공학박사학위논문

An Analytical Study of Blockchain-based Digital Assets: Focusing on Central Bank Digital Currencies, Stablecoins, and Non-Fungible Tokens

블록체인 기반 디지털 자산에 대한 분석 연구: 중앙은행 디지털 화폐, 스테이블코인, 대체 불가능 토큰을 중심으로

2023 년 2 월

서울대학교 대학원

산업공학과

이 윤 영

An Analytical Study of Blockchain-based Digital Assets: Focusing on Central Bank Digital Currencies, Stablecoins, and Non-Fungible Tokens

블록체인 기반 디지털 자산에 대한 분석 연구: 중앙은행 디지털 화폐, 스테이블코인, 대체 불가능 토큰을 중심으로

지도교수 이재욱

이 논문을 공학박사 학위논문으로 제출함

2022 년 12 월

서울대학교 대학원

산업공학과

이윤영

이윤영의 공학박사 학위논문을 인준함

2023 년 1 월

위 원 장 이덕주 (인)

부위원장 이재욱 (인)

위 원 장우진 (인)

위 원 손영두 (인)

위 원 장희수 (인)

Abstract

An Analytical Study of Blockchain-based Digital Assets: Focusing on Central Bank Digital Currencies, Stablecoins, and Non-Fungible Tokens

Yunyoung Lee
Department of Industrial Engineering
The Graduate School
Seoul National University

This dissertation provides an in-depth analysis of three promising assets in the DeFi market: CBDCs, stablecoins, and NFTs. For CBDCs, a blockchain-based CBDC settlement model is proposed using cross-chain atomic swaps and lattice-based sequential aggregate signature scheme to address two challenging issues. For stablecoins, the connectedness and information transmission between the stablecoin and cryptocurrency market is quantified to conclude that CBDCs can mitigate financial risks. For NFTs, the return-volume causal relationships in the NFT markets are analyzed due to the low transaction volume.

For CBDCs, we propose a blockchain-based CBDC settlement model which addresses two fundamental challenges in CBDC design. It introduces an administrator ledger to the settlement system to provide auditability and allows the administrator node to participate in every transaction. The model also uses cross-chain atomic swap technology and a lattice-based sequential aggregate signature scheme to ensure safety and enable cross-border payments. These features make the model suitable for the growing needs for stable and reliable digital currencies. Our model provides a secure and reliable way to track transaction records and match the identity of transaction participants, while also protecting against malicious behavior and quantum computer attacks.

Stablecoins backed with their own protocol's native tokens are highly susceptible to death spirals if the corresponding blockchain protocol is met with public distrust. During normal market conditions, the impact of stablecoins on the cryptocurrency market is difficult to measure as their prices remain fairly stable. To quantify the impact of the stablecoin, we analyze the recent Terra-Luna crash with econometric methodologies such as the spillover index and effective transfer entropy. Hourly and 5-minute cryptocurrency prices, Google Trends index and tweets posted on StockTwits were collected and used to measure the spillover effect. Results showed that the spillover effect of the stablecoin increased rapidly as the depeg started, and LUNA gained influence in the overall cryptocurrency market. The effective transfer entropy from LUNA to other cryptocurrencies such as BTC and ETH also increased dramatically. However, investor sentiment lost its role as an information transmitter during the crash, as the effective transfer entropy from the investor sentiment to LUNA decreased significantly. We conclude that the collusion between bearish and bullish opinions about the future of LUNA led to the market sentiment losing its influence.

NFT markets are distinct from traditional cryptocurrency markets due to their uniqueness. This makes it difficult to find the right buyer and seller pair for each individual NFT. To understand the relationship between trading volume of NFTs and their prices, we used the Granger causality test in quantiles. Our data included daily transaction volume and price of NFTs. The results showed that the causality from overall NFT volume to return became stronger in extreme market conditions. However, different NFT projects had different behaviors. For example, Axie Infinity had strong causality in every quantile, while Decentraland only had a causal relationship around the median. Additionally, the transaction volume of The Sandbox was only helpful in forecasting The Sandbox prices during bearish markets conditions. Lastly, we found a strong causal relationship between NFT returns and the return of its in-protocol native cryptocurrencies. Overall, our analysis showed that NFT volume and prices are closely related and should be taken into account when trading NFTs.

This dissertation has explored the various types of digital assets, such as blockchain-based CBDCs, stablecoins, and NFTs. It has proposed a blockchain-based CBDC model to address the current obstacles in traditional and decentralized financial markets. The econometric analysis of stablecoin death spiral has revealed the significant impact of stablecoin on the cryptocurrency and DeFi markets. Additionally, the return-volume causal relationships in the NFT markets have been confirmed, providing guidance to NFT investors in different market conditions.

Keywords: Blockchain, Central Bank Digital Currencies, Stablecoin, Non-Fungible Tokens

Student Number: 2020-34024

Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Motivation of the Dissertation

Blockchain technology was firstly introduced by Nakamoto [2008], along with its native cryptocurrency named Bitcoin. This innovative payment system enabled the users to settle financial transactions without the support of third-parties. Bitcoin achieved this goal by adopting a decentralized framework, which every users in the system are responsible for correctly verifying the transactions and storing the results of the transactions. This system can be considered as a decentralized framework, and unlike the traditional financial transaction systems, blockchain technology does not depend on a single ledger for record keeping. Instead, the participating nodes of the system independently keep their own ledger. As a result, if there is any modification to the historical data of the blockchain, the node can easily detect the modification by comparing it with their own ledger (Tapscott and Tapscott [2017]). However, since the participants can have multiple states of the ledger, the most important goal of the blockchain technology is to achieve consensus among the nodes so that the minority of the nodes cannot tamper the transaction records for their own benefits (Garay et al. [2015], Lashkari and Musilek [2021]). To successfully accomplish this goal, blockchain technology is compromised of different backbone theories including technological concepts such as cryptography (Raikwar et al. [2019]), consensus mechanisms (Mingxiao et al. [2017]), distributed computing (Herlihy [2017]) and also non-technological concepts such as game theory (Liu et al. [2019]), tokenomics (Lo and Medda [2020]), and monetary policy theory (Peters et al. [2015]). With the integration of these state-of-art technologies together, blockchain-based systems were able to provide security of the system while maintaining anonymity of the participants and achieving data integrity.

After the success of Bitcoin as a peer-to-peer ledger system, other blockchain-based cryptocurrency projects were initiated to provide various services with specific purposes. Some of the famous projects are Ethereum(Wood et al. [2014]), Litecoin (Lee [2011]), Algorand (Chen and Micali [2016]), Filecoin (community [2014]), Cardano(Kiayias et al. [2016]) and etc. Since newly developed blockchain projects are emerging everyday until now, there is no doubt that blockchain technology is definitely attracting the talented entrepreneurs to seek opportunities for innovating the current financial market. As a result, we believe that blockchain technology will play a huge role in different financial sectors in the future. Ethereum is one of the most successful blockchain project after Bitcoin, as it is ranked as number two cryptocurrency after Bitcoin in terms of market capitalization. The fundamental difference that Etehreum has brought to the blockchain ecosystem is that it introduced the concept of *smart contracts*. Smart contracts are digital instructions that can be specified by the users, which defines the conditions for spending assets from Ethereum addresses. Smart contract machine of the Ethereum is called as the Ethereum Virtual Machine (EVM) and EVM is known to be Turing complete, assuming that the users have sufficient gas to execute the machine. The Turing completeness of EVM brought numerous innovations to the blockchain ecosystem, as now the users are able to specifically address the terms of financial contracts similar to the ones in the current financial markets directly to the blockchain systems. As a result, many real-life financial applications were implemented on Ethereum. For example, timelock contracts can be used to implement atomic swaps between multiple assets Poon and Dryja [2016]. Currently, the usability of these smart contracts grew even larger, and it led to the formulation of decentralized financial market in the blockchain ecosystems, also called as DeFi. In the next paragarph, we briefly explain the concept of DeFi and stablecoins .

Decentralized Finance (DeFi) With the emergence of smart contracts, DeFi was newly introduced to blockchain systems, offering a new financial infrastructure that is permissionless, publicly verifiable, anonymous and efficient in terms of capital efficiency (Werner et al. [2021]). For a safe implementation of DeFi on top of blockchain systems, the underlying smart contracts should satisfy some conditions. (1) Smart contracts must be expressive enough to fully describe the complicated financial protocols. (2) Smart contracts should support atomic transactions. In other words, the transactions should either success fully, or the transactions should not happen at all. (3) Smart contracts should also support conditional executions so that financial executions are done only when the conditions are met. With proper smart contract functionalities supported, many useful DeFi protocols can be proposed. The most well-known DeFi protocol is decentralized exchanges (DEX), where the users are able to exchange assets on-chain, so that every transactions are publicly verifiable and recorded on the blockchain. Many DEXes such as Uniswap (Adams et al. [2021]), Balancer, and Sushiswap adopt automated market makers (AMMs) (Egorov [2019], Adams et al. [2021]) as their core market making function. In traditional finance, designated market makers are responsible for boosting the liquidity and provide depth in the market by participating in the trades. They possess financial risks on holding the volatile assets, but this risk is compensated as they gain profits from the difference in the bid-ask spreads. On the other hand, AMMs use fairly simple mathematical formulas to automatically provide liquidity and alter the exchange rates between the assets. Liquidity providers in the AMM liquidity pool receive liquidity provider tokens, to prove their portion of the liquidity pool. The transaction fees accumulated from the pool is also distributed to the liquidity providers according to the amount of liquidity provider tokens held. Lending protocols are also prevalent in DeFi, where a market participant can directly borrow loans from the smart contract reserves, by paying the market interest rate. Lending protocols usually come in two different types, namely over-collateralized loans and flash loans. Over-collateralized loans require the borrowers to post collateral, which has a larger value than the value of the borrowed amount. In this way, the protocol ensures the liquidity providers to safely reclaim their lent assets. When the value of collateral falls under certain threshold, liquidators attempt to purchase the collateral that have fallen in price and close the borrower's dept position. On the other hand, Flash loans are borrowed and repaid in a single transaction. If the internal transactions fail or the loans are not repaid at the end of the transaction, then the whole transaction is not executed. With this atomicity, Flash loans are mainly used in DEX arbitrages, where the trades should be completed in a short duration of time.

Stablecoin As these DeFi protocols gain remarkable attention from the public, many complex trading strategies are performed in the DeFi markets. However, due to the volatility of the cryptocurrency markets, these traders need assets with stable prices to mitigate the unexpected risk in their investments. As a result, stablecoins were developed to meet these needs. Stablecoins aim to retain their price relative to their target currencies, mostly the USD, by implementing different stability algorithms and reserve designs. Stablecoins can be categorized by the type of assets that make up their reserves (Catalini and de Gortari [2021]). The key difference between the stablecoins is the different levels on the trust of their reference assets, as some stablecoins are backed with its own blockchain protocol's native cryptocurrency (Kereiakes et al. [2019]), while some are backed with fiat-like assets such as USD or U.S. Treasury bills (Lipton et al. [2020]). The risk and instability of these stablecoins should be analyzed in two perspectives. First, the volatility in the value of the reserves should be measured based on a real world reference asset like USD. Second, the intrinsic relationship between the reserve asset and the stablecoins should be considered (Catalini et al. [2021]). The volatility of the reserved assets can be reduced if the reserves are backed with real-world fiat currencies. However, even though the reserves are backed with highly reliable assets, the protocols still need to provide appropriate capital buffers to mitigate operational risks and an unexpected large-scale liquidation of reserves in short amount of time. The intrinsic relationship between the reserve asset and the stablecoin shows another fundamental risk of stablecoin. If the success of its ecosystem is high correlated with maintaining the value of stablecoin, the likelihood of death spiral is high as the distrust of its native token and protocol among the public can lead to a rapid withdrawal of the stablecoin, not leaving enough time for the arbitragers to gain profit from the depeg and recover the peg. The aforementioned risks can be efficiently mitigated the adoption of central bank digital currencies. Central bank digital currencies are backed by the central banks, so the digital assets and the reserves are both fully controlled by the central bank. Also, the stability of central bank digital currencies is obviously independent from the success of blockchain system.

Central Bank Digital Currencies (CBDCs) The digitalization of economies has led to public demand for digital forms of physical cash, as electronic devices and payment systems become pervasive in people's daily lives (Auer et al. [2022]). To comply with these needs, central banks around the world are considering the adoption of CBDCs as a digital fiat currency. BIS (Bank for Internation Settlments) stated that more than 80% of the central banks worldwide are positive about introducing CBDCs to their domestic payment systems. While there is an ongoing debate on the technological choices of CBDC architecture, blockchain technology is definitely one of the powerful candidates. The advantages of blockchain are expected to benefit CBDC systems, as blockchain can guarantee new efficiency and security for the traditional payment systems Zhang and Huang [2022]. As a result, many researchers have proposed various blockchain-based CBDC schemes (Sun et al. [2017], Tsai et al. [2018], Han et al. [2019], Tian et al. [2018]). The technical definition of CBDCs could differ depending on the purpose of the issuing entity (Committee et al. [2018]). Kumhof and Noone [2018] defines CBDCs having a separate operating structure distinct from the central bank to provide functions for retail transactions and interest payment based on a wider access range than that of bank reserves. Yao

[2018] expands the discussion of CBDCs to digital currencies based on high-level techniques beyond the simple digitization of a fiat currency and refers to the relationship between CBDCs and cryptocurrencies such as Bitcoin or Ethereum , which are based on distributed ledger technologies. Bordo and Levin [2017] divides CBDCs into "token-based" and "account based" according to the configuration rules. Account-based CBDCs would lower transaction costs under the control of the central bank and token-based CBDCs would use to utilize distributed ledger system, like Bitcoin or Ethereum. Bjerg [2017] aims to identify the role of CBDC in each scenario in which CBDCs are used as a complement to cash or deposits, bank reserves or accounting units. The current controversy on the design of CBDC leaves room for financial and technological researchers to continue examining the feasibility of adopting blockchain for financial systems.

Non-Fungible Token (NFT) NFTs are new type of digital currency origniated from blockchain technology. It was proposed in Ethereum blockchain as Ethereum Request for Comment (ERC))-721 token standard, and further developed in ERC-1155 (Wang et al. [2021b]). The main difference between existing cryptocurrencies and NFTs is their uniqueness, which means they cannot be exchanged for equal value with other NFTs. Such feature led to remarkable attention from the public, as now people can store various types of digitalized assets such as digital arts, videos, certificates of ownership on the blockchain. NFTs have been widely implemented, especially in the gaming and metaverse industries. By converting the game itmes into NFTs, the users are able to gain profits by selling NFTs on the secondary NFT markets. Similarly, the users in metaverse can purchase virtual real estate either for their own usage or future investments. As NFTs show significant differences with traditional cryptocurrencies, technlogical and economic analysis on NFTs should be conducted independently.

In this dissertation, we aim to conduct analytical studies on the three types of special digital assets, namely CBDCs, stablecoins, and NFTs. The concept of these assets emerged with the advent of blockchain technology and DeFi, but there has not been a sufficient amount of research on these fields of assets compared to the traditional cryptocurrencies. Therefore, we believe that we can provide a guidance to the future DeFi researchers on selecting their research directions by analyzing the behavior of these assets. (In the case of security tokens, they are still in a very early stage and the size of the funds is small, so they were excluded from the analysis.) For CBDCs, we propose a blockchain-based model to conduct simulation experiments, since there is no CBDC in use yet. For stablecoins and NFTs, we conduct econometric analysis based on their price time series in order to dissect the market behaviors.

1.2 Aims of the Dissertation

This thesis aims to investigate the DeFi market by analyzing three special types of assets originiated from the blockahin technology. First of all, this thesis focuses on developing the blockchain-based CBDCs settlement system, which can mitigate the current financial risks of the existing stablecoins and cryptocurrency markets. As CBDCs are backed by the central banks, we believe that the adoption of CBDCs can enhance the trust among the cryptocurrency market so that the market participants can fully utilize the advantages of DeFi protocols. Also, blockchain-based CBDCs can offer an alternative to current financial transaction systems since it can reduce some of the frictions in the current trade processes. Secondly, we analyze the impact and the connectedness of stablecoins to the overall cryptocurrency market by using econometric methodologies. We specifically focus on the recent crisis of the Terra protocol, which was one of the most prominent stablecoin-based blockchain system. This analysis is also very meaningful when arguing the adoption of CBDCs, as it emphasizes the importance of stability and trust of the stablecoins in the cryptocurrency markets. Lastly, we attempt to understand the NFT markets, by finding causal relationships between NFT volume, NFT return and its in-protocol native cryptocurrencies.

In Chapter 2, we address the major research challenges in CBDCs in terms of security and privacy. Security and privacy of CBDCs emerged as a fundamental issue in the development of CBDCs, as blockchain-based systems greatly differ from the technical structure of current traditional financial systems. We define the two main research challenges in the development of CBDC infrastructure. First, many CBDC researchers inevitably consider a scheme where the authorized participants who manage the transaction details or users identities are introduced, in order to protect user privacy and achive regulatory compliance. Second, most CBDC projects aim to cover both the domestic payment process and payments that occur across geographical distances. Therefore, researchers should pay attention to the multi-chain environment for CBDCs. To address these challenges, we propose a blockchain-based settlement system for CBDCs.[1] as Our model is suitable for CBDCs as it solves the research challenges stated in 2.1. The proposed model adds an administrator ledger to the system to remove settlement failure and improve efficiency in market man-

[1] The work in Chapter 2 was published as Lee et al. [2021a,b].

agement. This administrator ledger achieves auditability for the settlement system, as all the transactions are recorded in the administrator ledger. The main advantage is that even though the proposed model is developed on a multi-chain environment, the adminstrator ledger can collect transaction records from both ledgers (ex.cash and securities ledger). Since our model is designed for different ledgers to trade assets, it can support the cross-border payments setting of two different CBDCs, if both CBDC systems can implement the hashed-timelock contract and our signature scheme. Also, we propose a new lattice-based sequential aggregate signature scheme for the signing process of our proposed model. Lattice-based cryptography is generally known to have advantage on resisting future quantum attacks. Then, security analysis of our system and the proposed signature scheme are conducted. Finally, proof-of-concept experimental results are described.

In Chapter 3, we analyze the impact of stablecoin instability to the cryptocurrency market by investigating the recent historical crash of Terra protocol.[2] We examined the impact of the Terra-LUNA crash on the cryptocurrency market. Based on the hourly return and realized volatility from April 2022 to May 2022, we used the spillover index and effective transfer entropy to configure the interlinkage change between cryptocurrency markets. We conclude that the Terra-LUNA crash had a significant impact on the connectedness of the cryptocurrency market, investor attention, and market sentiment. Our findings confirm that the death spiral of stablecoin can bring about significant shock to the overall cryptocurrency market. Consequently, this result strongly supports the adoption of CBDC, which can perfectly substitute the current stablecoins with zero risk for the market participants.

[2] The work in Chapter 3 was published as Lee et al. [2022].

In Chapter 4, we attempt to spot the causality for return-volume relationship of NFTs i.e. Overall NFT, Axie Infinity, Decentraland, The Sandbox. The price and volume data for the NFTs was collected from Jan 1, 2018 to Mar 30, 2022. Using the Granger causality test in quantiles, we reveal the existence of strong causal relationships between trading volume and log return of NFTs at extreme market conditions. Additionally, we also examine the relationship between NFTs and their in-protocol native cryptocurrencies.

Lastly, we discuss the contributions and future works of this dissertation in Chapter 5.

1.3 Organization of the Disseration

The remainder of the dissertation is organized as follows. In Chapter 2, we list the fundamental research challenges in the development of CBDCs in terms of security and privacy. Then, we propose a CBDC settlement model based on cross-chain atomic swaps. Along with our model, we also propose a lattice-based sequential aggregate signature scheme which can be implemented to our system. In Chapter 3, we analyze the Terra-Luna crash with spillover index and effective transfer entropy to quantify the impact of the death spiral to the other cryptocurrencies market. In Chapter 4, the return-volume relationship of NFT market is examined through Granger causality test in quantiles. Chapter 5 concludes the dissertation by addressing the contributions and future works of the research.

Chapter 2

Analysis on Blockchain-based CBDC Settlement System

2.1 Chapter Overview

CBDCs refer to fiat currencies issued in digital form by a central bank, which is distinct from physical money or the reserve/settlement accounts. However, the technical definition of CBDCs differ because the governments that are considering issuing CBDCs have different purposes. In general, the main purposes for issuing CBDCs are financial stability, monetary policy implementation, financial inclusion, payment efficiency (domestic, cross-border), and payment safety/robustness. However, the situations of each issuing country (dramatic decrease in cash flow, highly volatile fiat currency value, etc.) and the purpose of the CBDC issued (small settlements, large settlements) are different, so the importance of each major purpose will change (Boar et al. [2020]). The issuance of CBDCs can lead to changes in the long-established financial system, such as the emergence of new payment methods, dis-intermediation of commercial banks, and difficulties managing policy management are often cited as problems that CBDCs still need to solve (Auer and Böhme [2020]). In particular, security and privacy in CBDCs emerged as one of the most important discussions because, CBDC can cause structural changes in the financial system itself. The security and privacy issues of CBDC have characteristics that distinguish them from centralized financial systems or public blockchains. Most CBDCs do not aim to make all transaction details public, like Bitcoin, or private, like Zcash. The CBDC issuer is likely to prefer to provide personal information protection to users of the CBDC system under normal circumstances with the ability to reveal transaction information in special situations such as for anti money laundering (AML) provisions or law enforcement.

To this end, in order to weigh the potential of adopting CBDC to the current financial system, we propose a blockchain-based middle ground CBDC model, especially focusing on the securities settlement.[1] Such model can be considered as a type of wholesale CBDC model, because only the designated financial institutions can participate in the securities settlement system. However, we believe that our model can be extended for various purposes in the future. We now briefly explain the obstacles in the current settlement system, and the potential of blockchain technology to them.

Modern financial systems are mostly designed based on delivery versus payment (DvP) (Mills Jr and Nesmith [2008], Summers [1991]), to ensure safety in both cash and securities transfer. In addition, these systems are operated by trusted third parties, usually the central bank and the central securities depository (CSD) (Kroszner et al. [2006]). The central bank is responsible for transferring the cash, and CSD is responsible for trasnferring the securities ownership. The system also needs other intermediaries such as payment agents and brokers, and these intermediaries result in extra financial costs and time due to increased back-office cost and operation risk (Sachs [2016]). As a result, most of the current settlement systems implement

[1] This model is an extended work from Lee [2020], and some of the figures and experimental results from Lee [2020] are used again in this chapter to fully explain our work.

netting process to their system and settle the transactions at T+1, T+2, and so on (Devriese and Mitchell [2006]).

To address this issue, many researchers and central banks are examining the adoption of CBDC (Shah et al. [2020], Ward and Rochemont [2019]), and blockchain technology became one strong candidate for its backbone technology. Blockchain-based CBDC models are frequently discussed in research communities, as blockchain technology can guarantee the transparency of the ledger and the atomicity of the transaction without relying on the third parties Benos et al. [2017], Collomb and Sok [2016]. With the advent of smart contracts (Buterin et al. [2014]), the settlement process can be implemented in the blockchain system with better security and functionalities, by using scripts like Hashed-Timelock Contracts (HTLC).

Nevertheless, with the rapid development of quantum computers, former encryption/signature schemes such as the Elliptic Curve Digital Signature Algorithm (ECDSA) used by Bitcoin and Ethereum, face severe threats. ECDSA enables users to create a 256-bit private key and a public key that can be shared with third parties. With the current technology, it is almost impossible to find the private key by looking at the generated public key. However, as adversaries are equipped with quantum computers, the risk of finding the private keys of these traditional schemes is greatly increased. *Shor's algorithm* Shor [1999] proposed a method that leads to a dramatic improvement in the efficiency of factoring large numbers using the quantum Fourier transform which can pose a serious threat to current ECDSA and, RSA schemes. In addition, the hash functions of proof of work (PoW)-based blockchains are at risk as Grover [1996] showed with his proposal of *Grover's algorithm*, which is a quantum computing solution to the problem of finding a pre-image of a value of a function that is difficult to invert. With quantum computers, attackers can cause hash collision problems. In addition, the adversary can generate modified blocks much faster by speeding up the nonce generation and mining time, which can lead to a regeneration attack on the whole blockchain Li et al. [2018]. To overcome this danger, several post-quantum blockchains based on quantum-secure signature/cryptocurrency schemes have been proposed Li et al. [2018], Gao et al. [2018], Li et al. [2021], Wu et al. [2021], Shahid et al. [2020]. To enable our settlement protocol to address these future threats, we introduce a lattice-based signature scheme into our settlement model, which is widely known to be resistant to quantum attacks Gao et al. [2018].

To this end, our work focuses on these three issues. We propose a blockchain-based CBDC settlement system along with a lattice-based digital signature scheme, and then we conduct extensive experiments and security analysis to verify our proposed approach. The contributions of this chapter are summarized as follows:

- We provide a comprehensive taxnonomy on the current CBDC research and list the main challenges in the current CBDC research/design.
- We propose a blockchain-based settlement protocol for CBDC that ensures safe trading among the market participants.
- We propose a lattice-based sequential aggregate signature scheme for our settlement protocol, as lattice-based cryptography is generally known to have the advantage on resisting future quantum attacks.
- We conduct proof-of-concept (PoC) experiments for our model using the real-world securities settlement data.

In this chapter, we aim to deal with major issues related to the privacy and security of CBDCs upon implementation from a middle-ground position. Section 2.2.1 describes the privacy and security issues related to the implementation of CBDCs and define our research goal. Section 2.3 explain the background for our research. Section 2.4 describes our proposed model. Section 2.6 shows the experimental results. Finally, Section 2.7 discusses the summary and significance of the study.

2.2 Defining our CBDC research goal

2.2.1 Security and Privacy issues in CBDCs

There are different kinds of CBDC design models, and each has its own level of privacy and security. For example, in a permissioned blockchain where a small number of entities can see and verify all transactions, the whole transaction log including the identities of the participants, is open to those entities, but the transactions are completely hidden from the public. However, the entity nodes should be highly trusted. If they get attacked or hacked, all the transaction data might be leaked, so this entails a huge security risk. Otherwise, single points of failure are less likely to happen in a public blockchain, like Bitcoin and Ethereum. If all transactions are unencrypted on the public blockchain, then we need not trust any third party and can have relative security from specific node attacks. However, the transactions are open to everyone participating in the blockchain, thus providing a low level of privacy. As shown in Nick [2015], although users take pseudonyms that seem to be anonymous, they are linked with outside information and it is easy to uncover the identities of real users.

From the perspective of the middle ground in designing CBDCs, it is necessary to provide a sufficient level of privacy and security to users, while ensuring compliance with regulations such as AML. There are several cryptographic and systematic approaches that can be applied to the blockchain to enhance security and privacy at the cost of complexity, which we discuss in the following sections.

Identity Privacy

Identity Privacy is the ability to hide the identities of the users participating in the system. Identity privacy might vary considerably between systems, differing in its openness and transaction verifying process. Darbha and Arora [2020] summarizes the privacy level of many different platforms including Bitcoin, the credit card system, and cash. User identities might be leaked in three different situations. First, as mentioned above, blockchain systems that only use pseudonyms for privacy are vulnerable to de-anonymization. The transaction patterns of each user might be exposed, such that it is possible to predict his or her future behavior. In a worse case, the transaction itself would be combined with outside information and the transaction participants might be linked with their real identities. Figure 2.1 shows that blockchain users can be easily de-anonymized when transactions are open to all and outside information is obtainable. Second, at a network level, a light node might ask the full node about the existence of transactions, and those queries as well as network data(e.g., IP address) might be good hints at a user's identity, as discussed in Allen et al. [2020]. Third, CBDCs are likely to comply with know your customer(KYC) provisions to easily deal with AML, and law enforcement. Middle-ground CBDCs, unlike public blockchain systems, might require some special nodes to store personal data with proper classification. These special entities are highly likely to be exposed to a single point of failure, which can result in the indirect leakage of personal data, including user identities.

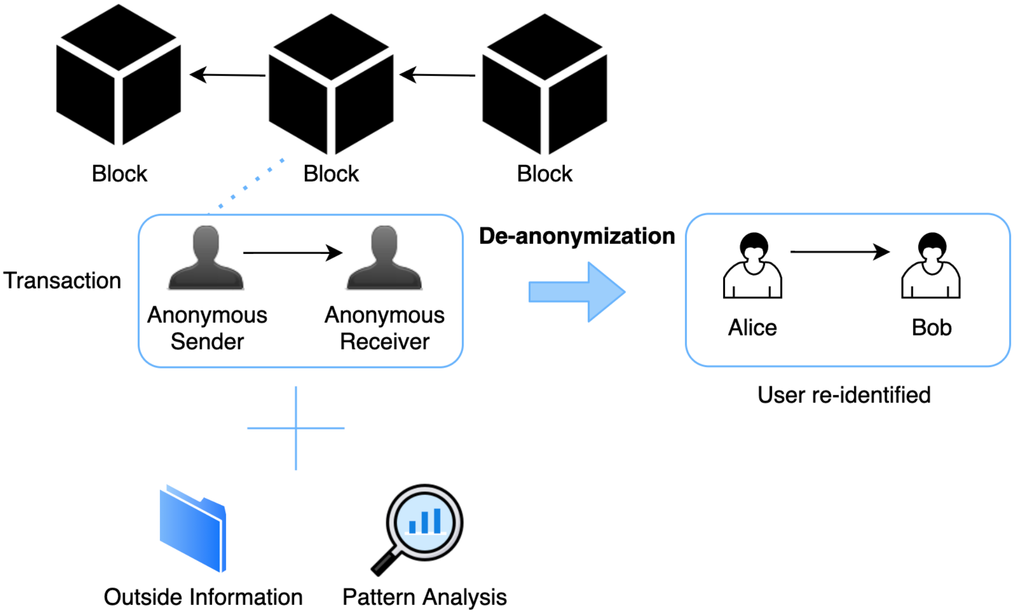


Figure 2.1: De-anonymization of users by combining the transaction pattern with auxiliary user information

De-anonymization

Many public blockchain systems, such as Bitcoin and Ethereum, have transaction structures that show the sender and receiver addresses explicitly. Because of this property of openness, a large proportion of the users can be re-identified by different ways. Feng et al. [2019] lists several attacks for de-anonymizing users' real identities: network analysis, address clustering, and transaction fingerprinting. These attacks make use of IP addresses, clustered addresses, and transaction analysis and combine them with any outside information to identify users. Several cryptographic approaches can make this re-identification process intractable and ensure that the transactions are encrypted. Some studies apply them to propose new blockchain-based CBDC designs.

Secure Multi Party Computations (MPC) One way to prevent de-anonymization is to implement MPC, which enables jointly computing a function with participants' inputs while keeping each input private. This idea can be applied to Real-time Gross Settlement (RTGS) systems, where several commercial banks make high-value fund transfers to each other. Atapoor et al. [2021] proposes a MPC based solution to perform the liquidity optimization for decentralized RTGS system, keeping their transactions confidential. They show three versions, one of which keeps the source and destination private, as well as the transaction amount.

Zero Knowledge Proof (ZKP) ZKP is also being used as a building block for private identities. Zerocash (Sasson et al. [2014]), known as Zcash is widely known for using zerok-knowledge succinct noninteractive argument of knowledge proofs (zk-SNARKs) to prove the validity of transactions without revealing the participants or the amount. However, as shown in Kappos et al. [2018], Zcash users are identifiable using heuristics based on patterns of usage. Dai et al. [2020] attempts to protect the anonymity of commercial banks in an indirect CBDC model by proposing a supervised anonymous issuance (SAI) scheme, using zk-SNARKs and a multi-receiver signature encryption scheme. The scheme ensures that the issuer's identity remain hidden while allowing other commercial banks to verify whether the issuance is allowable and the issuer is qualified. Gross et al. [2021] proposes a CBDC system design that allow fully private transfers between users while still complying with AML regulations by imposing limits on private transfers, using zk-SNARKs.

Ring Signatures Ring signatures are another option to obscure identities in a transaction. First introduced by Rivest et al. [2001], ring signatures make it possible to specify a set of possible signers without revealing which member actually produced the signature. Monero uses Ring Confidential Trasnaction (RingCT) Noether [2015] to hide the sender's identity by combining it with a set of fake senders and amount of the transaction. However, Miller et al. [2017] shows that this mixing strategy is still vulnerable to re-identification. There are few studies on CBDC designs attempting to take advantage of ring signatures. Goodell et al. [2021] proposes a CBDC system based on a permissioned blockchain, with non-custodial wallets for privacy-preserving purposes. The proposed model suggests ring signatures, ZKP, and stealth address as building blocks of non-custodial wallets, which offer retail users cash-like anonymity.

Systematic Approaches There are some proposed systematic approaches for hiding transactions, including the identities of the participants. Calle and Eidan [2020] proposes Corda, which creates a private permissioned environment where, all transaction data are shared only between the counterparties of transaction, so outsiders cannot even know that the transaction is happening in the first place. The transaction is validated by those counterparties, and a notary pool attests the uniqueness of each transaction, ensuring the security of the transactions.

Network-level attack

De-anonymization of identities is not the only risk in CBDC designs. There might be risks inherent to the network or node communication. For example, nodes that have more permissions compared to other nodes are likely to receive more privacy-sensitive requests. Retail users, especially when using their mobile phones, are not likely to hold the full set of block data. They might ask the validator node or full node, which stores the whole blockchain, if a specific transaction they are interested in is contained in the block or not. In that situation, the validator node itself, which takes the light client's requests, might know which transaction this client is interested in. In p2p networks, another malicious peer node might see this request unless it is encrypted.

The Bitcoin network has a similar privacy issue. To solve this issue, SPV nodes in Bitcoin use a bloom filter to ask for transactions of interest. They do not specify the exact transaction, and they can handle the level of privacy by controlling the parameters of bloom filters.

From the perspective of the middle-ground, network-level attacks might be more severe since those requests are more likely to contain more privacy-sensitive data to enable the compliance with AML/ Combating the Financing of Terrorism (CFT) regulations. The Skipchain (Kokoris Kogias [2019]) structure enables validation of blocks without the need for privacy-preserving queries. CBDC designs can adopt this structure for a robust approach.

Transaction privacy

Public blockchain networks make every participating nodes able to save the blockchain which holds the transaction history. It strengthens the transparency and privacy of the blockchain network because everyone can see the change in the blockchain when a malicious attacker tries to manipulate previously issued and recorded transactions on the blockchain. However, compared to the current securities settlement system or bank account system, opening transaction details to the public is an apparent threat to privacy.

As discussed above, privacy issues on the blockchain exist because transaction details are recorded in the blockchain. Therefore, we classify potential privacy threats according to the content of the transaction to be protected. The first category is data privacy, which implies the protection of the identities of the sender and receiver, or protecting the token amount of the transaction. The second is program privacy. Blockchain transactions can contain any type of programming code (i.e., a smart contract). Even when smart contract issuers intend to use them for commercial purposes, smart contract code becomes open-source intentionally. Finally, program privacy explains how to protect program code on blockchain.

Data Privacy

Data privacy includes protecting the participant identities and transactions amount in a transaction. It is hard problem to solve because the key property to maintain is the recording of the transaction on the blockchain. Therefore, schemes hiding transaction details using encryption techniques are proposed.

Secure MPCs The goal of MPC (Yao [1982]) is to ensure that make multiple parties can compute a function that requires inputs from parties jointly while not revealing their own private inputs to each other. After Yao [1982] proposed a two-party MPC protocol, Goldreich et al. [2019] proposed a general framework for multi-party MPCs.

Rethinking the purpose of recording transactions on a public blockchain in a block, blockchain systems must be able to check the transaction availability by computing the sum of the sending transaction amount and receiving transaction amount.

If we think of the computing procedure as the objective function of an MPC, the MPC can be used to protect transaction data details by encrypting transactions by setting participating receivers and senders as parties of the MPC.

Atapoor et al. [2021] proposed a secure MPC-based solution to manage the RTGS system in decentralized settings. The proposed system ensures the privacy of the entities in an MPC, by hiding the amounts, the source addresses of each transaction, or the destinations. Corda, the protocol proposed by Calle and Eidan [2020] uses similar scheme as MPC. It makes participants of a transaction share data only with each other and ensures that the private input of any party is not revealed to the public. It is different from MPCs in which other parties participating in transactions can find other participants' private inputs, but MPCs are still applicable to Corda.

Homomorphic Encryption Rivest et al. [1978] introduced homomorphic encryption, which is a scheme that enables computation on ciphertext resulting in the same result as computation on plaintext. In the same sense as MPCs, homomorphic encryption enables the system to encrypt transaction amounts while the blockchain system can verify the transaction. For an application of homomorphic encryption in a blockchain system, Wang et al. [2020] proposed an improved system of Zerocoin (Miers et al. [2013]), a Bitcoin-based transaction system that can hide the amounts of the transaction. The proposed scheme encrypts the transaction amounts with a homomorphic property. In terms of functionality, the proposed scheme can arbitrarily encrypt amounts in frequent transactions and use them for homomorphic computations, while Zerocoin supports only certain divided values besides other arbitrary values in real transactions.

ZKPs ZKPs are one of the most widely used privacy-preserving schemes. ZKP schemes enable entities to prove a claim without revealing their own private inputs. When a ZKP scheme is applied in blockchain system, transaction participants can prove their positive balance without revealing the actual transaction amount. Hopwood et al. [2016] proposed a shielded payment scheme Zcash using zk-SNARKs to hide the addresses of the transaction sender and receiver.

Program Privacy

Writing smart contract requires the code writer to understand cryptographic technologies and consensus algorithms of a distributed ledger. Furthermore, one of the biggest problems in executing smart contracts on a blockchain is the privacy limitation. The privacy of smart contracts means both privacy for the programming code and privacy for the input data of the smart contract.

Kosba et al. [2016] protected the input of smart contracts by executing the smart contract off-chain. It restricts the role of the on-chain blockchain system to verify the result of the executions using ZKP. Al-Bassam et al. [2017] and Kalodner et al. [2018] proposed similar ideas around executing smart contracts somewhere away from the main blockchain. Even though the proposed schemes protect privacy for most entities, potential threats remain because centralized nodes such as a manager or client are responsible for executing the smart contract. Protean, proposed by Alp et al. [2019], provides special functional units to avoid having all nodes keep smart contracts and computations. The functional units consist of a randomness unit, state unit, execution unit, and private storage unit to run secure specialized modules that cannot be implemented securely by a smart contract.

For a specific application of secure smart contracts, Niya et al. [2018] used se-

	Identity Privacy	
	De-anoymization	Network-level attack
Secure Multiparty Computation	Atapoor et al. [2021]	-
Zero Knowledge Proof	Sasson et al. [2014] , Kappos et al. [2018] , Dai et al. [2020] , Gross et al. [2021]	-
Ring Signature	Rivest et al. [2001] , Miller et al. [2017] , Goodell et al. [2021]	-
Homomorphic Encryption	-	-
Others	Calle and Eidan [2020]	Kokoris Kogias [2019]

Table 2.1: Classification of the privacy-preserving techniques used in CBDC models: Identity privacy

	Transaction Privacy	
	Data Privacy	Program Privacy
Secure Multiparty Computation	Atapoor et al. [2021], Calle and Eidan [2020]	-
Zero Knowledge Proof	Hopwood et al. [2016]	-
Ring Signature	-	-
Homomorphic Encryption	Wang et al. [2020]	-
Others	-	Kosba et al. [2016] , Al-Bassam et al. [2017], Kalodner et al. [2018] , Alp et al. [2019] , Niya et al. [2018] , Unterweger et al. [2018]

Table 2.2: Classification of the privacy-preserving techniques used in CBDC models: Transaction Privacy

cure device-to-device communication mechanism in a trading system to protect the deposit data of sellers and buyers. Unterweger et al. [2018] implemented a privacy-preserving smart contract on the Ethereum platform with their proposed smart contract structure. Table 2.1 and 2.2 summarize the classification of various privacy-preserving techniques implemented in past research that aim to maintain identity and transaction privacy.

Consensus and Auditability

Blockchain-based models for CBDCs differ from the existing public cryptocurrencies as most CBDCs aim to take the advantage of blockchain technology while maintaining control over monetary issuance and supply. While blockchain technology can bring about innovation in the current financial market structure as it enables value transfer between two entities without a trusted third-party, it also possesses some problems in terms of scalability and resource allocation due to its distributed setting. To solve such problems, many researchers proposed blockchain-based middle-ground CBDC architectures with different layers where the participating entities of each layer are given different permissions and roles. In this section, we discuss the security issues to consider when designing these middle-ground models.

Consensus

The traditional blockchain consensus mechanisms such as Proof-of-Work(PoW) cannot be implemented directly in middle-ground models as these consensus mechanisms require all nodes to be "full" nodes. In other words, typical PoW mechanisms require that all nodes have the ability to mine a new valid block and store the full blockchain in their own storage system. However, as CBDCs aim to become a versatile currency throughout a nation, it is very impractical for all users to participate in the consensus protocol. Thus, several variations in which only the designated nodes participate in the consensus process were proposed for CBDCs. These specific security properties should be considered in these CBDC models.

No Double-Spending: Double-spending is the act of transferring cash that has already been used previously. Different from a physical currency, CBDC transactions should be verified to check whether the currency was used only once by one user at a time. This is the most basic security property that blockchain-based CBDCs should meet.

Non-Repudiation: Non-repudiation requires that all the participants' actions in the payment process are recorded correctly, so they cannot deny any of the actions that they processed in the past.

Unforgeability: Similar to preventing counterfeiting of physical cash, CBDCs should not be issued by institutions or individuals besides the central bank.

Danezis and Meiklejohn [2015] proposed the first hybrid blockchain-based CBDC framework, namely RSCoin, which can provide the centralization of a monetary authority to a certain entity (eg. central banks) and keep the blockchain's transparency. RSCoin introduces mintettes as their system intermediaries, which are responsible for maintaining the transaction ledger. These mintettes can be represented as the full node in the traditional blockchain, but the difference is that they produce a lower-level block, which should be sent to the central bank for higher-level block production. These higher blocks form a chain, which is then exposed to the other external users. Zhang et al. [2021] argued the limitations of traditional PoW, Proof-of-Stake(PoS), Practical Byzantine Fault Tolerance(PBFT) and Delegated Proof-of-Stake(DPOS) mechanisms in their hybrid model, and proposed a new consensus mechanism called POA-PBFT which showed improvements over the DPOS-BFT algorithm. POA-PBFT changes the election process of bookkeeping nodes from voting by all the participants to direct modifications by the central bank. Additionally, the block producers in the original DPOS algorithm have freedom to increase the block number as they wish, but in the POA-PBFT setting, a designated node specified by the central bank has the authority to produce a fixed block-number block. This can effectively reduce the probability of forked chains, as the chain cannot grow freely if the specified node does not proceed in block production.

Auditability

As we mentioned in the previous section, blockchain-based CBDC systems with a middle ground approach differ from the traditional blockchain mechanisms as they permit different levels of authority for different nodes. Consequently, most CBDC architectures divide the participating nodes into different layers, and the main difference between these CBDC schemes and decentralized cryptocurrencies is in the regulatory layer nodes. The nodes in the regulatory layer are responsible for monitoring the whole CBDC cycle including verifying transactions, issuing the CBDC, and monitoring the system, such that the CBDC system can provide a safe asset transfer environment for the lower-level users.

Regulatory compliance is one of the key areas with which CBDC must comply. Most governments or related institutions, potential operators of CBDCs, aim to protect the economy against malicious economic activities such as money laundering or tax evasion. CBDC systems should have auditability as a function; however this conflicts with the fundamental characteristics of a public blockchain. The fundamental characteristics of a blockchain include that the owner of the asset has full authority to decide when, how much, and to whom a transaction is issued and whether or not to disclose the details. In contrast, the auditability of a CBDC must prevent transactions that do not comply with regulations, regardless of the intent or preference of the asset owner, while maintaining the privacy and security of legitimate transactions. CBDCs are inevitably distinct from public blockchains or the existing centralized structure, and have no choice but to have a middle-ground form. Recent research efforts explored how to implement an auditable distributed ledger system. How to implement auditability in CBDC systems is an open research area. There are various technological building blocks for such designs already. We provide a taxonomy of auditability technologies based on system configuration considerations including which ledger is introduced to the CBDC system, the extent that it covers privacy, and the cryptographic techniques leveraged. A CBDC ledger could be "permissioned" or "permissionless" depending on whether authorization is required to read, maintain, or especially, write, the ledger. Most CBDC designs prefer a "permissioned" ledger because most of them force predetermined auditors audit assigned transactions. However, a few studies implement auditability in ledgers such as a public blockchain. We also cover how auditability functions are implemented differently for the two types of ledgers: "ledger-based" and "token-based" also known as the untransacted transaction output(UTXO) model. We investigate the extent to which each implemented audit function guarantees the privacy range discussed in Section 2.2.1 and 2.2.1. In accordance with the extent to which privacy is guaranteed, we use the following notations: S(sender identities), R(receiver identities), and T(transactions).

Camenisch et al. [2006] do not mention that they propose permissioned ledgers, but discuss auditability under the assumption that there are authorized users who can manage the database. The authors implement auditability by limiting the total amount of tradable transactions for a certain period instead of verifying the transaction contents in a zero-knowledge-based manner. In this system, only the sender remains anonymous, regardless of the recipient and transaction amount. Only when the transaction amount limit is reached, can the public key of the sender can be estimated through the signatures of the auditor and the recipient, though it is also possible to track the transaction history with the public key.

In the context of permissioned ledgers, Androulaki et al. [2020] presents a privacy-preserving token management system for permissioned blockchains that also supports fine-grained auditing. The authors leverage advanced cryptographic techniques such as verifiable random function (VRF), Elgamel encryption, Groth signatures, Pedersen commitments, Pointchevavl-Sanders signatures to overcome the strong trusted setup assumption, which is a common and well-known disadvantage of zk-SNARK. Authorized auditors audit transactions without disclosing the contents of the transactions within their framework. Garman et al. [2016] proposes implementing auditability based on strong privacy protection using zkSNARKs under the permissioned and UTXO-based CBDC structure. They propose a modified Zcash model that includes predetermined administrators who proceed with additional signatures when the transaction amount exceeds the upper limit. The disadvantage of this method is that it requires strong trust setup assumptions as mentioned above. Bontekoe [2020] is similar to Garman et al. [2016], but, adopts an account-based ledger system. They introduce the KYC process before participating to the transaction network and implements dedicated agencies to manage transaction details post-event.

Chaum et al. [2021] suggests a similar technique, called the blind signature (Chaum [1983]), for implementing a CBDC system that preserves transaction privacy and fulfill regulatory requirements. Their asymmetric approach can conceal the identity of senders, but not that of receivers.

Tinn and Dubach [2021] provides a similar privacy function with the technology of Chaum et al. [2021] through zkSNARKs. Veneris et al. [2021] propose a CBDC framework that does not expose transaction details, but keeps the identity of the sender private. They also adopt a hardware-based solution to provide private execution of transactions, even when users are offline. Table 2.3 summarizes the taxonomy of the auditability techniques in CBDCs.

Auditability system	Ledger structure	Assumptions	UTXO or Account-based	Cryptographic shemes	Privacy
Camenisch et al. [2006]	-	Total limit	UTXO	ZKP	S
Androulaki et al. [2020]	Permissioned	Authorized auditors	UTXO	VRF Groth sig.	S,R,T
Garman et al. [2016]	Permissioned	Authorized auditors	UTXO	zkSNARKs	S,R,T
Bontekoe [2020]	Permissioned	Authorized auditors	Account -based	zkSNARKs	S,R,T
Chaum et al. [2021]	Permissioned	Authorized auditors	UTXO	blind-sig.	S
Tinn and Dubach [2021]	Permissioned	Authorized auditors	UTXO	zkSNARKs	S
Veneris et al. [2021]	Permissioned	Authorized auditors	Account -based	temper-proof hardware	S

Table 2.3: Taxonomy of the auditability techniques of the CBDC

2.2.2 Our Research Challenges in CBDC

From the consumer needs that CBDCs could address, Auer and Böhme [2020] derives the main design choices of CBDCs: architecture, central bank infrastructure, access technologies, and retail or wholesale interlinkages. The architecture of CBDCs constitutes whether the CBDC will be a direct claim on the central bank or an indirect claim through intermediaries and the operational roles of the participants in the CBDC system including the central bank or other intermediaries. The CBDC infrastructure decides whether the ledger database would be a decentralized ledger system or conventional central ledger system. Access technology addresses the privacy and accessibility issues for users. Most academic studies on cryptography with a focus on privacy-oriented digital payment systems contribute to the enhancement of access technology. Retail or wholesale interlinkages, which is the last design component of CBDCs, relate to specific tehcniques for implementing corss-border payments. Components besides access technology based on privacy-enhancing needs are relatively less discussed in academic and industrial fields. We present the research gaps in these sectors from a privacy and security perspectives. In consideration with designing CBDC, our research goal is to design a system with (1) an authorized auditor and (2) cross-chain functionalities. We briefly explain these goals in the next paragraph.

Authorized Auditor Risk All design elements of the CBDC system mentioned above should be closely connected and operated to implement a safe CBDC system that satisfies the needs of users. In relation to the architecture and infrastructure elements, the distribution of the roles of each system participant and the discussion of the ledger database structure relates directly to the consensus on the transaction details between users, which means the extent of the security of the entire ledger system. In particular, CBDC systems often suffer from high computational costs when applying privacy-enhancing technologies based on cryptography such as ZKP because a promising CBDC system, unlike public blockchains, aim to provide an additional auditability function. In addition, linking CBDC account with the identity of the real user when necessary is inevitable for AML/CFT control.

Therefore, many researchers inevitably adopt a scheme where the authorized participants who manage the transaction details or user identities are introduced to protect user privacy and achieve regulatory compliance simultaneously (Camenisch et al. [2006], Androulaki et al. [2020], Garman et al. [2016], Bontekoe [2020], Chaum et al. [2021], Tinn and Dubach [2021], Veneris et al. [2021]). It is necessary to specify the authority and limits of system members with authority besides the central bank; however, such discussions are relatively scarce. In addition, most studies assume that users with additional privileges are all honest and have no incentive to act maliciously in the system, which is in stark contrast to the general public blockchain. The field seems to need a wide discussion on how to keep malicious behavior between users with different privileges in check to claim enhanced privacy and security through the distribution of privileged users in a CBDC system beyond the centralized form. Currently, research on how the participation of malicious users affects the consensus and security of the entire network in general public blockchains such as Bitcoin and Ethereum is conducted from the game theory, economics, cryptographic, and computer network perspectives. Studies considering malicious authorized players in a CBDC system would bridge the gap between the security analysis of public blockchain consensus and that of the "middle-ground" CBDC system consensus.

Cross-border Payments with CBDCs Most CBDC projects aim to cover both the domestic payment process and, payments that occur across geographical distances, or cross-border payments. Many researchers believe in the potential of CBDC technology to reduce the current inefficiency in cross-border payments. To incorporate cross-border payments in CBDC system, blockchain-based CBDCs should consider cross-chain swap methods, as cross-border payments typically must transfer multiple currencies on different ledgers. Auer et al. [2021] argues that the benefits of CBDC technology would be difficult to achieve in cross-border environments, unless the government or central banks consider the cross-border aspects from the ground when designing their own CBDC systems. However, most of the current research on security or privacy in CBDCs are not focused on multi-chain environments, but rather on a single-chain payment system. Thus, cross-border payments on CBDCs introduces new challenges. Although it is common to assume that the central banks responsible for individual CBDC chains are trustworthy, the trustworthiness of foreign central banks cannot be guaranteed. Accordingly, the privacy model and the security model of cross-border CBDC payments requires fresh consideration.

Privacy-preserving techniques with multiple chains, should guarantee that the participating nodes have access to only the transactions they are related to. Therefore typical homomorphic encryption schemes cannot be used because the secret key holders should not be able to utilize a common secret key to decrypt the other chain's transaction data. Thus, some variants of the fully homomorphic encryption schemes can be used to solve such problems. López-Alt et al. [2012] proposed an on-the-fly multiparty computation model based on a multikey homomorphic scheme, which is capable of computing inputs encrypted with multiple secret keys. Additionally, Chen et al. [2019] designed a multikey-homomorphic encryption using TFHE (Chillotti et al. [2016]) (homomorphic encryption scheme based on ring learning with errors), which enables the secure computation of multiple ciphertexts encrypted with different keys followed by bootstrapping. Future researchers might refer to these multikey homomorphic encryption schemes to design CBDC payment systems that can successfully execute transactions with other CBDC chains that use different secret keys.

In terms of consensus mechanisms, cross-chain payment systems should also meet the security requirements mentioned in Section 2.2.1. As ledger updates in different chains occur asynchronously, new transaction execution protocols are needed to account for the atomicity of transactions between the nodes on distinct blockchains. Herlihy [2018] proposed a method to safely transfer numerous assets between multiple blockchains that incorporates a hashed timelock contract (HTLC) in the transactions. HTLC is a technology that uses pre-defined time boundaries (timelock) and secret hash values (hashlock) for executing the transactions. Some ongoing CBDC projects such as European Central Bank, Bank of Japan [2019] considered cross-border payments with on-ledger escrow using HTLC or conditionial payment channels with HTLC. However, there is still room for improvement as the proposed protocol guarantees the safety of payments only with several preconditions. In addition, HTLC possesses its own failure-to-deliver scenarios that require analysis.

2.3 Preliminaries

2.3.1 CBDC: State of Adoption

This section addresses the current state of CBDC research worldwide. Many central banks are showing great interest in examining the strength of blockchain-based CBDC systems. We briefly introduce some of them.

Project Stella Project Stella is a joint research effort between the Bank of Japan and the European Central Bank aimed at exploring the use of distributed ledger technology (DLT) for handling linked obligations such as securities and cash (European Central Bank, Bank of Japan [2018]).The research focuses on developing a cross-ledger delivery versus payment system without connections, and has demonstrated its viability as a new settlement system. The study utilizes the hash time-locked contract (HTLC) technology as its core. In the process, one participant (buyer/seller) acts as the leader in the settlement and creates a secret and a transaction, while the counterparty then creates a transaction with the same secret. However, the research is limited as it does not solve the critical risk of the HTLC, where the follower is exposed to failure-to-deliver scenarios.

Project Ubin Project Ubin is a collaboration between MAS and SGX aimed at demonstrating the feasibility of using Distributed Ledger Technology (DLT) for interbank payments(MAS, SGX, Anquan Capital, Deloitt, Nasdaq [2018]). It is comprised of six phases, with phase III focusing on two separate blockchain-based DvP functionality. The project also employs HTLC as its trading technology, with the addition of RMO node to act as an arbitrator to prevent failure-to-deliver scenarios. The RMO node acts as the leader in trade, choosing a secret value and timelock for transactions, and the protocol uses a multi-signature system for settlement which can be rolled back with the agreement of two of the three participants (RMO, buyer, and seller).

Project Jasper Project Jasper is a study aimed at examining the potential and capabilities of implementing a DLT-based securities market in Canada (Bank of Canada, TMX Group, Payments Canada, Accenture, R3 [2018]). The proof of concept focused on three areas: technical, operational, and cash/collateral efficiency. The PoC involved setting up a CDS node as the central counterparty (CCP). At the end of each market day, the CDS node collects all transaction records and performs a netting process to calculate the individual net positions of all market intermediaries. The settlement process is then carried out in a sequential order from the largest transaction amount to the smallest, and all completed settlements can be used for the next settlement.

2.3.2 Cryptographic Background

Lattice-based Scheme Shor [1999] proposed the use of quantum algorithms that can efficiently solve integer factorization or discrete logarithm problems, whose hardness is the basis of the most number-theoretic cryptography. However, no quantum algorithm has been proposed to efficiently solve widely used lattice problems. The seminal work of Ajtai [1996] introduced the average-case short integer solution (SIS) problem and showed that, in the worst case, its solution is at least as difficult as the other lattice problems including GapSVP_γ and SIVP_γ.

Definition 2.1. *Shortest Vector Problem (SVP_γ) : Given an n-dimensional lattice $\mathcal{L}(\mathbf{B})$ with its basis $\mathbf{B}$, find a nonzero $\mathbf{v} \in \mathcal{L}$ such that $\|\mathbf{v}\| \leq \gamma \cdot \lambda_1(\mathcal{L})$. Here $\lambda_1(\mathcal{L})$ is the shortest nonzero vector in $\mathcal{L}$.*

Definition 2.2. *Decisional approximate SVP (GapSVP_γ) : Given an n-dimensional lattice $\mathcal{L}(\mathbf{B})$ with its basis $\mathbf{B}$, determine whether $\lambda_1(\mathcal{L}) \leq 1$ or $\lambda_1(\mathcal{L}) > \gamma$.*

Definition 2.3. *(Approximate) Shortest Independent Vectors Problem (SIVP_γ) : Given an full-rank n-dimensional lattice $\mathcal{L}(\mathbf{B})$ with its basis $\mathbf{B}$, find n linearly independent vectors $\mathbf{s}_i \in \mathcal{L}$ ($i = 1, \dots, n$) such that $\|\mathbf{s}_i\| \leq \gamma \cdot \lambda_n(\mathcal{L})$ for all i. Here $\lambda_n(\mathcal{L})$ is the smallest value of u where the maximum norm of n independent vectors in $\mathcal{L}$ is at most u.*

Definition 2.4. *Short Integer Solution ($SIS_{q,n,m,\beta}$) : Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ whose columns $\mathbf{a}_i \in \mathbb{Z}_q^n$ are chosen uniformly randomly, output a nonzero $\mathbf{v} \in \mathbb{Z}^m$ with $\|\mathbf{v}\| \leq \beta$ which satisfies $f_{\mathbf{A}}(\mathbf{v}) := \mathbf{A}\mathbf{v} = \sum_i \mathbf{a}_i \cdot v_i = \mathbf{0} \in \mathbb{Z}_q^n$.*

In the above definition, the function family $\{f_{\mathbf{A}}\}$ should be collision resistant for the hardness of the SIS problem. In addition, the SIS problem can be considered as an average-case SVP for "q-ary" m-dimensional integer lattices, which are defined as:

$$\mathcal{L}_q^{\perp}(\mathbf{A}) := \{\mathbf{v} \in \mathbb{Z}^m : \mathbf{A}\mathbf{v} = \mathbf{0} \in \mathbb{Z}_q^n\} \tag{2.1}$$

Definition 2.5. *The continuous Gaussian distribution over $\mathbb{R}^n$ is defined by probability density function $f(\mathbf{x}) := \rho^n_{\mathbf{z},\sigma}(\mathbf{x}) = (\frac{1}{\sqrt{2\pi\sigma^2}})^n \exp(-\frac{\|\mathbf{x}-\mathbf{z}\|^2}{2\sigma^2})$, where the distribution is centered at $\mathbf{z}$.*

Definition 2.6. *The discrete Gaussian distribution $D^n_{\mathbf{z},\sigma}$ over $\mathbb{Z}^n$ is defined as $D^n_{\mathbf{z},\sigma}(\mathbf{x}) := \rho^n_{\mathbf{z},\sigma}(\mathbf{x})/\rho^n_\sigma(\mathbb{Z}^n)$, where $\rho^n_\sigma(\mathbb{Z}^n) = \sum_{\mathbf{y}\in\mathbb{Z}^n} \rho^m_{\mathbf{z},\sigma}(\mathbf{y})$ is the scaling factor.*

Definition 2.7. *A digital signature scheme consists of 3 (probabilistic) polynomial-time algorithms, KeyGen, Sign, Verify that satisfy for any message $\mathbf{m}$, $\Pr[\mathsf{Verify}(\mathbf{p}, \mathbf{m}, \sigma) = 1 : (\mathbf{p}, \mathbf{s}) \leftarrow \mathsf{KeyGen}(1^\lambda), \sigma \leftarrow \mathsf{Sign}(\mathbf{s}, \mathbf{m})] = 1$*

Sequential Aggregate Signatures Aggregate signatures (AS)Boneh et al. [2003] are designed to allow multiple users to sign distinct messages on one unified signature. In an AS scheme, each participant i produces his or her own signature σ_i and the signatures are combined into an aggregate signature σ whose size does not differ from an individual signature. However, in several real-world applications including certificate chains, it is important to verify the order of the signatures. Signature schemes that support this type of situation are called sequential aggregate signatures (SAS).

As stated in Lysyanskaya et al. [2004], SAS scheme takes signing and aggregation as a single operation. The operation takes as input each participant i's private key SK_i, a message m_i, and a previous sequential aggregate σ_{i-1} on messages m_1 to m_{i-1} under public keys PK_1 to PK_{i-1}. Then it combines the signature on the new message m_i to σ_{i-1}, producing a sequential aggregate σ_i on all i messages m_1 to m_i. The verifying algorithms return errors when the order of public keys and messages (and probably some additional information) does not match the signing order under given keys. Borrowing much of Neven [2008]'s idea, El Bansarkhani and Buchmann [2014] developed the first SAS scheme based on a lattice problem. The scheme is demonstrated in the famous GPV-signature scheme Gentry et al. [2008] and can be easily applied to any lattice trapdoor-based hash-and-sign signatures.

In addition to trapdoor-based hash-and-sign digital signature schemes, several signature schemes have been proposed based on the Fiat-Shamir heuristic and rejection sampling. With some developments and optimization techniques, these types of schemes generally show better performance than hash-and-sign schemes in terms of key size, signing time and verification time, for the same security level. In particular, the operating time of Ducas et al. [2013] did not lag behind the operating time of RSA-2048. Therefore, they are considered to be more suitable for practical use.

However, not many of prior SAS schemes focused on exploiting these advantages of the Fiat-Shamir heuristics. Also, despite the popularity of lattice-based cryptography due to its post-quantum security, there is not much work devoted on the construction of lattice-based (sequential) aggregate signature schemes. After the work of El Bansarkhani and Buchmann [2014], Wang and Wu [2019] proposed a practical SAS scheme based on the hardness of lattice-based trapdoor function. Yao et al. [2020] designed a unified framework of identity-based sequential aggregate signatures from 2-level hierarchical identity-based encryption schemes, which can be used to constructed under a lattice hardness assumption. In this study, to the best of our knowledge, we provide the first construction of the Fiat-Shamir lattice-based SAS scheme which can be implemented to our settlement system. Our SAS scheme is demonstrated on the signature scheme of Lyubashevsky [2012], and it can be extended to other Fiat-Shamir signature schemes to achieve better performance.

2.4 Proposed Model

In this section, we propose a blockchain-based securities settlement system for CBDC. We first describe the key characteristics of our model. Then, we explain the settlement process of our model with a specific trading scenario.

2.4.1 Model Description

Our model is based on the atomic cross-chain swaps proposed by Herlihy [2018]. The main difference is that we adopt a new administrator ledger to enhance the auditability of our model, which is essential for CBDC to be implemented in the real-world. Table 2.4 shows how our model is different from other central banks' blockchain-based settlement projects in terms of HTLC usage, trade leader, DLT usage, record-keeper, settlement time, failure-to-deliver, and netting.

Table 2.4: System Comparisons

Features	**Current System**	**Project Stella**	**Project Ubin**	**Project Jasper**	**Ours**
HTLC Usage	Not used	Used	Used	Not used	Used
Trade Leader	None	Designated Buyer or Seller	RMO (Arbitrator)	None	Buyer and Seller
DLT Usage	Not Used	Cross-ledger	Cross-ledger	Single-ledger	Cross-ledger
Record Keeper	Central Bank/CSD	Buyer and Seller	Buyer and Seller	CDS node	Buyer and Seller
Settlement Time	T+1	Real-time	Real-time	T+1	Real-time
Failure-to Deliver	None	Possible	None	None	None
Netting	One-day Netting	Not used	Not used	One-day Netting	Flexible Netting

Our model implements the cross-ledger DvP model as its settlement environment design under the following considerations: securities and payment institutions for securities settlement are separated in most countries and scalability is crucial for various types of asset settlements in the future. We briefly list some of the key characteristics of our model.

DLT Platform Choices Our proposed system was designed to be platform-free. In other words, our protocol does not depend on the type of blockchain used, as long the selected platform can support our proposed signature scheme. Theoretically, different DLT platforms can be used for each ledger. However, the computational complexity of the protocol should be considered when choosing the appropriate platform architecture as some platforms such as Ethereum charge fees for computations.

Settlement Failure and Arbitrator Removal In traditional HTLC settings, if we set the leader of the trade as A and the receiver as B, these two failure scenarios are possible.

1) If B fails to sign the transaction after A has signed, A receives the expected asset or cash without paying for it.

2) If A fails to sign the transaction, then there are no trades.

(Figure 2.2 shows graphical illustration of a successful HTLC and Figure 2.3 shows the first case of settlement failure.)

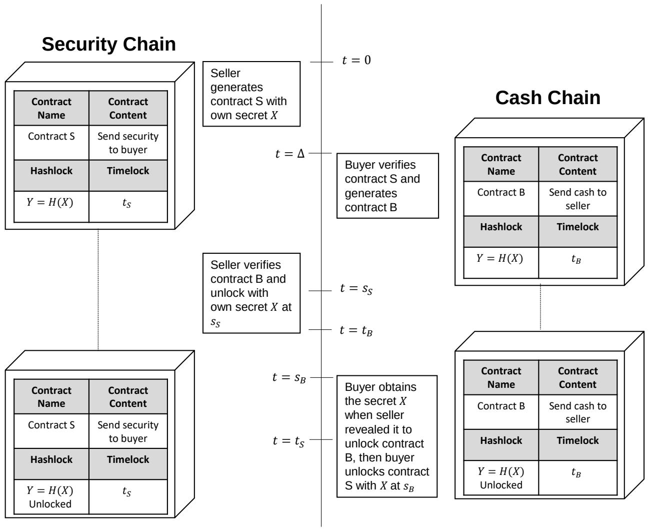


Figure 2.2: Example of HTLC - The buyer and the seller both successfully complete their contracts.

If we assume that the absence of trades does not result in any economic loss for either participant, any settlement failure can only harm the follower (B), making the trade unfair. To address this problem, the proposed model selects both participants as leaders, constructing a more equal and fair settlement system compared to the traditional HTLC.

Additionally, the proposed system differs from other existing protocols in that it

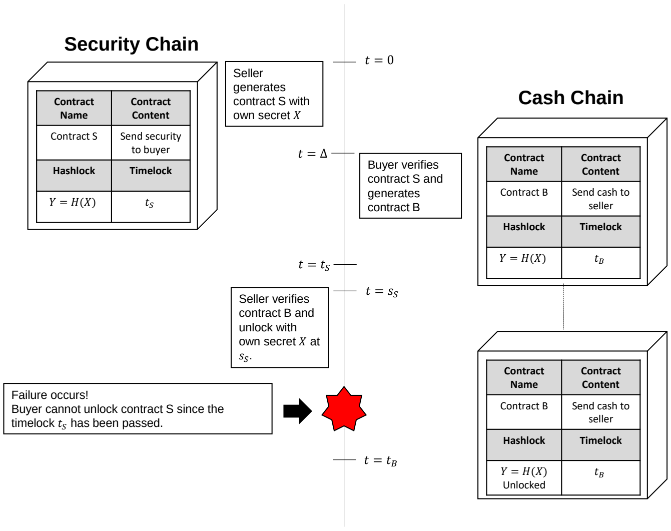


Figure 2.3: Example of HTLC Settlement Failure ($t_B > t_S$) - The buyer fails to receive the securities while the seller succeeds in retrieving the cash.

removes the arbitrators from the system. The system adopts administrators to participate in the trading protocol, but they can be distinguished from past arbitrators because they do not receive or send any real assets. The administrators only provide their signatures in the protocol to ensure safe and fair trading, and the assets are traded only between trading entities.

Netting Choices The proposed model can implement different netting choices via simple smart contract modifications. This can be advantageous compared to the current system, because the settlement can now occur on the day when the trade actually happened.

Automated Administrator Ledger The model introduces an administrative ledger to the system which allows government agencies or market operators to effectively track transactions on various blockchains. The blockchain records all transactions automatically once both asset transfers (such as cash and securities) have been completed, fulfilling the need for a comprehensive and easily accessible record of the transaction history.

Privacy Issues The proposed protocol can be used in private blockchain settings, where only trusted entities can participate in trading. These trusted entities can agree to share their transaction histories with themselves. However, if we extend our discussions to the public blockchains, privacy issues can be a severe problem as all parties might have to share their transaction records with other untrusted parties. To solve such issues, privacy-preserving mechanisms such as multi-party computations, homomorphic encryption, or zero-knowledge proof can be implemented to ensure the privacy of market participants Atapoor et al. [2021], Wang et al. [2021a, 2020], Bai et al. [2020], Pu et al. [2020].

2.4.2 Model Architecture

In this section, we briefly summarize the settlement process proposed by our model. Readers are recommended to read Lee [2020], Lee et al. [2021a] for more details. Imagine a scenario in which Bank S (Seller) and Bank B (Buyer) agree to trade fixed amount of securities with cash. In addition to the seller and the buyer, the administrator A (Admin A) seeks to preserve a record of this transaction on a separate blockchain for the purpose of tracking all completed transactions. The settlement process is depicted in Figure 2.4 and involves three blockchain ledgers: the cash ledger (red), the securities ledger (blue), and the administrator ledger (black).

During the first phase, the buyer and the seller generate and deploy the contracts.

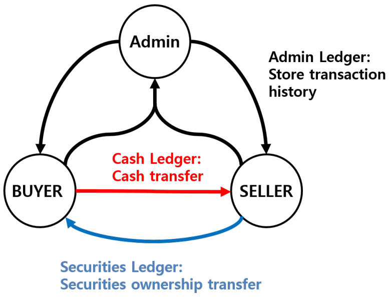

Admin
Admin Ledger: Store transaction history
Cash Ledger: Cash transfer
BUYER
SELLER
Securities Ledger: Securities ownership transfer

Figure 2.4: The Settlement Process

Both buyer and seller act as leaders, and generate secrets S_b and S_s as messages for their new contracts. The buyer establishes a contract for cash transfer on the cash blockchain and the seller establishes a contract for the securities transfer on the securities blockchain. Both then send these contracts to the admin blockchain for verification. Each contract includes transaction details, signature requirements, and a suitable timelock value. The contracts will not activate until all necessary conditions are met, and contracts that haven't been activated are represented by solid lines in Figure 2.5.

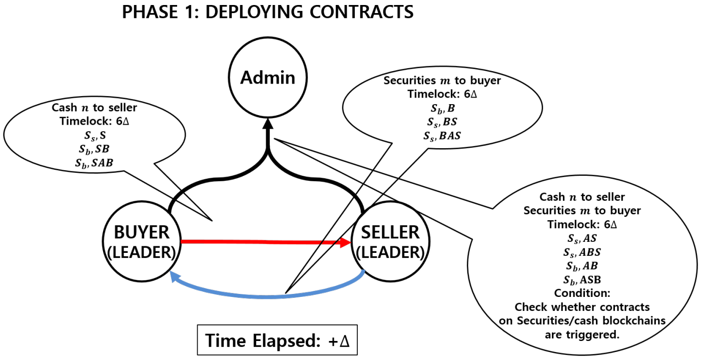

PHASE 1: DEPLOYING CONTRACTS
Admin
Cash n to seller Timelock: 6Δ S_s, S S_b, SB S_b, SAB
Securities m to buyer Timelock: 6Δ S_b, B S_s, BS S_s, BAS
BUYER (LEADER)
SELLER (LEADER)
Cash n to seller Securities m to buyer Timelock: 6Δ S_s, AS S_s, ABS S_b, AB S_b, ASB Condition: Check whether contracts on Securities/cash blockchains are triggered.
Time Elapsed: +Δ

Figure 2.5: Phase 1 - Contract are generated and deployed by buyer and seller

Signatures are generated as sequential path keys using a latticed-based signature scheme proposed in the following section (Algorithms 1 and 2). We denote the output of the proposed signature process as $\mathsf{AggSign}()$. The simplified version of the signing process is presented in Equations 2.2 to 2.4, where s denotes the secret carried by a message and $sk()$ denotes the secret key of each participant.

$$sig(s, A) = \mathsf{AggSign}(sk(A), s(message)) \tag{2.2}$$

$$sig(s, BA) = \mathsf{AggSign}(sk(B), sig(s, A)) \tag{2.3}$$

$$sig(c, CBA) = \mathsf{AggSign}(sk(C), sig(s, BA)) \tag{2.4}$$

During Phase 2 where the contracts are actually triggered, buyers and sellers provide their secrets S_b and S_s to sign the contracts they received. The signing process is progressed as they can sign on a contract by using their secret keys and previously signed signatures. When the signing requirements are completed, assets are traded instantly. The model incentivizes the participants to correctly sign the contracts as their signatures are required to obtain their desired assets. Finally, the administrator on the admin ledger confirms the correct execution of all asset transfers, and records all the transaction details in the admin ledger. Figure 2.6 illustrates the completion of the process, with all contracts having been triggered.

2.4.3 Our signature scheme: AggSign

We propose a lattice-based digital signature scheme that can be implemented to our settlement system for future quantum-resistance. The secret key of each individual is given by a matrix $\mathbf{S} \in \mathbb{Z}_q^{m\times k}$, while the public (verification) key is a pair of matrices $(\mathbf{A}, \mathbf{T} = \mathbf{AS}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^{n\times k}$. For simplicity, the key size parameters n, m, k are assumed to be shared among all users. We require that for any user, her secret key

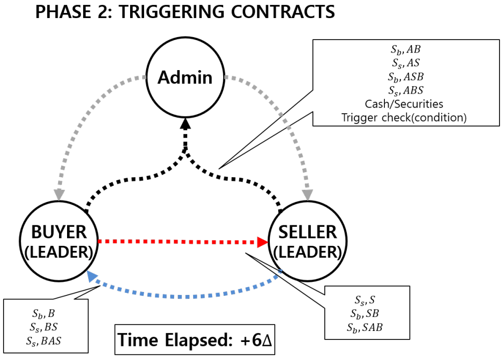


Figure 2.6: Phase 2 - All the assets are transferred and the transaction history is recorded in the admin ledger

satisfies $\|S\|_{\max} \leq d$ (i.e., every entry of the secret key lies between $-d$ and d), and put $R_k := \{v : v \in \{-1, 0, 1\}^k, \|v\|_1 \leq \kappa\}$. Here the bounding constants $d \in \mathbb{N}$ and $\kappa > 0$ are parameters related to the hardness of the problem to which the security of our scheme resorts.

Subsequently, we introduce the hash functions to be used in our scheme: the 'compressing hash' $H : \{0,1\}^* \to \{0,1\}^\ell$ and the 'domain-adjusting hash' $G : \{0,1\}^* \to R_k$. For our construction, the input space for G may be replaced by $\mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^n \times \{0,1\}^\ell$, since the inputs whose G-hash value is required for the signing process are always of the form $(\mathbf{Ay}, \mathbf{c})$ for some $\mathbf{y}$ sampled from D_σ^m and $\mathbf{c} \in \{0,1\}^\ell$.

The sequential aggregate signature scheme is now ready to be presented. Suppose that there are N users, each with secret keys $\mathbf{S}_1, \ldots, \mathbf{S}_N$, public keys $(\mathbf{A}_1, \mathbf{T}_1), \ldots, (\mathbf{A}_N, \mathbf{T}_N)$, and messages $\mu_1, \ldots, \mu_N$ to be signed. The symbol $\overrightarrow{\mathbf{S}}$ would denote the ordered list $(\mathbf{S}_1, \ldots, \mathbf{S}_N)$ of secret keys. For each $1 \leq i \leq N$, $\overrightarrow{\mathbf{S}_i}$ denotes the partial list $(\mathbf{S}_1, \ldots, \mathbf{S}_i)$, and $\overrightarrow{\mathbf{S}_0}$ is the empty list $\varnothing$. The same notational principles apply to $\overrightarrow{\mathbf{A}}$, $\overrightarrow{\mathbf{T}}$ and $\overrightarrow{\boldsymbol{\mu}}$. Note the presence of a constant M, which governs the probability that the scheme successfully outputs a signature. Although the signing algorithm should be run until a signature is successfully returned, under the correct choice of parameters, M is within the range where the applicability scheme is not hindered.

Algorithm 1 AggSign: Sequential Aggregate Signing

```
Input: $\mathbf{\Sigma}_i = (\overrightarrow{\mathbf{A}_i}, \overrightarrow{\mathbf{T}_i}, \overrightarrow{\mathbf{z}_i}, \overrightarrow{\mathbf{g}_i}, \overrightarrow{\boldsymbol{\mu}_i}, \mathbf{c}_i)$, $\mathbf{A}_{i+1}$, $\mathbf{S}_{i+1}$, $\boldsymbol{\mu}_{i+1}$
Output: $\mathbf{\Sigma}_{i+1}$
if $\mathsf{AggVerify}(\mathbf{\Sigma}_i) = \mathsf{False}$ then return $\perp$
end if
$\mathbf{y}_{i+1} \overset{\$}{\leftarrow} D_\sigma^m$
$\mathbf{c}_{i+1} \leftarrow \mathbf{c}_i \oplus H(\overrightarrow{\mathbf{A}}_{i+1}, \overrightarrow{\boldsymbol{\mu}}_{i+1})$
$\mathbf{g}_{i+1} \leftarrow G(\mathbf{A}_{i+1}, \mathbf{A}_{i+1}\mathbf{y}_{i+1}, \mathbf{c}_{i+1})$
$\mathbf{z}_{i+1} \leftarrow \mathbf{S}_{i+1}\mathbf{g}_{i+1} + \mathbf{y}_{i+1}$
$\mathbf{\Sigma}_{i+1} \leftarrow (\overrightarrow{\mathbf{A}}_{i+1}, \overrightarrow{\mathbf{T}}_{i+1}, \overrightarrow{\mathbf{z}}_{i+1}, \overrightarrow{\mathbf{g}}_{i+1}, \overrightarrow{\boldsymbol{\mu}}_{i+1}, \mathbf{c}_{i+1})$ return $\mathbf{\Sigma}_{i+1}$
Success $\leftarrow$ False
With probability $\min\left(\frac{D_\sigma^m(\mathbf{z}_{i+1})}{M D^m_{\mathbf{S}_{i+1}\mathbf{g}_{i+1},\sigma}(\mathbf{z}_{i+1})}, 1\right)$,
Success $\leftarrow$ True
if Success $=$ False then return $\mathbf{\Sigma}_i$
end if
    return $\mathbf{\Sigma}_{i+1}$
```

The symbol $\perp$ in Algorithm 1 (AggSign) indicates the rejection of signing owing to the invalid input aggregate signature $\mathbf{\Sigma}_i$ from the previous step. If AggSign has returned the same object as the input signature, it indicates that the signing was not rejected, but the probabilistic signing algorithm failed to augment a new signature on trial, so AggSign has to be run again on the same input. Finally, we assume that when $i = 0$, the only nontrivial input $\mathbf{c}_0$ should equal a pre-specified initial value *init*.

The corresponding verification process is given as Algorithm 2. It simply checks whether $\mathbf{z}_i$'s are 'small enough', and whether the published values of $\mathbf{z}_i, \mathbf{g}_i$ and $\mathbf{c}_i$

are consistent with the signing procedure, in which

$$\mathbf{A}_i\mathbf{z}_i - \mathbf{T}_i\mathbf{g}_i = \mathbf{A}_i(\mathbf{S}_i\mathbf{g}_i + \mathbf{y}_i) - \mathbf{T}_i\mathbf{g}_i = \mathbf{A}_i\mathbf{y}_i, \tag{2.5}$$

(since $\mathbf{A}_i\mathbf{S}_i = \mathbf{T}_i$), and therefore $G_i(\mathbf{A}_i, \mathbf{A}_i\mathbf{z}_i - \mathbf{T}_i\mathbf{g}_i, \mathbf{c}_i) = \mathbf{g}_i$ must hold true.

Algorithm 2 AggVerify: Verification of SAS

```
Input: $\mathbf{\Sigma}_N = (\overrightarrow{\mathbf{A}_N}, \overrightarrow{\mathbf{T}_N}, \overrightarrow{\mathbf{z}_N}, \overrightarrow{\mathbf{g}_N}, \overrightarrow{\boldsymbol{\mu}_N}, \mathbf{c}_N)$
Output: Boolean value True or False
for $i = N$ to 1 do
    if $\|\mathbf{z}_i\|_1 > \eta\sigma\sqrt{m}$ or $\mathbf{g}_i \neq G(\mathbf{A}_i, \mathbf{A}_i\mathbf{z}_i - \mathbf{T}_i\mathbf{g}_i, \mathbf{c}_i)$ then return False
    end if
    $\mathbf{c}_{i-1} \leftarrow \mathbf{c}_i \oplus H(\overrightarrow{\mathbf{A}}_i, \overrightarrow{\boldsymbol{\mu}}_i)$
end for
if $\mathbf{c}_0 \neq$ $init$ then return False
end ifreturn True
```

2.5 Security Analysis

2.5.1 Security of the Settlement System

In this section, we aim to demonstrate the atomicity of the proposed model using principles of graph theory and game theory. The proof builds upon the idea of atomic cross-chain swaps by Herlihy [2018] and shows how the settlement model ensures atomicity despite not being a strongly connected graph.

Payoff of the Participants Consider a directed graph where market participants are represented as vertices and transactions between them as edges. A transaction from node u to node v signifies an asset transfer from u to v. When all market participants are rational economic agents, they prefer edges directed towards them. This is because these edges represent the assets being transferred to the market participants. Hence, deciding whether to comply with the protocol or not becomes a strategic decision in a game. As illustrated in Figure 2.7, there are five possible outcomes for the players: Discount, Deal, Freeride, Nodeal, and Underwater. These terms were first introduced by Herlihy [2018] and will be explained in detail below.

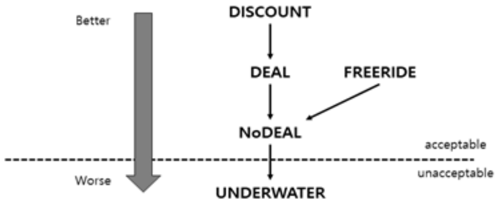


Figure 2.7: Payoff of the participants

1) **Discount**: The participant acquires all the assets while paying less than expected. All the edges entering node v are triggered, but not all the edges leaving node v are triggered.
2) **Deal**: The participant acquires all the assets while paying all as expected. All the edges entering node v are triggered and all the edges leaving node v are triggered.
3) **Freeride**: The participant acquires any of the assets while not paying at all. At least one of the edges entering node v is triggered but all the edges leaving node v are not triggered.
4) **Nodeal**: The participant does not acquire or pay for any asset. All the edges remain untriggered.
5) **Underwater**: The participant does not acquire all of the asset while paying. At least one of the edges entering node v is untriggered and at least one of the edges leaving node v is triggered.

The participants' economic incentives influence their preference for the different outcomes. They prefer Discount over Deal, and Deal over Nodeal. Furthermore, they prefer Freeride over Nodeal and Nodeal over Underwater.

Security of the Model The previously defined payoffs are established by the activation and termination of a node's incoming and outgoing edges.In this model, the administrator node is responsible for maintaining a record of all transactions to enhance social welfare. Deviating from the protocol can result in penalties for the administrator nodes as it reduces social welfare.

Definition 2.8. *The settlement protocol S is **uniform** under these conditions:*

1. *If all participants conform to the protocol, everyone should end with Deal.*
2. *If any participants attempt to deviate from the protocol, no other participants should end with Underwater.*

A uniform protocol is ineffective if rational participants lack incentives to abide by it. The protocol must also be a strong Nash equilibrium, meaning no participant should benefit from deviating from it.

Definition 2.9. *The settlement protocol S is **atomic** if it is uniform and a strong Nash equilibrium.*

Definition 2.9 states that an atomic protocol must ensure that all compliant participants end with Deal or better, while all deviating participants end with Deal or worse. If all participants follow the protocol S, they will all end up with Deal. However, it is necessary to determine what happens if any participant tries to deviate from the protocol. The discussion will be limited to the buyer and seller, as the administrator always adheres to the protocol, as the administrator node is not a real asset trader.

Proposition 2.1. *A conforming participant always do not end up with payoff Underwater.*

Proof. Under the settlement protocol, buyers and sellers have a symmetric graph structure. Therefore without loss of generality, assume that a conforming buyer ended with Underwater. In other words, at least one of the edges entering the buyer from the seller remains untriggered while at least one of the edges leaving the buyer is triggered. Specifically, a contract (Seller,Buyer) should remain untriggered while (Buyer,Seller) gets triggered. (Buyer,Seller) edge consists of three signatures: $(S_s, S), (S_b, SB), (S_b, SAB)$, so all the participants can get access to these signature values if (Buyer,Seller) gets triggered. With known (S_s, S), the admin node can provide signature (S_s, AS) and propagate it to the buyer. Then, the buyer can sign (S_s, BS) and (S_s, BAS) using all the known information, satisfying the triggering condition for (Seller,Buyer) edge. This contradicts the assumption that (Seller,Buyer) remains untriggered. □

Proposition 2.2. *Any deviating participant ends up with payoff Deal or less.*

Proof. Assume that the buyer attempts to deviate from the protocol without loss of generality because the graph is symmetric for both buyer and seller. In order to better off by deviation, the buyer should end up with Discount or Freeride. In other words, (Seller,Buyer) should be triggered while (Buyer,Seller) should remain untriggered. However, by proposition 2.1, no conforming participants should end up Underwater so (Buyer,Seller) should be triggered for the seller. This contradicts the assumption that (Buyer,Seller) edge should remain untriggered. □

The proposed settlement protocol ensures that no compliant participant will end up with Underwater. Deviating participants will only receive Deal or lower, making it uneconomical for them to deviate from the protocol. As a result, all participants will either successfully trade their desired assets (Deal) or have all assets returned to their original owners (No Deal), guaranteeing atomicity with the protocol.

2.5.2 Security of AggSign

In this section, we prove that the proposed signature scheme is strongly existentially unforgeable under chosen-message attack, in the random oracle model. The security is based on the worst-case hardness assumption for the ℓ_2-$\mathrm{SIS}_{q,n,m,\beta}$ problem under appropriate choice of parameters.

Description of Security Model We first give a description of the forger (adversary) $\mathcal{F}$ in the SAS setup.

- $\mathcal{F}$ makes at most q_H, q_G, q_S queries to the H-random oracle, G-random oracle, and the signing oracle, respectively.

- $\mathcal{F}$ is given a target (challenge) public key $(\mathbf{A}, \mathbf{T}) = (\mathbf{A}_j, \mathbf{T}_j)$ of the jth signer, and is not aware of the corresponding secret key. However, $\mathcal{F}$ is allowed to collude with other signers, and is provided with both their public and secret keys.

- $\mathcal{F}$ either forges an SAS $\mathbf{\Sigma} = (\overrightarrow{\mathbf{A}}_i, \overrightarrow{\mathbf{T}}_i, \overrightarrow{\mathbf{z}}_i, \overrightarrow{\mathbf{g}}_i, \overrightarrow{\boldsymbol{\mu}}_i, \mathbf{c}_i)$, $j \leq i$, without making a signing query on messages $\overrightarrow{\boldsymbol{\mu}}_j$ and $(\overrightarrow{\mathbf{A}}_j, \overrightarrow{\mathbf{T}}_j)$. Or, it makes an SAS query on the the same ordered list of messages and outputs an SAS different from the oracle output.

The security proof is done by constructing an algorithm $\mathcal{A}$ which operates interactively with $\mathcal{F}$ to find a short integer solution to $\mathbf{A}_* \mathbf{v} = \mathbf{0}$ by assigning $\mathcal{F}$ with the challenge public key $\mathbf{A}_*$.

Theorem 2.3. *Let $q, n, m, k, d, \kappa, \sigma, \eta$ be parameters of the proposed signature scheme, with $\sigma \geq \alpha d \kappa \sqrt{m}$ for some $\alpha > 0$, and $m > 64 + \frac{n \log q}{\log(2d+1)}$. Let $\beta = (2\eta\sigma + 2dk)\sqrt{m}$. Suppose that there exists a polynomial-time forger $\mathcal{F}$ which forges a valid SAS with probability $\delta > 0$, after at most q_S queries to Aggsign and q_G, q_H queries to G, H random oracles, respectively. Then there exists a polynomial-time algorithm $\mathcal{S}$ for solving the $\ell_2 - SIS_{q,n,m,\beta}$ problem with probability at least*

$$\left(\frac{1}{2} - \frac{1}{2^{100}}\right) \delta' \left(\frac{\delta'}{q_G + q_S} - \frac{1}{|R_k|}\right)$$

where $\delta' = \delta - \frac{q_S \cdot 2^{-99}}{M} - \frac{q_S(q_G+q_S)}{2^{n-1}} - \frac{1}{|R_k|}$ and $M = \exp\left(\frac{12}{\alpha} + \frac{1}{2\alpha^2}\right)$.

Theorem 2.3 states that if it is hard to solve the $\ell_2 - SIS_{q,n,m,\beta}$ problem with non-negligible probability, then it is also hard to forge an SAS within our scheme with non-negligible probability in polynomial time.

Proof of the Theorem We start by constructing an algorithm $\mathcal{A}$ which attains a forged SAS from $\mathcal{F}$ using an imitating signing oracle $\mathsf{OAggSign}$.

$\mathsf{OAggSign}(\mathbf{S}_*, \mathbf{A}_*, \boldsymbol{\mu}_i, \boldsymbol{\Sigma}_{i-1})$: $\mathcal{A}$ parses $\boldsymbol{\Sigma}_{i-1}$ as

$$\boldsymbol{\Sigma}_{i-1} = (\overrightarrow{\mathbf{A}}_{i-1}, \overrightarrow{\mathbf{T}}_{i-1}, \overrightarrow{\mathbf{z}}_{i-1}, \overrightarrow{\mathbf{g}}_{i-1}, \overrightarrow{\boldsymbol{\mu}}_{i-1}, \mathbf{c}_{i-1}).$$

If $H(\mathbf{A}_*, \boldsymbol{\mu}_i)$ was queried before, then set $\mathbf{h}_i \leftarrow H(\mathbf{A}_*, \boldsymbol{\mu}_i)$, i.e., with the previously answered value. Otherwise, take $\mathbf{h}_i \overset{\$}{\leftarrow} \{0,1\}^l$ and program the hash as $H(\mathbf{A}_*, \boldsymbol{\mu}_i) \leftarrow \mathbf{h}_i$. Set $\mathbf{c}_i \leftarrow \mathbf{c}_{i-1} \oplus \mathbf{h}_i$, and take $\mathbf{z}_i \overset{\$}{\leftarrow} D_\sigma^{m_i}$ and $\mathbf{g}_i \overset{\$}{\leftarrow} R_{k_i}$.

If $G(\mathbf{A}_*, \mathbf{A}_*\mathbf{z}_i - \mathbf{T}_*\mathbf{g}_i, \mathbf{c}_i)$ has already been defined before (as a response to previous signing or hash query), $\mathcal{A}$ aborts and say BAD_0 occurred. Otherwise, with probability $1/M$, set $G(\mathbf{A}_*, \mathbf{A}_*\mathbf{z}_i - \mathbf{T}_*\mathbf{g}_i, \mathbf{c}_i) \leftarrow \mathbf{g}_i$ and return

$$\boldsymbol{\Sigma}_i \leftarrow (\overrightarrow{\mathbf{A}}_i, \overrightarrow{\mathbf{T}}_i, \overrightarrow{\mathbf{z}}_i, \overrightarrow{\mathbf{g}}_i, \overrightarrow{\boldsymbol{\mu}}_i, \mathbf{c}_i).$$

The signing procedure $\mathsf{OAggSign}$ differs from that of the authentic SAS ($\mathsf{AggSign}$) in that $\mathsf{i})$ $\mathsf{OAggSign}$ does not explicitly sample $\mathbf{y}_i$ and then compute $\mathbf{z}_i = \mathbf{S}_i\mathbf{g}_i + \mathbf{y}_i$, but instead samples $\mathbf{z}_i$ directly from the discrete Gaussian and programs the hash accordingly, and $\mathsf{ii})$ $\mathsf{OAggSign}$ outputs $(\mathbf{z}, \mathbf{g})$ with constant probability $1/M$ unlike the real signature scheme. The next lemma, which summarizes the related arguments from Lyubashevsky [2012], shows that despite such differences, there is only a negligible statistical discrepancy between their results.

Lemma 2.4. *Suppose $\sigma \geq \alpha d\kappa\sqrt{m}$. Then, unless BAD_0 occurs during the runtime of $\mathcal{A}$, the advantage of any distinguisher $\mathcal{D}$ of distinguishing between the output of*

Algorithm 1 and the oracle answer to the signing query to $\mathcal{A}$ is at most $\frac{2^{-100}}{M}$.

Proof. Let $\mathbf{S}_i$ denote the secret key of the ith user; the one whose signature is queried.
For $\mathbf{v} \in \mathbb{Z}^m$, define

$$E_{\mathbf{v}} = \{\mathbf{z} \in \mathbb{Z}^m : D_\sigma^m(\mathbf{z}) < M \cdot D_{\mathbf{v},\sigma}^m(\mathbf{z})\},$$

and define

$$V = \{\mathbf{v} \in \mathbb{Z}^m : \mathbf{v} = \mathbf{S}_i\mathbf{g}, \mathbf{g} \in R_k\}.$$

Note that because $\|\mathbf{S}_i\|_{\max} \leq d$ and $\|\mathbf{g}\|_1 \leq \kappa$, so $\|\mathbf{S}_i\mathbf{g}\| \leq d\kappa\sqrt{m}$ and thus $\sigma \geq \alpha\|\mathbf{v}\|$ holds for any $\mathbf{v} \in V$. Then, by the following lemma, a sample from D_σ^m belongs to $E_{\mathbf{v}}$ with high probability.

Lemma 2.5 (Theorem 3.4, Lyubashevsky [2012])**.** *Let $\mathbf{v} \in \mathbb{Z}^m$ and $\sigma \geq \alpha\|\mathbf{v}\|$. Then $\Pr[D_\sigma^m(\mathbf{z})/D_{\mathbf{v},\sigma}^m(\mathbf{z}) < M : \mathbf{z} \overset{\$}{\leftarrow} D_\sigma^m] > 1 - \epsilon$, where $\epsilon = 2^{-100}$.*

Let $v : V \to \mathbb{R}$ denote the probability mass function for the distribution of $\mathbf{v} \in V$, where $\mathbf{v} = \mathbf{S}_i\mathbf{g}$ and $\mathbf{g} \overset{\$}{\leftarrow} R_k$. For a fixed $\mathbf{v}$, denote by $h_{\mathbf{v}} : R_k \to \mathbb{R}$ the conditional probability mass function

$$h_{\mathbf{v}}(\mathbf{g}) = \Pr[\mathbf{g} \overset{\$}{\leftarrow} R_k; \mathbf{S}_i\mathbf{g} = \mathbf{v}].$$

Now, $\mathcal{F}$ denotes the output distribution of Algorithm 1 and $\mathcal{F}_{\mathcal{A}}$ denotes that of $\mathcal{A}$. Because the advantage of distinguishing outputs of two procedures is bounded above by the total variation (TV) distance between the distributions of their outputs, it suffices to show that $d_{TV}(\mathcal{F}, \mathcal{F}_{\mathcal{A}})$ does not exceed $\frac{\epsilon}{M}$. The candidate output $(\mathbf{z}_i, \mathbf{g}_i)$ of $\mathcal{F}$ is, in distribution, the same as a random draw $\mathbf{g}_i \overset{\$}{\leftarrow} R_k$, followed by $\mathbf{z}_i \overset{\$}{\leftarrow} D_{\mathbf{v},\sigma}^m$ under the random oracle model (here $\mathbf{v} = \mathbf{S}_i\mathbf{g}_i$). Then, $(\mathbf{z}_i, \mathbf{g}_i)$ is outputted with probability $\frac{D_\sigma^m(\mathbf{z})}{M \cdot D_{\mathbf{v},\sigma}^m}$ if $\mathbf{z}_i \in E_{\mathbf{v}}$ and 1 if $\mathbf{z}_i \notin E_{\mathbf{v}}$. Therefore, the probability $p_{\mathcal{F}}$ of $\mathcal{F}$

succeeding (i.e. outputting a signature) satisfies

$$\begin{aligned}
&\Pr[\mathcal{F} \text{ succeeds}] \\
&= \sum_{\mathbf{v} \in V} v(\mathbf{v}) \left[\sum_{\mathbf{z} \in E_{\mathbf{v}}} D^m_{\mathbf{v},\sigma} \cdot \frac{D^m_\sigma(\mathbf{z})}{M \cdot D^m_{\mathbf{v},\sigma}} + \sum_{\mathbf{z} \notin E_{\mathbf{v}}} D^m_{\mathbf{v},\sigma}(\mathbf{z}) \right] \\
&\geq \frac{1}{M} \sum_{\mathbf{v} \in V} \sum_{\mathbf{z} \in E_{\mathbf{v}}} D^m_\sigma(\mathbf{z}) \\
&= \frac{1}{M} \sum_{\mathbf{v} \in V} \Pr[\mathbf{z} \notin E_{\mathbf{v}} : \mathbf{z} \xleftarrow{\$} D^m_\sigma] \geq \frac{1-\epsilon}{M}.
\end{aligned}$$

Moreover,

$$\begin{aligned}
&\Pr[\mathcal{F} \text{ succeeds}] \\
&= \sum_{\mathbf{v} \in V} v(\mathbf{v}) \left[\sum_{\mathbf{z} \in E_{\mathbf{v}}} \frac{D^m_\sigma(\mathbf{z})}{M} + \sum_{\mathbf{z} \notin E_{\mathbf{v}}} D^m_{\mathbf{v},\sigma}(\mathbf{z}) \right] \\
&\leq \sum_{\mathbf{v} \in V} v(\mathbf{v}) \left[\sum_{\mathbf{z} \in E_{\mathbf{v}}} \frac{D^m_\sigma(\mathbf{z})}{M} + \sum_{\mathbf{z} \notin E_{\mathbf{v}}} \frac{D^m_\sigma(\mathbf{z})}{M} \right] \\
&= \frac{1}{M} \sum_{\mathbf{v} \in V} v(\mathbf{v}) = \frac{1}{M}.
\end{aligned}$$

For each $(\mathbf{z}, \mathbf{g}) \in \mathbb{Z}^m \times R_k$, the probability that $\mathcal{F}$ and $\mathcal{F}_\mathcal{A}$ outputs $(\mathbf{z}, \mathbf{g})$ are each given by

$$\mathcal{F}(\mathbf{z}, \mathbf{g}) = \sum_{\mathbf{v} \in V} v(\mathbf{v}) h_{\mathbf{v}}(\mathbf{g}) D^m_{\mathbf{v},\sigma}(\mathbf{z}) \cdot \min \left(\frac{D^m_\sigma(\mathbf{z})}{M \cdot D^m_{\mathbf{v},\sigma}(\mathbf{z})}, 1 \right)$$

and

$$\mathcal{F}_\mathcal{A}(\mathbf{z}, \mathbf{g}) = \sum_{\mathbf{v} \in V} v(\mathbf{v}) h_{\mathbf{v}}(\mathbf{g}) \cdot \frac{D^m_\sigma(\mathbf{z})}{M}.$$

Therefore, we have

$$\begin{aligned}
&d_{TV}(\mathcal{F}, \mathcal{F}_{\mathcal{A}}) \\
&= \frac{1}{2}\Bigg[\sum_{\mathbf{g}\in R_k}\sum_{\mathbf{z}\in\mathbb{Z}^m}\big|\mathcal{F}(\mathbf{z},\mathbf{g}) - \mathcal{F}_{\mathcal{A}}(\mathbf{z},\mathbf{g})\big| \\
&\qquad\qquad + \big|(1-p_{\mathcal{F}}) - (1-p_{\mathcal{F}_{\mathcal{A}}})\big|\Bigg] \\
&\leq \frac{1}{2}\Bigg[\sum_{\mathbf{v}\in V}\sum_{\mathbf{z}\in\mathbb{Z}^m}\big|\mathcal{F}(\mathbf{z},\mathbf{v}) - \mathcal{F}_{\mathcal{A}}(\mathbf{z},\mathbf{v})\big| \cdot \sum_{\mathbf{g}\in R_k} h_{\mathbf{v}}(\mathbf{g})\Bigg] \\
&\qquad\qquad + \frac{1}{2}\left|\frac{1}{M} - p_{\mathcal{F}}\right| \\
&\leq \frac{1}{2}\Bigg[\sum_{\mathbf{v}\in V}\sum_{\mathbf{z}\in\mathbb{Z}^m}\big|\mathcal{F}(\mathbf{z},\mathbf{v}) - \mathcal{F}_{\mathcal{A}}(\mathbf{z},\mathbf{v})\big|\Bigg] + \frac{\epsilon}{2M},
\end{aligned}$$

where we have used the expressions

$$\mathcal{F}(\mathbf{z},\mathbf{v}) = v(\mathbf{v})D^m_{\mathbf{v},\sigma}(\mathbf{z}) \cdot \min\left(\frac{D^m_{\sigma}(\mathbf{z})}{M \cdot D^m_{\mathbf{v},\sigma}(\mathbf{z})}, 1\right)$$

and $\mathcal{F}_{\mathcal{A}}(\mathbf{z},\mathbf{v}) = v(\mathbf{v}) \cdot \frac{D^m_{\sigma}(\mathbf{z})}{M}$. Because we have $\mathcal{F}(\mathbf{z},\mathbf{v}) = \mathcal{F}_{\mathcal{A}}(\mathbf{z},\mathbf{v})$ for $\mathbf{z} \in E_{\mathbf{v}}$, we obtain

$$\begin{aligned}
&\sum_{\mathbf{v}\in V}\sum_{\mathbf{z}\in\mathbb{Z}^m}\big|\mathcal{F}(\mathbf{z},\mathbf{v}) - \mathcal{F}_{\mathcal{A}}(\mathbf{z},\mathbf{v})\big| \\
&= \sum_{\mathbf{v}\in V} v(\mathbf{v}) \cdot \left(\sum_{\mathbf{z}\notin E_{\mathbf{v}}}\left|D^m_{\mathbf{v},\sigma}(\mathbf{z}) - \frac{D^m_{\sigma}(\mathbf{z})}{M}\right|\right) \\
&\leq \sum_{\mathbf{v}\in V} v(\mathbf{v}) \cdot \sum_{\mathbf{z}\notin E_{\mathbf{v}}} \frac{D^m_{\sigma}(\mathbf{z})}{M} \\
&= \frac{1}{M}\sum_{\mathbf{v}\in V} v(\mathbf{v}) \cdot \Pr[\mathbf{z} \notin E_{\mathbf{v}} : \mathbf{z} \xleftarrow{\$} D^m_{\sigma}] \\
&\leq \frac{1}{M}\sum_{\mathbf{v}\in V} \epsilon \cdot v(\mathbf{v}) = \frac{\epsilon}{M},
\end{aligned}$$

which concludes the proof. □

The following lemma combines Lemma 2.4 together with probabilistic arguments bounding the probability of occurrence of BAD_0.

Lemma 2.6 (Lemma 4.3, Lyubashevsky [2012]). *By running upon $\mathcal{F}$ using the signing oracle* $\mathsf{OAggSign}$*, the algorithm $\mathcal{A}$ produces a valid forgery with probability at least*

$$\delta - q_S \cdot \frac{2^{-99}}{M} - q_S(q_G + q_S) \cdot 2^{-n+1}.$$

The SIS-solving algorithm We now explain the construction of the algorithm $\mathcal{S}$ which efficiently finds a short solution to $\mathbf{A}\mathbf{v} = \mathbf{0}$. The algorithm $\mathcal{S}$ first runs $\mathcal{A}$ against $\mathcal{F}$. Suppose that $\mathcal{F}$ has outputted a forged SAS $\boldsymbol{\Sigma} = (\overrightarrow{\mathbf{A}}, \overrightarrow{\mathbf{T}}, \overrightarrow{\mathbf{z}}, \overrightarrow{\mathbf{g}}, \overrightarrow{\boldsymbol{\mu}}, \mathbf{c}_N)$, where $N \leq N_{\max}$ and $\mathbf{A}_j = \mathbf{A}_*$ for some $1 \leq j \leq N$. Now, if the hash value $G(\mathbf{A}_j, \mathbf{A}_j\mathbf{z}_j - \mathbf{T}_j\mathbf{g}_j, \mathbf{c}_j)$ was not programmed during the run-time of $\mathcal{A}$, then its value would be given at random during the verification process, and the probability that the signature gets confirmed as valid is only $1/|R_k|$. Therefore, we consider only the case when $G(\mathbf{A}_j, \mathbf{A}_j\mathbf{z}_j - \mathbf{T}_j\mathbf{g}_j, \mathbf{c}_j)$ corresponding to the index j of the target signer has been programmed by $\mathcal{A}$. Note that by Lemma 2.6, the probability of such occurrence is at least

$$\delta' := \delta - q_S \cdot \frac{2^{-99}}{M} - q_S(q_G + q_S) \cdot 2^{-n+1} - 1/|R_k|.$$

If, either $\mathcal{F}$ fails to output a signature or the G query required for the verification of (forged) target signature has not been made before, we assume that BAD_1 occurred and $\mathcal{S}$ aborts.

We may assume that, without loss of generality, $\mathcal{A}$ chooses its random oracle answers $\mathbf{r}_1, \cdots, \mathbf{r}_{q_H+q_S}$ for H queries and $\mathbf{t}_1, \ldots, \mathbf{t}_{q_G+q_S}$ for G queries at random, prior to the interaction with $\mathcal{F}$, and then $\mathcal{A}$ answers each query from $\mathcal{F}$ with those values, in order. In addition, we predetermine the random coin draws $\phi_{\mathcal{A}}$ from $\mathcal{A}$ and $\phi_{\mathcal{F}}$ from $\mathcal{F}$, that is, all possible randomness involved in the execution of the algorithm, except for the hash query values.

Unless BAD_1 occurs, we have $G(\mathbf{A}_j, \mathbf{A}_j\mathbf{z}_j - \mathbf{T}_j\mathbf{g}_j, \mathbf{c}_j) = \mathbf{g}_j = \mathbf{t}_i$ for some $1 \leq i \leq q_G + q_S$. Now, draw new random elements $\tilde{\mathbf{t}}_i, \ldots, \tilde{\mathbf{t}}_{q_G+q_S} \overset{\$}{\leftarrow} R_k$, and run $\mathcal{A}$ and $\mathcal{F}$ with randomness

$$(\phi_{\mathcal{A}}, \phi_{\mathcal{F}}, \mathbf{r}_1, \ldots, \mathbf{r}_{q_H+q_S}, \mathbf{t}_1, \ldots, \mathbf{t}_{i-1}, \tilde{\mathbf{t}}_i, \ldots, \tilde{\mathbf{t}}_{q_G+q_S}).$$

If $\mathcal{F}$ fails to forge a new SAS $\tilde{\mathbf{\Sigma}}$, $G(\mathbf{A}_j, \mathbf{A}_j\tilde{\mathbf{z}}_j - \mathbf{T}_j\tilde{\mathbf{g}}_j, \tilde{\mathbf{c}}_j) = \tilde{\mathbf{g}}_j = \tilde{\mathbf{t}}_{i'}$ but $i' \neq i$, or if $\mathbf{t}_i = \tilde{\mathbf{t}}_i$, then $\mathcal{S}$ aborts, saying BAD_2 has occurred. Otherwise, since $\mathcal{F}$ would have operated in the same way as it did with the initial list of randomness up to this point, we see that $\mathbf{A}_j\mathbf{z}_j - \mathbf{T}_j\mathbf{g}_j = \mathbf{A}_j\tilde{\mathbf{z}}_j - \mathbf{T}_j\tilde{\mathbf{g}}_j$. Therefore,

$$\mathbf{A}_j(\mathbf{z}_j - \tilde{\mathbf{z}}_j + \mathbf{S}_j\tilde{\mathbf{g}}_j - \mathbf{S}_j\mathbf{g}_j) = 0.$$

We say that BAD_3 has occurred if $\mathbf{v} := \mathbf{z}_j - \tilde{\mathbf{z}}_j + \mathbf{S}_j\tilde{\mathbf{g}}_j - \mathbf{S}_j\mathbf{g}_j = 0$. Otherwise, $\mathcal{S}$ has found a nonzero solution $\mathbf{v}$ satisfying

$$\begin{aligned} \|\mathbf{v}\| &\leq \|\mathbf{z}_j\| + \|\tilde{\mathbf{z}}_j\| + \|\mathbf{S}_j\tilde{\mathbf{g}}_j\| + \|\mathbf{S}_j\mathbf{g}_j\| \\ &\leq (2\eta\sigma + 2d\kappa)\sqrt{m}, \end{aligned}$$

which is a solution to the $\ell_2 - SIS_{q,n,m,\beta}$ problem with $\beta = (2\eta\sigma + 2d\kappa)\sqrt{m}$.

The probability that $\mathcal{S}$ finds a solution is given by

$$\begin{aligned} &\Pr[\sim \mathrm{BAD}_1 \wedge \sim \mathrm{BAD}_2 \wedge \sim \mathrm{BAD}_3] \\ =&\Pr[\sim \mathrm{BAD}_1 \wedge \sim \mathrm{BAD}_2] \cdot \Pr[\sim \mathrm{BAD}_3 \mid \sim \mathrm{BAD}_1 \wedge \sim \mathrm{BAD}_2] \end{aligned}$$

Applying the general forking lemma Bellare and Neven [2006], we see that

$$\Pr[\sim \mathrm{BAD}_1 \wedge \sim \mathrm{BAD}_2] \geq \delta' \cdot \left(\frac{\delta'}{q_G + q_S} - \frac{1}{|R_k|}\right).$$

Given that neither BAD_1 or BAD_2 occurred, we analyze the conditional probability that BAD_3 happens, i.e., $\mathbf{v} = 0$. Since $\mathcal{S}$ chooses $\mathbf{S}_j$ at random and only $(\mathbf{A}_j, \mathbf{T}_j)$ (but not $(\mathbf{A}_j, \mathbf{S}_j)$) is provided as input in the game between $\mathcal{A}$ and $\mathcal{F}$, the (conditional) probability of BAD_3 is taken over the randomness of $\mathbf{S}_j$. If $\mathbf{v} = 0$ holds, then one has $\mathbf{g}_j = \mathbf{t}_i \neq \tilde{\mathbf{t}}_i = \tilde{\mathbf{g}}_j$ and thus there exists a component index $1 \leq a \leq k$ such that $(\mathbf{g}_j)_a$ and $(\tilde{\mathbf{g}}_j)_a$ differ. Now note that the number of $\mathbf{s} \in \{-d, \ldots, 0, \ldots, d\}^m$ without collision (i.e. another $\mathbf{s}'$ with $\mathbf{A}\mathbf{s} = \mathbf{A}\mathbf{s}'$) is at most $|\mathrm{Range}(\mathbf{A})| = q^n$ (because $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$). Therefore, a uniform random $\mathbf{s} \overset{\$}{\leftarrow} \{-d, \ldots, 0, \ldots, d\}^m$ has a collision $\mathbf{s} \neq \mathbf{s}' \in \{-d, \ldots, 0, \ldots, d\}^m$ with probability at least $1 - \frac{q^n}{(2d+1)^m} \geq 1 - \frac{1}{(2d+1)^{64}} > 1 - 2^{-100}$. Thus, with this probability, one may modify the ath column $(\mathbf{S}_j)^{(a)}$ of $\mathbf{S}_j$ to obtain a new matrix $\mathbf{S}'_j$ with $\mathbf{A}_j \mathbf{S}'_j = \mathbf{A}_j \mathbf{S}_j = \mathbf{T}_j$. Clearly,

$$\begin{aligned}\mathbf{v}' &= \mathbf{z}_j - \tilde{\mathbf{z}}_j + \mathbf{S}'_j \tilde{\mathbf{g}}_j - \mathbf{S}'_j \mathbf{g}_j \\ &= \mathbf{v} + [(\mathbf{g}_j)_a - (\tilde{\mathbf{g}}_j) a] \cdot (\mathbf{S}_j)^{(a)} \\ &= [(\mathbf{g}_j)_a - (\tilde{\mathbf{g}}_j)_a] \cdot (\mathbf{S}_j)^{(a)} \neq 0.\end{aligned}$$

This shows that a pair $(\mathbf{S}_j, \mathbf{v})$ for which BAD_3 occurs (given that $\sim\mathrm{BAD}_1$ and $\sim\mathrm{BAD}_2$) has at least one "conjugate" pair $(\mathbf{S}'_j, \mathbf{v}')$ for which BAD_3 does not occur, with probability $1 - 2^{-100}$. Note that the two instances have the same probability mass, since the probability that either $\mathbf{S}_j$ or $\mathbf{S}'_j$ is chosen as the secret key are the same. Therefore, we have

$$\Pr[\sim \mathrm{BAD}_3 \mid \sim \mathrm{BAD}_1 \wedge \sim \mathrm{BAD}_2] \geq \frac{1}{2} - \frac{1}{2^{100}}.$$

This concludes the proof of Theorem 2.3.

2.6 Proof-of-Concept Experiments and Analysis

This section shows the experimental results of the proposed settlement system to prove its feasibility. The simulation was created in Python using the SimPy library for discrete-event simulations. For simplicity, the proposed signature scheme was not included in the simulation. The aim of the experiment is to examine how the system behaves as its parameters change, rather than comparing it to other systems. Further comparison with benchmark systems is left as future work.

2.6.1 Simulation Setting

Trading Environment For the purpose of the experiment, we created random transaction data based on simulation data provided by the Bank of Korea. We built three blockchains (Cash, Securities, and Admin) and assumed that there was only one mining node that also acted as the admin node, as previously discussed. Ten nodes participated in the settlement as buyers and sellers, generating an average of 1200 daily transactions. The transaction amount was expressed in units of cash, with an average transaction size of 5500 units. It is important to note that the simulation runtime is not equivalent to real time and that the time is measured in predefined units within the simulation.

Simulation Variables The variables used in the simulation model are as follows.

- *Average transaction amount*: The transaction amount for each transaction is determined using the average amount and a pre-defined random distribution. We used a random Gaussian distribution for the simulations.

- *Block size*: The block size determines the total storage capacity of a block. The possible number of contracts that can be stored in a block is calculated by dividing the block size by the contract size.

- *Contract size*: The contract size determines the size of each contract.

- *Block time*: The block time determines the time interval between block generation.

- *Contract time*: Contract time determines the time interval between contract generation.

- *Start balance*: The start balance sets the nodes' starting balances before the trades begin.

- *Sign time*: The sign time determines the average time taken by the nodes to sign the contracts.

- *Node latency*: The node latency is given in the form of a matrix. Each element L_{ij} of the matrix is the time required for node i to send a contract to node j.

-*Num. nodes lag*: Num. nodes lag determines the number of nodes with slower latency.

-*Num. of attacking nodes*: Num. of attacking nodes provides a number of adversarial nodes, that intentionally sign the received contracts slowly. The sign time for these nodes was set to 10 * *Sign Time.*

-*Balance cut*: The balance cut is the lower bound for each node's balance. If one's balance reaches the balance cut, then all the transactions for this node as a buyer are suspended until the balance is replenished.

2.6.2 Experimental Results

In the experiment, we introduce three new metrics to evaluate the performance of blockchain systems with varying configurations. The Completed Contract Ratio (CCR) is the proportion of successfully completed contracts compared to the total number of contracts generated. The Liquidity Deficiency Ratio (LDR) calculates the ratio of contracts in which nodes have a negative balance to the total number of generated contracts. Lastly, the Liquidity Failure Ratio (LFR) measures the proportion of contracts that were cancelled due to insufficient funds compared to the total number of contracts generated. We presume that in cases where a participant's balance falls below zero, additional liquidity is supplied by a central entity like a central bank, allowing the participants to continue trading despite having negative balances.

To begin, we analyze the impact of varying the block time on the performance of the proposed system by looking at changes in the CCR and average settlement time. Figure 2.8 displays the change in CCR as the block time increases. The graph indicates that there exists a certain threshold for block time that results in a significant decrease in CCR. As predicted, if the block size increases, the blockchain system can maintain a longer block time with a certain level of CCR. Figure 2.9 shows that the average settlement time has a direct positive relationship with the block time.

We conducted experiments with varying latency among market participants. Figure 2.10(a), 2.10(b), and 2.10(c) demonstrate the effect of increasing the number of nodes with longer latency and the increase of each latency on the CCR. The results

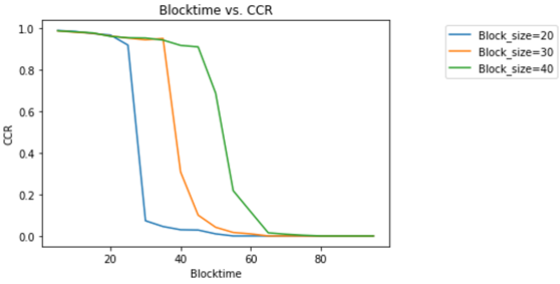


Figure 2.8: Variation of CCR with increasing block time. This figure shows that there is a certain block time for each block size that leads to significant drop in CCR.

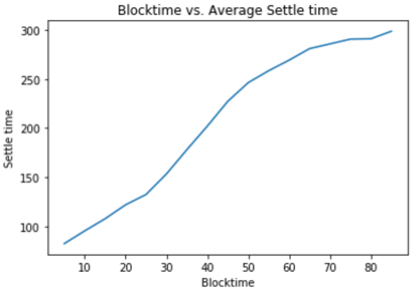
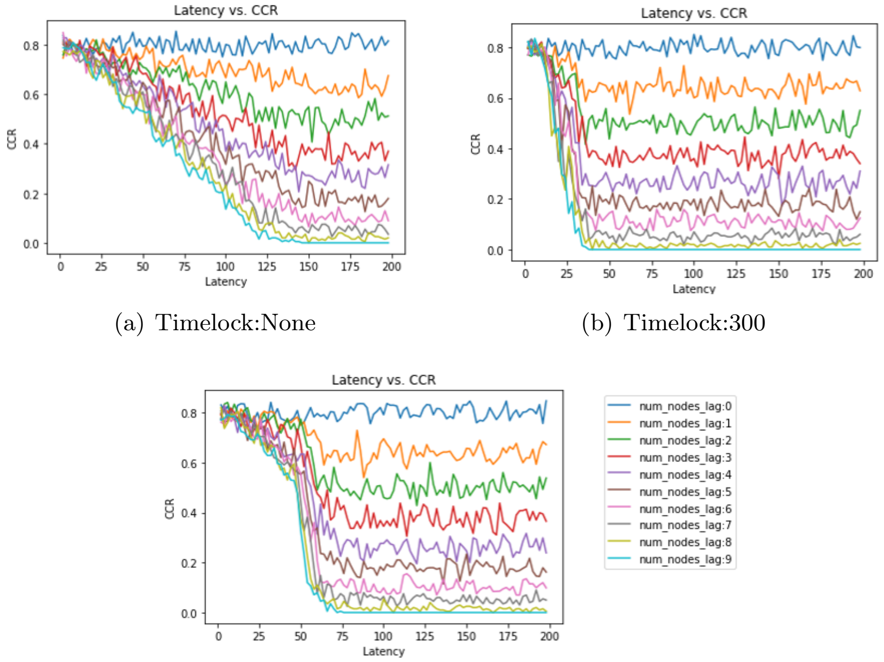


Figure 2.9: Variation of estimated average settlement time with increasing block time. The figure implies that, as expected, the average settlement time increases as the block time increases.

suggest that the number of nodes with slow latency has a greater impact on CCR than the difference in latency as longer latency does not significantly harm CCR, while a larger number of lagged nodes does. An important finding was that the timelock values of transactions play a crucial role in the system. As the timelock value decreases, CCR experiences a significant drop at much smaller latency levels.

In our attack scenario, we assume that adversarial nodes attempt to harm the system or market participants by not signing contracts regularly. We give these adversarial nodes a 10 * *sign time*. Figure 2.11 indicates that if the time taken to sign the contract is much shorter than the transaction's timelock value, the CCR



(a) Timelock:None

(b) Timelock:300

(c) Timelock:500

Figure 2.10: CCR results for different latency and lagged number of nodes settings

remains normal. However, as the sign time increases, the system is unable to settle the majority of contracts.

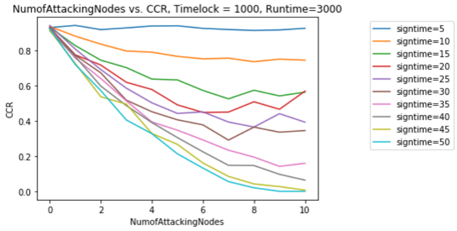
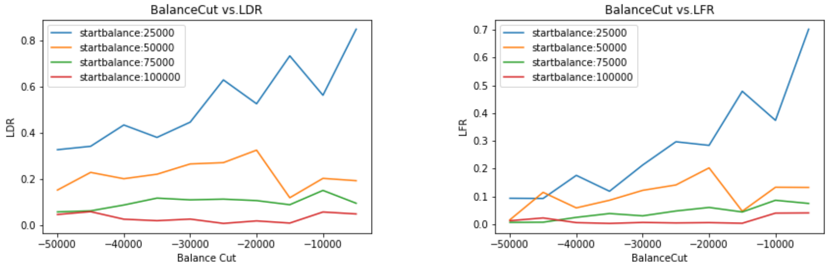


Figure 2.11: Variation in CCR as the number of attacking nodes increases. The system holds its CCR when the sign time is low (=5), but contract failures increase as the sign time increases.

Furthermore, we conducted experiments to assess the impact of each node's balance on the system. Node balances are significant in the system due to the predefined *balance cut*. Figure 2.12(a) and 2.12(b) depict the LDR and LFR of the system with varying balance cuts. As predicted, LDR and LFR rise as the starting balances decrease and balance cut of nodes increase.



(a) Liquidity deficiency ratios

(b) Liqudity failure ratios

Figure 2.12: LDR and LFR for different starting balances. The results show that the participating nodes with larger balances tend to succeed in more contracts.

2.7 Chapter Summary

With the growing need for quick settlement systems in today's fast-paced markets, many experts recognize the potential of blockchain technology to create new decentralized settlement systems. Blockchain provides the added benefits of flexibility and automation in the settlement process without relying on intermediaries such as CSDs or central banks. In this chapter, we present a blockchain settlement protocol that leverages cross-chain atomic swaps to maximize these benefits.

Our proposed protocol incorporates three blockchains: cash, securities, and admin. Unlike previous studies, our model includes an admin ledger to improve the fairness and efficiency of the settlement system. First, by utilizing the admin ledger, the original HTLC protocol becomes more equitable, allowing for fair asset trading without principal risk by selecting both participants as leaders. Additionally, the admin ledger provides a more streamlined experience for market operators and government institutions by automatically combining records from different blockchains and making it easier to monitor and manage market activity.

Moreover, we propose a lattice-based sequential digital signature scheme for our blockchain system. Our proposed signature scheme maintains the sequence of signed signatures, which is essential for our system design. We also proved that our proposed scheme is secure against chosen-message attacks in the random oracle model. However, additional analysis and implementation of the proposed signature scheme should be provided in the future to prove its security in quantum random oracle model and test its practicality. Finally, we performed PoC experiments to demonstrate how the proposed system behaves differently in various blockchain settings. The experimental results have provide some issues to consider when implementing the proposed model.

We believe that various technologies useful for settlement such as liquidity-saving mechanisms or privacy-preserving computations, can be incorporated into our model in the future to build a more efficient and pragmatic settlement system.

Chapter 3

Quantifying the Connectedness between the Algorithmic-based Stablecoin and Cryptocurrency: The Impact of Death Spiral

3.1 Chapter Overview

Before its epic meltdown in May 2022, the Terra protocol, which was developed by Terraform Labs, had been evaluated as a successful blockchain project among investors. LUNA - a native token of Terra - had the 8th largest market capitalization among cryptocurrencies with nearly 40 billion USD in April 2022. The role of LUNA is to maintain the value of TerraUSD (UST), which is a stablecoin pegged to the US dollar in the Terra ecosystem. Unlike other well-known stablecoins, such as USDC and USDT, whose stability is secured with reserves of assets, a dollar peg of UST solely relies on the use of LUNA. According to the Terra whitepaper (Kereiakes et al. [2019]), LUNA absorbs the short-term volatility of UST value by providing an arbitrage opportunity to LUNA holders. Within the Terra ecosystem, anyone can swap UST with LUNA at the target exchange rate regardless of their current values. This means that users and arbitragers can instantaneously swap $1 worth of LUNA with one UST and profit from the difference when the demand for UST increases and its value suddenly exceeds the target value of $1. Similarly, if the value of UST falls below $1, UST token holders could swap their UST token holdings with that of LUNA to make a risk-free profit. This arbitrage system provides an incentive to market participants to anchor a dollar peg of UST. The pegging mechanism of UST is presented in Figure 3.1.Before UST collapsed in May 2022, the UST peg had remained stable.

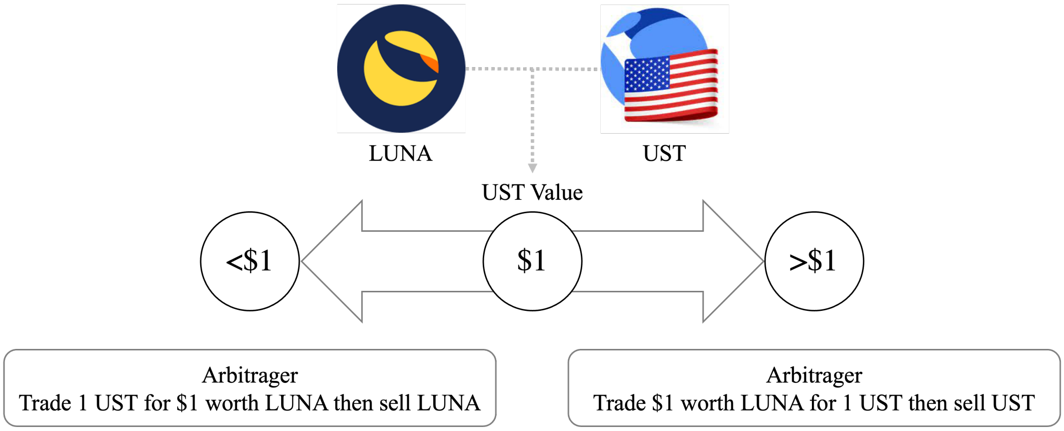

LUNA
UST
UST Value
<$1
$1
>$1
Arbitrager
Trade 1 UST for $1 worth LUNA then sell LUNA
Arbitrager
Trade $1 worth LUNA for 1 UST then sell UST

Figure 3.1: Figure 3.1 represents the pegging mechanism of UST. When UST is traded above peg, arbitragers can trade $1 worth of LUNA for 1 UST then sell the UST on the open market. When UST is traded below peg, arbitragers can trade 1 UST to $1 worth of LUNA and sell LUNA on the open market.

On May 9, 2022, 15:00 (UTC), the UST started to lose its dollar peg. It suffered from a de-anchoring to $0.985 the previous day before its value plunged much more quickly and drastically to as low as $0.35, showing extreme volatility within a day. The LUNA price plunged almost simultaneously with the UST depeg, but even more severely that it became less than $0.1 on May 12, 2022. Although the Terra blockchain officially halted on May 12, Terra tokens were still traded in the market. On May 25, Do Kwon's plan of launching a new blockchain called "Terra 2.0" was approved by chain validators, and LUNA and UST were renamed to LUNC and USTC, respectively. This epic saga ended as Terra 2.0 launched on May 28, which officially made LUNA and UST useless in the ecosystem. Figure 3.2 illustrates the LUNA and UST price movement during this period.

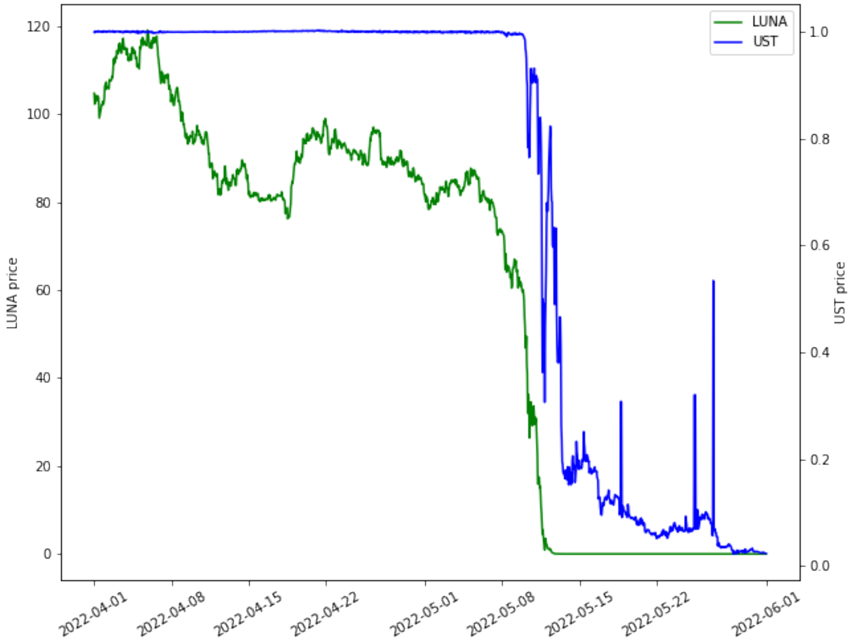


Figure 3.2: LUNA, UST price from April 2022 to May 2022

To the best of our knowledge, this thesis is a pioneer study analyzing the Terra-LUNA crash and its impact on the cryptocurrency market. Several studies have reported on the connectedness within the cryptocurrency market using the spillover effect(Ji et al. [2019], Yi et al. [2018], Corbet et al. [2018], Moratis [2021]), and have adopted the methodology suggested by Diebold and Yilmaz [2009, 2012]. Along with spillover effect, analyses based on information theory were also widely conducted to understand the interlinkage in the market (Assaf et al. [2022], Aslanidis et al. [2022]). Katsiampa [2019] used a bivariate diagonal BEKK model to understand volatility movements in the cryptocurrency market.

There are several studies investigating shock transmission within the cryptocurrency market. Using a nonlinear autoregressive distributed lag model, Demir et al. [2021] provided evidence that the asymmetric effect of Bitcoin price change on altcoins is mostly detected in the short-run. Bouri et al. [2019] and Zięba et al. [2019] focused on the shock transmission generated by Bitcoin to explain its influence on the entire market. Recently, some studies have reported how the cryptocurrency market has changed after the COVID-19 outbreak. Bouri et al. [2021], Demiralay and Golitsis [2021], and Aslanidis et al. [2021] reported a stronger connectedness between cryptocurrencies during the pandemic.

In this chapter, we aim to explore the relationship between Terra tokens and the cryptocurrency market, focusing on the impact brought by the Terra-LUNA crash. The effect of the instability of stablecoins on the market was reported by Wei [2018], who demonstrated that Tether does not have a serious impact on the Bitcoin market. However, the relationship between UST and LUNA is quite different from that of Tether and Bitcoin. LUNA and UST construct the basic ecosystem of the Terra blockchain, which makes them highly dependent on each other. In other words, the depeg of UST can drive risk in the Terra ecosystem, which was what eventually lead to the shocking crash of the Terra-LUNA project. Considering the market capitalization and ecosystem that Terra blockchain accomplished, the Terra-LUNA crash is an unprecedented collapse of a blockchain project. This amount of collapse in such a short period of time is also hard to be found in the entire financial market. Faced with an unprecedented collapse, investors' attention to LUNA skyrocketed during the crash period and debates on Terra project's future became widespread on social media. We used the spillover effect and effect transfer entropy to explain how the Terra-LUNA crash influenced the cryptocurrency market, investor attention, and market sentiment. Our results confirm that the Terra-LUNA crash had a significant impact to the overall cryptocurrency market, implying that stablecoins backed with fiat currencies is desperately needed for a more healthy cryptocurrency market in the future.

The rest of the chapter is organized as follows. Section 3.2 describes the data and methodology. Section 3.3 discusses our experimental results and main findings. Lastly, Section 3.4 concludes.

3.2 Data and Methodology

3.2.1 Data

We utilized four hourly and 5-minute cryptocurrency prices for our empirical analysis, namely BTC (Bitcoin), ETH (Ethereum), LUNA (Luna), and UST (TerraUSD). The price series was downloaded from the CoinMarketCap API [1]. Our data covers the period from April 2, 2022 to May 30, 2022, and were split into pre/post-Terra-LUNA crash, which started on May 9 at 15:00:00 (UTC), to capture the potential market changes driven by the crash. As our analysis was conducted on an hourly basis, we used the hourly log return of each cryptocurrency. We then constructed the hourly realized volatility by summing up the 12 squared 5-minute log returns.

We use the Google Trends index and tweets posted on StockTwits [2] containing the keyword "LUNA" as a proxy to quantify investor attention during the crash. Since Google Trends only provides hourly indexes for up to one week, we calibrated

[1] https://api.coinmarketcap.com/data-api/v3/cryptocurrency/detail/

[2] https://stocktwits.com/

Table 3.1: Descriptive Statistics

Panel A: Full Period				
	LUNA	UST	BTC	ETH
Mean	-0.0104	-0.0027	-0.0004	-0.0005
Median	-0.0017	0.0000	-0.0002	-0.0002
Standard Deviation	0.1291	0.1360	0.0071	0.0088
Min	-2.7023	-1.9701	-0.0702	-0.1009
Max	1.1786	2.2441	0.0550	0.0681
Skewness	-9.0439	0.9042	-0.4203	-1.1130
Kurtosis	194.2254	141.9541	14.2093	19.6799
Jarque Bera	2092830.9949***	1108438.0220***	11136.9389***	21566.1152***
Panel B: Pre-Terra-LUNA Crash period				
	LUNA	UST	BTC	ETH
Mean	-0.0009	0.0000	-0.0005	-0.0005
Median	-0.0009	0.0000	-0.0003	-0.0002
Standard Deviation	0.0105	0.0009	0.0050	0.0058
Min	-0.0493	-0.0043	-0.0341	-0.0311
Max	0.0543	0.0039	0.0190	0.0266
Skewness	-0.0915	0.0652	-0.6670	-0.5643
Kurtosis	3.9297	2.7602	5.0400	4.3215
Jarque Bera	532.0117***	262.0924***	935.8159***	686.5126***
Panel C: Terra-LUNA Crash period				
	LUNA	UST	BTC	ETH
Mean	-0.0267	-0.0072	-0.0002	-0.0005
Median	-0.0084	-0.0041	0.0003	-0.0002
Standard Deviation	0.2110	0.2238	0.0096	0.0123
Min	-2.7023	-1.9701	-0.0702	-0.1009
Max	1.1786	2.2441	0.0550	0.0681
Skewness	-5.3924	0.6128	-0.3388	-1.0003
Kurtosis	70.7229	51.0731	9.6962	12.5048
Jarque Bera	102802.6500***	52400.5717***	1893.0245***	3216.2989***

Note. Table 3.1 reports descriptive statistics of hourly returns of LUNA, UST, BTC, ETH. Panels A, B, and C report the values for the full period(April 02, 2022 to May 30, 2022), the pre-Terra-LUNA Crash period(April 02, 2022 to May 08, 2022), and the Terra-LUNA Crash period(May 09, 2022 to May 30, 2022). Asterisks flag levels of statistical significance of result statistic using t-test. The significance levels are flagged as follows: *** : p-value < 0.01, ** : p-value < 0.05

the index on a weekly basis by overlapping one item continuously to obtain the overall hourly Google Trends index for the selected period. Based on the positive (Bullish tag) and negative (Bearish tag) labels used by StockTwits users for their tweets, we directly calculated the hourly sentiment score related to LUNA as follows:

$$\text{Sent}_t = \frac{Positive_t - Negative_t}{Positive_t + Negative_t} \tag{3.1}$$

where $Positive_t$ and $Negative_t$ refer to the number of positive and negative labels during the period. Table 3.1 presents the descriptive statistics of the hourly asset returns for LUNA, UST, BTC, and ETH.

3.2.2 Methodology

Return and Volatility Spillovers To investigate the return and volatility connectedness of cryptocurrency markets, the methodology developed by Diebold and Yilmaz [2009, 2012] (DY framework hereafter) was used. The DY framework quantifies the spillover effect between the variables in the system by using the generalized vector autoregression model (VAR), which eliminates the effect of variable ordering in forecast-error variance decompositions. Consider an N-variable VAR(p) model, $x_t = \sum_{i=1}^{P} \Phi_i x_{t-i} + \epsilon_t$, where $\epsilon \sim (0, \Sigma)$ is a vector of i.i.d. disturbances. Then, the moving average form of such VAR model can be formulated as $x_t = \sum_{i=0}^{\infty} A_i \epsilon_{t-i}$, where A_i is the coefficient matrix with $A_i = 0$ for $i < 0$ and A_0 being an $N \times N$ identity matrix. To calculate the variance decompositions, the DY framework exploited the VAR framework of Koop et al. [1996] and Pesaran and Shin [1998] (KPPS hereafter), which does not attempt to orthogonalize shocks, but rather use the generalized approach with correlated shocks based on the historical distribution of errors. The strength of such framework is that the variance decompositions do not depend on the ordering of variables. For the variable x_i, for $i = 1, 2, ...N$, and the variable x_j causing the shock, the KPPS H-step ahead forecast error variance decompositions $\theta_{ij}^{g}(H)$ can be calculated as:

$$\theta_{ij}^{g}(H) = \frac{\sigma_{jj}^{-1} \sum\limits_{h=0}^{H-1} (e_i' A_h \Sigma e_j)^2}{\sum\limits_{h=0}^{H-1} (e_i' A_h \Sigma A_h' e_i)} \tag{3.2}$$

where e_i is the selection vector, Σ is the variance matrix for ϵ, and σ_{jj} is the standard deviation of the error for the j-th equation. By normalizing $\theta_{ij}^{g}(H)$ so that the sum of all entries equal to 1, we obtain the following $\tilde{\theta}^g_{ij}(H)$:

$$\tilde{\theta}^g_{ij}(H) = \frac{\theta^g_{ij}(H)}{\sum\limits_{j=1}^{N} \theta^g_{ij}(H)} \tag{3.3}$$

Then, the total spillovers, directional spillovers, net spillovers and net pairwise spillovers can be expressed as follows:

$$S^g(H) = \frac{\sum\limits_{\substack{i,j=1\\ j\neq i}}^{N} \tilde{\theta}^g_{ij}(H)}{\sum\limits_{i,j=1}^{N} \tilde{\theta}^g_{ij}(H)} \cdot 100 = \frac{\sum\limits_{\substack{i,j=1\\ j\neq i}}^{N} \tilde{\theta}^g_{ij}(H)}{N} \cdot 100 \tag{3.4}$$

$$S^g_{i\cdot}(H) = \frac{\sum\limits_{\substack{j=1\\ j\neq i}}^{N} \tilde{\theta}^g_{ij}(H)}{\sum\limits_{i,j=1}^{N} \tilde{\theta}^g_{ij}(H)} \cdot 100 = \frac{\sum\limits_{\substack{j=1\\ j\neq i}}^{N} \tilde{\theta}^g_{ij}(H)}{N} \cdot 100 \tag{3.5}$$

$$S^g_i(H) = S^g_{\cdot i}(H) - S^g_{i\cdot}(H) \tag{3.6}$$

$$\begin{aligned} S^g_{ij}(H) &= \left(\frac{\tilde{\theta}^g_{ji}(H)}{\sum\limits_{i,k=1}^{N} \tilde{\theta}^g_{ik}(H)} - \frac{\tilde{\theta}^g_{ij}(H)}{\sum\limits_{j,k=1}^{N} \tilde{\theta}^g_{jk}(H)} \right) \cdot 100 \\ &= \left(\frac{\tilde{\theta}^g_{ji}(H) - \tilde{\theta}^g_{ij}(H)}{N} \right) \cdot 100 \end{aligned} \tag{3.7}$$

Transfer Entropy To measure information flows between cryptocurrency markets, Shannon Transfer Entropy (TE) can be used (see Schreiber [2000] for more details). TE overcomes the well-known limitations of Granger causality (Granger [1969]), such as the linearity assumption, because it can be reduced to Granger causality for vector autoregressive processes. TE can be useful in analyzing the linkage between two time series, as it is can determine the direction of information flows and their magnitude. TE relies on the Kullback-Leibler distance to quantify the deviation between the transition probabilities. Considering two time series I and J, the information flow from J to I can be measured as:

$$T_{J \to I}(k,l) = \sum_{i,j} p(i_{t+1}, i_t^{(k)}, j_t^{(l)}) \cdot \log_2 \left(\frac{p(i_{t+1}|i_t^{(k)}, j_t^{(l)})}{p(i_{t+1}|i_t^{(k)})} \right) \tag{3.8}$$

where $p(i)$ and $p(j)$ are the marginal probability distributions of I and J, and $p(i,j)$ is the joint probability distribution. k and l denote the order of each process.

However, TE can be easily biased for the series with small sample sizes. As a result, Marschinski and Kantz [2002] suggested the Effective Transfer Entropy (ETE), which modifies TE by shuffling the time series J. Such modification eliminates the time series dependencies of J and the statistical dependencies between J and I. ETE can be calculated as:

$$ETE_{J \to I}(k,l) = T_{J \to I}(k,l) - T_{J_{\text{shuffled}} \to I}(k,l) \tag{3.9}$$

As our analysis focuses on a fairly short time frame (before and after the Terra-LUNA crash), we adopted ETE for our empirical analysis to correctly identify the linkage among the cryptocurrency markets during the crash.

3.3 Empirical Findings

3.3.1 Return and volatility spillover effects

To analyze the market situation during the testing period, we first calculated the spillovers between the markets. Table 3.2 reports the spillover matrix for hourly asset

Table 3.2: Directional Return Spillover

Panel A: Full Period

	LUNA	UST	BTC	ETH	from others
LUNA	80.6568	1.9412	9.0912	8.3106	19.3431
UST	1.7119	96.1950	1.1304	0.9625	3.8049
BTC	3.4916	0.6354	50.7683	45.1045	49.2316
ETH	3.5365	0.7278	45.1129	50.6226	49.3773
to others	8.7401	3.3046	55.3345	54.3778	30.4392

Panel B: Pre-Terra-LUNA Crash period

	LUNA	UST	BTC	ETH	from others
LUNA	53.9226	1.9854	21.9487	22.1431	46.0773
UST	2.8644	91.8533	2.3194	2.9626	8.1466
BTC	18.0365	0.9415	43.9119	37.1099	56.0880
ETH	18.4208	0.9086	37.0854	43.5850	56.4149
to others	39.3218	3.8357	61.3536	62.2157	41.6817

Panel C: Terra-LUNA Crash period

	LUNA	UST	BTC	ETH	from others
LUNA	77.6687	2.3796	11.2273	8.7244	22.3313
UST	2.0172	93.2487	2.5398	2.1943	6.7513
BTC	3.5992	0.8651	50.1467	45.3891	49.8533
ETH	3.7268	0.9038	45.8620	49.5074	50.4926
to others	9.3432	4.1484	59.6291	56.3078	32.3571

Note. Table 3.2 reports spillover matrix for hourly returns of LUNA, UST, BTC, ETH. Panels A, B, and C report the values for the full period(April 02, 2022 to May 30, 2022), the pre-Terra-LUNA Crash period(April 02, 2022 to May 08, 2022), and the Terra-LUNA Crash period(May 09, 2022 to May 30, 2022). The last column shows the total impact that the asset in each row received from the other assets and the last row shows the total impact sent to the other assets by the corresponding assets in each column.

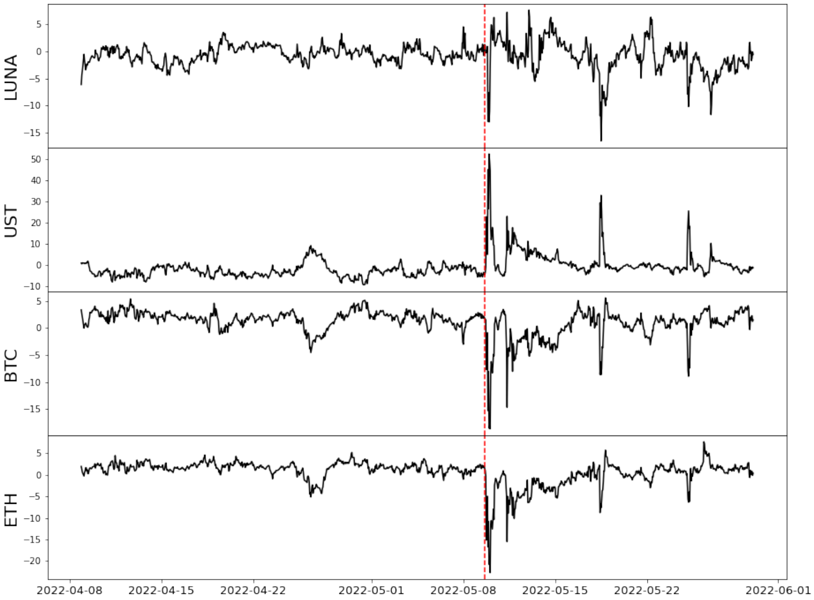


Figure 3.3: Net spillover from hourly returns

Note. The red line denotes the time (2022-05-09 15:00(UTC)) when UST started to depeg from its target value.

returns. Comparing the diagonal elements for Panels B and C in Table 3.2, values for LUNA increased from 53.9226 to 77.6687. This increase in portion value states that LUNA returns during the crash period are more likely to be attributable to the endogenous variation. Since the price crash of LUNA is claimed to have started due to the systematic risk of the Terra protocol, the enhancement of intrinsic impact on asset return is in line with the market situation. A similar characteristic can also be found in UST in that it also experienced an increase of endogenous impact on its hourly return.

We applied the rolling VAR based spillover index to calculate the net spillover

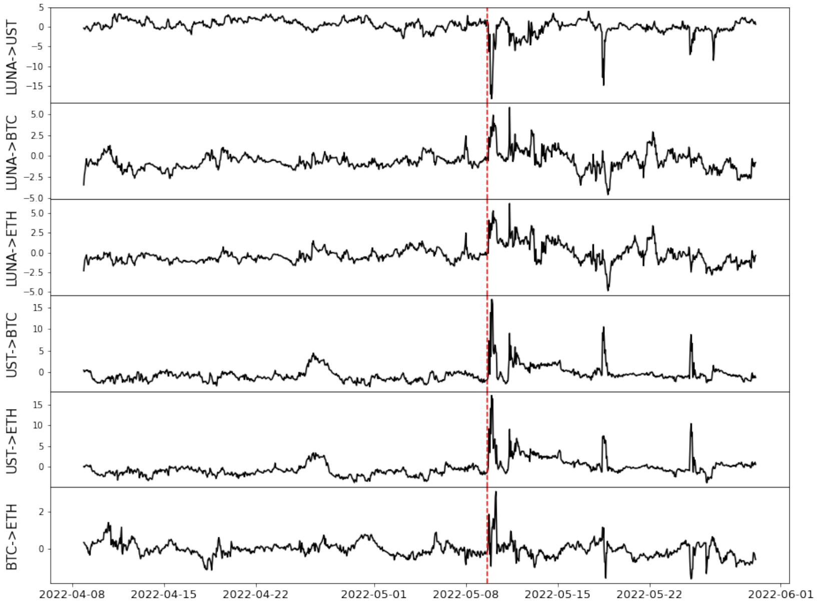


Figure 3.4: Pairwise spillover between assets from hourly returns

Note. The red line denotes the time (2022-05-09 15:00(UTC)) when UST started to depeg from its target value.

index for each asset and pairwise net spillover index for every asset combination throughout the testing period. The results are shown in Figures 3.3 and 3.4. Figure 3.3 shows that the net spillover from hourly returns suddenly changes immediately after the start of the depeg of UST. UST's net spillover rapidly increases to 50 while the net spillover of the other cryptocurrencies plunge to negative values. Net spillover indexes of UST and LUNA mostly remain positive for a week after the start of the depeg, which makes BTC and ETH lose its influence during this period. Figure 3.4 also suggests that UST's net pairwise spillover suddenly increases after the depeg and led to the dynamic change in market connectedness. This suggests that the

Table 3.3: Directional Volatility Spillover

Panel A: Full Period					
	LUNA	UST	BTC	ETH	from others
LUNA	94.9909	0.6057	1.5220	2.8815	5.0091
UST	0.1705	97.6094	1.2858	0.9343	2.3906
BTC	0.2024	0.2211	50.0209	49.5557	49.9791
ETH	0.3451	0.2931	43.5771	55.7847	44.2153
to others	0.7179	1.1199	46.3849	53.3715	25.3985
Panel B: Pre-Terra-LUNA Crash period					
	LUNA	UST	BTC	ETH	from others
LUNA	64.8200	0.8491	15.5723	18.7587	35.1800
UST	5.2307	93.0103	1.2130	0.5460	6.9897
BTC	14.1800	0.8635	48.2365	36.7199	51.7635
ETH	16.7207	0.9985	36.6384	45.6424	54.3576
to others	36.1315	2.7111	53.4236	56.0246	37.0727
Panel C: Terra-LUNA Crash period					
	LUNA	UST	BTC	ETH	from others
LUNA	92.5806	0.9108	2.8771	3.6315	7.4194
UST	0.3300	95.7481	2.3773	1.5447	4.2519
BTC	0.3871	0.6978	48.6801	50.2350	51.3199
ETH	0.4732	0.7369	44.6548	54.1351	45.8649
to others	1.1903	2.3455	49.9091	55.4112	27.2140

Note. Table 3.3 reports spillover matrix for hourly realized volatility of LUNA, UST, BTC, ETH. Panels A, B, and C report the values for the full period(April 02, 2022 to May 30, 2022), the pre-Terra-LUNA Crash period(April 02, 2022 to May 08, 2022), and the Terra-LUNA Crash period(May 09, 2022 to May 30, 2022). For each panel, items in the first column are risk transmitters and the items in the first row are risk receivers. The last column shows the total impact that the asset in each row received from the other assets and the last row shows the total impact sent to the other assets by the corresponding assets in each column.

Terra-LUNA crash was originated from the depeg of UST and not the meltdown of LUNA.

Table 3.3 reports the spillover matrix for asset volatility. In line with the findings in Table 3.2, the diagonal elements in Panel C increase compared to those in Panel B. LUNA especially shows an increase from 64.8200 to 92.5806, and the magnitude of this increase is even larger than that reported in Table 3.2. We conclude that this is due to the huge inflow of short-term investors right after the depeg of UST. After the start of the Terra-LUNA crash, many short-term investors entered the LUNA market and took positions to make a profit using high volatility. This caused the

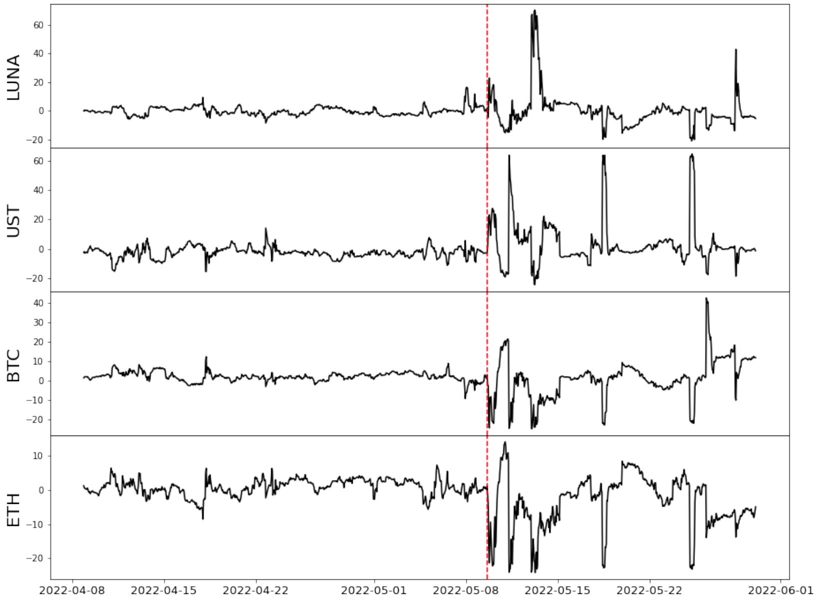


Figure 3.5: Net spillover from realized volatility of asset returns

Note. The red line denotes the time (2022-05-09 15:00(UTC)) when UST started to depeg from its target value.

market to become extremely volatile with a significant amount of trading volume, which naturally increased LUNA's volatility spillover on its own. Regarding net spillover index, LUNA's net spillover grew after the depeg, while UST also showed a significant increase, as shown in Figure 3.5. For net pairwise spillover indexes, according to Figure 3.6, LUNA and UST transmitted high volatility to the market right after the start of the depeg. This pattern is similar to that shown in Figure 3.3 implying that the Terra-LUNA crash brought about a significant change in both market returns and volatility. In order to examine the impact of the crash on the other cryptocurrencies as well, we also report the directional return and volatility

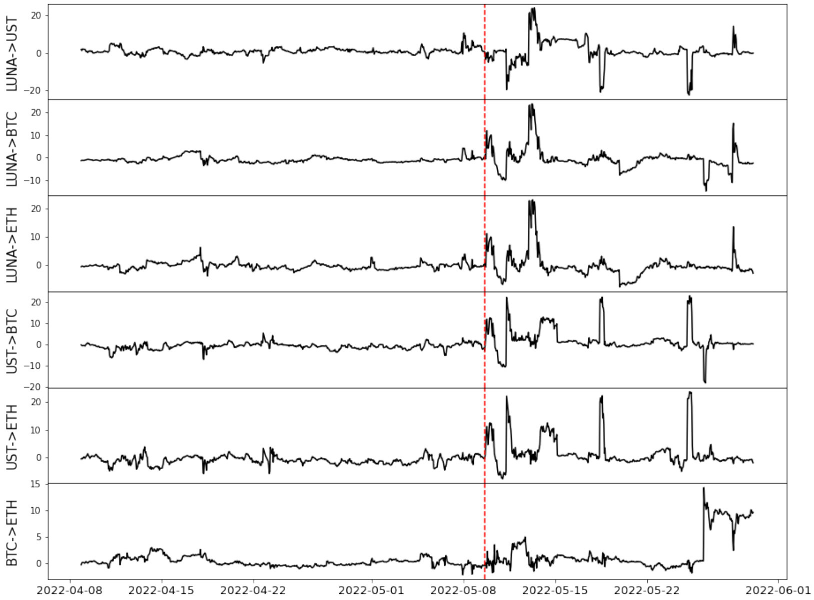


Figure 3.6: Pairwise spillover between assets from realized volatility of asset returns

Note. The red line denotes the time (2022-05-09 15:00(UTC)) when UST started to depeg from its target value.

spillover matrices for the top 10 cryptocurrencies by market capitalization. The market capitalization and names of 10 cryptocurrencies are reported in Table 3.6 and the directional spillover matrices are shown in Table 3.4 and Table 3.5. We confirm that the results are quite similar to Table 3.2 and Table 3.3. However, one significant difference is that the diagonal element of UST in Panel C decreases compared to the one in Panel B for both return and volatility, confirming that the other cryptocurrencies had a stronger connectedness to UST than BTC and ETH.

Table 3.4: Directional Return Spillover

Panel A: Full Period

	LUNA	UST	BTC	ETH	DOGE	ADA	BNB	XRP	DOT	SOL	MATIC	from others
LUNA	68.3253	3.1127	7.7938	7.2544	1.2387	1.5801	3.3732	2.8160	1.7345	1.5989	1.1724	31.6747
UST	2.0595	93.5181	1.1494	0.8509	0.3481	0.1057	0.2850	0.3334	0.1963	0.7955	0.3581	6.4819
BTC	4.9639	0.8236	47.6385	42.0862	0.5382	0.4868	0.6574	0.8106	1.1270	0.4964	0.3715	52.3615
ETH	4.8023	0.9640	41.9496	47.5529	0.7796	0.3492	0.5855	0.8971	1.0021	0.5528	0.5649	52.4471
DOGE	5.4258	0.6849	24.1461	26.1619	26.4595	2.3859	3.0039	3.5556	3.3330	2.2532	2.5902	73.5405
ADA	5.4229	1.0521	30.2692	32.1784	1.5620	11.8881	3.2726	3.4097	3.6045	3.3282	4.0122	88.1119
BNB	5.6303	0.7419	31.1165	33.3612	1.5002	3.0854	12.2119	2.5477	3.8783	2.7445	3.1821	87.7881
XRP	7.0961	0.7433	27.0015	28.9767	2.5632	3.6696	3.0223	14.7957	4.5863	3.5642	3.9811	85.2043
DOT	5.5827	0.7891	28.0519	30.2676	1.4252	3.5494	3.2423	3.9640	14.2714	4.3654	4.4911	85.7286
SOL	5.2948	0.8796	28.3938	30.2382	1.3917	3.2853	3.3779	3.3669	4.9500	13.6663	5.1555	86.3337
MATIC	5.6799	0.7928	28.6190	30.7704	1.4498	4.1416	3.4875	3.5921	4.6078	4.8282	12.0307	87.9693
to others	51.9581	10.5840	248.4908	262.1460	12.7969	22.6390	24.3076	25.2932	29.0199	24.5273	25.8790	67.0583

Panel B: Pre-Terra-LUNA Crash period

	LUNA	UST	BTC	ETH	DOGE	ADA	BNB	XRP	DOT	SOL	MATIC	from others
LUNA	51.0975	2.1814	21.4255	22.0659	0.0999	0.3076	0.8318	0.2697	0.6029	0.7272	0.3907	48.9025
UST	2.6017	84.9141	2.0573	2.6915	1.5141	1.2652	0.7325	1.7087	1.0159	1.1348	0.3642	15.0859
BTC	17.6788	1.0117	41.7566	35.3806	0.4191	0.5055	0.7580	0.7086	1.0265	0.4196	0.3349	58.2434
ETH	18.4460	1.0846	35.4304	41.5192	0.5742	0.3512	0.4062	0.5595	0.8980	0.4093	0.3214	58.4808
DOGE	9.7045	0.8728	17.4697	18.4711	37.4669	3.4284	2.8113	3.7806	2.0822	2.1616	1.7508	62.5331
ADA	15.2283	0.8517	23.0977	24.1358	1.5813	14.3326	4.5391	4.0012	4.9343	4.0458	3.2522	85.6674
BNB	15.5256	1.1584	24.6173	26.0564	1.1883	3.9203	13.9259	2.9071	4.0192	3.7121	2.9695	86.0741
XRP	13.0128	0.4709	21.4613	22.3442	1.8205	5.1517	4.1930	20.1325	4.6581	3.4788	3.2761	79.8675
DOT	15.7433	1.0369	23.6671	25.0143	0.8849	4.0896	4.2615	3.3943	14.0504	4.7566	3.1011	85.9496
SOL	16.4670	0.8554	22.7990	23.4126	1.0158	4.1020	3.8897	2.4217	5.1452	15.5066	4.3850	84.4934
MATIC	14.4255	0.9660	22.0177	22.7657	1.0614	4.1123	3.9607	3.1194	4.4469	5.6073	17.5171	82.4829
to others	138.8335	10.4899	214.0429	222.3381	10.1596	27.2338	26.3840	22.8708	28.8292	26.4531	20.1458	67.9800

Panel C: Terra-LUNA Crash period

	LUNA	UST	BTC	ETH	DOGE	ADA	BNB	XRP	DOT	SOL	MATIC	from others
LUNA	56.6986	3.1410	7.4190	7.5241	5.2476	3.0122	4.7971	5.5252	2.1260	2.9832	1.5261	43.3014
UST	4.1143	77.0469	2.7972	1.9184	1.5518	1.2519	1.4553	2.7703	1.9457	2.7529	2.3953	22.9531
BTC	7.6126	1.1939	41.6455	38.3821	1.1328	1.6236	2.0225	1.7407	1.6734	1.6028	1.3702	58.3545
ETH	7.9356	1.3409	37.8404	42.6655	1.0883	1.3893	2.0115	1.7388	1.4999	1.4187	1.0711	57.3345
DOGE	8.7930	0.9169	24.3044	28.4545	12.2144	2.7518	4.8714	4.7970	4.6675	4.2182	4.0109	87.7856
ADA	7.8015	1.3124	30.3187	33.3969	2.9739	9.6398	2.9093	2.8159	3.0020	2.8047	3.0246	90.3602
BNB	7.5604	1.3329	28.8237	32.4303	2.4150	3.5158	11.7215	2.3255	4.4177	2.1830	3.2742	88.2785
XRP	9.5577	0.9053	27.2670	32.0675	4.2263	2.9496	2.9593	9.7907	3.8238	3.2509	3.2019	90.2093
DOT	7.3027	1.0441	27.2082	30.9489	4.0175	2.7458	3.6541	3.6160	11.5524	3.7006	4.2098	88.4476
SOL	7.2904	1.0642	28.0355	31.4740	3.7041	2.6391	3.9048	3.3567	4.2821	10.0252	4.2238	89.9748
MATIC	7.3813	1.0860	28.7041	31.8455	3.2193	4.3227	3.8994	3.0821	4.5686	4.1526	7.7384	92.2616
to others	75.3493	13.3375	242.7182	268.4422	29.5767	26.2018	32.4848	31.7683	32.0066	29.0677	28.3078	73.5692

Note. Table reports spillover matrix for hourly returns of LUNA, UST, BTC, ETH, DOGE, ADA, BNB, XRP, DOT, SOL, and MATIC. Panels A, B, and C report the values for the full period(April 02, 2022 to May 30, 2022), the pre-Terra-LUNA Crash period(April 02, 2022 to May 08, 2022), and the Terra-LUNA Crash period(May 09, 2022 to May 30, 2022). The last column shows the total impact that the asset in each row received from the other assets and the last row shows the total impact sent to the other assets by the corresponding assets in each column.

Table 3.5: Directional Volatility Spillover

Panel A: Full Period

	LUNA	UST	BTC	ETH	DOGE	ADA	BNB	XRP	DOT	SOL	MATIC	from others
LUNA	82.7404	3.9802	1.0477	1.2787	1.0472	0.9401	2.9024	1.1032	1.2435	1.4112	2.3055	17.2596
UST	0.2966	81.5437	1.3848	0.8644	0.2938	2.1697	1.8636	2.6889	2.7934	3.3126	2.7886	18.4563
BTC	0.4639	0.0689	30.4551	30.9047	2.2466	4.3237	5.5474	6.2414	5.6058	7.4993	6.6432	69.5449
ETH	0.5956	0.1293	26.7704	36.5596	1.9419	3.5918	4.9494	5.9514	5.3147	7.6191	6.5768	63.4404
DOGE	0.8451	0.1644	10.2734	16.0323	36.0727	4.5167	5.8314	6.3012	6.0145	7.2255	6.7229	63.9273
ADA	0.5589	0.3624	15.6200	22.3346	2.2313	12.1390	8.7345	8.1535	8.9903	10.6337	10.2418	87.8610
BNB	0.7154	0.2948	14.2045	21.5513	2.5042	9.4758	15.7605	7.5983	8.4692	9.6704	9.7558	84.2395
XRP	0.5821	0.2140	14.6001	21.9262	2.8219	6.0957	6.9922	12.9428	10.5994	12.1676	11.0581	87.0572
DOT	0.6913	0.2489	15.3971	23.6958	2.5201	5.0765	5.5943	10.8537	12.2199	12.2844	11.4179	87.7801
SOL	0.4387	0.4347	13.8234	21.4617	2.5341	6.9316	7.9709	10.2305	10.6251	14.0284	11.5211	85.9716
MATIC	0.6220	0.3001	15.0991	22.8972	2.4582	6.3189	7.0887	9.6706	10.2860	11.8036	13.4557	86.5443
C. to others (spillover)	5.8097	6.1976	128.2203	182.9469	20.5992	49.4403	57.4748	68.7925	69.9421	83.6273	79.0316	68.3711

Panel B: Pre-Terra-LUNA Crash period

	LUNA	UST	BTC	ETH	DOGE	ADA	BNB	XRP	DOT	SOL	MATIC	from others
LUNA	55.7043	1.2191	10.0569	13.0199	0.6486	2.1370	7.1917	1.0240	1.5678	3.1136	4.3173	44.2957
UST	7.0385	79.4591	1.4858	0.6345	2.2710	2.4257	1.0099	1.6180	1.1231	1.6284	1.3060	20.5409
BTC	9.6215	0.7945	37.9405	28.4617	1.5381	3.9145	7.1486	1.6298	3.5399	2.0819	3.3290	62.0595
ETH	12.1988	1.3360	29.0507	37.5687	1.4144	3.4850	5.7299	1.2084	2.3324	2.5797	3.0959	62.4313
DOGE	1.4861	1.3393	1.4983	1.1295	62.4829	6.9851	5.8983	11.6312	2.6134	2.0632	2.8727	37.5171
ADA	1.1514	0.7334	3.8298	3.8618	0.9016	25.7854	16.0060	11.1924	14.0054	11.1803	11.3526	74.2146
BNB	2.4260	0.7507	3.4976	3.6677	1.3334	16.1254	28.9771	9.2390	13.3428	9.7416	10.8988	71.0229
XRP	1.5240	0.5479	2.8079	3.5478	1.7764	14.5472	12.6596	33.0526	11.8162	8.4253	9.2950	66.9474
DOT	2.1807	0.1690	5.1438	4.8491	0.8262	14.5315	13.8633	9.7777	27.6205	11.2055	9.8326	72.3795
SOL	3.7205	0.4772	4.1125	5.4066	1.0985	13.6832	11.9240	8.1827	12.2357	29.0696	10.0895	70.9304
MATIC	2.3765	0.7710	4.3777	4.4815	0.6775	13.1567	13.2682	8.3066	11.3570	10.3040	30.9234	69.0766
C. to others (spillover)	43.7239	8.1381	65.8610	69.0601	12.4857	90.9911	94.6994	63.8098	73.9338	62.3236	66.3894	59.2196

Panel C: Terra-LUNA Crash period

	LUNA	UST	BTC	ETH	DOGE	ADA	BNB	XRP	DOT	SOL	MATIC	from others
LUNA	62.2341	7.6061	1.5458	1.7762	5.8919	2.2838	2.5314	4.5166	4.0307	3.9477	3.6357	37.7659
UST	0.7134	55.8580	2.3156	2.1037	3.2200	4.7541	5.4153	5.5849	6.9342	7.1838	5.9171	44.1420
BTC	0.8781	0.8759	28.6515	28.1251	7.7689	3.2353	4.1494	7.0751	4.7460	7.9015	6.5930	71.3485
ETH	1.1497	1.0302	27.4569	33.2478	7.4368	2.4130	3.6191	6.3205	4.2389	7.0112	6.0759	66.7522
DOGE	1.6309	1.1514	18.2425	23.7062	14.3353	4.7863	6.6414	7.5019	6.4903	7.6847	7.8289	85.6647
ADA	0.9201	1.4260	22.2232	26.7157	7.3147	7.8998	5.4091	6.6907	6.3666	7.4091	7.6250	92.1002
BNB	1.0584	1.1844	20.7898	26.6211	7.7424	5.5888	11.0793	6.0130	5.9391	6.4600	7.5237	88.9207
XRP	1.2906	1.0526	18.7881	21.9565	8.9288	5.0469	6.8715	9.8044	7.5814	9.6815	8.9978	90.1956
DOT	1.2008	1.1073	20.3895	25.9042	8.3069	3.7133	4.7969	8.7190	8.6080	8.6670	8.5873	91.3920
SOL	1.4562	1.2749	18.4928	22.9930	7.5717	6.2382	7.9027	8.1993	7.4669	9.7378	8.6664	90.2622
MATIC	1.2861	1.3741	21.2947	27.2753	7.7103	4.5916	5.6213	7.3625	6.7435	7.9204	8.8202	91.1798
C. to others (spillover)	11.5843	18.0829	171.5390	207.1769	71.8925	42.6513	52.9582	67.9835	60.5377	73.8668	71.4508	77.2476

Note. Table reports spillover matrix for hourly realized volatility of LUNA, UST, BTC, ETH, DOGE, ADA, BNB, XRP, DOT, SOL, and MATIC. Panels A, B, and C report the values for the full period(April 02, 2022 to May 30, 2022), the pre-Terra-LUNA Crash period(April 02, 2022 to May 08, 2022), and the Terra-LUNA Crash period(May 09, 2022 to May 30, 2022). For each panel, items in the first column are risk transmitters and the items in the first row are risk receivers. The last column shows the total impact that the asset in each row received from the other assets and the last row shows the total impact sent to the other assets by the corresponding assets in each column.

Table 3.6: Market capitalization of the 10 cryptocurrencies

Name	Symbol	Market Capitalization
Bitcoin	BTC	$884,585,801,886
Ethereum	ETH	$412,362,544,752
BNB	BNB	$72,623,207,488
Solana	SOL	$43,111,128,032
Ripple	XRP	$39,815,777,701
Cardano	ADA	$39,180,026,439
Terra	LUNA	$37,747,677,146
Polkadot	DOT	$21,529,251,333
Dogecoin	DOGE	$18,463,699,718
Polygon	MATIC	$13,083,649,216

Note. Table 3.6 reports the top 10 cryptocurrencies by market capitalization as of April 02, 2022. The price data was collected from *coinmarketcap.com*.

3.3.2 Effective Transfer Entropy

As suggested in Section 3.2, we used ETE to measure the information transfer between time series sequences. Additional to the hourly asset return and volatility, we included hourly sequences of Google Trends index for LUNA, as well as the number of tweets with the cashtag "$LUNA.X" and the sentiment score for "$LUNA.X" on StockTwits in the analysis. This was done to measure the information transfer during the Terra-LUNA crash, including that on investor attention (Google Trends and the number of tweets) and market sentiment (sentiment score). Tables 3.7 and 3.8 report the ETE values calculated with asset return and volatility, respectively.

The results in Panel B in Table 3.7 show that there was an information flow from the sentiment score to LUNA returns before the Terra-LUNA crash. However, this flow disappears during the crash period and investor attention measured by Google Trends index and the number of tweets are shown to transmit information to LUNA returns. In other words, LUNA returns received information flow from

Table 3.7: Effective Transfer Entropy: Return

Panel A: Full Period							
	LUNA	UST	BTC	ETH	Google Trends	Number of Tweets	Sentiment Score
LUNA		0.0197***	0.0218***	0.0314***	0.005	0.0217***	0.0004
UST	0.0023		0.0059**	0.0088***	0.0004	0.006	0.0017
BTC	0.0122***	0.0002		0.0063**	0.0000	0.0055	0.0005
ETH	0.0199***	0.0048**	0.0000		0.0000	0.0086***	0.0023
Google Trends	0.0172***	0.0137***	0.0105***	0.0127***		0.0365***	0.0000
Number of Tweets	0.0191***	0.0158***	0.0025**	0.0057***	0.0266***		0.0000
Sentiment Score	0.0000	0.0004	0.0051***	0.0023	0.0000	0.0021	
Panel B: Pre-Terra-LUNA Crash period							
	LUNA	UST	BTC	ETH	Google Trends	Number of Tweets	Sentiment Score
LUNA		0.0043	0.0000	0.0102**	0.0000	0.0014	0.0031
UST	0.0029		0.0000	0.0005	0.0002	0.0002	0.0071**
BTC	0.0000	0.0000		0.0006	0.0010	0.0018	0.0009
ETH	0.0009	0.0019	0.0000		0.0000	0.0005	0.0030
Google Trends	0.0000	0.0016	0.0018	0.0000		0.0217***	0.0000
Number of Tweets	0.0039	0.0000	0.0002	0.0000	0.0048		0.0000
Sentiment Score	0.0103***	0.0091***	0.0000	0.0071***	0.0031	0.0058**	
Panel C: Terra-LUNA Crash period							
	LUNA	UST	BTC	ETH	Google Trends	Number of Tweets	Sentiment Score
LUNA		0.0189**	0.0374***	0.0353***	0.0045	0.0083	0.0000
UST	0.0001		0.0173***	0.0045	0.0000	0.0000	0.0000
BTC	0.0191***	0.0038		0.0000	0.0096	0.0028	0.0135
ETH	0.0160**	0.0007	0.0058		0.0099	0.0052	0.0068
Google Trends	0.0132***	0.0053	0.0158***	0.0142***		0.0283***	0.0042
Number of Tweets	0.0276***	0.0000	0.0017	0.0026	0.0056		0.0000
Sentiment Score	0.0000	0.0040	0.0308***	0.0106***	0.0003	0.0000	

Note. Table 3.7 reports effective transfer entropy values calculated with hourly asset returns. Panels A, B, and C report the values for the full period(April 02, 2022 to May 30, 2022), the pre-Terra-LUNA Crash period(April 02, 2022 to May 08, 2022), and the Terra-LUNA Crash period(May 09, 2022 to May 30, 2022). For each panel, items in the first column are sequences that transmit information and the items in the first row are sequences that receive information. Asterisks flag levels of statistical significance of result statistic using t-test. The significance levels are flagged as follows: *** : p-value < 0.01, ** : p-value < 0.05

Table 3.8: Effective Transfer Entropy: Volatility

Panel A: Full Period

	LUNA	UST	BTC	ETH	Google Trends	Number of Tweets	Sentiment Score
LUNA		0.0136***	0.0289***	0.0250***	0.0035**	0.0161***	0.0000
UST	0.0031		0.0010	0.0026	0.0023	0.0058**	0.0010
BTC	0.0239***	0.0007		0.0002	0.0040**	0.0075***	0.0000
ETH	0.0293***	0.0010	0.0171***		0.0059**	0.0054**	0.0004
Google Trends	0.0114***	0.0056***	0.0080***	0.0133***		0.0365***	0.0000
Number of Tweets	0.0122***	0.0021	0.0063**	0.0105***	0.0266***		0.0000
Sentiment Score	0.0029	0.0000	0.0015	0.0013	0.0000	0.0021	

Panel B: Pre-Terra-LUNA Crash period

	LUNA	UST	BTC	ETH	Google Trends	Number of Tweets	Sentiment Score
LUNA		0.0000	0.0055	0.0140***	0.0000	0.0033	0.0081***
UST	0.0000		0.0010	0.0012	0.0000	0.0018	0.0005
BTC	0.0158***	0.0000		0.0021	0.0047	0.0047	0.0000
ETH	0.0129***	0.0000	0.0037		0.0006	0.0035	0.0000
Google Trends	0.0013	0.0011	0.0000	0.0003		0.0217***	0.0000
Number of Tweets	0.0053	0.0000	0.0000	0.0052	0.0048		0.0000
Sentiment Score	0.0002	0.0000	0.0003	0.0008	0.0031	0.0058**	

Panel C: Terra-LUNA Crash period

	LUNA	UST	BTC	ETH	Google Trends	Number of Tweets	Sentiment Score
LUNA		0.0185***	0.0000	0.0000	0.0050	0.0065	0.0000
UST	0.0074		0.0000	0.0003	0.0000	0.0000	0.0006
BTC	0.0038	0.0000		0.0000	0.0085***	0.0196***	0.0000
ETH	0.0000	0.0045	0.0059		0.0059	0.0077	0.0000
Google Trends	0.0000	0.0000	0.0000	0.0024		0.0283***	0.0042
Number of Tweets	0.0023	0.0000	0.0116**	0.0000	0.0056		0.0000
Sentiment Score	0.0000	0.0014	0.0013	0.0000	0.0003	0.0000	

Note. Table 3.8 reports effective transfer entropy values calculated with hourly realized volatility of each asset. Panels A, B, and C report the values for the full period(April 02, 2022 to May 30, 2022), the pre-Terra-LUNA Crash period(April 02, 2022 to May 08, 2022), and the Terra-LUNA Crash period(May 09, 2022 to May 30, 2022). For each panel, items in the first column are sequences that transmit information and the items in the first row are sequences that receive information. Asterisks flag levels of statistical significance of result statistic using t-test. The significance levels are flagged as follows: *** : p-value < 0.01, ** : p-value < 0.05

investor attention, not investor sentiment, during the Terra-LUNA crash period. We conclude that the keen collusion between bearish and bullish opinions about the future of LUNA's price is the reason why market sentiment lost its influence. While investors had different opinions about LUNA on StockTwits, its price plunged drastically because the extent of the meltdown was unprecedented and LUNA seemed to be too large to collapse considering its market capitalization. Since the sentiment among investors became too diverse to be aggregated, it naturally lost its power as a transmitter of information flow to LUNA returns. On the other hand, investor attention drastically increased during the crash period; along with the LUNA meltdown, attention could have become a significant information transmitter.

The relationship between cryptocurrency returns also changed according to the findings in Panels B and C in Table 3.7. Before the crash, except for the flow from LUNA to ETH returns, asset returns did not show evidence of information flows. However, Panel C reports that LUNA returns transmitted information flow to UST, BTC, and ETH returns during the crash period, while also receiving information flows from BTC and ETH returns. This finding is in line with that from Corbet et al. [2022], which interlinkages between cryptocurrencies becoming stronger during bear markets. An interesting point is that entropy values that LUNA returns transmit to other assets are larger than the values that LUNA returns receive. This indicates that LUNA returns show a strong influence on the market during the crash period and the bearish trends of the cryptocurrency market during this time may be explained by the LUNA meltdown. This corroborates our finding on the net pairwise spillover in Figure 3.4, which suggests that LUNA mostly showed a positive net pairwise spillover during its price crash.

In terms of volatility, according to Table 3.8, investor sentiment before the Terra-LUNA crash transmitted information flow to LUNA volatility. However, during the price crash, this information flow no longer becomes valid. We conclude that this is due to the diversification of investor sentiment during the crash period, similar to the situation with LUNA's returns. Although sentiment score is a recipient of information flow for volatility, chaos in market sentiment during the price crash may also lead to the loss of information flow. Additionally, from Panel B in Table 3.8, BTC and ETH used to transmit information flow to LUNA in terms of volatility, but this flow disappears during the crash period. This finding is in line with our result on spillover matrix from Table 3.3, which shows that LUNA's volatility became more dependent on its intrinsic risk and not the market situation during its crash. In order to quantify the information transfer between a wider range of cryptocurrencies, we report the ETE values with 10 cryptocurrencies in Table 3.9 and 3.10. We confirm that the results are quite similar to Table 3.7 and Table 3.8.

3.4 Chapter Summary

In this chapter, we analyzed the impact of the Terra-LUNA crash on the cryptocurrency market from April 2022 to May 2022 by investigating the spillover effect and ETE. We confirm that the internal spillover effect for the returns and volatility of both LUNA and UST increased during the crash, which means that the crash was due to the systematic risk of the project and not the market situation. LUNA and UST also show an increase in net spillovers during this period, which implies that their crash brought a significant change to the market.

For effective transfer entropy, we included sequences that could represent in-

Table 3.9: Effective Transfer Entropy: Return

Panel A: Full Period

	LUNA	UST	BTC	ETH	DOGE	ADA	BNB	XRP	DOT	SOL	MATIC	Google Trends	Number of Tweets	Sentiment Score
LUNA		0.0197***	0.0218***	0.0314***	0.0226***	0.0416***	0.0385***	0.0350***	0.0399***	0.0410***	0.0476***	0.0050	0.0222***	0.0004
UST	0.0023		0.0059***	0.0091***	0.0088***	0.0172***	0.0189***	0.0158***	0.0210***	0.0154***	0.0196***	0.0003	0.0060	0.0013
BTC	0.0122***	0.0003		0.0061***	0.1205***	0.1793***	0.1867***	0.1589***	0.1494***	0.1524***	0.1780***	0.0000	0.0053	0.0005
ETH	0.0199***	0.0050***	0.0000		0.1262***	0.2213***	0.2199***	0.1748***	0.1868***	0.1859***	0.2138***	0.0000	0.0088***	0.0023
DOGE	0.0038	0.0055***	0.0163***	0.0137***		0.0039***	0.0034	0.0000	0.0001	0.0042	0.0000	0.0059	0.0017	0.0000
ADA	0.0146***	0.0106***	0.0066***	0.0113***	0.0000		0.0048***	0.0000	0.0000	0.0074***	0.0011	0.0020	0.0025	0.0012
BNB	0.0203***	0.0105***	0.0149***	0.0189***	0.0000	0.0015		0.0000	0.0017	0.0000	0.0041	0.0038	0.0075***	0.0006
XRP	0.0172***	0.0069***	0.0099***	0.0064***	0.0000	0.0020	0.0021		0.0039	0.0080***	0.0021	0.0053	0.0039	0.0000
DOT	0.0189***	0.0063***	0.0158***	0.0104***	0.0013	0.0030	0.0077***	0.0044***		0.0112***	0.0003	0.0067***	0.0121***	0.0001
SOL	0.0095***	0.0065***	0.0206***	0.0185***	0.0019	0.0111***	0.0094***	0.0046***	0.0057***		0.0054***	0.0000	0.0049	0.0000
MATIC	0.0156***	0.0084***	0.0188***	0.0185***	0.0000	0.0007	0.0074***	0.0024	0.0000	0.0003		0.0014	0.0053	0.0000
Google Trends	0.0176***	0.0135***	0.0108***	0.0132***	0.0086***	0.0277***	0.0262***	0.0216***	0.0240***	0.0188***	0.0136***		0.0365***	0.0000
Number of Tweets	0.0190***	0.0162***	0.0028***	0.0059***	0.0032***	0.0149***	0.0194***	0.0076***	0.0197***	0.0148***	0.0139***	0.0268***		0.0000
Sentiment Score	0.0000	0.0010	0.0049***	0.0024	0.0063***	0.0000	0.0016	0.0009	0.0009	0.0043***	0.0022***	0.0000	0.0018	

Panel B: Pre-Terra-LUNA Crash Period

	LUNA	UST	BTC	ETH	DOGE	ADA	BNB	XRP	DOT	SOL	MATIC	Google Trends	Number of Tweets	Sentiment Score
LUNA		0.0042	0.0000	0.0096***	0.0750***	0.1004***	0.0920***	0.0680***	0.0866***	0.1006***	0.1016***	0.0000	0.0013	0.0032
UST	0.0026		0.0000	0.0003	0.0000	0.0011	0.0047	0.0000	0.0006	0.0058	0.0045	0.0002	0.0003	0.0071***
BTC	0.0000	0.0000		0.0006	0.0516***	0.1391***	0.1405***	0.1260***	0.1542***	0.1309***	0.1116***	0.0011	0.0022	0.0006
ETH	0.0010	0.0015	0.0000		0.0966***	0.1592***	0.1688***	0.1506***	0.1940***	0.1255***	0.1507***	0.0000	0.0000	0.0032
DOGE	0.0057	0.0000	0.0000	0.0000		0.0000	0.0000	0.0000	0.0000	0.0000	0.0018	0.0000	0.0000	0.0030
ADA	0.0007	0.0000	0.0000	0.0021	0.0000		0.0000	0.0000	0.0000	0.0003	0.0000	0.0009	0.0000	0.0000
BNB	0.0023	0.0000	0.0000	0.0000	0.0000	0.0000		0.0000	0.0000	0.0000	0.0024	0.0012	0.0051	0.0020
XRP	0.0071***	0.0000	0.0000	0.0000	0.0008	0.0000	0.0054		0.0056	0.0000	0.0048	0.0022	0.0055	0.0000
DOT	0.0037	0.0000	0.0000	0.0000	0.0047	0.0118***	0.0020	0.0082***		0.0011	0.0038	0.0054	0.0003	0.0047
SOL	0.0056***	0.0032	0.0000	0.0006	0.0090***	0.0079***	0.0015	0.0090***	0.0072***		0.0035	0.0000	0.0000	0.0000
MATIC	0.0081***	0.0007	0.0007	0.0057	0.0030	0.0000	0.0000	0.0022	0.0000	0.0000		0.0022	0.0000	0.0000
Google Trends	0.0000	0.0019	0.0019	0.0000	0.0000	0.0017	0.0000	0.0000	0.0004	0.0042***	0.0000		0.0215***	0.0000
Number of Tweets	0.0035	0.0000	0.0000	0.0000	0.0004	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0049		0.0000
Sentiment Score	0.0101***	0.0095***	0.0000	0.0073***	0.0008	0.0004	0.0015	0.0015	0.0010	0.0026	0.0005	0.0032***	0.0056***	

Panel C: Terra-LUNA Crash Period

	LUNA	UST	BTC	ETH	DOGE	ADA	BNB	XRP	DOT	SOL	MATIC	Google Trends	Number of Tweets	Sentiment Score
LUNA		0.0189***	0.0371***	0.0353***	0.0532***	0.0457***	0.0499***	0.0515***	0.0586***	0.0228***	0.0299***	0.0048	0.0081	0.0000
UST	0.0000		0.0169***	0.0071	0.0017	0.0063***	0.0087***	0.0023	0.0136***	0.0084***	0.0070	0.0000	0.0000	0.0003
BTC	0.0191***	0.0022		0.0000	0.1593***	0.1689***	0.1392***	0.1413***	0.1618***	0.1793***	0.1754***	0.0094	0.0024	0.0134***
ETH	0.0164***	0.0012	0.0056		0.1987***	0.2249***	0.2122***	0.1493***	0.1724***	0.1891***	0.2144***	0.0101	0.0055	0.0058
DOGE	0.0299***	0.0030	0.0400***	0.0248***		0.0224***	0.0111***	0.0274***	0.0237***	0.0306***	0.0198***	0.0026	0.0108	0.0097
ADA	0.0236***	0.0048	0.0242***	0.0354***	0.0000		0.0011	0.0033	0.0014	0.0000	0.0022	0.0172***	0.0099	0.0056
BNB	0.0330***	0.0054	0.0154***	0.0285***	0.0108***	0.0081		0.0005	0.0036	0.0000	0.0000	0.0050	0.0178***	0.0092
XRP	0.0263***	0.0047	0.0156***	0.0361***	0.0072	0.0063	0.0072		0.0120***	0.0041	0.0044	0.0031	0.0195***	0.0065
DOT	0.0252***	0.0111	0.0158***	0.0301***	0.0018	0.0000	0.0000	0.0007		0.0000	0.0000	0.0162***	0.0083	0.0059
SOL	0.0039	0.0093	0.0261***	0.0258***	0.0183***	0.0188***	0.0093***	0.0194***	0.0195***		0.0204***	0.0053	0.0102	0.0068
MATIC	0.0274***	0.0115***	0.0110***	0.0080***	0.0063	0.0001	0.0000	0.0000	0.0059	0.0000		0.0118	0.0102	0.0075
Google Trends	0.0121***	0.0051	0.0152***	0.0136***	0.0033***	0.0239***	0.0050	0.0156***	0.0207***	0.0092***	0.0177***		0.0285***	0.0036
Number of Tweets	0.0275***	0.0000	0.0007	0.0016	0.0077***	0.0000	0.0013	0.0007	0.0096***	0.0086***	0.0076***	0.0048		0.0000
Sentiment Score	0.0000	0.0042	0.0293***	0.0123***	0.0105***	0.0000	0.0000	0.0000	0.0000	0.0000	0.0005	0.0007	0.0000	

Note. Table 3.9 reports effective transfer entropy values calculated with hourly asset returns. Panels A, B, and C report the values for the full period(April 02, 2022 to May 30, 2022), the pre-Terra-LUNA Crash period(April 02, 2022 to May 08, 2022), and the Terra-LUNA Crash period(May 09, 2022 to May 30, 2022). For each panel, items in the first column are sequences that transmit information and the items in the first row are sequences that receive information. Asterisks flag levels of statistical significance of result statistic using t-test. The significance levels are flagged as follows: *** : p-value < 0.01, ** : p-value < 0.05

Table 3.10: Effective Transfer Entropy: Volatility

Panel A: Full Period

	LUNA	UST	BTC	ETH	DOGE	ADA	BNB	XRP	DOT	SOL	MATIC	Google Trends	Number of Tweets	Sentiment Score
LUNA		0.0134***	0.0292***	0.0248***	0.0108***	0.0222***	0.0198***	0.0203***	0.0296***	0.0201***	0.0342***	0.0032	0.0157***	0.0000
UST	0.0038***		0.0005	0.0025	0.0015	0.0048***	0.0030	0.0095***	0.0074***	0.0102***	0.0024	0.0027	0.0058***	0.0011
BTC	0.0241***	0.0004		0.0003	0.0256***	0.0476***	0.0459***	0.0277***	0.0271***	0.0316***	0.0350***	0.0043***	0.0078***	0.0000
ETH	0.0286***	0.0013	0.0168***		0.0268***	0.0449***	0.0391***	0.0307***	0.0376***	0.0292***	0.0311***	0.0063***	0.0054***	0.0004
DOGE	0.0085***	0.0000	0.0139***	0.0146***		0.0065***	0.0027	0.0022	0.0055***	0.0050***	0.0049***	0.0015	0.0000	0.0000
ADA	0.0084***	0.0036	0.0109***	0.0084***	0.0019		0.0050***	0.0000	0.0014	0.0083***	0.0049***	0.0000	0.0052***	0.0000
BNB	0.0065***	0.0000	0.0158***	0.0073***	0.0011	0.0038		0.0000	0.0040	0.0120***	0.0089***	0.0084***	0.0051	0.0000
XRP	0.0107***	0.0044***	0.0090***	0.0111***	0.0029	0.0070***	0.0013		0.0106***	0.0109***	0.0056***	0.0028	0.0051	0.0000
DOT	0.0087***	0.0003	0.0153***	0.0078***	0.0031	0.0000	0.0060***	0.0064***		0.0070***	0.0097***	0.0009	0.0052***	0.0000
SOL	0.0103***	0.0000	0.0080***	0.0114***	0.0075***	0.0058***	0.0067***	0.0046***	0.0069***		0.0034	0.0000	0.0027	0.0000
MATIC	0.0081***	0.0000	0.0095***	0.0116***	0.0000	0.0007	0.0030	0.0000	0.0011	0.0046***		0.0000	0.0049	0.0015
Google Trends	0.0111***	0.0052***	0.0078***	0.0136***	0.0043***	0.0216***	0.0154***	0.0201***	0.0248***	0.0184***	0.0197***		0.0365***	0.0000
Number of Tweets	0.0120***	0.0024	0.0062***	0.0103***	0.0027	0.0167***	0.0107***	0.0058***	0.0167***	0.0200***	0.0195***	0.0268***		0.0000
Sentiment Score	0.0026***	0.0000	0.0016	0.0014	0.0049***	0.0024	0.0014	0.0065***	0.0002	0.0000	0.0007	0.0000	0.0018	

Panel B: Pre-Terra-LUNA Crash Period

	LUNA	UST	BTC	ETH	DOGE	ADA	BNB	XRP	DOT	SOL	MATIC	Google Trends	Number of Tweets	Sentiment Score
LUNA		0.0000	0.0054***	0.0147***	0.0002	0.0132***	0.0063***	0.0059***	0.0040	0.0047	0.0049	0.0000	0.0039	0.0080***
UST	0.0000		0.0001	0.0012	0.0000	0.0034	0.0000	0.0087***	0.0021	0.0070***	0.0000	0.0000	0.0024	0.0004
BTC	0.0154***	0.0000		0.0021	0.0007	0.0131***	0.0229***	0.0032	0.0132***	0.0019	0.0086***	0.0045***	0.0042	0.0000
ETH	0.0134***	0.0002	0.0041		0.0012	0.0157***	0.0196***	0.0062	0.0141***	0.0046	0.0117***	0.0004	0.0037	0.0000
DOGE	0.0000	0.0000	0.0056	0.0008		0.0000	0.0000	0.0000	0.0013	0.0061	0.0000	0.0000	0.0000	0.0000
ADA	0.0000	0.0000	0.0013	0.0000	0.0016		0.0000	0.0000	0.0000	0.0000	0.0004	0.0000	0.0061	0.0000
BNB	0.0017	0.0005	0.0000	0.0027	0.0008	0.0000		0.0000	0.0007	0.0000	0.0000	0.0000	0.0000	0.0000
XRP	0.0000	0.0000	0.0048	0.0000	0.0000	0.0000	0.0000		0.0000	0.0000	0.0002	0.0000	0.0039	0.0004
DOT	0.0033	0.0001	0.0048	0.0020	0.0091***	0.0057	0.0026	0.0000		0.0033	0.0032	0.0001	0.0031	0.0002
SOL	0.0000	0.0000	0.0013	0.0031	0.0030	0.0024	0.0000	0.0016	0.0010		0.0042	0.0000	0.0005	0.0001
MATIC	0.0000	0.0000	0.0050***	0.0032	0.0000	0.0037	0.0000	0.0000	0.0044***	0.0000		0.0041	0.0038	0.0025
Google Trends	0.0020	0.0019	0.0000	0.0002	0.0000	0.0070***	0.0000	0.0000	0.0050***	0.0000	0.0000		0.0215***	0.0000
Number of Tweets	0.0050	0.0000	0.0000	0.0059	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0049		0.0000
Sentiment Score	0.0003	0.0000	0.0000	0.0010	0.0023	0.0000	0.0000	0.0037	0.0000	0.0000	0.0007	0.0032***	0.0056***	

Panel C: Terra-LUNA Crash Period

	LUNA	UST	BTC	ETH	DOGE	ADA	BNB	XRP	DOT	SOL	MATIC	Google Trends	Number of Tweets	Sentiment Score
LUNA		0.0174***	0.0000	0.0000	0.0054	0.0000	0.0028	0.0000	0.0000	0.0021	0.0000	0.0041	0.0051***	0.0000
UST	0.0078		0.0000	0.0002	0.0000	0.0051	0.0000	0.0024	0.0000	0.0000	0.0012	0.0000	0.0000	0.0015
BTC	0.0027	0.0000		0.0000	0.0165***	0.0260***	0.0089	0.0400***	0.0252***	0.0064	0.0199***	0.0083***	0.0200***	0.0000
ETH	0.0000	0.0041	0.0067***		0.0320***	0.0440***	0.0238***	0.0202***	0.0323***	0.0144***	0.0339***	0.0060	0.0074	0.0000
DOGE	0.0016	0.0000	0.0219***	0.0044		0.0140***	0.0093***	0.0176***	0.0048	0.0183***	0.0084	0.0070	0.0000	0.0000
ADA	0.0000	0.0000	0.0112***	0.0008	0.0000		0.0000	0.0000	0.0000	0.0055	0.0000	0.0079***	0.0012	0.0146***
BNB	0.0000	0.0000	0.0359***	0.0024	0.0082	0.0290***		0.0021	0.0049	0.0205***	0.0233***	0.0068***	0.0056	0.0031
XRP	0.0000	0.0000	0.0183***	0.0154***	0.0019	0.0124***	0.0000		0.0056	0.0129***	0.0152***	0.0000	0.0012	0.0000
DOT	0.0079	0.0019	0.0194***	0.0029	0.0000	0.0078	0.0030	0.0000		0.0045	0.0007	0.0098***	0.0019	0.0007
SOL	0.0000	0.0033	0.0061	0.0000	0.0000	0.0183***	0.0000	0.0023	0.0009		0.0040	0.0096***	0.0000	0.0000
MATIC	0.0029	0.0000	0.0100***	0.0120***	0.0015	0.0049	0.0039	0.0069	0.0000	0.0173***		0.0069	0.0052	0.0039
Google Trends	0.0000	0.0000	0.0000	0.0019	0.0059	0.0162***	0.0088***	0.0000	0.0000	0.0002	0.0000		0.0285***	0.0036
Number of Tweets	0.0027	0.0000	0.0116***	0.0000	0.0112***	0.0138***	0.0157***	0.0103***	0.0093***	0.0072***	0.0044	0.0048		0.0000
Sentiment Score	0.0005	0.0004	0.0023	0.0000	0.0000	0.0068	0.0000	0.0022	0.0000	0.0010	0.0039	0.0007	0.0000	

Note. Table 3.10 reports effective transfer entropy values calculated with hourly asset returns. Panels A, B, and C report the values for the full period(April 02, 2022 to May 30, 2022), the pre-Terra-LUNA Crash period(April 02, 2022 to May 08, 2022), and the Terra-LUNA Crash period(May 09, 2022 to May 30, 2022). For each panel, items in the first column are sequences that transmit information and the items in the first row are sequences that receive information. Asterisks flag levels of statistical significance of result statistic using t-test. The significance levels are flagged as follows: *** : p-value < 0.01, ** : p-value < 0.05

vestor attention and market sentiment during this period using Google Trends and StockTwits. We show that market sentiment loses its role as a transmitter and recipient of information flow to LUNA's returns and volatility, respectively, during the crash. We conclude that this is due to the growing discrepancy in investors' opinions about the future of the Terra-LUNA project. Investor attention, however, rapidly increases during the price crash and transmitted information flow to LUNA returns. Moreover, while the information flow between asset returns emerged during the price crash, LUNA's volatility loses its connectedness to the volatility of BTC and ETH after the price crash.

In future research, our investigation could be enriched by including traditional assets, such as equities and bonds, into the universe to measure the impact that the Terra-LUNA crash brought to the returns and volatility of traditional asset classes. Also, future researchers can consider providing an early warning system to the public before the crisis. With our experimental results showing that the sentiment score loses its role as an information transmitter during the crisis, one can track the mismatch between investor sentiment and the sentiment of the messages or twits to capture signals for future crashes. We believe that our study is not only limited to the cryptocurrency markets, but also can be extended to the traditional asset markets such as stocks.

Chapter 4

Return-Volume Relationship in Non-Fungible Tokens: Evidence from the Granger Causality in Quantiles

4.1 Chapter Overview

Since the beginning of 2021, NFTs have gained significant public attention as a new form of digital asset from the blockchain and cryptocurrency industries (Nadini et al. [2021]). NFTs can store any form of digtal assets: art, collectibles, game items, virtual real estates and etc. (Wang et al. [2021b]). During August 2021, the daily sales volume of NFTs once reached up to \$400M and it still maintains about average of \$30M in 2022. Traditional cryptocurrencies (e.g Bitcoin or Ethereum) are considered to be fungible, as all the cryptocurrencies have equal values. On the other hand, even though some NFTs belong to the same project (e.g Cryptopunks or Decentraland), each individual NFTs have its own originality, thus creating different valuations independently. However, since NFTs are frontier innovations that were developed in very recent year, the ongoing researches on NFTs are not sufficient compared to the researches on the overall cryptocurrency markets (Dowling [2022b], Ante [2022]). To fill this gap, we aim to study the return-volume relationship in the NFT markets.

The return-volume relationship between cryptocurrencies was regularly discussed in many fields of research. Borri and Shakhnov [2020] examines the spillover effect of changes in Chinese domestic regulation of cryptocurrencies to Bitcoin prices. The results imply that the trading volume and relative Bitcoin prices increase in neighboring countries. Naeem et al. [2020] provides the evidence of tail dependence in the return-volume of leading cryptocurrencies. They show that extreme cryptocurrency returns are correlated with extreme trading volume. Fousekis and Tzaferi [2021] analyzes the causality between returns and volumes in cryptocurrency markets, by utilizing the flexibe frequency connectedness methodology. They confirm that the trading volume information play a role as a significant technical indicator to gain higher profits from the trading. Yarovaya and Zięba [2022] confirms the existence of significant bidirectional causalities between trading volume and returns across the top 30 most traded cryptocurrencies.

As mentioned above, even though there has been sufficient researches on examining the return-volume relationship between the cryptocurrencies, the return-volume relationship between NFTs are not examined thoroughly in the past literature. NFTs have significantly different technological characteristics compared to the traditional cryptocurrencies, as the liquidity of tokens are extremely low compared to regular cryptocurrencies, due to their independent uniqueness of the assets. As a result, the trading volume of the NFTs are much smaller, and the NFT owners might even have difficulties in searching the suitable buyer of their assets. Therefore, we believe that this nature of NFTs can lead to different patterns in the return-volume relationship in comparison to other types of digital assets.

Additionally, NFTs are built on diverse blockchain platforms with different purposes. These platforms usually provide different services to let its NFT owners to actually use their NFTs in the blockchain ecosystem, so that there are actual benefits for purchasing the NFTs. For example, LAND tokens of Decentraland and The Sandbox represent the ownership on the virtual land in the metaverse world. So by purchasing the LAND tokens, the land in the virtual world becomes the user's property (Dowling [2022a]). Along with NFTs, most of these platforms also have its own native cryptocurrencies. These cryptocurrencies are mainly used for two purposes. First, they are traded as a means of transaction on the corresponding platform. Second, the owners can participate in the governance of the blockchain system. To this end, the demand and the price for these cryptocurrencies highly reflects the success of the blockchain system. Therfore, we attempt to examine the relationship between the price of NFTs and its native cryptocurrencies, to check whether the market performance of the blockchain system is reflected in the price of the NFTs. To examine this causal relationship between volume and return, we implement the Granger causality test in quantiles. The details of the methodology is described in Section 4.2. By testing the statistically significant Granger causality between NFT return and volume along with NFTs' native cryptocurrencies, we aim to solve the following two research questions. (1) Under what market conditions can a strong causal relationship be found between NFT return and NFT trading volume? (2) Are the price of NFTs related to the price of its protocol's native cryptocurrencies?

The rest of the chapter is organized as follows. Section 4.2 describes the data and methodology. Section 4.3 discusses our experimental results and main findings. Lastly, Section 4.4 concludes.

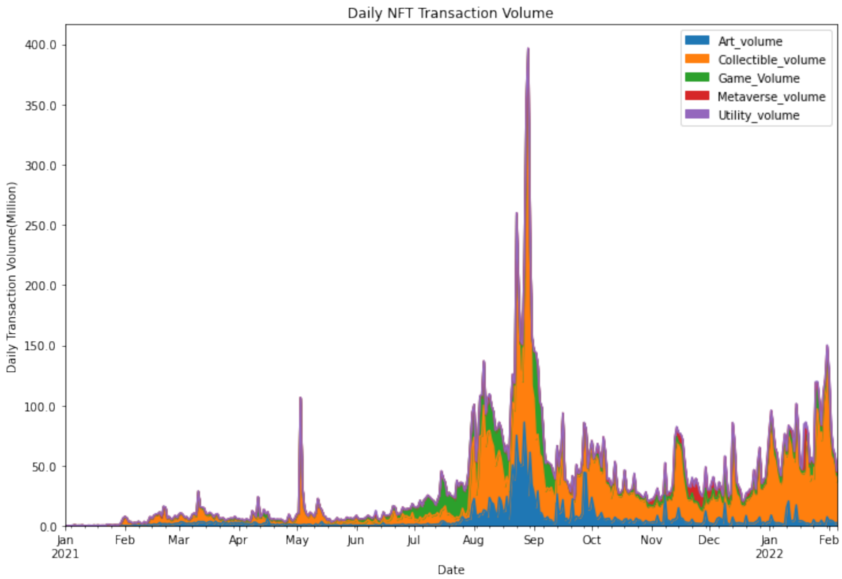


Figure 4.1: Daily transaction volume of NFTs for different categories.

4.2 Data and Methodology

4.2.1 Data

To identify the causal relationships between NFT return (r_t) and trading volume (v_t), we use the daily average price and trading volume of the overall NFT market. Our daily data is collected from *nonfungible.com*, covering from Jan 1, 2018 to Mar 30, 2022. There are total 1550 observations. We calculated the log return of the average price series as $r_t = 100 \times \ln p_t - \ln p_{t-1}$. For analyzing the causality between the individual NFT markets and their corresponding cryptocurrencies, we chose three NFT service platforms which provide their own fungible tokens to facilitate the transactions and purchases in their own ecosystems: Axie Infinity-AXS, Decentraland-MANA, and The Sandbox-SAND. We chose these three tokens as MANA is the largest, AXS is the third largest, and SAND is the fourth largest

NFT-related cryptocurrency market in terms of market capitalization. Table 4.1 reports the summary statistics for the price returns and volume for the overall NFTs, Axie Infinity, Decentraland, and The Sandbox respectively. Table 4.2 reports the summary statistics for the price returns for the NFT-related cryptocurrencies: AXS, MANA, and SAND. [1]

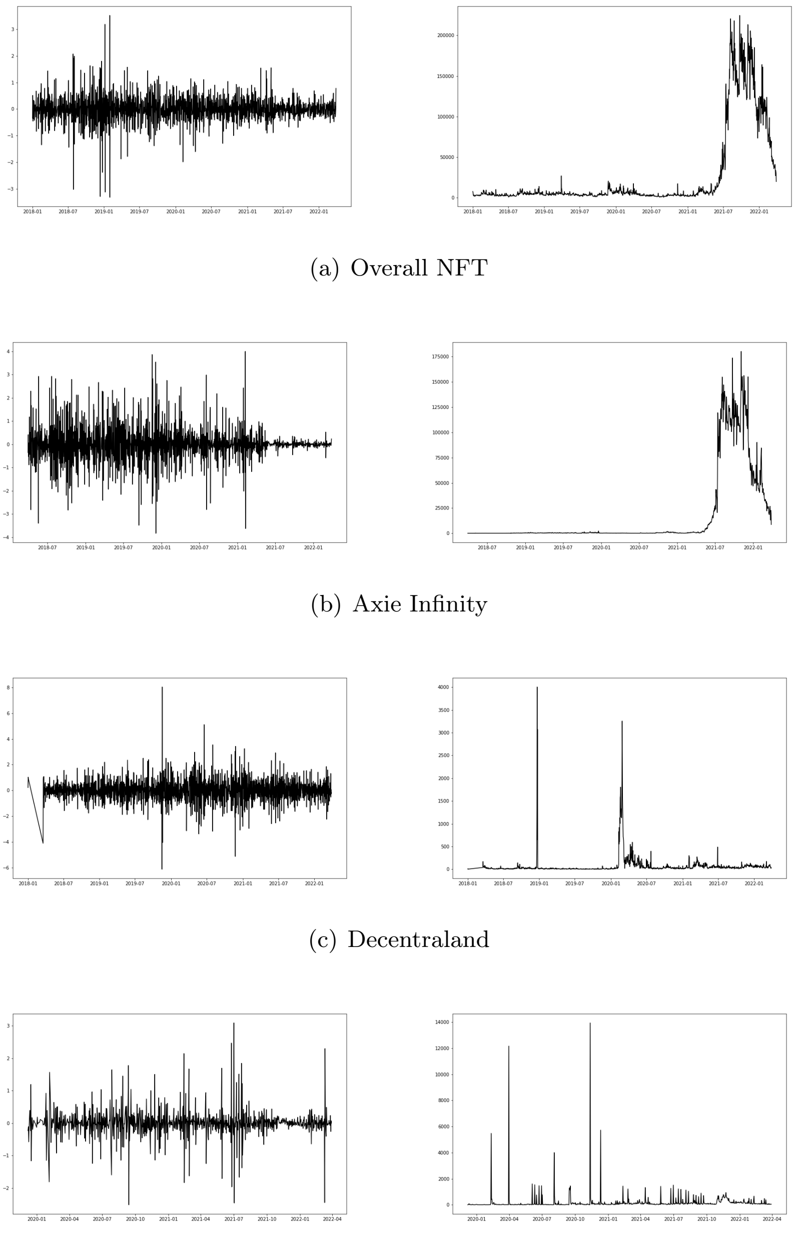
Table 4.1: Summary statistics for NFT returns and volume

	Overall NFTs		**Axie Infinity**	
	Return(r_t)	Volume(v_t)	Return(r_t)	Volume(v_t)
Mean	0.0029	2.5888	-0.0013	1.6596
Median	-0.0035	0.4294	-0.0101	0.0322
Std.	0.4944	5.0150	0.7623	3.7601
Min.	-3.3237	0.0242	-3.8348	0.0001
Max.	3.5278	22.4768	3.9929	18.0232
Skew.	-0.1684	2.2140	0.23785	2.2990
Kurto.	8.3015	3.5605	4.5245	3.9741

	Decentraland		**The Sandbox**	
	Return(r_t)	Volume(v_t)	Return(r_t)	Volume(v_t)
Mean	0.0006	0.0070	0.0060	0.0183
Median	0.0014	0.0024	0.0099	0.0064
Std.	0.9227	0.0229	0.4558	0.0751
Min.	-6.1235	0.0001	-2.51557	0.0001
Max.	8.0366	0.4005	3.0861	1.3947
Skew.	0.1835	9.8291	0.1786	14.0087
Kurto.	7.2917	122.861	10.7020	228.5471

Note. Volumes here are the number of sales times 10^{-4}

[1] Bored Ape Yacht Club's APE, launched in March 2022, is the second largest, but it was omitted from our analysis due to insufficient observations.



(a) Overall NFT

(b) Axie Infinity

(c) Decentraland

(d) The Sandbox

Figure 4.2: The time series of log return (left) and trading volume (right).

Table 4.2: Summary statistics for NFT-related cryptocurrency return series

	AXS	**MANA**	**SAND**
Mean	0.0086	0.0017	0.0054
Median	0.0008	-0.0002	-0.0008
Std.	0.1023	0.1168	0.2050
Min.	-0.4986	-2.3312	-1.4616
Max.	0.5408	2.2851	1.5897
Skew.	0.7550	0.0587	0.2422
Kurto.	4.4586	206.8258	25.6980

4.2.2 Methodology: Granger causality test in quantiles

Granger causality was first proposed by Granger [1969], to decide the direction of causality between two related variables in time series. Formally, for two time series x_t and y_t, x does not Granger cause y if

$$F_{y_t}(\eta|(y,x)_{t-1}) = F_{y_t}(\eta|y_{t-1}), \quad \forall \eta \in \mathbb{R} \tag{4.1}$$

where F_{y_t} is the conditional distribution of y_t and $(y,x)_{t-1}$ is the past information generated by x and y until time $t-1$. Thus, x does not Granger cause y if the past information of x does not change the conditional distribution of y. To estimate and test this conditional distribution F_{y_t}, we test the following:

$$\mathbb{E}(y_t|(y,x)_{t-1}) = \mathbb{E}(y_t|y_{t-1}) \tag{4.2}$$

where $\mathbb{E}(y_t|\cdot)$ is the mean of the conditional distribution. We test 4.2 by fitting the linear regression model:

$$y_t = \alpha_0 + \sum_{i=1}^{q} \alpha_i y_{t-i} + \sum_{j=1}^{q} \beta_j x_{t-j} \tag{4.3}$$

The null hypothesis becomes $H_0 : \beta_j = 0, j = 1, \dots q$, which states that the past information of x does not have significant impact on forecasting the condition mean of y_t. However, this only reveals information about the Granger causality in mean and the causality in other quantiles should be discussed separately. To verify the causal relationship between two time series x_t and y_t for various qunatiles, Chuang et al. [2009] propose a Granger causality test based on the quantile regression method (See Koenker and Bassett Jr [1978], Koenker and Hallock [2001] for more details on quantile regression). For a given quantile interval $[a, b]$, we can confirm that x_t does not Granger cause y_t if the following equality holds:

$$\mathcal{Q}_{y_t}(\tau|((\mathcal{Y}, \mathcal{X})_{t-1}) = \mathcal{Q}_{y_t}(\tau|(\mathcal{Y}_{t-1})), \quad \forall \tau \in [a, b] \tag{4.4}$$

where $\mathcal{Q}_{y_t}(\tau|\mathcal{F})$ denotes the τ-th quantile of $F_{y_t}(\cdot|\mathcal{F})$ which is the conditional distribution of y_t. Also, $(\mathcal{Y}, \mathcal{X})_{t-1}$ is the information set generated by $x_{t-1}, \dots, x_{t-q}$ and $y_{t-1}, \dots, y_{t-q}$. Letting $\mathbf{y}_{t-1:q} = [y_{t-1}, \dots, y_{t-q}]', \mathbf{x}_{t-1:q} = [x_{t-1}, \dots, x_{t-q}]'$ and $\mathbf{z}_{t-1} = [1, \mathbf{y}'_{t-1:q}, \mathbf{x}'_{t-1:q}]'$ To test (4.4), consider the following τ-th conditional quantile regression model :

$$\mathcal{Q}_{y_t}(\tau|(\mathbf{z}_{t-1}) = a(\tau) + \mathbf{y}'_{t-1:q}\boldsymbol{\alpha}(\tau) + \mathbf{x}'_{t-q:1}\boldsymbol{\beta}(\tau) = \mathbf{z}'_{t-1}\boldsymbol{\theta}(\tau) \tag{4.5}$$

where $\boldsymbol{\theta}(\tau) = [a(\tau), \boldsymbol{\alpha}(\tau)', \boldsymbol{\beta}(\tau)']'$ is the k-dimensional parameter vector with $k = 1 + 2q$. Then, the null hypothesis for the Granger non-causality over $\tau \in [a, b]$ is

$$H_0 : \boldsymbol{\beta}(\tau) = \mathbf{0}, \quad \forall \tau \in \text{(a,b)}. \tag{4.6}$$

To check the significance of $\boldsymbol{\beta}(\tau)$ for $\forall\tau \in$ (a,b), we must calculate the Wald statistic. The Wald statistic for a given τ is

$$\mathscr{W}_T(\tau) \doteq T\frac{\hat{\boldsymbol{\beta}}_T(\tau)'\hat{\Omega}(\tau)^{-1}\hat{\boldsymbol{\beta}}_T(\tau)}{\tau(1-\tau)} \tag{4.7}$$

where $\hat{\Omega}(\tau)$ is a consistent estimator of $\Omega(\tau)$, which is the variance-covariance matrix of $\boldsymbol{\beta}(\tau)$. Under suitable conditions, Koenker and Machado [1999] suggest that the weak limit of the Wald statistic is the sum of squares of q independent Bessel processes, so the Wald statistic converges to:

$$\mathscr{W}_T(\tau) \Rightarrow ||\frac{\mathbf{B}_q(\tau)}{\sqrt{\tau(1-\tau)}}||^2, \quad \tau \in [a,b] \tag{4.8}$$

Note that $\mathbf{B}_q(\tau)$ denotes the Bessel process, which is a vector of q independent Brownian bridges. (A Brownian bridge equals $[\tau(1-\tau)]^{1/2}\mathscr{N}(0,\mathbf{I}_q)$ in distribution.) Therefore, we can write the supremum of the Wald statistic using the continuous mapping theorem as follows:

$$\sup_{\tau\in[a,b]} \mathscr{W}_T(\tau) \xrightarrow{D} \sup_{\tau\in[a,b]} ||\frac{\mathbf{B}_q(\tau)}{\sqrt{\tau(1-\tau)}}||^2 \tag{4.9}$$

Practically, we may choose n different $\tau_i(i = 1,\ldots,n)$ in $[a,b]$ so that $a \leq \tau_1 < \tau_2 <,\ldots,< \tau_n \leq b$, to compute the sup-Wald statistic for (4.6) as $\sup_{i=1,\ldots,n}\mathscr{W}_T(\tau_i)$. Therefore, we can identify the Granger causality over various quantile range between two time series using the sup-Wald test results. When n becomes larger, the right hand side of (4.8) is known to be a good approximation to the null limit of sup-Wald statistic. Thus, the critical values for the sup-Wald test can be obtained via simulating the Bessel processes. Some of the critical values from the simulations are presented in Table 4.3. [2] For example, if the results of the sup-Wald test reject the null hypothesis (4.6) on the entire range (ex. $[0.05, 0.95]$), but cannot reject it on a certain smaller range $[a, b]$, we may confirm that there exists a Granger causality from x_t to y_t on the outside of $[a, b]$.

Table 4.3: The critical values of the sup-Wald test on $[0.05, 0.95]$ quantile range. We used the standard Brownian motion with 3,000 Gaussian random walks followed by 20,000 replications.

	$q = 1$	$q = 2$	$q = 3$
1%	13.24	16.71	19.12
5%	9.66	12.90	15.38
10%	8.13	11.06	13.50

4.3 Empirical results

4.3.1 Causal effects of NFT volume on return

To investigate the causal effects between NFT return and NFT trading volume, consider the following regression model which predicts the NFT return in time t using the past NFT return and volume series:

$$r_t = a(\tau) + \sum_{j=1}^{q} \alpha_j(\tau) r_{t-j} + \sum_{j=1}^{q} \beta_j(\tau) \ln v_{t-j} + e_t \tag{4.10}$$

In the case of traditional stock markets, it is known that there exist a noticeable pattern in the trading volume series (Chuang et al. [2009], Gallant et al. [1992], Chen et al. [2001], Lee and Rui [2002]), so many researchers have detrended the log volume series by regressing it on a time trend term, such as t/T and $(t/T)^2$. To reflect the trend that the trading volume tends to grow as the time passes, we add

[2] Other critical values for various quantile ranges can be provided upon request. Readers can also see Andrews [1993] for a more comprehensive simulation results.

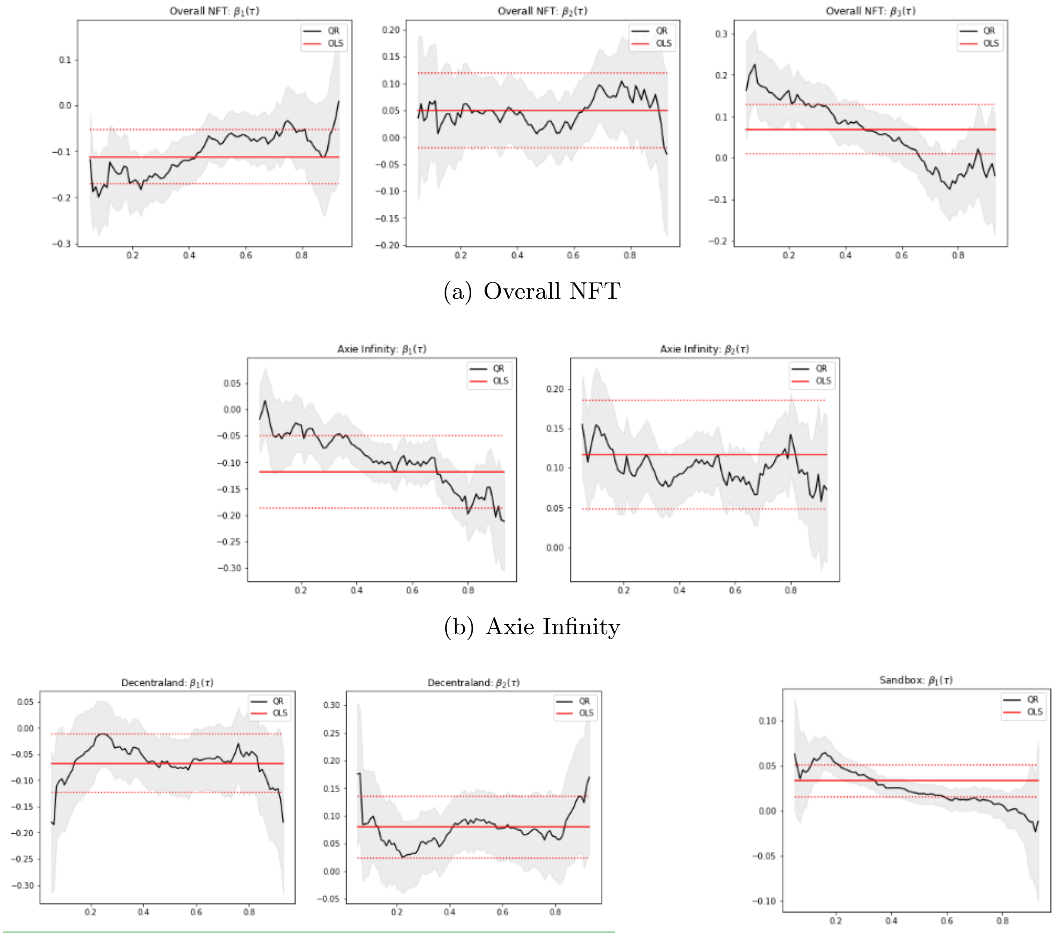
these time trend terms to our regression model:

$$r_t = a(\tau) + b(\tau)\frac{t}{T} + c(\tau)\left(\frac{t}{T}\right)^2 + \sum_{j=1}^{q} \alpha_j(\tau) r_{t-j} + \sum_{j=1}^{q} \beta_j(\tau) \ln v_{t-j} + e_t \qquad (4.11)$$

where T is the sample size of the data. The model was estimated using the quantile regression (QR) and ordinary least squares (OLS) methods . In order to select the optimal lag order q^*, we applied the sup-Wald test to the coefficients $\beta_j(\tau)$. For a given $q = k$, if $\beta_k(\tau)$ is not statistically significant while $\beta_{k-1}(\tau)$ for $q = k-1$ is significant, we chose our optimal lag order as $q^* = k - 1$. The selected lag orders for the overall NFT market, Axie Infinity, Decentraland and The Sandbox are 3,2,2,1 respectively.

Figure 4.3 shows the QR (black line) and OLS (red line) coefficients of the return-volume regression model against various quantiles (τ) for the selected NFTs. We also plotted the 95% confidence intervals for QR (grey area) and OLS (red dotted line) together. Except for The Sandbox, the OLS estimates confirm that there is a negative causality in mean at lag 1 as the coefficients are below zero, while there exist a positive causality in mean for the higher lags. However, the QR estimates exhibit different patterns. For the overall NFT market, β_1 and β_3 show that the magnitude of causal effect decreases at the upper quantiles, as the coefficients move towards zero. β_1 of Axie Infinity implies that the magnitude becomes larger for the upper quantiles, as the coefficient moves away from zero. On the other hand, the QR estimates for Decentraland have larger magnitude at both lower and upper tails, compared to median. Finally, β_1 of The Sandbox shows similar pattern with β_3 of the overall NFT market, which implies decrease in magnitude as τ moves up.

For further investigation, we report the Granger non-causality test results in



(a) Overall NFT

(b) Axie Infinity

(c) Decentraland

(d) The Sandbox

Figure 4.3: QR and OLS estimates for the causal effects of NFT volume on return

quantiles for 13 different quantile intervals. Table 4.4 reports the sup-Wald test results for Granger non-causality in these quantile ranges. The results show that for the interval $\tau \in [0.05, 0.95]$, there exist a strong causal relationship in the overall NFT market, Axie Infinity and The Sandbox. Overall NFT market has shown the existence of significant Granger causality in most of the quantiles, except the quantiles around the median. We can also confirm that the test statistics grow larger in the tail, implying that NFT volume can be a good predictor of returns in extreme market conditions. For Axie Infininty, strong causality is shown in every quantiles, indicating that the trading volume of Axie Infininty is useful in forecasting the log return of Axie Infininty NFTs. Decentraland showed a different behavior from others, as it only exhibits a causal relationship around the median. This suggests that under extreme market conditions, the trading volume of Decentraland NFTs does not transmit valuable information in predicting the return. Finally during the bearish market condition (lower quantiles), there is a causal relationship from The Sandbox NFT volume to The Sandbox NFT return.

We conclude that the difference in the return-volume causal relationships betwen Axie Infinity, Decentraland and The Sandbox comes from their different NFT characteristics. As NFTs in Axie Infinity are mostly game items, they are traded frequently in all of the quantiles. As a result, there exist a significant causal relationship in every quantiles. However, the NFTs in Decentraland and The Sandbox are mainly the LAND tokens, which proves the ownership of virtual land. Due to the fact that these LAND tokens are not traded frequently compared to the NFTs in Axie Infinity, the frequency of significant return-volume causal relationship is relatively low.

Table 4.4: The sup-Wald test results for Granger non-causality in diffrent quantile ranges: NFT volume to NFT return.

	Overall	Axie Infinity	Decentraland	The Sandbox
$[a,b]$	$\beta_1(\tau)=\beta_2(\tau)=\beta_3(\tau)=0$	$\beta_1(\tau)=\beta_2(\tau)=0$	$\beta_1(\tau)=\beta_2(\tau)=0$	$\beta_1(\tau)=0$
$[0.05, 0.95]$	59.5034^{***}	347.0823^{***}	6.3488	52.0135^{***}
$[0.05, 0.5]$	59.5034^{***}	347.0823^{***}	6.3488	52.0135^{***}
$[0.5, 0.95]$	18.4365^{***}	220.3025^{***}	6.129	11.2376^{**}
$[0.05, 0.1]$	59.5034^{***}	347.0823^{***}	5.5473^{*}	10.1485^{***}
$[0.1, 0.2]$	54.1248^{***}	208.7984^{***}	3.4666	51.7666^{***}
$[0.2, 0.3]$	27.6963^{***}	129.9591^{***}	2.158	52.0135^{***}
$[0.3, 0.4]$	24.4081^{***}	65.3337^{***}	4.0169	45.6814^{***}
$[0.4, 0.5]$	11.8158^{**}	29.2621^{***}	6.3488^{**}	21.9004^{***}
$[0.5, 0.6]$	5.6666	21.4458^{***}	6.129^{**}	11.2376^{***}
$[0.6, 0.7]$	4.6809	52.0911^{***}	3.9021	5.3671^{*}
$[0.7, 0.8]$	6.3897	95.4597^{***}	3.0527	4.6104^{*}
$[0.8, 0.9]$	18.4365^{***}	131.2367^{***}	3.6524	0.6282
$[0.9, 0.95]$	16.4348^{***}	220.3025^{***}	3.44	0.6066

4.3.2 Causal effects of NFT return on volume

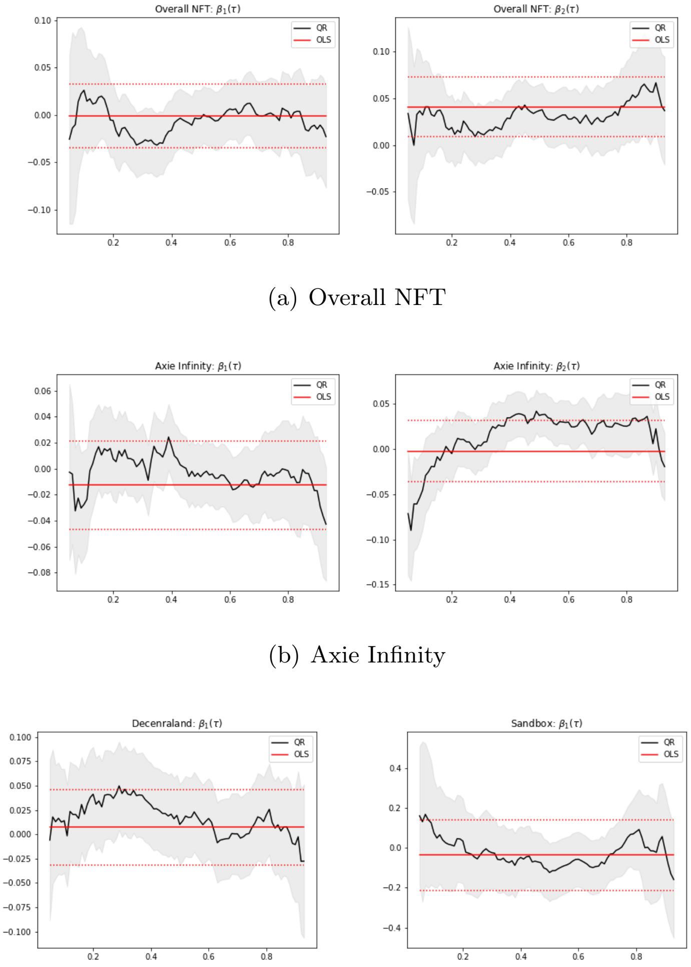
To see if there exist a bi-directional causality between NFT return and volume, we now consider the following models:

$$\ln v_t = a(\tau) + b(\tau)\frac{t}{T} + c(\tau)\left(\frac{t}{T}\right)^2 + \sum_{j=1}^{q} \alpha_j(\tau)\ln v_{t-j} + \sum_{j=1}^{q} \beta_j(\tau) r_{t-j} + e_t \quad (4.12)$$

Similar to 4.3.1, we first choose the approximate lag order q^* for each regression model. The selected lag orders are $q^* = 2$ for the overall NFTs, $q^* = 2$ for Axie Infinity, $q^* = 1$ for Decentraland and $q^* = 1$ for the Sandbox. We first plot the LS and QR estimates of $\beta_j(\tau)$ for each regression model for different quantiles $\tau \in [0.05, 0.95]$ in Figure 4.4. We can find that the OLS estimates for most of the models are around zero, which implies that there is not a significant causality from return to log volume around the mean. The QR estimates are also comparably consistent except for $\beta_2(\tau)$ of Axie Infinity, confirming that the causality effect is fairly small compared to the opposite direction (return → volume). We also report the sup-Wald statistics of the Granger non-causality test for 13 different quantiles. The results are described in Table 4.5. It shows that for all of the NFT assets, there are no signs of significant Granger causality in all 13 quantiles. This is in line with the results of Figure 4.4. To summarize, from our results, we can find that the causality between log volume and return is one-directional, as the log volume only significantly Granger causes the return. Thus, we confirm that the log volume precedes the return, so the log volume can play a role as a signal for the extreme returns afterward.

Table 4.5: The sup-Wald test results for Granger non-causality in diffrent quantile ranges: NFT return to NFT log volume.

	Overall	Axie Infinity	Decentraland	The Sandbox
$[a, b]$	$\beta_1(\tau) = \beta_2(\tau) = 0$	$\beta_1(\tau) = \beta_2(\tau) = 0$	$\beta_1(\tau) = 0$	$\beta_1(\tau) = 0$
$[0.05, 0.95]$	5.7281	8.4144	4.4529	2.9109
$[0.05, 0.5]$	5.7281	8.4144	4.4529	2.9076
$[0.5, 0.95]$	4.9523	7.4672	1.3428	2.9109
$[0.05, 0.1]$	1.1155	7.9433*	0.8673	0.9583
$[0.1, 0.2]$	2.3366	2.5535	2.4313	0.3094
$[0.2, 0.3]$	3.0482	0.6243	4.4529	0.3172
$[0.3, 0.4]$	4.2168	4.2888	4.3444	1.1588
$[0.4, 0.5]$	5.7281	8.4144*	1.9843	2.9076
$[0.5, 0.6]$	4.0852	7.4672*	1.3248	2.9109
$[0.6, 0.7]$	2.1308	5.6429	0.598	2.2854
$[0.7, 0.8]$	2.5202	3.9716	0.7451	0.8416
$[0.8, 0.9]$	4.9523	3.955	1.3227	0.9422
$[0.9, 0.95]$	3.4136	2.1389	0.7218	2.421



(a) Overall NFT

(b) Axie Infinity

(c) Decentraland

(d) The Sandbox

Figure 4.4: QR and OLS estimates for the causal effects of NFT return on log volume

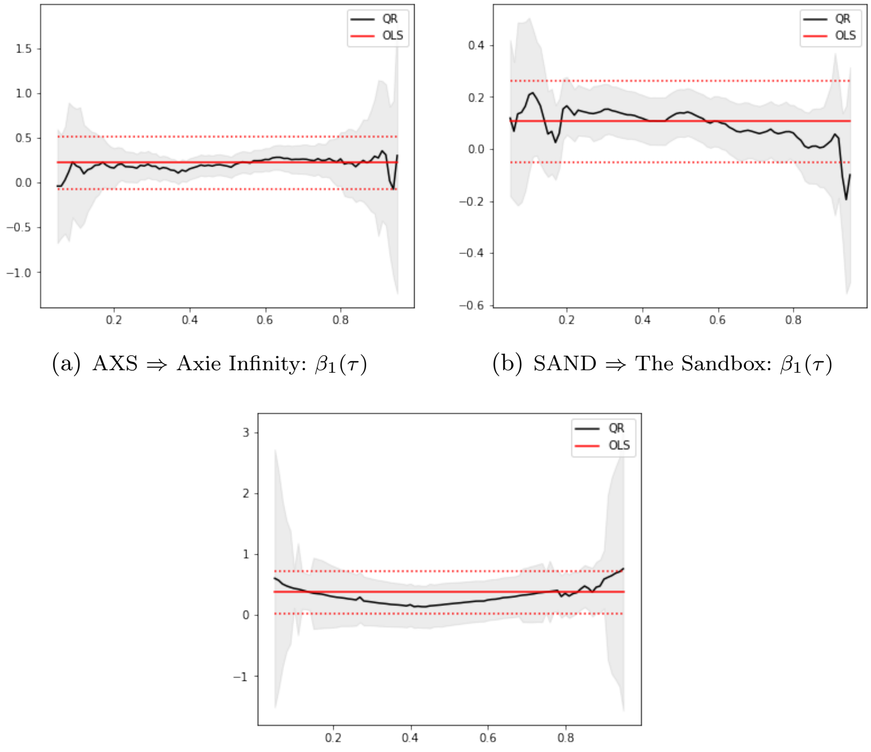
4.3.3 Causal effects between NFTs and their native cryptocurrencies

We now investigate the causal relationship between NFTs and their corresponding native cryptocurrencies. In order to do so, we selected 3 NFT service platforms which also provide their own fungible tokens to facilitate the transactions and purchases in their own ecosystems: Axie Infinity-AXS, Decentraland-MANA, and The Sandbox-SAND. For each pair, we apply the Granger causality test in quantiles between daily NFT returns and their fungible token returns. Similar to the previous section, we fitted the quantile regression models and performed the sup-Wald test to check if the fitted $\beta(\tau)$ rejects the null hypothesis (4.6). Only the results for setting the NFT return as predictor were reported, because the opposite (NFT $\Rightarrow$ cryptocurrency) did not show any significant causality effect. For Axie Infinifty and AXS, the sup-Wald statistic for $\beta_2(\tau)$ in lag-2 model is 5.943 (which is statistically insignificant) and the sup-Wald statistic for $\beta_1(\tau)$ in lag-1 model is 17.189 (significant at 1% level), so lag 1 was chosen for our model. The Sandbox and SAND also showed similar results, so lag-1 was chosen ($\beta_1(\tau)$: 10.16 which is significant at 5% level, $\beta_2(\tau)$: 3.764). On the other hand, the sup-Wald test for Decentraland and MANA did not exhibit any Granger causality at all, so we reported the results for the lag-1 model.

Similar to Figure 4.3, Figure 4.5 shows the QR and OLS coefficients of the NFT return - cryptocurrency return regression model. For every assets, the OLS estimates confirm that there is a positive causality in mean at lag 1 as the coefficients are above zero. The QR estimates show a similar pattern, as most of the coefficients are greater than zero, implying that the cryptocurrency prices are positively correlated with NFT prices regardless of the market conditions. One noticeable difference is that on the upper quantiles of The Sandbox, the coefficient drasticalyl decreases to negative value. Similar to the result of Figure 4.3, the QR estimates for Decentraland have larger magnitude at both lower and upper tails, compared to median.

Table 4.6 summarizes the sup-Wald test results for identifying the non-Granger causality in 13 different quantiles. The results show that for the interval $\tau \in [0.05, 0.95]$, there exist a significant Granger causality from AXS return to Axie Infinity NFT return and SAND return to The Sandbox NFT return. As we were not able to spot any causal relationships from any of the NFTs to cryptocurrency returns, the test results exhibit an unidirectional causal relationship from AXS to Axie Infinity and SAND markets to The Sandbox NFT markets. These findings are quite different from the previous results of Dowling [2022b], as the study suggests that in terms of volatility spillover, NFT pricing is distinct from the cryptocurrency pricing. Our results suggest that even though NFT prices are not related with Bitcoin or Ethereum, they can have causal relationships with the cryptocurrencies from the same blockchain.

To go further, we analyzed the causality effects for 10 smaller quantile intervals. For Axie Infinity, there exist strong causal relationships in the center and upper quantiles. The Sandbox shows significant causalities in the center and lower quantiles. Interestingly, these results are quite different from the causal relationships between cryptocurrencies, as cryptocurrencies have strong causal relationships in the tails (Kim et al. [2021]), rather than around the median. On the other hand, Decentraland has been found to have the weakest relationship with MANA, only showing causal relationship on the lower tails.



(a) AXS ⇒ Axie Infinity: $\beta_1(\tau)$

(b) SAND ⇒ The Sandbox: $\beta_1(\tau)$

(c) MANA ⇒ Decentraland: $\beta_1(\tau)$

Figure 4.5: QR and OLS estimates for the causal effects of cryptocurrency return on NFT return

Table 4.6: The sup-Wald test results for Granger non-causality in diffrent quantile ranges: Cryptocurrencies to NFTs.

	AXS ⇒ Axie Infinity	SAND ⇒ The Sandbox	MANA ⇒ Decentraland
$[a, b]$	$\beta_1(\tau) = 0$ [1]	$\beta_1(\tau) = 0$ [1]	$\beta_1(\tau) = 0$ [1]
$[0.05, 0.95]$	17.189***	10.162**	7.386
$[0.05, 0.5]$	11.904***	10.07**	7.143*
$[0.5, 0.95]$	17.189***	10.162**	7.386*
$[0.05, 0.1]$	0.614	1.893	7.115**
$[0.1, 0.2]$	2.645	8.554**	7.143**
$[0.2, 0.3]$	7.634**	9.796***	1.537
$[0.3, 0.4]$	6.969	10.07***	1.347
$[0.4, 0.5]$	11.904***	8.535**	1.054
$[0.5, 0.6]$	16.458***	10.162***	2.156
$[0.6, 0.7]$	17.189***	4.519*	3.408
$[0.7, 0.8]$	10.008***	1.91	5.601*
$[0.8, 0.9]$	3.08	0.95	7.386**
$[0.9, 0.95]$	1.126	1.125	5.938*

Notes. Each entry is a sup-wald test statistic for the null hypothesis that there are no Granger causality between two time series. A ⇒ B denotes the Granger causality from A to B. () denotes the selected lag order for the quantile regression model. *, **, and *** each represents the statistical significance at 10%, 5%, and 1% level respectively.

4.4 Chapter Summary

In this chapter, we focus on investigating the causality for return-volume nexus of NFTs i.e. Overall NFT, Axie Infinity, Decentraland, The Sandbox. The NFTs are selected in terms of market capitalization of their native cryptocurrencies, and the data was collected from Jan 1, 2018 to Mar 30, 2022. Using the Granger causality test in quantiles, we reveal the existence of strong causal relationships between trading volume and log return of NFTs at extreme market conditions. This result implies that there is an asymmetric causality of trading volume with returns depending on the market conditions. Then, we also examine the relationship between NFTs and their corresponding in-protocol cryptocurrencies. Empirical results show that the price of cryptocurrencies can help in predicting the NFT prices. For future work, we can also examine the causality in different quantiles between NFTs and traditional assets or macroeconomic variables, to investigate the causal relationship between the traditional finance markets and the emerging NFT markets. Also, we can investigate the connectedness between the NFT markets in order to capture the co-movement in the NFT prices or volumes.

Chapter 5

Conclusion

5.1 Contributions of the Dissertation

This dissertation provides an in-depth analysis for three promising assets in the DeFi market. For CBDCs, we propose a blockchain-based CBDC settlement model using cross-chain atomic swaps and lattice-based sequential aggregate signature scheme. Our proposed model attempts to resolve two challenging issues in designing the CBDC architecture: implementation of authorized auditor and cross-chain swap environment. For stablecoins, we quantify the connectedness and information transmission among the stablecoin and cryptocurrency market to confirm that the fall of stablecoin generates significant shocks to the overall cryptocurrency market. As a result, we conclude that adopting CBDC as a substitution for the current stablecoins can mitigate the financial risks of them. For NFTs, we the return-volume causal relationships in the NFT markets are analyzed, as the transaction volume of NFTs can be low compared to the original cryptocurrency markets.

In order to reflect the growing needs for stable and reliable digital currencies, we propose a blockchain-based CBDC settlement model which addresses two fundamental challenges in CBDC design. First, the need for authorized auditor is considered in our model by introducing the administrator ledger to the settlement system. Since

CBDC architectures are essentially different from the current fully decentralized cryptocurrencies, the auditability functionality is crucial. Central banks should be able to track the transaction records and match the identity of transaction participants, in order to meet regulatory compliance. Therefore, we add an administrator ledger to our CBDC system and let the administrator node to participate in every transactions. This new functionality has two advantages: (1) For settling two different assets on different ledgers, it is hard to match the full transaction together, as the parts of transactions are executed in different ledgers. However, the administrator ledger can record the full transaction history for every transactions, greatly enhancing the auditability of the blockchain-based settlement system. (2) In our model, the administrator node should always participate in the transaction signing process. Thus, if a transaction with malicious behavior is detected, the administrator node can halt the transaction by not signing on the contract. Also, cross-border payments for CBDCs can easily implemented by extending our model. Our model is based on the cross-chain atomic swap technology with hashed timelock contract, so when these functionalities are guaranteed in different CBDCs, they can easily develop the cross-border payment system by extending our model. Additionally, we propose a lattice-based sequential aggregate signature scheme for our model. Lattice-based cryptography is gaining greater attention now-days, as it is generally known to be resistant to quantum computer attacks. By introducing the latticed-based signature schemes, our model can still guarantee safety in the future when quantum computers become widespread.

For the stablecoins backed with its own protocol's native tokens, the likelihood of death spiral is significantly high as the success of the protocol is directly related to the price stability of stablecoin. Therefore, public distrust on the corresponding blockchain protocol can directly lead to dramatic crash of the stablecoin. However, during the normal stable market conditions, the impact of stablecoin to the cryptocurrency market cannot be measured as the price of stablecoin remains fairly stable. Therefore we focus on the crash period where the price of stablecoin shows large fluctuations. In order to quantify this impact, we dissect the recent Terra-Luna crash by using econometric methodologies such as the spillover index and effective transfer entropy. We use the hourly and 5-minute cryptocurrency prices, Google Trends index and tweets posted on StockTwits for our empirical analysis. With the collected data, we quantify the spillover effect using the spillover index methodology for both the return and volatility of the cryptocurrencies. For the spillover index based on the rolling-window framework, our results confirm that the spillover effect of the stablecoin (UST) rapidly increases as the depeg started. Consequently, its native token LUNA also showed positive net spillover index during the crash, implying that it gained influence in the overall cryptocurrency market. For the effective transfer entropy, we confirm that the interlinkages between the cryptocurrencies become stronger during the crash, as the effective transfer entropy from LUNA to other cryptocurrencies such as BTC and ETH increased dramatically. On the other hand, one interesting point is that the investor sentiment loses its role as a information transmitter during the crash. This can be confirmed by the change in effective transfer entropy from the investor sentiment to LUNA, since there was a significant information flow before the crash and it disappears after the crash began. We conclude that the keen collusion between bearish and bullish opinions about the future of LUNA led to the market sentiment losing its influence as a information transmitter.

NFT markets are different from the traditional cryptocurrency markets, because of its uniqueness. As a result, every individual NFT is traded one by one, and finding the right seller and buyer pair can be challenging. Therefore, the trading volume of NFTs should be analyzed together with their prices. To do so, we examine the causal relationship between NFT return and NFT volume by using the Granger causality test in quantiles. Our data includes daily transaction volume and price of NFTs. Our results confirm that the causality from overall NFT volume to return becomes stronger in extreme market conditions. Individual NFT projects showed somewhat different behavior. For Axie Infinity, strong causality was prevalent in every quantiles. Decentraland only showed a causal relationship around the median. On the other hand, the transaction volume of The Sandbox helps forecasting The Sandbox prices only during the bearish markets conditions. Additionally, we address the relationship between NFT returns and the return of its in-protocol native cryptocurrencies. Our empirical analysis show that there exist a strong causal relationship between these two.

This dissertation has shed light on the various kinds of emerging digital assets. We first developed blockchain-based CBDC model to overcome the current obstacles in both traditional and decentralized financial markets. We believe that blockchain-based CBDC can play a vital role in the DeFi markets, since it provides minimum risk in formulating trading strategies with stablecoins for the investors. The econometric analysis on stablecoin death spiral confirm the signifcant impact of the stablecoin to the overall cryptocurrency and DeFi markets. Empirical results show that the depeg of stablecoin have potential to shake up the entire market. Finally, we confirmed the return-volume causal relationships in the NFT markets, to provide guidance to

NFT investors in different market conditions.

5.2 Future Works

Several limitation of the dissertation should be addressed in future work. First, the econometric analysis only considers the cryptocurrency market itself. For a richer understanding on the interlinkages between stablecoins and overall financial markets including the traditional one, studies on measuring the connectedness between stablecoins, traditional assets and even macroeconomic factors can be accomplished. Also, a wider range of stablecoin and NFTs can be used for further research. For the proposed CBDC model, the analysis on the proposed model can be enriched by incorporating the liquidity savings mechanisms. We believe that liqudity-savings mechanism accompanied by privacy-preserving techniques can provide practicality to our model.

Bibliography

Hayden Adams, Noah Zinsmeister, Moody Salem, River Keefer, and Dan Robinson. Uniswap v3 core. *Tech. rep., Uniswap, Tech. Rep.*, 2021.

Miklós Ajtai. Generating hard instances of lattice problems. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 99–108, 1996.

Mustafa Al-Bassam, Alberto Sonnino, Shehar Bano, Dave Hrycyszyn, and George Danezis. Chainspace: A sharded smart contracts platform. *arXiv preprint arXiv:1708.03778*, August 2017.

Sarah Allen, Srjan Čapkun, Ittay Eyal, Giulia Fanti, Bryan A Ford, James Grimmelmann, Ari Juels, Kari Kostiainen, Sarah Meiklejohn, Andrew Miller, et al. Design choices for central bank digital currency: Policy and technical considerations. Technical report, National Bureau of Economic Research, August 2020.

Enis Ceyhun Alp, Eleftherios Kokoris-Kogias, Georgia Fragkouli, and Bryan Ford. Rethinking general-purpose decentralized computing. In *Proc. of the Workshop on Hot Topics in Operating Systems (HotOS'19), Bertinoro, Italy*, pages 105–112. ACM, May 2019.

Donald WK Andrews. Tests for parameter instability and structural change with unknown change point. *Econometrica: Journal of the Econometric Society*, pages 821–856, 1993.

Elli Androulaki, Jan Camenisch, Angelo De Caro, Maria Dubovitskaya, Kaoutar Elkhiyaoui, and Björn Tackmann. Privacy-preserving auditable token payments in a permissioned blockchain system. In *Proc. of the 2nd ACM Conference on Advances in Financial Technologies (AFT'20), New York, NY, USA*, pages 255–267. ACM, October 2020.

Lennart Ante. The non-fungible token (nft) market and its relationship with bitcoin and ethereum. *FinTech*, 1(3):216–224, 2022.

Nektarios Aslanidis, Aurelio F Bariviera, and Alejandro Perez-Laborda. Are cryptocurrencies becoming more interconnected? *Economics Letters*, 199:109725, 2021.

Nektarios Aslanidis, Aurelio F Bariviera, and Óscar G López. The link between cryptocurrencies and google trends attention. *Finance Research Letters*, page 102654, 2022.

Ata Assaf, Husni Charif, and Ender Demir. Information sharing among cryptocurrencies: Evidence from mutual information and approximate entropy during covid-19. *Finance Research Letters*, 47:102556, 2022.

Shahla Atapoor, Nigel P. Smart, and Younes Talibi Alaoui. Private liquidity matching using mpc. Cryptology ePrint Archive, Report 2021/475, 2021. https://eprint.iacr.org/2021/475.

Raphael Auer and Rainer Böhme. The technology of retail central bank digital currency. *BIS Quarterly Review, March*, March 2020.

Raphael Auer, Philipp Haene, and Henry Holden. Multi-cbdc arrangements and the future of cross-border payments. *BIS Papers*, (115), March 2021.

Raphael Auer, Jon Frost, Leonardo Gambacorta, Cyril Monnet, Tara Rice, and Hyun Song Shin. Central bank digital currencies: motives, economic implications, and the research frontier. *Annual review of economics*, 14:697–721, 2022.

Raphael A Auer, Giulio Cornelli, and Jon Frost. Rise of the central bank digital currencies: drivers, approaches and technologies. Technical Report 8655, CESifo Working Paper, 2020.

Shuangjie Bai, Geng Yang, Chunming Rong, Guoxiu Liu, and Hua Dai. Qhse: An efficient privacy-preserving scheme for blockchain-based transactions. *Future Generation Computer Systems*, 112:930–944, 2020.

Rushlene Kaur Bakshi, Navneet Kaur, Ravneet Kaur, and Gurpreet Kaur. Opinion mining and sentiment analysis. In *2016 3rd international conference on computing for sustainable global development (INDIACom)*, pages 452–455. IEEE, 2016.

Bank of Canada, TMX Group, Payments Canada, Accenture, R3. Jasper phase iii: Securities settlement using distributed ledgertechnology. `https://www.payments.ca/sites/default/files/jasper_phase_iii_whitepaper_final_0.pdf`, 2018. Accessed: 2020-10-10.

Mihir Bellare and Gregory Neven. Multi-signatures in the plain public-key model and a general forking lemma. In *Proceedings of the 13th ACM conference on Computer and communications security*, pages 390–399, 2006.

Evangelos Benos, Rod Garratt, and Pedro Gurrola-Perez. The economics of distributed ledger technology for securities settlement. *Available at SSRN 3023779*, 2017.

Bruno Biais, Christophe Bisiere, Matthieu Bouvard, and Catherine Casamatta. The blockchain folk theorem. *The Review of Financial Studies*, 32(5):1662–1715, 2019.

bitcoinwiki. Hashed timelock contracts. `https://en.bitcoin.it/wiki/hashed_Timelock_Contracts.`, 2019. Accessed: 2021-01-18.

Ole Bjerg. Designing new money-the policy trilemma of central bank digital currency. June 2017.

Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pages 329–349. October 2019.

Codruta Boar, Henry Holden, and Amber Wadsworth. Impending arrival–a sequel to the survey on central bank digital currency. *BIS paper*, (107), February 2020.

Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 416–432. Springer, 2003.

TH Bontekoe. Balancing privacy and accountability in digital payment methods using zk-snarks. Master's thesis, University of Twente, 2020.

Michael D Bordo and Andrew T Levin. Central bank digital currency and the future of monetary policy. Technical report, National Bureau of Economic Research, August 2017.

Nicola Borri and Kirill Shakhnov. Regulation spillovers across cryptocurrency markets. *Finance Research Letters*, 36:101333, 2020.

Elie Bouri, Syed Jawad Hussain Shahzad, and David Roubaud. Co-explosivity in the cryptocurrency market. *Finance Research Letters*, 29:178–183, 2019.

Elie Bouri, Tareq Saeed, Xuan Vinh Vo, and David Roubaud. Quantile connectedness in the cryptocurrency market. *Journal of International Financial Markets, Institutions and Money*, 71:101302, 2021.

Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. *white paper*, 3(37), 2014.

George Calle and Daniel Eidan. Central bank digital currency: an innovation in payments. *R3 White Paper, April*, 2020.

Jan Camenisch, Susan Hohenberger, and Anna Lysyanskaya. Balancing accountability and privacy using e-cash. In *International Conference on Security and Cryptography for Networks*, pages 141–155. Springer, September 2006.

Christian Catalini and Alonso de Gortari. On the economic design of stablecoins. *Available at SSRN 3899499*, 2021.

Christian Catalini, Alonso de Gortari, and Nihar Shah. Some simple economics of stablecoins. 2021.

David Chaum. Blind signatures for untraceable payments. In *Advances in cryptology*, pages 199–203. Springer, 1983.

David Chaum, Christian Grothoff, and Thomas Moser. How to issue a central bank digital currency. *arXiv preprint arXiv:2103.00254*, February 2021.

Gong-meng Chen, Michael Firth, and Oliver M Rui. The dynamic relation between stock returns, trading volume, and volatility. *Financial Review*, 36(3):153–174, 2001.

Hao Chen, Ilaria Chillotti, and Yongsoo Song. Multi-key homomorphic encryption from tfhe. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 446–472. Springer, November 2019.

Jing Chen and Silvio Micali. Algorand. *arXiv preprint arXiv:1607.01341*, 2016.

Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachene. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 3–33. Springer, November 2016.

Jonathan Chiu and Thorsten V Koeppl. Blockchain-based settlement for asset trading. *The Review of Financial Studies*, 32(5):1716–1753, 2019.

Chia-Chang Chuang, Chung-Ming Kuan, and Hsin-Yi Lin. Causality in quantiles and dynamic stock return–volume relations. *Journal of Banking & Finance*, 33 (7):1351–1360, 2009.

Alexis Collomb and Klara Sok. Blockchain/distributed ledger technology (dlt): What impact on the financial sector? *Digiworld Economic Journal*, (103), 2016.

CPMI & Markets Committee et al. Central bank digital currencies. *Committee on Payments and Market Infrastructures, Bank for International Settlements, March*, 2018.

Filecoin community. Filecoin: A cryptocurrency operated file storage network, Oct 2014. URL `http://filecoin.io/filecoin.pdf`. Accessed: 2014-10-14.

Shaen Corbet, Andrew Meegan, Charles Larkin, Brian Lucey, and Larisa Yarovaya. Exploring the dynamic relationships between cryptocurrencies and other financial assets. *Economics Letters*, 165:28–34, 2018.

Shaen Corbet, John W Goodell, and Samet Günay. What drives defi prices? investigating the effects of investor attention. *Finance Research Letters*, 48:102883, 2022.

Wenhao Dai, Xiaozhuo Gu, and Yajun Teng. A supervised anonymous issuance scheme of central bank digital currency based on blockchain. In *International Conference on Algorithms and Architectures for Parallel Processing*, pages 475–493. Springer, September 2020.

George Danezis and Sarah Meiklejohn. Centrally banked cryptocurrencies. *arXiv preprint arXiv:1505.06895*, May 2015.

Sriram Darbha and Rakesh Arora. Privacy in cbdc technology. Technical report, Bank of Canada, June 2020.

Ender Demir, Serdar Simonyan, Conrado-Diego García-Gómez, and Chi Keung Marco Lau. The asymmetric effect of bitcoin on altcoins: evidence from the nonlinear autoregressive distributed lag (nardl) model. *Finance Research Letters*, 40:101754, 2021.

Sercan Demiralay and Petros Golitsis. On the dynamic equicorrelations in cryptocurrency market. *The Quarterly Review of Economics and Finance*, 80:524–533, 2021.

Johan Devriese and Janet Mitchell. Liquidity risk in securities settlement. *Journal of Banking & Finance*, 30(6):1807–1834, 2006.

Francis X Diebold and Kamil Yilmaz. Measuring financial asset return and volatility spillovers, with application to global equity markets. *The Economic Journal*, 119 (534):158–171, 2009.

Francis X Diebold and Kamil Yilmaz. Better to give than to receive: Predictive directional measurement of volatility spillovers. *International Journal of forecasting*, 28(1):57–66, 2012.

Michael Dowling. Fertile land: Pricing non-fungible tokens. *Finance Research Letters*, 44:102096, 2022a.

Michael Dowling. Is non-fungible token pricing driven by cryptocurrencies? *Finance Research Letters*, 44:102097, 2022b.

Léo Ducas, Alain Durmus, Tancrède Lepoint, and Vadim Lyubashevsky. Lattice signatures and bimodal gaussians. In *Annual Cryptology Conference*, pages 40–56. Springer, 2013.

Michael Egorov. Stableswap-efficient mechanism for stablecoin liquidity. *Retrieved Feb*, 24:2021, 2019.

Rachid El Bansarkhani and Johannes Buchmann. Towards lattice based aggregate signatures. In *International Conference on Cryptology in Africa*, pages 336–355. Springer, 2014.

European Central Bank, Bank of Japan. Stella: Securities settlement systems: delivery-versus-payment in a distributed ledger environment. `https://www.boj.or.jp/en/announcements/release_2018/data/rel180327a1.pdf`, 2018. Accessed: 2021-02-25.

European Central Bank, Bank of Japan. Synchronised cross-border payments - stella project report phase 3. `https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical190604.en.pdf`, June 2019.

Qi Feng, Debiao He, Sherali Zeadally, Muhammad Khurram Khan, and Neeraj Kumar. A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*, 126:45–58, Januray 2019.

Panos Fousekis and Dimitra Tzaferi. Returns and volume: Frequency connectedness in cryptocurrency markets. *Economic Modelling*, 95:13–20, 2021.

A Ronald Gallant, Peter E Rossi, and George Tauchen. Stock prices and volume. *The Review of Financial Studies*, 5(2):199–242, 1992.

Yu-Long Gao, Xiu-Bo Chen, Yu-Ling Chen, Ying Sun, Xin-Xin Niu, and Yi-Xian Yang. A secure cryptocurrency scheme based on post-quantum blockchain. *IEEE Access*, 6:27205–27213, 2018.

Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol:

Analysis and applications. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 281–310. Springer, 2015.

Christina Garman, Matthew Green, and Ian Miers. Accountable privacy for decentralized anonymous payments. In *International Conference on Financial Cryptography and Data Security*, pages 81–98. Springer, May 2016.

Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 197–206, 2008.

Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game, or a completeness theorem for protocols with honest majority. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pages 307–328. Morgan & Claypool, October 2019.

Geoffrey Goodell, Hazem Danny Al-Nakib, and Paolo Tasca. A digital currency architecture for privacy and owner-custodianship. *Future Internet*, 13(5):130, May 2021.

Clive WJ Granger. Investigating causal relations by econometric models and cross-spectral methods. *Econometrica: journal of the Econometric Society*, pages 424–438, 1969.

Jonas Gross, Johannes Sedlmeir, Matthias Babel, Alexander Bechtel, and Benjamin Schellinger. Designing a central bank digital currency with support for cash-like privacy. *Available at SSRN 3891121*, July 2021.

Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.

Xuan Han, Yong Yuan, and Fei-Yue Wang. A blockchain-based framework for central bank digital currency. In *Proc. of the 2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Zhengzhou, China*, pages 263–268. IEEE, November 2019.

Maurice Herlihy. Blockchains and the future of distributed computing. In *Proceedings of the ACM Symposium on Principles of Distributed Computing*, pages 155–155, 2017.

Maurice Herlihy. Atomic cross-chain swaps. In *Proceedings of the 2018 ACM symposium on principles of distributed computing*, pages 245–254, 2018.

Daira Hopwood, Sean Bowe, Taylor Hornby, and Nathan Wilcox. Zcash protocol specification. *GitHub: San Francisco, CA, USA*, October 2016.

Qiang Ji, Elie Bouri, Chi Keung Marco Lau, and David Roubaud. Dynamic connectedness and integration in cryptocurrency markets. *International Review of Financial Analysis*, 63:257–272, 2019.

Harry Kalodner, Steven Goldfeder, Xiaoqi Chen, S Matthew Weinberg, and Edward W Felten. Arbitrum: Scalable, private smart contracts. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 1353–1370. USENIX Association, August 2018.

George Kappos, Haaroon Yousaf, Mary Maller, and Sarah Meiklejohn. An empirical analysis of anonymity in zcash. In *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pages 463–477. USENIX Association, August 2018.

Paraskevi Katsiampa. Volatility co-movement between bitcoin and ether. *Finance Research Letters*, 30:221–227, 2019.

Evan Kereiakes, Marco Di Maggio Do Kwon, and Nicholas Platias. Terra money: Stability and adoption. *White Paper, Apr*, 2019.

Mariana Khapko and Marius Zoican. How fast should trades settle? *Management Science*, 66(10):4573–4593, 2020.

Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol, 2016. URL `https://pdfs.semanticscholar.org/a583/3270b14e251f0b16d86438d04652b1b8d7f3.pdf`. Accessed: 2018-08-19.

Myeong Jun Kim, Nguyen Phuc Canh, and Sung Y Park. Causal relationship among cryptocurrencies: A conditional quantile approach. *Finance Research Letters*, 42: 101879, 2021.

Shee-Ihn Kim and Seung-Hee Kim. E-commerce payment model using blockchain. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–13, 2020.

Roger Koenker and Gilbert Bassett Jr. Regression quantiles. *Econometrica: journal of the Econometric Society*, pages 33–50, 1978.

Roger Koenker and Kevin F Hallock. Quantile regression. *Journal of economic perspectives*, 15(4):143–156, 2001.

Roger Koenker and Jose AF Machado. Goodness of fit and related inference processes for quantile regression. *Journal of the american statistical association*, 94(448): 1296–1310, 1999.

Eleftherios Kokoris Kogias. Secure, confidential blockchains providing high throughput and low latency. Technical report, EPFL, 2019.

Gary Koop, M Hashem Pesaran, and Simon M Potter. Impulse response analysis in nonlinear multivariate models. *Journal of econometrics*, 74(1):119–147, 1996.

Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *Proc. of the 2016 IEEE symposium on security and privacy (SP), San Jose, CA, USA*, pages 839–858. IEEE, May 2016.

Philip Koshy, Diana Koshy, and Patrick McDaniel. An analysis of anonymity in bitcoin using p2p network traffic. In *International Conference on Financial Cryptography and Data Security*, pages 469–485. Springer, November 2014.

Olivier Kraaijeveld and Johannes De Smedt. The predictive power of public twitter sentiment for forecasting cryptocurrency prices. *Journal of International Financial Markets, Institutions and Money*, 65:101188, 2020.

Randall S Kroszner et al. Central counterparty clearing: History, innovation, and regulation. *Economic Perspectives-Federal Reserve Bank Of Chicago*, 30(4):37, 2006.

Michael Kumhof and Clare Noone. Central bank digital currencies-design principles and balance sheet implications. May 2018.

Bahareh Lashkari and Petr Musilek. A comprehensive review of blockchain consensus mechanisms. *IEEE Access*, 9:43620–43652, 2021.

Bong-Soo Lee and Oliver M Rui. The dynamic relationship between stock returns and trading volume: Domestic and cross-country evidence. *Journal of Banking & Finance*, 26(1):51–78, 2002.

Charles Lee. Litecoin (2011), 2011.

Seungju Lee, Jaewook Lee, and Yunyoung Lee. Dissecting the terra-luna crash: Evidence from the spillover effect and information flow. *Finance Research Letters*, page 103590, 2022.

Yunyoung Lee. *Blockchain-Based Settlement System Using Cross-Chain Atomic Swaps.* PhD thesis, The Graduate School, Seoul National University, 2020.

Yunyoung Lee, Bumho Son, Huisu Jang, Junyoung Byun, Taeho Yoon, and Jaewook Lee. Atomic cross-chain settlement model for central banks digital currency. *Information Sciences*, 580:838–856, 2021a.

Yunyoung Lee, Bumho Son, Seongwan Park, Jaewook Lee, and Huisu Jang. A survey on security and privacy in blockchain-based central bank digital currencies. *J. Internet Serv. Inf. Secur.*, 11(3):16–29, 2021b.

Chao-Yang Li, Xiu-Bo Chen, Yu-Ling Chen, Yan-Yan Hou, and Jian Li. A new lattice-based signature scheme in post-quantum blockchain network. *IEEE Access*, 7:2026–2033, 2018.

Chaoyang Li, Yuan Tian, Xiubo Chen, and Jian Li. An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems. *Information Sciences*, 546: 253–264, 2021.

Alexander Lipton, Aetienne Sardon, Fabian Schär, and Christian Schüpbach. From tether to libra: Stablecoins, digital currency and the future of money. *arXiv preprint arXiv:2005.12949*, 2020.

Ziyao Liu, Nguyen Cong Luong, Wenbo Wang, Dusit Niyato, Ping Wang, Ying-Chang Liang, and Dong In Kim. A survey on applications of game theory in blockchain. *arXiv preprint arXiv:1902.10865*, 2019.

Yuen C Lo and Francesca Medda. Assets on the blockchain: An empirical study of tokenomics. *Information Economics and Policy*, 53:100881, 2020.

Adriana López-Alt, Eran Tromer, and Vinod Vaikuntanathan. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In *Pro. of the forty-fourth annual ACM symposium on Theory of computing (STOC'12), New York, New York, USA*, pages 1219–1234. ACM, May 2012.

Anna Lysyanskaya, Silvio Micali, Leonid Reyzin, and Hovav Shacham. Sequential aggregate signatures from trapdoor permutations. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 74–90. Springer, 2004.

Vadim Lyubashevsky. Lattice signatures without trapdoors. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 738–755. Springer, 2012.

Robert Marschinski and Holger Kantz. Analysing the information flow between financial time series. *The European Physical Journal B-Condensed Matter and Complex Systems*, 30(2):275–281, 2002.

MAS, SGX, Anquan Capital, Deloitt, Nasdaq. Project ubin: Delivery versus payment on distributed ledger technologies. `https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Project-Ubin-DvP-on-Distributed-Ledger-Technologies.pdf`, 2018. Accessed: 2020-09-16.

Ian Miers, Christina Garman, Matthew Green, and Aviel D Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin. In *Proc. of the 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, USA*, pages 397–411. IEEE, June 2013.

Andrew Miller, Malte Möser, Kevin Lee, and Arvind Narayanan. An empirical analysis of linkability in the monero blockchain. *arXiv preprint arXiv:1704.04299*, April 2017.

David C Mills Jr and Travis D Nesmith. Risk and concentration in payment and securities settlement systems. *Journal of Monetary Economics*, 55(3):542–553, 2008.

Du Mingxiao, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, and Chen Qijun. A review on consensus algorithm of blockchain. In *2017 IEEE international conference on systems, man, and cybernetics (SMC)*, pages 2567–2572. IEEE, 2017.

Cyrus Minwalla. Security of a cbdc. Technical report, Bank of Canada, 2020.

George Moratis. Quantifying the spillover effect in the cryptocurrency market. *Finance Research Letters*, 38:101534, 2021.

Matthieu Nadini, Laura Alessandretti, Flavio Di Giacinto, Mauro Martino, Luca Maria Aiello, and Andrea Baronchelli. Mapping the nft revolution: market trends, trade networks, and visual features. *Scientific reports*, 11(1):1–11, 2021.

Muhammad Naeem, Elie Bouri, Gideon Boako, and David Roubaud. Tail dependence in the return-volume of leading cryptocurrencies. *Finance Research Letters*, 36:101326, 2020.

Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260, 2008.

Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot, 2019.

Gregory Neven. Efficient sequential aggregate signed data. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 52–69. Springer, 2008.

Jonas David Nick. Data-driven de-anonymization in bitcoin. Master's thesis, ETH-Zürich, 2015.

Sina Rafati Niya, Florian Shüpfer, Thomas Bocek, and Bürkhard Stiller. Setting up flexible and light weight trading with enhanced user privacy using smart contracts. In *Proc. of the 2018-2018 IEEE/IFIP Network Operations and Management Symposium (NOMS), Taipei, Taiwan*, pages 1–2. IEEE, July 2018.

Shen Noether. Ring signature confidential transactions for monero. *IACR Cryptol. ePrint Arch.*, 2015:1098, December 2015.

H Hashem Pesaran and Yongcheol Shin. Generalized impulse response analysis in linear multivariate models. *Economics letters*, 58(1):17–29, 1998.

Gareth W Peters, Efstathios Panayi, and Ariane Chapelle. Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective. *arXiv preprint arXiv:1508.04364*, 2015.

Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments, 2016.

Yuwen Pu, Tao Xiang, Chunqiang Hu, Arwa Alrawais, and Hongyang Yan. An efficient blockchain-based privacy preserving scheme for vehicular social networks. *Information Sciences*, 540:308–324, 2020.

Mayank Raikwar, Danilo Gligoroski, and Katina Kralevska. Sok of used cryptography in blockchain. *IEEE Access*, 7:148550–148575, 2019.

Ronald L Rivest, Len Adleman, Michael L Dertouzos, et al. On data banks and privacy homomorphisms. *Foundations of secure computation*, 4(11):169–180, 1978.

Ronald L Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 552–565. Springer, November 2001.

Goldman Sachs. Profiles in innovation. source survey of 2000 us consumers, 2016.

Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized anonymous payments from bitcoin. In *Proc. of the 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA*, pages 459–474. IEEE, November 2014.

Thomas Schreiber. Measuring information transfer. *Physical review letters*, 85(2): 461, 2000.

Dinesh Shah, Rakesh Arora, Han Du, Sriram Darbha, John Miedema, and Cyrus Minwalla. Technology approach for a cbdc. Technical report, Bank of Canada, 2020.

Furqan Shahid, Abid Khan, Saif Ur Rehman Malik, and Kim-Kwang Raymond Choo. Wots-s: A quantum secure compact signature scheme for distributed ledger. *Information Sciences*, 539:229–249, 2020.

Dehua Shen, Andrew Urquhart, and Pengfei Wang. Does twitter predict bitcoin? *Economics Letters*, 174:118–122, 2019.

Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

Sandy Suardi, Atiqur Rahman Rasel, and Bin Liu. On the predictive power of tweet sentiments and attention on bitcoin. *International Review of Economics & Finance*, 79:289–301, 2022.

Bruce J Summers. Clearing and payment systems: The role of the central bank. *Fed. Res. Bull.*, 77:81, 1991.

He Sun, Hongliang Mao, Xiaomin Bai, Zhidong Chen, Kai Hu, and Wei Yu. Multi-blockchain model for central bank digital currency. In *2017 18th International conference on parallel and distributed computing, applications and technologies (PDCAT)*, pages 360–367. IEEE, 2017.

Alex Tapscott and Don Tapscott. How blockchain is changing finance. *Harvard Business Review*, 1(9):2–5, 2017.

Haibo Tian, Xiaofeng Chen, Yong Ding, Xiaoyan Zhu, and Fangguo Zhang. Afcoin: a framework for digital fiat currency of central banks based on account model. In *International Conference on Information Security and Cryptology*, pages 70–85. Springer, 2018.

Katrin Tinn and Christophe Dubach. Central bank digital currency with asymmetric privacy. *Available at SSRN 3787088*, February 2021.

Wei-Tek Tsai, Zihao Zhao, Chi Zhang, Lian Yu, and Enyan Deng. A multi-chain model for cbdc. In *2018 5th International Conference on Dependable Systems and Their Applications (DSA)*, pages 25–34. IEEE, 2018.

Andreas Unterweger, Fabian Knirsch, Christoph Leixnering, and Dominik Engel. Lessons learned from implementing a privacy-preserving smart contract in ethereum. In *Proc. of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France*, pages 1–5. IEEE, February 2018.

Andrew Urquhart. What causes the attention of bitcoin? *Economics Letters*, 166: 40–44, 2018.

Andreas Veneris, Andreas Park, Fan Long, and Poonam Puri. Central bank digital loonie: Canadian cash for a new global economy. *Available at SSRN 3770024*, February 2021.

Huaqun Wang, Debiao He, Kim-Kwang Raymond Choo, and Xi Chen. Blockchain-based multi-party proof of assets with privacy preservation. *Information Sciences*, 547:609–621, 2021a.

Qin Wang, Bo Qin, Jiankun Hu, and Fu Xiao. Preserving transaction privacy in bitcoin. *Future Generation Computer Systems*, 107:793–804, June 2020.

Qin Wang, Rujia Li, Qi Wang, and Shiping Chen. Non-fungible token (nft): Overview, evaluation, opportunities and challenges. *arXiv preprint arXiv:2105.07447*, 2021b.

Zhipeng Wang and Qianhong Wu. A practical lattice-based sequential aggregate signature. In *International Conference on Provable Security*, pages 94–109. Springer, 2019.

Orla Ward and Sabrina Rochemont. Understanding central bank digital currencies (cbdc). *Institute and Faculty of Actuaries*, 2019.

Wang Chun Wei. The impact of tether grants on bitcoin. *Economics Letters*, 171: 19–22, 2018.

Sam M Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William J Knottenbelt. Sok: Decentralized finance (defi). *arXiv preprint arXiv:2101.08778*, 2021.

Gavin Wood et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–32, 2014.

Chunhui Wu, Lishan Ke, and Yusong Du. Quantum resistant key-exposure free chameleon hash and applications in redactable blockchain. *Information Sciences*, 548:438–449, 2021.

Andrew C Yao. Protocols for secure computations. In *Proc. of the 23rd annual symposium on foundations of computer science (sfcs 1982), Chicago, IL, USA*, pages 160–164. IEEE, July 1982.

Q Yao. Technical aspects of cbdc in a two-tiered system. In *Proc. ITU Workshop Standardizing Digit. Fiat Currency (DFC) Appl.*, 2018.

Yanqing Yao, Zhoujun Li, and Hua Guo. A unified framework of identity-based sequential aggregate signatures from 2-level hibe schemes. *Information Sciences*, 516:505–514, 2020.

Larisa Yarovaya and Damian Zięba. Intraday volume-return nexus in cryptocurrency markets: Novel evidence from cryptocurrency classification. *Research in International Business and Finance*, 60:101592, 2022.

Shuyue Yi, Zishuang Xu, and Gang-Jin Wang. Volatility connectedness in the cryptocurrency market: Is bitcoin a dominant cryptocurrency? *International Review of Financial Analysis*, 60:98–114, 2018.

Jinnan Zhang, Rui Tian, Yanghua Cao, Xueguang Yuan, Zefeng Yu, Xin Yan, and Xia Zhang. A hybrid model for central bank digital currency based on blockchain. *IEEE Access*, 9:53589–53601, April 2021.

Tao Zhang and Zhigang Huang. Blockchain and central bank digital currency. *ICT Express*, 8(2):264–270, 2022.

Damian Zięba, Ryszard Kokoszczyński, and Katarzyna Śledziewska. Shock transmission in the cryptocurrency market. is bitcoin the most influential? *International Review of Financial Analysis*, 64:102–125, 2019.

국문초록

본 논문은 탈중앙화 금융 (DeFi) 시장에서 유망한 세 가지 자산인 중앙은행 디지털 화폐, 스테이블 코인 및 대체 불가능한 토큰에 대한 심층적인 실증분석을 제공한다. 먼저 현재 중앙은행 디지털 화폐 설계에 있어서 가장 큰 걸림돌이 되고 있는 두 가지 문제를 해결하기 위한 블록체인 기반 중앙은행 디지털 화폐 결제 시스템을 제안한다. 이 때, 크로스-체인 아토믹 스왑 기술과 격자 기반 순차적 통합 서명 (sequential aggregate signature) 기술이 함께 활용된다. 그리고 스테이블 코인 시장에 대한 심층적 이해를 위해 최근에 발생하였던 테라-루나 사태를 파급효과 지수와 효과적 전이 엔트로피를 활용하여 분석하였다. 이를 통해 스테이블코인과 암호화폐 시장 간의 연결성과 정보 전송을 정량화하였다. 그리고 대체 불가능 토큰의 경우, 대체 불가능 토큰의 특성상 기존 암호화폐에 비해 거래량이 적다는 점을 착안하여 대체 불가능 시장 내 수익률과 거래량 간의 인과관계를 분석한다.

중앙은행 디지털 화폐의 경우, 현재 중앙은행 디지털 화폐 설계의 두 가지 근본적인 과제를 해결하는 블록체인 기반 결제 시스템을 제안한다. 먼저 감사 가능성을 제공하기 위해 결제 시스템에 관리자 원장을 도입하고, 관리자 노드가 모든 거래에 참여할 수 있도록 하였다. 본 모델은 크로스 체인 아토믹 스왑과 격자 기반 순차적 통합서명을 활용하여 안전성을 보장하고 국가간 결제를 가능케한다. 또한 제안 모델은 거래 기록을 추적하고 거래 기록과 거래 참가자의 신원을 일치시킬 수 있으며, 격자 기반 암호 활용을 통해 미래의 양자 컴퓨터 공격에도 강건할 수 있다.

동일 프로토콜 내의 토큰을 준비금으로 갖는 스테이블 코인의 경우, 해당 프로토콜에 대한 대중의 신뢰가 무너진다면 데스 스파이럴에 빠질 위험이 매우 높다. 정상적인 시장 상황에서는 스테이블코인의 가격이 매우 안정적이기 때문에, 이에 대한 분석을 진

행하는 데에 어려움이 있다. 따라서, 스테이블코인의 시장 영향력을 정량화하기 위하여, 스테이블코인의 가격 변동성이 매우 심했던 최근의 테라-루나 폭락 사태를 분석하였으며 이 때, 파급효과 지수와 효과적 전이 엔트로피와 같은 계량 경제학적 방법론을 사용하였다. 분석에는 1시간 및 5분 단위 암호화폐 가격, 구글 트렌드 지수, 그리고 StockTwits에 포스팅된 트윗들을 사용하였다. 실험 결과, 디페그가 시작되면서 스테이블 코인의 파급효과가 급격하게 증가했고, 루나 코인이 전체 암호화폐 시장에서 큰 영향력을 가졌음을 확인하였다. 또한 루나에서 비트코인이나 이더리움과 같은 다른 주요 암호화폐로의 효과적 전이 엔트로피도 함께 증가하였다. 그러나 투자자 감성의 경우 루나로의 전이 엔트로피가 크게 감소함에 따라, 폭락 사태 동안 정보 송신자로서의 역할을 잃어버렸다. 이러한 현상이 일어난 이유는, 루나의 미래에 대한 투자자들의 의견이 매우 분분하여 시장 내 투자자 감성이 방향성을 잃었기 때문이라고 해석할 수 있다.

대체 불가능 토큰 시장은, 대체 불가능 토큰이 갖는 고유성이라는 특성으로 인해 기존 암호화폐 시장과는 차이점이 있다. 이에 따라 거래의 유동성이 매우 낮아지게 된다. 다시 말해, 개별 대체 불가능 토큰에 대한 적합한 매도자와 매수자를 찾는 작업이 비교적 오래 걸릴 수 있다. 이러한 특성을 알아보기 위하여 대체 불가능 토큰의 거래량과 가격 간의 인과관계를 알아보고자 하였다. 이 때, 분위수별 그레인저 인과관계 검정을 사용하였다. 데이터의 경우, 대체 불가능 토큰의 일일 거래량과 가격을 사용하였으며, 분석 결과 전반적인 대체 불가능 토큰 시장에 대해서는 극단적인 시장 상황 속에서 인과관계가 더욱 강하게 나타남을 보였다. 하지만 대체 불가능 토큰 프로젝트 별로 분석한 결과는 이와 다르게 나타났다. 예를 들어, 액시 인피니티는 모든 분위수에서 거래량과 수익률이 강한 인과관계를 가진 바면, 디센트럴랜드는 중앙값 주변에서만 인과관계를 보였다. 또한 샌드박스의 거래량은 오히려 약세장 속에서 샌드박스 가격을 예측하는 데에만 도움을 줄 수 있음을 확인하였다. 마지막으로, 대체 불가능 토큰과 해당 토큰이 존재하는 프로토콜 내 기본 암호화폐와의 인과관계를 분석하였다. 실증 실험 결과, 대체

불가능 토큰의 가격과 프로토콜 내 기본 암호화폐의 가격에는 밀접한 관계가 있으며, 대체 불가능 토큰 거래 및 투자 시에도 이러한 점을 고려해야함을 보였다.

본 논문은 블록체인 기반 중앙은행 디지털 화폐, 스테이블코인 및 대체 불가능 토큰과 같은 다양한 유형의 디지털 자산에 대한 실증분석을 진행하였다. 가장 먼저, 전통 금융시장과 탈중앙화 금융시장의 현 기술적 장애물을 해결하기 위한 블록체인 기반 중앙은행 디지털 화폐를 제안하였다. 또한 스테이블 코인의 데스 스파이럴에 대한 계량경제학적 분석을 통하여 스테이블코인이 암호화폐 및 탈중앙화 금융시장에 지대한 영향을 미치고 있음을 보였다. 또한, 대체 불가능 토큰 시장의 수익률-거래량 인과관계를 확인하였으며, 이를 통해 다양한 시장 상황에 놓여 있는 대체 불가능 토큰 투자자들에게 도움을 줄 수 있을 것으로 기대한다.

주요어: 블록체인,중앙은행 디지털화폐, 스테이블코인, 대체 불가능 토큰

학번: 2020-34024