purchase or the application or the consideration of the cryptocurrency (E9).

5.3.5. Optimizing the Framework: *Fiqh* and Strategic Recommendations

This theme realizes the gaps in the proposed framework from a *Fiqh*, as well as a technical, standpoint and extracts strategic recommendations provided by the experts to enhance and optimize the proposed *Fiqh* framework. In this section, we will suffice by providing a few evidence of the *Fiqh*i points raised by the experts before delving into the recommendations.

5.3.5.1. *Fiqh* Considerations

E7 highlighted that the maturity criteria should not be conflated with *Fiqh* legitimacy of the matter. This was also raised by E5 who explained that the maturity parameters are good to have, however basing a ruling of halal or haram on these parameters will be questionable. E6 explicated a similar *Fiqh* matter whereby he clarified that even if an authority embraces a cryptocurrency, this doesn't necessarily make it permissible.

Another significant *Fiqh* aspect that many have been overlooked in the realm of cryptocurrencies has been brought up by E5, namely, the concepts of al-'urf and ta'āmul al-Nās, in other words custom and people's practices, and how they have been established for cryptos.

On the relation between risk analysis and *Sharī'ah*-compliance, E8's excerpt, extracted from the interview, summarizes the whole concept in just a few words, "Risks alone are not a sufficient reason to prohibit cryptocurrencies, as evidenced by the legitimacy of Mudarabah, which is one of the riskiest investment tools… Nevertheless, I say it is a significant factor influencing ruling".

On the *Gharar* discussion, E5 articulated that only if *Gharar* is internal that it makes a transaction non-compliant. In contrast, *Gharar* that is related to an exogenous factor, like market dynamics, does not affect compliance. As such, E5 stipulated to add a fifth condition to the four *Gharar* conditions described in this study. The fifth condition is to determine whether the *Gharar* is intrinsic or extrinsic. The forbidden *Gharar* will be that which is related to an intrinsic factor. Perhaps this is the reason why E8 hasn't agreed with the four conditions of *Gharar* and explained that everyday transactions

are not free from *Gharar*. All agree on the aspect that minor *Gharar* is forgiven, however notably E7 argued that Bitcoin and PoW-based cryptos fall under this forgiven *Gharar*.

5.3.5.2. Strategic Recommendations

Table 5.3 lists the quick-win strategic recommendations based on the experts' views of the proposed framework. These will make for the improvement of the proposed framework which will be addressed in subsection 5.4.5.

Table 5.3: Strategic Recommendations for Optimizing the Proposed Framework

Expert	Recommendation
E1, E2	The proposed framework should capture the different types of cryptos.
E7	Merchant acceptance trend indicator doesn't make sense in non-payment-based cryptocurrencies.
E1	Although implicitly mentioned, the proposed framework needs to explicitly show the rejection of usury and gambling.
E2	Smart contracts are technically not contracts – this should be made clear.
E1	The framework should look at the permissibility of the project, its services, and it's token/coin use cases. This will fix it to show more of the *Fiqh* aspect of it.
E7	Platforms dominated by usurious projects or largely based on the usurious lending model are generally prohibited.
E7	Platforms where usurious projects are not promoted, then it is advised to have the usurious transactions avoided while the ruling remains dependable on what the original project is about.
E8	Segregate between the technical and market indicators
E2	Framework does not need to go to that extent of granularity in risk assessment.
E8	Proposed framework should check how much a crypto project possesses real investment assets. The more projects of cryptocurrencies have real investment assets, the more they contribute to building a real economy that achieves the Quranic vision of wealth.
E7	Table 4.10 should be reconsidered to demonstrate more logical weight allocations. Reevaluate the weightages to derive logical preferences.

Source: Author

The experts have also given further recommendations, depicted in Table 5.4, that warrant further discussion. Again, that discussion will be carried out in subsection

5.4.6, detailing the feasibility of their implementations and rationale behind adopting or rejecting them.

Table 5.4: Additional Framework Improvement Recommendations

Expert	Recommendation
E3	Make a separate risk severity analysis for economic feasibility.
E3	Make a separate risk severity analysis for each of governance and regulation.
E2	Stablecoin's peg stability should also be evaluated using scenario analysis.
E2	Reinforce the current evaluation by further determining factors and using proxies to measure them.
E4	Check the feasibility of measuring the frequency of attacks on a crypto and their success rates to give additional informed quantification of the indicators.
E3	Implement a mechanism of audits and governance before permitting the publishing of whitepapers.
E3	The framework should address misguided people and the meaning of screening.
E5	The proposed framework needs to be more flexible to address geopolitical implications such as sanctions on certain countries.
E9	More than one set of criteria need to be used for each indicator to address the differences between the developmental stages of the cryptos. This is necessary to avoid terminating an infant project prematurely. You can apply aggregate criteria to achieve this.

Source: Author

5.4. Discussion and Analysis

In this section we discuss and analyze the findings listed in section 5.3. The goal here is two-fold. First, is to discuss the extent to which these findings answer our research questions, that is align to our research objectives listed in Table 5.2. Second, is to optimize the proposed *Fiqh* framework resulting in the first version of a validated and applicable framework that can analyze various cryptocurrencies from a *Fiqh* perspective.

5.4.1. Sources of and Reasons for Confusion

The findings of this study confirmed five of the main sources of confusion that were identified in the literature. The findings further revealed two new sources for confusion – 'rapid changes', and 'divergent stakeholders agendas and backgrounds' that were not found via the literature review. While the literature did point to the confusion emerging from the diversity of the stakeholder backgrounds, however, it has been silent on the effect of the stakeholder agendas, which is deemed to be as equally important as the stakeholder background differences. Nonetheless, all of these sources of confusion acknowledge the four main issues of cryptocurrencies discussed in the first objective: 1. Contention on the definitions of cryptocurrency, 2. Limited understanding of the technical aspects of cryptocurrency, 3. Misconceptions of equating altcoins to Bitcoin, and 4. Cryptocurrency risks.

A word on terminological inconsistency is worth noting. The experts delineated the underlying reason for this confusion which lies in the word 'cryptocurrency' itself. The latter part 'currency' always gives the notion that people will be dealing with money, however, as it is the reality, cryptocurrencies are diverse and not all are monetary in nature as discussed earlier. That's why world organizations started to shift to the word 'crypto asset' rather than 'cryptocurrency' to avoid the monetary connotation in the latter. In this study, the author sticks to the word 'cryptocurrency' while making it very clear in section 4.2 that the proposed definition is that of a crypto asset. The reason for this decision is, firstly, this is how initially the study started and, secondly, since many people including researchers still use the word 'cryptocurrency' to denote the whole spectrum of crypto asset space.

5.4.2. Current Juristic Frameworks and Paradigms: Extent of Adequacy

The seven factors extracted from this theme, again, confirm what has been discussed in literature. Specifically, the factor 'superficial screening: regulatory and financial naivety', demonstrated by the experts of whom many are jurists themselves, acknowledges the superficiality by which a complex concept as 'cryptocurrency' has been addressed. Remarkably, the political influence has been, perhaps, a greatly prevailing driving factor for the shallowness by which the cryptocurrency topic has been addressed. Being discussed by almost 50 percent of the experts, it shows the

degree of inadequacy and dependency by which the researchers attempted to study the topic.

Despite the fact that E1, E5, and E6 had their reservations on speaking about the inadequacy of the *Fiqh* framework in addressing cryptocurrency issues, they still agreed with the remaining experts about the extent of triviality by which the research in this area has been undertaken. The disorientation in the definition of *Fiqh* framework between those experts on the one hand, and the other experts and the author on the other hand, led to the objections of the former against 'accusing' *Fiqh* of any deficiencies, which is quite understandable. Conversely, once this misunderstanding has been eliminated and made clear that the intention was the jurists' paradigms and their approaches based on their perceptions and views, all the experts agreed unanimously on the, what otherwise would be, conspicuous contentions, confusions, misconceptions, and misinterpretations found in the literature on the topic.

5.4.3. Viability and Validity of the Proposed Framework

In general, the proposed framework was accepted by the experts. E4 raised a flag on its viability which is understandable since at this stage the indicators and the whole framework are being validated. The doubts on the indicators and benchmarks were taken into consideration to feed into optimizing the proposed framework, discussed in subsection 5.4.5, which is the final main objective of this section.

As for the discussion by E5 and E9 related to prematurely terminating infant startups, it has to be noted that what these experts were mainly talking about was either centralized-type of crypto projects or smart contract projects. The cyber security controls discussed in the proposed framework are mainly applied on cryptos that form the whole system with network of nodes and a blockchain regardless of being characterized by a project team or just supported by a community. Even with the case of a project and project team, strict cybersecurity criteria is essential as the technical side is an intrinsic part of the crypto, which if not controlled well can lead to the impermissible *Gharar*. As emphasized by E8, technical risks are intolerable. Nonetheless, the crypto project team or smart contract have their own indicators, outlined in Table 4.9, which can be relaxed to address infant startups.

Furthermore, E3 argued that other means of cybersecurity need to be used in order to gauge the vulnerability of these cryptos based on non-economic intentions, such as

sabotage. The author disagrees with that view on the ground that gauging attacks based on non-economic intentions is not feasible nor logical. In analogy to a traditional setting, a bank can put various technical, and non-technical, security controls to safeguard the money and hinder any attempt for attacking based on robbery intentions. However, these security measures can't stop terrorist attacks for the sake of sabotage or any other external catastrophic actions that might occur, though disaster recovery measures might be implemented.

Following are the changes that will be incorporated in the framework, specifically the part that discusses the indicators and their benchmarks – see Table 5.5, based on the experts' feedback.

5.4.3.1. Developmental Stage and Cybersecurity Indicators

Taking the advice of E8, technical indicators will be separated from market ones and therefore merchant acceptance trend will no longer be relevant. The market cap has been deemed inadequate by the majority of the experts and therefore need to be omitted. As for the largest stake criteria, the opinion of E1 will be considered to increase security of PoS cryptos whereby resilience implies that the largest stake should be a single digit, that is less than 10 percent, and thousands of people having stakes less than 1 percent. The latter will appear as average stake less than 0.1 percent. As for stablecoins, there is a necessity of creating two different sets of criteria depending on the type of peg it is set with.

For smart contracts, E5 stipulated to also incorporate the ones built on their own substrate chains. It has to be noted that the latter are blockchains created using the Substrate framework. The framework is open source and provides modules that are already tested and optimized, in addition to providing the latest security controls. From a *Maqāṣidi* perspective this can be subjected to auditing using any of the popular crypto audit firms such as Certik.

5.4.3.2. Issuing Entity Criteria

Based on the extracts from the experts, the issuing entity criteria can be summarized in the following: 1) possess technical and managerial capabilities measured via the individual's operational history, 2) be transparent through performing timely periodical publicly published financial statements, and 3) conduct audits from reliable/reputable audit firms with public disclosures.

It is worth noting that the author disagrees with 'providing guarantee' as a criterion explicated by E6 for approving an issuing entity as this seems irrational or impracticable. No financial institution or team will guarantee losses for any reason. As for guaranteeing operations and the functionality of transactions, such a guarantee cannot be enforced. In an analogy to a traditional bank or financial institution, no bank will give you guarantee for its operations unless what is meant is guaranteeing the settlement of the transaction. With that being said, it has to be noted that the guarantee in this case is quintessential since the bank or financial institution acts as an intermediary that will be liable and responsible for making the finality of the payment. However, for a crypto setting, the issuing entity or project team is not involved in this process, rather this will be accomplished all through the technology. Which brings the issue back to evaluating the resilience of the technology against cyber-attacks while the code/protocol guarantees the end-to-end operation. Therefore, providing guarantee doesn't account for a practicable level of trustworthiness.

5.4.3.3. Platform and Wallet Management Criteria

Based on the experts' feedback, the 'inheritance' is seen as something related to the awareness of the individuals and does not require to be in an evaluation framework. As for the platform, the framework will need to explicitly mention the conditions: 1) Only spot trading should be allowed, 2) No futures, derivatives, loans, financial leverage, margins, or usury should be allowed, and 3) Avoid insider trading.

5.4.3.4. Risk Methods

The risk will be moved from the *Fiqh* implications in the framework to clearly show that it is part of the *Maqāṣidi* side. Therefore, the modifications that will take part in this section is: 1) explicitly mention that low and medium risk levels will be acceptable provided that the subject matter is not related to a prohibited activity, 2) although high and very high risk might be suspicious, however this depends on personal assessments; therefore, the stance of the framework is that of *Maqāṣidi* guidance rather than permitting or prohibiting, and 3) the mapping between the interpretations and the levels of impact and probability, Table 4.10, will move to the *Maqāṣidi* side of the framework.

5.4.4. Implementation Dynamics: Challenges and Prospects

The implementation dynamics theme discussed elements of challenges and prospects of the proposed framework should it be implemented. Most of the challenges revolved around the future practicality of the framework. This will be more clearly apparent as it becomes implemented by an institute with a collaboration of diverse team of experts who have market experience. The challenge related to the relation between risk and *Sharī'ah* compliance, this will be reflected in the optimized version in subsection 5.4.5 of the framework by segregating the *Sharī'ah* compliance from the regulatory part. As for the prospects outlined by the experts, it becomes very clear the importance of implementing such framework and its effect on the stakeholders.

5.4.5. Optimizing the Framework: *Fiqh* and Strategic Recommendations

In this subsection, we incorporate the results from the discussions and analysis made in the previous subsections of this chapter into the proposed framework. The enhanced framework is depicted in Figure 5.4. There are a few notable modifications. The most notable change is the conspicuous segregation, clearly showing the *Fiqh* evaluation part and the *Maqāṣidi* evaluation part. The experts' several emphasis requests to highlight the different types of cryptos in the framework is now more noticeable in several places. The first is in step '0. Start Here' where it clearly distinguishes between cryptos that are characterized by a project (and thus more centralized) and those that are non-project payment-based cryptos. The second occurs in step '4. Evaluate Issuing Entity' where it clearly shows the additional criteria to be followed for smart contracts and stablecoins. Another very significant adjustment made was to incorporate E1's advice, as shown in step 1 of Figure 5.4, for screening the project (if exists), its services, and coin/token use cases against any *Sharī'ah* violations, and step 2 for screening the contract against any conditions that might invalidate it.

In the subsequent paragraphs, the framework will be elaborated, walking through the examination of a certain crypto in a step-by-step methodical approach. It is noteworthy to know that the label '0. Start Here' in the figure is not a process step as per se, rather it is an indication where one should start. Additionally, this label shows one of two routes: 'YES' indicates that the crypto under examination is of the P2P payment-based type that has no underlying project. The other 'NO, Project Exists' designate that the crypto under scrutiny indeed has an underlying project. Moreover, it is critical to

understand that these steps are processes by themselves as they involve a lot of work within. Therefore, going forward, this study will continue with the same standard of using the word 'process' instead. Post the discussion of the processes, there will be a subsection to explore the infeasible recommendations given by the experts.

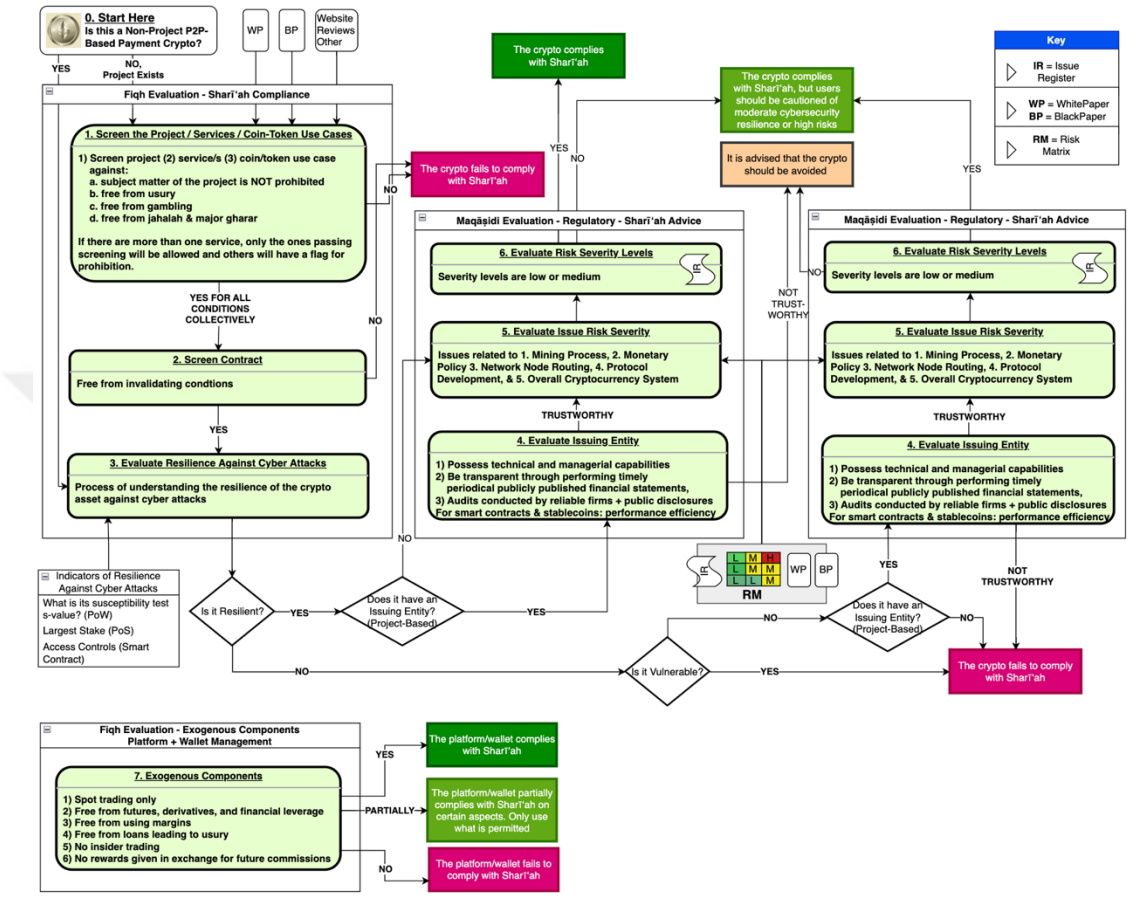

Figure 5.4: Optimized Version of the Proposed Contemporary *Fiqh* Framework
Source: Author

5.4.5.1. Process: Screen Project, Services, and Coin/Token Use Cases

This process screens the crypto project (if exists), its services, and coin/token use cases against any *Sharī'ah* violations. All of these (project, services, coin/token use cases) should be clear from dealing with any prohibited matter, like selling wine. They also should be free from usury, gambling, *Jahālah*, and major *Gharar*. Two important aspects that a jurist has to note. Firstly, if some services violate *Sharī'ah* rules, then the jurist can proceed with the permissible ones and dismiss the violations as impermissible while clearly pointing this out to people. Secondly, apart from the four conditions of *Gharar* (see the conditions here), major *Gharar* should be one that causes great uncertainty on something that is inherent to the crypto as was clearly put by E5

and many other experts. For example, E8 clearly mentioned that the *Gharar* in trading is what all jurists agreed to be minor. Also, E7 mentioned that PoW falls under the forgiven *Gharar*.

5.4.5.2. Process: Screen the Contract

In this process the jurist needs to verify that there are no clauses within the contract that can invalidate it. For example, taking immediate or full possession of the coins after exchange is mandatory in *Sharī'ah*. Otherwise, the crypto can't be *Sharī'ah* compliant. In summary, the contract between the two parties, the user/client and the crypto project/team, should be free from any invalidating clauses.

5.4.5.3. Process: Evaluate Resilience Against Cyber-Attacks

This is the revised version of evaluating the maturity of the crypto to determine its developmental stage. The reason for changing the name is two-folds. Firstly, during the qualitative study, the author identified a confusion that the word 'maturity' and 'developmental stage' produced. These words were understood differently, many of which thought of it from an investment perspective especially that it was coupled with several indicators related to the market, like market cap and merchant acceptance trend. That's one of the reasons why E8 recommended to segregate the technical indicators from the market ones. Hence, we come to the second point. This title now better captures the essence of the indicator where what is intended is understanding the security resilience of the cryptos against cyber-attacks. Thus, Table 4.9 is now revised to include the indicators and benchmarks shown in Table 5.5.

Table 5.5: Cybersecurity Indicators and Benchmarks for Resilience

		Resilient	**Further Scrutiny**	**Vulnerable**
PoW	S-value *	< 0.532	≥ 0.532 and < 0.826	≥ 0.826
PoS	Largest Stake	$< 10\ \%$	$\geq 10\ \%$ and $< 20\ \%$	$\geq 20\ \%$
	Average Stake	$< 0.1\ \%$	$< 0.2\ \%$	–
Smart Contracts	PoS or PoW Criteria Satisfied **	Yes	See PoS or PoW	None is Satisfied
	Access Controls	Recommended	Satisfied	

* S-value = Susceptibility test value
** Only if based on PoS or PoW – If it is based on substrate chain, then this is not required

Source: Author

Notice that Stablecoins are no longer included because all of their indicators are related to the issuing entity since these are centralized and their resilience will be based on the team behind them. Another note is that PoW and PoS have no further indicators since market cap and merchant acceptance trade were determined unnecessary in the previous discussions. Smart contracts, on the other hand, had some of the indicators shifted now to be part of evaluating the issuing entity. In this part, the controls of PoS or PoW, whichever it is built on, and the access controls determine its security against cyber-attacks and illegal access respectively.

In case the table shows that it is resilient, the crypto will go to the next scrutiny step either to evaluating the issuing entity (if it is centralized and project-based) or to evaluating the risk severities (if it is decentralized and have no project team behind it). If the result requires 'further scrutiny', non-project based cryptos will be deemed non-*Sharī'ah* compliant. Otherwise, the crypto will be subject to evaluation of the issuing entity.

5.4.5.4. Process: Evaluating the Issuing Entity

The criteria for this process have already been delineated in subsection 5.4.3. However, added to these criteria are the ones depicted in Table 5.6 which concern additional conditions for smart contracts, pegged stablecoins, and non-pegged algorithmic stablecoins.

Despite being technical and related to the underlying technology, the smart contracts indicators 'Require(), assert(), revert()' and 'Formal Verification' have been removed from the cybersecurity indicators table to the issuer's indicators. This is due to the fact that these verifications are related to errors and faults in the software rather than being a direct vulnerability to a security threat. Therefore, any issues with the software and coding should be referred back to the issuer in the sense that it should provide formal verification and proof of the reliability of its software.

Moreover, Table 5.6 elaborates on stablecoins by distinguishing between those that are pegged to certain assets, and those that are algorithmic with no pegs to any asset. As depicted in the table, algorithmic stablecoins do not require the indicator 'Track-record of peg stability'. This is because algorithmic stablecoins use algorithms to control the money supply in order to preserve the stability of their values.

Table 5.6: Smart Contracts & Stablecoins (pegged & non-pegged) Criteria

		Efficient	Not Sufficiently Efficient	Inefficient
Smart Contracts	Require(), assert(), revert()	Recommended	Satisfied	Not Satisfied
	Formal Verification	Recommended	Maybe	Not Satisfied
	External Audit by Reputable Auditors	Must	Not Satisfied	Not Satisfied
Pegged Stablecoin	Full Public Audits by Reputable Firms	Satisfied	Partial	No
	Track-record of peg stability	Yes	No	No
	Reserves Transparency	Yes	Not clear	No
Non-Pegged * Stablecoin	Full Public Audits by Reputable Firms	Satisfied	Partial	No
	Reserves Transparency	Yes	Not clear	No

* Algorithmic stablecoins have no pegs, but stability is achieved algorithmically

Source: Author

5.4.5.5. Process: Evaluate the Issues Risk Severities

In this process there were not many changes to the original framework as it was endorsed by some of the experts. However, E7 recognized an illogical weightage related to the probability and impact levels from Table 4.10. This can best be described by an example. Suppose a trader/user underwent a transaction that is marked with a certain probability (weight = 5) for loss but has an impact of marginal loss (weight = 3). In this case, the risk severity level will amount to $5 \times 3 = 15$. Suppose another trader/user underwent a transaction that is marked with a 50-50 chance of loss, that is a possible occurrence (weight = 3) but if occurs leads to a significant loss, that is critical impact (weight = 5). In this case also, the risk severity level will amount to $5 \times 3 = 15$. Rationally, no trader would prefer a significant loss even if it is uncertain. Therefore, both these situations should have a different risk severity level.

This illogical case stems from the fact that "Most traders tend to detest a potential significant loss by 1/2 more than they detest a certain marginal loss" (E7). Therefore, E7 suggested to correct this by giving the impact a weight of 0.75 and the probability a weight of 0.25.

As such, an event where someone has a 50 percent probability (measured as 3) for a significant loss (measured as 5) will end with a risk severity level:

$$0.25 \times 3 + 0.75 \times 5 = 0.75 + 3.75 = 4.5$$

Whereas an event where someone is certain (probability measured as 5) to have a marginal loss (measured as 3) will end with a risk severity level:

$$0.25 \times 5 + 0.75 \times 3 = 1.25 + 2.25 = 3.5$$

Therefore, these new weightages yield a more rational result. With that being said the risk levels will be modified as shown in Table 5.7.

Table 5.7: Risk Severity Matrix (Revised)

		Impact-0.75				
		Negligible (1)	**Minor (2)**	**Marginal (3)**	**Significant (4)**	**Critical (5)**
Probability-0.25	**Certain (5)**	Low (2.00)	Medium (2.75)	Medium (3.50)	High (4.25)	V. High (5.00)
	Probable (4)	Low (1.75)	Medium (2.50)	Medium (3.25)	High (4.00)	V. High (4.75)
	Possible (3)	Low (1.50)	Medium (2.25)	Medium (3.00)	High (3.75)	High (4.50)
	Improbable (2)	Low (1.25)	Low (2.00)	Medium (2.75)	Medium (3.50)	High (4.25)
	Highly Improbable (1)	Low (1.00)	Low (1.75)	Medium (2.5)	Medium (3.25)	High (4.00)

Source: Author

5.4.5.6. Process: Evaluate Risk Severity Levels

Continuing with the new levels and weightages, the risk levels and their corresponding severity range has been revised as shown in Table 5.8. Everything else remains the same as in the original framework. As can be seen, a low risk level would have a severity range of less than 2.25, a medium risk level would have a severity range between 2.25 (inclusive) and 3.75, a high-risk level would have a severity range between 3.75 (inclusive) and 4.75, and a very high-risk level would have a severity range greater than or equal to 4.75.

Table 5.8: Risk levels & Corresponding Severity Range (Revised)

Level	Severity Range
Low	Level < 2.25
Medium	$2.25 \leq$ level < 3.75
High	$3.75 \leq$ level < 4.75
Very High	Level ≥ 4.75

Source: Author

5.4.5.7. Process: Evaluating Exogenous Components

This remains the same as before in addition to the streamlining points added from subsection 5.4.3. These are summarized as: only spot trading is allowed, there should be no usury nor insider trader. It is important to notice that this process has been detached from the remaining framework. Naturally, the crypto itself subjected to scrutiny is not part of the exchange platform or the wallet that a user uses to fulfil his transactions. Therefore, it was rationale and logical to detach it, yet still include it to realize comprehensiveness.

5.4.6. Exploring Other Recommendations

In subsection 5.3.5.2, Table 5.4 presented additional recommendations that necessitate further discussions, and this subsection undertakes their analysis. E3's proposal to integrate a risk severity analysis for economic feasibility aligns with the assessment of *Sharī'ah* compliance of startup projects, their services, and token use cases in the optimized framework. Yet, delving into the economic evaluation requires additional research on its implications for the *Fiqh* dimension. Similarly, E3's recommendation for severity analysis on governance and regulation warrants future exploration.

An intriguing suggestion by E3 advocates for the framework to address misguided individuals. Although the current *Fiqh* framework primarily focuses on *Fiqh* and *Maqāṣidi* dimensions, the prospect of extending it to periodically report on various cryptocurrencies and their health may be considered by future institutions and sponsors.

E2's proposals to enhance indicators and incorporate a scenario analysis for stablecoin peg stability, along with E4's suggestion to study attack frequencies and success rates, and E3's idea for governance in whitepaper publishing, serve as valuable foundations for future research. Particularly, E9's proposition for an aggregate scale for issuing

entity criteria stands out as a promising avenue for distinguishing trustworthy entities from less reliable ones, although it necessitates further research for development.

Conversely, E5's recommendation to address geopolitical implications, such as sanctions, though displaying flexibility, appears impracticable and exceeds the framework's inherent capabilities.

5.5. Testing the Framework on Selected Issues

Subjecting a crypto to *Sharī'ah* assessment using this study's framework will result in one of four rulings:

A. The crypto fails to be *Sharī'ah* compliant – it is impermissible.
B. It is advised that the crypto should be avoided – the risk is either high or issuer is not trustworthy.
C. The crypto is *Sharī'ah* compliant, however users should be cautioned of moderate cybersecurity resilience or high risks.
D. The crypto is *Sharī'ah* compliant.

Table 5.9 enumerates all the scenario cases for which a crypto under scrutiny might pass through. The table gives the *Sharī'ah* ruling for each scenario. However, this table was unable to capture an additional scenario whereby the crypto can be moderately resilient against cyber-attacks, but it's of the P2P payment-based type that has no issuing entity. In this scenario, the crypto will fail the assessment and will be ruled impermissible. Out of the 11 (actually 12) scenarios, a crypto will have a ruling of being *Sharī'ah* compliant in two scenarios only. Intuitively, a crypto will have to pass all stages in order to be ruled permissible and this only happens with these two scenarios. On the other end, a crypto will be ruled impermissible in 4 out of 11 (actually 5 out of 12 if we take the uncaptured scenario) scenarios.

To test the framework on select issues, first we randomly choose a crypto for which to conduct the test on. In order to clear any bias, this study employed AI (ChatGPT) to pick up the crypto by random – which the AI selected to be Cardano.

Table 5.9: Shariah Ruling Scenarios on the Proposed Framework

Framework's Process	Scenarios										
	1	2	3	4	5	6	7	8	9	10	11
1. Screen Project, Services, Use Cases	P	P	P	P	P	P	P	P	P	P	F
2. Screen Contract	P	P	P	P	P	P	P	P	P	F	-
3. Evaluate Resilience Against Cyber-Attacks	P	P	P	P	P	F	F	F	F	-	-
4. Evaluate Issuing Entity	P	P	F	-	-	P	P	F	-	-	-
5. Evaluate Issue Risk Severity	P	P	-	P	P	P	P	-	-	-	-
6. Evaluate Risk Severity Level	P	F	-	F	P	P	F	-	-	-	-
Sharī'ah Ruling	**D**	**C**	**B**	**C**	**D**	**C**	**B**	**A**	**A**	**A**	**A**

Key:
P = Pass the process F = Fail the process
A = Impermissible **B** = Advise to avoid
C = Permissible with caution **D** = Permissible

Source: Author

5.5.1. Brief Background of Cardano

Cardano was founded in 2015 by Charles Hoskinson and launched in 2017 with the aim to be a decentralized development platform with verifiable smart contracts (Conway, 2023). The goal of the main project is to provide substantially lower fees, more scalability, and faster transaction throughput and speed than Ethereum (Jain, 2022). The blockchain platform utilizes PoS mechanism to add blocks and earn rewards. The first manifestation of Cardano allowed users to buy and sell using its own cryptocurrency, ADA, on a federated network running its proprietary consensus PoS protocol called Ouroboros (*Cardano Roadmap*, n.d.).

In its roadmap, Cardano is determined to move gradually to a decentralized network with a thousand of staking pools in order to avoid malicious behavior (*Cardano Roadmap*, n.d.). As such, Cardano aims to compete with Ethereum in establishing itself as a decentralized platform for hosting decentralized distributed applications using smart contracts; so, its main services focus is on smart contracts and security (Jain, 2022). Also, as of August 2022, Cardano was reported to have more than 3 million holders of ADA, of which 10 percent controlled 92 percent of the Cardano supply, while the top 10 holders controlled 6.71 percent (Jain, 2022).

5.5.2. Cardano: Preliminary Scrutiny with the Proposed Framework

Cardano's main project is to provide a decentralized blockchain backbone for carrying out two main purposes: 1) P2P payment-based transactions using its own

cryptocurrency ADA, and 2) an infrastructure for developing and deploying smart contracts that are faster than Ethereum at a fraction of the cost.

It has a plethora of services starting with its own wallet, to having its own deployment of smart contracts, and not ending with providing its own programming language for simple and secure development of smart contracts (*Cardano Roadmap*, n.d.). According to them, they plan to move to complete governance by having a voting system and treasury (*Cardano Roadmap*, n.d.).

With the cursory information about the project and its services, a preliminary assessment of Cardano can pass the *Sharī'ah* screening for the project, services, and use cases. However, the complete scrutiny requires considerable time looking at the whitepaper, roadmap, the intricacies of the services, and contracts. This is out of the scope of this study, and therefore, the thesis suffices with this preliminary check.

5.5.3. Testing Cardano on Select Issues

5.5.3.1. Test 1: What is the Risk of Majority Attack

Cardano will be tested on the issue 'The possibility of a miner (staking participant) to control more than 50 percent of the network'. This issue is extracted from issue 10 from Table 4.4.

As per the preliminary data, the largest holders of stakes seem worrying. However, with a quick estimation, since there are more than 3 million holders of ADA, then ten percent of those would amount to more than 300 thousand. The average stake would then be around $\frac{92}{300000} = 0.0003$ percent. The number is very much less than what the study have stipulated to be, i.e., the average stake should be less than 0.1 percent. This makes Cardano look to have a low risk on this issue. Furthermore, since the top 10 holders own 6.71 percent of ADA, then definitely the largest stake (top holder) will control less than that number which as stipulated in this study is a single digit number. Therefore, the probability for a stake holder to control 50 percent of the network is highly improbable. This leads to a low risk level.

5.5.3.2. Test 2: Testing KEVM – Cardano's Developed Smart Contract

KEVM is a smart contract developed by Cardano (*Cardano Roadmap*, n.d.). It will be tested against the issue 'Security of smart contracts'. This issue is extracted from issue 22 from Table 4.4. According to Table 5.5, smart contracts will be secure if the PoS

blockchain on which it runs is secure and it applies access controls. The PoS criteria has been already checked with the largest stake and average stake criteria from the previous subsection where Cardano's PoS has passed the test with low risk level. What is clear is that KEVM has undergone formal verification which satisfies the criteria for the issuing entity. However, there is lack of information or data about whether KEVM applies access controls within its software distribution. This can be verified by either being a user of KEVM or finding a technical paper outlining its stance. With the lack of this knowledge, the security risk of this specific smart contract is high.

In summary, this chapter presented the results of the qualitative study that employed a thematic analysis. Then a thorough analysis was conducted on these extracts and themes in order to validate the proposed framework. This experience allowed to optimize the framework while streamlining the *Fiqh* part from the *Maqāṣidi* part with a clear demarcation between them. Employing the optimized framework, the author conducted select tests on a randomly selected crypto, Cardano.

CHAPTER VI

CONCLUSION AND RECOMMENDATION

Historically, cryptocurrency started with the Bitcoin as a peer-to-peer payment system akin to a traditional financial system, albeit a one that can carry out a sales contract 'face-to-face' without any intermediaries analogous to a physical commercial setting. To realize this, the Bitcoin system had its own monetary currency which is also termed bitcoin[26]! Besides the disruptive technology, this created the first confusion among both people and researchers, diverting their attention from grasping the broader context. Instead, they focused solely on comprehending the currency and its implications, neglecting the network that underlies it. The birth of new cryptocurrencies with different purposes and types proliferated exponentially bringing in tremendous features and solutions. This further added to the confusion as no longer the 'currency' part of the word captured the essence for which they were created. Particularly, the confusion leaked to the Muslim world as scholars attempted to define it and understand the *Sharī'ah* stance towards such new innovations. The complexity of the concept and system shed its light on the *Sharī'ah*, legal, regulatory, financial, economic, and political dimensions and implications it made.

This study recognizes the importance and significance of this topic; consequently, the author attempted to uncover the underlying reasons for the confusion that occurred and their implications on research and understanding. Specifically, the study conducted a literature review to look at these issues from a *Fiqh* perspective touching upon the contentious debate on what constituted a cryptocurrency, the superficial understanding of the underpinning technology and technical aspects, the failure to realize the inherent differences among the different types of cryptos, and the risks and implications caused. Upon this examination, the study identified the significant inadequacy of the existing juristic frameworks and paradigms in addressing these issues. Hence, the author proposed an alternative contemporary *Fiqh* framework.

[26] Notice that bitcoin with lower case 'b' refers to the coin.

To validate the proposed framework, the study employed qualitative research by conducting semi-structured interviews with high caliber experts who possessed vast experience with cryptocurrencies and their *Fiqh* issues. These interviews were then processed using thematic analysis. The outcome of this analysis was very insightful.

Primarily, it illuminated and substantiated the confusion introduced by cryptocurrencies upon their inception, particularly the complexity it infused into the process of issuing *Fiqh* rulings, a central concern of this study. The analysis discerned distinct sources of this confusion, encompassing the intricate nature of the concept and the tendency to approach it superficially, divergent stakeholder agendas and backgrounds, the oversight of crypto diversity and typologies, and various influences, including state influence, on *Sharī'ah* rulings. Notably, the study identified a prominent discrepancy; while the level of risk does not inherently render an investment impermissible from a *Fiqh* perspective, E8 reported that the severity of risks constitutes the primary rationale for those advocating the prohibition of cryptocurrencies. This discrepancy suggested a potential conflation of risk with *Gharar*. Another illustration of the superficial treatment of the topic is the presumption that a lack of knowledge about the issuer leads to prohibited *Gharar*, stemming from a deficient comprehension of the underlying technology. Responding to this, E9 remarked that while familiarity with the issuer is generally preferred, other factors such as performance, stability, and external influences should be considered in risk assessment. This suggests that a cryptocurrency with an unknown issuer might ultimately demonstrate greater resilience and acceptability.

Secondly, the discussed sources of confusion directly impacted many scholars and jurists, exerting a negative influence on their frameworks and paradigms for approaching the subject. The inadequacy of these paradigms became strikingly evident as the interviewed experts elucidated the factors contributing to these shortcomings. The study identified several of these factors, most notably the traditional precedent paradox (where scholars applied tools and methodologies from historical contexts to contemporary innovations without adequately accounting for influential differences and contextual nuances), superficial screening, scholarly disagreement arising from the technical complexity of the concept, and sensitivity to state influence.

> *Here is the problem: the theory and the application. When you come and hear… a group of those [scholars] who spoke on this matter, their speech is not related to the legal Fiqh rules… If presented to the Fiqh rules, [their] talk collapses* (E1).

For instance, the stipulation that issuing money should be the exclusive right of the state was not properly justified. According to E7, the reason for this is attributed to a "deficiency in theoretical foundation and a lack of proper justification for restricting the issuance of [money] exclusively to the governing authority".

Thirdly, the proposed framework underwent further optimization by accentuating the *Fiqh* considerations highlighted by experts and implementing some of the strategic recommendations. On one hand, the *Fiqh* considerations encompassed an augmentation to the framework, introducing a screening layer for evaluating the primary project of the cryptocurrency, its services, and the use cases of its coins/tokens, in accordance with E1's six criteria for evaluating cryptocurrencies from a *Fiqh* perspective. A pivotal enhancement involved the explicit segregation between the *Fiqh* aspect and the regulatory *Maqāṣidi* component. This refinement rendered the proposed framework more robust, elucidating the dimensions of the subject matter for researchers or jurists, enabling a more objective ruling grounded in both *Sharī'ah* components. On the other hand, the strategic recommendations led to significant modifications that profoundly influenced the framework's viability. These recommendations validated the indicators, facilitated the refinement of benchmarks, enabled the identification of critical elements pertaining to *Fiqh* and *Maqāṣidi* considerations, and demarcated between technical indicators and market-oriented ones.

The testing and analysis of the validated proposed *Fiqh* framework on selected issues accomplished multiple objectives. Firstly, it served to test the applicability of the proposed framework, thereby validating the practical utility of the theoretical construct. Secondly, it evaluated the generalizability of the conceptual framework, enabling the exploration of its robustness for application to a broader range of issues or the identification of necessary adjustments for diverse contexts. Thirdly, the testing provided a foundational point from which practitioners, policymakers, and researchers could more readily adopt the framework. Fourthly, it facilitated the verification of the enhancements made to the refined indicators.

6.1. Originality of the Thesis

The originality of the thesis stems from its practical contributions. Firstly, the thesis underwent a task to simplify the complex concept by demonstrating several technical models that visually aided the understanding. Secondly, the author asserts that the general definition of cryptocurrencies has been refined to be more inclusive of their true nature, thus accurately encapsulating their essence. Thirdly, the thesis tackled the inadequacy of the existing juristic paradigms and frameworks, which, as exemplified by many of the interviewed experts, unveils the unique deficiencies in theoretical foundations and justifications. In other words, the contribution is a pioneering one that developed a contemporary *Fiqh* framework.

6.2. Challenges and Prospects of Implementing the Framework

6.2.1. Challenges

A subset of the interviewed experts deliberated on the challenges associated with implementing the proposed framework, emphasizing the necessity of a diverse and capable team along with institutional support for successful adoption. This challenge is multiplied by a potential obstacle pertaining to the willingness for change. Therefore, it becomes imperative for scholars to shift their paradigms to overcome this resistance for change and embrace the framework. The author acknowledges that the framework demands extensive real-world testing beyond the academic realm. However, the lack of a track record for this new initiative may lead to apprehension, resistance, or reservations among individuals, potentially trapping it in a loop and hindering widespread implementation.

6.2.2. Prospects

The inevitableness of effective risk management and the pronounced need for the establishment of robust standards are evident in the context of cryptocurrencies. This perspective resonated with the expert interviewee E5, who posited that the proposed framework could serve as a noteworthy tool or criterion for enhancing the *Sharī'ah* scholars' comprehension of cryptocurrencies and the dynamics of the associated market. The envisaged model facilitates the evaluation of a currency's maturity and risk level which helps to facilitate the formulation of a juristic legal opinion subject to scrutiny.

The comprehensive nature of the framework, encompassing Sharia compliance, operational intricacies, and risk considerations addresses the gaps and inadequacies found in the currently existing juristic frameworks and paradigms when dealing with the subject. This holistic approach caters to the fundamental requisites of a diverse spectrum of stakeholders, including *Sharī'ah* scholars, crypto investors, and regulatory researchers. The approach demonstrated by the framework holds promising potential for widespread implementation. This can potentially establish it as a pioneering standard for the intricate domain of digital cryptocurrencies. The framework could potentially serve as the foundation for a rating agency. In this scenario, cryptocurrencies would receive ratings and reports for public consumption, similar to established financial rating agencies such as Moody's, Fitch Ratings, and Standard & Poor's.

6.3. Limitations and the Way Forward

6.3.1. Limitations

Despite being validated conceptually via thematic analysis, the proposed framework necessitates further real-world testing to validate its practical applicability beyond the academic domain and to garner feedback for prospective refinements. It has to be noted that due to the time constraint of a PhD journey, further research on various parts fall out of the scope of the research objectives. However, such limitations can have their implications on the real-world practicality. Therefore, a real practical test on the institutional level can lead to profound results. On one hand, this will contribute to the establishment of a robust track record and facilitate the transition for a paradigm shift among scholars and researchers. On the other hand, it can yield empirical data to further solidify the benchmarks outlined in this study.

From the technical and market dynamics, this study acknowledges that cryptocurrency markets and technologies are rapidly evolving. The framework developed in this study definitely needs continual adaptation and updates to keep pace with the dynamic nature of the cryptocurrency landscape. This would only reinforce the challenge that such framework requires the adoption and sponsorship of an institution that can nurture a diverse team of experts.

6.3.2. Future Research

The exploration conducted in this PhD thesis study provided enduring insights into the subject of cryptocurrencies from a *Fiqh* perspective. While the study attempted to integrate many of these insights into the framework, some more substantial aspects were subject to the limitations of this study and fell outside the scope and time constraints of this thesis but merit consideration. Accordingly, the author recognizes that such insights can be valuable for future research and enhancements to this framework, potentially leading to subsequent versions in the future. Here, we highlight the most significant, interesting, and impactful insights, in our opinion.

Despite the widespread emphasis on scrutinizing white papers, including this study, to assess various aspects and issues of a cryptocurrency, this study identified a contrasting stance that expressed skepticism about relying solely on them. This viewpoint posited that anyone could publish a white paper with conditions seemingly compliant with *Sharī'ah* but lacking regulatory discipline. Consequently, the efficacy of using white papers in the framework is questionable. Therefore, it is suggested to implement a mechanism where regulators impose audit requirements and a governance structure before accepting such white papers. Further research could delve into this direction.

The study also has identified that track records might not be sufficient as a criterion for evaluating the issuer of a crypto asset. This is true for stablecoins as well. Therefore, another identified avenue for potential future research involves incorporating scenario analysis to evaluate stablecoins and supplement the criteria of track records. This applies to several other criteria and indicators. Therefore, further enhancement would be researching into developing more representative measurable proxies for the indicators and then determining the benchmarks. In parallel to this, an interestingly identified avenue for research is validating the security indicators by measuring the frequency and success rate of cyber-attacks whereby a high rate of successful attacks indicates a deficiency in the chosen indicators, while a lower rate suggests the indicator strength. However, the viability of such methodology itself requires research.

6.4. Recommendations

Although the research objectives of this thesis were to identify the confusion and contention the crypto landscape has created, to explore the inadequacy of the existing juristic paradigms and frameworks, to propose a contemporary *Fiqh* framework to address the issues of cryptocurrencies, and to validate its applicability, although these were the objectives, the ultimate purpose of the thesis was to address the stakeholders for such framework. Besides the general Muslims and academic researchers, the main stakeholders for this study are the jurists, standard-setting bodies like AAOIFI and IIFA, regulatory bodies, and policymakers at the institutional and governmental levels. The recommendations for academic researchers have already been outlined in subsection 6.3.2. 'Future Research'. The following are the recommendations for the jurists, institutions, regulatory bodies, and policymakers.

6.4.1. Recommendations for Jurists

- It has been identified that the reports and published information provided by authorities, including central banks, were not absent from the biases of governments and therefore were misleading to the judgements by which many jurists have based their rulings. Jurists need to have a more independent and informed observation of the topic. The study's proposed framework can help achieve this aspect.
- The study identified that many of the rulings given by jurists have conflated risks with *Gharar*. This directly contradicts with the *Fiqh* viewpoint that risk forms an entitlement for earning and therefore risky financial endeavors do not necessarily have to be forbidden. A more careful judgement on this aspect can be achieved by segregating the *Fiqh* view from the *Maqāṣidi* view.
- This study's models and systematic delineation of the technology can help demystify the complexities of the concept and make a ground for jurists from which judgements can be based.
- The study reveals that many jurists have put extensive emphasis on issues like infringing the state's right for minting and like the consideration of cryptocurrencies as money or not. These were rulings by early scholars based on public interest. It is safe to say that such rulings can change, especially with the number of innovations that haven't existed in those ancient times. There

are quite much more important issues that need to be looked at as delineated by the proposed framework.

6.4.2. Recommendations for Institutions

- The study reveals that Islamic standard-setting bodies, such as AAOIFI, have not yet incorporated clauses on the topic and types of cryptocurrencies. Such addition will help identify shortcomings and issues from a *Sharī'ah* point of view. The proposed framework and models can help identify and classify those types.
- There is a plethora of technical and economic academic writings about cryptocurrencies supported by western universities. However, academic institutions and universities have not taken serious steps to further progress the research in cryptocurrencies from the *Sharī'ah* perspective. This is partly due to the negative stance taken by governments, and partly due to the complexity of approaching it. The proposed framework and models can act as a foundation for future research with huge potential to build a common understanding from which to start with.
- There is a plethora of crypto assets, more than 20 thousand in existence today. The efforts of jurists will definitely not be enough to handle this large number of cryptos, especially that the study has identified a real requirement for a multidisciplinary team. The dissections of the proposed framework need to be sponsored and institutionalized with prospects to provide periodical reports of these cryptocurrencies.
- Based on the above point, it becomes inevitable and crucial for institutions to establish effective channels of communication and collaboration with *Sharī'ah* scholars. Institutions can benefit from incorporating the proposed framework as a tool for enhancing *Sharī'ah* scholars' comprehension of cryptocurrencies and the dynamics of the associated market.

6.4.3. Recommendations for Regulatory Bodies

- This thesis extracted huge concerns on the various scam schemes that easily spread in the space of Web3 and the crypto world. Regulating the virtual world was a common theme among the interviewed experts. The proposed framework consists of six main processes including the scrutiny of the project and its

services, the scrutiny of the issuer, and a comprehensive risk analysis. Such implementation can have profound effect in reducing the number of scams and their victims.

- The valuable insights revealed on the regulatory gaps of the crypto and virtual landscape can act as a foundation for informed regulations. Integrating the proposed framework into the regulatory guidelines can actively enhance the regulatory oversight and provide a systematic approach to regulating the cryptocurrency industry.

6.4.4. Recommendations for Policy-Makers

- Institutionalizing the proposed framework requires recognition and the realization of effective risk management. Endorsing and promoting the proposed framework can contribute to the development of a standardized approach that aligns with Sharia compliance and addresses existing gaps in juristic frameworks.
- The proposed framework can only be as good as the environment where it is setup. The collaboration with various regulatory bodies and other entities is crucial. Policymakers can play a pivotal role in supporting the implementation of the envisaged framework in a nurturing environment. This includes providing regulatory support, incentivizing compliance, and fostering an environment conducive to the adoption of standardized practices within the cryptocurrency sector.
- Considering the framework's potential to serve as the foundation for a rating agency, policymakers should explore the feasibility of integrating a rating system for cryptocurrencies. This could involve collaborating with relevant stakeholders to establish a mechanism similar to established financial rating agencies, which provide transparent ratings and reports for public consumption.

It has been accomplished with the guidance and support of **Allah**.

REFERENCES

A Guide to NFT Rarity. (2022). Binance Blog. https://bit.ly/49pDZla

Abdelhamid, A. S., & Ahmad, I. M. (2019). Athar al-'Umulāt al-Iftirāḍiyyah fi al-Siyāsah al-Naqdiyyah li al-Bunūk al-Markaziyyah. *The 15th International Conference of the College of Sharia and Islamic Studies at the University of Sharjah on "Virtual Currencies under Evaluation,"* 777–792.

Abdullah, A., Ng, A., Mahfudz, A. A., Pramanik, A. H., Ghani, G. M., Furqani, H., Saba, I., Zulkifli, I., Ahmed, K. T., Rahman, M. P., Obaidullah, M., Omar, M. A., Arshad, M. N. M., Barom, M. N., Zainal, M.-P., Kahf, M., Abojeib, M., Zarka, M. A., Khan, M. F., … Hasan, Z. (2018). Money and Monetary Policy. In M. Abojeib, M. A. Haneef, & M. O. Mohammed (Eds.), *Islamic Economics: Principles & Analysis* (2018th ed., pp. 513–568). International Shari'ah Research Academy for Islamic Finance (ISRA).

About | Consensys/Mythril. (n.d.). GitHub. Retrieved December 31, 2023, from https://github.com/Consensys/mythril

About Polkadot, a Platform for Web3. (n.d.). Polkadot. Retrieved December 31, 2023, from https://polkadot.network/about/

Abu-Bakar, M. M. (2017). Shariah Analysis of Bitcoin, Cryptocurrency, and Blockchain. *Blossom Labs*, *1*, 21.

Abu Ain, M. S. (2019). Al-Ḍawābiṭ al-Shar'iyyah li al-'Umulāt al-Iftirāḍiyyah. *The 15th International Conference of the College of Sharia and Islamic Studies at the University of Sharjah on "Virtual Currencies under Evaluation,"* 281–298.

Abū Ghuddah, A. al-S. (2018). al-Nuqūd al-Raqmiyyah al-Ru'yah al-Shar'iyyah wal-'āthār al-Iqtiṣādiyyah. *Fourth Doha Islamic Finance Conference*, 11–25.

Abu Husein, O. A. (2019). Al-Ḥukm al-Shar'ī li al-Ta'āmul bi al-'Umulāt al-Iftirāḍiyyah. *The 15th International Conference of the College of Sharia and Islamic Studies at the University of Sharjah on "Virtual Currencies under Evaluation,"* 107–134.

Abu Layl, M. M. (2019). Ḥukm Iṣdār al-'umulāt al-Raqamiyyah min Manẓūr al-

Siyāsah al-Shar'iyyah. *The 15th International Conference of the College of Sharia and Islamic Studies at the University of Sharjah on "Virtual Currencies under Evaluation,"* 135–156.

Afanah, H. A.-D. M. (2009). *Yas'alūnak 'an al-Mu'āmalāt al-Māliyyah al-Mu'āṣirah* (1st ed.). al-Maktabah al-Ilmiyyah and Dar al-Tayyib li al-Tiba'ah wa al-Nashr.

Al-'Adawī, A. A. M. (1994). *Ḥāshiyat al-'Adawī 'Alā Kifāyat al-Tālib al-Rabbānī* (Y. A.-S. M. Al-Biqai (Ed.); Vol. 2). Dar Al-Fikr.

Al-Aṣbaḥī, M. A. (1985). *al-Muwaṭṭa'* (M. F. Abdelbaqi (Ed.); Vol. 2). Dār "Iḥyā" al-Turāth al-'Arabī.

Al-Aṣbaḥī, M. A. (1994). *al-Mudawwanah al-Kubrā* (S. S. Al-Tanūkhī (Ed.); 1st ed., Vol. 3). Dar Al-Kotob Al-Ilmiyah.

Al-Bahūtī, M. Y. I. (1968). *Kashaf al-Qinā' "An Matn al-Iqnā"* (H. Msailhi (Ed.); Vol. 2). Maktabat al-Nasr al-Hadithah.

Al-Balādhurī, A. Y. J. D. (1988). *Futūḥ al-Buldān*. Dar wa Maktabat al-Hilal.

Al-Bukhārī, M. I. (1993). *Ṣaḥīḥ al-Bukhārī* (M. D. Albugha (Ed.); 5th ed., Vol. 2). Dār Ibn Kathīr, Dār al-Yamāmah.

Al-Dimashqī, J. 'Ali. (1900). *Kitāb al-Ishārah ilā Maḥāsin al-Tijārah*. Matba'at al-Mu'ayyad.

Al-Gharar.. Ma'nāhu wa Ḍawābiṭuhu. (2002). Islamweb.Net. https://bit.ly/49uf4Np

Al-Ḥajjāj, M. (1955). *Ṣaḥīḥ Muslim* (M. F. Abdelbaqi (Ed.); Vol. 3). Dār "Iḥyā" al-Turāth al-'Arabī.

Al-Ḥarīrī, M. 'Ali H. (1993). Awrāq al-Nuqūd wa Niṣāb al-Waraq al-Naqdī. *Majallat Al-Buḥūth Al-Islāmiyyah*, *39*(Aug to Dec), 239–343.

Al-Jaṣṣaṣ, A. 'Alī A. B. al-R. (1994). *Al-Fuṣūl fī al-Uṣūl* (Second, Vol. 4). Kuwaiti Ministry of Endowments.

Al-Jumayli, I. A. A. (2019). Iṣdār al-'Umulāt al-Iftirāḍiyyah bayna Ḍawābiṭ al-Shar' wa Mutaṭallabāt al-'Aṣr. *The 15th International Conference of the College of Sharia and Islamic Studies at the University of Sharjah on "Virtual Currencies under Evaluation,"* 85–106.

Al-Jumayli, O. A. A. (2019). Al-'Umulāt al-Iftirāḍiyyah Wāqi'uhā wa Takayyufuhā

al-Fiqhī wa Ḥukmuhā al-Shar'ī. *The 15th International Conference of the College of Sharia and Islamic Studies at the University of Sharjah on "Virtual Currencies under Evaluation,"* 173–192.

Al-Maknouzi, M. A.-H. (2019). Ṣu'ūbat Taḥdīd al-Ṭabī'ah al-Qānūniyyah li al-'Umulāt al-Iftirāḍiyyah: Dirāsah "alā Ḍaw" Mawqif al-Musharri'ayn al-Faransī wa al-'Urūbbī. *The 15th International Conference of the College of Sharia and Islamic Studies at the University of Sharjah on "Virtual Currencies under Evaluation,"* 531–550.

Al-Maqdisī, 'Abdullah Ahmed Qudāmah. (1997). *Al-Mughnī* (A. A. Al-Turki (Ed.); Third, Vol. 6). Dār 'Ālam al-Kotob.

Al-Maqrīzī, T. al-D. A. bin 'Abd al-Q. (1609). *Shudhūr al-'Uqūd fī dhikr al-Nuqūd*. Maktabat al-Riyād.

Al-Mosleh, K. A. (n.d.). *Al-Taḍakhum al-Naqdī fī al-Fiqh al-Islāmī*. www.almosleh.com.

Al-Nawawī, Y. S. (1991). *Rawḍat al-Ṭālibīn wa 'Umdat al-Muftīn* (Z. Al-Shaweesh (Ed.); Third, Vol. 3). al-Maktab al-Islāmī.

Al-Nawawī, Y. S. (2003). *Rawḍat al-Ṭālibīn* (A. A. AbdelMawjūd & A. M. Mu'awwad (Eds.); Special, Vol. 2). Dār 'Ālam al-Kotob.

Al-Qaradawi, Y. (1973). *Fiqh al-Zakāh* (2nd ed., Vol. 1). Muassat al-Risalah.

Al-Qurṭubī, M. A. al-A. (1964a). *Al-Jāmi' li Aḥkām al-Qur'ān* (A. Al Bardouni & I. Atfeesh (Eds.); 2nd ed., Vol. 9). Dār al-Kotob al-Miṣriyyah.

Al-Qurṭubī, M. A. al-A. (1964b). *Al-Jāmi' li Aḥkām al-Qur'ān* (A. Al Bardouni & I. Atfeesh (Eds.); 2nd ed., Vol. 4). Dār al-Kotob al-Miṣriyyah.

Al-Samirrai, A. S. M. (2019). Al-'Umulāt al-Iftirāḍiyyah-Ḍawābiṭ wa Ma'āyīr Shar'iyyah. *The 15th International Conference of the College of Sharia and Islamic Studies at the University of Sharjah on "Virtual Currencies under Evaluation,"* 299–318.

Al-Sarakhsī, M. A. (1989). *Al-Mabsūṭ* (Vol. 12). Dar Al-Ma'rifah.

Al-Shafi'ī, M. I. (1990). *al-Um* (Second, Vol. 3). Dar Al-Fikr.

Al-Shaykh, G. M. (2019). al-Ta'ṣīl al-Fiqhī li al-'Umulāt al-Raqamiyyah - al-Bitcoin

Namūdhajan. *The 15th International Conference of the College of Sharia and Islamic Studies at the University of Sharjah on "Virtual Currencies under Evaluation,"* 15–50.

Al-Shummari, A. R. (2019). Al-T'ṣīl al-Fiqhī li al-'Umulāt al-Iftirāḍiyyah. *The 15th International Conference of the College of Sharia and Islamic Studies at the University of Sharjah on "Virtual Currencies under Evaluation,"* 51–84.

Al-Ṭabarī, M. J. Y. K. G. (2001a). *Tafsīr al-Ṭabarī - Jāmi' al-Bayān 'an Ta'wīl 'Āy al-Qur'ān* (A. A. Al-Turki (Ed.); 1st ed., Vol. 13). Dār Hajr li al-Ṭibā'ah wa al-Nashr wa al-Tawzī' wa al-I'lān.

Al-Ṭabarī, M. J. Y. K. G. (2001b). *Tafsīr al-Ṭabarī - Jāmi' al-Bayān 'an Ta'wīl 'Āy al-Qur'ān* (A. A. Al-Turki (Ed.); 1st ed., Vol. 15). Dār Hajr li al-Ṭibā'ah wa al-Nashr wa al-Tawzī' wa al-I'lān.

Al-Yahya, B. A. A.-A. (2019). al-'Umulāt al-Iftirāḍiyyah Ḥaqīqatuhā wa Aḥkāmuhā al-Fiqhiyyah. *The 15th International Conference of the College of Sharia and Islamic Studies at the University of Sharjah on "Virtual Currencies under Evaluation,"* 221–264.

Al-Zarqa, A. M. (1989). *Sharḥ al-Qawā'id al-Fiqhiyyah* (2nd ed.). Dār al-Qalam.

All Cryptocurrencies. (2023). CoinMarketCap. https://coinmarketcap.com/all/views/all/

Ammous, S. (2018). *The Bitcoin Standard: The Decentralized Alternative to Central Banking*. Wiley.

Antonopoulos, A. M. (2014). *Mastering Bitcoin: Unlocking Digital Crypto-currencies* (M. Loukides & A. MacDonald (Eds.); First). O'Reilly Media.

ATO. (n.d.). *Crypto Asset Transactions*. Australian Taxation Office. Retrieved April 23, 2023, from https://www.ato.gov.au/individuals/investments-and-assets/crypto-asset-investments/transactions---acquiring-and-disposing-of-crypto-assets/crypto-asset-transactions/

Bakr, A. (2023). Developing a Cryptocurrency Susceptibility Test: Mathematical Modeling and Benchmarking. *Research Square*. https://doi.org/10.21203/rs.3.rs-3013756/v1

Banknotes: a short history. (n.d.). The Guardian. Retrieved April 16, 2022, from https://bit.ly/3HSyEXQ

Bitcoin (BTC): A Peer-to-Peer Electronic Cash System. (2020). Binance Research. https://research.binance.com/en/projects/bitcoin

Blockchain Size (MB). (2023). Blockchain.Com. https://bit.ly/3wf1rDB

Boddy, C. R. (2016). Sample size for qualitative research. *Qualitative Market Research: An International Journal*, *19*(4), 426–432. https://doi.org/10.2307/40269124

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research perspectives and challenges for bitcoin and cryptocurrencies. *2015 IEEE Symposium on Security and Privacy*, *2015-July*, 104–121. https://doi.org/10.1109/SP.2015.14

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/https://doi.org/10.1191/1478088706qp063oa

Bu Abdaly, A., & Saeed, H. A. (2019). Al-'Umulāt al-Iftirāḍiyyah: al-Furaṣ wa al-Taḥaddiyāt, Dirāsah Ḥālah Ṣadmah Nātijah 'an Istikhdām al-'Umlah al-Iftirāḍiyyah 'alā al-Iqtiṣād al-Jazā'rī. *The 15th International Conference of the College of Sharia and Islamic Studies at the University of Sharjah on "Virtual Currencies under Evaluation,"* 793–818.

Busch, S. (2023). *Smart Contract Security*. Ethereum.Org. https://ethereum.org/en/developers/docs/smart-contracts/security/

Canada Revenue Agency. (n.d.). *Guide for Cryptocurrency Users and Tax Professionals*. Canada Revenue Agency. Retrieved April 23, 2023, from https://www.canada.ca/en/revenue-agency/programs/about-canada-revenue-agency-cra/compliance/digital-currency/cryptocurrency-guide.html

Cardano Roadmap. (n.d.). Cardano. Retrieved January 1, 2024, from https://roadmap.cardano.org/en/

Chang, C.-C., & Wang, Y.-H. (2021). Using Phenomenological Methodology with Thematic Analysis to Examine and Reflect on Commonalities of Instructors' Experiences in MOOCs. *Education Sciences*, *11*(5).

https://doi.org/10.3390/educsci11050203

Closing Statement of Digital Crypto-Currencies Symposium. (2021). *Digital Crypto-Currencies Symposium*.

Conway, L. (2023). *Cardano (ADA): What It Is, How It Differs From Bitcoin*. Investopedia. https://bit.ly/48bODej

Creswell, J. W. (2009). *Research design qualitative, quantitative, and mixed methods approaches* (Third). Sage Publications, Inc.

Creswell, J. W. (2014). *Research Design Qualitative, Quantitative, and Mixed Methods Approaches* (V. Knight, B. Bauhaus, M. Markanich, & A. Hutchinson (Eds.); Fourth). Sage Publications, Inc.

CryptoSlate. (2023). CryptoSlate. https://cryptoslate.com/cryptos/proof-of-work/

Daghi, A. M. A.-Q. (2019). al-Maṣārif al-Iliktrūniyyah wal-Raqmiyyah: ’Āthāruhā, wa Makhāṭiruhā al-Shar’iyyah wa Ghayruhā. *Fifth Doha Islamic Finance Conference*, 27–69.

Dahshan, A. I. (2019). Al-’Umulāt al-Iftirāḍiyyah Ishkāliyyātuhā wa ’Āthāruhā ’alā al-Iqtiṣād al-Maḥallī wa al-’Ālamī. *The 15th International Conference of the College of Sharia and Islamic Studies at the University of Sharjah on “Virtual Currencies under Evaluation,”* 819–848.

DCI. (2020). *51% Attacks*. MIT Media Lab Digital Currency Initiative. https://dci.mit.edu/51-attacks

Deloitte. (2022). *Merchants getting ready for crypto: Merchant Adoption of Digital Currency Payments Survey*.

DeVon, C. (2022). *Nearly 75% of retailers plan to accept cryptocurrency payments within the next 2 years*. CNBC. https://cnb.cx/3HSy1gW

Dow, S., Johnsen, G., & Montagnoli, A. (2015). A Critique of Full Reserve Banking. *Sheffield Economic Research Paper Series*, *2015008*, 1–23.

El Amri, M. C., Mohammed, M. O., & Bakr, A. M. (2021). Enhancing Financial Inclusion Using FinTech-Based Payment System. In M. M. Billah (Ed.), *Islamic Fintech* (1st ed., pp. 505–542). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-45827-0_11

El Islamy, H. (2021). The Challenges of Cryptocurrencies and the Shariah Paradigm. In M. M. Billah (Ed.), *Islamic Fintech* (1st ed., pp. 755–794). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-45827-0_22

Etzrodt, C. (2018). Modern Sovereign Money-Part I: The Moral Hazard of Fractional Reserve Banking. *Open Journal of Social Sciences*, *6*(09), 101–115. https://doi.org/10.4236/jss.2018.69007

FinCEN. (2013). *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*.

Graneheim, U. H., Lindgren, B.-M., & Lundman, B. (2017). Methodological challenges in qualitative content analysis: A discussion paper. *Nurse Education Today*, *56*(June), 29–34. https://doi.org/10.1016/j.nedt.2017.06.002

Guest, G., MacQueen, K. M., & Namey, E. E. (2012). *Applied Thematic Analysis*. Sage Publications, Inc. https://doi.org/10.4135/9781483384436

Härdle, W. K., Harvey, C. R., & Reule, R. C. G. (2020). International Research Training Group 1792 Understanding Cryptocurrencies Understanding Cryptocurrencies. *Journal of Financial Econometrics*, *18*(2), 181–208.

Hayes, A. (2022). *What Happens to Bitcoin After All 21 Million Are Mined?* Investopedia. https://bit.ly/3HWhEjw

Hicks, C. (2022). *Different Types of Cryptocurrencies* (F. Powell (Ed.)). Forbes Advisor. https://bit.ly/3uE2vjM

Hinman, W. (2018). *Digital Asset Transactions: When Howey Met Gary (Plastic)*. U.S. Securities and Exchange Commission. https://bit.ly/48cyllm

Home | Tezos. (n.d.). Tezos. Retrieved December 31, 2023, from https://tezos.com/

How to Create an NFT. (2023). Binance Academy. https://bit.ly/3uwb0h2

How to Earn Rewards On Your Crypto Holdings. (2022). Binance Blog. https://bit.ly/3SCiLK8

HSB Survey Finds One-Third of Small Businesses Accept Cryptocurrency. (2020). Business Wire. https://bwnews.pr/3SBtowR

Ḥukm al-Ta'āmul bi al-Forex al-Islāmī! (2009). Islam Question & Answer. https://bit.ly/3OIGCXt

Ibn Mājah, M. Y. (n.d.). *Sunan Ibn Mājah* (M. F. Abdelbaqi (Ed.); Vol. 2). Dār Iḥyā' al-Kotob al-'Arabiyyah.

Ibn Qayyim al-Jawziyyah, M. (1991). *I'lām al-Muwaqqi'īn 'an Rab al-'Ālamīn* (M. A. Ibrahim (Ed.); 1st ed., Vol. 2). Dar al-Kutub al-'Ilmiyyah.

Ibn Taymiyyah, A. 'Abd al-Ḥalīm. (2004a). *Majmū' al-Fatāwā* (A. R. M. Qasim (Ed.); Vol. 19). King Fahd Glorious Qur'ān Printing Complex.

Ibn Taymiyyah, A. 'Abd al-Ḥalīm. (2004b). *Majmū' al-Fatāwā* (A. R. M. Qasim (Ed.); Vol. 29). King Fahd Glorious Qur'ān Printing Complex.

Ibn Taymiyyah, A. 'Abd al-Ḥalīm. (2004c). *Majmū' al-Fatāwā* (A. R. M. Qasim (Ed.); Vol. 28). King Fahd Glorious Qur'ān Printing Complex.

Ifegwu, O. (n.d.). *Gas*. Binance Academy. Retrieved January 12, 2023, from https://academy.binance.com/en/glossary/gas

Illien, N., Wilson, T., & Knauth, D. (2023). *FTX opposes new bankruptcy investigation as it probes Bankman-Fried connections*. REUTERS. https://reut.rs/497WhYI

IRS. (2014). *Notice 2014-21*.

Jackson, A., & Dyson, B. (2012). *Modernizing Money: Why Our Monetary System is Broken and How it Can be Fixed* (1st ed.). Positive Money.

Jain, A. (2022). *Who owns the most Cardano? Top 10% of ADA whales control bulk of circulating tokens*. Capital. https://bit.ly/3OFgWef

Kahf, M. (2014). *Notes on Islamic Economics: Theories and Institutions* (Vol. 1). Monzer Kahf.

Kay, J. (2009). *Narrow Banking: The Reform of Banking Regulation* (Issue 88). Centre for the Study of Financial Innovation (CSFI).

Kotlikoff, L. J., & Goodman, J. C. (2009). Solving Our Nation's Financial Crisis with Limited Purpose Banking. *Boston University*.

Kroll, J. A., Davey, I. C., & Felten, E. W. (2013). The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. *The Twelfth Workshop on the Economics of Information Security (WEIS 2013)*, *Weis*, 1–21.

Leirvik, T. (2022). Cryptocurrency returns and the volatility of liquidity. *Finance Research Letters*, *44*, 102031. https://doi.org/10.1016/J.FRL.2021.102031

Longhurst, R. (2016). Semi-structured interviews and focus groups. In *Key methods in geography* (Third, pp. 143–156). Sage.

Lovejoy, J. (2020). *Reorgs on Bitcoin Gold: Counterattacks in the Wild*. MIT Media Lab Digital Currency Initiative. https://bit.ly/3Sw9G5L

Mabout, A. (2019). Al-'Āthār al-Shar'iyyah li Tadāwul al-Nuqūd al-Iftirāḍiyyah. *The 15th International Conference of the College of Sharia and Islamic Studies at the University of Sharjah on "Virtual Currencies under Evaluation,"* 371–400.

Maghdeed, F. (2020a). *From Digital Currency to Cryptocurrency: What are the main differences between them*. Medium.Com. https://bit.ly/499k62h

Maghdeed, F. (2020b). *The Transformation of the Traditional Equity Market to a Blockchain Securitized Asset Market*. Medium.Com. https://bit.ly/4bAPLuY

Majaski, C. (2022). *Cryptocurrency Security Token: Definition, Forms, Investing In*. Investopedia. https://bit.ly/4bv108l

Maneei, A. S. (1984). *Al-Warāq al-Naqdī* (2nd ed.). Author.

Mashal, A. B. (2022). Nawāzil al-Teknolūjia al-Muta'alliqah bi al-Mu'āmalāt al-Māliyyah. *AMJA 18th Annual Imams' Conference*, 1–37.

Mcleay, M., Radia, A., & Thomas, R. (2014). Money Creation in the Modern Economy. *Bank of England Quarterly Bulletin 2014 Q1*, 14–27.

McLellan, E., MaCqueen, K. M., & Neidig, J. L. (2003). Beyond the Qualitative Interview: Data Preparation and Transcription. *Field Methods*, *15*(1), 63–84. https://doi.org/10.1177/1525822X02239573

Merkel, S. (2020). *The Macro Implications of Narrow Banking: Financial Stability versus Growth*.

Michael, K., & Jaromir, B. (2012). *The Chicago Plan Revisited* (12/202). International Monetary Fund.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook* (Second). Sage Publications, Inc.

Mishkin, F. S. (2022). What is Money? In *The Economics of Money, Banking, and Financial Markets* (13th ed., pp. 97–110). Pearson Education Limited.

Monett, D., & Navarro-Barrientos, J. E. (2016). Simulating the Fractional Reserve

Banking using Agent-based Modelling with NetLogo. *2016 Federated Conference on Computer Science and Information Systems (FedCSIS)*, *8*, 1467–1470. https://doi.org/10.15439/2016F373

Morris, C. (2021). *Bank of England governor: Cryptocurrency investors should be prepared to lose all their money*. Fortune. https://t.ly/IEg1U

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin.Org*, 1–9. https://doi.org/10.2139/ssrn.3977007

Neuman, W. L. (2014). *Social Research Methods: Qualitative and Quantitative Approaches* (Seventh). Pearson Education Limited.

Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities. *IEEE Access*, *7*, 85727–85745. https://doi.org/10.1109/ACCESS.2019.2925010

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*, *16*(1), 1–13. https://doi.org/10.1177/1609406917733847

Oliver, D. G., Serovich, J. M., & Mason, T. L. (2005). Constraints and Opportunties with Interview Transcription: Towards Reflection in Qualitative Research. *Soc Forces*, *84*(2), 1273–1289. https://doi.org/10.1353/sof.2006.0023

Open, Permissioned Distributed Platform: Capitalize on the New Digital Economy—Transact Openly and Securely, at Scale and Across Networks. (n.d.). R3. Retrieved December 31, 2023, from https://r3.com/products/corda/

Oudah, M. R. R. (2019). Waẓā'if wa Shurūṭ al-Nuqūd wa Madā Taḥaqquqihā fi al-'Umulāt al-Iftirāḍiyyah - Dirāsah Fiqhiyyah. *The 15th International Conference of the College of Sharia and Islamic Studies at the University of Sharjah on "Virtual Currencies under Evaluation,"* 193–220.

Owleksiy. (2021). *SMTChecker: (Almost) Practical Superpower*. Medium. https://t.ly/2yfcN

Pasha, A. C. (n.d.). al-Kitāb al-Awwal fī al-Buyū'. In N. Hawawini (Ed.), *Kitāb Majallat al-Aḥkām al-'Adliyyah*. Kar Khaneh Tijaret Kotob.

Samai, M. (2019). Al-Ta'līl bi al-Thamaniyyah wa Atharuhu fī Aḥkām al-'Umulāt al-Iftirāḍiyyah. *The 15th International Conference of the College of Sharia and Islamic Studies at the University of Sharjah on "Virtual Currencies under Evaluation,"* 157–172.

Sandelowski, M. (1998). Focus on Qualitative Methods: The Call to Experts in Qualitative Research. *Research in Nursing and Health*, *21*(5), 467–471. https://doi.org/10.1002/(sici)1098-240x(199810)21:5<467::aid-nur9>3.0.co;2-l

Savla, R. (2023a). *Bitcoin in Real Life: Wallet Mechanics, Mining, & More - Recipe for Mining*. CS198.1x: Bitcoin and Cryptocurrencies; edX - BerkeleyX. https://t.ly/3aS22

Savla, R. (2023b). *Bitcoin Mechanics & Optimizations: A Technical Overview - Summary*. CS198.1x: Bitcoin and Cryptocurrencies; edX - BerkeleyX. https://rb.gy/xn44we

Savla, R. (2023c). *Bitcoin Protocol & Consensus: A High Level Overview - Summary*. CS198.1x: Bitcoin and Cryptocurrencies; edX - BerkeleyX. https://rb.gy/08ftf0

Savla, R. (2023d). *Ethereum & Smart Contracts: Enabling a Decentralized Future - Summary*. CS198.1x: Bitcoin and Cryptocurrencies; edX - BerkeleyX. https://rb.gy/w3elh2

Security Token. (n.d.). CoinMarketCap. Retrieved January 19, 2023, from https://bit.ly/4bxmrWg

Selcuk, M., & Kaya, S. (2021). A Critical Analysis of Cryptocurrencies from an Islamic Jurisprudence Perspective. *Turkish Journal of Islamic Economics*, *8*(1), 137–152. https://doi.org/10.26414/a130

Smiran, M. A. S. (2019). Ḍawābiṭ 'Amaliyyat Iṣdār al-Nuqūd wa al-'Umulāt al-Raqamiyyah "Dirāsah Taḥlīliyyah Naqdiyyah." *The 15th International Conference of the College of Sharia and Islamic Studies at the University of Sharjah on "Virtual Currencies under Evaluation,"* 265–280.

Suliyanti, W. N., & Sari, R. F. (2019). Evaluation of Hash Rate-based Double-Spending based on Proof-of-Work Blockchain. *2019 International Conference on Information and Communication Technology Convergence (ICTC)*, 169–174. https://doi.org/10.1109/ICTC46691.2019.8939684

Sun, H. E. J. (n.d.). *About | TRON*. TRON. Retrieved December 31, 2023, from https://tron.network/about?lng=en

Ta'rīf wa Ma'nā Wariq fi Qāmūs al-Kul - Qāmūs 'Arabī 'Arabī. (n.d.). In *Al-Wasīṭ*. Almaany.com.

The Investopedia Team. (2022). *How Can I Use Market Capitalization to Evaluate a Stock?* Investopedia. https://rb.gy/jir02f

Wallets. (n.d.). Bitcoin Developer. Retrieved February 10, 2023, from https://bit.ly/49rZKRw

What's Crypto Market Cap? Why Does It Matter? (2022). Worldcoin. https://bit.ly/3utxCi5

What Is a Stablecoin? (2023). Binance Academy. https://rb.gy/3ovmk2

What Is a Utility Token? (2022). Worldcoin. https://bit.ly/3P1vfKD

What is Block Time? (2022). Bitstamp.Net. https://bit.ly/3UvTZ0Y

What is market cap? (2020). Coinbase. https://bit.ly/486VAO1

Yang, M. Y., Wu, Z. G., & Wu, X. (2022). An empirical study of risk diffusion in the cryptocurrency market based on the network analysis. *Finance Research Letters*, *50*(July), 103180. https://doi.org/10.1016/j.frl.2022.103180

APPENDICES

APPENDIX A – HASHRATES

Hashrate serves as a crucial metric representing the computational power available within a PoW blockchain system. Specifically, network hashrate signifies the cumulative number of hashes computed per second by all participating mining nodes. It is worth noting that any endeavor to modify the most recent block(s), commonly known as reorganizations (reorgs) within the technological realm, necessitates the possession of a majority of the mining nodes' computational power. In other words, an individual would need to acquire 51 percent of the network's hashrate, an attempt that typically involves substantial costs. Traditionally, it has been widely assumed that due to these high costs, potential attackers are effectively deterred.

However, the emergence of hashrate rental markets has significantly altered this landscape. These markets provide accessible access to requested hashrate capacities at considerably affordable costs, eliminating the need for substantial investments in expensive machinery, server racks, and physical space. As a result, the feasibility and practicality of executing 51% majority attacks have become more pronounced.

> *It is now commonly believed that low hashrate coins, coins that are not the largest in their proof-of-work algorithm class, and coins for which there is a liquid hashrate rental market are all susceptible to cheap 51% attacks and are insecure* (Lovejoy, 2020).

Indeed, recent reports from the MIT Digital Currency Initiative (DCI, 2020) have detected more than 40 reorganizations extending to six or more blocks deep, impacting a range of cryptocurrencies such as Bitcoin Gold (BTG), Hanacoin (HANA), Vertcoin (VTC), Verge (XVG), Expanse (EXP), and Litecoin Cash (LCC). The DCI's findings indicate that certain reorgs even encompassed instances of double-spending and extended hundreds of blocks deep. Additionally, there is compelling evidence suggesting the utilization of hashrate rental markets in executing a subset of these attacks. Suliyanti & Sari (2019) corroborate these concerns, demonstrating through simulation that an increase in an attacker's hashrate directly corresponds to a rise in the number of double-spending attacks.

APPENDIX B – QUESTIONNAIRE

Main Themes	Interview Questions
Technical Confusion and Contention about Cryptocurrencies	Q1. Why is there confusion among the researchers in differentiating between the types of cryptos and Bitcoin in terms of concept, limitation, and risk?
Adequacy of the Existing *Fiqh* Framework	Q2. Why is the current *Fiqh* framework (if exists) inadequate to address contemporary issues related to cryptocurrencies?
Validity of the Proposed Framework	Q3. With reference to the proposed framework/model, to what extent do you think it is viable and acceptable? Q4. With reference to 'Evaluate Maturity' process (Pg. Hata! Yer işareti tanımlanmamış.**)** of the proposed framework, why is it important to understand the stage of development (infancy, gaining momentum, advanced) of a cryptocurrency from a *Fiqh* perspective? Q5. With reference to 'Evaluate Maturity' process (Pg. Hata! Yer işareti tanımlanmamış.**)** of the proposed framework, what is your opinion about the indicators (s-value, market cap, merchant acceptance trends, public audits, peg stability etc.…) used in determining the stage of development of a crypto? Q6. With reference to 'Evaluate Issuing Entity' process (Pg. **Hata! Yer işareti tanımlanmamış.**) of the proposed framework, do you think the variables (truthful, trustworthy, and experienced body with proven-track record of due diligence and transparency) used to evaluate the issuing entity of a crypto are sufficient from a *Fiqh*i view? Q7. With reference to 'Evaluate Risk Severity' process (Pg. 99) of the proposed framework, why do you think integrating risk management methods and tools into the study of jurisprudential

	issues related to cryptocurrencies adds objectivity to the jurisprudential decisions and enhances a broader understanding of all aspects of the cryptocurrency system? Q8. With reference to **Hata! Başvuru kaynağı bulunamadı.**, do the interpretations of the impact and probability levels align with the *Fiqh* perspective? Why or why not? If not, how do you think they should be? Q9. With reference to 'Evaluate Risk Severity' process (Pg. 99) of the proposed framework, the evaluation of the risk severity of each issue will yield one of four results: low, medium, high, and very high. What is your opinion on considering issues with low and sometimes medium risks not leading to a violation of the Shariah rulings related to them? Q10. Refer to 'Evaluate Compliance to *Sharī'ah*' process (Pg. 102) of the proposed framework. Do you think that *Gharar* should be considered a reason for the impermissibility of cryptocurrencies only if all its 4 conditions are met? Q11. According to the methodology of the process 'Evaluate Compliance to *Sharī'ah*' (Pg. 102) in the proposed framework, the risk severity level of an issue will differ with different types of cryptos. What is your opinion about choosing a different severity level of an issue for different cryptos? Refer to the first three issues in **Hata! Başvuru kaynağı bulunamadı.** – **1.** Lack of regulations and regulatory bodies **2.** The extent to which authorities are concerned or non-supporting, and **3.** Lack of association with any financial institution – Do you agree that they can become less severe as the authorities become more indifferent or even embracing the crypto under study? Q12. According to the table in **Hata! Başvuru kaynağı bulunamadı.**, what is your opinion about the issues related to 'Trading Platform' and 'Wallet Management' and the extent of their compliance with the Shariah?
Challenges of Implementing	Q13. What are the challenges from *Fiqh* perspective to the relevant stakeholders [Shariah scholars, crypto investors, regulators, researchers, Islamic financial institutions, etc.] that might arise

the Proposed Framework	in implementing the proposed framework? What suggestions do you have to overcome those challenges?
Prospects and Significance of the Proposed Framework	Q14. What are the prospects and significance from *Fiqh* perspective of the proposed framework to the relevant stakeholders [Shariah scholars, crypto investors, regulators, researchers, Islamic financial institutions, etc.] if it is implemented?
Suggestions from Experts on the Proposed Framework	Kindly share your suggestions to improve the framework.

APPENDIX C – SAMPLE ISSUE REGISTER OUTPUTS

Table C.1: Issue Register 1 Sample – Color-Coded After Evaluating Bitcoin

Issue	Potential *Sharī'ah* Violations	Remarks
1. Lack of regulations and regulatory bodies (3 x 3 = **9**)	*Gharar*, Imbalance, Risk of deception	▪ **Theme**: Regulatory Concern ▪ Trading Platforms and Wallet Management providers are regulated in their own countries. ▪ Crypto-dependent
2. The extent to which authorities are concerned or non-supporting (3 x 2 = **6**)	Infringement upon the Sultan's right to issue money	▪ **Theme**: Regulatory Concern ▪ Can be flexible: - Non-state issuance is reprehensible - State is indifferent - State allows/uses it ▪ Crypto-dependent
3. Lack of association with any financial institution (1 x 5 = **5**)	*Gharar*	▪ **Theme**: Regulatory Concern ▪ Crypto-dependent
4. Stability and price fluctuations (3 x 3 = **9**)	Weakening of property and wealth Violation of "store of value"	▪ **Theme**: Financial consideration ▪ Crypto type-dependent ▪ Affected by endogenous factors: market forces (supply/demand), monetary policy ▪ Affected by exogenous factor: speculation
8. Not backed by any asset (1 x 5 = **5**)	*Gharar*	▪ **Theme**: Value concern ▪ Crypto type-dependent ▪ Fiat currency is not backed by any asset, yet has value
9. Lacking intrinsic value and are not legal tenders (1 x 5 = **5**)	*Gharar*	▪ **Theme**: Value concern ▪ Crypto type-dependent ▪ Value is derived from the network and market forces
10. Possibility of miner controlling more than 50% of the network / infanticide stage (3 x 1 = **3**)	*Gharar*	▪ **Theme**: Security concern (caused by technology) ▪ Network routing-related ▪ Several blocks deep, it becomes **improbable**
11. Short block times need more blocks to reach the desired level of security (1 x 1 = **1**)	*Gharar*	▪ **Theme**: Security concern ▪ Monetary policy-related ▪ The issue isn't that it's insecure, it's only that it requires more blocks to reach desired level of security.
14. Lack of proper randomization of the puzzle (1 x 1 = **1**)	Imbalance	▪ **Theme**: Operational Efficiency of Mining ▪ Mining-related

15. Mining pools/farms - influence in the hands of few (2 x 4 = **8**)	*Gharar*	▪ **Theme**: Security concern ▪ Mining-related (could lead to issue **10)**
16. Consequences of insufficient mining income (2 x 3 = **6**)	*Gharar*	▪ **Theme**: Security, Operational Efficiency of Mining ▪ Monetary-policy (could lead to issue **10** or **18)** ▪ This is a future anticipation that needs to be researched related to end of tokens supply
17. Racing attack causing double-spending (3 x 1 = **3**)	*Gharar* Loss of property and wealth	▪ **Theme**: Security concern ▪ Network routing-related ▪ Few blocks confirmation method makes it improbable
18. Rise of mining cartels capable of censoring transactions (3 x 1 = **3**)	Preservation of property is violated	▪ **Theme**: Operational Efficiency of Mining ▪ Mining-related
19. Lack of a clear process for changing transaction validation rules (2 x 3 = **6**)	*Gharar* Loss of property and wealth	▪ **Theme**: Security concern, Value concern ▪ Protocol development-related ▪ May lead to forks which might lead to loss of tokens ▪ Low probability for well-established and blockchains
22. Security of smart contracts	*Gharar*	▪ **Theme**: Security concern ▪ Crypto type-dependent
23. Application of NFT is not of value	Squander	▪ **Theme**: Value concern ▪ Crypto type-dependent
24. Inability of a stablecoin to maintain its peg	Weakening of property and wealth "Store of value" issue	▪ **Theme**: Financial consideration ▪ Monetary policy-related
25. The extent an issuer of a stablecoin releases full public audits	*Gharar*	▪ **Theme**: Financial consideration
26. The extent to which an issuer of a stablecoin can be trusted to have the reserves they claim	*Gharar*	▪ **Theme**: Value concern

Source: Author

Table C.2: Issue Register 2 Sample – Color-Coded After Evaluating Bitcoin

	Regulatory Concern	Financial Consideration	Security Concern	Value Concern	Mining Operational Efficiency
Mining Process			**15.** Mining pools and farms make the influence in the hands of few. (2 x 4 = **8**)		**14.** Lack of proper puzzle randomness (1 x 1 = **1**)
					18. Rise of cartels that can censor transactions (3 x 1 = **3**)
Monetary Policy		**24.** Inability of a stablecoin to maintain its peg	**11.** Short block times need more blocks to reach the desired security level. (1 x 1 = **1**)	**8.** Not backed by any asset (1 x 5 = **5**)	**16.** Implications of insufficient mining income (2 x 3 = **6**)
			16. Consequences of insufficient mining income (2 x 3 = **6**)	**9.** Lacking intrinsic value - not legal tender. (1 x 5 = **5**)	
Node Routing			**10.** Possibility of miner controlling > 50% of the network /infanticide stage (3 x 1 = **3**)		
			17. Racing attack causing double-spending.(3 x 1 = **3**)		
Overall Crypto System	**1.** Lack of regulations and regulatory bodies	**4.** Stability and price fluctuations (3 x 3 = **9**)	**22.** Security of smart contracts	**23.** Application of NFT is not of value	

	(3 x 3 = **9**)			
	2. The extent to which authorities are concerned or non-supporting. (3 x 2 = **6**)	**25.** The extent an issuer of a stablecoin releases full public audits		**26**. The extent to which an issuer of a stablecoin can be trusted to have the reserves they claim
	3. Lacks association with any financial institution (1 x 5 = **5**)			
Protocol Development			**19.** Lack of a clear process for changing transaction validation rules (3 x 2 = **6**)	**19.** Lack of a clear process for changing transaction validation rules (3 x 2 = **6**)

CURRICULUM VITAE

Name	:	Ayman M. BEKİROĞLU
Date of Birth	:	
Country of Citizenship/Residence	:	Palestinian / Istanbul, Turkey

ACADEMIC & PROFESSIONAL QUALIFICATIONS

PhD Candidate (Distinction)	Islamic Economics and Finance	Istanbul Sabahattin Zaim University (IZU) – Istanbul, Turkey	To Date
Master of Business Administration (Distinction)	Business Administration (Strategy)	University of Strathclyde – Glasgow, Scotland	2009
Bachelor of Art (Summa Cum Laude)	Mathematics	Southern New Hampshire University (SNHU) – US	2016
Bachelor of Science	Electrical Electronics Engineering	Bilkent University – Ankara / Turkey	2001

EMPLOYMENT

Director & Consultant	Al-Mal Consultancy Limited (ACL) – UK	- Developing Shari'ah compliant Investment models. - Researching Islamic benchmarking. - Researching developing artificial intelligence for Islamic green finance - Consulting and advisory role on FinTech-related products - Consulting and advisory role on training-related technology	Dec 2019 – Present
FinTech-Related Analyst	Abu Dhabi Investment Authority (ADIA) - UAE	- Overseeing reliability, availability, and full functionality of Investment FinTech products and software	Sep 2004 – Jan 2019

PUBLICATIONS & CONFERENCE PRESENTATIONS

Conference Presentations

1. Feasibility of Creating New Products from e-Waste – 12th ICIEF 2020
2. Artificial Intelligence and Islamic Green Finance – 7th IIMEFC 2021 & 13th ICIEF 2021

Publications

1. Mohammed, M. O., El Amri, M. C., & Bakr, A. (2021). SWOT analysis of benchmarking in the Islamic finance industry. In *Benchmarking Islamic Finance* (pp. 56-70). Routledge.
2. Bakr, A. (2021). Trading with National Currency: Is the Turkish Lira Stable?. *Journal of Contemporary Issues in Business and Government*, 27(1), 3459-3474.
3. Bakr, A., El Amri, M. C., & Mohammed, M. O. (2021). The Worldview of Islamic Ethical Wealth and Its Implications for SDGs: The Case of Waqf. *Islamic Wealth and the SDGs: Global Strategies for Socio-economic Impact*, 29.
4. Mohammed, M. O., El Amri, M. C., & Bakr, A. (2021). The Role of Islamic Ethical Wealth in Strategically and Technically Supporting 'No Poverty'-SDGs 1. *Islamic Wealth and the SDGs: Global Strategies for Socio-economic Impact*, 241.
5. El Amri, M., Mohammed, M., & Bakr, A. (2021). Enhancing Financial Inclusion Using FinTech-Based Payment System. In *Islamic FinTech* (pp. 191-207). Palgrave Macmillan, Cham.
6. Bakr, A., Mohammed, M., El Amri, M. (2022). Social Impact of COVID-19: a SWOT Analysis from the Islamic Perspective. (Forthcoming).
7. Bakr, A., El Amri, M. C., Mohammed, M. O., Yücel, E. (2022). The Challenges and Prospects of Adopting Best Methodologies in Teaching Islamic Finance. *Teaching and Research Methods for Islamic Economics and Finance* (pp. 152–163). Routledge.
8. Bakr, A. (2023). Developing a Cryptocurrency Susceptibility Test: Mathematical Modeling and Benchmarking. (Forthcoming) – in Electronic Commerce Research.
9. Bakr, A., El Amri, M. C., Mohammed, M. O., Kastaci, H., Erol, T. (2023). Proposing Circular Economy for Enhancing the e-Waste Recycling in Turkiye. (Forthcoming) – in Tujise.