# Applying Blockchain Technology to Financial Market Infrastructure

JI LIU

Supervisor: Shiping Chen and Dong Yuan

A thesis submitted in fulfilment of
the requirements for the degree of
Doctor of Philosophy

School of Electrical and Information Engineering
The University of Sydney

Australia

01 July 2023

# Thesis Statement of Originality

The work contained in the body of this thesis, except where otherwise acknowledged, is the result of my investigations.

This thesis has not been submitted for any other degree or purpose. I certify that the intellectual content of this thesis is the product of my work and that all the assistance received in preparing this thesis and sources have been acknowledged.

Ji Liu | 01 July 2023

# Author Attribution Statement

This thesis contains published material and material which is under review for publication. The mentioned material is highlighted as follows:

- Chapter 2 of this thesis is published at IET Blockchain.
- Chapter 3 of this thesis is published at Frontiers in Blockchain.
- Chapter 4 of this thesis is published at International Conference on Blockchain.
- Chapter 5 of this thesis is under review at Information Systems Frontiers.

I am the corresponding author of the above-published items except for the material in Chapter 4. I have been granted the corresponding author's permission to include this material in my thesis.

Ji Liu | 01 July 2023

As the supervisor for the candidature upon which this thesis is based, I can confirm that the authorship attribution statement above is correct.

Shiping Chen | 01 July 2023

# Abstract

The utilization of blockchain technology has gained widespread acceptance across various domains in recent years. Among them, blockchain integration in the financial sector is particularly noteworthy. Blockchain technology offers a range of features that can address various challenges in the financial industry, including decentralization, transparency, enhanced security, and tamper-proofing. Therefore, this thesis aims to investigate the issues that persist in academia and industry and address them through blockchain technology.

The research for this thesis was divided into three major stages. The first stage involved conducting an academic survey through a comprehensive literature review. The aim was to identify the pain points that academics have identified and to narrow down the problems that concern the academic community.

The second stage involved collecting requirements from industry experts. This helped to identify the real-world issues that currently exist in the financial industry. Based on these issues, the research moved on to the next stage.

The third stage involved an experimental study, further divided into two parts. Part 1 involved designing and developing a blockchain-based issuance and trading system for financial products. This system aimed to enhance participant trust, reduce costs, and increase efficiency. Part 2 involved the development of a risk monitoring system for blockchain-based financial products. This system aimed to assist participants in monitoring market risks, providing them with risk warning coefficients, and reducing the probability of systemic risks in the market.

The results of this thesis demonstrate that blockchain technology's feasibility and integration can positively impact financial markets from an experimental perspective. It can be helpful to adopt blockchain technology for financial and FinTech industries.

## Acknowledgements

First and foremost, I would like to extend my deepest gratitude to my academic supervisor, Professor Shiping Chen. Professor Chen allowed me to return to school and continue my studies. Despite any friction or misunderstandings that arose over the years, I sincerely appreciate all the help and guidance he provided me. As the saying goes in China, “A teacher for a day, a father for life.” I am forever grateful to him.

I would also like to extend my thanks to Dr Dong Yuan, my leading supervisor at the University of Sydney. He has been an incredibly responsible supervisor and has provided invaluable assistance throughout my research.

Lastly, I am eternally grateful to my parents and family. They have invested much time, money, and care into my student life. This doctorate is my gift to them, culminating in more than twenty years of being a student. Without their support and encouragement, I would not have had the courage or the opportunity to complete my PhD.

# Contents

# List of Figures

# List of Tables

CHAPTER 1

# Introduction

---

Currently, the financial market operates primarily within a centralised framework, relying on the support of financial institutions within this centralised system (Klagge & Martin, 2005). The centralisation of financial market infrastructure is considered as a means of maintaining financial stability. For instance, stock exchanges exhibit typical centralised characteristics, providing centralised matching services by pairing buyers and sellers together. This increases the efficiency of securities trading, reduces the cost of search and matchmaking, enables the transfer of capital between different times, regions, and industries, and ultimately facilitates the effective allocation of assets (Scholtens, 1992). As a securities exchange centre and clearing institution that provides settlement for securities transactions, it also establishes a centralised clearing method based on centralised securities transactions to ensure delivery efficiency, accuracy, and security after the transaction has been completed (Mehran & Stulz, 2007).

On the one hand, the centralisation of financial market infrastructure serves as an internal need of the market to improve efficiency, control risks, and reduce costs at the economic and financial levels (Chang et al., 2020). On the other hand, at the technical level, technological advancements have also significantly promoted the centralisation of financial market infrastructure (Walch, 2015). For example, payment and settlement methods have evolved from manual summarization to stock information exchange that can reach remote areas, then to telegraph technology, and finally to the widespread use of real-time settlement systems. The constant updating of computer technology can support large-scale real-time financial market transactions and more accurately assess transaction risks (Walch, 2015).

It is important to note that the centralised financial system has certain drawbacks. Firstly, market traders are subject to additional costs. When participating in market transactions relying on centralised financial infrastructure, traders need to pay commissions and other fees, which can be a significant transaction cost (Manaa et al., 2021). Secondly, centralisation brings about new efficiencies and risk issues. As a legally mandated financial market infrastructure, all data and records of financial transactions need to be kept by a single institution. This not only slows down transaction speed but also poses risks arising from the improper operation of the financial market infrastructure, which acts as a credit converter (Walch, 2015).

Additionally, financial products that rely on centralised exchanges tend to be less personalised. Financial products that rely on centralised transactions are often in a standardised form, making it challenging to meet some personalised financial needs (Mills et al., 2016). Finally, the accessibility of the centralised financial system is relatively weak (Blackwell & Kohl, 2018).

The integration of blockchain technology in the financial field has the potential to address the limitations of the centralised financial system. Blockchain is a distributed ledger technology that operates on a peer-to-peer network, allowing for the secure storage of simple, sequenced, and verifiable data (Troncia et al., 2019). The technology combines data blocks into a distributed data structure in a chain and uses cryptography to ensure data immutability (Zhu et al., 2018). This allows for a new and universal credit mechanism and means of value exchange.

The decentralised nature of blockchain technology means that financial transactions no longer have to rely on central processing nodes, enabling distributed recording, storage and updating of information (Niranjanamurthy et al., 2019). This also ensures the transaction security of both parties without the need for a centralised intermediary and can solve credit issues. Additionally, many traditional financial processes through intermediaries or brokers can be streamlined, potentially resulting in a zero-cost financial transaction environment (Tilooby, 2018).

Furthermore, blockchain applications in the financial field can blur traditional divisions of labour in the financial market while improving payment and transaction capabilities (Guo & Liang, 2016). Overall, blockchain technology has the potential to revolutionise the financial industry by solving the limitations of centralised systems and providing new opportunities for efficient, secure, and cost-effective financial transactions.

Nowadays, the boundaries between financial intermediaries, the financial market, financial service providers, and market participants are becoming more blurred (Hoffmann et al., 2021), thus promoting the intelligence and decentralisation of financial infrastructure to a certain extent. With blockchain technology's application in the financial market, blockchain's transformation ability in the payment and settlement field is the most obvious and is especially suitable for financial transactions where collaborators are untrustworthy, have conflicting interests or lack authoritative third-party intervention (Zhang et al., 2020). Therefore, in exploring blockchain applications, financial asset issuance and transactions, credit transfers, new financial risks, private equity transactions, and other non-standardised financial product transactions are key research areas for scholars and the industry.

In recent years, the boundaries between financial intermediaries, the financial market, financial service providers, and market participants have become increasingly blurred (Hoffmann et al., 2021), which has led to increased intelligence and decentralisation of financial infrastructure. The application of blockchain technology in the financial market has been particularly significant in the payment and settlement field, as it is particularly suitable for financial transactions where collaborators are untrustworthy, have conflicting interests, or lack authoritative third-party intervention (Zhang et al., 2020).

Therefore, fundamental research areas for scholars and industry experts in employing blockchain applications include financial asset issuance and transactions, credit transfers, new financial risks, private equity transactions, and other non-standardised financial product transactions. These areas can potentially revolutionise the financial industry by providing new and efficient ways to conduct transactions and manage risks.

## 1.1 Objectives

As a distributed ledger system, blockchain has unique characteristics such as decentralisation, tamper-proofing, and enhanced privacy, which can make the transaction of financial assets more confidential and increase participant confidence in a deal (Zhang et al., 2020). Additionally, the decentralised system prevents tampering with transaction data and market manipulation, effectively reducing systemic risks (Zheng et al., 2018).

This thesis focuses on the trading behaviour of financial assets in the financial market and embeds blockchain technology as a practical solution for infrastructure optimisation. On the one hand, by analysing existing relevant academic literature, we identify the issues faced by the financial market infrastructure by analysing the industry's actual pain points and using the theory of crypto economics as a logical starting point. On the other hand, by constructing a blockchain-based financial assets issuance system and risk monitoring system, this thesis uses the characteristics of blockchain technology as a solution to financial market issues, contributing to the application of blockchain in financial market scenarios. Furthermore, in terms of risk monitoring, the interaction of regulators is included to ensure that they can respond quickly in the event of market risks breaking out.

In summary, this thesis aims to utilise blockchain technology to improve trust in the financial market. The proposed framework aims to enhance trust in issuance and trading and strengthen the monitoring of market risks, thereby reducing systemic risk.

## 1.2 Contributions

The contributions of this thesis are summarised as follows.

- We explore the industry's issues from a practical perspective, providing insights for the academic community on the requirements in practice.

- Based on our requirement collection, we propose a new financial assets issuance mechanism based on industry issues and demonstrate a new bidding model for this mechanism. We also develop a blockchain-based system for financial assets.
- According to the requirement collection, we construct a new risk monitoring mechanism that provides monitoring and warning for blockchain-based financial assets. We also develop a system that can interact with regulatory agencies, thereby reducing the occurrence of systemic risks with the help of our new risk monitoring mechanism.

## 1.3 Thesis Outline

The outline of this thesis is organised as follows. Chapter 2 presents an academic survey of blockchain technology, from its innovation to application scenarios within the financial industry. Chapter 3 examines the requirements for the industry using a blended strategy approach that combines qualitative and quantitative methods. Chapter 4 proposes a blockchain-based system for financial security issuance and trading. Chapter 5 introduces a new mechanism for risk warning and monitoring systems for blockchain-based financial assets. Finally, Chapter 6 provides a general conclusion of the thesis.

CHAPTER 2

# Applying Blockchain for Primary Financial Market: A Survey

According to market functions, financial markets are divided into primary and secondary markets for share exchange (Szabo, 1997). The primary market investment covers all stages of equity investment before the initial public offering (IPO) of its equity, including venture capital (VC) and private equity (PE), while the secondary market is one in which shares are traded among investors under standardised supervision. In other words, trading shares of a company before the IPO is regarded as the primary market, and trading shares after the IPO is named the secondary market. Regardless of whether academically or in the industry, there are numerous studies for the secondary market. However, there are relatively fewer studies for the primary market.

The size of the primary market is significant. The 'McKinsey Global Private Markets Review 2020' (Q. Yang et al., 2019), shows that total global private equity market transactions in 2019 plateaued at 1.47 trillion USD versus 1.49 trillion USD in 2018. Before 2019, global private equity market transactions grew by 12% annually from 2013 to 2018. However, the primary financial market has never been as booming as its cousin (i.e., the secondary market) due to the following key issues:

The ecosystem of the primary financial market is fragmented, and its infrastructure is not as well established as the second financial market. The main reasons for hindering the primary market are the high cost of discovering each other correctly, asymmetric information, the high cost and complex process of trading stages, and poor financial derivatives in the primary market.

With the rapidly increasing information technology in past decades, it has played the most critical role in our daily life in the fields of living, health, communication, entertainment, etc. One of the most significant innovations in information technology is blockchain, proposed by Nakamoto (2008). This peer-to-peer electronic cash system enlightened new methods of data sharing, data security and privacy, incentives for involvers, and decentralisation, which has the potential to address the above issues for the primary financial market.

This chapter focuses on adopting blockchain technology with financial services, especially for private equity exchange in the primary financial market. According to our survey, there are many challenges in the market, an inefficient asset trading structure, difficulty in matching mechanisms, less standardised asset management procedures, etc. Due to the feature of blockchain technology, it is considered a potential solution for the above challenges. In this literature review, the existing efforts to improve the limitations of the primary financial market with the help of blockchain will be collected and (Treleaven et al., 2017; Walch, 2015; Yuan & Wang, 2016; Zyskind et al., 2015).

For contribution, this chapter investigates the application of blockchain in the field of private equity exchange as the core content, combing the research literature on this issue, especially the research results in recent years, thus ensuring that the industry and academia more intuitively understand the status of the application of blockchain technology to the construction of the new generation of financial market infrastructure. From the perspective of academic research, this chapter provides support and exploration direction for the deepening research of the innovative application of blockchain in the private equity trading field by systematically combing the current research results. From the perspective of the construction of new financial market infrastructure, the conclusions of this chapter have specific application value for using the "blockchain + securities" model in actual work, innovating the private equity trading model, and improving the structure of the primary financial market.

The rest of the chapter is organised as follows. Section 2.1 provides a brief introduction to the business process of the primary financial market. Section 2.2 collects and introduces blockchain key technologies and notations as a taxonomy for this survey. Section 2.3 introduces how blockchain is applied in the financial market. The combination and the primary market will be further discussed in Section 2.4, while Section 2.5 gives a conclusion and future work.

## 2.1 Financial Market

Since the 1970s, the development of information technology has vigorously promoted the popularisation and application of the electronic and networked transaction settlement system in the financial market, realising the rapid development of the multi-level securities market and the informatisation of market participants. The most prominent feature of securities trading is a centralised third-party credit or information intermediary agency as a guarantee, which realises value transfer by reducing information asymmetry and relying on traditional institutions to establish a trust mechanism, whether in primary or secondary markets.

### 2.1.1 Workflow of primary market

Due to the unique characteristics of the primary market, there is no recognised trading platform for trading in the real world (Kaplan & Strömberg, 2009). In the industry, when private equity transactions are usually conducted, they are based on the following process:

Buyers and sellers get to know each other through broker introductions and sometimes through friends' introductions, but most deals are made through brokers, often referred to as FA (financial advisors). After the introduction, if the buyer and seller intend to proceed with the deal, they will sign the NDA (Non-Disclosure Agreement). After signing NDA, the seller will send some of its basic information to the buyer for review through the broker or itself.

After the buyer reconfirms that this is their interested target, they will continue to follow up. This time they will go to the seller's company for an interview. After the interview, the buyer will start its DD (Due Diligence), and TS (Term Sheet) will be signed if both interview and DD are satisfied by the buyer's requirements, which means that the deal has been completed chiefly. TS is a letter of intent for investment and is not legally binding. Finally, the buyer and seller will sign the SPA (Share Purchase Agreement) and other agreements to determine the investment contract, which confirms the investment.

It is not difficult to see during the transaction process that these characteristics of trust, data sharing, and data security are the main reasons leading to the current status in the primary market (Nadauld et al., 2019; Ozili, 2018; Robinson & Sensoy, 2016).

## 2.1.2 Primary Market Exchange & Clearing House

### 2.1.2.1 Private Equity Exchange

In this chapter, corporate shares are the target assets in both the primary and secondary markets. The difference is that the primary market invests in the equity of companies that have not yet been listed, and the secondary market invests in the equity of companies that have been listed (Koeplin et al., 2000).

The equity price in the primary market is not transparent and can only be estimated, so there is only a valuation for the unlisted companies (Anson, 2013). Since it is a valuation, there will be an overestimation, underestimation, and accurate and false evaluations. Estimating and underestimating can happen in actual practice, but different valuation methods can lead to different results (Chemmanur & Fulghieri, 1994). Many companies do not only focus on valuation when choosing investors but also depend on investors' business reputation and so on (Nelson, 2018). Therefore, in terms of equity transactions in the primary market, every case is different, and it is a deal that both buyers and sellers need to recognise, but not the buyers only. False evaluation refers to the fact that provided data is falsified, which leads to inaccurate estimation. In addition, due to the lack of supervision by regulatory agencies in the primary market, it is easy for buyers and sellers to have mismatched information and be deceived after time and effort (Mendelson, 1982).

### 2.1.2.2 Over-the-counter

Most of the transactions in the primary market are OTC (Over-the-counter) transactions (Acharya et al., 2012). OTC transaction is based on the credit of both parties to the transaction. Both parties to the transaction bear the credit risk themselves. The transaction can only be carried out after establishing a bilateral credit. However, the credit risk level is very high, and no one would like to bear it with an easy decision. Hence, liquidity for the primary market is very low.

The OTC market discussed above is the generalised OTC transaction without a clearinghouse, not a standard OTC market for commodities, derivatives, bonds etc. Therefore, the OTC market size for the primary market is minimal. If there is a clearinghouse in the primary market, the liquidity problem will cease.

In a centralised OTC market, each transaction subject uses a centralised clearinghouse or exchange trading centre as the counterparty, and the clearinghouse is responsible for bearing the market traders' credit risk (Mendelson, 1982). Because the essence of OTC is private transactions between buyers and sellers, both parties can freely negotiate prices, and the terms are not known to outsiders. Therefore, the intervention of the clearinghouse is to clarify the risks and clear the settlement (Roe, 2013). Especially after Dodd-frank, the US government hopes that all foreign OTC transactions involving US interests will be settled through a CCC (Central counterparty clearinghouse). Nevertheless, plenty of scholars are worried that all the risks like this are concentrated in this CCC, and there will be a systemic risk among the CCC (Bignon & Vuillemey, 2020; Griffith, 2011; Kress, 2011; Lawrence, 2012).

#### 2.1.2.3 Clearinghouse

The clearinghouse is an independent institution responsible for delivering, hedging, and settling futures contracts in the futures exchange. The clearinghouse is a clearing and settlement structure established with the development of futures trading and the emergence of standardised futures contracts (Hasenpusch, 2009). Establishing the clearinghouse perfected the futures trading system in the development of futures trading. It ensures that futures trading can proceed smoothly in the futures exchange and becomes the core of the futures market operating mechanism. Once the futures transaction is reached, both parties will have relations with the clearinghouse. The clearinghouse is the buyer and seller of all futures contracts (Bliss & Steigerwald, 2006).

Through the clearinghouse, the transfer, trading, and actual delivery of futures contracts can be carried out at any time without notifying the counterparty. It is responsible for the unified settlement, clearing and delivery of goods. This is the particular “replacement function” of the clearinghouse. All these actions of the clearinghouse can be successfully realised because it has substantial financial resources and has implemented a margin system, which is a set of strict debt-free financial operation systems (Chen et al., 2015).

In this chapter, we mainly explain the issues of equity transferring. Therefore, the clearinghouse’s target asset should only consider equity derivatives.

### 2.1.3 Challenges in Private Equity Market

There are many challenges in the primary market for making a deal. Many scholars demonstrated their research (Kollmann et al., 2014; Nadauld et al., 2019; Robinson & Sensoy, 2016; Wright et al., 2009), which results in a fragmented ecosystem of the primary market: 1) High cost of making a deal; 2) Low liquidity; 3) Lack of trust; 4) Less data security.

Under the traditional model, the efficiency of mutual discovery between financing companies and investors is relatively low, and high costs are required. Currently, the mainstream method of discovery and matching is through an introduction by an intermediary, a financial agency. However, the financial agency cannot fully understand the needs of both parties, and in order to earn returns or from the perspective of their interests, increases the cycle of matching between two parties (Batjargal, 2007; Hsu & Shiu, 2010; Layne, 2007).

Besides, the liquidity of the primary market needs to be improved. For investors who hold assets objectively, there is also a need to sell assets, especially when facing a shortage of funds or the fund needs to exit at maturity. The process of the implementation of asset trading is relatively cumbersome, and many complex procedures are involved in completing the settlement of funds and the transfer and registration of assets. The resulting inconvenience of trading directly restricts the improvement of market liquidity (Lerner & Schoar, 2004; Meuleman et al., 2009; Wright et al., 2009).

Regarding transaction procedures, it is difficult for primary market transactions to ensure the authenticity and integrity of transactions fully. In addition to investors, asset transaction participants also involve sellers and third-party intermediaries such as securities companies, accounting firms, law firms, etc. Under the traditional trading model, there is often information asymmetry between investors and financiers, resulting in long transaction cycles. On the one hand, sellers, intermediaries, and other stakeholders have been "colluding" to achieve a listing. On the other hand, due to the inability to accurately determine the authenticity and credibility of the underlying assets, coupled with insufficient information disclosure on time, it is difficult for investors and intermediaries to control risks, and this results in high transaction risk (Cumming, 2005; Kollmann et al., 2014).

At present, primary market transactions have not yet achieved the asymmetric encryption of transaction information with cryptographic technology, and the transmission of information is mainly through email or USB copy. The confidentiality and security of transaction data are still facing challenges (Ozili, 2018).

Currently, the global primary market size is large, but considering the actual investment and financing needs, the primary market size is supposed to be more significant. The following reasons mainly cause this situation. 1. Achieving rapid matching between investors and companies is difficult. Investors cannot quickly find suitable companies when they want to invest. Small and medium sized enterprises cannot quickly find investors when they want to raise funds. 2. Asymmetric investment and financing information can easily lead to unfair business. 3. Since the issuance and registration of private securities mainly rely on third-party institutions and involve multiple parties, the current lack of an efficient integration platform results in high costs and low efficiency in private securities management. 4. Compared with the secondary market, the primary market lacks various options, such as leveraged trading, which limits scale expansion to a certain extent.

Recently, the emergence of a relatively novel technology, blockchain, may alter he above issues, and securities transactions can be redesigned and optimised through blockchain technology. Blockchain technology can realise the transformation of securities trading from centralised trust to weak centralisation and decentralisation and is expected to become an important technological innovation to change the securities industry. The characteristics of blockchain have different expressions in different papers. However, the following characteristics have reached a consensus: decentralisation, high transparency, enhanced security, and immutability of information. Its technical characteristics overlap with the mentioned issues and are now reviewed.

The main issues in the primary market are summarised in the following order:

**Issue 1**: Difficult to discover each other. The buyers and sellers are challenged to match the demands and requirements of each other, the probability of a deal is minimal, and the cost of a deal is very high.

**Issue 2**: Information asymmetry. Both the buyers and the sellers have a solid intention to provide false information to maximise their interests.

**Issue 3**: High cost and complex trading process. During the trading process in the primary market, third-party intermediary companies are usually involved in helping them conduct target assets. Third-party companies include accounting firms, law firms, appraisal companies, etc. Third-party intermediary companies might have an intention to defraud for their own benefits. Since the cost of fraud is low and difficult to discover, they will use fraud for some bribery and benefits. The bribery and benefits are usually conveyed by the sellers, but sometimes also by the buyers as well.

**Issue 4**: Poor financial derivatives in the primary market. The financial derivatives market is significantly developed in the secondary market but inferior in the primary market. However, many excellent companies can provide derivatives before they go public, which can significantly improve the liquidity of the primary market.

## 2.2 Blockchain

Blockchain is another disruptive technology after cloud computing, the Internet of Things, and big data. Blockchain does not simply increase the efficiency of digital collaboration in the original business format but through a new technology-economic paradigm can provide an infrastructure based on value interconnection for the securities industry and securities trading models. Relying on its unique characteristics of “decentralization” and “trust”, applying blockchain technology appropriately might ensure the establishment of trust between multiple parties while protecting data privacy and is expected to become an essential part of the financial market infrastructure (Evans-Pughe, 2012).

## 2.2.1 Blockchain

A critical purpose of blockchain technology innovation is to serve financial transactions. It is an append-only distributed ledger of transactions. First presented with Bitcoin (Nakamoto, 2008), the blockchain started as a decentralized electronic instalment framework, eliminating the requirement for any outsider association for instalment moves. The first Bitcoin blockchain composed information as a chain of squares coordinated using the square hash esteems, henceforth the name “blockchain.” As Nakamoto (2008) introduced, Bitcoin was the first to present blockchain as the comprehensive framework of a distributed system.

## 2.2.2 Core technologies of blockchain

### 2.2.2.1 Cryptographic algorithm

The blockchain uses many cryptographic technologies such as Hash algorithms (SHA3-256), asymmetric encryption, elliptic curve digital signatures, secure multi-party calculations, zero-knowledge proofs, etc. It uses cryptographic technology to realize functions such as transaction verification and transaction privacy. In layperson’s terms, through cryptographic algorithms, the identities of both parties to the transaction will not be impersonated by a third party, nor will the information be stolen by a third party, and the functions of ensuring the integrity and non-repudiation of the information can be realized.

### 2.2.2.2 Consensus mechanisms

Consensus mechanisms, such as the POW (Proof of Work), POS (Proof of Stake), DPoS (Delegated Proof of Stake) and BFT (Byzantine Fault Tolerance), Algorithm, etc., are mainly employed to solve the strategies and methods of how multiple consensus nodes achieve data consistency and correctness. Different application scenarios will use different consensus mechanisms to balance the system's efficiency, security, and data consistency.

#### 2.2.2.3 Smart Contract

The term "smart contract" was proposed by Nick Szabo in 2003, long before the popularization of blockchain (Shrier et al., 2016). He believes that a smart contract is a set of commitments defined in digital form, including agreements on which contract participants can execute these commitments. Generally speaking, it is a contract that can be automatically executed when certain conditions are met on a computer system. Running smart contracts on the blockchain can ensure the entire process is open and transparent and cannot be tampered with. At the same time, it can also avoid the influence of centralized institutions so that smart contracts must operate efficiently. Nick's work theory on intelligent contracts was not realized until the innovation of blockchain. An important reason is the lack of digital systems and technologies supporting programmable contracts. The emergence of blockchain technology solves this problem. It supports programmable contracts and has the advantages of decentralization, non-tampering, transparent and traceable processes, and is naturally suitable for intelligent contracts. Therefore, it can also be said that smart contracts are one of the characteristics of blockchain technology.

Blockchain-based smart contracts include transaction processing and storage mechanisms, a complete state machine for accepting and processing various smart contracts, and transaction storage and state processing are completed on the blockchain (Norta, 2015). The transaction mainly contains the data that needs to be sent, and the event is the data description. After the transaction and event information is passed into the smart contract, the resource status in the contract resource collection will be updated, which triggers the smart contract to make state machine judgments. If the trigger condition of one or several actions in the automatic state machine is met, the state machine selects the contract action to execute automatically according to the pre-set information. According to the trigger condition in the event description information, the smart contract system automatically sends out pre-set data resources and events, including the trigger condition, from the smart contract when the trigger condition is met. The core of the smart contract system lies in the smart contract with the transaction and the event processed by the smart contract module. It is still a group of transactions and events. The smart contract is simply a system comprising a transaction processing module and a state machine. It does not generate a smart contract, nor does it modify the smart contract. It exists only to enable a complex set of digital commitments with trigger conditions to be executed correctly according to the participants' will.

#### 2.2.2.4 Incentives

The incentive mechanism is one of the essential cores of blockchain. In the blockchain, the more nodes in the chain, the safer it is, and the more incentive mechanism can attract more people willing to become data nodes and attract everyone to rush into the "mining circle" frantically (O'Dwyer & Malone, 2014). To put it simply, the incentive mechanism under the blockchain is to encourage nodes to participate in maintaining the safe operation of the blockchain system through economic balance and to prevent tampering with the general ledger, which is the driving force for the long-term maintenance of the blockchain network (Nakamoto, 2008).

Incentive mechanisms are not available in all blockchains. Some alliance chains and private chains do not have incentive mechanisms. The nodes in alliances and private chains are designated or composed of communities of interests, so there is no need for incentives. Incentives mainly exist in the form of a public chain. The nodes in the public chain are distributed worldwide; everyone on the chain does not know each other, and there is no central organization to endorse, which requires all nodes to work together to maintain the security and stability of the system. To achieve this goal, the blockchain system encourages participants to work actively so that there are enough nodes in the system to ensure the regular operation of the system.

In the blockchain, digital currency is used an incentive method, such as Bitcoin (BTC) and Ethereum (ETH), which result from incentives. BTC is shown as an example to illustrate how the incentives are obtained. Bitcoin is issued in the form of mining. The first transaction recorded in each block is defined as a coin base transaction. That is, a certain amount of Bitcoin is used as a reward for miners who find the block. This particular transaction was made from nothing. It was just a digital number at the beginning, and as the number of miners supporting the network gradually increased, this digital number was given the attributes of value and liquidity, and it became a digital currency (Bradbury, 2016; Mauer & Senbet, 1992).

#### 2.2.2.5 Multi-signature (Privacy)

Multi-signature technology provides more security than traditional single-signature methods by eliminating a single point of failure in the system. If a key is lost or hacked, unauthorized access to your account is not allowed if you still have the remaining keys. The anonymity of Bitcoin makes transactions untrustworthy and ultimately makes users afraid to make transactions. However, with the signature function, there is an effective means to confirm the information of both parties (Tian et al., 2020). Multi-signature can be simply understood as multiple signatures of a digital asset. Multi-signature indicates that digital assets can be controlled and managed by multiple people. Multi-signature means that the use of this fund requires multiple private vital signatures. Usually, the funds or digital assets will be stored in a multi-signature address or account (Rozario & Thomas, 2019). It is similar to a document in life that needs to be signed by multiple departments to become effective.

Multi-signature solves the vulnerabilities in existing methods by using multiple private keys. The transaction cannot continue in this scenario unless all required private keys are provided. This makes any individual key useless to thieves because they must steal all of the private keys to make it work. This is no different from what banks have been doing for decades because some banks require multiple signatures on cheques to process them.

Multi-signature utilizes digital signature as the underlying technology and yet enforces higher security. It helped to make it possible to apply blockchain-related technologies to various industries. A multi-signature address can be associated with n private keys in the operation process. When transfers and other operations are required, funds can be transferred if m private keys are signed, where m must be less than or equal to n, so that m/n is less than 1 and can be 2/3, 3/5, etc. It must be determined when the multi-signature address is established. Under certain circumstances, digital assets need to be controlled by multiple people. In other words, under certain conditions, if a digital asset cannot be confirmed to belong to a specific person, it is best to let related parties jointly sign its ownership.

## 2.2.3 Core advantages and applications of blockchain

### 2.2.3.1 Data Sharing

Data sharing is one of the most useful applications that Blockchain systems can offer (Ma et al., 2018). Blockchain can facilitate setting up a secure, trusted and decentralised intelligent exchanging ecosystem to address information-sharing issues in this way contributing to making better utilisation of the transport infrastructures and resources (Kang et al., 2019).

### 2.2.3.2 Data Security

Data security is one of the most critical factors and challenges for people in the digital world (Shrier et al., 2016). Blockchain technology uses its distributed system, giving a solution to the challenge. Buterin (2014) introduces the blockchain mechanism to ensure data security and privacy. It is briefly summarised in the following:

a) Use signatures to ensure the data integrity of the information.

b) Use the relevant principles of cryptography for data verification to ensure that it cannot be tampered with.

c) In authority management, multiple private critical rules are used for access authority control.

In authority management, multiple private critical rules are used for access authority control. Combining the above three points creates high data security under the blockchain system.

#### 2.2.3.3 Trust

Blockchain is based on the design principle of a distributed ledger. People have never been able to transfer assets with complete Trust through the Internet directly, and must be achieved through a third-party, centralised ledger. Most scholars believe that a centralised system only provides little Trust for the users, which is only for their reputation (Abadi & Brunnermeier, 2018; Beck et al., 2016; Datta et al., 2003; Z. Yang et al., 2019). In other words, it means no absolute trust exists in a centralised system. With a distributed ledger, there is no such intermediary, and the transaction record is visible to everyone and cannot be tampered with.

It can be considered that the trusted source of the blockchain is an internal code, which is distributed rather than relying on a person or an intermediary. For each member in the system, this member's basic information, integrity, transaction status, etc., are visible to both parties during the transaction. Simply put, both parties to the transaction exist in the form of codes. It is unnecessary to consider whether the other party is trustworthy (trestles) because the system's coding will force the adoption of the principle of good faith. If the regulations are violated, more time, money, and personal credibility will be consumed, and the gain will not be worth the loss.

Nakamoto (2008) has established a consensus mechanism. The intermediary role is redundant, and its status can be replaced by code, allowing the system to reach a consensus on the transactions that occur through the consensus algorithm and record it on the block. Wang and Vassileva (2007) noted that consensus is a social process. Even without algorithm help, humans are very good at handling consensus issues.

So, to reach a consensus, the system now adopts a "proof of work" mechanism. It describes a distributed system that requires a not insignificant but feasible amount of effort to deter frivolous or malicious uses of computing power, such as sending spam emails or launching denial of service attacks (Nunes, 2017). This process is essential because the blockchain differs from the high-speed circulation of Internet information. It is stored completely. Every transaction will be printed with a timestamp to ensure the integrity of transaction records. Therefore, the trust level of a distributed system can be considered the highest.

#### 2.2.2.4 Distributed autonomous organization

DAO (Distributed Autonomous Organization) is an organisational structure based on the blockchain. It can operate autonomously without interference and management through some open and fair rules (Schär, 2020). These rules often appear in the form of open-source software, and anyone can become a participant in the organisation by purchasing shares or providing services. Typical examples of DAO are Bitcoin and Ethereum. Most rules are open and transparent, such as the number limit, the consensus method, and the rules of competitive accounting.

To some extent, it can be regarded as an unmanned payment system. Institutions and those who hold Bitcoin or Ether are shareholders of this institution, and those miners and developers also become participants of the institution by contributing their services. When more people need the institution, the equity in their hands may appreciate, and after the appreciation, they can share the organisation's income and participate in its growth.

DAO operates autonomously without intervention and management through open and fair rules (Titman & Grinblatt, 1998). After all its programs are successfully set, it can automatically operate according to the original rules.

There are many changes in the form of DAO. It can be a digital currency, system, organisation, or driverless car. They provide customers with valuable services that can be currency transmission (such as Bitcoin), application platforms (such as Ethereum), domain name management systems (such as domain currency), or any other business model (Angieri et al., 2020). These business models are prominent, more like stocks of specific institutions than a single currency. Each DAO has its terms and conditions. There is always the right to view the disposable and digital currency DAO shares, and dividends (such as GXS) may be received from them.

Blockchain-based DAO can be regarded as an autonomous organisation or company built on the blockchain, entirely controlled by code. In this company, all the articles of association, governance, management regulations, systems, etc., are written into smart contracts, which connect individuals to individuals, individuals to organisations, or organisations to organisations through intelligent contracts. These individual members or organisations can be distributed all over the world and can even participate anonymously. Compared with traditional companies, there is no need for CEOs, CTOs, etc., no water, gas, food, or other supplements; no actual office locations or geographic limitations are needed. It has the characteristics of quick registration and creation, low operating costs, openness, and transparency.

The primary characteristics of the DAO organisation are "decentralisation" and "autonomy." Decentralisation is mainly reflected in its organisational form that keeps running through smart contracts and can encode its financial transactions and rules on the blockchain. Its daily activities are entirely based on the written code, effectively avoiding dependence on the central authority.

Autonomy is achieved due to its smart contract rules being automatically executed. Once the DAO is released, no one can stop it, and no one can change it from the outside.

#### 2.2.2.5 DeFi – Decentralised finance

Defi is the abbreviation of Decentralised Finance, also named distributed finance. Compared with the traditional highly centralised financial system, decentralised finance uses blockchain technology, such as mobile wallet software developed based on blockchain technology, to eliminate the role of third-party institutions and intermediaries through smart contract codes. Moreover, it can directly connect both parties to the transaction for financial transactions, such as transfer, financial management, currency exchange, lending, mortgage, etc., to avoid the waste of money and time costs caused by complex intermediate links (Chen & Bellavitis, 2019).

In short, Defi is the improvement and solution of blockchain for the traditional financial industry's high degree of centralisation, low efficiency, complicated processes, and high thresholds. Its root lies in building code trust through blockchain technology and smart contracts to help people realise decentralised transactions, and point-to-point transfers, simplify transaction procedures and reduce transaction costs. At the same time, it is also meant to refer to inclusive finance, that is, making money and financial transactions more familiar and accessible, no matter how the person was born or where he stays (Goldreich et al., 1991).

The closed nature of traditional finance lies in the extreme asymmetry in the information field between institutions and ordinary people, which makes it difficult for ordinary people to enjoy the financial value contained in their financial assets. The Defi system is open. On the one hand, its smart contract code is an open source for people to query and supervise. On the other hand, in Defi-based transactions, in addition to encrypting the private information of the parties to the transaction, the transaction data is open to everyone. Anyone can query blockchain data and develop related applications through the open interface, and in its system, all transaction records and behaviours generated are also traceable. Therefore, the entire Defi system is highly transparent and open.

The traditional financial system is usually regionalised. For example, PayPal is used in Australia and other western countries, but it cannot be used in many Asian and African countries. Because traditional finance is limited by geopolitics, humanistic economics, and other factors, the friction costs of the entire transaction process are reasonably high, and the development of inclusive finance has also slowed down.

Taking traditional cross-border payment as an example, the entire basic process found online is approximately: After domestic individuals purchase goods at the displayed foreign currency quotations on overseas websites, they pay the corresponding AUD amount to non-financial institutions, and then the non-financial institutions' Domestic cooperative banks purchase foreign exchange in bulk and enter it into the personal foreign exchange settlement and sales management system of the foreign exchange bureau. After receiving payment success information from non-financial institutions, overseas merchants mail goods to domestic residents. After receiving the goods, domestic residents will send clearing instructions to non-financial institutions. Non-financial institutions shall, following settlement agreements with overseas merchants, remit payments in foreign currencies to overseas merchant bank settlement accounts through domestic cooperative banks and complete cross-border settlement.

An essential point of Defi is that it is developed based on the underlying public chain. What is the public chain? It means that any individual or group worldwide can send a transaction, the blockchain can effectively confirm the transaction, and anyone can participate in the consensus process. In other words, with the further development of Defi and its peer-to-peer network transmission mechanism, users can enjoy the financial services provided by this system as long as they join it, no matter where they are. The time and money costs incurred are compared with traditional finance, which is much lower, which is of great significance for promoting the development of inclusive finance.

In the real world, the regulation and compliance of each government restrict the development of its financial market. A centralised financial system inherently restricts the freedom of the market. Therefore, the existence of Defi has a special meaning to the world.

So far, blockchain has gone through multiple stages of development, the origin of technology, blockchain 1.0 and blockchain 2.0, has entered the smart contract application stage, namely blockchain 3.0. Based on the above technical attributes and characteristics, the blockchain challenges the traditional logic of financial intermediaries for credit endorsement and reduction of adverse selection and moral hazard. Blockchain relies on the security, Trust, privacy, incentives, governance, and consensus created by mathematical laws, making it possible to realise asset transactions without resorting to third-party financial intermediaries. This is having an impact on the underlying financial infrastructure. With the support of blockchain technology, securities investors and issuers can realise direct securities transactions and realise cross-time allocation without financial intermediary credit endorsement.

## 2.3 Applying Blockchain to Primary Market

With the further development of technology, information technology plays a vital role in developing the financial industry. In the new era, information technology has become a key technology for the development of the financial industry, helping to improve the financial system, and plays a vital role in improving operational efficiency. At present, most scholars believe that the IoT (Internet of Things), AI (Artificial Intelligence), big data and blockchain will be the leading technologies in building the future financial market industry (Rabah, 2018). In addition, besides the IoT, the other three technologies are significantly related to the construction of primary financial market infrastructure.

Compared within these three technologies, in the financial market scenario, big data is mainly used in operations, industry forecasting, sales, interrelations, etc.; AI is mainly used in robo-advisory, anti-fraud, investment forecasting, risk management, etc.; Blockchain is mainly used in infrastructure, risk control, business processes and so on (Garcia, 2020).

According to the preceding, it is not difficult to determine that the technical characteristics of blockchain are very suitable for the construction of financial market infrastructure and will have a significant impact on the payment system, central custody, securities settlement, central counterparty, and transaction databases. As a fundamental technology, blockchain can effectively encrypt and classify data, reduce data redundancy, and increase the effectiveness of data exchange (Wu & Liang, 2017).

From a theoretical point of view, blockchain technology has broad application prospects in securities trading, and the application scenarios can cover three links: before, during and after transactions. For example, before the transaction, as a system technology, the blockchain can be applied to the customer, i.e., know your clients (KYC) anti-money laundering, information disclosure and other scenarios. During the transaction, as data storage or data exchange technology, the blockchain can be applied to issuing and transferring stocks, bonds, collective debt instruments, and derivatives. After the transaction, as a recognition technology, blockchain can be applied to scenarios such as registration, depository, liquidation, settlement, data sharing, share splitting, shareholder voting, dividend payment, and collateral management.

Due to the advantages of blockchain technology, the application of adopting blockchain in the secondary market, insurance and other financial fields is appropriate. The securities industry has already begun exploring the blockchain in recent years. Among them, exploring applications in the secondary market and exchanges started earlier with many landing application scenarios. The development of exploration of primary market applications is relatively slow, and landing application scenarios need to be further enriched. Based on this, the following will examine the development trend of the application of blockchain technology in the securities market and follow the sequence from the secondary market, the exchange, to the primary market.

Overall, applying blockchain technology in securities trading presents a gradual process. In the early days, as the technology was in its infancy, blockchain technology was mainly applied to data sharing and data security (Manning, 2017). With technology's gradual maturity and development, it has gradually explored its application in settlement and clearing processes, etc. After the further development of technology, the application of blockchain technology will bring changes to the financial infrastructure and industry structure of the securities industry.

### 2.3.1. Status of secondary market

The combination of the secondary market and blockchain technology is a popular opic for academia and the industry. Tsai et al. (2020) studied the use of blockchain technology with Ethereum on the secondary market exchanges, which can solve some of the problems of the traditional exchange system, such as transaction fees, lack of transparency, centralization, etc.

Not only in theory but also in practical applications, the application of blockchain technology at the centre of the exchange is also adopted. At present, the officially announced application systems are focused on issuing and trading private equity and other over-the-counter market securities and post-trade services in the on-exchange market. LSE (London Securities Exchange) is considering adding blockchain technology to their exchange centre to reduce costs. In 2018, IBM developed a blockchain base trading system for LSE (Jacobs, 2018). The ASX (Australian Securities Exchange) had also prepared to apply blockchain technology in its system by the end of 2020 or early 2021 to facilitate various financial markets services, such as clearing, settlement and other post-trade services (Dunkley, 2018), although it has ultimately scrapped the plan. In order to reduce costs, HKEX (Hong Kong Exchange) has also planned to use blockchain technology and is now cooperating with ASX (Pop et al., 2018). SGX (Singapore Exchange) applied a distributed system to its combining blockchain-based platform ISTOX (Pan, 2019). The application of blockchain technology has proven reliable in secondary exchanges. In the future, more and more stock exchanges will choose to apply blockchain technology.

Nasdaq announced the launch of Nasdaq Linq, a private equity trading platform based on blockchain technology, in cooperation with blockchain start-up Chain.com (Jacobs, 2018). The platform serves the equity transfer of non-listed companies and can complete the settlement of private equity transactions. Many financial institutions, such as Deutsche KfW Financial Institutions, have conducted blockchain-based simulation securities trading business tests (Dogru et al., 2018). For example, KFW Bank has developed Euro commercial paper based on distributed ledger technology. In 2016, the French government implemented new regulations and approved banks and financial technology companies to build a blockchain platform, “Securities Electronic Distributed Recording Facility,” for unlisted securities transactions. The French government approved using blockchain technology to trade unlisted securities (Khujamurodov, 2020). The Korea Stock Exchange uses blockchain technology to develop a counter-trading system. Citigroup and CME Group launched a blockchain platform for back-end management of securities trading (Jacobs, 2018).

## 2.3.2 Current status of clearinghouse

Similar to exchanges, the combination of clearinghouse and blockchain is also a research hotspot with many practical use cases. On the one hand, many scholars have researched clearinghouse-related technologies such as settlement, clearing, interbank transactions, etc. On the other hand, many scholars conduct comprehensive research. Since 2015, the clearinghouse has been the most critical application scenario by adopting blockchain technology into the financial industry, and many clearinghouses have started their blockchain projects (Wu & Liang, 2017).

The American Securities Depository and Clearing Corporation (DTCC) was established in 1999 by the integration of the American Depository Trust Company (DTC) and the American Securities Clearing Corporation (NSCC). Since its development, almost all stock transactions, corporate and government bonds, mortgage-backed securities, money market instruments, and over-the-counter derivatives in the United States have been handed over to DTCC subsidiaries for clearing and settlement. DTCC has launched a blockchain project named Project Whitney to enhance its business efficiency. DTCC can reach the level required to handle the highest transaction volume of the entire transaction day through distributed ledger technology (DLT), equivalent to 115,000,000 per day, which means 6,300 transactions per second for five consecutive hours. This equals dozens of times the actual speed (DTCC, 2020).

Mvula et al. (2019) proposed that the characteristics of blockchain technology applications can replace the central clearinghouse's limitations. By considering the transaction relationship between traders on the blockchain and whether there is a logic of trusted parties involving transactions among entities, a system is designed to effectively clear and settle transactions with trusted and untrusted entities, dramatically improving efficiency (Hughes et al., 2019). Wu and Liang (2017) pointed out that the current limitations faced by the clearinghouse include the following: 1) Workflows are too complicated; 2) It is too slow to receive information from the exchange, or there is too much redundant information; 3) The information received from other exchanges is not certified, especially from the bank, the information is even more asymmetrical. Therefore, they have designed a clearinghouse system using blockchain technology in Fig. 2.1, which can ultimately compensate for these limitations and significantly improve the system's clearing speed. Guangdong Clearing Corporation used this model for a two-month experiment. As a result, the processing data of these two months is equivalent to 16 months of trading at NASDAQ or 13 years of trading at the London Stock Exchange. In addition, Wu and Liang (2017) also illustrate the following advantages of this model: secured data updates between exchanges, secured updates from clearinghouses to banks, and effective identification and certification.

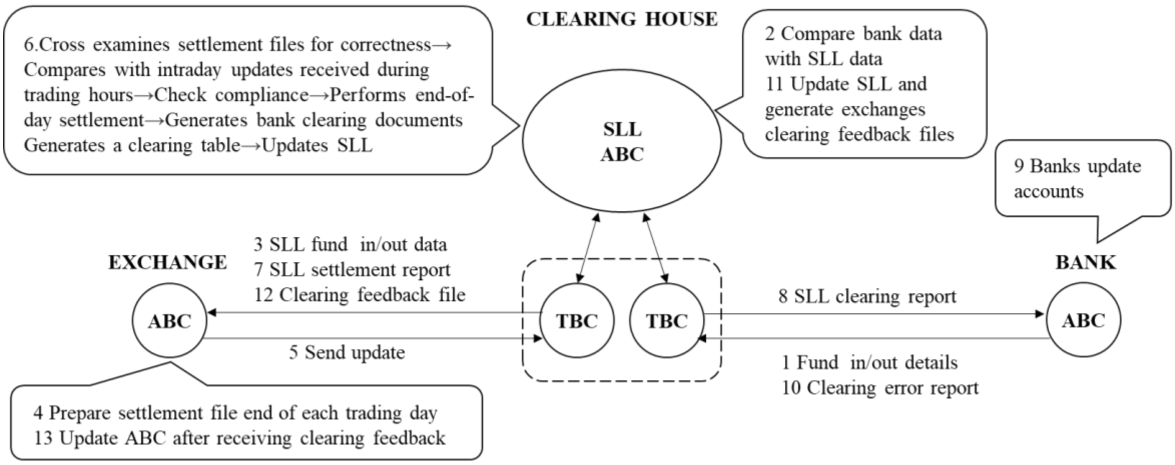


Fig. 2.1: Workflow of applying blockchain into clearinghouse.

Based on blockchain technology, combined with X-swap, a matching credit system, Foroglou and Tsilidou (2015) designed and explored a China Foreign Exchange Trade System, which effectively solves the related problems of low efficiency and high cost in interbank transactions. According to the complicated operation process of settlement and clearinghouse, a mobile phone clearing system was proposed and designed by Ganti et al. (2017), which can be used for mobile financial services in Zambia. Through the smart contract and rule pre-set in advance, the mobile phone can be used for settlement and clearing services with high-level data security and data origin authentication.

### 2.3.3 Current status of primary market

Compared with the secondary market and clearinghouse system, the primary market also has similar requirements for applying blockchain technology to similar problems. Specifically, the issues like transaction, liquidity, trust, data security, etc., have similar application requirements in the primary market as well, which can be solved by blockchain technology (Xu et al., 2019).

For example, non-standardized OTC contracts based on a “smart contract” blockchain are presented as executable code, and non-automated trading of standardized contracts may offer potential. Each participant in the blockchain has a complete transaction record. By “anchoring” the assets associated with the transaction on the blockchain, it can ensure that both parties can perform and reduce the counterparty’s default risk.

At present, the issuance and application of blockchain technology in the securities industry are mainly concentrated in the field of digital securities. For example, as early as 2014, Nasdaq used blockchain technology in its exchange system (Jacobs, 2018). The US Securities and Exchange Commission has approved an online retailer Overstock.com’s S-3 application to issue the company’s newly listed stock on the blockchain. In August, World Bank (2018) issued the world’s first bond created and managed using blockchain technology, the “Bondi” bond.

Nevertheless, there are also differences in demands. Firstly, the scenario in the primary market is more complicated, which requires a higher intelligent system to deal with. Secondly, the secondary market has less liquidity than the secondary market. Thirdly, there are only a few derivatives for the primary market but plenty of varieties in the secondary market. Based on the advantages of blockchain above, there is practical significance to applying blockchain technology in the primary market.

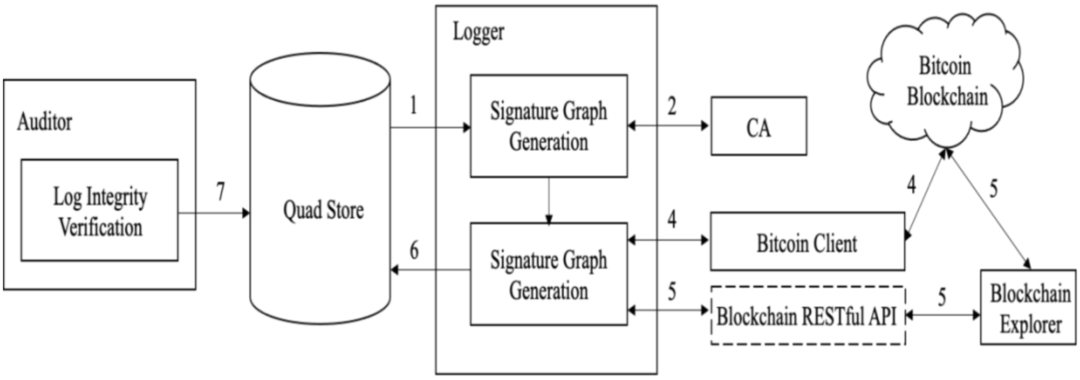


Fig. 2.2: Linked Data-based Model by Ahmad et al. (2018)

Regarding securities issuance, Halevi et al. (2019) state that replacing the third parties of securitization in the primary market with a blockchain-based system can track process details more accurately, reduce costs, increase issuance speed, increase transparency, and thereby increase liquidity. Buterin (2014) believes that applying blockchain technology can reduce the risk of fraud due to information asymmetry. Ahmad et al. (2018) propose a Linked Data-based model in Fig. 2.2, which gives the data both verification and tamper-proof features to prevent collusion efficiently and increase trust in the financial market.

Sulkowski (2018) established a model for considerations for changes to an existing Blockchain, shown in Fig. 2.3. Once someone modifies financial or business data, all participants in the blockchain will receive the modification information. It is difficult for the operator to eliminate the traces of their modification. Data sharing helps the system effectively prevent the problem of property fraud.

Technically speaking, although the application of blockchain in the primary market is feasible, the current development in practice is slow. It is mainly due to regulatory restrictions and no uniform standard (Zhu & Zhou, 2016). However, with the government's recognition of blockchain and the technological advancement of distributed systems, some current regulatory restrictions will be released in the future.

Throughout the process of issuing certificates for securities in the primary market, with the help of blockchain decentralization, participating institutions can no longer operate independently, realize the joint participation and supervision of each node, solve the problem of vital intermediary, and protect the legitimate rights and interests of both parties to the transaction. With the help of distributed ledgers to record the openness and transparency of the information generated during the IPO business process, the problem of information asymmetry is effectively solved, thereby avoiding moral hazards. The tamper-proof modification and asymmetric encryption technology are beneficial to improve the security of transaction information and effectively prevent malicious attacks, thus improving the issuance efficiency and reducing the issuance cost.

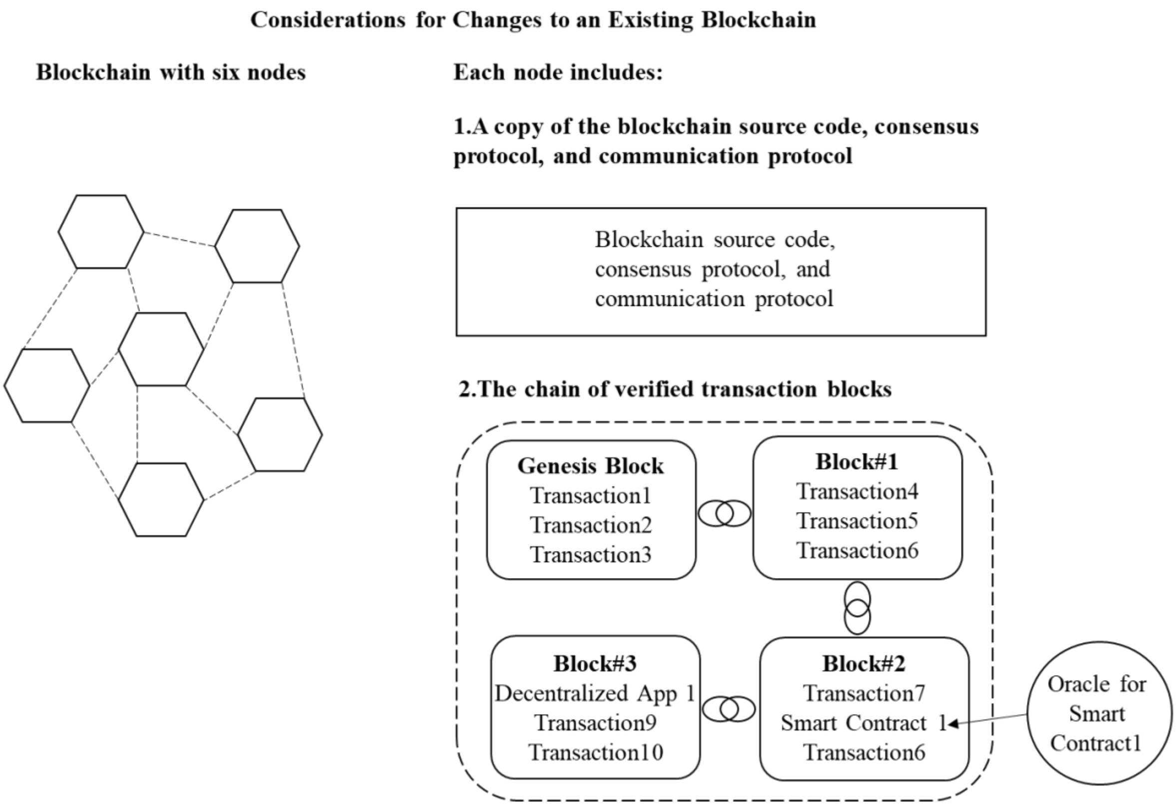


Fig. 2.3: Considerations for Changes to an Existing Blockchain

The core technology of the blockchain can better solve some challenges in the issuance and trading of the securities market, such as trust problems, information asymmetry problems, etc. However, the blockchain technology itself also has some shortcomings, mainly reflected in the low physical performance, which leads to the low transaction frequency of the blockchain and the deviation of the flexibility of the transaction process, which cannot meet the transaction needs. How to improve the security performance and operating efficiency of the blockchain is the key technical challenge for the blockchain to achieve large-scale issuance and trading in the securities market in the future. At present, some scholars have discussed key technologies in blockchain performance improvement technology, such as sharding (Wang et al., 2019), scalable consensus (Luu et al., 2015), snowflake to avalanche (Rocket, 2018), DAG (Directed Acyclic Graphic) (Pervez et al., 2018), off-chain computing, layer 2 lightning network (Kiayias & Litos, 2020), hash algorithm optimization (Wu et al., 2020), etc. Since this survey mainly discusses articles related to primary financial market applications the performance improvement literature will not be addressed further.

## 2.4 Observations and Taxonomy

Table 2.1: Problems in primary financial market and solutions from blockchain

| Issues in Primary Market | Blockchain Technology |
|---|---|
| Asymmetry Information | Multi-signature |
| Complex trading process (Low efficiency) | Smart contract |
| Complex Validation Process (High cost, low efficiency) | Proof of work |
| Data Fraud (Asymmetry information) | Multi-party authentication |
| Data Privacy and Data Sharing (Discovery, low efficiency, lack at trust, high cost) | Distributed Autonomous Organization |
| High Due Diligence Cost (Low efficiency, high cost, lack at trust) | Tamper-proof |
| Inefficient Execution of Contracts (Lack at trust, low efficiency) | Smart contract |
| Lack at Trust | Tamper-proof |
| Mismatch (Discovery, low efficiency) | Permissioned blockchain |

From the existing research, the following observations have been made:

1. Currently, relying on centralized intermediary credit, the secondary market has formed an effective quotation and transaction system. Exploring new technology applications is continuously expanding and deepening, and the market development is generally mature and complete (Caprio et al., 2012; Harvey & Aldridge, 2014; Nabilou, 2020).

2. Relying on blockchain technology, the "decentralization" of the secondary market clearing, settlement and custody omits the back-end system in the trading system. Many institutions and researchers in the market have explored and practised this. The domain application is still in a gradual process (Bradbury, 2015; Chen & Bellavitis, 2019; Zetzsche et al., 2020).

3. For the primary market, the centralized issuance system is relatively complete but only limited to large-scale infrastructure, such as exchanges endorsed by the states and governments, e.g., Nasdaq, London Exchange, Chicago Exchange etc. However, on small scales, the governments are trying to improve (Duffie, 2014; Santo et al., 2016) and (Swanson, 2021).

4. In contrast, the use of blockchain to build a decentralized primary market has not received enough attention in research and practice, and the use of blockchain technology to establish a primary market with diverse distribution methods is still in its infancy (DTCC, 2020; Funcke & Bauknecht, 2016).

5. It is believed that blockchain technology can increase trust, improve data-related problems, and meet the most basic needs in the primary financial market. Meanwhile, it is foreseen that by combining the blockchain's decentralized ideas and smart contracts, more financial derivatives can be created for the primary market.

To drive future research, a taxonomy for the primary financial market with blockchain is shown in Fig. 2.4.

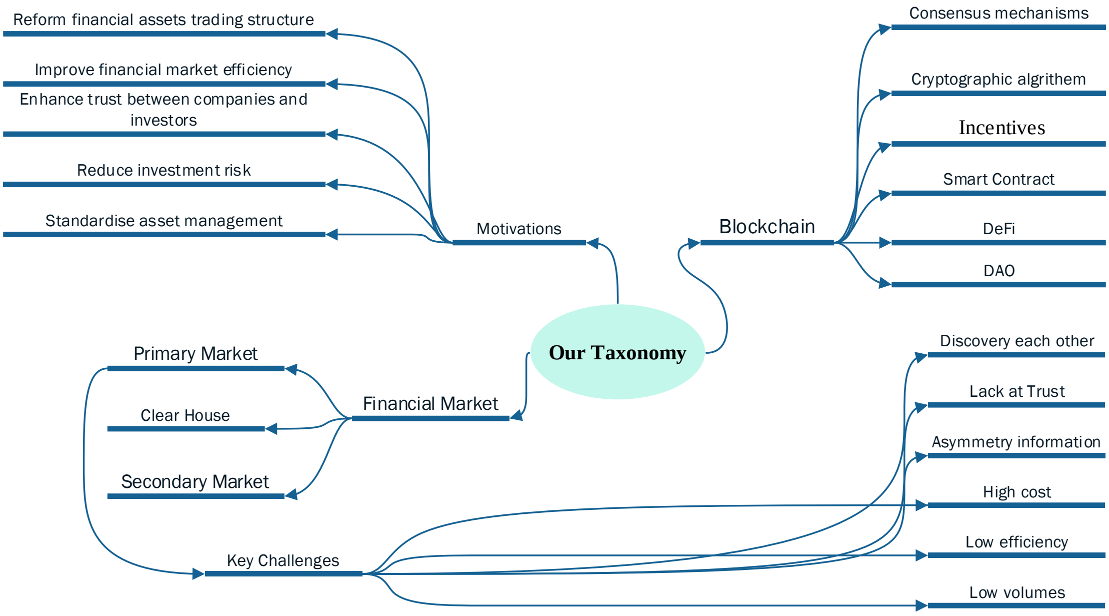


Fig. 2.4: Our Taxonomy for Primary Financial Market vs. Blockchain

## 2.5 Conclusion

Blockchain technology provides special empowerment for financial transactions, triggering subversive innovations in the financial market. This survey conducts the literature on the principle and application of blockchain technology and focuses on blockchain research in financial asset trading. The development of blockchain technology, especially the maturity of stable-coin technology, makes it possible to become the enabling technology supporting the next-generation infrastructure of the future financial market. After several years of development, blockchain technology has proven suitable for financial scenarios requiring multi-party sharing, high-frequency repetition, and long transaction chains.

This survey highlights the importance of applying essential blockchain technology to the financial market, especially in the primary market. The essential blockchain technologies for the primary market include, but are not limited to, a smart contract, multi-signature, distributed autonomous organization, tokenization, etc. It is expected that this survey can be helpful to the community, providing an idea for the future design of a new ecology of the primary market.

However, there are still challenges to applying blockchain for solving the issues in the financial market: a) regulation and compliance of governments are challenging to build into blockchain; b) technology development and application of blockchain is still at an early stage; c) privacy preservation of blockchain applications is hard to satisfy each party's requirements in the financial market.

In the future, I will focus on combining blockchain and the financial market around the above three challenges to amend the fragmented ecosystem of the primary financial market.

In the subsequent chapter, I undertake a more thorough exploration of practical aspects related to primary financial market issues.

CHAPTER 3

# Digging into Primary Financial Market: The Issues of Primary Financial Market Issuance and Investigations from the Perspective of Blockchain

The financial market can be divided into two types of market: the primary market and the secondary market (Stiglitz, 1989). The primary market is where companies conduct transactions before IPO (Initial Public Offering). Stock and bonds have not undergone a standardised review process before going public. Thus, many issues exist, such as trust, authenticity, privacy, etc., in the market. The secondary market is a market for stock/bond trading transactions that have been standardised and reviewed by regulation. There are four parts in the transaction chain of the primary market: raising funds, investing assets, asset monitoring, and existence. Financing companies, investment institutions, brokers, valuation firms, law firms, accounting firms, etc., are participating in the primary market. Each participant has a unique purpose and role. These participants help the market to maintain stability.

The primary financial market is enormous. The 'McKinsey Global Private Markets Review 2020' shows that total global private equity market transactions in 2019 plateaued at 1.47 trillion USD versus 1.49 trillion USD in 2018. Before 2019, global private equity market transactions grew 12% annually from 2013 to 2018.

In the current primary market, securities issuance must go through registration, filing, custody, listing and circulation processes. Securities trading includes price inquiry, transaction, order confirmation, order matching, transaction amount accounting, and settlement. It is a long and tedious process, from preparing for issuance to successful listing, including many instructions and involving multiple market institutions.

As the primary market lacks standardisation, information asymmetry, fraud, and high cost of due diligence have led to seriously fragmented ecosystems. Under the background that the development of the securities market puts forward higher requirements for transaction costs, transaction efficiency and transparency, such a cumbersome business process cannot sufficiently meet the needs of investment and financing entities. Industry and academia have tried to change this status quo, but there has been no noticeable effect. The infrastructure of the primary financial market is not so easy to optimise without solving the challenges listed.

Since Bitcoin was invented, the blockchain technology which supports it has quickly entered people's eyes (Zheng et al., 2018). One of the essential purposes of the invention of blockchain was to develop the financial industry (Kshetri, 2018). The decentralised idea and unique features of blockchain, such as decentralisation, high transparency, enhanced security, and immutability of information, make blockchain the most appropriate technology along with the logic of financial markets (Walch, 2015).

Blockchain technology can rely on encryption algorithms, consensus mechanisms, timestamps, and other means to conduct a highly secure and credible point-to-point transaction with a multi-party peer-to-peer flat structure. In general, blockchain technology can provide full-process, multi-angle technical solutions for securities registration, issuance, trading, clearing and other links and make subversive changes in business processes. Currently, the securities industry has high hopes for using blockchain technology. Institutions in the financial market industry are also actively conducting pilot projects and proof-of-concept of blockchain technology, hoping that it can reduce industry operational risks, improve industry operational efficiency, and breed new business models.

These institutions have seen blockchain technology as the next major technological innovation that could change the securities industry. Nevertheless, significant changes never happen overnight. What are the pain points and difficulties the current primary market financial infrastructure development urgently needs to solve? Can blockchain bring new value to the securities industry? Are various institutions ready to embrace blockchain technology faster and invest in its implementation? These are all questions worth exploring. Only by clarifying these questions can institutions understand blockchain implementation's difficulty and commercial value in the primary market.

To help advance research in primary financial market infrastructure development, the authors conducted an empirical study to investigate the work practice and potential challenges primary market involvers face. The authors followed a blended strategy approach that combines interviews (qualitative method) and surveys (quantitative method). In particular, the authors interviewed 15 primary financial involvers with various backgrounds and expertise. They were asked participants about their everyday work and relevant challenges faced during their responsibilities in the primary financial market during the interviews. Next, the authors adopted open card sorting (Spencer, 2009) to analyse the interview results. The following categories produced by open card sorting were grouped into three groups, i.e., complex due diligence, mismatching, and difficult monitoring. After that, the authors performed a validation survey with 54 participants to confirm various insights from the interviews, including challenges, best practices, and desired improvements based on the interviews.

According to the interview and survey, the authors realised that the primary market participants cared a lot about due diligence but did not effectively avoid the complex process. Besides, the asymmetric information and lack of trust among the participants make it hard to settle. Also, it is hard to discover each other, which makes the market lack liquidity. The limitations influenced their day-by-day work, particularly for large companies.

The significant contributions of the research are as follows:

- As far as the authors know, this is the first in-depth research investigating primary market participants' insights on the current status of the primary financial market and blockchain technology through interviews and surveys.
- The authors analyse both qualitative and quantitative data and highlight potential opportunities and implications that investors, financiers, brokers, and other financial market participants can use to improve their daily work under a new infrastructure in the future.

The following sections are organised as follows: The next section provides background materials on the primary market and blockchain. Section 3.2 presents a 2-parts methodology, both quantitative and qualitative. The findings of this study are discussed in Section 3.3. In Section 3.4, the authors discuss the threats to the validity of the research. Section 3.5 is the related work. The final section gives conclusions and future work.

## 3.1 Background

### 3.1.1 Primary financial market

Since the 1970s, the development of information technology has vigorously promoted the popularization and application of the electronic and networked transaction settlement system in the financial market, realizing the rapid development of the multi-level securities market and the informatization of market participants. The most prominent feature of securities trading is a centralized third-party credit or information intermediary agency as a guarantee, which realizes value transfer by reducing information asymmetry and relying on traditional institutions to establish a trust mechanism, whether in the primary or secondary market.

Because of the unique characteristics of the primary financial market, it seems impossible to have a unified exchange system in the world (Kaplan & Strömberg, 2009). In practice, the following process shown in Fig. 3.1 is how to conduct simple private equity transactions in the primary market:

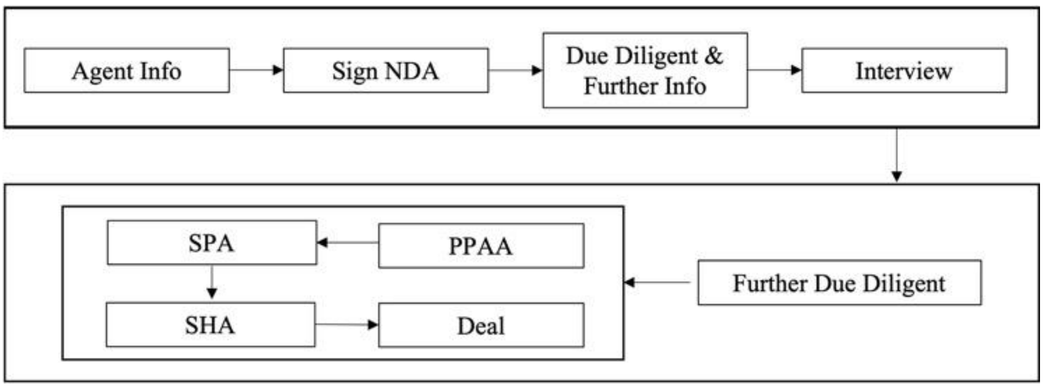


Fig. 3.1: Workflow of primary market

Buyers and sellers know each other through the introduction of a broker, sometimes through a friend's introduction, but most transactions are reached through a broker, usually called an FA (Financial Advisor). After the buyer and seller contact, if the buyer and seller intend to continue the transaction, they will sign a non-disclosure agreement (NDA). After signing the NDA, the seller sends some of its basic information to the buyer, and the buyer will need to hire third-party service companies to validate the authenticity.

After the buyer reconfirms that this firm or project is the target it is interested in, the buyer will forward to the next step, an on-site interview. After the interview, the DD (Due Diligence) process will be launched, and if both the interview and DD meet the buyer's requirements, they will sign a TS (Term Sheet), which can be regarded as a promised investment agreement. TS is a letter of intent to invest and is not subject to legal restrictions. Finally, the buyer and seller will sign SPA (Share Purchase Agreement) and other relevant agreements to confirm the investment contract, which is the final step of the investment activity. Other relevant agreements typically include SHA (Shareholders Agreement) and PPAA (Predict Profit Allocation Agreement).

Trust, data sharing, data security, and related personalization characteristics are the main reasons for the existing problems in the primary market (Franzoni et al., 2012).

### 3.1.2 Blockchain

As this thesis has introduced blockchain in Chapter 1, this part will not introduce blockchain again.

## 3.2 Methodology

Fig. 3.2 illustrates the overview of the methodology design, which combines the interview and survey parts. Interview part: 15 experts from the primary financial market are interviewed to get insights into the primary market. Survey part: it is used to validate the findings from the interviews. The authors present how to design and implement the interview and survey in the following.

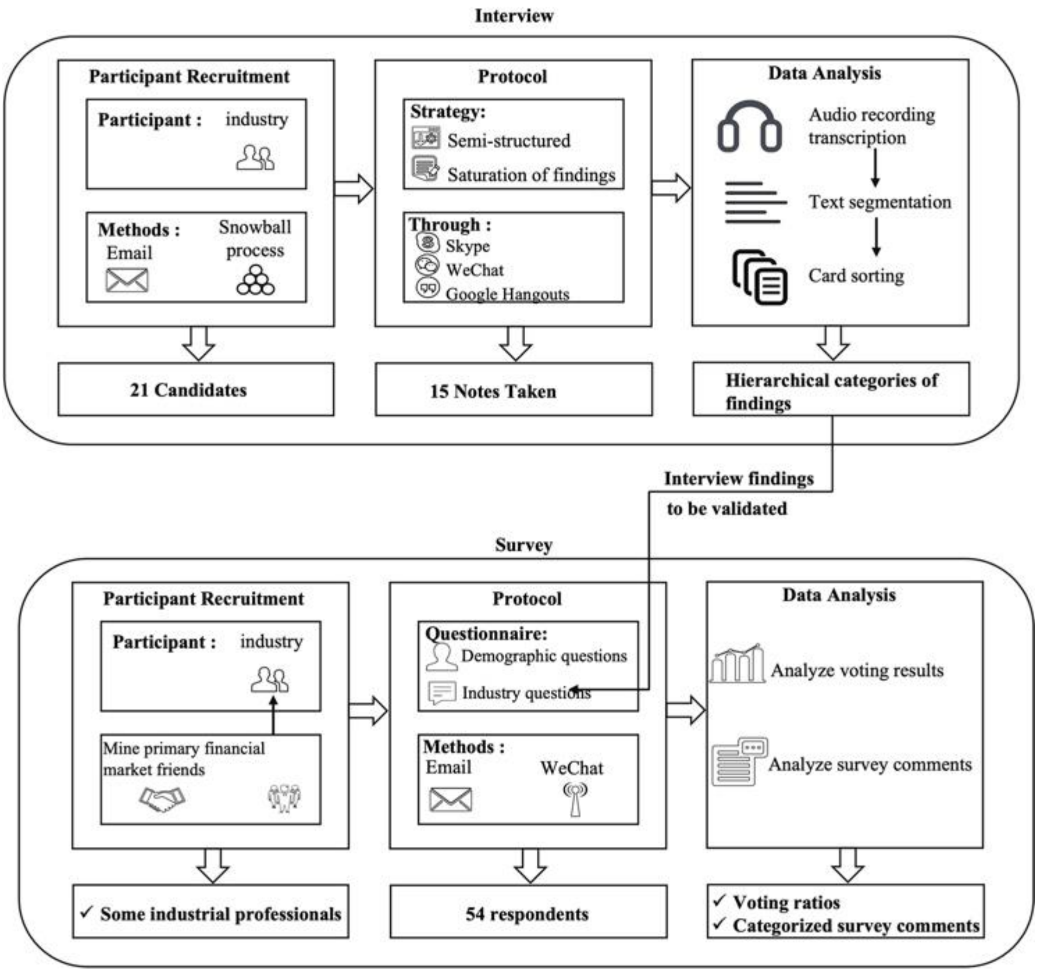


Fig. 3.2: Methodology design

### 3.2.1. Interview

This research adopts a semi-structured interview (Shull et al., 2008). The authors first exchanged introductory information, such as respective institutions and positions, with the interviewees and then introduced the research and purpose. Next, the authors asked some basic qualitative questions to the interviewees. Then, some open questions are designed to guide the interviewee with the ideal directions (Questions are listed in Table 3.1). These open questions probed the interviewees about their perspectives on the primary financial market and applying blockchain in the primary market. Since the design of semi-structured interviews, the authors arranged subsequent questions to delve further into the interview participant's perspectives at a later stage. In the end, the authors asked the interviewee to give whatever other significant data the interviewers may have missed during the interviews.

Table 3.1: Problems in primary financial market and solutions from blockchain

| | Issues |
|---|---|
| 1. | What is your role in the primary market? Please describe your main duty and goal. |
| 2. | What are the 3 most common pain points/difficulties in your business? |
| 3. | Let us discuss these pain points one by one: |
| | 1) Regarding pain point 1, please describe in detail, can you explain what you think is causing it? |
| | 2) Regarding pain point 2, please describe in detail, can you explain what you think is causing it? |
| | 3) Regarding pain point 3, please describe it in detail. Can you explain what you think is causing it? |
| | 4) Optional: If the respondent does not list any cost, trust or efficiency issues, we will need the following questions. What do you think of these issues in the industry? |
| 4. | In view of the above pain points, which one do you think needs to be solved urgently? Do you know or understand any innovations/solutions to these problems? |
| 5. | Have you heard of blockchain? (If not, please skip; if yes, please continue to ask). Do you think that applying it in the industry can solve the above problems? |
| 6. | If a product/technology can solve the above problems in some way, will your industry group be willing to use it? |
| 7. | Do you think you have any relevant supplements in our interview today? For example, you think it is important, but we forgot to ask. |

In this interview, a total of 15 interviewees were interviewed. Among them, 5 are at or above the partner level of equity investment institutions, 4 are from third-party service agencies, 4 are corporate financing directors or directors of the financing department, and 2 are from investment banks with solid experience. The interviewees covered the prominent participants in the primary market.

There is a total number of 21 candidates prepared for the interview, but due to uncontrollable reasons, such as COVID-19 and timing, only 15 of them were interviewed by us. During the interviews, the authors followed the procedure utilized by Aniche et al. (2018) and Singer et al. (2014) to choose when to stop the meeting, i.e., halting interviews when there is enough saturation of findings. Saturation is a methodology widely used in qualitative research (Fusch & Ness, 2015; Guest et al., 2006; Morse, 2015).

To ensure that the interviews are of broad-spectrum significance, the interviewees covered most types of primary market participants, such as investment institutions, financing companies, law firms, accounting firms, etc.

The authors interviewed interviewees from various backgrounds (as demonstrated in Table 3.2) before deciding whether saturation had been reached. In every interview, the interviewers cooperated to pose questions and take notes. After completing each interview, the interviewers would contrast their notes with past ones to check whether there were any new insights from the interview.

Because of COVID-19, all interviews were conducted remotely via Zoom and WeChat, and the interviewers took notes. The average and standard deviation of the interview time were 35 and 30 minutes, respectively. Table 3.2 illustrates the basic demographics of the interviewees. According to the table, the interviewees had an average experience of 12.13 years of working experience and 10.4 years in the primary financial market by the time of the interviews.

Table 3.2: Interviewee's background

| ***No.*** | ***Role*** | ***General Experience*** | ***Primary Market Experience*** |
|---|---|---|---|
| *1* | PE/VC Partner | 10 | 10 |
| *2* | Financing VP | 17 | 15 |
| *3* | PE/VC Partner | 12 | 11 |
| *4* | PE/VC Director | 11 | 6 |
| *5* | PE/VC Director | 8 | 8 |
| *6* | PE/VC Director | 9 | 9 |

| *No.* | *Role* | *General Experience* | *Primary Market Experience* |
|---|---|---|---|
| *7* | Financing VP | 12 | 10 |
| *8* | CFO | 13 | 10 |
| *9* | PE/VC Partner | 16 | 13 |
| *10* | Financing VP | 12 | 8 |
| *11* | Financing VP | 22 | 18 |
| *12* | PE/VC Director | 14 | 12 |
| *13* | PE/VC Partner | 10 | 10 |
| *14* | Financing VP | 7 | 7 |
| *15* | PE/VC Director | 9 | 9 |
| * | *Minimum | *7 | *6 |

#### 3.2.1.1 Participant recruitment

Two authors used to work in the primary financial market and used their connections to contact an initial group of 10 candidates. The authors utilized a snowball process to generate another group with another 11 candidates (Goodman, 1961), i.e., current participants refer the interview to their target participants. There are a total of 21 experts agreed to participate in the interview.

#### 3.2.1.2. Data analysis

Card sorting (Spencer, 2009) is applied to recognize the classifications from each interview. It is a particular procedure to get classifications from data (Kim et al., 2016, 2018). There are three different types: closed card sorting with predefined categories for data, open card sorting with no predefined categories, and hybrid card sorting, which combines the previous two types (Zimmermann, 2016). Considering the research is exploratory, with categories (i.e., challenges of the primary market) being unknown, the authors conducted an open card sorting process to analyse these data.

After a card was made for each textual unit in the card sorting, the cards were then bunched into influential groups with a theme or topic meanings: these groups, i.e., low-level, mid-level, and high-level categories. The consequences of remarkably open card sorting would allow us to acquire various hierarchical categories designs. Two authors were involved in the card-sorting process. Every card was identified and analysed by them. The authors identified three high-level categories using card sorting, i.e., complex due diligence, mismatching, and difficult monitoring.

## 3.2.2 Survey

### 3.2.2.1 Design

The questionnaire includes three demographic questions, 7 primary financial market questions, and 2 blockchain-related questions. The demographic questions are single-choice and designed to understand the background and experience of participants. The primary financial market questions are designed to validate insights that the authors have found from the interview part. The participants who have been interviewed are not asked to respond to the survey. There are both single choices and 2 choices questions included. The authors regard the 2 choices questions as sorting to analyse more straightforward rather than plan sorting method. The blockchain-related questions are mainly designed to validate the idea that blockchain technology will improve the infrastructure of the primary financial market. The complete list of the survey questions can be found in Appendix 1.

### 3.2.2.2 Survey respondent recruitment and statistics

The potential survey participants are professional experts involved in the primary financial market, and their primary roles include investment, financing, brokerage, audit, etc. Since the main participants are from China and some are from Australia and the United States, Chinese and English versions are prepared. This survey is released through the application of Questionnaire Star. The respondents can use any mobile phone/computer/pad to respond to the survey by scanning the code.

When selecting respondents, the authors pay more attention to their work experience in the primary market, preferably compound working experience, to make a more efficient result. There are no other factors, such as academic qualifications, to limit the selection of respondents. Because most of the participants in the primary financial market have higher academic qualifications, and all the target participants have master's or doctoral degrees. To eliminate similar ideas from the same company or the same period of work, the authors control that at most two respondents are from the same company.

Totally 54 respondents were recruited. From the perspective of the participants' roles, 40.7% of them are from investment institutions, 24.07% from financing parties, 20.37% from third-party service intermediaries, and 14.81% from brokers. For general working experience, 70.37% of people have more than 4 years of work experience, and only 29.63% have less than 3 years of work experience. For primary financial market working experience, 55.56% of people have more than 4 years of primary market experience, and only 44.44% have less than 3 years of relevant work experience. Pie charts of broad working experience and primary financial market working experience are shown in Fig. 3.3. It is a relatively convincing work background structure.

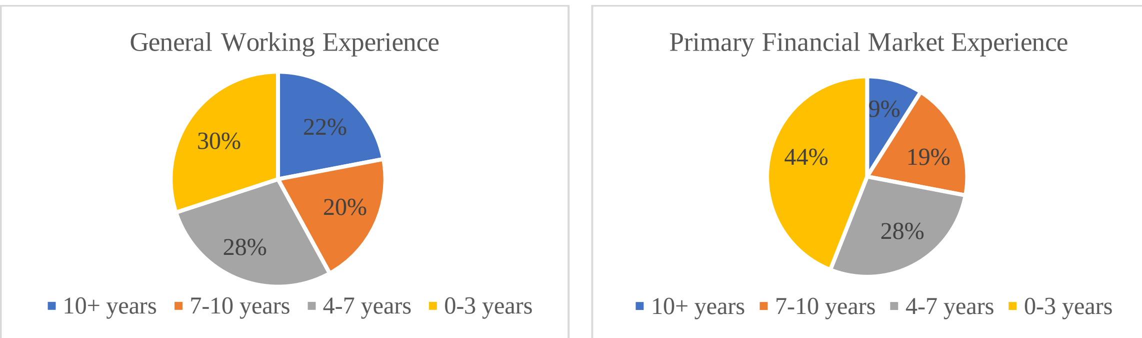


Fig. 3.3: Pie charts of general working experience and primary financial market experience in percentage

### 3.2.2.3 Data analysis

After terminating the questionnaire collection, the authors analysed the closed-ended questions by adopting different analysis methods. The authors calculated the number of votes for each answer option. Next, the percentage rate for each answer option was calculated by dividing the number of votes by 54 (the total respondents' number).

To better understand respondents' perspectives of the primary financial market's challenges, the authors divided the participants into several demographic groups and compared their voting results with each other's. Based on previous studies by Halevi et al. (2019) and Buterin (2014), the authors constructed the following demographic groups:

- Respondents from the investment field (Inv)
- Respondents from the financing field (Fin)
- Respondents from third parties (Thi)
- Respondents from brokerage (Bro)
- Respondents with high general working experience (>=10 years) (GExpH)
- Respondents with low general working experience (<=3 years) (GExpL)
- Respondents with medium general working experience (>3, and <10 years) (GExpM)
- Respondents with high primary financial market-related working experience (>=7 years) (FExpH)
- Respondents with low primary financial market-related working experience (<=3 years) (FExpL)
- Respondents with low primary financial market-related working experience (>3 and <7 years) (FExpM)

The authors calculated the percentage ratios of their answers to the primary financial market challenges and desired improvements collected from the interview separately for each demographic group. According to Zou et al. (2020), Fisher's (1922) exact test was applied with Bonferroni correction (McDonald, 2009) to these numbers to make sure if one group tended to vote differently from others. Fisher's exact test reveals the frequency distribution of the variables (e.g., each option votes from each group in the research) in the analysis of contingency tables. It can determine if the observed difference between two proportions (i.e., the ratio of votes) is statistically significant. The family-wise error could be controlled by Bonferroni correction while making multiple comparisons. Section 4.4.2 shares the analysis results in detail.

## 3.3 Findings

In this part, the authors first present the findings for each category (a total of three categories) identified using open card sorting on the interview data. There are subcategories for each category, and the authors select some of the most effective content and analyse some statistics according to the survey feedback to highlight the generality of these findings. Next, it introduces the voting results of each population group in response to these challenges, the potential solutions mentioned by the interviewees, and the related significance tests of these results. Finally, it briefly concludes the interview and survey results.

### 3.3.1 Complex due diligence

The due diligence process of primary market transactions is mainly carried out through written reviews, on-site inspections, public channel searches, interviews, and entrusted third-party investment. As investors continue to pay more attention to issues such as consistency of interest and information transparency, the level of detail in their preliminary due diligence process has also increased. Although detailed and meticulous due diligence meets investors' specific requirements for companies to some extent, it often takes too long, reduces transaction efficiency, and increases transaction costs. On the other hand, due to the lack of a standardised due diligence checklist, some investors do not know the extent of their due diligence on the company.

### 3.3.2 Mismatching

The primary market is dominated by "over-the-counter transactions". The two parties may negotiate between the two parties or through the "matching" of third-party service agencies to complete the transaction. In this process, the transaction has asymmetric and redundant information, making it difficult for both parties to match the transaction accurately, and the transaction time is lengthened indefinitely. At the same time, some trading platforms lack the guarantee of credibility, and the ability to label information is weak. Forming a mature trading loop in the primary market is difficult. This also leads to low matching efficiency between the two parties in the primary market, and it is not easy to achieve transactions quickly.

### 3.3.3 Difficult monitoring

Post-investment monitoring means that investors need to understand the company's trends in time, understand the direction of capital use, identify problems in the company's development process, help companies carry out standardised management, and to a certain extent, restrict and deter the company. It is necessary to grasp the appropriate degree to meet your needs and not make the invested company feel too troublesome and controlled in the monitoring step. Much of the post-investment work in the primary market is in a state of groping. Post-investment work is relatively casual, lacks standardised procedures, and lacks assessment standards. The most direct consequence is that post-investment personnel do not know what to do, which causes laxity. Investors seem to have paid human and financial resources, but the monitoring effect is unsatisfactory.

### 3.3.4 Survey result

#### 3.3.4.1 Interview

A. Primary market pain points and complex issues.

Primary market transactions' pain points and difficulties run through all the links of "funding, investment, monitor and withdrawal". Funding is to raise funds. People who need to maintain or increase their assets will invest the money in investment institutions for management. Investment is to find a good company or project to invest in equity or debt. The monitoring is to track and manage invested projects and conduct follow-up reviews. Withdrawal is the process of finally selling the investment product and cashing out.

Among the 15 respondents, 14 respondents (93.3%) believed that the current due diligence procedures for securities issuance are too complicated, time-consuming, and costly, and they are on the premise of ensuring the quality of issuance. The issuance efficiency will be affected to a certain extent under complex due diligence. 10 respondents (66.67%) believe it is difficult to match investment institutions' needs with those of invested companies. For the equity investment process, 7 (46.67%) believe that the drawer agreement is difficult to implement. Regarding the follow-up management of equity investment, 11 respondents (73.3%) believe that effective post-investment management is facing specific difficulties and that there are challenges in fully obtaining various types of information on invested companies. At the same time, due to the imperfect exit mechanism, lack of professional intermediaries, and insufficient attention to exit management in the primary market, it is difficult for the primary market to exit equity.

B. Causes of the issues in the primary market.

All respondents agreed that the pain points and difficulties in the current primary market are rooted in a lack of trust (100%) and difficulty in ensuring the authenticity of data (100%).

C. Issues that need to be solved in the primary market.

Faced with the current pain points and difficulties in the primary market, respondents believe that the complexity of the due diligence process (93.3%) and post-investment management and exit (66.67%) should be resolved first. In addition, 79.63% of the respondents believe that improving the matching of the needs of investment institutions and invested companies is also an urgent problem that needs to be resolved.

D. Can the blockchain solve the primary market's pain points and complex issues?

Although all the interviewees have varying degrees of understanding of blockchain technology, there are still disagreements on whether blockchain technology can solve the pain points and difficulties of the primary market. 86.67% of the respondents have a positive attitude towards the application of blockchain technology, believing that based on the advantages of blockchain technology, the application of this technology can solve some of the pain points and difficulties. Furthermore, for the specific application scenarios of blockchain technology in the primary market, most interviewees did not have a deeper understanding and knowledge, and only one person was familiar with the application scenarios of blockchain technology and believed that part of the trust and process problems could be solved through the characteristics of the blockchain.

E. The acceptance of blockchain products in the primary market

100% of the interviewees believe that, on the premise that the transaction cost has not increased significantly, if the products based on blockchain technology can better solve the pain points and difficulties of the primary market, they will choose to use related products.

#### 3.3.4.2 Survey

Table 3.3 lists 20 challenges and 7 desired improvements mentioned by interviewees in the above sections. C1 to C4 were significant challenges of the pre-investment stage. C5 to C16 were significant challenges during the investment stage, and C17 to C20 were significant challenges in the post-investment stage. I21 to I24 were desired internal optimisation in the primary financial market environment in the future. I25 to I27 were expected external support in the future. The last column is the ratio (percentage) of respondents who voted for the second column challenges.

Table 3.3: Votes of challenges and desired improvements from interview

| ID | Challenges/Desired Improvements | Votes (Percentage) |
|---|---|---|
| | **Pre-investment Stage** | |
| C1 | Looking for investment channels and reliable partners | 47 (87.04%) |
| C2 | Methods and experience of screening companies | 24 (44.44%) |
| C3 | Forecast the development space prospects of the industry | 21 (38.89%) |
| C4 | Investment risk analysis | 16 (29.63%) |

| ID | Challenges/Desired Improvements | Votes (Percentage) |
|---|---|---|
| | **Investment Stage** | |
| C5 | Due diligence | 43 (79.63%) |
| C6 | Evaluation of matching needs between investment and financing parties | 43 (79.63%) |
| C7 | The authenticity of the information provided by the target company | 40 (74.07%) |
| C8 | Monitoring | 33 (61.11%) |
| C9 | Fair and objective industry/company information sources | 30 (55.56%) |
| C10 | Fundraising | 26 (48.15%) |
| C11 | Find high-quality companies as investment targets | 23 (42.59%) |
| C12 | Investment decision and execution | 21 (38.89%) |
| C13 | Performance evaluation | 20 (37.04%) |
| C14 | Realization of investment income | 18 (33.33%) |
| C15 | Professional and authoritative judgments on the development trend of the target | 15 (27.78%) |
| C16 | Information system support | 12 (22.22%) |
| | **Post-investment Stage** | |
| C17 | Exit mechanism | 38 (70.37%) |
| C18 | Information transparency | 31 (57.41%) |
| C19 | Post-investment risk management | 27 (50.00%) |
| C20 | Participation in major decisions of the company | 12 (22.22%) |
| | **Desired Internal Optimization** | |
| I21 | Integrate internal and external data to better analyze and judge service investment | 21 (38.89%) |
| I22 | Use new technology to improve the efficiency of investment process | 16 (29.63%) |
| I23 | Use new technologies to match investment needs more intelligently | 11 (20.37%) |
| I24 | Understand the application mode and applicability of new technologies in investment | 6 (11.11%) |
| | **Desired External Support** | |
| I25 | Professional resource support, providing industry/company evaluation and judgment information | 21 (38.89%) |
| I26 | Docking with outstanding target companies and tapping investment opportunities | 20 (37.04%) |
| I27 | Use third-party service organizations to apply and develop new technologies | 24.07%) |

After analysing the overall voting result of individual challenges and desired improvements, the authors will analyse them by different demographic groups. Table 3.3 illustrates the detailed results of the voting.

Table 3.4: Voting results of different groups towards 20 challenges and 7 desire improvements highlighted by questionaries. The Total row illustrates the number of respondents in each group. The rows C1 to I27 represent the percentages (%) of respondents from each group.

| **ID** | **Inv** | **Fin** | **Thi** | **Bro** | **GExpH** | **GExpL** | **GExpM** | **FExpH** | **FExpL** | **FExpM** |
|---|---|---|---|---|---|---|---|---|---|---|
| Total | 22 | 13 | 11 | 8 | 12 | 16 | 26 | 15 | 24 | 15 |
| C1 | 81.82 | 100.00 | 81.82 | 87.50 | 91.67 | 75.00 | 92.30 | 93.35 | 79.17 | 93.33 |
| C2 | 40.91 | 38.46 | 45.45 | 62.50 | 50.00 | 37.50 | 46.15 | 46.66 | 37.50 | 53.33 |
| C3 | 27.27 | 53.85 | 45.45 | 37.50 | 41.67 | 50.00 | 30.76 | 26.68 | 50.00 | 33.33 |
| C4 | 50.00 | 7.96 | 27.27 | 12.50 | 16.67 | 37.50 | 30.76 | 33.34 | 33.33 | 20.00 |
| C5 | 77.25 | 92.31 | 63.64 | 87.50 | 75.00 | 75.00 | 84.62 | 86.67 | 79.17 | 73.33 |
| C6 | 86.36 | 61.54 | 90.91 | 75.00 | 75.00 | 68.75 | 88.46 | 86.67 | 70.83 | 86.67 |
| C7 | 68.18 | 84.62 | 72.73 | 75.00 | 83.33 | 68.75 | 73.08 | 80.00 | 70.83 | 73.33 |
| C8 | 63.64 | 46.15 | 63.64 | 75.00 | 66.67 | 62.50 | 57.69 | 66.67 | 66.67 | 46.67 |
| C9 | 59.09 | 61.54 | 54.55 | 37.50 | 50.00 | 37.50 | 57.69 | 66.67 | 41.67 | 66.67 |
| C10 | 54.55 | 61.54 | 18.18 | 50.00 | 58.33 | 50.00 | 42.31 | 46.67 | 54.17 | 40.00 |
| C11 | 50.00 | 23.08 | 45.45 | 50.00 | 41.67 | 56.25 | 42.31 | 33.33 | 50.00 | 40.00 |
| C12 | 31.82 | 30.77 | 54.55 | 50.00 | 8.33 | 37.50 | 53.85 | 33.33 | 41.67 | 40.00 |
| C13 | 36.36 | 46.15 | 45.45 | 12.50 | 41.67 | 37.50 | 34.62 | 26.67 | 66.67 | 53.33 |
| C14 | 27.27 | 46.15 | 36.36 | 25.00 | 58.33 | 43.75 | 15.38 | 33.33 | 33.33 | 33.33 |
| C15 | 22.73 | 30.77 | 27.27 | 37.50 | 25.00 | 37.50 | 23.08 | 20.00 | 37.50 | 20.00 |
| C16 | 22.73 | 15.38 | 27.27 | 25.00 | 16.67 | 25.00 | 23.08 | 20.00 | 20.83 | 26.67 |
| C17 | 81.82 | 61.54 | 45.45 | 87.50 | 83.33 | 75.00 | 53.85 | 80.00 | 75.00 | 53.33 |
| C18 | 50.00 | 53.85 | 81.82 | 50.00 | 41.67 | 56.25 | 38.46 | 53.33 | 54.17 | 66.67 |
| C19 | 50.00 | 46.15 | 54.55 | 50.00 | 50.00 | 50.00 | 65.38 | 46.67 | 54.17 | 46.67 |
| C20 | 18.18 | 38.46 | 18.18 | 12.50 | 25.00 | 18.75 | 42.31 | 20.00 | 16.67 | 33.33 |
| I21 | 54.55 | 30.77 | 27.27 | 25.00 | 25.00 | 37.50 | 46.15 | 40.00 | 37.50 | 40.00 |
| I22 | 22.73 | 38.46 | 36.36 | 25.00 | 50.00 | 18.75 | 26.92 | 33.33 | 29.17 | 26.67 |
| I23 | 9.09 | 23.08 | 27.27 | 37.50 | 16.67 | 25.00 | 46.15 | 20.00 | 16.67 | 26.67 |
| I24 | 13.64 | 7.69 | 9.09 | 12.50 | 8.33 | 18.75 | 38.46 | 6.67 | 16.67 | 6.67 |
| I25 | 45.45 | 23.08 | 36.36 | 50.00 | 33.33 | 43.75 | 38.46 | 46.67 | 33.33 | 40.00 |
| I26 | 13.64 | 69.23 | 45.45 | 37.50 | 50.00 | 43.75 | 26.92 | 40.00 | 41.67 | 26.67 |
| I27 | 40.91 | 7.69 | 18.18 | 12.50 | 16.67 | 12.50 | 34.62 | 13.33 | 25.00 | 33.33 |

From Table 3.4, it could observe that the voting results varied among demographic groups. For example, for C17, FexpH and FExpL were 80% and 75%, while the ratio was only 53.33% for group FExpM. Another example for I22, the ratios of GexpH, GexpL, and GExpM were 50%, 18.75%, and 26.92%, respectively. To check whether the observed ratio differences are statistically significant, for each challenge/desired improvement, the authors applied Fisher's exact test with Bonferroni correction on three sets of demographic groups, i.e., groups with different roles (Inv vs Fin vs Thi vs Bro), groups with different general working experience (GExpH vs GExpL vs GExpM), and groups with different primary financial market-related working experience (FExpH vs FExpL vs FExpM).

After conducting 270 (10 group pairs ⇥ 27 challenges/improvements), Fisher's exact tests with Bonferroni corrections found that three tests showed that the relevant difference is statistically significant. It is Inv vs Fin L on I26 (p-value=0.002<0.05/6 after Bonferroni correction).

Based on the testing results, it can say with some certainty that: respondents from the financing field (Fin) are significantly more likely to rate I26 (Docking with outstanding target companies and tapping investment opportunities) as a significant desired external support than those respondents from investment field (Inv) (69.23% vs 13.64%).

### 3.3.5 Summary of results

From the analysis of the interview and survey, the authors could find the following:

Solving problems with complex due diligence processes, mismatching, and difficulty monitoring is urgent. Traditional solutions are challenging to eliminate the cost increase and efficiency loss caused by these problems. In the future, you can consider choosing emerging technologies, such as blockchain, to solve these problems in the primary market. The traditional solution is to reduce the friction of information/trust issues by introducing a financial agency, proving inefficient.

The respondents pay more attention to the primary market issues, mainly focusing on the following aspects:

In the initial stage: mismatch of investors and financiers. As the starting point for primary market trading, searching for suitable counterparties puts forward high requirements for investors and financiers. At present, primary market participants generally encounter difficulties in limited information access channels, low information credibility and high potential business ethics risks when screening counterparties. Participants often invest huge costs and spend much time screening counterparties, making it difficult to match the needs of the supply and demand of funds. The feature of blockchain, open and verifiable to the whole network nodes, can help to solve the problems. Participants can view the open market for inquiry and quotation information, which helps both parties to understand the actual needs.

In the pre-investment stage: complex due diligence processes. Under the influence of multiple factors such as an increasingly complex business environment, accelerated business model change and opaque information, it is more difficult for investors to identify transaction risks accurately, and often face difficulties such as excessive transaction valuation, problems in subsequent integration and challenges to achieve synergies. Although complex due diligence processes are conducive to ensuring transaction security and reducing transaction risk, they also bring about reduced efficiency and increased cost. Therefore, it is imperative to explore how the information that significantly impacts investment decisions in securities issuance or investment, such as an annual report, financial report, and significant matters, improves the efficiency of due diligence and reduces costs. The feature of blockchain can ensure that all transaction information is not tampered with and is trustworthy and effective through the consensus mechanism.

In the post-investment stage: difficulty monitoring. Post-investment management needs to ensure that the use of funds is consistent with due diligence and supervise the financing party. The purpose of the investment funds shall not be changed. Post-investment management relies more on tracking capital flow and monitoring enterprise business conditions, so it is difficult to establish a multi-dimensional and full-cycle post-investment evaluation and supervision system. The distributed ledger automatically operates business logic and regulatory rules through smart contracts based on consistent data among all parties. Smart contracts are transparent and open, and all parties (all nodes) will participate in the verification of the contract during the execution process. Synchronously ensure that each transaction meets the requirements of business logic and regulatory rules, automatically find problems, prevent in advance and intervention, provide a safe and credible execution environment for multi-party cooperation, and force the performance, to ensure the safety of transactions.

In addition to the above problems, exit mechanisms, fair and objective company information sources, information transparency, and other issues are also the main issues for investors in the primary market. These issues also reflect the same information asymmetry, trustworthy and practical information, mutual trust mechanism, etc. Therefore, these problems can also be solved through blockchain technology.

## 3.4 Threats to Validity

### 3.4.1 Internal validity

In this research, the survey questions are designed based on the interview's conclusion. However, it may sometimes misunderstand or fail to understand the interviewees' intentions fully. To eliminate this threat, the authors slowed down as much as possible during the interview and confirmed the content once it did not understand clearly. The card sort step is handled by two authors together, so there is the possibility of mistakes, but the authors have tried their best to avoid making mistakes.

Interviews and surveys also have the possibility of interviewees providing dishonest answers for any reason. To reduce this bias, the authors have made the following efforts in the survey: 1) In the letter of invitation, the authors stated that the research team would not publish and try their best to avoid leaking personal information (if provided) and it is entirely confidential; 2) The survey is anonymous, and it is guaranteed that it will not track the participants by answering the questionnaire content. If the interviewee wants to provide contact or other personal information, it can be added voluntarily. Based on (Ong & Weiss, 2000), confidentiality and anonymity might help obtain honest interviewees' answers.

In addition, based on the following suggestion (Kitchenham & Pfleeger, 2008), that is, to provide services to prospective respondents in an appropriate language. Besides the English version of the survey, there is also a Chinese version. The Chinese version of the survey can help Chinese respondents more easily understand the questions from the questionnaire. Again, it may also draw wrong analysis based on the answers to the survey. The authors read their answers as carefully as possible to avoid this threat.

Besides, the authors have adopted a reliability test for the questionnaire. In general, the primary consideration is the internal reliability of the scale, whether there is a high internal consistency between data. Cronbach's alpha coefficient is widely used in the reliability test. In this research, Stata software is used to test the alpha coefficient. The overall alpha coefficient of the questionnaire is 0.97, which is greater than the acceptable range of reliability of 0.7, indicating that the research has a specific reference value. In addition, the questions related to the primary market investigated by the questionnaire have undergone many discussions and revisions, and pre-investigation experiments have been carried out. Respondents generally gave authentic and accurate feedback when answering the survey questions. Therefore, the authors believe that the questionnaire has high content validity.

### 3.4.2 External validity

According to the interview strategy (Aniche et al., 2018; Singer et al., 2014), there are only 15 interviewees because the authors believe saturation has been reached. It is clear that the number of interviews is not very large, and the strategy is saturated and cannot fully represent all situations, but the interviewees have been reset to cover all essential primary market roles.

Considering that some interviewers will have some ideas or opinions that the authors might miss or have new and meaningful ideas after being interviewed by us, all interviewees are experienced. Their rich work experience will increase the completeness of the answers to open questions.

To validate the results of an interview, 54 participants were surveyed. Since most survey respondents are from China, Australia, and the United States, the authors cannot guarantee that the results apply globally. It is anonymous and does not require identity verification, so the interviewees are not guaranteed to include all participants in the primary financial market. To further improve the generalizability of the research results, the authors encourage other scholars to replicate the research with a more extensive group of participants in the future.

## 3.5 Related Work

This section highlights related work on applying blockchain technology to the primary financial market, including proposed systems to help the primary ecosystem, core technologies of blockchain, and core advantages and applications of blockchain.

Blockchain is continuously innovated and expanded on top of Bitcoin's infrastructure. At present, blockchain can be divided into the public chain, alliance chain, and private chain according to the access mechanism of nodes and the degree of decentralization. Blockchain technology has gone through the Bitcoin era of blockchain 1.0 and the blockchain 2.0 era represented by the alliance chain. Blockchain technology has transitioned to the blockchain 3.0 era represented by EOS. In terms of technical application, according to different actual application scenarios and design concepts, current blockchain projects are heterogeneous blockchains developed using different technical frameworks.

There are relatively few articles talking about the application of blockchain technology in the primary financial market in practice compared with the secondary market. However, the relevant issues still attracted the attention of some scholars.

Regarding securities issuance, Buterin (2014) points out that replacing the securitization third party in the primary market with a blockchain-based system can more accurately track process details, reduce costs, increase issuance speed, and increase transparency and liquidity. Ahmad et al. (2018) believe that the fraud issues of information asymmetry in the primary market can be reduced by adopting blockchain technology in the financial market infrastructure. It proposes a Linked Data-based model, which provides data verification and tamper-proof functions to prevent collusion and effectively increase trust in financial markets.

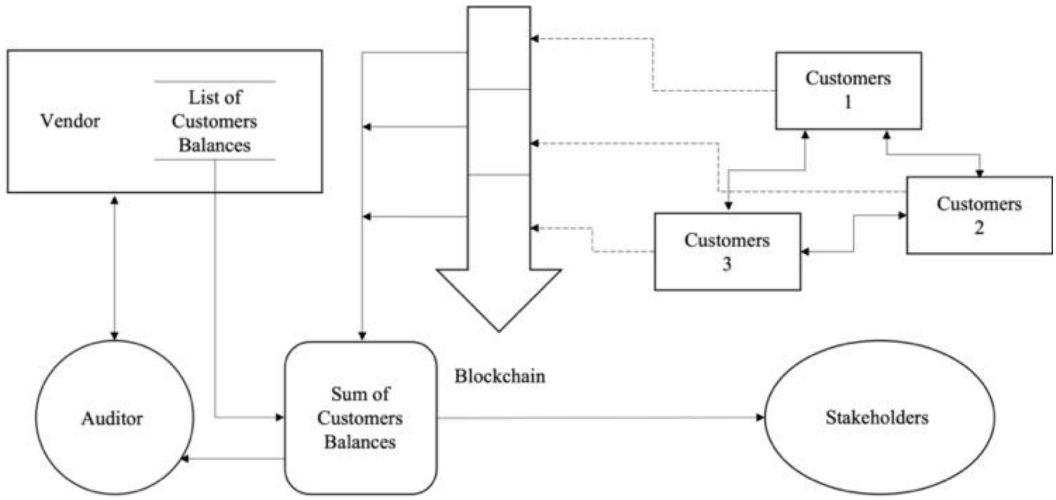


Fig. 3.4: Public and private access for accounting information system

Authorized participants may get all information on the blockchain immediately, and the information accessed by all parties is consistent, which saves a lot of due diligence expenses and probable errors in the copying process, according to Cohen et al. (2017). It proposed a prototype in Fig. 3. 4 for an accounting information system with public and private access to record the entity's access data or update the information. It will improve the accuracy of financial reporting information provided to shareholders and other approved persons. Dddder and Ross (2017) demonstrate that due diligence data is on-chain, open, and transparent, significantly increasing information transparency, reducing information asymmetry, and lowering fraud risks. It presented the ORM model in Fig. 3. 5, which includes a copy of the data before entering the database and a blockchain-verified mirror file. The blockchain will genuinely update the verified data given to the database after relaying it back to the database, preventing the original information from being tampered with.

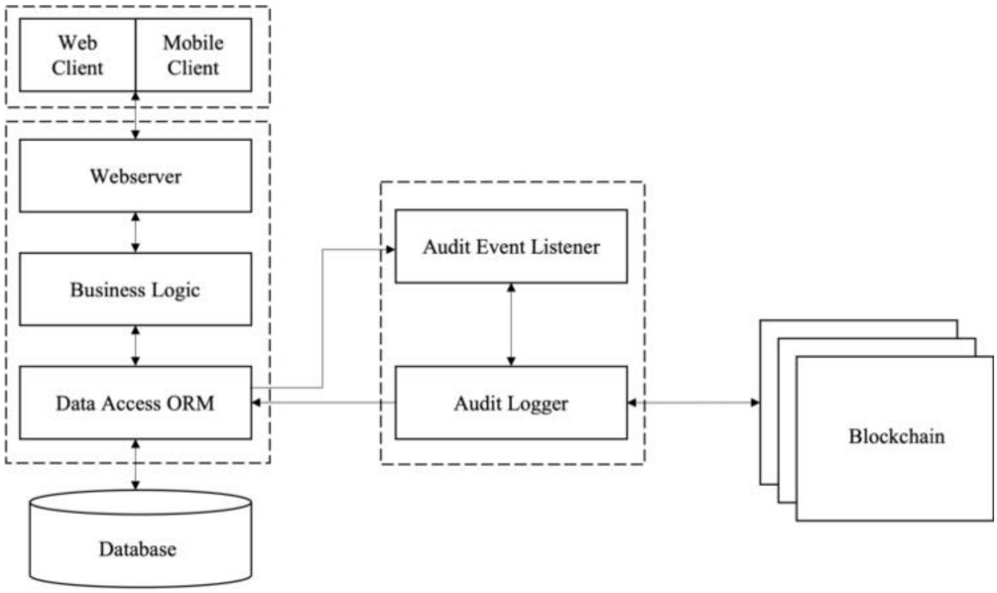


Fig. 3.5: ORM model

Scholars also debate how blockchain technology may help save expenses and increase efficiency. Tinn (2017) claims that using blockchain to promote corporate governance and legal frameworks may promote corporate transparency and efficiency when the record is established and that blockchain technology has enhanced automation. Sutton and Samavi (2017) showed that when pre-set criteria are satisfied, equity transactions may be automatically completed by putting smart contract terms into an automated programming language. More specifically, it employs machine learning to assess the desire and ability of borrowers, and it leverages a blockchain-based system to instantaneously predict the borrower's future willingness.

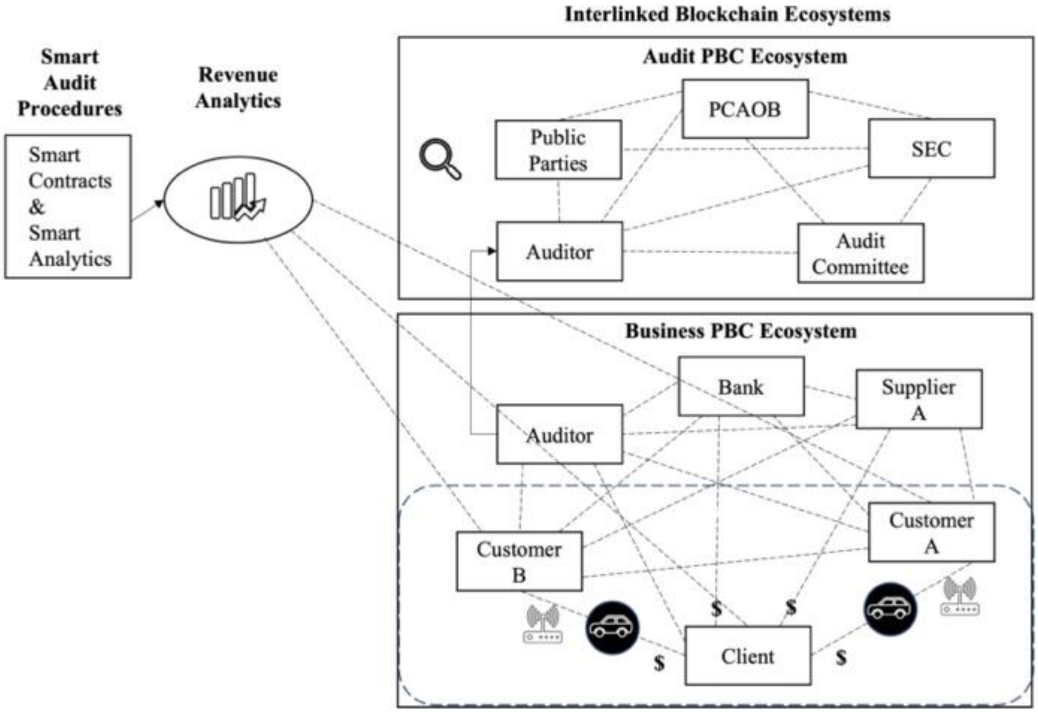


Fig. 3.6: Interlinked Blockchain Ecosystems

Furthermore, several publications are based on a governance standpoint, believing that apps aid departmental monitoring. Aitzhan and Svetinovic (2018) outline why blockchain technology can replace finance agencies and discusses the history of employing blockchain in the primary market at an early level. Lamarque (2016) describes how the supervision department identifies the nodes on the chain and acquires the public key to monitor the fundamental data in real time. At the same time, owing to the blockchain's infallibility, the information's validity and traceability are ensured. McCallig et al. (2019) show that auditing and supervision might no longer be limited to sampling but will collect and process all data via a blockchain network that is maintained and shared, in contrast to the previous architecture (Fig. 3. 6), the auditor can evaluate the data inside before going outside (Sheldon, 2019). In Fig. 3.6, the auditor system will place in the external ecosystem to prevent external institutions and customers from altering the data regularly after the auditing process. It eliminates data transmission manipulation and leakage while increasing data authenticity.

Although the deployment of blockchain in the primary market is technically viable, the present progress in practice is modest. It is mainly due to regulatory constraints and no consistent norm (Zhu & Zhou, 2016). Some current regulatory prohibitions will be lifted because of the government's acknowledgement of blockchain and the future technological progress of distributed systems.

## 3.6 Conclusion

Based on our research combining qualitative and quantitative methods, the authors concluded that the most concerning issues in the primary financial market are complex due diligence, mismatch, and difficult monitoring. When the current challenges are combined with the advantages of blockchain technology, it clearly shows that blockchain may be a suitable technology that can solve the above challenges in primary financial markets.

The blockchain has an available feature. Except that the private information of each transaction party is encrypted, market participants can query and obtain data on the blockchain through a public interface. Therefore, the information transparency of the entire system is extremely high. It is more convenient for transaction parties to obtain information, which is conducive to reducing the information asymmetry of both parties in the market, improving the matching efficiency of both parties, and faster settlement.

The use of blockchain technology can reduce the reduction in transaction efficiency and the increase in transaction costs caused by the excessively long due diligence process. Using the consensus of blockchain technology, tamper-proof, traceable features, and the automaticity of timely update of node information, all aspects of information involved in the transaction can be recorded on the blockchain. Therefore, investors can clearly understand and view the investment and, based on ensuring the credibility of assets, minimize the complicated process involved in the due diligence process.

The block-based intelligent contract technology can help non-standard off-site contracts be presented in executable code form, making it easier to realize automated transactions of non-standardized contracts. Each market participant in the blockchain has a complete transaction record, and the transaction assets are anchored on the blockchain. The conclusion of the contract becomes flat and automatically executed, which improves the ability of both parties to perform the contract and reduces the transaction counterparty risk.

For post-transaction events, like derivatives transactions and clearing, etc., rely on blockchain technology to manage the DLT network, monitor related assets, and redesign and optimize related processes, improving market transparency and enhancing the efficiency of derivatives transaction management and reducing transaction costs.

Due to the difficulty in carrying out large-scale survey activities, obtaining a large amount of research data is difficult. Although this survey has covered all types of primary financial market participants with different roles, the overall sample size is still limited. In addition to the technical, application, supervision and other factors involved in the practice, this chapter only provides a relatively comprehensive and suggestive application framework for the application of blockchain to improve the infrastructure of the primary financial market. A more continuous systematic investigation is required to grasp the application prospects of the district cross-chain comprehensively, accurately, and scientifically in the primary market. Further refinement and development have not been carried out for more specific application details involving the primary market.

Blockchain technology can potentially bring the infrastructure of the primary financial market into the next generation. Conducting a continuous and systematic investigation and research on a cross-chain application in the primary financial market is significant. In the future, the authors will focus on combining technology and business. The authors will also try to build a blockchain system to solve the existing issues in the primary financial market, according to the result of this research.

The forthcoming two chapters focus on the design and development of two systems that aim to address real issues within the primary financial market. These systems will incorporate the utilization of blockchain technology and algorithms to enhance their functionality and effectiveness.

CHAPTER 4

# i-Bond: A Next Generation Bond's Issuing Service System

The low transparency of the bond market and the asymmetric information disclosure system have impacted the bond market for a long time, which affects the high-quality development of the bond market (Stiglitz, 1989). As a distributed network system, blockchain technology has the characteristics such as being tamper-proof, transparent, open, anonymous, and verifiable execution etc. It is inherently consistent with the current limitations for the sustainable development of the bond market, which can provide new technical solutions to the limitations of alleviating the growth of the bond market.

The authors have conducted an empirical study to investigate the rules of the primary financial market in practice, which adopted a hybrid method combining interviews and online surveys (Liu, Xu, Zhang, et al., 2022). The results further confirmed some critical issues facing the primary bond issuing market: asymmetric information and low transparency. As a follow-up to the previous work, this chapter presents a design and prototype of a blockchain-based bond issuing system to address the above challenges in the bond issuing market.

The application of blockchain in the bond market can divide into two types (Mori, 2016): (1) using alliance chain technology to optimise the bond issuance process, improve efficiency and reduce costs; (2) adopting public chain technology to implement bond issuance and trading. In traditional online transactions, the parties have their ledgers, and transaction records are not interoperable. However, each party involved in a transaction has its ledger in a standard visible network to see various historical records with blockchain technology. In this way, a reliable database with tamper-proof, open, and transparent capabilities is required. Specifically, adopting blockchain technology to issue bonds is reflected in three aspects.

(1) Reducing the risk of information asymmetry in the bond issuance process. The blockchain uses distributed ledger technology, and the information on the chain is recorded in the entire network in real-time, which reduces the risk of single-node accounting failure and helps ensure information security.

(2) Reducing the cost of bond issuance and improving the efficiency of bond issuance. Smart contracts can automatically execute bond issuance, automate complex business processing procedures, and reduce manual intervention and operation costs. In addition, the completion of agreement signing certification on the blockchain can potentially replace the current offline paper agreement process and improve the efficiency of agreement signing.

(3) It is helpful for post-audit and management. Information related to bond issuance is recorded on the blockchain in a form that cannot be tampered with, which facilitates the retrospective verification of the bond issuance process in the future and reduces the workload of data verification. In addition, the information on the chain can automatically generate credible reports and statistics as needed to facilitate post-transaction management. In this chapter, the contributions of our research are as follows:

- We developed a set of concrete requirements from our previous experiment study, which was used to guide our design.
- We designed a new mechanism of bond issuing by adopting a decentralised system.
- We developed a decentralised bond issuing service system, and we conducted evaluation testing on its performance.

## 4.1 Requirement Analysis

### 4.1.1 Traditional bond market

The traditional bond issuance process usually involves several participants: issuers, investment banks, distributors, rating agencies, audit agencies, law firms, evaluation companies, etc. The traditional process can be summarised as shown in Fig. 4.1.

(1). The issuer needs to find one or more investment banks to organise the entire bond issuance, and then the selected investment banks recommend some distributors to conduct bond sales services better.

(2). Subsequently, the issuer must hire a law firm, audit firm, rating agency and other tripartite institutions to analyse the issuer's solvency.

(3). After all institutions have performed due diligence and issued the required reports, the investment bank will submit all the materials to the regulation institutions to apply for bond issuance.

(4). After the exchange approves, the investment bank will lead all distributors to issue bonds.

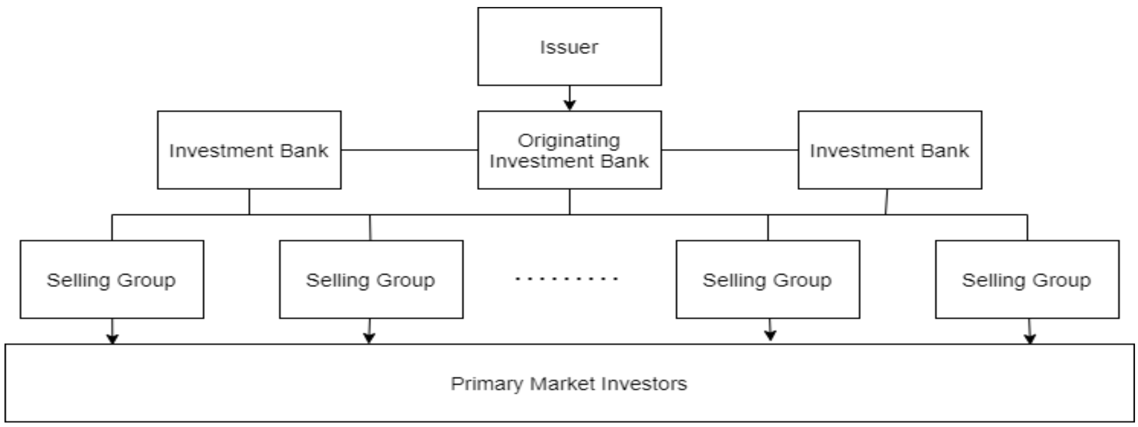


Fig. 4.1: A Traditional bond issuance process. Traditional bond issuance process

## 4.1.2 Limitations on traditional bond issuance process

Due to a lack of standardization, information asymmetry, fraud, and the high cost of due diligence, the primary financial market has developed into a highly fragmented ecosystem structure. With the increasing development of the securities market, higher requirements are placed on transaction costs, transaction efficiency, and transaction transparency. The cumbersome nature of such a business process cannot meet the needs of investment and financing entities. Even though industry and academia have attempted to change this status quo, no significant changes have been noticed (Mori, 2016). Without solving the challenges listed above, it is difficult to optimize the infrastructure of the primary financial market.

The financial market's asymmetric information and low transparency issues can be reflected in high bond issuance costs. Bond issuance costs mainly refer to the debt financing costs of a company. Issuance costs are generally relatively high and cannot be omitted when calculating the cost of capital. Specifically, bond issuance costs include the lead underwriter and underwriting syndicate fees, other intermediary agency fees (including accounting firm fees, credit rating agency fees, law firm fees, asset evaluation fees (if any), and regulatory bank fees (such as Yes)) etc.

The underwriting expense of bond issuance has a specific proportional relationship with the financing scale. The relevant regulatory agencies stipulate the underwriting fee rate of certain types of bonds, and there are also some types of bonds with different costs. The relevant regulatory agencies have not issued guiding fee rate guidelines. The specific lead underwriters and underwriting group fee collection standards can be referred to for certain types of bonds. The lead underwriter and underwriting syndicate fees are typically paid after the bond issuance. The average underwriting fee for investment-grade and junk bonds has been 0.7% and 1.2% in recent years (Manju, 2018).

There are extra intermediary agency fees in the market. Other intermediaries for bond issuance mainly include accounting firms, credit rating agencies, law firms, asset appraisal companies (if any) and regulatory banks (if any). These fees are the fees that need to be paid when issuing securities due to hiring the intermediary, as mentioned earlier, agencies to deal with issues related to the issuance.

Besides, if the issuer's credit rating is not high enough to reduce the coupon rate of corporate bonds, it can pay for additional guarantors to increase the credit rating of corporate bonds.

At this time, a guaranteed premium need to be considered. It ranges from 1% to 5% of the total issue amount (Manju, 2018).

In addition to paying high issuance costs, the issuance of bonds must also consider time. According to the report of The Organisation for Economic Co-operation and Development, globally, the preparation time for the issuance of bonds is usually not less than 5.5 months. In extreme cases, it can even reach over two years (Çelik et al., 2019).

Therefore, under the traditional bond issuance system, it is incredibly costly in terms of money and time.

### 4.1.3 Requirement specifications

Based on the content above, we designed the following system with blockchain technology as the core to solving the issues mentioned. In the proposed system, the issuance process can be divided into three steps: the submission of legal documents before the issuance, the auction of bonds at the time of issuance, and the supervision of funds after the issuance.

i-Bond will replace the underwriter to complete the bond sale responsibilities. Therefore, we can simplify actors as third-party institutions, investors, and issuing companies. The core functions of the system will also be changed. The changed functions are uploading, bidding, bidding, settlement, and supervision. The system includes the following features:

R1. The platform consists of three types of users. Bond issuers and investors are the main interaction objects of the system. Third-party institutions only need to submit relevant legal documents before bond issuance.

R2. Before the bond issuance, third-party institutions must submit documents such as guarantee letters, financial statements, credit ratings, and legal certifications. These documents will be stored in the shared repository for investors to review.

R3. After the relevant documents are ready, the issuer must initiate pricing and auction successively so that investors can evaluate and bid on them.

R4. The Investors can participate after receiving the news of pricing and auction if they are interested in investing. It is worth noting that in the auction link, investors need to mortgage the related property before participating in the price.

R5. The system will set the initial auction price according to the market trend.

R6. Investors who have won the bid will have the right to purchase a corresponding bond amount.

The online bond issuance bookkeeping process is standardized, intelligent, and transparent with a blockchain-based bond issuing system. The system uses blockchain technology to design smart contracts for bond businesses and ensure credible information sharing through a consensus mechanism. On the one hand, it realizes the on-chain certificate deposit. Essential information, such as bond details during the bond issuance process, is uploaded to the chain in real-time to realize distributed bookkeeping. On the other hand, it realizes the grouping on the chain. After the underwriting group is formed, the system will use the CA certificates of each participant to complete the group signature verification on the blockchain layer one by one.

## 4.2 Architecture Design

The system design is based on the core concept of parallel split (Zhang et al., 2006) and horizontal expansion (Jenkins & Strauser, 1999) at the service architecture level. It splits services according to business functions to achieve loosely coupled parallel operation of the system. At the same time, through a horizontal expansion and fault-tolerant recovery mechanism, the new services can be quickly deployed and released in grayscale, improving the system's agility. At the level of process construction, the system realizes multi-role, sub-authority online interaction, promotes paperless and online operations, and reduces the number of manual operations. In addition, multi-dimensional monitoring of the bond purchase process facilitates the real-time presentation of issuance dynamics.

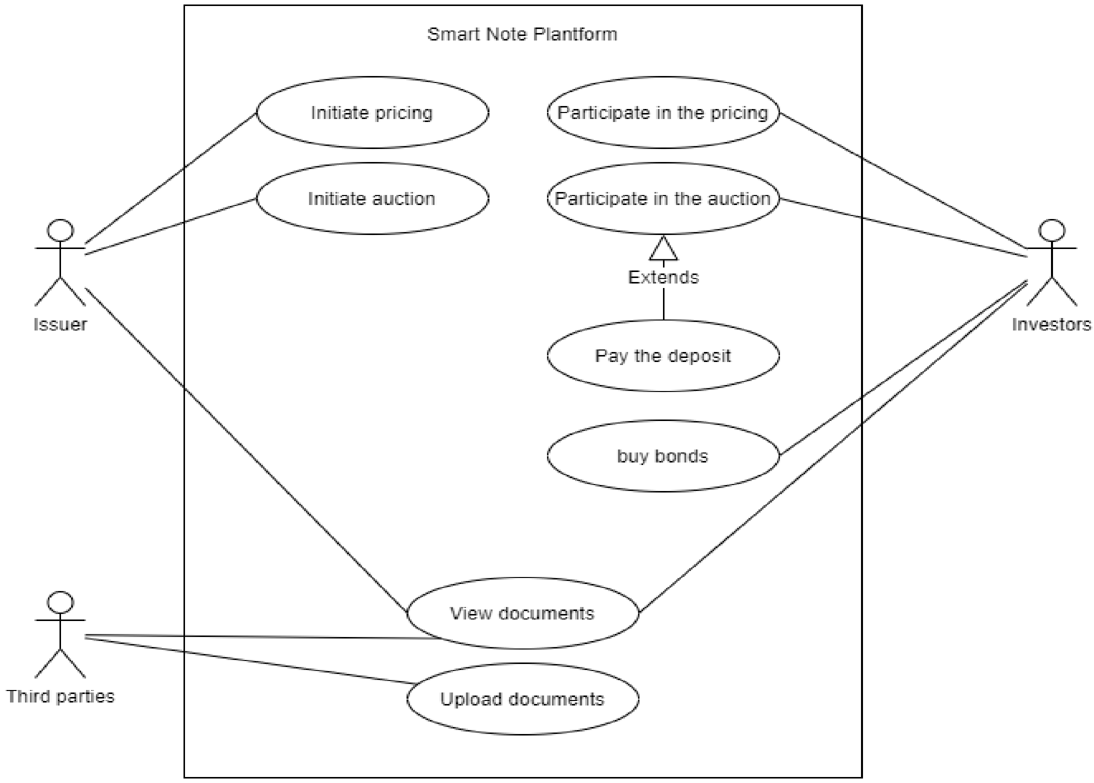


Fig. 4.2: Key roles in i-Bond

Fig. 4.2 demonstrates the overall use case diagram of the i-Bond. In the system, there are three organizations of users, called the Issuer, Investor and Third Party. All of whom can register and log in to their account type. Aside from account registration and sign-in, Third Party users can also view and upload files to the blockchain. Issuer users can view pricing submitted by the Investor users and the bidding information. Investor users can submit pricing and bidding and pay for their biddings.

Based on the above-designed functionalities, there are four layers in the system. Fig. 4.3 shows the architecture of i-Bond and how different components interact.

This system mainly comprises two layers: the presentation layer and the business layer. The system has three target users: issuer, investor, and third-party organization. The display layer interacts with the target users, which can provide users with all operations related to bond issuance. All users have access to the presentation Layer. The front-end users can issue and trade bonds, set bidding, upload files, download files, and use the wallet in this layer.

The front-end application will obtain or transfer the required data to the business layer through the API. With the Hyperledger Fabric API, the system's front end can interact with the smart contract stored in the blockchain network at the business layer. Smart contracts are deployed on the Hyperledger in the data layer, and the system relies on it to maintain the operation of the entire program. Smart contracts can manage to trade and clear instructions for account holders, e.g., deposit and withdraw from the user's wallet, logging in or out, uploading files accordingly, etc. From the view of business model, Hyperledger is the trade off solution for centralized and decentralised systems, as the system is designed as a semi-environment for all users.

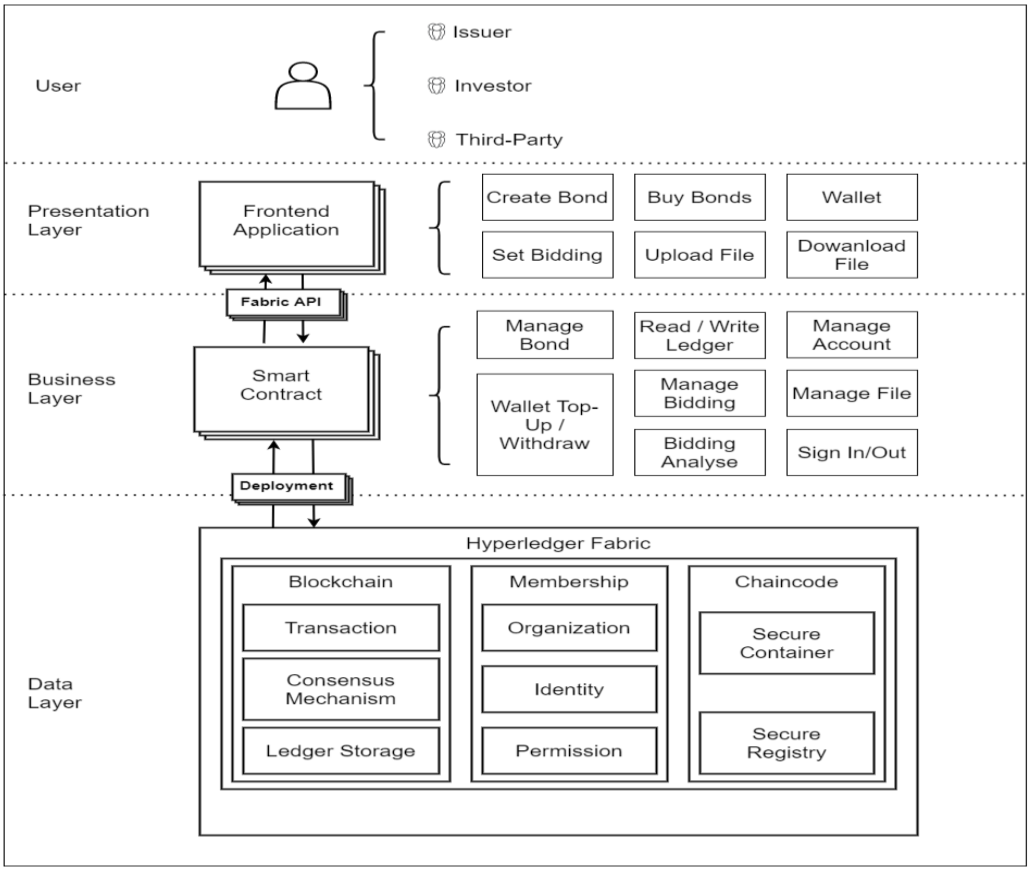


Fig. 4.3: Architecture of i-Bond

## 4.2.1 Data layer

In this architecture, the bottom layer is the data layer. Since the authors use Hyperledger Fabric as a platform to develop the project, all data will be stored in Hyperledger. The structure diagram of Hyperledger includes block management, member management, and Chaincode management, which means a high level of data security.

This project uses the latest version of Hyperledger 2.3, which can make progress not hindered by the defects of the old version and ensure that the project will not be required to update in a short time due to the rapid upgrading of technology. The system has a channel to deploy smart contracts when building Hyperledger. All transactions and records in the system are transmitted through this channel. In addition, three organizations were added to the channel when creating a network, representing the system's three identities of issuer, investor, and third parties. Each organization generates a CA server that issues certificates for all users in the organization to verify that new users added are valid users. Each newly joined user (peer) generates an MSP (Member Service Provider) that provides authentication when conducting transactions. Therefore, the system can also automatically identify the current user's identity through this mechanism and provide related services.

## 4.2.2 Business layer

The business layer is above the data layer. The business layer is mainly implemented by smart contracts written in Javascript. Javascript is selected as the programming language of chaincode, as it is the most popular language in writing smart contracts compared with all other languages. In this project, all business logic (e.g., bidding management, bidding analysis, bond quote, document management) will be processed through smart contracts, and the necessary data will be written into the ledger and stored in the blockchain.

Smart contracts are the core of communication between the system and the blockchain. The storage method of data in Hyperledger consists of key-value pairs. After the smart contract gets the parameters returned by the system, it calculates and stores the necessary data in the blockchain.

Hyperledger provides three primary operations: put, get, and delete, which are sufficient to meet all our requirements for data storage and modification. The project's smart contract is mainly composed of two parts: TokenERC20Contract and SmartNote. The authors adopted the ERC-20Token standard regarding currency transactions to make the system's currency management and transaction processes more standardized. In order to meet the ERC-20 standard, the system implements many methods declared in its interface, such as totalSupply, transfer, balanceOf, approve, etc. After perfecting these methods, the system can get a complete currency transaction method. The SmartNote contract is mainly used to provide business services for the system. It covers many functions, such as bond management, bidding management, document management, etc.

When logging in, the system will generate a Transaction ID as the user's id. The data security level is high since the blockchain obtains the Transaction ID through algorithms such as hash. For security reasons, we use not only the user ID but also the Bond ID and File ID, and we use Transaction ID as their unique identifier. However, these transaction IDs are often very long due to Hash calculations and poor readability.

Therefore, the authors have added the name attribute to Bond and File separately. When the user queries and browses the bond, the name will be used for identification, and only the internal processing of the system will select the Transaction ID as the identification code. This dramatically improves the system's ease of use and makes it easier for users to find and remember a bond.

### 4.2.3 Presentation layer and user layer

The top layer of the architecture is the display layer. JavaFx is chosen for the UI section. As JavaFX has its UI component library and runs in the Java virtual machine, the entire system can maintain the same UI interface no matter which system it runs in. Since it can obtain the current user's identity when the system is started, it can omit the login interface and jump directly to the organization's interface (Issuer, Investor or Third Party) to which the user belongs. In addition, the system can use the API and SDKs provided by Fabric to call smart contracts to achieve data interoperability between Java and Javascript.

The system needs to use the Gateway class in the SDK to establish a connection with the blockchain and then use the getNetwork() method to find the channel to which the current system belongs when the frontend needs to call thnally, using the getContract() method to obtain the required smart contract, and then passing in the parameters and the name of the contract method to be called in the evaluateTransaction() method so that a call to the smart contract can be completed.

## 4.2.4 System flow design

Fig. 4.4 shows the Business flowchart for this project. A brief description lists below:

(1) Third-party organizations submit relevant legal documents to the system

(2) Interested investors review and analyze these documents

(3) The issuer initiates the first round of pricing contracts

(4) Investors give the corresponding price for the bond based on their analysis, and the system will calculate a price range by itself

(5) The issuer initiates the second round of bidding contracts

(6) Investors pay a deposit for bidding, and the deposit will be returned after the bidding is over

(7) The winning investor buys bonds

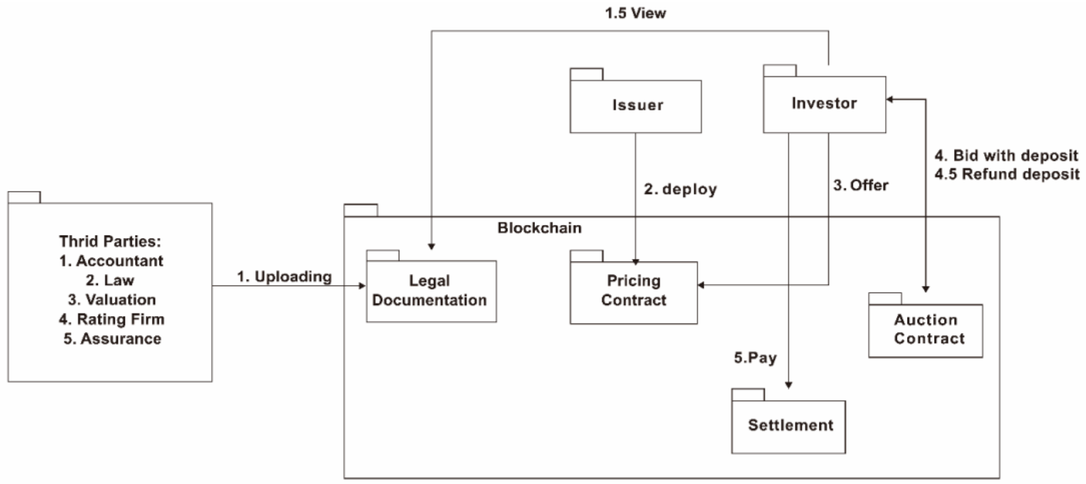


Fig. 4.4: Business flow chart

## 4.2.5 Model design

### 4.2.5.1 E-R diagram design

The E-R diagram clearly shows the attributes of the data objects and the connections between the data objects. Through the E-R diagram, we can more directly understand the possible interactions of the various objects in the system and the attributes they need. Here we select Account and Bond as the representatives of the entities for description.

The account contains 6 attributes: ID, Name, Balance, Bonds, E-mail and Type. Balance records the funds held by the account. All funds in this system will be managed through ERC20Token. Type distinguishes whether the account belongs to Issuer, Investor or Third Party. The bond contains 10 attributes. Advertised records whether the bond needs to be placed in the front of the list; Rate records the interest rate range of the bond in the auction; Files records all file IDs related to the bond.

E-R diagram of the entire system is shown in Fig. 4.5. An Issuer can create multiple bonds and hire multiple third-party agencies to provide legal documents. An Investor can view multiple documents and purchase multiple bonds. Each bond can have multiple legal documents, and each legal document can only belong to one bond.

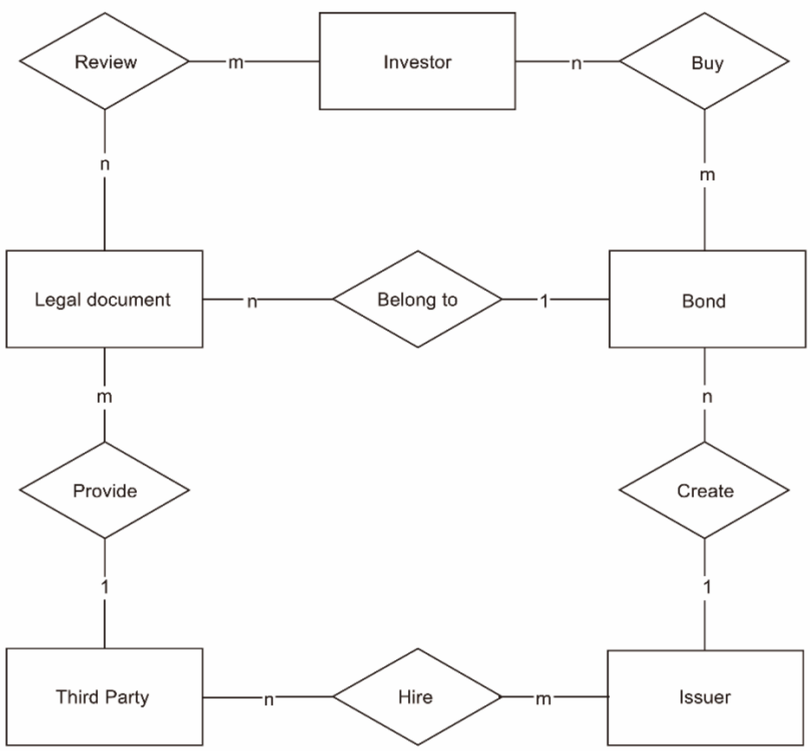


Fig. 4.5: System E-R diagram

#### 4.2.5.2 Data Model Design

As Hyperledger's data storage method is limited to storing key-value pairs, it is impossible to design a database like a traditional project. The following modes are used to clarify the required attributes of an object:

a) Account Model

Table 4.1: Account model table

| field | Type |
|---|---|
| ID | String |
| Name | String |
| Balance | Double |
| RelatedBonds | String[] |
| E-mail | String |

b) Bond Model

Table 4.2: Bond model table

| field | Type |
|---|---|
| ID | String |
| Name | String |
| ownerId | Double |
| amount | String[] |
| price | String |
| rate | String |
| interest | Int |
| tpId | String[] |
| status | String |
| advertised | Boolean |
| endTime | Date |
| files | String[] |
| Bids | String[] |

c) File Model

Table 4.3: File model table

| field | Type |
|---|---|
| ID | String |
| Name | String |
| relatedBond | String |
| Content | String |

## 4.3 Issuance Mechanism and Auction Algorithm Design

According to the theoretical models of Holmberg (2009) and Wang and Zender (2002), the issuance mechanism of the primary bond market is discussed.

### 4.3.1 Market participants

Market participants involved in bond issuance mainly include:

(1) Financing party (sell-side)

The financier plans to issue a certain number of bonds for financing. The total amount of financing is $Q$, and the face value of the bonds is $v^t$. Before issuing bonds, the financier will select an underwriter and entrust the underwriter to organize the public bidding and issuance of bonds.

(2) Investors (buy-side)

There are potential bidders' amounts $n(n \geq 2)$ in the market, and any bidder $i(i = 1, 2, \cdots, n)$ has an appraisal value $v_i$ of the bond, and the appraisal value of each other is kept secret. The bidder $i$ has a quasilinear utility function:

$$U_i(q_i, v_i) = u_i(q_i, v_i) + e_i \tag{1}$$

Where, $q_i$ is the number of bonds that won the bid, and $e_i$ represents other costs. It is assumed that the utility function is a quadratic function $u_i(q_i, v_i) = v_i q_i - 0.5\alpha q_i^2$, $\alpha$ which is used to measure the convexity of the utility function, which reflects the risk aversion of the bidders. The bidder's utility function is $mv(q_i, v_i) = v_i - \alpha q_i$ . After the issuing of bonds, the bonds will be re-priced through transactions in the secondary market. At this time, bidders who hold the same amount of bonds will face the same market value, that is $v_i = v$ . The strategy $b_i$ of a bidder $i$ is a function of demand and value, which is $b_i(v_i, q_i): \mathbb{R}_+^2 \to \mathbb{R}_+$ .

(3) Platform (exchange)

The platform signs an underwriting agreement with the financier to provide services for bond issuance, which mainly includes formulating issuance rules and organizing the issuance process but does not participate in actual transactions. In addition, bonds issued on the platform are standardized products. Standardization can be understood as splitting bonds into equal $Q$ parts, corresponding to the size of financiers issuing bonds. According to the Bayesian Nash equilibrium, starting from the maximization of the overall benefit, the mean number of bonds per bidder is $\overline{Q} = Q / n$, where the joint distribution function of $\overline{Q}$ and the face value $v$ of the bond is $F\left(\overline{Q}, v\right)$.

## 4.3.2 Bidding and issuance mechanism

### 4.3.2.1 Bidding process

The bidding process adopts a sealed quotation, and the bidder directly reports the assessed value of the bond (according to the bond pricing principle, each corresponds to a quotation rate) and the number of bids on the platform. Specifically, any bidder's offer consists of a series of “price-quantity”. The timing of the bidding game is as follows:

Step 1: The platform announces the bidding rules. The platform organizes the bidding process and announces the bidding rules, mainly including reserved price (or interest rate), configuration rules and payment rules, etc., and the bidding begins.

Step 2: Investors bid. Investors make quotations after understanding the bidding rules, which comprise a series of “price-quantity”, the bidding strategy function $b_i\left(v_i, q_i\right)$.

Step 3: Transaction and payment. The platform sorts the investors’ quotations from high to low (or from low to high bidding rates) and wins the bids in turn until the scale of the financing plan of the financier is met. When determining the equilibrium issue price $v^e$, the platform will add up the bidders (bidders who satisfy $r_i \le r_0$) that satisfy the financier’s reservation price in advance ( $v_0$, the corresponding reservation interest rate $r_0$ ) to obtain the total market demand. According to the principle of equal supply and demand $Q = \sum_i q_i\left(v^e\right)$, the equilibrium price (corresponding equilibrium interest rate $r^e$ ) is determined, generally greater than or equal to the reservation price $v_0$ given by the financing party in advance. Then, configure and pay accordingly according to the bidding rules, and the bidding ends.

#### 4.3.2.2 Issuance mechanism

The issuance mechanisms commonly used in the bond issuance market include the Dutch and American issuance mechanisms. When the Dutch issuance mechanism is adopted, the winning bidder subscribes for the number of bonds awarded at the same price (usually the lowest price of all winning bids, that is, the highest winning interest rate). When the American-style issuance mechanism is adopted, the winning bidders subscribe for the number of bonds won at their respective quoted prices (or the weighted average of the winning prices, that is, the weighted average winning rate). Considering that most of the bonds in the market currently use the Dutch issuance mechanism, this chapter focuses on the Dutch issuance mechanism, allocation rules and payment rules. The specific provisions are as follows:

Configuration rules: bidders whose bids exceed the equilibrium price will win the bid, and the winning bidder will obtain the quantity corresponding to the equilibrium price $q_i^e = q_i\left(v^e\right) = \left\{q : b_i\left(q, v\right) \geq v^e\right\}$.

Payment Rules: The winning bidder will pay all the winning bond quantities at the equilibrium price, with a total payment of $pay_i^{DBM} = q_i^e \times v^e$.

#### 4.3.2.3 Equilibrium price of bidders

It is assumed that the game of all parties in the bidding process is a game of incomplete information, and its corresponding equilibrium is a Bayesian Nash equilibrium. The expected utility of each investor is maximized given the probability distribution of the investor and other participants' choices (“winners”/”not winners”), so that no player is willing to change its behaviour or strategy. Based on the above assumptions, define the investor's return function as $U\left(q_i, v_i\right) - pay_i$, and the investor's expected return as $ER\left(q_i\left(v_i\right)\right)$, then the investor's expected return is maximized as

$$\max ER(q_i(v_i)) = \Pr ob\left[b\left(q_i, v_i\right) \geq v^e\right] \times E\left[U\left(q_i, v_i\right) - pay_i \middle| b\left(q_i, v_i\right) \geq v^e\right] \quad (2)$$

Where, $\Pr ob\left[b\left(q_i, v_i\right) \geq v^e\right]$ represents the probability of the investor winning the bid, and $E\left[U\left(q_i, v_i\right) - pay_i \middle| b\left(q_i, v_i\right) \geq v^e\right]$ represents the conditional expected return of the investor winning the bid. Based on the linear Bayesian Nash equilibrium model (Holmberg, 2009; Wang & Zender, 2002), the investor's equilibrium quotation is a linear function of demand and value, Specifically, at equilibrium, given that other investors adopt a linear quotation strategy, an investor using a linear quotation is a weakly dominant strategy. Define the supply function faced by the investor:

$$S\left(\overline{Q}, q_i, v_i\right) = n\overline{Q} - \sum_{j \neq i} q_j\left(v_j\right) \quad (3)$$

From the perspective of marginal utility, the equilibrium price is the price at which the investor's demand is equal to its supply, which is $q_i\left(v^e\right) = S_i\left(v^e\right)$. On this basis, the inverse supply function faced by investors $i$ is $p\left(\overline{Q}, q_{i,} v_i\right) = c(q_i, v_i) + k_i S_i$, where $p$ is the bond price; $c(q_i, v_i)$ is the intercept term, and its distribution function is expressed as $G(\bullet)$ (the probability density function is $g(\bullet)$), which can be obtained $k_i (k_i \geq 0) = \partial v^e / \partial q_i, \partial c(q_i, v_i)/\partial q_i < 0$ by $F\left(\overline{Q}, v\right)$.

Under the Dutch issuance mechanism, the winning bidder purchases the bond shares obtained at a uniform equilibrium price. According to the maximization expression of the expected revenue of the winning bidder, the first-order condition for maximizing expected revenue is obtained, that is, marginal utility and marginal cost are equal:

$$v_i - \alpha q_i = p_i + k_i q_i \tag{4}$$

Where the left side of the equation is the investor's marginal utility, the right side of the equation is the investor's marginal cost (or marginal expenditure), $p_i$ represents the price of an additional unit of the winning bond, and $k_i q_i$ represents that the high quotation may lead to an increase in the equilibrium price, thereby increasing the price of the winning bond. From the above equation (4), the investor's optimal quotation function can be obtained as:

$$q_i = \frac{v_i - p_i}{k_i + \alpha} \tag{5}$$

To get the investor's optimal value $q_i$, it is necessary to obtain the optimal value $k_i^e$ in the equilibrium state. In the equilibrium state, other investors $j(j \neq i)$ adopt the optimal quotation strategy of the above equations, and this time $k_j(j \neq i)$ becomes $k_j^e(j \neq i)$. Substitute Equation (5) into the market clearing condition $q_i = S_i = n\overline{Q} - \sum_{j \neq i} q_j\left(v_j\right)$ to obtain the investor's equilibrium quotation condition as follows:

$$p_i = v_i + \left( \sum_{j \neq i} \left( k_j^e + \alpha \right)^{-1} \right)^{-1} \left( q_i - n\overline{Q} \right) \tag{6}$$

Therefore,

$$k_i^e = \left( \sum_{j \neq i} \left( k_j^e + \alpha \right)^{-1} \right)^{-1} \tag{7}$$

It can be shown that in the case of $n > 2$, there is a unique and symmetric equilibrium solution for the system of equations formed by equations (7). Solve to get:

$$k_i^e = k_j^e = \frac{\alpha}{\alpha - 2} \tag{8}$$

Substituting the above (8) into (5), the bidder's linear Bayesian Nash equilibrium bid function is obtained as:

$$q_i^e = \frac{n-2}{\alpha(n-1)}(v_i - p_i) \tag{9}$$

Further averaging the equilibrium quotation function (9), according to the market clearing conditions, the equilibrium quotation faced by investors is obtained as:

$$v^e = v_i - \frac{n-1}{n-2}\alpha\overline{Q} \tag{10}$$

Thus, $v^e < v_i - \alpha\overline{Q}$, the investor's equilibrium offer will be lower than its true marginal value for the bond.

The equilibrium price may be obtained through a specific algorithm while running the system in the future. At present, for the algorithms to solve the Nash equilibrium, there are mainly algorithms for finding stable fixed points in GANs (such as gradient descent, optimistic mirror descent, and simultaneous gradient descent), Symplectic Gradient Adjustment, Mean-Based Learning Algorithms, etc.

## 4.4 Tests and analysis

We implemented our design and algorithms using Hyperledger blockchain technology and deployed the system onto Amazon Cloud for performance testing. The authors used baseline and stress tests to evaluate the system's performance. The server's performance is tested in terms of response time and throughput. Response time is measured under a variety of circumstances. On the other hand, throughput is used to measure how many requests the server can handle in the given unit of time (ordinarily a second).

The testing environment is shown below: AWS EC2 instance having 16 vCPUs, 3.3 GHz AMD EPYC 7R32 processors and 32GB RAM was used to run the test benchmark platform. The AWS EC2 instance ran Ubuntu 20.04 LTS and peers, CA, orderer, and Caliper with Fabric release v2.3.0. Each component of the Hyperledger Fabric, including 3 peers, 1 orderer and 1 Certificate Authority (CA), was launched as a Docker container. The results were obtained by putting the network under a static load of 500 transactions (sending rate is adjusted to maintain 500 unprocessed txs in the network).

For write txs:

(1) AddIssuer, AddInvestor, and AddThirdparty add new acting parties into the system, and the parameters (company name, contact detail, id, etc.) are randomly generated.

(2) Then SubmitBond is benchmarked because the operation depends on existing parties in the system (added in step 1). Party ids in the parameters are randomly picked from existing parties, while other parameters, such as bond ID, are randomly generated. Bond data model can be found in the architecture section.

(3) Then StartFirstBidding, SubmitInterest, and EndFirstBidding are benchmarked in order because the operations depend on existing bonds in the system (added in step 2). Bond ids/Party ids in the parameter are randomly picked from existing bonds/parties, while other parameters are randomly generated. (Algorithm for the first bidding can be found in the algorithm section.)

(4) Then StartSecondBidding, SubmitBid, and EndSecondBidding are benchmarked in order (The algorithm for second bidding can be found in the algorithm section). Bond ids/Party ids in the parameter are randomly picked from existing bonds/parties, while other parameters are randomly generated.

For read txs, ReadItem is the operation to obtain an object by id. Ids for each object type are provided to the operation when benchmarking. The ids are picked randomly from existing objects created in steps 1-4 above. Object types include Issuer, Investor, Third-party, bond, interest, and bid. The test results show in table 4.4.

In summary, the server does offer high availability and reliability both write and read. The latency is acceptable. Moreover, throughput is enough to handle the workload.

Table 4.4: Test results

| | **Throughput (TPS)** | **Latency (s)** |
|---|---|---|
| AddIssuer | 227.4 | 1.15 |
| AddInvestor | 214.9 | 1.23 |
| AddThirdParty | 230.4 | 1.1 |
| SubmitBond | 193.2 | 1.48 |
| StartFirstBidding | 208.5 | 1.28 |
| SubmitInterest | 185.3 | 1.56 |
| EndFirstBidding | 190.7 | 1.46 |
| StartSecondBidding | 203.3 | 1.33 |
| SubmitBid | 190.5 | 1.4 |
| EndSecondBidding | 179 | 1.54 |
| ReadIssuer | 447.3 | 0.01 |
| ReadInvestor | 442.3 | 0.01 |
| ReadThirdParty | 422.7 | 0.01 |
| ReadBond | 426.7 | 0.01 |
| ReadInterest | 424 | 0.01 |
| ReadBid | 433.2 | 0.01 |

## 4.5 Related Work

Exploring the application of blockchain technology to the issuance of bonds in the primary market can start from two aspects: bond pricing using digital currency and bond contracts using smart contracts. Currently, the main parties involved in traditional bond issuance on the primary market include accounting firms, law firms, rating agencies, guarantee agencies, underwriters and other service agencies, and there is a lack of information sharing among these parties. Due to insufficient trust mechanisms, low cost of fraud, and easy collusion between service agencies and issuers, the information disclosed by issuers may have fraud, causing investors to suffer losses due to information asymmetry. Blockchain technology can price the currency from the bottom. Take precautions concerning bond contracts.

### 4.5.1 Credit analysis research

After the use of blockchain technology to popularise digital currency, due to tamper-proof, the issuer's accounting system and cash flow system will be more transparent than it is now (Kolehmainen et al., 2021). Credit risk information such as financial fraud, legal disputes, financial deterioration, and misappropriation of funds that investors are worried about can be monitored (Hyvärinen et al., 2017). The quality of corporate information will be significantly improved, prompting corporate operations to focus more on the main business. With the introduction of blockchain technology, credit analysis research may be weakened, which also means that the role of service agencies in the future will be weakened, financial statement fraud can be eliminated technically, and the workload of credit rating agencies and accounting firms will be reduced (Garg et al., 2021). The record of information on the blockchain has strongly promoted the formation of financial decentralisation and flattening (Ye & Zeng, 2021).

### 4.5.2 Issuer information disclosure

In the current state, if an issuer has credit risk defaults, regulators, banks, and lead underwriters need to verify the flow of funds for pedestrians, which will cost colossal human resources, material, and financial resources. By adopting blockchain technology, the immutability of data and the retention of decentralised nodes will significantly reduce audit costs and improve the timeliness of information disclosure (Yu et al., 2018).

Investors can also grasp information promptly or get feedback from the issuer, helping functional agencies such as the debt committee improve credit monitoring efficiency. In addition, with the application and maturity of blockchain technology, small and medium-sized enterprises with good financial status may have more comprehensive qualifications than large enterprises that currently have bond issuance qualifications, thus playing the role of survival of the fittest (Joo et al., 2019). The precise positioning of the issuer's qualifications is conducive to investor protection, improves the availability and allocation efficiency of funds for SMEs, and enables financial support for the real economy to be more effectively implemented (Blemus & Guégan, 2020).

### 4.5.3 The application of smart bond contracts

Smart contract was proposed by Szabo (1996), and their essence is to use programs to process contract terms intelligently. However, due to the limitations of the technical conditions at the time, smart contracts have not been widely used. In recent years, blockchain technology's programmable, traceable, tamper-proof, and decentralised characteristics have quickly promoted the development of smart contracts. Combined with the features of automatic execution and smart execution of smart contracts, smart contracts can be naturally applied to financial scenarios (Cong & He, 2019).

Specific to the bond market, smart bond contracts can realise the connectivity of various markets by adding bond parameters (bond elements, legal text, pledge conditions, etc.) and using standardised codes in bond transactions to reduce the supervision costs of bond regulators or industry associations. At the same time, it will help reduce the corporate default rate and the cost of bond issuance, improve the bond issuance process, and promote a healthier development of the bond market (Tian et al., 2021).

### 4.5.4 Industry practices

In August 2015, the smart contract platform Symbiont announced the first issuance of "smart securities" in the Bitcoin blockchain (Smart Securities, 2015). In May 2018, the Russian Federation Sberbank completed Russia's first block-based Chain of commercial bond transactions (Sberbank, 2017). In October 2019, Deutsche Bank's first digital bond was successfully issued on the EOS blockchain (EOS Go, 2019). In December, the Bank of China (2019) launched the first domestic bond issuance system based on blockchain technology. In September 2020, the Singapore Stock Exchange announced on its official website a digital bond project that had just been completed (SGX, 2020). In November 2020, China Construction Bank planned to sell digital bonds worth USD 3 billion on the blockchain based on Ethereum technology (Alun, 2020). Although subsequent issuances are cancelled, it is symbolic of using blockchain technology for bond issuance.

## 4.6 Conclusion

This chapter mainly focuses on the issues faced by the practical application of blockchain in bond issuing. The involvement of blockchain in a bond issue, trade and settlement will weaken the reliance on financial intermediaries. Bond issuers and investors can achieve self-certification through blockchain transactions and historical behaviours. Thus, they can gain the trust of each other and trade freely without limitations from a central system. It will help the bond issue market to decrease fraud and collusion. From the view of financial infrastructure, it will balance digital transaction efficiency, supervision efficiency, offline production relations, and social distribution patterns.

Theoretically, technologies such as blockchain should be fully utilised to explore further how to improve the digital trading mechanism of the bond market. Technically, there are still many problems in the current blockchain bond trading system worthy of further analysis and Research:

(1). Extending the ring signature technology (multi-party authentication mechanism) proposed in this chapter to other blockchain transaction systems is significant. It maintains distributed ledger data jointly by nodes and must consider the issue of privacy leakage. It is necessary to use ring signature technology in other applications of blockchain to provide privacy protection.

(2). Research on consensus protocols with faster transaction processing speed is still an essential topic in the blockchain field. The demand for transactions processed by the blockchain transaction system will increase with the continuous development of network technology. Continuous improvement based on the consensus protocol proposed in this chapter can increase the processing speed of the blockchain system in an open distributed network.

(3). Studying the specific details of the reward distribution scheme in the blockchain system is of great significance for maintaining the system's security. The consensus protocol proposed in this chapter should share block rewards by members of the verification group, but this chapter does not set a reward distribution scheme. The reward mechanism in the blockchain transaction system is an essential guarantee for motivating nodes to maintain blockchain data jointly.

CHAPTER 5

# Risk Monitor System for Blockchain-based Security Issuing System

The debt market is the largest financial asset market in the financial market, and its size reached 126.9 trillion USD in 2021 (SIFMA Research, 2022). Under the traditional bond issuance system, the bond is mainly issued through government-based exchanges in various countries and then traded within each issuing exchange. With the birth of the concept of the digital economy, more and more industry experts and scholars are considering whether a distributed system can be used for bond issuance (Codagnone & Martens, 2017). Under the traditional exchange issuance system, the friction cost is too high. According to Informa statistics, the average cost of bond issuance in 2021 is 3.7% of its issuing size (Informa, 2022). Among them, 72% is used for investment banking-related institutions, 15% is used for third-party service institutions, and 13% is used for friction fees in exchanges. Adopting a decentralized issuance can reduce various costs, increase efficiency, and reduce systemic risks (Fung & Halaburda, 2017).

Therefore, based on the above existing argues, the authors have come to positive conclusions through surveys from the views of academia (Liu et al., 2021) and requirement collection research from the industry (Liu, Xu, Zhang, et al., 2022). Based on the practical requirement of the industry, the authors have made a blockchain-based bond issuance system for different research purpose (Liu, Xu, Sai, et al., 2022). This system has been tested for several months, and the result shows that the system is acceptable from the perspective of academic discussion.

On 11 November 2022, FTX Trading Company, the world's second-largest cryptocurrency trading platform, announced that the company and other affiliated companies of the FTX Group had initiated voluntary bankruptcy proceedings following relevant US laws. Founded in 2019, FTX has more than 1 million users worldwide, and the valuation of FTX, a cryptocurrency exchange, has reached $32 billion. FTX will have no reason to go bankrupt if it is purely an exchange centre. But on 02 November 2022, the crypto market news site Coindesk reported that Alameda Research (The parents' company of FTX) borrowed tens of billions of dollars from the FTX exchange and bought most of the money into FTT to support the market value of FTT. Because Alameda has a whopping $6.112 billion in FTT tokens issued by FTX on its balance sheet, the dominoes began to fall.

For FTX Exchange, if clients do not withdraw all their money, FTX Exchange can use the money deposited by new investors to pay for the withdrawal needs of previewers investors. But as soon as the news came out, investors were immediately worried about the liquidity of FTT. Investors with a large amount of FTT began to sell FTT, and the price of FTT fell along with the trend dramatically.

In just 3 days, investors withdrew more than $6 billion from FTX's exchanges. However, both Alameda Research and FTX failed to give a convincing response to the outside world promptly, which led to an intensified run effect. After that, FXT lost its liquidity and had to file for bankruptcy. The systemic risks of cryptocurrencies have begun to explode after FXT company fell. The market value of the entire cryptocurrency market is evaporating, and more than thousands of large financial institutions worldwide face huge losses, such as Morgen Stanley, JP Morgan, Soft Bank, Goldman Sachs, etc. As a result of systemic risk, the traditional financial market has also been infected.

Therefore, monitoring the systemic risk of the cryptocurrency market is essential. In the traditional financial need, the best indicator for monitoring the risk of financial assets is VaR (Value-at-Risk). Every bank, large investment institution, and exchange has determined its var-based risk monitoring model according to its circumstances and Basel Framework. The Basel Framework is the complete set of standards of the Basel Committee on Banking Supervision (BCBS), which is the primary global standard setter for the prudential regulation of banks. The membership of the BCBS has agreed to fully implement these standards and apply them to the internationally active banks in their jurisdictions. Banks in more than 100 countries conduct risk monitoring according to the Basel Framework, and the newest version is Basel III (Prakash, 2008).

In this chapter, I aim to assess the risk associated with crypto assets using Value-at-Risk (VaR) measurements. This study consists of two experimental tests to evaluate the efficiency and accuracy of using VaR to measure crypto assets. The results of the experiments demonstrate that VaR can be effectively utilized to measure the risk of crypto assets under certain constraints.

The rest of this chapter is organized as follows. Section 5.1 acknowledges the literature review regarding cryptocurrency and Value at Risk measurement. Section 5.2 describes the data collection and summarizes this research's methodologies and data results. Section 5.3 introduces the demo of the monitoring risk system. Section 5.4 is the conclusion.

## 5.1 Cryptocurrency and VaR Measurement

### 5.1.1 Cryptocurrency

Digital technology has gradually changed the monetary system, and online digital transactions are increasing (Scott et al., 2017). To ensure the security of currency transactions, it is necessary to record and update the electronic ledger, the blockchain. Cryptocurrency is the encrypted digital currency that runs on the blockchain. Unlike traditional currencies, the price of cryptocurrencies is entirely determined by investors' perceptions and willingness to pay. There is no centralised control but the "peer-to-peer" participation of all investors in the market (Sovbetov, 2018). Since the movements of the cryptocurrency market are directly dependent on investor behaviours, currency prices can be explained by supply and demand based on investor behaviours. The mathematical equation for the Hash of the current block (the primary determinant of price) can be expressed as (Nakamoto, 2008):

$$Hash\ of\ current\ block = f\left(\theta_t - 1, \varphi, \phi\right)$$

Among them, θ is the Hash, φ is the mining difficulty, and Φ is the random key generated in the current process (the key is unique at a specific stage). Cryptocurrencies have no intrinsic or tangible value but are freely tradable and, therefore, highly volatile.

Digital currencies have become a class of assets that have snowballed in recent years (Borri, 2019), drawing widespread attention from investors and regulators. Regarding the nature of cryptocurrencies, there is still no consensus in academic and practical circles. In the past, the literature mainly divided cryptocurrencies into three categories: currency, commodities, and financial assets.

Scholars generally believe that the monetary properties of digital currencies are not yet apparent, but their commodity properties have been widely recognised (Baek & Elbeck, 2015). Although there are still liquidity constraints in digital currencies (Easley et al., 2019), with the emergence of stable-coins such as Tether and cryptocurrency transactions, it has achieved global liquidity through cryptocurrency exchanges.

Digital currencies also have asset characteristics. Specifically, cryptocurrencies have high volatility (Gkillas & Katsiampa, 2018), thick tails, leverage, and other notable features (Phillip et al., 2019). Many investors have considered cryptocurrencies as alternative assets or diversification options to reduce risk in their portfolios (Tiwari et al., 2019).

As a financial asset, the trading of encrypted cryptocurrencies is carried out on a global scale. There is no market closure, breaking the limitations of time and space. It can quickly respond to changes in the global financial market, making the cryptocurrency market as a market signal faster reflect market and investor sentiment (Choi et al., 2022). In addition, as an emerging investment asset, cryptocurrencies have similar properties to gold, such as decentralisation and scarcity. They may have investment properties identical to gold to hedge the investment risks of some traditional financial assets (Selmi et al., 2018).

### 5.1.2 Value at risk measurement

Value at risk (VaR) refers to the maximum possible loss suffered by an asset (asset portfolio) at a specific time in the future under certain normal conditions and a certain confidence level

$(1-\alpha)$. It is a widely recommended risk measurement tool used to measure the extreme tail risk of financial asset distribution (Beder, 1995).

The value of var is always non-negative. From a statistical point of view, var is defined as:

$$Prob\{y < -VaR\} = \alpha$$

Prob represents the probability of a random event, $y$ represents the return of an asset or investment portfolio, and when the return is negative, it means a loss. VaR represents the VaR value of the purchase at confidence level $1-\alpha$.

VaR is usually generated under the condition that the return distribution of financial assets is normal. However, in practice, its distribution generally has the characteristics of peak kurtosis and thick tails, which do not meet normal conditions. VaR can be seen as the quantile of the return distribution of an asset (or portfolio) over a certain period (Campbell et al., 2001). The quantile regression method analyses the degree of influence of the explanatory variables on the explained variables at different quantile points. It does not need to consider the distribution form of the explanatory variables. Therefore, the quantile regression method can calculate the VaR of financial assets.

The graphic definition of VaR is shown in the following Fig. 5.1, which illustrates the distribution of gains and losses of an asset or asset portfolio. Among them, VaRt (α) (e.g., 1 day ago from the value of VaR at time t) is the critical quantile in the lower tail of the distribution.

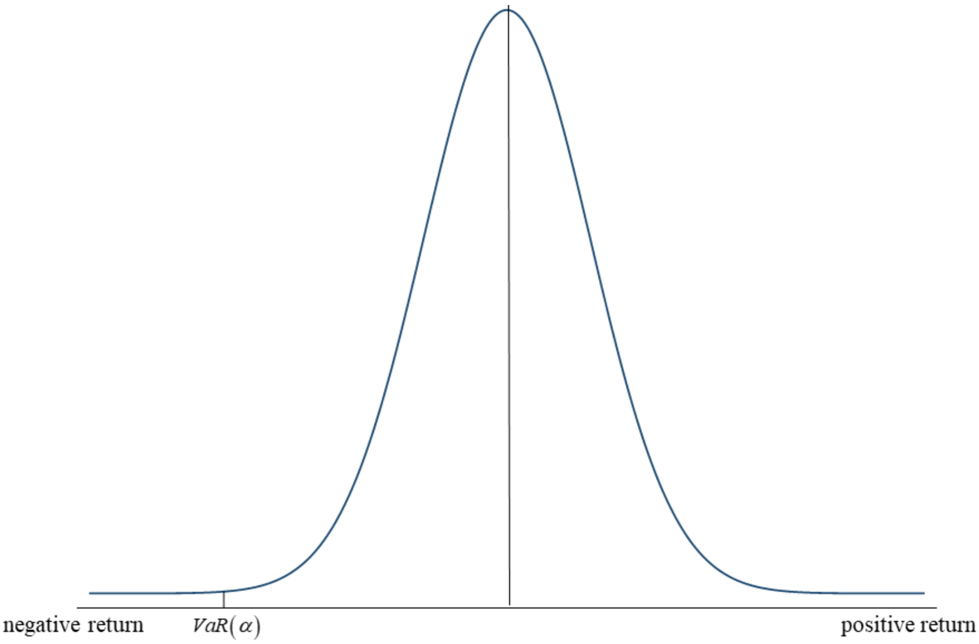


Fig. 5.1: Graphic definition of VaR

As a measure of asset risk, VaR combines the expected rate of return and rate of return fluctuation and is a comprehensive evaluation of asset risk.

### 5.1.3 Risk monitor on cryptocurrency

Cryptocurrencies behave differently than traditional fiat currencies. Cryptocurrencies' returns are more volatile and riskier than conventional currencies and exhibit heavier tail behaviours (Phillip et al., 2019). However, these assets indicate extreme price changes that violate the normality assumption, and a significant challenge in risk management is the appropriate selection of asset returns. Therefore, studying the tail behaviours and primary distribution of cryptocurrency returns is of great significance.

Taking Bitcoin as an example, the research on Bitcoin price began to shift from theoretical structural models to data-driven models, including VaR models, Bayesian models, wavelet analysis methods, and GARCH models. Bouoiyour et al. (2014) use the VaR model to analyse how Bitcoin's attractiveness to investors affects its price based on google's view and empirically found that speculative bubbles cause Bitcoin price volatility. Koutmos (2018) also uses the VAR model and found a strong correlation between Bitcoin returns and trading volume. Demir et al. (2018) used the Bayesian vector autoregression model, least squares method and quantile regression model to estimate and found that political and economic uncertainty has a specific predictive power for the Bitcoin price trend. Gronwald (2021) studied the causes of the dramatic price fluctuations of Bitcoin through the autoregressive jump strength GARCH model and pointed out that the immaturity of the Bitcoin market led to the dramatic price changes. Katsiampa (2017) measures multiple time series models, confirming that the AGARCH model is ideal for studying Bitcoin data.

The characteristics of all-day trading and significant price fluctuations of cryptocurrencies provide prerequisites for the widespread use of programmatic trading in cryptocurrency exchanges. Currently, the cryptocurrency trading platform mainly provides cryptocurrency trading functions and issuer services. However, relying on the cryptocurrency trading platform to manage cryptocurrency's trading risks still faces specific problems and challenges. For example, because the trading system of cryptocurrencies has its characteristics of cross-border, all-day, etc., the trading system formulated by traditional stock exchanges to reduce transaction risks cannot be fully applied to cryptocurrency transactions. Taking the more representative traditional securities risk limit management as a sample, the one-day limit on the rise and fall is impossible because digital currencies are traded on multiple platforms, and the arbitrage cost between platforms is low. Therefore, it has attracted particular attention to strengthening the risk management of cryptocurrency trading platforms (Li & Zhou, 2021).

Guo et al. (2022) point out the need for trading platforms to enhance the authenticity and transparency of trading information. The trading platform should maintain a neutral position between the asset and capital sides. It should disclose information such as the actual situation of the transaction and the objective market environment in a way that is easier for investors to obtain and understand. El-Hawary et al. (2007) state that exchanges can establish investor suitability management systems. Investor suitability management is not only to ensure the matching between investment product risks and investors' risk tolerance but also to comply with national regulatory laws and not to provide services to users in countries that prohibit centralised cryptocurrency trading. Mollah et al. (2021) illustrate that considering that most digital currencies do not have a clear issuer, the open-source community mainly maintains their systems. Hence, the trading platform only needs to strengthen the inflow or outflow of significant assets. Although the above studies have discussed how to improve the risk of the trading platform from different perspectives, there are still relatively few discussions on how to integrate the risk management system with the trading system and build a risk management mechanism embedded in the trading system.

## 5.2 Efficiency of Volatility for Cryptocurrency

### 5.2.1 Data and collection

The data selected in this chapter is collected from Yahoo Finance. The data set contains 8 encrypted digital currency prices from 18 September 2014 to 06 April 2022, with 2759 trading days (Top 7 largest market value on 06 April 2022, and FTT). This chapter defines the rate of return Rt of encrypted cryptocurrencies as the first-order logarithmic difference of the settlement price (closing price) of the cryptocurrencies on day t. Rt acts as a measure of cryptocurrency's market risk and measures the price fluctuations of these digital currencies.

Fig. 5.2 respectively depicts the volatility of the yields of these cryptocurrencies. From the time series graphs of these yields, it can be observed that there is a phenomenon of volatility aggregation in these yields, so the ARCH family model is used to describe them. In addition to the volatility clustering phenomenon, the return distribution of the two city indexes also showed pronounced peak and thick tail phenomenon.

Table 5.1 illustrates that the skewness of the seven cryptocurrencies is not 0, and the kurtosis is greater than 4, indicating that the distribution of these cryptocurrencies has a peak and a thick tail. The ADF and PP test statistics of all cryptocurrencies significantly differ from 0 at the 1% level, indicating that these cryptocurrencies' return series are stationary time series. In addition, the Jarque-Bera test statistics of these cryptocurrencies show that the returns of these cryptocurrencies do not obey the normal distribution.

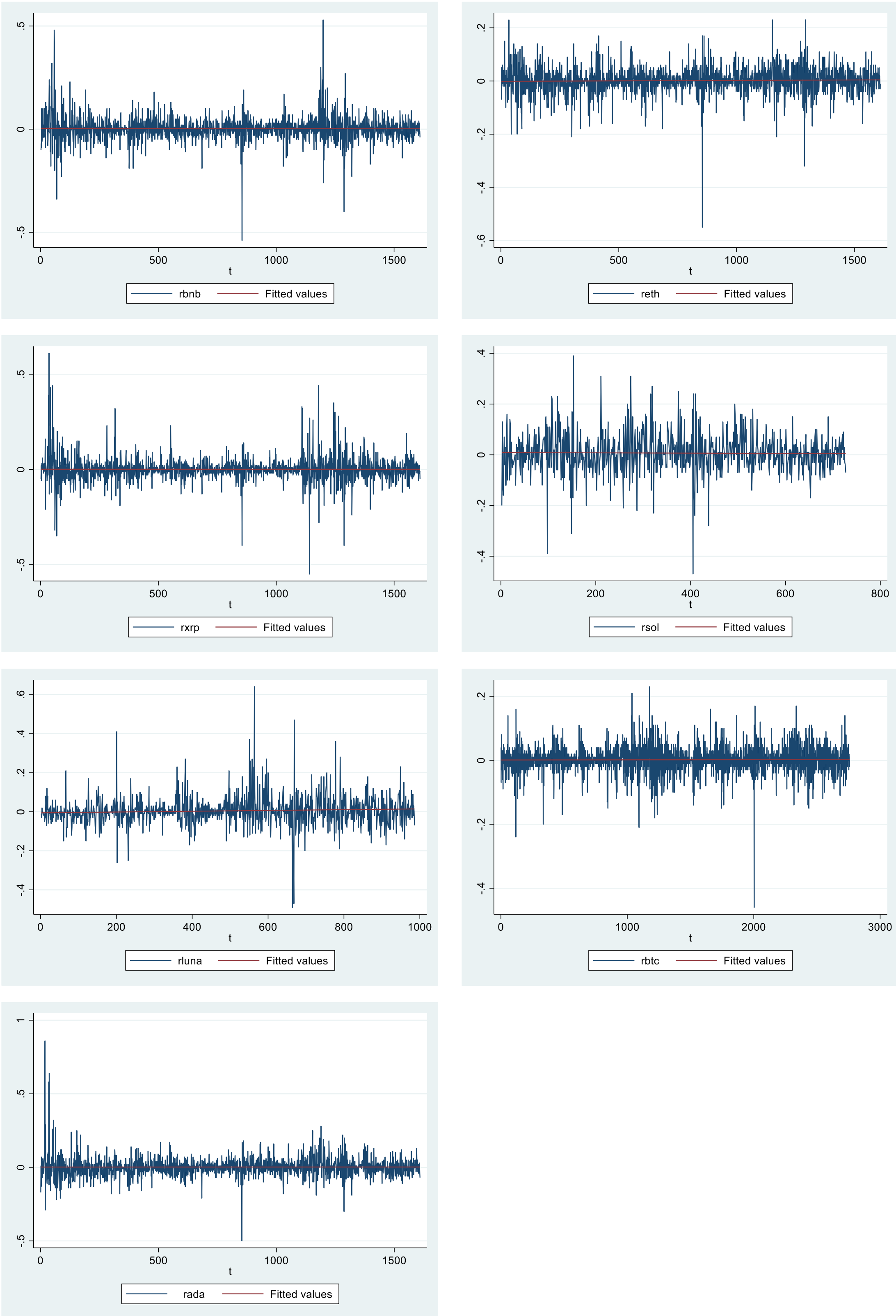


Fig. 5.2: Volatility of the yields of these cryptocurrencies

Table 5.1: Variable Descriptive Statistical Analysis

| | Sample size | Mean | STD | Max | Min | Skewness | Kurtosis | Jarque-Bera | ADF | PP |
|---|---|---|---|---|---|---|---|---|---|---|
| Bnb | 1610 | 0.0032 | 0.0613735 | 0.53 | -0.54 | 0.4090331 | 16.92751 | 0.000*** | 0.000*** | 0.000*** |
| Eth | 1610 | 0.0015351 | 0.0522296 | 0.23 | -0.55 | -0.974257 | 13.14899 | 0.000*** | 0.000*** | 0.000*** |
| Xrp | 1610 | 0.0008639 | 0 .0662523 | 0.61 | -0.55 | 0.8394417 | 18.9441 | 0.000*** | 0.000*** | 0.000*** |
| Sol | 727 | 0.0066391 | 0 .0828709 | 0.39 | -0.47 | -0.071203 | 6.456916 | 2.3e-79 (0.000***) | 0.000*** | 0.000*** |
| Luna | 986 | 0.0044975 | 0.0785888 | 0.64 | -0.49 | 0.851759 | 13.01125 | 0.000*** | 0.000*** | 0.000*** |
| Btc | 2758 | 0.0016497 | 0 .0391485 | 0.23 | -0.46 | -0.742279 | 13.72878 | 0.000*** | 0.000*** | 0.000*** |
| Ada | 1610 | .0021815 | 0 .0699122 | 0.86 | -0.50 | 2.019761 | 26.84706 | 0.000*** | 0.000*** | 0.000*** |
| FTT | 365 | -0.01 | 0.1010739 | 0.42 | -1.39 | -8.650039 | 111.8185 | 0.000*** | 0.000*** | 0.000*** |

The results of Jarque-Bera test, ADF test, and PP test are P value. ***, **, * represents the significant level of 1%, 5%, and 10% respectively.

## 5.2.2 Modelling

The GARCH model is a regression model based on the characteristics of sequence volatility aggregation proposed in 1986. It is an extension and expansion of the ARCH model, also called the generalized conditional heteroscedastic model. GARCH models exploit the error terms of the equations extensively to reduce their impact. The idea of the GARCH model is to establish a specific relationship between the current volatility and the historical volatility, expand the variance of each period into a conditional variance, and modify the conditional variance of the current period into a linear combination of the conditional variances of several historical periods.

GARCH can be expressed as follows:

Mean equation: $\alpha_t = \sigma_t \varepsilon_t$

Variance equation: $\sigma_t^2 = \alpha_0 + \sum_{i=1}^{p} \alpha_t \alpha_{t-1}^2 + \sum_{q}^{j=1} \beta_j \sigma_{t-j}^2$

The mean equation has a residual term, and e is a sequence of random variables with mean 0 and variance 1. In variance equation, $\sigma_t$ is conditional variance, $\alpha_0 > 0, \alpha_t \geq 0, \beta_j \geq 0, 0 < \sum_{i-1}^{\max(p,q)} \left(\alpha_i + \beta_j\right) < 1$.

In the variance equation, this chapter uses the GARCH family model to describe the marginal distribution of various asset returns and selects the optimal marginal distribution model according to the LL and AIC criteria. To capture the asymmetry and fat-tailed characteristics of asset returns, this chapter uses the Skewed-t distribution for estimation.

In this chapter, VaR is used to measure the risk of various assets for risk measurement. The specific expression of VaR is as follows:

$$VaR_{i,t}^{D,\alpha} = \mu_{it} + t_{v,\eta}^{-1}(\alpha)\sigma_{it}$$

$VaR_{i,t}^{D,\alpha}$ is downside risk, $\mu_{it}$ represents the conditional mean, $\sigma_{i,t}$ is the standardized residual of return $r_{i,t}$ . $t_{v,\eta}^{-1}(\alpha)$ is the quantile of T-distribution under level $\alpha$ .

### 5.2.3 Modelling results of volatility and VaR analysis

This chapter first estimates the marginal distribution of various cryptocurrency asset return sequences. The descriptive statistics in Table 5.2 shows that most sequence distributions have significant skewness (Skewness is not 0 significantly) and thick tails (Kurtosis is not 0 significantly). Each sequence is stationary (the ADF test is substantial), and there is an ARCH effect (the LM test rejects the null hypothesis). From the results, each cryptocurrency asset return sequence has important asymmetric fluctuation characteristics, which the GARCH-sstd model describes with the partial t distribution. According to the minimum information criterion test (AIC test) for the goodness of model fitting, the specific model selection is shown in the table.

According to the estimation results of the marginal distribution models of various cryptocurrencies returns and the VaR calculation formula, the daily VAR values of multiple cryptocurrencies return series under different confidence levels are calculated, and the corresponding statistical results are obtained. From the absolute value of the results, comparing different cryptocurrencies, the extreme risks of Bnb, Xrp, and Luna are greater than other cryptocurrencies. In particular, FTT has had a greater extreme risk in the recent half year.

Table 5.2: Estimation results of various cryptocurrencies revenue marginal distribution models

| | **Bnb** | **Eth** | **Xrp** | **Sol** | **Luna** | **Btc** | **Ada** | **Ftt** |
|---|---|---|---|---|---|---|---|---|
| Model | GARCH(1, 1) | GARCH(2, 1) | GARCH(1, 1) | GARCH(1, 1) | GARCH(2, 1) | GARCH(1, 2) | GARCH(1, 1) | GARCH(2, 1) |
| $\alpha_0$ | 0.0001719*** | 0.0002099*** | 0.0001082*** | 0.0005884** | 0.0002166** | 0.000022** | 0.0002895 | 0.0007718* |
| $\alpha_1$ | 0.1467017*** | | 0.2239222** | 0.1116637 | | 0.2259776*** | 0.1491101*** | |
| $\alpha_2$ | | 0.1201887*** | | | 0.2441497*** | | | 0.1713237 |
| $\beta_1$ | 0.819108*** | 0.8282396*** | 0.8801311*** | 0.8004184*** | 0.8106141*** | | 0.8052588*** | |
| $\beta_2$ | | | | | | 0.8612495*** | | 0.611969*** |
| df | 3.653651 | 3.436296 | 2.377844 | 5.384835 | 2.99342 | 2.644496 | 3.603735 | 2.871069 |
| LM | 0.000*** | 0.0129** | 0.000*** | 0.0001*** | 0.000*** | 0.000*** | 0.000*** | 0.0109** |
| AIC | -5163.047 | -5317.52 | -5297.554 | -1671.867 | -2611.132 | -11138.86 | -4683.86 | -1219.985 |
| | (-5.163) | (-5.317) | (-5.298) | (-1.672) | (-2.611) | (-11.139) | (-4.684) | (-1.219) |

LM test is P value, ***, **, * represents 1%, 5%, 10% significant level respectively.

Table 5.3: VaR value of various cryptocurrencies return series under downside risk and upside risk.

| **Significant level 95%** | **Bnb** | **Eth** | **Xrp** | **Sol** | **Luna** | **Btc** | **Ada** | **Ftt** |
|---|---|---|---|---|---|---|---|---|
| Mean | -0.0000565 | -0.00000695 | -.0001572 | -.0001169 | -0.0001153 | -0.0000297 | -0.0001181 | -0.0002719 |
| Max | 0.0327241 | 0.00843837 | 0.0490689 | 0.0131931 | 0.0627139 | 0.0054725 | 0.0168367 | 0.1408397 |
| Min. | -0.0379739 | -0.00760131 | -0.0884529 | -0.0148477 | -0.0652994 | -0.0144563 | -0.0687401 | -0.4268707 |
| STD | 0.0020523 | 0.00061155 | 0.0053641 | 0.0017362 | 0.004705 | 0.0006297 | 0.0028106 | 0.0246704 |
| Significant level 99% | Bnb | Eth | Xrp | Sol | Luna | Btc | Ada | Ftt |
| Mean | -0.0001019 | -0.0000128 | -0.0002461 | -0.0001926 | -0.0002227 | -0.0000604 | -0.000217 | -0.0005336 |
| Max | 0.0590042 | 0.0155095 | 0.0767806 | 0.0217262 | 0.1211078 | -0.0294387 | 0 .0051643 | 0.2764168 |
| Min | -0.0684702 | -0.013971 | -0.1384068 | -0.0244509 | -0.1261008 | 0.0111442 | -0.1263068 | -0.8377911 |
| STD | 0.0037005 | 0.001124 | 0.0083934 | 0.0028591 | 0.0090858 | 0.0012822 | 0.0309366 | 0.0484189 |

## 5.3 Design of Risk Monitor System

Platforms and investors can monitor cryptocurrency transaction risks with a risk monitoring system. The platform can realise comprehensive coverage and online monitoring and timely identify risks. Risks such as credit, operational, and liquidity risks can be determined first.

Other advantages, such as quantifying risk management indicators, early risk warning, and blocking illegal operations, can also be actioned before risk events start. Based on the above risk report, investors can further understand their risk exposure, risk appetite, and investment preference.

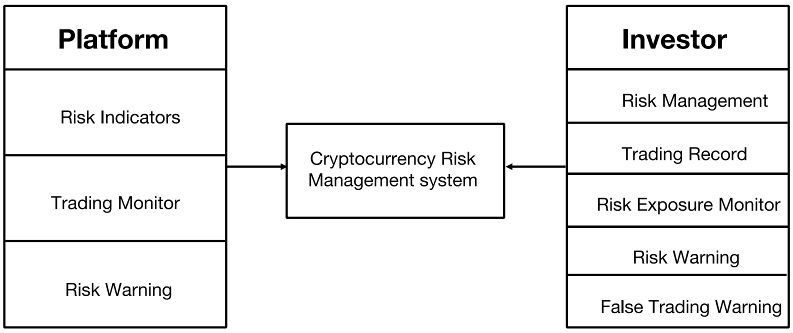


Fig. 5.3: Flow of cryptocurrency risk management system

### 5.3.1 Functionality

The market risk management system has the following functions: (1) Upload daily trading position indicators, sensitivity, related environment, and other data from the front-end system promptly. (2) Ability to check data quality and track and solve problems. (3) Establish a centralised and shared market data warehouse. (4) Establish centralised and shared scenario settings and scenario tests. (5) Establish a centralised computing platform so that various cryptocurrencies can be calculated through the same computing model to ensure the consistency of standards. (6) An effective computing platform supporting diversification, daily VaR value calculation and stress testing. (7) It reconciles back-to-front-and middle-office systems so that the system can obtain position data entirely and continuously. (8) A flexible and efficient reporting environment supporting platform and investor-level reporting.

| Risk Management Flow | | | |
|---|---|---|---|
| Audit Tracking | | | |
| **Data Acquisition** | **Data Quality** | **Risk Valuation** | **Report/Analysis** |
| Position data | Data adjustment | Data adjustment | Standard trading report |
| Reference data | Rule recognition | Rule recognition | Market report |
| Market data | Proxy server logic | Proxy server logic | AD-HOC report |
| Outside impact | Exceptions | Exceptions | Scenario analysis |
| | | | Backtrack test |
| | | | Profitability analysis |
| Data Acquisition & Upload to Regulation System | | | |

Fig. 5.4: Flow of risk management system

## 5.3.2 Indicators setting

This design provides a comprehensive set of metrics, including fully configurable Value at Risk (VaR) analysis and Expected Loss (ES) analysis.

| Traditional Risk Indicators | | Modern Risk Indicators |
|---|---|---|
| Volatility | Kurtosis | VaR (Value at Risk) |
| Variance | Skewness | Marginal VaR |
| Theoretical Gain/Loss | Correlation | Component VaR |
| Real Gain/Loss | Concentration ratio | Incremental VaR |
| Gain/Loss under stress test | | Stress VaR |
| | | ES (Expected Shortfall) |

Fig. 5.5: Risk indicators comparation between traditional and modern

### 5.3.3 Risk warning alarm

Considering the risk characteristics of cryptocurrencies, the price of cryptocurrencies is easily affected by market sentiment, policy, technology, etc. It is sometimes difficult to identify the impact source in a short period when the price changes drastically. Therefore, the cryptocurrency price data flow is dynamic, and the volatility distribution may change after being subjected to specific obvious or hidden shocks. Concept drift can describe the change mentioned earlier; that is, the target concept of data has changed to a certain extent under the influence of certain factors. These changes are not easy to be found or cannot be figured out within a certain period, and the reason for concept drift is the change of these hidden factors.

Concept drift can be divided into two categories: abrupt concept drift and gradual concept drift. Abrupt concept drift mainly refers to concept drift caused by sudden changes, while gradual concept drift is relatively mild. Platforms and investors are more concerned about the concept drift of mutations for cryptocurrencies. Currently, there are mainly two approaches to dealing with concept drift. One is a case-based derivation, where a global classifier is selected for comparative analysis with cases related to the current concept. The other is based on classifier integration, aggregating historical data to form a corresponding concept data set. Therefore, the integrated classifier is selected through this concept data set to understand the concept drift situation. Since cryptocurrencies have relatively rich historical data, it can be considered to use classifier-based integration to deal with concept drift. Based on the above, this chapter designs a cryptocurrency risk early warning system based on concept drift.

The process of the risk warning alarm system is designed as follows:

(1) Divide the alarm level.

According to whether the cryptocurrencies have experienced extreme fluctuations, the cryptocurrencies risk alert is divided into two alert levels: risk and normal.

(2) Build a quantitative risk indicator system.

This is an integral part of the cryptocurrencies risk warning alarm system based on concept drift. Warnings are issued when risk indicators are abnormal, often indicating the emergence of cryptocurrency risks. Therefore, this process is also a process of analysing the degree of risk.

(3) Build a cryptocurrencies risk warning alarm device。

This is a crucial step based on this type of risk early warning. It is necessary to select a suitable classifier algorithm, compare the quantitative relationship between the risk early warning indicator and the risk degree indicator (risk level), and construct a cryptocurrency risk early warning model that predicts the risk degree indicator from the risk early warning indicator.

(4) Risk warning alarm.

The early warning signal of the cryptocurrency risk indicator is processed by the risk early warning device, which outputs the cryptocurrency risk level. It will alarm and send the relevant details to the platform and investors when the risk level shows that the cryptocurrencies are at risk.

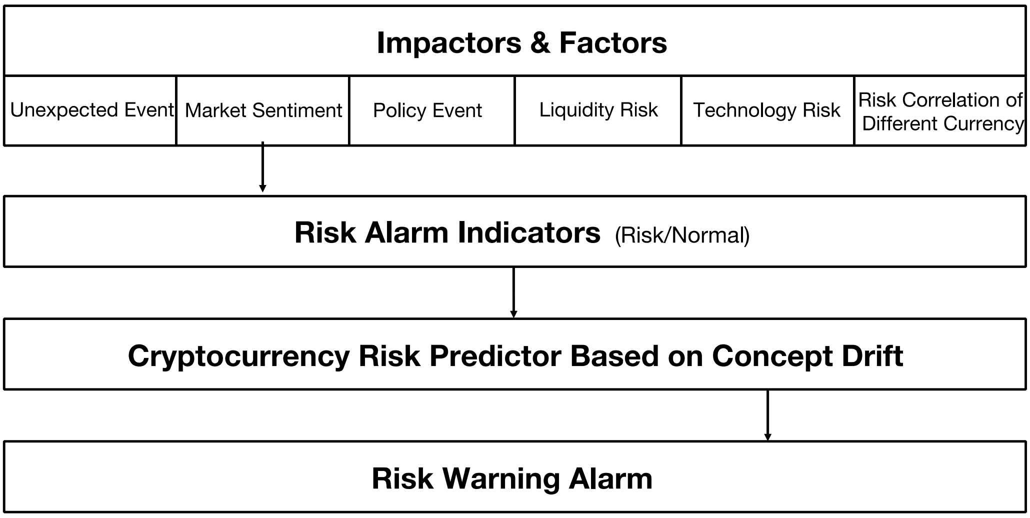


Fig. 5.6: Flowchart of risk warning alarm system

## 5.3.4 System integration

The authors attempt to design a risk monitor system that is suitable for cryptocurrencies trading platforms and investors and can provide risk monitor and management system integration solutions for platforms and investors. The solution is to develop and implement an interface standard package based on the trading platform, which can realize the connection between the risk monitor/management system and the trading system, external market data, regulatory agencies, etc. In this way, it can meet the risk management needs of transaction, risk and regulation, therefore, improve the efficiency of transaction process and risk management level.

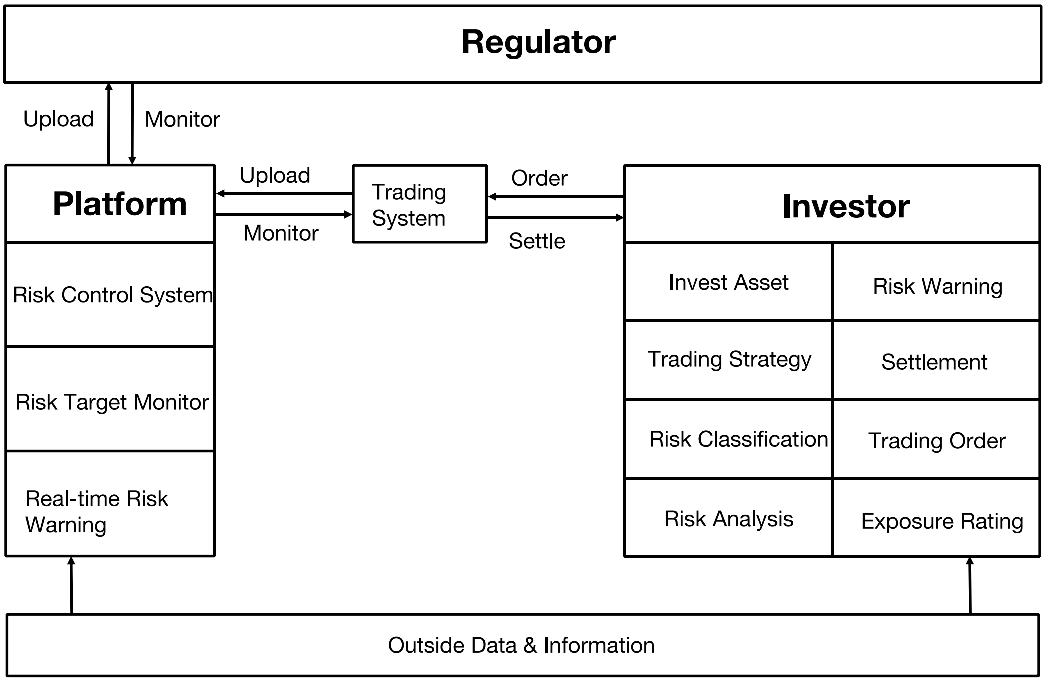


Fig. 5.7: Framework of risk monitor system

### 5.3.4.1 Functionality

The risk system deployment architecture has core and optional components, and it is critical to decide which components to use in a custom environment. Additionally, infrastructure components such as operating systems, database systems, application servers, and load balancers need to be decided. Before installing and deploying the architecture, it is also necessary to formulate clear installation and deployment goals, and based on this, determine the installation topology that meets these goals.

The market risk management system has the following functions: (1) Upload daily trading position indicators, sensitivity, related environment, and other data from the front-end system in a timely manner. (2) Ability to check data quality and track and solve problems. (3) Establish a centralized and shared market data warehouse. (4) Establish centralized and shared scenario settings and scenario tests. (5) Establish a centralized computing platform, so that various cryptocurrencies can be calculated through the same computing model to ensure the consistency of standards. (6) An effective computing platform that can support diversification, daily VaR value calculation and stress testing. (7) It has the function of reconcile back-to front- and middle-office systems, so that the system can obtain position data completely and continuously. (8) A flexible and efficient reporting environment capable of supporting platform and investor-level reporting.

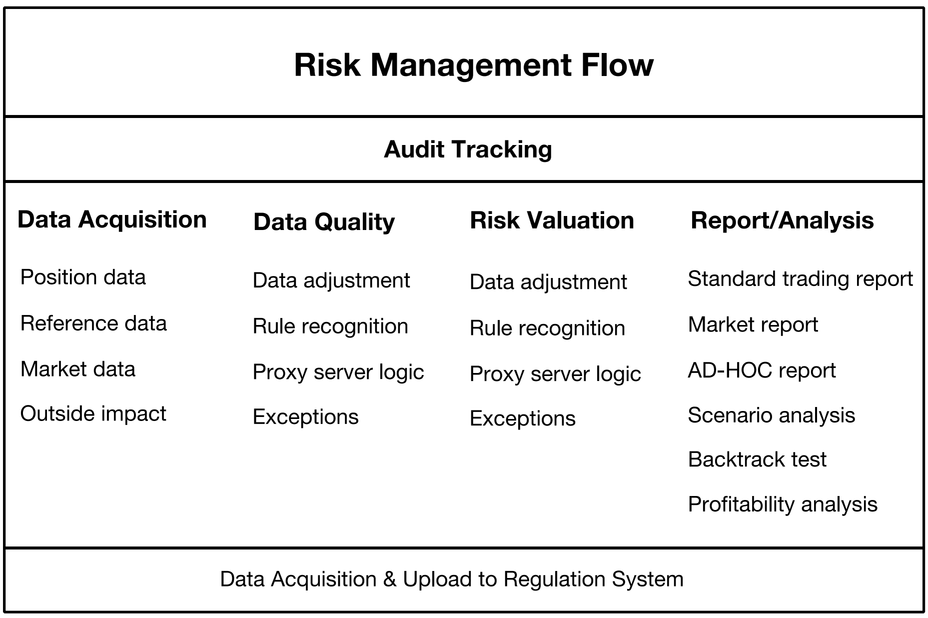


Fig. 5.8: Flow of risk management system

#### 5.3.4.2 Indicators setting

This design provides a comprehensive set of metrics, including fully configurable Value at Risk (VaR) analysis and Expected Loss (ES) analysis.

| Traditional Risk Indicators | | Modern Risk Indicators |
|---|---|---|
| Volatility | Kurtosis | VaR (Value at Risk) |
| Variance | Skewness | Marginal VaR |
| Theoretical Gain/Loss | Correlation | Component VaR |
| Real Gain/Loss | Concentration ratio | Incremental VaR |
| Gain/Loss under stress test | | Stress VaR |
| | | ES (Expected Shortfall) |

Fig. 5.9: Risk indicators comparation between traditional and modern

#### 5.3.4.3 Risk warning alarm

Considering the risk characteristics of cryptocurrencies, the price of cryptocurrencies is easily affected by market sentiment, policy, technology, etc. It is sometimes difficult to identify the source of the impact in a short period of time when the price changes drastically. Therefore, the cryptocurrencies price data flow is dynamic, and the volatility distribution may change after being subjected to certain obvious or hid-den shocks. Concept drift can describe the above-mentioned change issue, that is, the target concept of data has changed to a certain extent under the influence of certain factors. These changes are not easy to be found or cannot be figured out within a certain period of time, and the reason for concept drift is the change of these hidden factors.

Concept drift can be divided into two categories: abrupt concept drift and gradual concept drift. Abrupt concept drift mainly refers to the phenomenon of concept drift caused by sudden changes, while gradual concept drift is relatively mild. For crypto-currencies, platforms and investors are more concerned about the concept drift of mutations. Currently, there are mainly two approaches to deal with concept drift. One is case-based derivation, where a global classifier is selected for comparative analysis with cases related to the current concept. The other is based on classifier integration, which aggregates historical data to form a corresponding concept data set. Therefore, through this concept data set to understand the concept drift situation, the integrated classifier is selected. Since cryptocurrencies has relatively rich historical data, it can be considered to use classifier-based integration to deal with concept drift. Based on above, this chapter designs a cryptocurrencies risk early warning system based on concept drift.

The process of the risk warning alarm system is designed as follows:

(1) Divide the alarm level.

According to whether the cryptocurrencies has experienced extreme fluctuations, the cryptocurrencies risk alert is divided into two alert levels: risk and normal.

(2) Build a quantitative risk indicator system.

This is an important part of the cryptocurrencies risk warning alarm system based on concept drift. Warnings are issued when risk indicators are abnormal, which often indicates the emergence of cryptocurrencies risks. Therefore, this process is also a process of analysing the degree of risk.

(3) Build a cryptocurrencies risk warning alarm device.

This is a key step based on this type of risk early warning. It is necessary to select a suitable classifier algorithm, compare the quantitative relationship between the risk early warning indicator and the risk degree indicator (risk level), and construct a cryptocurrencies risk early warning model that predicts the risk degree indicator from the risk early warning indicator.

(4) Risk warning alarm.

The early warning signal of the cryptocurrencies risk indicator is processed by the risk early warning device, which outputs the cryptocurrencies risk level. It will alarm and send the relevant details to the platform and investors when the risk level shows that the cryptocurrencies is at risk.

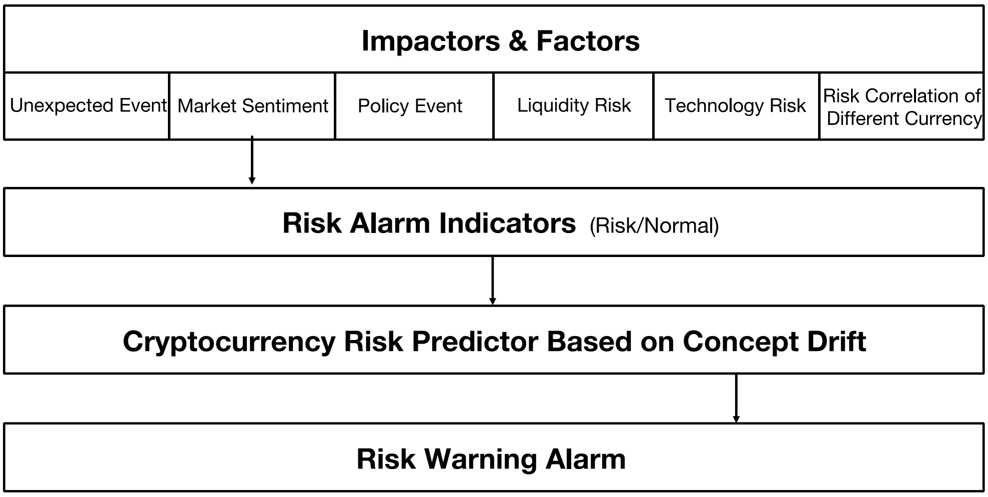


Fig. 5.10: Flowchart of risk warning alarm system

#### 5.3.4.4 System integration

The authors attempt to design a risk monitor system suitable for cryptocurrency trading platforms and investors and can provide risk monitoring and management system integration solutions for venues and investors. The key is to develop and implement a standard interface package based on the trading platform, which can realize the connection between the risk monitor/management system and the trading system, external market data, regulatory agencies, etc. In this way, it can meet the risk management needs of transactions, risk, and regulation, improving the efficiency of the transaction process and risk management level.

The deployment architecture of the risk system has both core and optional components. The choice of features to use depends on the environment's specific needs. Essential infrastructure components such as operating systems, database systems, application servers, and load balancers must also be considered. It is crucial to establish clear installation and deployment goals before installing and deploying the architecture and determine the installation topology that meets these goals.

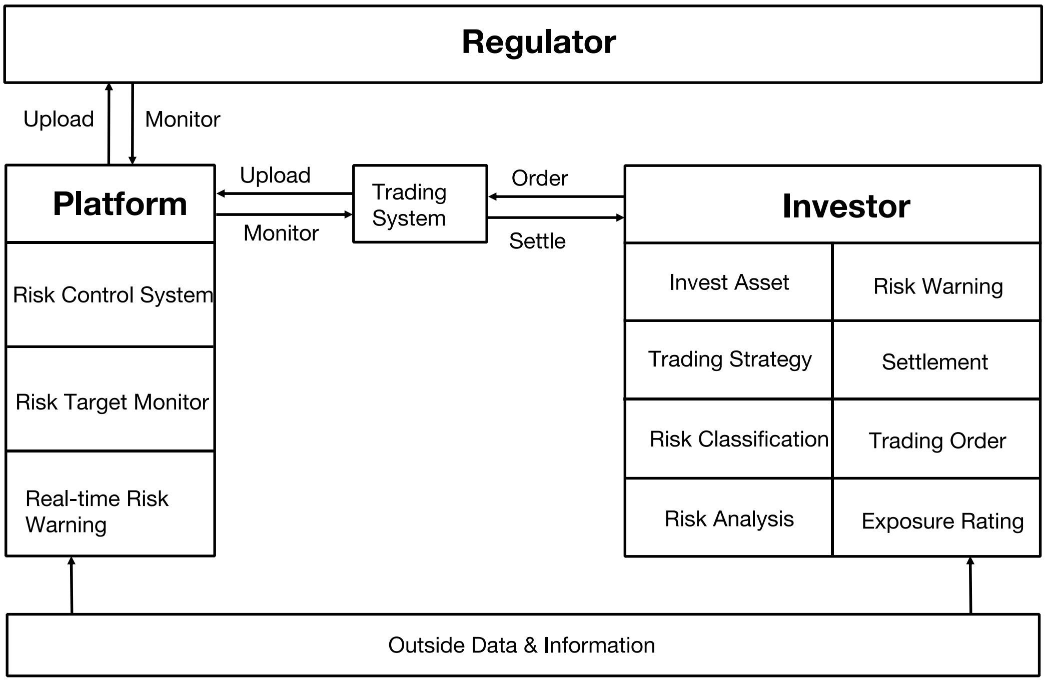


Fig. 5.11: Framework of risk monitor system

#### 5.3.4.5 Empirical experiment

For research purposes, the authors designed a demo to test the ability of the prediction to capture the trend of risk. Unsupervised clustering was chosen as the data was too complex to be labelled. The authors performed experiments on the selected 7 sets, eliminating two groups (Sol and Luna) to reduce invalid data due to their short-term interval. The remaining data were pooled into sets of samples every seven days, featuring variables such as GPR (geopolitical risk index), USDX (US Dollar Index), GEPU (Global Economic Policy Uncertainty Index), MSCI index, investor confidence index, the benchmark interest rate in the US dollar area, price ratio, and volatility. Latitude reduction was performed using PCA (Principal Component Analysis), and each clustering algorithm was applied.

The experiment uses three different clustering algorithms:

1) Kmeans in prototype-based clustering. The training set is divided into k sample clusters with high similarity within the cluster and low similarity between clusters. The algorithm

starts by assigning each training sample to the cluster represented by the nearest centroid based on its distance from the centroid. The centroids of all clusters are then recalculated and updated to the mean of all training samples in the cluster. This process is repeated until convergence is reached.

2) Linkage in hierarchical clustering. This algorithm divides the data set into different levels to form a tree-like clustering structure. In the beginning, each data point is its cluster. Clusters close to each other are merged into larger clusters until the desired number of risk categories is reached.

3) DBSCAN (Density-Based Spatial Clustering of Applications with Noise) in density-based clustering. The algorithm is based on neighbourhood parameters that describe the distribution of samples. It divides the high-density area into clusters, finds clusters of any shape in the spatial database, and defines clusters as the most extensive collection of density-connected points. The algorithm then classifies all topics through iteration.

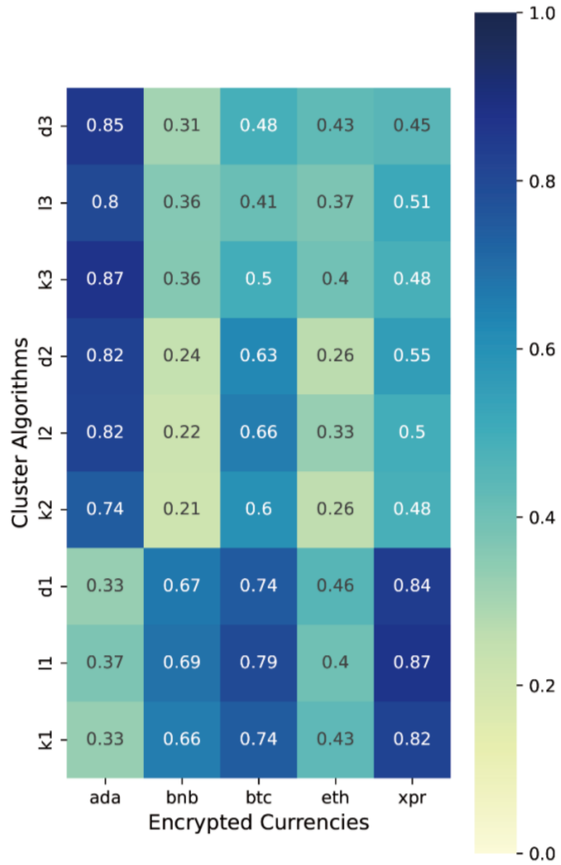

Fig. 5.12: Plot of Risk Prediction

The horizontal axis represents various cryptocurrencies, while the ordinate axis corresponds to three algorithms: Kmeans (k), Linkage (h), and BDSCAN (d). The plot shows three groups of samples for each currency, corresponding to each algorithm. The values in the heat map indicate the level of risk, which the authors have defined as high risk for values greater than or equal to 0.7, medium for values between 0.5 and 0.7, low for values between 0.3 and 0.5, and no risk for values less than 0.3. (Note that the risk value is calculated based on the relative distance between each point and the cluster centre. The benchmark values of 0.7, 0.5, and 0.3 were arbitrarily selected and can be adjusted as needed.)

The authors obtained three sets of data through random sampling and used three clustering algorithms to assess the risk of each group. The results of the cluster analysis are shown in Fig. 5.12. The results of the risk warning obtained by the three methods for each digital currency are relatively consistent. The authors chose k1, l1, and d1 to evaluate the risk levels of different currencies and found that the risk level of ADA was lower and the risk level of XPR was higher. The results between the groups were also considered to be consistent. In sample 1, the risk of ETH and ADA was low, while the risk of BNB, BTC, and XPR was high, in line with the experimental results. The results from the other two samples were also generally consistent with the experimental results. Hence, the experimental results are considered robust.

## 5.4 Conclusion

This research is mainly based on improving the follow-up work done by the authors on the previous issuance system. In the future, the analysis will be carried out on infrastructure, such as the issuance, transaction, and system management of blockchain-based exchanges. Meanwhile, the authors will also focus on the quantitative research of risk, return, control, and exit mechanism from different views.

An effective risk monitoring system can reduce liquidity risk and the occurrence of run effects, thereby reducing systemic risk. At the same time, when the system detects a risk factor. The system can report to the regulatory agency as quickly as possible. Regulators can rescue the market in the first place, increasing the effect of the rescue and reducing the losses of investors. In this way, the regulators can establish a healthy cryptocurrency market ecosystem.

CHAPTER 6

# Conclusion

Blockchain technology has the potential to revolutionise financial market infrastructure by improving efficiency and revolutionising how assets are maintained, obligations are fulfilled, transactions are conducted, and risks are managed. In the financial market, there are many issues, such as many participants, high costs of credit evaluation, low settlement efficiency of intermediaries, and difficulty in managing risks. These issues lead to long-standing problems in the financial market, such as information asymmetry, high information verification (trust) costs, and complex and redundant processes (efficiency).

The core purpose of financial market transactions is to improve the level and efficiency of investment and financing and to better complete asset allocation. Therefore, safety, trust, and efficiency have become essential factors restricting financial development. Blockchain technology can effectively address these pain points in the financial market by enabling all market participants to access all transaction information and asset ownership records without discrimination, effectively solving the problem of information asymmetry.

Simultaneously, the transparent information and new trust mechanisms among all participants eliminate the need for costly and time-consuming information verification, thereby reducing the cost of trust among institutions and the price of financial services. The use of smart contracts can reduce errors in the payment and settlement process, simplify the process, and improve efficiency. Privacy features such as tamper-proofing and traceability can ensure the security of financial activities and provide adequate technical support for effective risk prevention measures.

Therefore, this thesis aims to fill this gap in research by investigating the application of blockchain technology in the financial market, specifically in the construction of financial market infrastructure. Through conducting an academic survey and requirement collection from the industry, I identify the pain points and issues present in the current financial market infrastructure. I then propose a blockchain-based financial assets issuance and trading system and a risk monitoring mechanism to address these issues and evaluate their effectiveness through experimental studies. Our research contributes to understanding blockchain technology's potential to improve trust, efficiency, and risk management in the financial market and provides valuable insights for further research in this field.

Based on this, the research results of this thesis are as follows:

1) An academic survey of blockchain technology and its application in the financial market is conducted, providing a comprehensive understanding of the current state of research and identifying key issues that need to be addressed.

2) A requirement collection from the industry is conducted, providing insights into the pain points of the financial market and the specific requirements for blockchain-based solutions.

3) A blockchain-based financial assets issuance system is proposed and implemented, designed to improve trust and efficiency in issuing and trading financial assets.

4) A risk monitoring system for blockchain-based financial products is proposed and implemented, which can provide real-time monitoring and warning of market risks, reducing the probability of systemic risks.

5) The proposed solutions are evaluated and tested in real-world scenarios, demonstrating their effectiveness in improving trust, efficiency, and risk management in the financial market.

Overall, this thesis significantly contributes to understanding blockchain technology and its potential applications in the financial market. The proposed solutions can potentially revolutionise the financial market's infrastructure, providing a more efficient and secure environment for transactions.

In conclusion, during my doctoral studies, my research revolved around integrating blockchain technology into existing financial systems to address the issues present in the current financial market and utilizing available technologies to achieve these goals. However, due to limitations in time, support, and resources during my doctoral program, I was only able to complete a portion of the envisioned experiments and research. In the future, I will continue to pursue my current research focus: applying blockchain technology to financial infrastructure.

The following research topics are areas I would explore further if provided with sufficient time and resources:

1) Enhancing the embedding of smart contracts within derivative trading contracts to improve trust processes and speed in over-the-counter trading.

2) Investigating anonymous transactions in distributed systems with high trust, efficiency, and effective guarantee mechanisms.

3) Researching the mechanisms, modelling, trading logic design, and system development of equity exchanges in a distributed structure.

These research topics will further advance the development of blockchain technology in the financial domain and provide vital support for innovation in future financial markets. I look forward to continuing my in-depth research and contributing to the development of financial technology.

# Bibliography

Abadi, J., & Brunnermeier, M. (2018). *Blockchain Economics* (w25407). National Bureau of Economic Research. http://www.nber.org/papers/w25407.pdf

Acharya, V. V., Engle, R. F., Figlewski, S., Lynch, A. W., & Subrahmanyam, M. G. (2012). Centralized clearing for credit derivatives. In V. V. Acharya & M. P. Richardson (Eds.), *Restoring financial stability* (pp. 251–268). John Wiley and Sons. https://doi.org/10.1002/9781118258163.ch11

Ahmad, A., Saad, M., Bassiouni, M., & Mohaisen, A. (2018, 2018/11//). *Towards blockchain-driven, secure and transparent audit logs* [Paper presentation]. Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, New York.

Aitzhan, N. Z., & Svetinovic, D. (2018). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*, *15*(5), 840–852.

Alun, J. (2020, November 10). *China Construction Bank unit raising $3 bln via blockchain bond*. NASDAQ. https://www.nasdaq.com/articles/china-construction-bank-unit-raising-%243-bln-via-blockchain-bond-2020-11-10

Angieri, S., García-Martínez, A., Liu, B., Yan, Z., Wang, C., & Bagnulo, M. (2020). A distributed autonomous organization for internet address management. *IEEE Transactions on Engineering Management*, *67*(4), 1459–1475.

Aniche, M., Treude, C., Steinmacher, I., Wiese, I., Pinto, G., Storey, M.-A., & Gerosa, M. A. (2018). *How modern news aggregators help development communities shape and share knowledge* [Paper presentation]. Proceedings of the 40th International conference on software engineering, New York.

Anson, M. (2013). Performance measurement in private equity: Another look at the lagged beta effect. *Journal of Private Equity*, *17*(1), 29–44.

Baek, C., & Elbeck, M. (2015). Bitcoins as an investment or speculative vehicle? A first look. *Applied Economics Letters*, *22*(1), 30–34.

Bank of China. (2019, December 7). *Bank of China Issues $2.8B in bonds for small businesses using blockchain tech*. Yahoo. https://au.finance.yahoo.com/news/bank-china-issues-2-8b-180500855.html

Batjargal, B. (2007). Network triads: Transitivity, referral and venture capital decisions in China and Russia. *Journal of International Business Studies*, *38*(6), 998–1012.

Beck, R., Czepluch, J. S., Lollike, N., & Malone, S. (2016). *Blockchain–the gateway to trust-free cryptographic transactions* [Paper presentation]. Twenty-Fourth European Conference on Information Systems (ECIS), İstanbul, Turkey, 2016, Istanbul.

Beder, T. S. (1995). VAR: Seductive but dangerous. *Financial Analysts Journal, 51*(5), 12–24.

Bignon, V., & Vuillemey, G. (2020). The failure of a clearinghouse: empirical evidence. *Review of Finance, 24*(1), 99–128.

Blackwell, T., & Kohl, S. (2018). The origins of national housing finance systems: a comparative investigation into historical variations in mortgage finance regimes. *Review of International Political Economy, 25*(1), 49–74.

Blemus, S., & Guégan, D. (2020). Initial crypto-asset offerings (ICOs), tokenization and corporate governance. *Capital Markets Law Journal, 15*(2), 191–223.

Bliss, R. R., & Steigerwald, R. S. (2006). Derivatives clearing and settlement: A comparison of central counterparties and alternative structures. *Economic Perspectives, 30*(4), 22–29.

Borri, N. (2019). Conditional tail-risk in cryptocurrency markets. *Journal of Empirical Finance, 50*, 1–19.

Bouoiyour, J., Selmi, R., & Tiwari, A. (2014). *Is Bitcoin business income or speculative bubble? Unconditional vs. conditional frequency domain analysis* (No. 59595). MPRA. https://mpra.ub.uni-muenchen.de/59595/

Bradbury, D. (2015). In blocks we trust [bitcoin security]. *Engineering and Technology, 10*(2), 68–71.

Bradbury, D. (2016). Blockchain's big deal [financial IT]. *Engineering & Technology, 11*(10), 44–44.

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *Ethereum White Paper, 3*(37), 1–36.

Campbell, R., Huisman, R., & Koedijk, K. (2001). Optimal portfolio selection in a value-at-risk framework. *Journal of Banking & Finance, 25*(9), 1789–1804.

Caprio, G., Arner, D. W., Beck, T., Calomiris, C. W., Neal, L., & Veron, N. (2012). *Handbook of key global financial markets, institutions, and infrastructure*. Academic Press.

Çelik, S., Demirtaş, G., & Isaksson, M. (2019). *Corporate bond markets in a time of unconventional monetary policy*. OECD

Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., & Arami, M. (2020). How Blockchain can impact financial services – The overview, challenges and recommendations from expert interviewees. *Technological Forecasting and Social Change, 158*, Article 120166.

Chemmanur, T. J., & Fulghieri, P. (1994). Investment bank reputation, information production, and financial intermediation. *The Journal of Finance, 49*(1), 57–79.

Chen, L. H., Dyl, E. A., Jiang, G. J., & Juneja, J. A. (2015). Risk, illiquidity or marketability: What matters for the discounts on private equity placements? *Journal of Banking and Finance, 57*, 41–50.

Chen, Y., & Bellavitis, C. (2019). *Decentralized finance: Blockchain technology and the quest for an open financial system*. SSRN. https://ssrn.com/abstract=3418557

Choi, K. H., Kang, S. H., & Yoon, S. M. (2022). Herding behaviour in Korea's cryptocurrency market. *Applied Economics, 54*(24), 2795–2809.

Codagnone, C., & Martens, B. (2017). *Scoping the sharing economy: Origins, definitions, impact and regulatory issues* (No. 2016/01). Institute for Prospective Technological Studies. https://www.econstor.eu/bitstream/10419/202218/1/jrc-dewp201601.pdf

Cohen, L. R., Samuelson, L., & Katz, H. (2017). How securitization can benefit from blockchain technology. *Journal of Structured Finance, 23*(2), 51–54.

Cong, L. W., & He, Z. (2019). Blockchain disruption and smart contracts. *Review of Financial Studies*, *32*(5), 1754–1797.

Cumming, D. J. (2005). Agency costs, institutions, learning, and taxation in venture capital contracting. *Journal of Business Venturing*, *20*(5), 573–622.

Datta, A., Hauswirth, M., & Aberer, K. (2003, 24-27 June 2003). *Beyond "web of trust": Enabling P2P e-commerce* [Paper presentation]. EEE International Conference on E-Commerce, 2003. CEC 2003., Newport Beach, CA.

Dddder, B., & Ross, O. (2017). Timber tracking: Reducing complexity of due diligence by using blockchain technology. *SSRN Electronic Journal*, Article 3015219.

Demir, E., Gozgor, G., Lau, C. K. M., & Vigne, S. A. (2018). Does economic policy uncertainty predict the Bitcoin returns? An empirical investigation. *Finance Research Letters*, *26*, 145–149.

Dogru, T., Mody, M., & Leonardi, C. (2018). *Blockchain technology & its implications for the hospitality industry* (201802). Boston University. https://www.bu.edu/bhr/files/2018/02/Blockchain-Technology-and-its-Implications-for-the-Hospitality-Industry.pdf

DTCC. (2020). *Project whitney: Case study*. https://perspectives.dtcc.com/articles/project-whitney

Duffie, D. (2014). Financial market infrastructure. In M. N. Baily & J. B. Taylor (Eds.), *Across the great divide: New perspectives on the financial crisis* (Vol. 652, pp. 251–256). Hoover Institution Press.

Dunkley, E. (2018). *HKEX working with ASX on blockchain*. Financial Times. https://www.ft.com/content/b9b17762-2c0e-11e8-9b4b-bc4b9f08f381

Easley, D., O'Hara, M., & Basu, S. (2019). From mining to markets: The evolution of bitcoin transaction fees. *Journal of Financial Economics*, *134*(1), 91–109.

El-Hawary, D., Grais, W., & Iqbal, Z. (2007). Diversity in the regulation of islamic financial institutions. *The Quarterly Review of Economics and Finance*, *46*(5), 778–800.

EOS Go. (2019, October 12). *Deutsche Bank bond tokenized on the EOS mainnet*. https://www.eosgo.io/news/deutsche-bank-bond-tokenized-on-the-eos-mainnet

Evans-Pughe, C. (2012). From megabytes to megabucks [e-currency]. *Engineering and Technology, 7*(4), 59–61.

Fisher, R. A. (1922). On the Interpretation of χ 2 from Contingency Tables, and the Calculation of P. *Journal of the Royal Statistical Society*, *85*(1), 87–94.

Foroglou, G., & Tsilidou, A. L. (2015). *Further applications of the blockchain* [Paper presentation]. 12th student conference on managerial science and technology, Athens.

Franzoni, F., Nowak, E., & Phalippou, L. (2012). Private equity performance and liquidity risk. *Journal of Finance, 67*(6), 2341–2373.

Funcke, S., & Bauknecht, D. (2016). Typology of centralised and decentralised visions for electricity infrastructure. *Utilities Policy, 40*, 67–74.

Fung, B. S. C., & Halaburda, H. (2017). Central bank digital currencies: A framework for assessing why and how. *SSRN Electronic Journal*, Article 2994052.

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *Qualitative Report, 20*(9), 1408–1416.

Ganti, R. K., Srivatsa, M., & Verma, D. C. (2017). *Efficient clearinghouse transactions with trusted and un-trusted entities (U.S. Patent No. 9,824,031)*. U.S. Patent and Trademark Office.

Garcia, A. R. (2020). AI, IoT, big data, and technologies in digital economy with blockchain at sustainable work satisfaction to smart mankind: Access to 6th dimension of human rights. In N. V. M. Lopes (Ed.), *Smart governance for cities: Perspectives and experiences* (pp. 83–131). Springer International Publishing. https://doi.org/10.1007/978-3-030-22070-9_6

Garg, P., Gupta, B., Chauhan, A. K., Sivarajah, U., Gupta, S., & Modgil, S. (2021). Measuring the perceived benefits of implementing blockchain technology in the banking sector. *Technological Forecasting and Social Change*, *163*, Article 120407.

Gkillas, K., & Katsiampa, P. (2018). An application of extreme value theory to cryptocurrencies. *Economics Letters, 164*, 109–111.

Goldreich, O., Micali, S., & Wigderson, A. (1991). Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM (JACM), 38*(3), 690–728.

Goodman, L. A. (1961). Snowball Sampling. *The Annals of Mathematical Statistics*, *32*(1), 148–170.

Griffith, S. J. (2011). Governing systemic risk: Towards a governance structure for derivatives clearinghouses. *Emory Law Journal*, *61*, 1153–1169.

Gronwald, M. (2021). The economics of Bitcoins -- Market characteristics and price jumps. *SSRN Electronic Journal*, Article 2548999.

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough?: An experiment with data saturation and variability. *Field Methods*, *18*(1), 59–82.

Guo, L., Chen, J., Li, S., Li, Y., & Lu, J. (2022). A blockchain and IoT-based lightweight framework for enabling information transparency in supply chain finance. *Digital Communications and Networks, 8*(4), 576–587.

Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial Innovation, 2*(1), 1–12.

Halevi, T., Benhamouda, F., Caro, A. D., Halevi, S., Jutla, C., Manevich, Y., & Zhang, Q. (2019, 14-17 July 2019). *Initial public offering (IPO) on permissioned blockchain using secure multiparty computation* [Paper presentation]. 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA.

Harvey, O., & Aldridge, C. (2014). Evolution of Australian financial market infrastructure. *JASSA*, (3), 27–34.

Hasenpusch, T. P. (2009). *Clearing services for global markets: A framework for the future development of the clearing industry*. Cambridge University Press.

Hoffmann, P., Laeven, L. A., & Ratnovski, L. (2021). Financial Intermediation and Technology: What's Old, What's New? *SSRN Electronic Journal*, Article 3642562.

Holmberg, P. (2009). Supply function equilibria of pay-as-bid auctions. *Journal of Regulatory Economics, 36*(2), 154–177.

Hsu, Y., & Shiu, C. Y. (2010). The overconfidence of investors in the primary market. *Pacific Basin Finance Journal*, *18*(2), 217–239.

Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International Journal of Information Management*, *49*, 114–129.

Hyvärinen, H., Risius, M., & Friis, G. (2017). A blockchain-based approach towards overcoming financial fraud in public sector services. *Business and Information Systems Engineering, 59*(6), 441–456.

Informa. (2022). *Debt summary*. https://www.informa.com/investors/debt-summary/

Jacobs, S. (2018). *The ASX says its new blockchain platformwill be ready by the end of 2020*. Business Insider. https://www.businessinsider.com.au/asx-blockchain-distributed-ledger-technology-chess-replacement-2018-4

Jenkins, W., & Strauser, D. R. (1999). Horizontal expansion of the role of the rehabilitation counselor. *Journal of Rehabilitation, 65*(1), Article 4.

Joo, M. H., Nishikawa, Y., & Dandapani, K. (2019). *ICOs, the next generation of IPOs*. Managerial Finance. https://ideas.repec.org/a/eme/mfipps/mf-10-2018-0472.html

Kang, J., Yu, R., Huang, X., Wu, M., Maharjan, S., Xie, S., & Zhang, Y. (2019). Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE Internet of Things Journal, 6*(3), 4660–4670.

Kaplan, S. N., & Strömberg, P. (2009). Leveraged buyouts and private equity. *Journal of Economic Perspectives, 23*(1), 121–146.

Katsiampa, P. (2017). Volatility estimation for Bitcoin: A comparison of GARCH models. *Economics Letters, 158*, 3–6.

Khujamurodov, A. (2020). Analysis of development of the infrastructure of the stock market in Uzbekistan and the methodology of its estimation. *Архив научных исследований, 33*(1), 168–176.

Kiayias, A., & Litos, O. S. T. (2020, 22-26 June 2020). *A composable security treatment of the lightning network* [Paper presentation]. 2020 IEEE 33rd Computer Security Foundations Symposium (CSF), Boston, MA.

Kim, M., Zimmermann, T., DeLine, R., & Begel, A. (2016, 2016/05//). *The emerging role of data scientists on software development teams* [Paper presentation]. Proceedings of the 38th International Conference on Software Engineering, Austin, TX.

Kim, M., Zimmermann, T., Deline, R., & Begel, A. (2018). Data scientists in software teams: State of the art and challenges. *IEEE Transactions on Software Engineering*, *44*(11), 1024–1038.

Kitchenham, B. A., & Pfleeger, S. L. (2008). Personal opinion surveys. In F. Shull, J. Singer, & D. I. K. Sjøberg (Eds.), *Guide to advanced empirical software engineering* (pp. 63–92). Springer. https://doi.org/10.1007/978-1-84800-044-5_3

Klagge, B., & Martin, R. (2005). Decentralized versus centralized financial systems: Is there a case for local capital markets? *Journal of Economic Geography*, *5*(4), 387–421.

Koeplin, J., Sarin, A., & Shapiro, A. C. (2000). The private company discount. *Journal of Applied Corporate Finance*, *12*(4), 94–101.

Kolehmainen, T., Laatikainen, G., Kultanen, J., Kazan, E., & Abrahamsson, P. (2021). *Using blockchain in digitalizing enterprise legacy systems: An experience report* [Paper presentation]. Software business, Cham.

Kollmann, T., Kuckertz, A., & Middelberg, N. (2014). Trust and controllability in venture capital fundraising. *Journal of Business Research*, *67*(11), 2411–2418.

Koutmos, D. (2018). Return and volatility spillovers among cryptocurrencies. *Economics Letters*, *173*, 122–127.

Kress, J. C. (2011). Credit default swaps, clearinghouses, and systemic risk: Why centralized counterparties must have access to central bank liquidity. *Harvard Journal on Legislation*, *48*, 49–93.

Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, *39*, 80–89.

Lamarque, M. (2016). *The blockchain revolution: new opportunities in equity markets* [Master's thesis, Massachusetts Institute of Technology]. MIT Lib. https://dspace.mit.edu/handle/1721.1/104522

Lawrence, D. (2012). *Proprietary risk management clearinghouse (U.S. Patent No. 8,209,246)*. Patent and Trademark Office.

Layne, K. A. (2007). *Collection agency data access method (U.S. Patent No. 7,167,839)*. U.S. Patent and Trademark Office.

Lerner, J., & Schoar, A. (2004). The illiquidity puzzle: Theory and evidence from private equity. *Journal of Financial Economics*, *72*(1), 3–40.

Li, X., & Zhou, P. (2021). Research on risk management of digital currency based on blockchain technology in mobile commerce. In G. Salvendy & J. Wei (Eds.), *Design, operation and evaluation of mobile communications* (pp. 45–67). Springer International Publishing.

Liu, J., Xu, Z., Li, R., Zhao, H., Jiang, H., Yao, J., Yuan, D., & Chen, S. (2021). Applying blockchain for primary financial market: A survey. *IET Blockchain, 1*(2-4), 65–81.

Liu, J., Xu, Z., Sai, Y., Zhang, Y., Yuan, D., & Chen, S. (2022). i-Bond: A next generation bond's issuing service system. In S. Chen, R. K. Shyamasundar, & L.-J. Zhang (Eds.), *Blockchain – ICBC 2022* (pp. 29–47). Springer Nature Switzerland.

Liu, J., Xu, Z., Zhang, Y., Dai, W., Wu, H., & Chen, S. (2022). Digging into primary financial market: Challenges and opportunities of adopting blockchain. *arXiv preprint*, arXiv:2204.09544.

Luu, L., Narayanan, V., Baweja, K., Zheng, C., Gilbert, S., & Saxena, P. (2015). *Scp: A computationally-scalable byzantine consensus protocol for blockchains*. Weusecoins. https://www.weusecoins.com/assets/pdf/library/SCP%20-%20%20A%20Computationally-Scalable%20Byzantine.pdf

Ma, Z., Huang, W., & Gao, H. (2018). Secure DRM scheme based on blockchain with high credibility. *Chinese Journal of Electronics, 27*(5), 1025–1036.

Manaa, M., Chimienti, M. T., Adachi, M. M., Athanassiou, P., Balteanu, I., Calza, A., Devaney, C., Diaz Fernandez, E., Eser, F., Ganoulis, I., Laot, M., Günther, P., Poignet, R., Sauer, S., Schneeberger, D., Stracca, L., Tapking, J., Toolin, C., Tyler, C., & Wacket, H. (2021). Crypto-assets: Implications for financial stability, monetary policy, and payments and market infrastructures. *SSRN Electronic Journal*, Article 3391055.

Manju, D. (2018, January 3). *The new floor for bond underwriting fees: $1*. The Wall Street Journal. https://www.wsj.com/articles/the-new-floor-for-bond-underwriting-fees-1-1514973603

Manning, J. (2017, December 18). *How stock exchanges are utilising blockchain techonology*. International Banker. https://internationalbanker.com/brokerage/stock-exchanges-utilising-blockchain-technology/

Mauer, D. C., & Senbet, L. W. (1992). The effect of the secondary market on the pricing of initial public offerings: Theory and evidence. *The Journal of Financial and Quantitative Analysis*, *27*(1), 55–79.

McCallig, J., Robb, A., & Rohde, F. (2019). Establishing the representational faithfulness of financial accounting information using multiparty security, network analysis and a blockchain. *International Journal of Accounting Information Systems*, *33*, 47–58.

McDonald, J. H. (2009). *Handbook of biological statistics*. Sparky House Publishing.

Mehran, H., & Stulz, R. M. (2007). The economics of conflicts of interest in financial institutions. *Journal of Financial Economics*, *85*(2), 267–296.

Mendelson, H. (1982). Market behavior in a clearing house. *Econometrica*, *50*(6), 1505–1524.

Meuleman, M., Wright, M., Manigart, S., & Lockett, A. (2009). Private equity syndication: Agency costs, reputation and collaboration. *Journal of Business Finance and Accounting*, *36*(5-6), 616–644.

Mills, D. C., Wang, K., Malone, B., Ravi, A., Marquardt, J., Badev, A. I., Brezinski, T., Fahy, L., Liao, K., & Kargenian, V. (2016). Distributed ledger technology in payments, clearing, and settlement. *SSRN Electronic Journal*, Article 095.

Mollah, M. B., Zhao, J., Niyato, D., Lam, K. Y., Zhang, X., Ghias, A. M. Y. M., Koh, L. H., & Yang, L. (2021). Blockchain for future smart grid: A comprehensive survey. *IEEE Internet of Things Journal*, *8*(1), 18–43.

Mori, T. (2016). Financial technology: Blockchain and securities settlement. *Journal of Securities Operations & Custody*, *8*(3), 208–227.

Morse, J. M. (2015). Data were saturated. *Qualitative Health Research*, *25*(5), 587–588.

Mvula, F., Phiri, J., & Tembo, S. (2019). *A conceptual secure blockchain based settlement and clearinghouse for mobile financial services in Zambia* [Paper presentation]. Proceedings of The International conference INICT (ICIC2019). Lappeenranta.

Nabilou, H. (2020). Bitcoin governance as a decentralized financial market infrastructure. *SSRN Electronic Journal*, Article 3555042.

Nadauld, T. D., Sensoy, B. A., Vorkink, K., & Weisbach, M. S. (2019). The liquidity cost of private equity investments: Evidence from secondary market transactions. *Journal of Financial Economics*, *132*(3), 158–181.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, Article 21260.

Nelson, T. (2018). *Mergers and Acquisitions from A to Z*. Amacom.

Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2019). Analysis of blockchain technology: Pros, cons and SWOT. *Cluster Computing*, *22*, 14743–14757.

Norta, A. (2015, 2015//). *Creation of smart-contracting collaborations for decentralized autonomous organizations* [Paper presentation]. Perspectives in Business Informatics Research, Cham.

Nunes, B. d. S. R. (2017). *Virtual currency: a cointegration analysis between bitcoin prices and economic and financial data* [Master's thesis, Instituto Universitário de Lisboa]. ISCTE. https://repositorio.iscte-iul.pt/handle/10071/16078

O'Dwyer, K. J., & Malone, D. (2014). *Bitcoin mining and its energy footprint* [Paper presentation]. 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014), Limerick.

Ong, A. D., & Weiss, D. J. (2000). The impact of anonymity on responses to sensitive questions. *Journal of Applied Social Psychology*, *30*(8), 1691–1708.

Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review*, *18*(4), 329–340.

Pan, D. (2019, October 4). *Singapore exchange–backed iSTOX raises series a for tokenized securities trading*. Coin Desk. https://www.coindesk.com/thai-bank-backs-series-a-funding-for-tokenized-securities-startup-istox

Pervez, H., Muneeb, M., Irfan, M. U., & Haq, I. U. (2018, 19-21 Dec. 2018). *A comparative analysis of DAG-based blockchain architectures* [Paper presentation]. 2018 12th

International Conference on Open Source Systems and Technologies (ICOSST), Lahore.

Phillip, A., Chan, J., & Peiris, S. (2019). On long memory effects in the volatility measure of Cryptocurrencies. *Finance Research Letters, 28*, 95–100.

Pop, C., Pop, C., Marcel, A., Vesa, A., Petrican, T., Cioara, T., Anghel, I., & Salomie, I. (2018, 6-8 Sept. 2018). *Decentralizing the stock exchange using blockchain an ethereum-based implementation of the bucharest stock exchange* [Paper presentation]. 2018 IEEE 14th International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca.

Prakash, A. (2008). Evolution of the Basel framework on bank capital regulation. *Reserve Bank of India Occasional Papers, 29*(2), 81–122.

Rabah, K. (2018). Convergence of AI, IoT, big data and blockchain: A review. *The lake institute Journal, 1*(1), 1–18.

Robinson, D. T., & Sensoy, B. A. (2016). Cyclicality, performance measurement, and cash flow liquidity in private equity. *Journal of Financial Economics, 122*(3), 521–543.

Rocket, T. (2018, June 3). *Snowflake to avalanche: A novel metastable consensus protocol family for cryptocurrencies*. Metadata. http://muratbuffalo.blogspot.com/2018/06/snowflake-to-avalanche-novel-metastable.html

Roe, M. J. (2013). Clearinghouse overconfidence. *California Law Review, 101*, 1641–1691.

Rozario, A. M., & Thomas, C. (2019). Reengineering the audit with blockchain and smart contracts. *Journal of Emerging Technologies in Accounting, 16*(1), 21–35.

Santo, A., Minowa, I., Hosaka, G., Hayakawa, S., Kondo, M., Ichiki, S., & Kaneko, Y. (2016). *Applicability of distributed ledger technology to capital market infrastructure*. JPX. https://www.finextra.com/finextra-downloads/newsdocs/e_jpx_working_paper_no15.pdf

Sberbank. (2017, Novomber 29). *Sberbank carries out Russia's first payment transaction using blockchain technology*. https://www.sberbank.ru/en/press_center/all/article?newsID=9f676571-5219-4cfb-bbb7-c9c6e1de983ablockID=1539regionID=77lang=entype=NEWS

Schär, F. (2020). Decentralized finance: On blockchain- and smart contract-based financial markets. *SSRN Electronic Journal*, Article 3571335.

Scholtens, L. J. R. (1992). Centralisation in international financial intermediation: theory, practice, and evidence for the European Community. *PSL Quarterly Review*, *45*(182), 255–304.

Scott, B., Loonam, J., & Kumar, V. (2017). Exploring the rise of blockchain technology: Towards distributed collaborative organizations. *Strategic Change*, *26*(5), 423–428.

Selmi, R., Mensi, W., Hammoudeh, S., & Bouoiyour, J. (2018). Is Bitcoin a hedge, a safe haven or a diversifier for oil price movements? A comparison with gold. *Energy Economics*, *74*, 787–801.

SGX. (2020, September 1). *SGX, in collaboration with HSBC and Temasek, completes pilot digital bond for Olam International*. https://www.sgx.com/media-centre/20200901-sgx-collaboration-hsbc-and-temasek-completes-pilot-digital-bond-olam

Sheldon, M. D. (2019). A primer for information technology general control considerations on a private and permissioned blockchain audit. *Current Issues in Auditing*, *13*(1), A15–A29.

Shrier, D., Wu, W., & Pentland, A. (2016). Blockchain & infrastructure (identity, data security). *Massachusetts Institute of Technology-Connection Science*, *1*(3), 1–19.

Shull, F., Singer, J., & Sjøberg, D. I. K. (2008). *Guide to advanced empirical software engineering*. Springer.

SIFMA Research. (2022). *Capital markets fact book*. https://www.sifma.org/resources/research/fact-book/

Singer, L., Figueira Filho, F., & Storey, M. A. (2014, 2014/05//). *Software engineering at the speed of light: How developers stay current using twitter* [Paper presentation]. Proceedings of the 36th International Conference on Software Engineering, Hyderabad.

Smart Securities. (2015). *Homepage*. https://www.symbiont.io

Sovbetov, Y. (2018). Factors influencing cryptocurrency prices: Evidence from bitcoin, ethereum, dash, litcoin, and monero. *Journal of Economics and Financial Analysis*, *2*(2), 1–27.

Spencer, D. (2009). *Card sorting: Designing usable categories*. Rosenfeld Media.

Stiglitz, J. E. (1989). Financial markets and development. *Oxford Review of Economic Policy, 5*(4), 55–68.

Sulkowski, A. J. (2018). Blockchain, business supply chains, sustainability, and law: The future of governance, legal frameworks, and lawyers. *Delaware Journal of Corporate Law, 43*, 303–353.

Sutton, A., & Samavi, R. (2017, 2017). *Blockchain enabled privacy audit logs* [Paper presentation]. International Semantic Web Conference, Cham.

Swanson, T. (2021). Decentralized financial market infrastructures. *SSRN Electronic Journal*, Article 3530996.

Szabo, N. (1996). Smart contracts: Building blocks for digital markets. *The Journal of Transhumanist Thought,* (16), 28–29.

Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday, 2*(9), Article 548.

Tian, H., Ge, X., Wang, J., Li, C., & Pan, H. (2020). Research on distributed blockchain-based privacy-preserving and data security framework in IoT. *IET Communications, 14*(13), 2038–2047.

Tian, Y., Adriaens, P., Minchin, R. E., Chang, C., Lu, Z., & Qi, C. (2021). Asset Tokenization: A blockchain Solution to Financing Infrastructure in Emerging Markets and Developing Economies. *SSRN Electronic Journal*, Article 3837703.

Tilooby, A. (2018). *The impact of blockchain technology on financial transactions* [Master's thesis, Georgia State University]. Scholarworks. https://scholarworks.gsu.edu/cgi/viewcontent.cgi?article=1111&context=bus_admin_diss

Tinn, K. (2017). Blockchain and the future of optimal financing contracts. *SSRN Electronic Journal*, Article 3061532.

Titman, S., & Grinblatt, M. (1998). *Financial markets and corporate strategy*. McCraw-HilI.

Tiwari, S., Atluri, V., Kaushik, A., Yndart, A., & Nair, M. (2019). Alzheimer’s disease: Pathogenesis, diagnostics, and therapeutics. *International Journal of Nanomedicine, 14*, 5541–5554.

Treleaven, P., Brown, R. G., & Yang, D. (2017). Blockchain technology in finance. *Computer*, *50*(9), 14–17.

Troncia, M., Galici, M., Mureddu, M., Ghiani, E., & Pilo, F. (2019). Distributed ledger technologies for peer-to-peer local markets in distribution networks. *Energies, 12*(17), Article 3249.

Tsai, W. T., Luo, Y., Deng, E., Zhao, J., Ding, X., Li, J., & Yuan, B. (2020). Blockchain systems for trade clearing. *Journal of Risk Finance, 21*(5), 469–492.

Walch, A. (2015). The bitcoin blockchain as financial market infrastructure: A consideration of operational risk. *N.Y.U. Journal of Legislation & Public Policy, 18,* Article 837.

Wang, G., Shi, Z. J., Nixon, M., & Han, S. (2019, 2019/10//). *Sok: Sharding on blockchain* [Paper presentation]. Proceedings of the 1st ACM Conference on Advances in Financial Technologies, Zurich.

Wang, J. J. D., & Zender, J. F. (2002). Auctioning divisible goods. *Economic Theory, 19*(4), 673–705.

Wang, Y., & Vassileva, J. (2007, 2007). *A review on trust and reputation for web service selection* [Paper presentation]. 27th international Conference on distributed computing systems workshops (ICDCSW'07), Toronto.

World Bank. (2018). *World bank prices first global blockchain bond, raising a$110 million*. https://www.worldbank.org/en/news/press-release/2018/08/23/world-bank-prices-first-global-blockchain-bond-raising-a110-million

Wright, M., Amess, K., Weir, C., & Girma, S. (2009). Private equity and corporate governance: Retrospect and prospect. *Corporate Governance: An International Review*, *17*(3), 353–375.

Wu, T., & Liang, X. (2017, 2017/10//). *Exploration and practice of inter-bank application based on blockchain* [Paper presentation]. 2017 12th International Conference on Computer Science and Education, Houston, TX.

Wu, Y., Song, P., & Wang, F. (2020). Hybrid consensus algorithm optimization: A mathematical method based on POS and PBFT and its application in blockchain. *Mathematical Problems in Engineering, 2020,* Article 7270624.

Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. *Financial Innovation, 5*(1), Article 27.

Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology, 10*(2), 1–19.

Yang, Z., Yang, K., Lei, L., Zheng, K., & Leung, V. C. M. (2019). Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet of Things Journal, 6*(2), 1495–1505.

Ye, S., & Zeng, J. (2021, 2021/12//). *The mechanism and strategy of blockchain technology driving the development of supply chain finance* [Paper presentation]. 2021 International Conference on Social Sciences and Big Data Application, Xi'an.

Yu, T., Lin, Z., & Tang, Q. (2018). Blockchain: The Introduction and Its Application in Financial Accounting. *Journal of Corporate Accounting and Finance, 29*(4), 37–47.

Yuan, Y., & Wang, F. Y. (2016, 2016/12//). *Towards blockchain-based intelligent transportation systems* [Paper presentation]. 2016 IEEE 19th International Conference on Intelligent Transportation Systems, Rio de Janeiro.

Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized finance (DeFi). *Journal of Financial Regulation, 6*(2), 172–203.

Zhang, F., Sun, H., Xu, L., & Lun, L. K. (2006, 2006). *Parallel-split shadow maps for large-scale virtual environments* [Paper presentation]. Proceedings of the 2006 ACM international conference on Virtual reality continuum and its applications, New YorkNY.

Zhang, L., Xie, Y., Zheng, Y., Xue, W., Zheng, X., & Xu, X. (2020). The challenges and countermeasures of blockchain in finance and economics. *Systems Research and Behavioral Science, 37*(4), 691–698.

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 14*(4), 352–375.

Zhu, H., Wang, Y., Hei, X., Ji, W., & Zhang, L. (2018, 2019/02//). *A blockchain-based decentralized cloud resource scheduling architecture* [Paper presentation]. 2018 International Conference on Networking and Network Applications, Xi'an.

Zhu, H., & Zhou, Z. Z. (2016). Analysis and outlook of applications of blockchain technology to equity crowdfunding in China. *Financial Innovation*, *2*(1), Article 29.

Zimmermann, T. (2016). Card-sorting: From text to themes. In T. Menzies, L. Williams, & T. Zimmermann (Eds.), *Perspectives on data science for software engineering* (pp. 137–141). Morgan Kaufmann. https://doi.org/https://doi.org/10.1016/B978-0-12-804206-9.00027-1

Zou, W., Lo, D., Chen, Z., Xia, X., Feng, Y., & Xu, B. (2020). How practitioners perceive automated bug report management techniques. *IEEE Transactions on Software Engineering, 46*(8), 836–862.

Zyskind, G., Nathan, O., & Pentland, A. (2015). Enigma: Decentralized computation platform with guaranteed privacy. *arXiv preprint*, arXiv:1506.03471.