Blockchain Technologies

Paul Moon Sub Choi
Seth H. Huang *Editors*

Fintech with Artificial Intelligence, Big Data, and Blockchain

Springer

Blockchain Technologies

This book series aims to provide details of blockchain implementation in technology and interdisciplinary fields such as Medical Science, Applied Mathematics, Environmental Science, Business Management, and Computer Science. It covers an in-depth knowledge of blockchain technology for advance and emerging future technologies. It focuses on the Magnitude: scope, scale & frequency, Risk: security, reliability trust, and accuracy, Time: latency & timelines, utilization and implementation details of blockchain technologies. While Bitcoin and cryptocurrency might have been the first widely known uses of blockchain technology, but today, it has far many applications. In fact, blockchain is revolutionizing almost every industry. Blockchain has emerged as a disruptive technology, which has not only laid the foundation for all crypto-currencies, but also provides beneficial solutions in other fields of technologies. The features of blockchain technology include decentralized and distributed secure ledgers, recording transactions across a peer-to-peer network, creating the potential to remove unintended errors by providing transparency as well as accountability. This could affect not only the finance technology (crypto-currencies) sector, but also other fields such as:

Crypto-economics Blockchain
Enterprise Blockchain
Blockchain Travel Industry
Embedded Privacy Blockchain
Blockchain Industry 4.0
Blockchain Smart Cities,
Blockchain Future technologies,
Blockchain Fake news Detection,
Blockchain Technology and It's Future Applications
Implications of Blockchain technology
Blockchain Privacy
Blockchain Mining and Use cases
Blockchain Network Applications
Blockchain Smart Contract
Blockchain Architecture
Blockchain Business Models
Blockchain Consensus
Bitcoin and Crypto currencies, and related fields

The initiatives in which the technology is used to distribute and trace the communication start point, provide and manage privacy, and create trustworthy environment, are just a few examples of the utility of blockchain technology, which also highlight the risks, such as privacy protection. Opinion on the utility of blockchain technology has a mixed conception. Some are enthusiastic; others believe that it is merely hyped. Blockchain has also entered the sphere of humanitarian and development aids e.g. supply chain management, digital identity, smart contracts and many more. This book series provides clear concepts and applications of Blockchain technology and invites experts from research centers, academia, industry and government to contribute to it.

If you are interested in contributing to this series, please contact msingh@endicott.ac.kr OR loyola.dsilva@springer.com

More information about this series at http://www.springer.com/series/16276

Paul Moon Sub Choi · Seth H. Huang
Editors

Fintech with Artificial Intelligence, Big Data, and Blockchain

Springer

Editors
Paul Moon Sub Choi
Ewha Womans University
Seoul, South Korea

Seth H. Huang
The Hong Kong University of Science and Technology
Clear Water Bay, Kowloon, Hong Kong

ISSN 2661-8338 ISSN 2661-8346 (electronic)
Blockchain Technologies
ISBN 978-981-33-6136-2 ISBN 978-981-33-6137-9 (eBook)
https://doi.org/10.1007/978-981-33-6137-9

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Contents

Blockchain, Cryptocurrency, and Artificial Intelligence in Finance

Yun Joo An, Paul Moon Sub Choi, and Seth H. Huang

Abstract This chapter describes the principles of blockchain, cryptocurrency, and artificial intelligence (AI) and their applications to the financial sector. We first discuss blockchain, and discuss cryptocurrency, the best-known application of blockchain. We present the question of whether a cryptocurrency is a currency or an asset and whether it can be a new safe haven asset. We summarize the controversy regarding the issuance of a central bank digital currency (CBDC). We argue that digital currencies only show the potential to inject liquidity into an economy during market stress. Additionally, most of the recognized advantages of blockchain applications relate to two concepts: decentralization and consensus. Blockchain's decentralization can be used to democratize banking services, corporate governance, and the real estate industry. Finally, we present the strengths of and concerns in using AI technologies in banking, lending platforms, and asset management, bearing in mind the most recently developed applications in these areas. This chapter provides a contribution to the literature that incorporates both theory and practice in blockchain, presenting a detailed review of performances and limitations of AI techniques in finance, including recent publications relating to the COVID-19 pandemic, CBDC, and alternative data.

Keywords Blockchain · Cryptocurrency · Artificial intelligence · Fintech · Banking · Corporate governance · Lending · Investing · Bitcoin · Safe haven asset · Central bank digital currency

Y. J. An
School of Economics, Yonsei University, 50 Yonsei-ro, Seodaemun-gu, Seoul 03722, South Korea
e-mail: yjan@yonsei.ac.kr

P. M. S. Choi (✉)
College of Business Administration, Ewha Womans University, 52-Ewhayeodae-gil, Seodaemun-gu, Seoul 03760, South Korea
e-mail: paul.choi@ewha.ac.kr

S. H. Huang
Department of Business Management, The State University of New York, 119-2 Songdo Moonhwa-ro, Yeonsu-gu, Incheon 21985, South Korea
e-mail: seth.huang@stonybrook.edu

P. M. S. Choi and S. H. Huang (eds.), *Fintech with Artificial Intelligence, Big Data, and Blockchain*, Blockchain Technologies,
https://doi.org/10.1007/978-981-33-6137-9_1

1 Introduction

Fintech (financial technology) is the interactions between information and communication technologies and the established business of the financial industry. In this book, We examine three core concepts: blockchain, artificial intelligence (AI), and big data. This surveys the theories of blockchain and AI and its application to the financial sector. We present what blockchain is, how it works, how it is used in finance, and how it can disrupt or support the financial industry. We also summarize the performance and limitations of the AI techniques in banking, lending, and asset management.

Fintech firms have been increasingly prominent in the financial sector since the Global Financial Crisis (GFC) in 2008, increasing banking competition, improving payment technologies, expanding lending institutions, altering corporate governance, and leaving their mark on real estate and supply chain management. Fintech has caused breakthroughs in these areas by showing the potential to alleviate information asymmetries between managers and customers, reduce manual work, enable adoption of innovative techniques, and escape regulation. The opposites of these changes, namely information asymmetry, operational risk, slower adaptation to innovation, and heavy regulation, are prevalent in the conventional financial system, most evidently in banks [1].

Blockchain is a database of records where transactions are recorded and shared. It provides a decentralized peer-to-peer network where nodes can cooperate to reach consensus. Its integrity is a particularly remarkable feature, in which the blocks that hold the records of transactions are linearly linked into a chain in chronological order [2]. These blocks prevent any currency from being spent twice. Additionally, blockchain technology enables the following: cryptocurrency, pioneered by Bitcoin [3], and central bank digital currency (CBDC), which has been proposed as a complement for monetary policy; discussion of Bitcoin as a new safe haven asset; greater shareholder democracy in corporate governance; novel universality in the real estate industry; and prediction of customers' future orders based on historical records.

Most of the proposed advantages of blockchains relate to decentralization and consensus. The advantages shift demand and supply. Blockchain technology, by design, removes financial intermediaries, which lowers barriers and allows easy entry. That said, there are contrasting arguments claiming that current blockchain relies on skewed miners, so it is not fully decentralized, thus unable to yield the proposed advantages.

The advantages of AI include the utilization of novel data, generation of new customer profiles, sometimes in opposition to conventional data. For example, AI-based lending platforms can integrate large market segments because they can provide lower-priced credit to customers who have subprime ratings according to conventional criteria. In developing economies, AI techniques can enhance the penetration of the financial system because in remote areas, low-cost lending, banking, and payment services are more accessible than traditional banks. In asset management, machine investors follow pre-specified investing strategies to enhance their performance, while human investors are high-cost and more vulnerable to emotions during decision processing.

Despite their strengths, blockchain and AI techniques have limitations. Cryptocurrencies are subject to pseudonymity and fraudulent identity, which reduced user trust. Specifically, cryptocurrency the payment of choice for illegal activities. Blockchain inevitably faces fork problems because multiple equilibria can be formed in games induced by proof-of-work in blockchain protocols. Moreover, because some scholars argue that blockchain is not completely decentralized, its supposed advantages cannot be realized. Some blockchain protocols rely on only a handful of miners, so the protocols are vulnerable to the 51% attack. Further, there is concern regarding the massive energy consumption in mining.

Although AI techniques are attractive, the financial industry is slow to adopt them. AI is apparently not in the mainstream of current banking due to banking regulations, scarcity of skilled IT personnel, long-built rigidity in current IT systems, and banks' innate risk aversion. Although AI can enlarge the size and quality of data, big data will never mean that all entities will have equal access to it. Only market leaders and innovative firms can take advantage of rare alternative data, while most other firms will fall behind.

Fintech is viewed in two contrasts. The idea of sustainable fintech holds that fintech firms will provide healthy, competition in the financial industry. In this way of thinking, the established financial sector will experience improve customer service, and accelerate product innovation. However, the disruption will also take customers away from the conventional financial sector. Employees in banks, corporations, and insurance companies will be laid off. The literature that describes fintech as potentially disruptive calls for banks to enhance their customer relationship management.

Discussing economic policy in relation to central banking, Lagarde [4] argues that even though fintech may ameliorate technological problems, it can never replace the financial system as it is constituted. This is because in these areas, storytelling, earning the trust of the public, forming public expectations, and active communication among peer experts are the most critical in driving policy changes.

Section 2.1 introduces the idea of blockchain, how it works, and two of its most important properties in this context: consensus and decentralization. Section 2.2 presents the ways in which standard currencies and asset-pricing models are applied to cryptocurrencies. This subsection also presents a debate over whether Bitcoin is a new safe haven asset. Section 3 describes applications of blockchain to the banking industry (including CBDC), corporate governance, and the real estate industry. This section also describes concerns regarding the application of blockchain in the financial sector. Section 4 reviews the ways in which AI techniques are altering banking, lending, and asset management. It studies the performance and limitations to the implementation of AI techniques in finance, as well as the debate between the views of fintech as sustainable or disruptive. Section 5 gives the conclusion to the study.

2 Logic of Blockchain

2.1 Introduction to Transactions in Blockchain

Blockchain is a decentralized, peer-to-peer records database where transactions are recorded and shared. It brings (or is intended to bring) distributed consensus, where the majority of participants in a public ledger verifiably agree on transactions. We present the process of distributed consensus in blockchain in Fig. 1, following Böhme et al. [5]. Alice, a user, wants to send Bitcoins to another user, Bob. Alice would need to prove two points, namely, that she has ownership of a private key and that she has sufficient cryptocurrency in her account. Then, Alice's order to Bob is recorded in a block.

Alice receives the report of the transaction in her private key, and the report is also sent to Bob's public key. Bob verifies Alice's private key and sends his public key to a peer-to-peer network. All participating entities share the records of the transactions in a decentralized peer-to-peer network. Nodes in the network reach a consensus and then approve that the orders are truthful. If the verification is agreed to by every node, then the transaction is recorded in a public ledger. Unlike a traditional payment service or conventional finance services, there are no higher authorities who provide intermediation.

Next, the block that records the order from Alice to Bob is inserted into a blockchain. All blocks are added linearly to the chain, which is the origin of the name. Finally, the payment from Alice to Bob is held. Instead of being referred to a third, higher authority, blockchain requires cryptographic proof that two willing

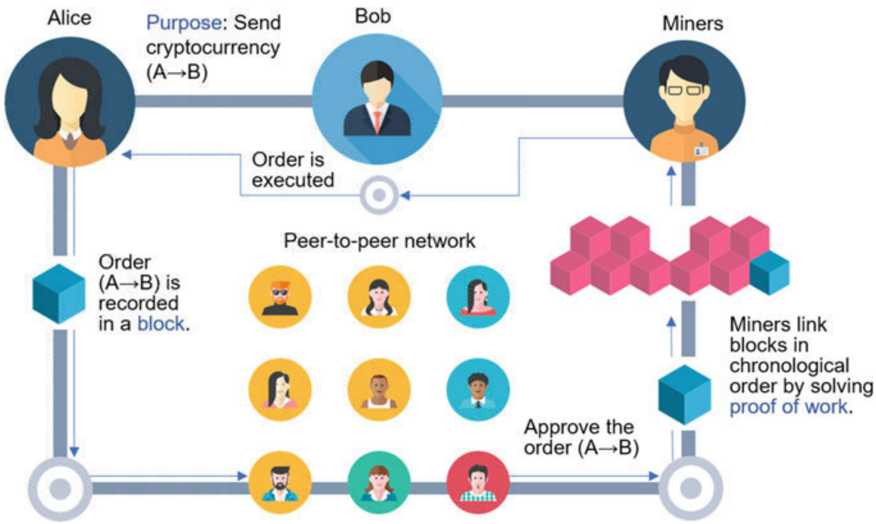

Fig. 1 Process of distributed consensus in blockchain. *Source* Authors

parties have made an online transaction. In this way, each unit of cryptocurrency can be traced through all of its transactions to the start of its circulation. Everyone can read all of the transactions in records that are stored in a widely replicated data structure. Crosby et al. [2] argue that although cryptocurrency is highly controversial in some areas, the blockchain system itself is flawless.

Consensus is the developed agreement between nodes in a peer-to-peer network. In particular, for blockchain, it is agreement on the validity of transactions and a history of orders. Many types of consensus algorithms exist for blockchain. Public blockchain relies on several nodes, and they typically require agreement on a single value. Agreement on a common value between multiple nodes is called distributed consensus.

How do nodes achieve consensus on the transaction between Alice to Bob? How can we ensure that the relevant blocks are linearly added? Blockchain incorporates two principal technologies: public–private key (asymmetric) cryptography and cryptographic validation of transactions. Asymmetric encryption involves an algorithm in which an encryption key (denoted the public key) and the decryption key (denoted the private key) are distinct. This method has the strength that its transmission can pass through unsecured channels. However, there is also the concern that it may be too slow because these keys involve the processing of large formulae in mathematical problems.

Proof-of-work is a highly computational mathematical puzzle that must be solved for the use of cryptocurrency. A block is inserted into a blockchain only if it solves proof-of-work. This puzzle becomes more difficult to solve with each new block added to the system. A node that solves proof-of-work earlier is added to the blockchain before the next node that solves it. This chronological order prevents double spending and falsified identity. The economic significance of proof-of-work is that it ensures the scarcity of currency. The prevention of double spending is an important prerequisite for blockchain to be used to issue money. In cryptocurrency, blockchain preserves scarcity of money by verifying the validity of transactions in the peer-to-peer network through proof-of-work and mining technologies.

Blockchain prevents double spending by what is called mining. To prevent recording a transaction that did not happen, each newly added block is compared to the most recently published block. In this transaction, the new block solves a mathematical puzzle that relates to previous blocks. If other users verify the solution, the peer-to-peer network agrees that the new block contains a valid transaction. Thus, the network and miners together ensure that the blockchain is chronologically ordered.

In a blockchain, transactions are arranged in a properly linear chronological order. Accounting for the mixture of orders was a daunting task for distributed records management prior to the adoption of blockchain technology [2]. Blockchain prevents a mixture of orders by placing transactions simultaneously inside a single block. Hence, all transactions in one block can be ordered at once. The ledger arranges multiple blocks in which every previous block intersects with the beginning of the following block. Yermack [6] describes the integrity of blockchain as follows. Assume that one agent wants to change an earlier block, say block 74, simultaneously adding the new block 91. Then, because blocks are ordered chronologically, the hypothetical agent would have to rearrange all the blocks from 74 to 91. This process would need to be done before the new block 92 is inserted. This would be extremely expensive, if it is even possible, so such an agent would be prevented from disrupting the order of chronologically linked blocks. We call the preservation of this property the integrity of blockchain.

There are three main types of blockchain: public, consortium, or private, distinguished by who is able to participate in the consensus. In public blockchain, any miner can participate in the peer-to-peer network and the public ledger, that is, the blockchain is read by the public. In consortium blockchain, a pre-selected handful of nodes engage produce consensus. Private blockchain entails a consensus determined by a given organization. In consortium blockchain and private blockchain, reading can be either public or restricted. Consortium blockchain shares the scope of its participants with private blockchain, but transactions in private blockchain are irreversible.

2.1.1 Blockchain Design: Decentralization

Decentralization describes how consensus is generated, distributed, and stored. Bitcoin is a pioneer in creating consensus protocols for blockchains. Conventional systems, including traditional banking, are centralized. Higher authorities like central banks seek efficiency in designing and implementing monetary policies. Centralization brings order, but in this arrangement, corruption is possible, as well as political dependence, which is especially a concern for central banks in developing economies. The GFC of 2008 demonstrated the vulnerability of financial systems and the limitations of conventional monetary policy as administered by central banks.

By design, blockchain eliminates the necessity of a centralized authority. Bashir [7] presents two ways in which decentralization can be implemented: disintermediation and contest-driven decentralization. Disintermediation is simply the absence of banks or any intermediaries that exist between sender and receiver in conventional financial system. Contest-driven decentralization, by contrast, involves competition between candidates seeking to perform a transaction service between buyer and seller. This method is not a perfect decentralization because there necessarily is an intermediary agent; however, it prevents monopoly. Blockchain technology can yield varying levels of decentralization.

Decentralization has certain advantages. First, it prevents single point of failure (SPOF) in a system, that is, it avoids structures in which if a part malfunctions, the entire system fails. Blockchain alleviates SPOF because it maintains irreversible records that are distributed among decentralized nodes. In this arrangement, the failure of a single node is unlikely to cause the peer-to-peer consensus to fail. Likewise, no single node can reverse or change any record and the order of any transactions.

Secondly, decentralization prevents monopoly power. The literature exhibits widespread acceptance that blockchain lowers barriers and allows participants to easily enter. Decentralization increases information interaction. Peer-to-peer networks allow agents to exchange digital assets with surplus information aggregation or exchange. It must be acknowledged that blockchain has achieved something that no prior technology in computer science had achieved: it increases information interaction while preserving data privacy [8]. Barenji et al. [9] merge blockchain technology with cloud manufacturing and highlight that the decentralization possible with blockchain can enhance its flexibility, efficiency, and availability. Blockchain would allow auditing firms to exchange encrypted information while preserving clients' propriety information. Early users of Bitcoin praise the decentralization possible with blockchain.

However, other work argues that the decentralization in blockchain systems is not perfect, and it has only limited benefits. Among other observations, it is noted that a handful of entities control decision making, mining, and consensus in Bitcoin protocol, so it is not fully decentralized.

Nakamoto consensus assumes that each mining node has similar computational power and thus a similar probability of extending the blockchain. Chu and Wang [10] argue that current blockchain technology is not fully decentralized because physical nodes in the blockchain have uneven computing power. If the price of cryptocurrency grows, the mining power of a single node can become many times that of other nodes. Their findings suggest that 53% of the mining power for Bitcoin is controlled by the top four Bitcoin miners. This means that the blockchain is maintained by a small handful of entities. A small, decentralized financial system entails higher risk than a centralized financial market. The small, decentralized financial system is vulnerable to adverse economic shocks because it is not controlled by regulators and is inclined to risky investing behaviors [5].

Moreover, blockchain decentralization is vulnerable to the fork problem, which occurs when blockchain diverges into two potential paths forward with conflicts appearing between the old and new rules. A hard fork is when the old node requires strict verification. A hard fork has only one chain and instantly requires old nodes to require new agreement simultaneously, so it negatively affects the whole stability of system. A soft fork is when new node verification requires strict conditions. This produces multiple chains. Here, if old nodes are unaware of the upgrade, they are given some time until they follow it.

Biais et al. [11] indicate that fork problems are inevitable because there are several equilibria in games induced by proof-of-work in blockchain protocols. This entails different versions of ledgers rather than a single unique ledger that reaches consensus. The fork problem is caused by these multiple equilibria in the blockchain protocol, information delay, and upgrades in the software. Böhme et al. [5] propose five types of intermediaries that prevent decentralization: currency exchange, digital wallet services, mixers, mining pools, and payment processors.

Chen et al. [12] propose the impossibility triangle to indicate that blockchain cannot achieve the three key virtues of decentralization, consensus, and scalability at the same time. Decentralization requires distribution of ownership and governance. If blockchain is decentralized, then a network is unlikely to reach a consensus. However, even if this does occur, it would entail duplicate storage, queries, and recordings. Accordingly, Lee and Choi [13] suggest an algorithm and a consensus protocol that synthesizes the conventional blockchain framework [3] and the directed acyclic graph [14].

Chu and Wang [10] argue that instead of this trilemma there is a dilemma between decentralization and scalability alone. Here, there is a trade-off between decentralization and scalability. Decentralized blockchain must sacrifice scalability. If it hypothetically were to become fully decentralized, a low upper bound would be found in the platform software layer. This layer would prevent the scaling of smart contract execution. In a smart contract layer, blockchain replicates sequential programming models, which prevent smart contract execution from scaling.

Blockchain depends on incentives to encourage honesty. Here, trust is the key component for interaction between entities. Decentralization involves sharing information among agents with divergent preferences and beliefs, in which the common ledger mitigates information asymmetry. In the computer science environment, trust involves executing transactions in a fault-tolerant way. The blockchain approach requires qualified searching and matching in storage computing, verifying transcripts of computations, and randomization of public ledgers.

Gandal et al. [15] provide empirical evidence of price manipulation of Bitcoin during a period that saw an unprecedented boom in exchange rate between the United States Dollar and Bitcoin, when Bitcoin's value spiked from $150 to $1,000 in late 2013.

2.2 Controversy Regarding Public Blockchain Application: Cryptocurrency

2.2.1 Cryptocurrency: A Currency or an Asset?

Nakamoto [3] marks the birth of Bitcoin, a type of cryptocurrency generated from the Bitcoin protocol that is entered into a ledger in a public blockchain. By design, Bitcoin works on a peer-to-peer decentralized network to evade the intervention of financial institutions. Blockchain takes root in digital currency applications. Any digital asset can be transacted with blockchain protocols, but Bitcoin is the pioneer cryptocurrency. Figure 2 and Table 1 present the close price history and market capitalization of cryptocurrencies, respectively. Bitcoin features the highest price and market capitalization of the five major types of cryptocurrencies arranged by market capitalization.

Despite the reputed perfection of blockchain technology [2], cryptocurrencies are highly controversial. The debates surrounding them can be boiled down to the following unresolved issue: Is cryptocurrency in fact a real currency or is it an asset?

The assessment of the topic in the literature relies upon theories of pricing dynamics. A basic understanding of macroeconomics would indicate that if real incomes or the velocity of money rises, the price of money also rise. Additionally, if the nominal interest rate increases, the price of money falls. These relationships

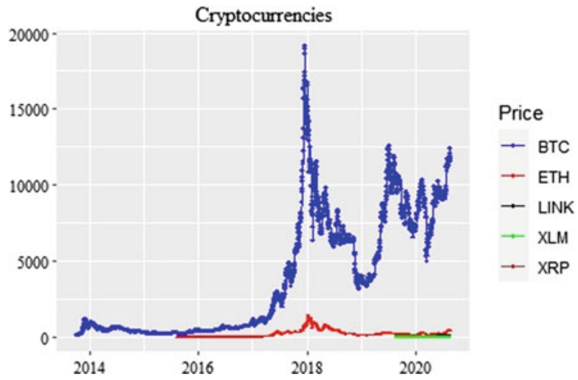

Fig. 2 Prices of Cryptocurrencies. *Note* Data are from monthly close prices in U.S. dollars from October 2013 to July 2020

Table 1 Cryptocurrencies by market capitalization

Currency	Market capitalization
Bitcoin	$217.84B
Ethereum	$45.52B
XRP	$28.90B
Chainlink	$15.67B
Stellar	$11.07B

Note Data are from https://www.coindesk.com/price/Bitcoin

are part of money demand theory. Bitcoin follows these macroeconomics rules. Its price rises in response to increases in the real interest rate and increased velocity of Bitcoin. Moreover, its price drops as the nominal interest increases [16].

However, other standard economic theories, such as the future-cash-flow model, the purchasing power parity idea, and the conception of uncovered interest rate parity, explain a limited amount of the variation in Bitcoin prices [17]. The soaring price of Bitcoin cannot be attributed to macroeconomic fundamentals such as gross domestic product (GDP), inflation, and unemployment. In a cryptocurrency market, the supply of the currency is fixed, or it is driven by a completely different algorithm from that which guides conventional pricing dynamics. The demand function is not driven by the macroeconomic fundamentals of an underlying economy but rather by buyers' and sellers' expectations of profits. Investment sentiment dominates the Bitcoin market, and it is mostly full of short-term noise traders. Against this background, the dominant view in the literature is that Bitcoin is a speculative bubble. Investors in the Bitcoin market are typically young and unexperienced, and they tend to make irrational trading decisions.

Yermack [6] argues that Bitcoin does not play the three functions of money, namely as store of value, a unit of account, and a common means of exchange. Hence, Bitcoin is not a currency. Cachanosky [18] uses Friedman's quantitative theory of money (MV = PY) as an analytic framework to analyze Bitcoin pricing,[1] finding that Bitcoin does not a follow a good monetary rule, indicating that it has serious limitations to becoming an independent currency.

Corbet et al. [19] propose what they call the cryptocurrency trilemma, in which regulatory alignment, cybercriminality, and potential for inherent bubbles cannot be alleviated simultaneously. Abadi and Brunnermeier [20] present a more general account, which they term the blockchain trilemma, in which blockchain cannot simultaneously achieve the three ideals of all database records: correctness, decentralization, and cost efficiency. If a blockchain wants to decrease its costs, then it must allow the free entry of record-keepers and information portability. In that case, however, correctness, which is driven by heavy computations and expensive proof-of-work algorithms, may become unaffordable. If a blockchain wants correct reporting in a cost-effective way, then the ledgers must incentivize correct reporting, which is typically available in a centralized record-keeper and its monopoly. Therefore, just as in traditional centralized intermediaries, blockchain and cryptocurrencies are restricted from pursuing all three ideals.

In markets that are integrated, shocks to prices of Bitcoin in one market affect price in the global market. However, if markets are segmented, such as that for Kimchi Premium, which is limited to Korea, then the price of Bitcoin in such a market has a marginal effect on the movement of the global price of Bitcoin [21].

In the literature, it is admitted that Bitcoin is not a perfect currency. However, even if cryptocurrency does not meet the requirements to be considered money, it nevertheless offers investment opportunities as an asset, given its high volatility and high returns.

Against this background, the literature applies standard textbook empirical asset-pricing models such as the efficient markets hypothesis (EMH) and the Fama–French asset-pricing factors. Bartos [22] applies the EMH to the movement of Bitcoin prices. Bartos finds that, unlike many conventional assets that provide poor empirical evidence for the EMH, Bitcoin does follow the logic of the EMH. The pricing of Bitcoin reflects all known information. All investors know all public information, and no investor can outperform the market by using other information. Thus, Bitcoin immediately reacts to public announcements of information by applying the error correction model to daily data from 2013 to 2014. The price of Bitcoin is highly sensitive to events and information. Investors in countries with inadequate financial institutions or tighter capital controls tend to buy Bitcoin aggressively, thus driving up the price [21]. Bitcoin prices in these countries are highly sensitive to positive shocks, including those of news or events.

Examining the asset-like nature of cryptocurrency, the literature has used classical empirical asset-pricing methods for cryptocurrencies. Evidence is presented in the literature for the Fama–French three-factor, Carhart four-factor, and Fama–French five-factor approaches on global stock markets [23]. However, Liu et al. [24] claim that they are the first to apply these approaches to cryptocurrency. The Fama–French

[1] M: money supply, V: money velocity, P: GDP deflator, and Y: real GDP.

three-factor and five-factor models explain very little of the returns of cryptocurrencies. This finding is not surprising because the three factors and the five factors explain the fundamental values of stocks by design. Cryptocurrency and stocks have different fundamentals, so Fama–French's factors necessarily have weak power to predict the expected returns of cryptocurrency.

Benchmarking the asset-pricing models of Fama–French and Carhart, Liu and Tsyvinski [25] construct the market factor, size factor, momentum factor, and value factor for the counterparts of cryptocurrency. The market and size factors do not affect expected cryptocurrency returns. The market factor does not explain zero-investment long-short strategies. These strategies indicate asset returns against market returns without concern for investment strategies held. The researchers employ the standard Fama and MacBeth cross-sectional regression.[2]

However, the counterpart to cryptocurrency in Cahart's fourth factor, namely the momentum factor, exhibits statistically significant power to predict the expected returns of cryptocurrency. Current returns positively and significantly predict returns 1, 3, 5, and 6 days ahead. The same holds true for Bitcoin weekly returns for 1, 2, 3, and 4 weeks ahead. The momentum factor generates alphas with significant long-short strategy returns. The researchers further report that the top quintiles do not outperform the bottom quintiles from the fifth to the hundredth weeks.

Working from Liu and Tsyvinski's [25] approach, Nguyen et al. [26] argue that short-term momentum predicts the expected returns of cryptocurrency, but the market, size, and long-term momentum factors do not affect Jensen's alpha for cryptocurrency. The nonsignificance of Jensen's alpha indicates that long-term momentum portfolios do not generate abnormal returns. Long-term momentum does not outperform the cryptocurrency market in that investors had rewarded the risks associated with market, size, and short-term momentum. The coefficient for the market factor is close to one, suggesting the possibility of random walk.

The literature also reports determinants of cryptocurrency from novel variables related to the Internet. Empirical evidence is provided that there are no underlying fundamentals in Bitcoin as a financial asset. Speculation, noise trading, and trend chasing evidently dominate Bitcoin pricing dynamics. Liu and Tsyvinski [25] argue that Google searches on Bitcoin, ripple, and Ethereum measure investor attention to cryptocurrency. Kristoufek [27] indicates that search queries on Google Trends and daily views on Wikipedia exhibit strong correlations with Bitcoin returns. The researcher further shows that greater Google search volumes cause the price of Bitcoin to increase (and vice versa). However, decreases in Bitcoin price has no statistically significant effects for search queries.

Mai et al. [28] claim to be the first to incorporate social media as a predictive determinant of Bitcoin returns. Increases in Bitcoin price are positively and significantly associated with lagged social media, implying that social media movements

[2]First, they sort the returns of individual cryptocurrencies into quintiles given the factor. Then, they track the returns of each portfolio in the following week and calculate the excess return over the risk-free rate. Next, they form long-short strategy based on the difference between the fifth and first quintiles.

can predict Bitcoin price movements. Microblogging has hourly effects, and Internet forums, which are largely a silent majority, show daily effects.

2.2.2 Cryptocurrency: Is It the New Safe Haven Asset?

The most intriguing question of cryptocurrency is rooted to its apparent resilience during the GFC in 2008 and to region-specific crises, such as bailouts in Europe in 2010–2013, and the demonetization initiatives of the Indian and Venezuelan governments.

The rising returns of Bitcoin during a bearish stock market have triggered (and in certain extent, have given hope to) academic research and the finance industry that Bitcoin could be a novel safe haven asset. Figure 3 presents closing prices of Bitcoin and stock indexes, including the Morgan Stanley Capital International (MSCI) USA, MSCI Asia, MSCI Europe, and MSCI UK. The nickname for Bitcoin, digital gold, relates to the safe haven asset properties of gold.

Figure 4 presents returns for Bitcoin-gold, Bitcoin-oil, and Bitcoin-U.S. dollar exchange rate. Bitcoin exhibits higher return volatility than gold, oil, or U.S. dollar. These simple plots ground a skeptical view of whether the return volatility of Bitcoin is stable enough for it to become a safe asset.

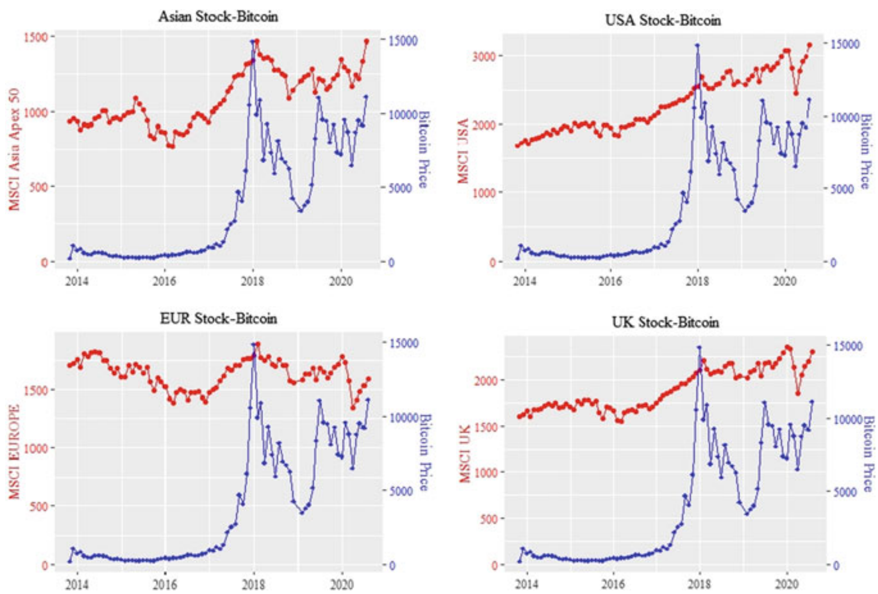

Fig. 3 Price of stock and Bitcoin. *Note* Data are monthly close prices of Bitcoin and MSCI stock indexes from October 2013 to July 2020, retrieved from https://www.msci.com/end-of-day-data-country

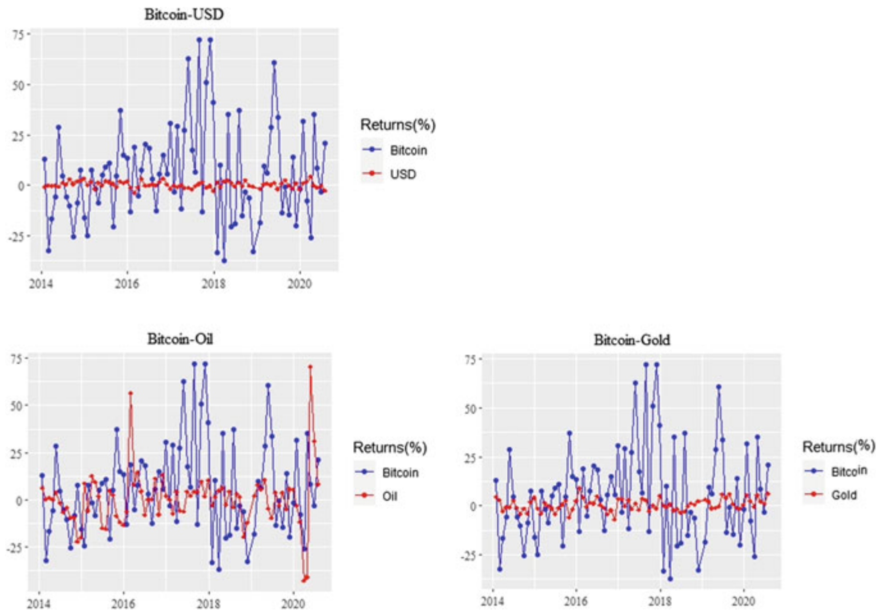

Fig. 4 Returns for the exchange rates between Bitcoin–gold, Bitcoin–oil, and Bitcoin and the U.S. dollar. *Note* These are monthly returns (%) from January 2014 to July 2020. We use the gold fixing price at 10:30 a.m. in the London bullion market in U.S. dollars, West Texas intermediate (WTI) crude oil price, and trade-weighted U.S. dollar: broad, goods, and services, with data from the Federal Reserve Bank of St. Louis Economic Research (FRED)

The literature supports mixed conclusions regarding whether Bitcoin is a safe haven asset. We review the literature that examines whether Bitcoin as a safe haven asset, grouping studies into three categories: Bitcoin as a hedge (diversifier) against risky assets, as a safe haven asset by definition, and as a safe haven asset by properties.

Regarding Bitcoin as a hedge, we adhere to Ratner and Chiu's [29] definition of a hedge, namely, when an instrument is uncorrelated with another asset on average. A strong hedge denotes an instrument that is negatively correlated with the other asset, on average.

Dyhrberg [30] employs the GARCH method and finds that Bitcoin serves as strong hedge against stocks and the U.S. dollar. These properties of Bitcoin are similar to the properties of gold. Their findings suggest that investors should include Bitcoin in their investment portfolios to hedge market risk.

Baur et al. [31] replicate Dyhrberg's [30] research and analyze contrasting results. Baur et al. [32] use an alternative model—Glosten et al. [33] asymmetric GARCH model, which does not include exogeneous variables in the variance equation. Their findings suggest that Bitcoin prices are uncorrelated with the value of the U.S. dollar. The return volatilities of Bitcoin are different from those of currency FX, equity indexes, gold futures, and gold spot. Because gold is strongly negatively related to U.S. dollar value, Bitcoin does not serve as a strong hedge against U.S. dollars.

Equity indexes such as the Financial Times Stock Exchange 100 return and the MSCI World return are all negatively correlated with the change in value of U.S. dollar. In the definition of hedging used here, Bitcoin can be a hedge but not a strong hedge against U.S. dollars.

On the other hand, Brière et al. [34] argue that Bitcoin has remarkably low correlation with stocks, bonds, currencies, commodities, hedge funds, and real estate. If an investor incorporates Bitcoin into a well-diversified portfolio, then alpha returns are improved. However, this result should be interpreted with a degree of caution because the time-series period in their research is relatively short, from 2010 to 2013 only.

The hedging effects of Bitcoin against stocks are associated with distinct fundamentals. Bitcoin and stocks have different underlying fundamentals. Accounting practices and macroeconomic fundamentals underlie the price movements of stocks, they do not influence the movements of Bitcoin. Standard economic theories on currency and asset pricing do not explain variations in Bitcoin price. The literature reports determinants of Bitcoin prices from unconventional variables, including Internet searches, social network activity, and microblogging.

However, hedging is insufficient to become a safe haven asset. Most studies of hedging are based on the statistical properties of Bitcoin returns. Safe haven assets are uncorrelated or only negatively correlated with risky assets in times of market stress. Does Bitcoin serve as a safe haven asset during financial turmoil? Research has found mixed results. We first review reports that support Bitcoin as a safe haven asset, and then, we examine the literature that opposes this.

Bouri et al. [35] argue that Bitcoin is a safe haven asset in the Asia-Pacific, China, and Japan because its prices are negatively correlated with stock prices during economic crises. The researchers proxy economic crises with heighted implied stock volatility (VIX). Bitcoin exhibits resilience to both normal times and financial turmoil, so the researchers conclude that Bitcoin is a safe haven asset in these regions.[3]

The literature investigates the effects of economic uncertainty on Bitcoin pricing. Wang et al. [36] measure the effects of VIX and the U.S. Economic Policy Uncertainty (EPU) [37] on Bitcoin pricing. The risk spillover shocks from VIX and EPU shocks are negligible for Bitcoin in most conditions, as shown in the multivariate quantile model and Granger causality tests. Bitcoin acts both as a hedge and a safe haven asset under EPU shocks.

Selmi et al. [38] claim that they are the first to examine hedging and the safe haven asset properties of Bitcoin, oil prices, and gold all together. They also consider different uncertainty measures, including Monetary Policy Uncertainty (MPU), financial uncertainty, and political uncertainty. Following a comprehensive measure of uncertainty, Bitcoin serves not only as a hedge against oil price movements but also as a safe haven asset in conditions of financial turmoil.

---

[3] The researchers claim that Bitcoin is not a safe haven asset against U.S. stocks because in bearish stock markets, it is positive and statistically significantly correlated with them.

Selmi et al. [38] compare the gold market, the oil price market, and the Bitcoin market by using a model that captures the interdependence between these markets. Bitcoin acts as a safe haven asset when the investor incorporates both Bitcoin and oil into a portfolio, but not both gold and oil. This study is comprehensive because it incorporates different traditional types of safe haven assets, uncertainties, and portfolios (risk-minimizing portfolio, equally weighted portfolio, and a hedge strategy portfolio), and it is robust to different methodologies (CoVaR and quantile-on-quantile regression).

Economic uncertainty has large and negative effects on the connectedness of six cryptocurrencies, namely Bitcoin, Ripple, Stellar, Litecoin, Monero, and Dash [39]. Therefore, cryptocurrencies can serve as a hedge against economic uncertainty. The larger U.S. EPU is positively associated with high demand for cryptocurrencies, which in turn is negatively associated with connectedness. VIX, crude oil volatility (OVX), and gold market volatility (GVZ) comprehensively decrease connectedness in cryptocurrencies, again exhibiting the safe haven asset property of Bitcoin.

Demir et al. [40] find that EPU and Bitcoin returns are negatively associated; thus, it serves as a hedge in conditions of uncertainty. They use the Bayesian graphical structural vector autoregressive model, ordinary least squares, and quantile-on-quantile regression. Incorporating Bitcoin into a U.S. stock portfolio lowers systematic and market risk. Bitcoin hedges against global geopolitical risks, and it is negatively associated with trade policy uncertainty during periods of regime change.

Because Nakamoto [3] proposed Bitcoin following the inception of the GFC that it is innately difficult to measure the behavior of Bitcoin prices during the GFC. Bitcoin first came to public attention after its soaring returns in the late 2013. Thus, there are little past data that can be used to test whether Bitcoin was a safe haven asset during the GFC. However, the COVID-19 pandemic crisis of 2020 is a good opportunity to supplement our understanding. This bearish market provides a timely test for the safe haven properties of Bitcoin. The literature has begun to examine the movement of Bitcoin prices during the pandemic.

Bitcoin clearly appears not to be a safe haven asset because its price decreased when the S&P 500 index dropped during the COVID-19 pandemic [41, 42]. In fact, its drop was even deeper than that of the S&P 500 index, confirming that judgment. The price movement of Bitcoin is neither uncorrelated nor negatively correlated with the price of stocks during this financial turmoil. Gold and soybean commodity futures, by contrast, are irreversible safe haven assets during financial turmoil, and Bitcoin was shown not to be one during the COVID-19 pandemic [43].

An important property of a safe haven asset is high liquidity because investors pursue safe haven assets in crises. They seek to sell risky securities and quickly buy liquid assets. Against this background, cash and government bonds attracted more demand during the GFC. Smales [44] finds that Bitcoin is illiquid compared to cash, government bonds, and gold. Hence, Bitcoin does not meet the criteria to become a safe haven asset. Smales proxies liquidity with bid–ask spreads, transaction fees, and differences in trading volume. The bid–ask spreads for Bitcoin are higher than those for stocks, bonds, gold, and stock indexes. The average daily volume of Bitcoin transactions is significantly lower than those for the comparison terms. Transaction costs are higher for Bitcoin than for other assets. The transaction fees of Bitcoin cannot be anticipated. These findings suggest that Bitcoin is even less liquid than risky assets.

The liquidity of Bitcoin is highly dependent on exchanges, where Bitfinex relates to exchanges with the most liquid Bitcoin transactions. On average, stocks are more liquid than Bitcoin. Illiquidity makes Bitcoin useless as a hedge because a successful hedge instrument requires that the investor can easily buy or sell it. Because investors tend to rush for safe haven assets during crises, Bitcoin has an undesirable property, illiquidity.

3 Blockchain in the Financial Industry

Enhancing performance against risk, is the ultimate goal for anyone working in the financial industry. Blockchain has improved performance in this way by lowering costs and improving efficiency. The distributed character of records in blockchain reduces operational risk. Because it is not subject to interference from intermediaries, less manual work is involved between entities. Proof-of-work facilitates automation in blockchain technology.

Blockchain decreases the cost of trust. The current financial system imposes high costs on customers in trade for ensuring trust between institutions and users. Blockchain technology can lower costs, particularly in back-office or post-trade functions.

Centralized intermediaries entail concentrated risks and owe significant economic rents. Decentralized blockchain improves the administration of financial services in payments, digital identity, primary securities, processing derivatives, post-trade reporting, and trade finance. In this section, we review the literature on the application of blockchain to banking, corporate governance, and real estate.

3.1 Blockchain and Banking Industry

First, we examine the application of blockchain to banking. Blockchain has the potential to revolutionize how payment, credit information systems, and financial transactions are taken care of in banking. Digital finance enhances customer experience, efficiency, cost, and safety. It has the potential to bring technological breakthroughs to the financial industry, in four areas in particular: infrastructure, platform, channel, and scenario. Because the Internet is now ubiquitous in banking services, commercial banks must inevitably rely on new technological growth. Blockchain enhances economic efficiency, operational efficiency, and efficient service in the banking industry.

Blockchain disrupts the banking industry by facilitating smart contracts or automating banking ledgers. It is now quite common for tech firms and social networking companies to do provide payment services, for example, Apple Pay, PayPal, Android Pay, and Kakao Pay. Internet banking now allows customers to do perform transactions themselves without needing to visit a bank.

Blockchain reduces monopoly power and lowers barriers to entry. Catalini and Gans [45] claim that it entails two main costs: that of verification and that of networking. The cost of verification represents the expense of verifying the counterparty, including information on past transactions and the current ownership of the cryptocurrency. The cost of networking represents the ability to bootstrap a marketplace in the absence of any centralized intermediary.

Blockchain has noteworthy impacts on alleviating information asymmetry in the banking industry. In traditional financial markets, moral hazard and adverse selection are well known to destroy market equilibria. Blockchain alleviates information asymmetry and improves welfare and consumer surplus. This surplus is earned by a shared, transparent ledger and distributed information through a consensus. Cong and He [46] build an economic mechanism for consensus generation. They optimize the quality of consensus, as each contracted record-keeper optimizes its own utility. As a result, competition is enhanced and barriers to entry are lowered.

Blockchain can reach its full potential if the entire banking system adopts it. A single bank acting alone does not gain any competitive advantage by adopting it. Blockchain provides infrastructure for sharing information in a secure way, automating registration processes and detecting fraudulent identities. The cross-chain interoperability of blockchain is important for facilitating it as a medium of exchange in the banking industry.

3.1.1 Central Bank Digital Currencies: Pros and Cons

The GFC of 2008 exhibited the limitations of conventional monetary policy and the vulnerability of the financial system. Nakamoto [3] proposed Bitcoin during this time. Bitcoin's blockchain technology could affect the entire financial industry, including the banking sector. The outsize attention paid to blockchain in the banking context prompts us to inquire after the role that central banks can play in the use of blockchain. Should a central bank issue digital currency? The need for adequate liquidity has caught the attention of central banks who are considering issuing CBDC.

Most central banks in developed economies target a 2% inflation level, but this goal is not easy to achieve using conventional monetary policy. CBDC enjoys three features that can enhance monetary policy: nominal anchor, tools and operations, and policy strategy. CBDC is a credible nominal anchor, built on publicly posted prices. It injects liquidity and facilitates the central bank's role as a lender of last resort. The researchers propose an analogy to Taylor Rule, replacing nominal interest with a CBDC interest rate.

Fernandez-Villaverde et al. [47] claim that during normal economic times, CBDC helps capital to be efficiently allocated in private financial intermediation. During crises, central banks are more stable than investment or commercial banks because central banks have rigid contracts. Williamson [48] shows that CBDC can reduce crimes related to physical money. Moreover, it allows interest payments on central bank liabilities. CBDC economizes on scarce safe collateral. If banks have market power in the deposit market, CBDC stimulates competition.

Meaning et al. [49] design an economy in which they assume that CBDC is universally accessible. They develop monetary policies using CBDC that share equivalent processes with conventional monetary policies. First, the central bank injects CBDC, thus determining the interest rates paid to its balances. Next, the variations in CBDC interest rates are changed into variations in other assets' interest rates.

Digital currency improves payment efficiency, although privately issued digital currencies do not achieve these efficiencies. For example, CBDC can coexist with bank notes. It increases financial stability and transparency if the central bank uses it to implement a consistent monetary policy. If economists effectively analyze the data attached to CBDC, they can measure network externality.

No type of money is perfect, so there is a need for different forms of it. Cash is a rudimentary type of money, is highly liquid, does not suffer from counterparty risk, and allows anonymity. A user of cash does not require financial intermediaries to perform transactions. CBDC is well-qualified as a substitute for cash.

CBDC and cash have similar features. Both are denominations of sovereign currency, legal tender, easily convertible, not subject to an interest rate, without central bank fees, enjoy high liquidity and 24/7 accessibility, anonymous, in a bilateral network, and irrevocable. CBDC injects liquidity to an economy in times of crisis. CBDC preserves the advantages of cash but excludes the rudimentary features of cash payment.

The literature reviews the effects of CBDC launched as a pilot in some countries. Bergara and Ponce [50] review the e-Peso launched by the Banco Central del Uruguay between November 2017 and April 2018. This test demonstrates that CBDC enhances monetary policy and lowers barriers to entry. Juks [51] finds that the preliminary launch of the e-krona does not harm the financial stability of Swedish banking system. Brunnermeier and Niepelt [52] review the Chicago Plan for the use of CBDC, and its pass-through funding did not harm financial stability.

Following the well-known idea of the impossible trinity, Bjerg [53] proposes the following policy trilemma in relation to CBDC,[4] in which the free exchange rate, monetary autonomy, and free capital flow in conventional currency are, respectively, matched to parity, monetary sovereignty, and free convertibility in CBDC. The trilemma here is that parity, monetary sovereignty, and free convertibility cannot be achieved at the same time.

CBDC benefits monopoly banking. It increases financial inclusion and reduces monopoly profits. During the initial phase of CBDC implementation, a bank panic

[4]The impossible trinity (also known as the impossible trilemma) is a concept regarding the value of a conventional currency in international economics. The trilemma is that it is impossible to simultaneously achieve three goals: a fixed foreign exchange rate, free movement of capital, and independent monetary policy.

arises. In this period, CBDC decreases the supply of private credit in commercial banks, raises the nominal interest rate, and lowers the reserve-deposit ratio in commercial banks. However, the researchers claim that once CBDC becomes available for all commercial banks, the increased quantity of CBDC amplifies the supply of private credit and lowers the nominal interest rate.

Despite the potential advantages of CBDC, central banks do not show any resolute intention of issuing it on a full scale. Although CBDC has the potential to replace cash, current blockchain technology is ineligible for it because blockchain protocols cannot transact large amounts of transfers or payments. Because of this, CBDC is not likely to have significant implications for central bank seigniorage. Davoodalhosseini [54] finds that welfare gains are not high where an economy has both cash and CBDC. Without additional regulations, CBDC is vulnerable to criminal activity. If disclosure restrictions are imposed, then CBDC loses the advantages of anonymity.

Lagarde [4] argues that fintech can never replace conventional central banking, although he also predicts that controversies over digital currency will be resolved in time, as the questions of volatility and energy consumption relate mostly to technological questions. More important to Lagarde [4] is storytelling. Communication, suggestions, and critiques among peers stimulate the development and expression of diverse opinions. The exchange is crucial to good policymaking. Central banks should clearly present their idea of the targeting price level to the public in plain English and form public expectations for future monetary policies, earning the trust of the public. He doubts that AI can communicate to the public in plain English and deliver monetary policies or target a price level.

3.2 Blockchain and Corporate Governance

We review the application of blockchain to corporate governance. Blockchain technology embedded in corporate governance is related to internal and external actors for corporate ownership rights, decision authority, and board structure.

Yermack [55] presents the impact of blockchain on corporate governance. It enhances the balance of power among managers, institutional investors, small shareholders, and auditors. It lowers cost and increases liquidity, transparency, and the accuracy of record-keeping.

Key features of blockchain are transparency and irreversibility. Because it enhances transparency in ownership records, it helps shareholders observe share transfers in real-time with lower trading fees. Blockchain's irreversibility benefits managerial ownership because manipulation of stock compensation becomes much more difficult. Corporate voting becomes accurate and transparent. Yermack [55] notes that if blockchain became dominant in corporate governance, its vulnerability to sabotage or exploitation of collective action would need to be overcome.

Blockchain technology alleviates the agency problem. Conventional internal and external monitoring lead to agency problems in corporate governance. Blockchain technology reduces the agency costs that stem from contracting with agents in a firm. It also provides a decentralized network that removes internal and external monitoring, which inevitably yield agency problems.

Blockchain also sustainably lowers shareholder voting costs and organizational costs in corporate governance. Annual general meetings require much less manual work. Panisi et al. [56] argue that blockchain can bring about or encourage shareholder democracy because share ownership can become transparent and trackable. Leonhard [57] claims that holders of cryptocurrencies can replace traditional shareholders where cryptocurrency holders can trade through decentralized autonomous organizations (DAO). Here, corporations would use smart contracts that could operate without government intervention thanks to the blockchain protocol that DAO uses.

Blockchain can foster universality. A public blockchain system is an optimal form for a nationwide industry. Blockchain's greatest opportunity is that it provides a fundamentally new type of database technology, which can be distributed across an entire country. Moreover, it makes online voting feasible. Shared distributed ledgers enhance transparency; the irreversibility of records improves credibility, and a peer-to-peer network fosters responsibility; smart contracts are positively associated with fairness.

3.2.1 Blockchain Concerns for the Financial Sector

There have been concerns regarding the implementation of blockchain technology in the financial sector. In the literature, the 51% attack is highlighted, which refers to vulnerability that if a single node controls more than 51% of computing power, the entire blockchain can be maliciously destroyed. A strong entity can modify transaction data and to stop verification and mining. The 51% attack can also lead to double spending, in which a few miners can enforce verification of a fraudulent transaction and insert a fraud block into the blockchain. If this occurs, other entities have no power because consensus has already been reached, with 51% of miners agreeing.

Bitcoin's technical burden increases the operating costs of blockchain to a possibly fatal level because it requires continuous consumption of electricity. The Bitcoin Sustainability report (2018) shows that the energy consumption of Bitcoin is increasing.[5] The consumption for one transaction in a ledger is on par with that of a U.S. household for 13 days.

The foremost virtue of the blockchain is honesty. Miners are expected to be honest and are provided with rewards for it. However, dishonest strategies are increasing. A game theory framework is used to show that the current Bitcoin system is vulnerable to subversive strategies and to mining cartel attacks. Blockchain users are experiencing threats and malware.

Bitcoin is not immune from questions of pseudonymity, privacy, and anonymity [58]. If pseudonymity in a public ledger leads to double spending, blockchain cannot be used for transactions of cryptocurrency. A substantial amount of cryptocurrency

[5] https://digiconomist.net/bitcoin-sustainability-report-01-2018.

transactions is associated with illegal activities [59]. Illegal users use cryptocurrencies to fake their identities and trade in illegal goods or services. Criminals often repeatedly order small amounts of cryptocurrencies because large transactions are unavailable on most blockchain protocols. These illegal transactions are associated with rapidly growing speculative investment sectors in Bitcoin and the emergence of alternative cryptocurrencies that allow the concealment of identity. Sustainable ownership in conventional financial systems has previously been studied [60, 61], the recent literature studies the sustainability of cryptocurrency and blockchain technology.

Blockchain has only limited availability for preserving identity and transaction privacy [62]. Privacy of identity entails that certain information, such as real identities and past transactions, should not be discoverable. Transaction privacy entails that the contents of a transaction should only be accessible to the agents who placed the transaction orders, not to the public. However, blockchain is vulnerable to replay attack, impersonation attack, and Sybil attack, major weaknesses in preserving identity privacy [63]. Blockchain also suffers from eclipse attacks, transaction malleability, and timejacking, showing a limited ability to preserve transaction privacy.

4 Artificial Intelligence and Big Data in Finance

There is no unified definition of AI, but there are different methods of implementing it, including machine learning (with neural networks at the forefront), random forest, or classification and regression trees. As more and more data become relevant, techniques can be expected to evolve. Newer AI techniques significantly affect companies that are developing prediction methods. Increases in the size of data are insufficient to enhance prediction. What is more important is preprocessing the data, improving computation algorithms, and minimizing errors [64]. Automated teller machines are among the earliest uses of IT in banking, beginning in the 1960s. Online payments and transfers are simply an early stage of the fintech era.

AI has changed both demand and supply in the financial industry. For demand, geographical borders are fading. Social networks are spreading massive amounts of information, regardless of its accuracy. In this context, people often act irrationally, showing herd behavior. On supply side, IT-based systems participate in lending, payments, and deposits.

Sironi [65] claims that fintech launched a new era of banking democratization, in which investors become price-makers and banks become price-takers. Fintech lessens the information asymmetry between economic agents and managerial insiders. It is consumer friendly, providing a positive interface, and it is mostly used on mobile phones.

Will fintech reduce costs and heighten profits for existing financial firms? Will fintech start-ups instead disrupt the conventional financial industry? Fintech has a large and positive effect on the value that accrues to innovators. However, market leaders only survive if they invest heavily in innovations and research and development expenditure.

4.1 Fintech and Banking Industry

Because banks are historically resilient to technological disruption, at least before the GFC, they often appear passive in relation to adopting innovations and technological breakthroughs. This lack of innovation motivates tech firms from the Silicon Valley to enter the financial sector. Tech firms launch fintech platforms in a relatively low cost way thanks to open source software or cloud services, such as the Tenserflow library and Google Cloud. Fintech firms can satisfy niche demand related to specific groups of customers.

Banks are often less inclined to innovate and are slow to respond. A major reason for this is the existence of banking regulations. Because fintech firms are less regulated, they are showing large increases in activities such as robotic shipping, AI-based start-ups, automation, and patent counting.

Fintech firms are forcing banks to reconsider their own competence. Jakšič and Marinč [66] urge banks to realize that they "have no time for complacency." Traditional banks, they write, should increase their competitiveness against fintech firms by standardizing back-office functions, investing in business-to-consumer services, and controlling the risks associated with financial innovations.

Fintech can bring structural change to the financial system. Philippon [1] urges that current banking regulations can never deliver deep-down structural change. A focus on regulations inevitably leads to controversies regarding the level-playing field and leverage. The growth of finance is attributed to efficient capital allocation. Financial incomes do not grow with per-capita GDP. Expenses, including asset management fees, are expensive. There is a dichotomy between the top-down regulation of the current banking system and the bottom-up regulation of fintech firms.

Philippon [1] argues that fintech can resolve issues that conventional banking will never be able to, such as for example, market entry and making a level-playing field, leverage controversies, and consumer protections. Regulations will be more effective if they are put into place early, when the industry is young. Because fintech start-ups are not held back by pre-existing systems, the start-ups have the chance to build the right system from the start.

The ability to conduct customer relationship management is a comparative advantage of conventional banks relative to fintech firms. This strategy incorporates the brand value, loyalty, voice-to-voice consulting, and work experience of the employees [67]. Although crowdfunding provides a lending platform, it is based on big data rather than on long-term relationships. Banks should seek to earn and maintain customer trust if they are to compete against fintech firms.

Stulz [68] argues that regulation is both a blessing and a curse for banks. It forms a barrier to entry, so it protects pre-existing banks threat to their profits. Most banks must follow capital requirements even though most transactions, including repossession and payment, do not necessarily require capital if fintech firms conduct them. The curse of regulations is that they make banks more rigid, allowing little innovation. They are also costly. Fintech firms are less regulated than banks, and they enjoy the ability to perform transactions in a floating value account. This float is the major source of profits for fintech firms. Moreover, these firms are funded with more abundant equity than existing banks.

4.1.1 Performance of AI Techniques in the Banking Industry

Data envelopment analysis (DEA) is a data-oriented approach that evaluates financial performance. It converts multiple inputs to multiple outputs with the use of decision-making units. DEA evaluates the efficiency of banks based on their technical and allocative efficiencies.

There is important research on the effects of AI on banking industry using country-level data. AI enhances auditing with planning, evaluation, analysis, pitching an opinion, reporting, and internal auditing in Nigeria [69]. Visual recognition enhances the identification of subjects, thus facilitating inventory checks. Vives [70] claims that residents of African countries have better access to a mobile phone than to banking, so mobile payment systems and P2P loans are more important than conventional banking in developed financial markets. Vives emphasizes that Africa should not fall behind developed economies in learning and implementing AI technologies.

Lee [71] uses Korean data on banking from questionnaires. He finds that information system risk management improves due to AI. Artificial neural networks enhance loan decisions in commercial banks in Jordan by visual identification [72]. Commercial banks in Japan cannot benefit from technological innovations, because the high level of non-performing loans in that country remains inefficient [73]. Likewise, restructuring is also blocked for current segments of regional banks in that country. Avkiran [74], using the dynamic network DEA approach, finds that in China, foreign commercial banks are more efficient than domestic ones, after considering divisional interactions, and interest-bearing and non-interest-bearing operations.

There are strict licensing regulations for fintech start-ups for developing economies. Saksonova and Kuzmina-Merlino [75] argue that fintech innovation has not yet begun in Latvia as most respondents in their study do not know what fintech services are. Fintech firms should improve their marketing to raise public awareness of them. Using experimental studies, Lee et al. [76] find that mobile banking in Bangladesh has increased urban-to-rural remittances by 26%; increased rural consumption by 7.5%, and decreased extreme poverty among both rural households and urban migrants.

4.1.2 Sustainable Fintech or Disruptive Fintech

The literature examines sustainable fintech, in which the pre-existing financial industry protects itself by implementing technological service themselves. Liu et al.