cryptography

MDPI

Article

A Review of Blockchain in Fintech: Taxonomy, Challenges, and Future Directions

Keerthi Nelaturu *, Han Du and Duc-Phong Le

Fintech Research, Bank of Canada, 234 Wellington Street, Ottawa, ON K1A 0G9, Canada; hdu@bankofcanada.ca (H.D.); dle@bankofcanada.ca (D.-P.L.)

* Correspondence: knelaturu@bankofcanada.ca

Abstract: The primary purpose of this paper is to bridge the technology gap between Blockchain and Fintech applications. Blockchain technology is already being explored in a wide number of Fintech sectors. After creating a unique taxonomy for Fintech ecosystems, this paper outlines a number of implementation scenarios. For each of the industries in which blockchain is already in use and has established itself as a complementary technology to traditional systems, we give a taxonomy of use cases. In this procedure, we cover both public and private blockchains. Because it is still believed to be in its infancy, especially when it comes to financial use cases, blockchain has both positive and negative aspects. As a result, it is critical to be aware of all of the open research issues in this field. Our goal is to compile a list of open research challenges related to various aspects of the blockchain's protocol and application layers. Finally, we will provide a clear understanding of the applications for which blockchain can be valuable, as well as the risks associated with its use in parallel.

Keywords: blockchain; fintech; use-cases; security; privacy; cryptography; smart contract

Citation: Nelaturu, K.; Du, H.; Le, D.-P. A Review of Blockchain in Fintech: Taxonomy, Challenges, and Future Directions. *Cryptography* **2022**, *6*, 18. https://doi.org/10.3390/cryptography6020018

Academic Editor: Joseph K. Liu

Received: 15 March 2022
Accepted: 11 April 2022
Published: 19 April 2022

1. Introduction

Until recently, banks were the primary players in the financial services landscape. However, as a result of technological and entrepreneurial advancements, new business models have emerged, introducing new participants such as start-ups and technology firms into to the mix. This development has significantly altered how businesses and retail customers manage their finances. These new disruptive companies, as well as the components that contributed to it, are now commonly referred to as "Fintech". Between 2010 and now, the amount of investment in this Fintech industry has increased dramatically, reaching a peak of $215.4 billion USD in 2019 [1]. The market is predicted to increase at a steady 20% rate over the next four years, reaching roughly $305 billion by 2025 [2].

1.1. The Fintech Ecosystem

The Fintech ecosystem is composed of a diverse range of players who are all committed to innovating, increasing the competition in the financial sector, ultimately benefiting the welfare of clients and boosting economic productivity. In [3], Lee and Shin highlighted five distinct components of the Fintech ecosystem: Fintech startups, technology developers, government, financial stakeholders, and traditional financial institutions.

The last decade has witnessed several technological upheavals involving domains such as social media [4,5], artificial intelligence [6–8], big data and cloud computing [9,10], augmented/virtual reality [11,12], and most notably blockchain [13]. Based on the applications and innovation of Fintech [14], one can classify it into numerous verticals, including: payments and banking, investments and capital markets, lending, crowdfunding, insurance services and loyalty programs (as shown in Figure 1).

Digital Payments and Banking Digital payments and banking were created to facilitate financial transactions by leveraging global technical advancements. Digital banking

is no longer limited to electronic banking [15]. It entails internet banking, mobile banking, and the use of electronic cards for payment, among other things. Similarly, the global market for digital payments is predicted to expand by $361.30 billion USD by 2030 [16]. The payments industry encompasses any kind of transaction that enables a payment to be made digitally.

Investments and Capital Markets Capital markets [17] are financial markets in which buyers and sellers come together to trade stocks, bonds, and other financial assets. Banks and investors can act as suppliers, while enterprises, governments, and individuals can act as purchasers. These markets connect suppliers and those seeking funds, providing a venue for the trading of securities.

Lending and Borrowing Digital lending and borrowing refers to the process of borrowing, disbursing, and managing digital channels through which credit decision-making and intelligent client engagement are guided by digital data [18]. This sector encompasses technology that enables financial institutions to increase production and loan profits while simultaneously delivering faster service at the point of sale (POS). It enables prospective borrowers to apply for loan products—such as Buy Now Pay Later (BNPL)—from any internet-connected device and from any location in the world.

Insurance Fintech insurance is the use of technological innovation to the insurance industry. Since the GFC (https://www.gfcinsurance.com/, accessed on 15 March 2022), insurance, like other sectors of the financial services industry, has seen numerous technological and data-driven advances. Many of advancements make use of connected devices. Due of the volume of data that can be provided, fintech enables insurance companies to offer dynamic pricing.

Crowdfunding Crowdfunding is a method of obtaining money for for-profit and not-for-profit organizations by reaching out to individuals who can invest in funding projects. The ease with which technology and social media may be used has enabled crowdfunding to reach a large audience.

Loyalty Programs Loyalty programs are critical for modern businesses because they increase customer engagement, increase retention, and give new channels for effective marketing efforts. Numerous businesses offer loyalty programs and encourage customers to use their products in the current market. However, these programs can be enhanced in terms of maintenance and usage by clients through the use of cutting-edge technology.

Law and Regulation In terms of information technology, the phrase regulation refers to Fintech applications that are used in the context of regulatory monitoring, reporting, and compliance. The rapid pace of technological innovation in financial services necessitates a close examination of the regulatory implications. Without which, end consumers who are unaware of these technical advancements are the most exploited. As stated in [19], the primary potential of regulatory technology (RegTech) resides in the current stage of technological evolution's move from Know Your Customer (KYC) to Know Your Data (KYD) approaches.

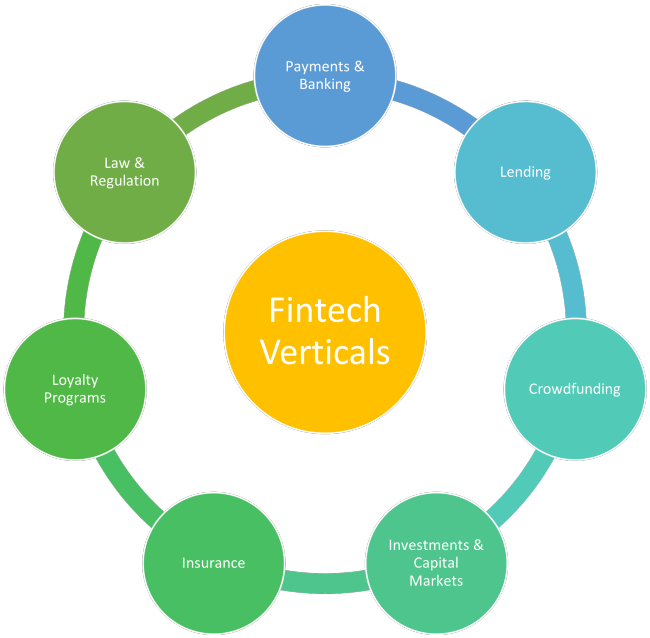

Figure 1. Fintech Verticals.

1.2. What Is Blockchain?

In 2008, the pseudonym Satoshi Nakamoto, who is the inventor of the cryptocurrency Bitcoin, published a white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" [20]. The paper described in detail a payment system in which people would directly send/receive payments to/from each other. The technology illustrated a mechanism by which payments could be performed securely without any intermediary financial institution. Arguably, Bitcoin was the world's first decentralized public ledger and it has since gained global status around the world.

The underlying technology standing behind the success of Bitcoin is the blockchain technology. This technology has also recently become a hot topic for researchers and been argued to be an even more revolutionizing phenomenon than Bitcoin.

Simplistically, the blockchain or distributed ledger technology(DLT) as defined in the Bitcoin whitepaper is a public, trusted and shared ledger, which is distributed to all participants in a community over a peer-to-peer network. In this community, people may or may not know each other, however, each member maintains his/her own copy of the information and all members must collectively validate any change on the blockchain. This removes the need for an intermediary third party. Blockchain is comprised by a continuously growing list of records called blocks that contain transactions. Blocks are protected from tampering by employing cryptographic hashes and consensus mechanisms. This allows the blockchain to be a transparent system of machines that originates and preserves the truth.

Public vs. Private Blockchains

Blockchains can be *public* (or *permissionless*), *private* or *consortium* (or *permissioned*). Bitcoin [20] or other cryptocurrencies (e.g., Ethereum [21]) are public. Cryptocurrencies are typically open to anyone to join the network and contribute to maintaining the integrity of transactions. However, in many other blockchain-based applications (e.g., related to company's private database), service providers may want to limit access rights to some specific groups of people. Answering the question: "who is able to join in the network, participate in the consensus algorithm and maintain the distributed ledger" allows developers to determine the suitability of a public or private blockchain.

In a private or a consortium blockchain platform, as opposed to a public platform, will allow organizations to retain control and privacy while still cutting down their costs and

transaction speeds. Typical examples include Hyperledger Fabric [22] and Multichain [23]. While clients are allowed to submit transactions, only pre-determined participants have permission to execute the consensus protocol, and update the distributed ledger as well. These participants must be governed by informal arrangements, formal contracts or confidentiality agreements. The private or consortium systems will have lower costs and faster speeds than a public blockchain platform can offer.

1.3. Related Work

This section discusses in detail previous works in the field of fintech and blockchain. We begin by discussing briefly review papers in Fintech. Then we will look at articles that are specifically related to blockchain and fintech. Finally, we describe how our work compares to earlier works.

Numerous studies have previously been conducted to showcase disruptive technologies for Fintech applications [24–28]. The majority of these works are heavily focused on Blockchain and Artificial Intelligence. Specifically, the authors in [25] discussed the developments in the use of these technologies in supply chain finance. They also address ongoing technical, research, and educational challenges. Numerous works discuss various research approaches for comprehending the Fintech landscape and provide a high-level overview of current research trends and recognized obstacles. The research methodology entails conducting meta-analysis [26] on several Fintech business models. This also has ramifications for and breakthroughs in technology. Even the examination of citations and co-citations, as demonstrated in [27], can provide scholars with a starting point for delving deeper into a particular area of inquiry. The other direction seen was evaluating the value derived from various companies' use of digital advances in Fintech [29]. In [30], a topical evaluation of Fintech research was offered, as well as analysis from a stakeholder perspective, which is unique among review works. The authors of [31] propose an industrial framework for Fintech, outlining the numerous economic entities that make up the monetary and capital markets umbrella of Fintech. All of the works described above address regulatory concerns and the likelihood of financial loss that might occur when digital innovation is implemented without conducting extensive risk analysis. Milian et al. [32] conducted a comprehensive study of the Fintech literature dating all the way back to the 1980s. They compiled a list of the most influential publications and created a classification system for Fintech literature. Their study is a comprehensive review of Fintechs, however it makes no mention of blockchain-based fintech.

In [33], Xu et al. conducted a statistical analysis of research publications on blockchain, with a particular emphasis on business and economics. Their investigation was confined to the quantity of research papers published in specific years, nations, or categories, including citations. The authors of [13,34] set out to accomplish a similar goal. Their research paper mapping study concentrated on the research subjects, constraints, gaps, and future trends of blockchain in FinTech businesses. Rabbani et al. [35] conducted an academic study of the scholarly literature on Islamic financial technology. Their analysis divides Islamic FinTech into three major categories: (i) possibilities and difficulties for Islamic FinTech, (ii) sharia compliance for cryptocurrency/blockchain, and (iii) law/regulation. Their analysis is confined to Islamic Fintechs and is purely commercial in nature. Ref. [36] is another review article focusing on the domestic implications of blockchain technology, specifically on Chinese research. Finance is one of the topics they addressed in their work. The writers in [37] conducted a comprehensive mapping analysis on 23 selected articles from a number of fields. The work can aid the scientific community by creating a map of the available literature, which can serve as a leaping point for future studies. Frizzo et al. [38] conducted a comprehensive review to ascertain the current state of the art in developing blockchain applications for enterprises in the following sectors: banking and finance, legal, accounting, and healthcare. The authors in [39,40] conducted a systematic evaluation of the literature to examine blockchain applications in the financial services sector. Their evaluations were limited to the application of blockchain technology in Fintechs, rather than classifications

of blockchain-based Fintechs based on the technology's technical properties. Ref. [40] is a complementary work to ours that focuses on the e-finance and fintech industries. Their research topic focuses on the fundamental concepts of blockchain technology, followed by a consideration of the technology's difficulties and applications. Ref. [41] is a similar work which discusses more on the technological aspects of blockchain with limited set of case studies. Ref. [42] conducted in-depth analyses of existing literature in order to determine the technology's growth into commercial spaces. In [43], the objective is to provide an overview of the risks, costs, and benefits associated with the use of blockchain technology in banking and financial applications. In [44] demonstrates that there is still a need for research topics to be handled with security and privacy in mind. Works such as [45] focus on a single technical advancement, such as IoT(Internet of Things), and provide blockchain applications in fintech that are particular to the use of IoT devices. Several publications focus on delving deeply into a single case study and doing a full architectural examination of how adopting blockchain enhances the application. For instance, Ref. [46] focused on the Triple Accounting Framework application and discussed how blockchain may be integrated into this space. Ref. [47] focuses on production industries and the use of blockchain for achieving faster targets. Ref. [48] targets how the concepts of smart contracts can be implemented to enhance the current business models between individuals and health insurance organizations. More technical papers like [49] delve into specific software patterns used in blockchain applications and these kind of works help upcoming researchers in implementing and using optimized patterns for blockchain applications.

In comparison to earlier research, a primary objective of this study was to expand on both technical and non-technical aspects of blockchain, specifically in the Fintech industry. Not only scholarly papers were included in our review, but also reports from various financial institutions and project-specific content. We discuss a variety of use cases for each of the fintech verticals mentioned. The use cases will demonstrate the applicability of blockchain not just in permissionless settings, but also in the enterprise sector. This work's taxonomy for use cases and characterization of blockchain properties are highly unique. We address all use cases not just from a commercial standpoint, but also from a technical standpoint, demonstrating how they are implemented in a production-grade system. Finally, we arrive at a prioritized list of open research issues covering all of the technical components of blockchain that remain unexplored. This provides an obvious diving point for any researcher interested in pursuing a topic specific to a technological field. To our knowledge, no other publication conducts such an in-depth technical research of the full blockchain ecosystem, complete with specifics on use cases.

1.4. Research Methodology

We describe the technique utilized to perform this review in this section, which involves identifying research questions, acquiring resources, and screening relevant studies.

1.4.1. Research Questions

As part of our review, the first step was to identify a set of research questions that would define the goal of this study. We define the following six research questions:

RQ1: *What are the key features of blockchain-based Fintech applications?*

RQ2: *What are the benefits or advantages of using blockchain in Fintech?*

RQ3: *What are the challenges and limitations of using blockchain in Fintech?*

RQ4: *Are there any use cases for blockchain in Fintech?*

RQ5: *Identify relation between blockchain use cases and traditional financial services?*

RQ6: *What are the future research directions for blockchain in Fintech?*

When working with two complex industries such as Blockchain and Fintech, the first step is to comprehend the characteristics that these two sectors provide. In Section 1.1, we define the Fintech streams' typical verticals. **RQ1** is focused on demonstrating the

well-known aspects of Blockchain that are applicable to Fintech applications. We would also want to study the interaction of the Fintech sector and Blockchain technology using the features offered. This is accomplished through **RQ2** in the process of recognizing the benefits and advantages of the technology. Even though blockchain was introduced in 2008, the practicing community is currently experiencing significant modifications and there are even plenty of new innovations being shaped within. This progress also entails a number of theoretical and practical difficulties. We highlight the problems and constraints associated with using this technology in the Fintech industry throughout all of the characteristics we examine. **RQ3** is concerned with identifying these constraints. The study will be reported in Section 5. Both **RQ4** and **RQ5** focus heavily on case study analysis. There are several use cases in Fintech, but are there any that are enhanced by the addition of blockchain? Due to the presence of blockchain in the technological stack, we are curious to learn if new paradigms are being brought into the Fintech sector, as well as monitor the evolution of traditional financial services. By studying these questions, we will provide a taxonomy of blockchain-based Fintech applications in Section 3. **RQ6** is to propose future research objectives for each of these domains. This will be covered in Section 5 as well.

1.4.2. Screening Process and Resources

The search approach we utilized was critical to our research. The search method began with the identification of digital libraries and web resources that would be screened for relevant materials. To begin, we selected indexing services that would include all publications pertaining to engineering, more specifically to computer science and developing technologies. We utilized Dimensions AI (https://www.dimensions.ai/, accessed on 15 March 2022) a tool that encompasses publications both open and closed majorly comparable to the below mentioned indexers. It is a database that offers the most comprehensive collection of linked data in a single platform.

1. Google Scholar
2. Scopus
3. Web of Science

We again narrowed the list of papers to those published in peer-reviewed journals. We choose four digital libraries for this purpose:

1. IEEE Xplore
2. ACM Digital Library
3. Science Direct (Elsevier)
4. Springer

One novel aspect of Blockchain is that it is available to everyone who understands how to utilize the technology, regardless of their experience or degree. This has attracted a large number of people who are not academics but rather technologists who have contributed several ideas. Thus, a substantial amount of knowledge relating to blockchain is available not just in academic papers but also in external resources. We chose a few well-known resources for our review, listed below:

1. *Fintech Reports from key financial institutions e.g., KPMG, JP Morgans, PWC, etc.*
2. *Research statements from Central Banks across different countries.*
3. *Medium.com articles from prominent opinion leaders in the industry*

The third list of resources included blockchain-specific organizations that are pioneers in educating both the blockchain and financial technology sectors.

1. Consensys (https://consensys.net/, accessed 15 March 2022)
2. BlockGeeks (https://blockgeeks.com/, accessed 15 March 2022)
3. Eth.research (https://ethresear.ch/, accessed 15 March 2022)
4. Enterprise Ethereum Alliance (https://entethalliance.org/, accessed 15 March 2022)
5. Cointelegraph (https://cointelegraph.com/, accessed on 15 March 2022)
6. Websites dedicated to projects discussed in this work

After conducting the search, we were left with a massive collection of papers and publications. To filter out irrelevant information, we utilized a set of selection criteria below:

1. Figure 2 shows the research trends on Blockchain for Fintech with the number of publications per year. These results are collected by querying "Blockchain for Fintech" from Google Scholar. It showed that the research interests for applying Blockchain to Fintech have been exponentially increasing since 2015. While there were only 18 publications in 2013 (five years after the introduction of Bitcoin), there were 6540 papers published in 2021. Similar pattern can be observed in other indexing sources as well. Hence, our first criterion was to restrict the publishing year between 2016 to 2022.
2. Based on keywords found in the publications' titles and abstracts. These keywords were determined primarily by compiling a list of all Fintech verticals, blockchain-specific phrases, and use cases. Some of the example keywords are listed in Table 1. The search strings were built by combining the keywords using connectors like **AND** and **OR**. For example, one of the search strings would be: (Fintech OR Payments OR Banking OR Lending) AND Blockchain.
3. We were also able to restrict the search results by citation count using a solution for information research datasets in Dimensions AI. We utilized the technique to identify extremely popular works in this field. This was accomplished by first searching the tool using various search terms and then selecting references with a citation count greater than 5 for each year beginning in 2018. Figure 3 shows the increase in the citation count for the works since 2013 with mean citation around 5.30.
4. Additionally, Dimensions AI delivers a search rank based on the publication's relevance. We chose resources with a rank greater than 100 for all search keywords.
5. Apart from the search restrictions, we additionally eliminated several entries using the criteria listed below:
   (a) Papers written in other languages than English.
   (b) Master and doctoral dissertations.
   (c) Duplicated articles obtained from all four indexing databases.

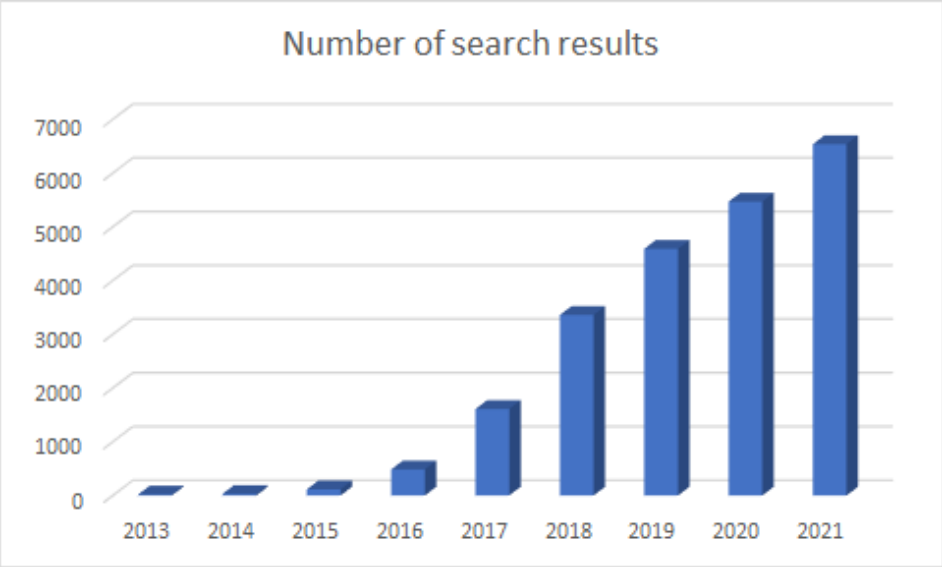

Figure 2. Research Trends on Blockchain for Fintech (Source: Google Scholar).

The complete refinement process is depicted in Figure 4 for a single search string—"review of fintech in blockchain". Using the approach we utilized, we were able to filter the results for this particular search string from 8876 to the 23 most relevant publications. To facilitate reading, we have included the top twenty search phrases we used to locate works relevant to the use cases in Table 2, along with the unique resource count for

each. The search phrase is constructed by prefixing "Blockchain OR DLT AND Fintech" to serve as a common string for all of the terms listed. For instance, the correct search term for decentralized applications would be "Blockchain OR DLT AND Fintech AND Decentralized Applications".

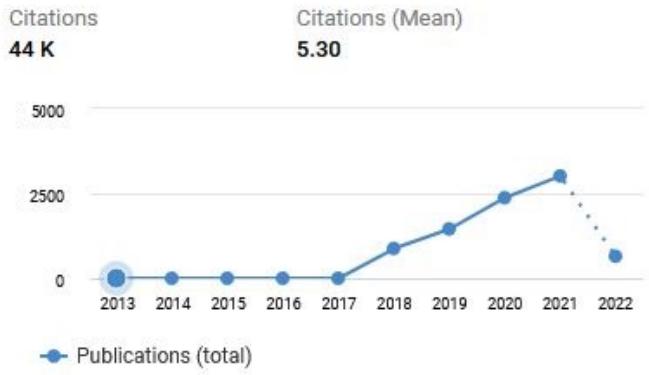

Figure 3. Citations Total (Source: Dimensions AI).

Table 1. Keywords selection.

Criterion	Keywords
General	Fintech, Blockchain, DLT, Enterprise blockchains
Fintech Verticals	payments, banking, investments, capital markets, lending, crowdfunding, insurance services, loyalty programs, supply chain
Blockchain related	Public or private blockchains, permissioned, permissionless, bitcoin, ethereum, hyperledger, smart contracts
Use cases	Decentralized Applications, stablecoins, digital currency, exchanges, oracles, decentralized finance

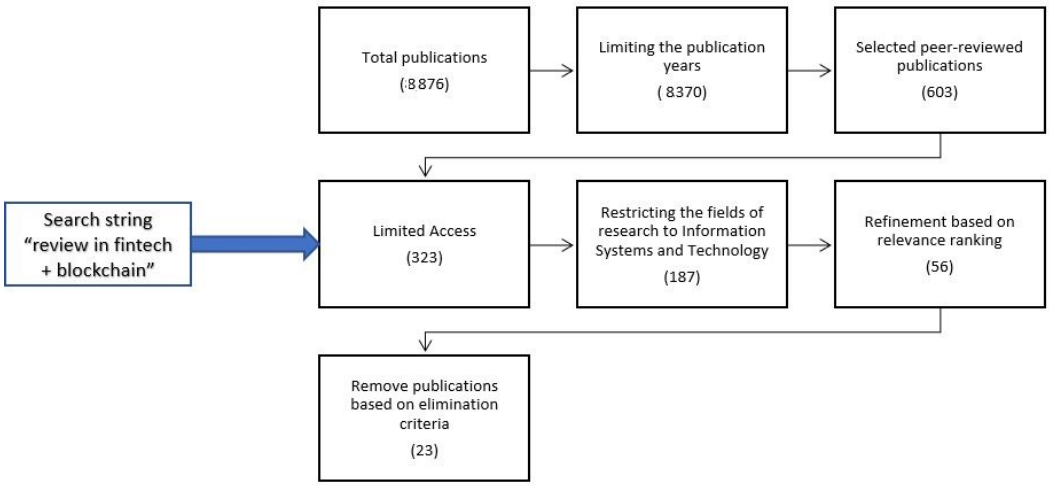

Figure 4. Sample search results refinement process.

Table 2. Keywords selection.

Search String	Count
Decentralized applications	5
Payments OR Digital Banking	4
Capital markets	3
Insurance	2
Health	4
Stablecoins	2
Digital currency	2
Oracles	2
Decentralized Finance	2
Smart contracts	5
Digital lending	7
Digital Borrowing	3
Regtech	1
Law AND Regulation	3
Governance	1
Identity	2
CBDC	1
Decentralized Exchanges	3
Storage	5
Marketplaces	1

Numerous academic areas have examined blockchain technology. We conduct a thorough evaluation of existing research in order to gain a better understanding of how blockchain might be used in Fintech. On the one hand, we examine the roles that blockchain technology may play in resolving current Fintech challenges like as access control, data storage, privacy, and confidentiality. On the other hand, we examine the possible difficulties that blockchain-based solutions may encounter as a result of their unique properties. We make recommendations based on our findings about how to overcome such obstacles when integrating blockchain to Fintech.

The rest of the paper is organized as follows: Section 2 delves into the fundamental principles and characteristics of Blockchain and smart contracts. Section 3 introduces a taxonomy organized on financial sectors and blockchain work streams. In this section, we provide with a list of key characteristics that blockchain provides with when included along with Fintech services which is to answer our question in **RQ1**. In the same section, we also highlight how blockchain transforms the Fintech industry by listing out all the features. This is to cover question **RQ2**. In Section 5, we examine the open research problems in the blockchain finance field as to cover the question in **RQ3**. Additionally, we discuss existing blockchain use cases that fit inside the finance industry. This is to answer question in **RQ4** and **RQ5**. In Section 6, we summarize our work and make recommendations for future work as a means to answer **RQ6**.

2. Background

Firstly, this section briefly recalls basic concepts in the blockchain technology. Then, we review its core principles, as well as cryptographic primitives used in the blockchain. Lastly, we explore the concept of smart contracts.

Table 3 describes some important concepts that are used in blockchain and applicable to Fintech applications.

Table 3. Concepts used in DeFi.

Concept	Definition
AMM	Automated Market Makers, a type of decentralized exchange (DEX) protocol that relies on a mathematical formula to automatically price assets.
Block	A data structure within the blockchain database that collects transactions in a period of time and permanently recorded on the blockchain
Blockchain	A distributed ledger stored across a peer-to-peer (P2P) network. A blockchain consists of blocks where transactions are permanently recorded by appending blocks.
Consensus	A mechanism that is used in blockchain systems to reach an agreement on the network's current state for the network's nodes.
Cross-chain	Complete decentralisation cannot be achieved unless people on different blockchains are interconnected with each other through one common protocol. Cross-chain technology aims to solve this problem by adding interoperability between different blockchains. It means they will all be able to communicate with each other and share data.
dApps	Decentralized Applications that can operate autonomously, typically through the use of smart contracts, that runs on a decentralized computing, blockchain system.
DAO	A decentralized autonomous organization (DAO) is a software running on a blockchain that offers users a built-in model for the collective management of its code.
Ethereum	A decentralized, open-source blockchain with smart contract functionality
Fork	A change of blockchain protocol or data in a public blockchain. It can be a *hard fork*, resulting in two blockchains or a *soft fork*, still maintaining one blockchain.
Genesis Block	Also called Block 0, is the very first block upon which additional blocks in a blockchain are added.
Node	A copy of the ledger operated by a user on the blockchain.
Mining	The process of creating a new valid block of transactions to the blockchains. Nodes mining are called *miners*.
Mining pool	A collection of miners who come together to share their processing power over a network and agree to split the rewards of a new block found within the pool.
Smart Contract	A contractual governance of transactions between two or more parties that is enforced and verified programmatically with blockchain technology instead of by a central authority.
UTXO	UTXO stands for Unspent Transaction Output. The remaining amount of digital currency after executing a cryptocurrency transaction.
Wallet	A digital wallet that allows users to store and manage their digital assets such as Bitcoin, Ether, and other cryptocurrencies. Basically, it includes an wallet address derived from the user's public key, and a private key authenticating for transactions related to the wallet.

2.1. How Does a Blockchain Work?

The nomenclature of blockchains derives from the how the data structure is essentially a chain of transaction blocks. Each block is in chronological order and linked to the previous block. As defined in [20], Bitcoin, known as the first *blockchain*, is "a chain of digital signatures". The Bitcoin system allows the self-mediation of exchange by enabling each coin owner to transfer an amount of coins directly to any other party in the network without the need of a trusted third party to act as the intermediary financial institution.

Furthermore, these transactions are recorded, publicly verified and stored on the blockchain network without a central governing authority.

Figure 5 describes how a transaction works on blockhain-based systems. Each transaction has an identifying code, known as a hash, generated using a *cryptographic hash algorithm*. This hash value contains the original piece of information of the transaction. The hash values of the transactions in a period of time are combined together in a *block* by using "Merkle Tree". Each block also is back-linked to the previous block, so-called *parent block*, through the "previous block hash field" in its block header. This sequence of linking hash values creates a chain to the first block, so-called *genesis block*. The previous hash in the new block ensures that the blocks are not tampered with and hinders cheating. The timestamp on the other hand proves that the transactions were made at the specific time [20].

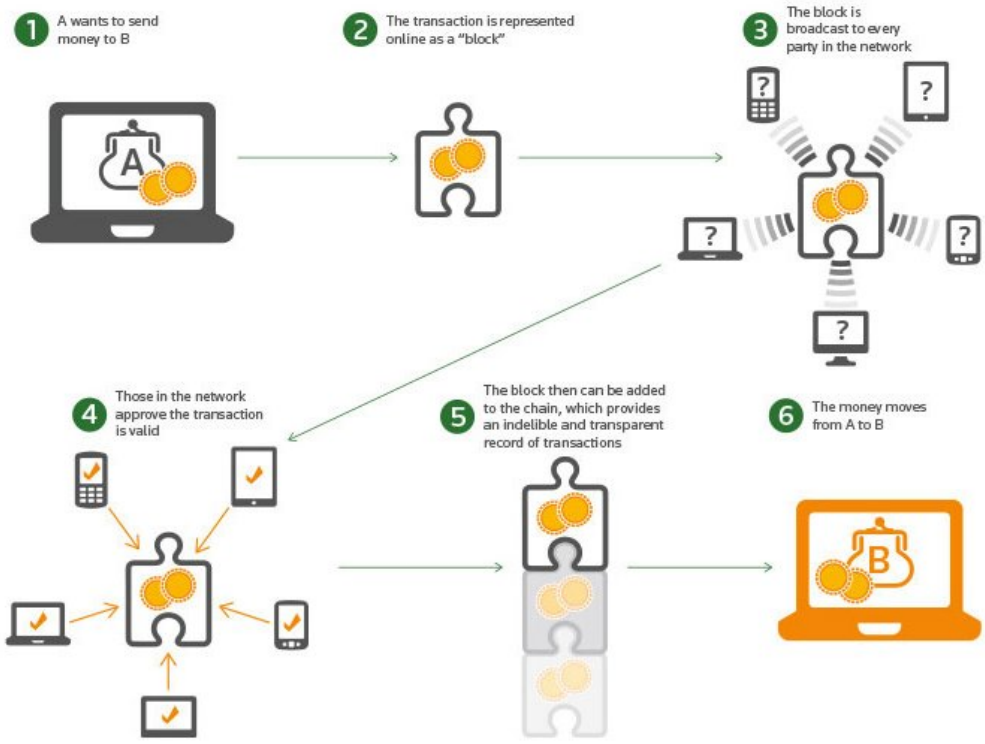

Figure 5. How does a blockchain work? (https://blogs.thomsonreuters.com/answerson/blockchain-technology/, accessed 15 March 2022).

The participants together enhance and continue the blockchain by complying strict rules and general *agreement*, which mean that the participants agree on how the chain will be updated. This agreement is called "*the consensus mechanism*". The cryptographic algorithms and techniques used in blockchain technology such as Merkle tree, digital signatures protect the blockchain's integrity, authenticity and anonymity.

The building blocks in the blockchain technology are as follows:

- **Cryptography:** In the first blockchain system, Bitcoin, the main purpose of cryptography is to provide the integrity and authenticity of transactions [20]. While the former is ensured by using hash functions [50], the latter is ensured by secure digital signatures [51]. The signatures play a double role additionally serving as an identity due to the properties of public-private key pairs. Only one who possesses the private key can generate a digital signature for a document. This digital signature hence ensures the strong control of ownership. In subsequent developments, with new found focuses around digital privacy, new cryptographic primitives such as special digital signatures [52], zero-knowledge proofs [53] or cryptographic commitments [54] have been developed to provide solutions in blockchain systems.

- **Smart Contract:** Bitcoin was initially designed for peer-to-peer (P2P) money transfer only. However, it soon showed the potential to be used for any kind of P2P value transaction on top of the Internet. The concept of smart contracts [55] was later introduced but ignited significant interest and popularity. Typically the contract layer is decoupled from the blockchain layer, where the ledger itself is used by smart contracts that trigger transactions automatically when certain pre-defined conditions are met. By decoupling the smart contract layer from the blockchain layer, blockchains like Ethereum aim to provide a more flexible development environment than the Bitcoin blockchain.
- **A Distributed Network:** Blockchain technology functions via a peer-to-peer network where information is stored in all participant nodes [20]. Validators (i.e., nodes) work come to a consensus about a fact witnessed by all parties in a common epoch. To secure the network against majority attacks, the network must have enough competing entities who are large enough to weather sudden arrivals/departures of competitors.
- **Network servicing protocol:** A block containing a list of transactions, a Merkle root value, previous block's hash value, timestamp, etc., is broadcast to and maintain on participants in the network. Public blockchain such as Bitcoin usually offers an available reward for computing power that serves the network [20]. The nodes serving the network create and maintain a history of transactions by working to solve proof-of-work mathematical problems. More serving nodes the blockchain is more secure.

Blockchain technology possesses the following characteristics that would make blockchain-based applications secure:

- First, the consistency of the global state is probabilistic. In most decentralised consensus mechanisms, it is not possible to determine which entity will update and solve the challenge next or at any given time. To obtain a good chance to be chosen as the next block's creator, an attacker must own more than 50% computing power of the total network.
- Second, all transactions' integrity and authenticity are protected by using hash functions and digital signatures.
- Third, consistency and correctness is enhanced because of the block history. Each block is chained by the hash of the previous block in the chain. Tampering with a transaction would make the hash value of all subsequent blocks in the chain wrong. This would be immediately noticed by other validators in the network who are continuously keeping verifying the transactions and refusing to accept transactions that are not consistent with the known longest chain.

2.2. Cryptographic Primitives

This section briefly reviews cryptographic techniques currently used in the blockchain technology. A taxonomy is depicted in Figure 6. These cryptographic algorithms can be classified in five (5) groups: hash functions, commitments, accumulators, signatures, and proofs.

2.2.1. Hash Functions

A *hash function* $\mathcal{H}$ is a cryptographic function that maps an arbitrary message to a fixed length output, that is, $\mathcal{H} : \{0,1\}^* \rightarrow \{0,1\}^{L_h}$, where L_h is a constant, the length of the hash function. A hash function have the following cryptographic properties:

- *First-preimage resistant* or *one-way*: Given a hash value $h = \mathcal{H}(m)$, it should be *impossible* to recover the message m.
- *Second-preimage resistant*: Given a message m, it should be *infeasible* to find a message $m' \neq m$ such that $\mathcal{H}(m') = \mathcal{H}(m)$.
- *Collision resistant*: For a hash function $\mathcal{H}$, it should be *infeasible* to find two messages $m \neq m'$ such that $\mathcal{H}(m) = \mathcal{H}(m')$. .
- *Zero resistant*: It is *infeasible* to find a message m such that $\mathcal{H}(m) = 0$.

While SHA-2 [50], especially the variant SHA256, were widely implemented in blockchains, RIPEMD160 [56,57] were also used in Bitcoin [20] and Ethereum [21]. Litecoin [58], forking from Bitcoin, and some other blockchains implemented SCrypt [59] instead of SHA256 to avoid ASIC hardware mining. Other hash functions, including Ethash [21] and Equihash [60] were also implemented in blockchain systems.

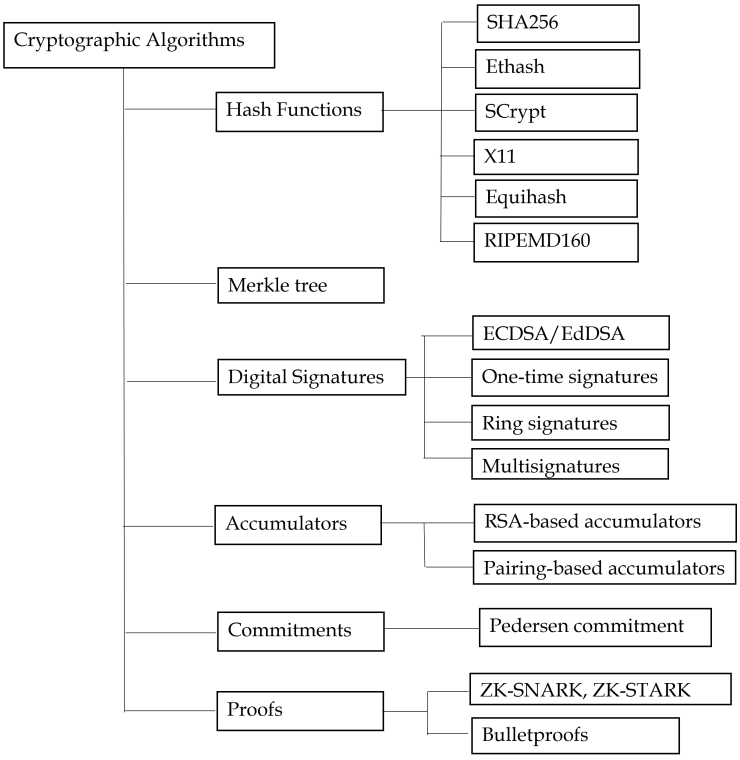

Figure 6. Cryptographic Algorithms used in the Blockchain Technology.

2.2.2. Merkle Tree

A *Merkle tree* [61] is a binary tree where the parent's node values are hash values of the concatenation of the children's node values.

$$\mathcal{F}(x_{parent}) = \mathcal{H}(\mathcal{F}(x_{left}) \| \mathcal{F}(x_{right})),$$

where $\mathcal{H}$ denotes the one-way function. In practice, cryptographic hash functions, e.g., SHA-2 would be chosen to implement such a one-way function.

In blockchains, leaves at the bottom of the Merkle tree are the hash values of the transactions during a period of time (see Figure 7). The nodes in the above row are the hash values of the concatenation of the corresponding two hashes below it in the tree. The number of nodes reduces by half. This processes is repeated recursively until the root of the tree that is a single hash. Figure 7 shows how to create a block with four transactions A, B, C and D. The Merkle tree allows users to copy/store just the small part of the tree, the *authentication path*, but still be assured that all of data's correctness is verified. The authentication path of a leaf $leaf_i$ is a list of the nodes that are siblings on the path from the Merkle root to the leaf $leaf_i$. For example, the authentication path of node A consists of $H(B)$ and $H(C\|D)$. If a attacker tries to make a fake transaction into the bottom of a Merkle tree, this will effect to all the node at the higher levels, including the Merkle root that was stored in all users. That is an invalid proof of work.

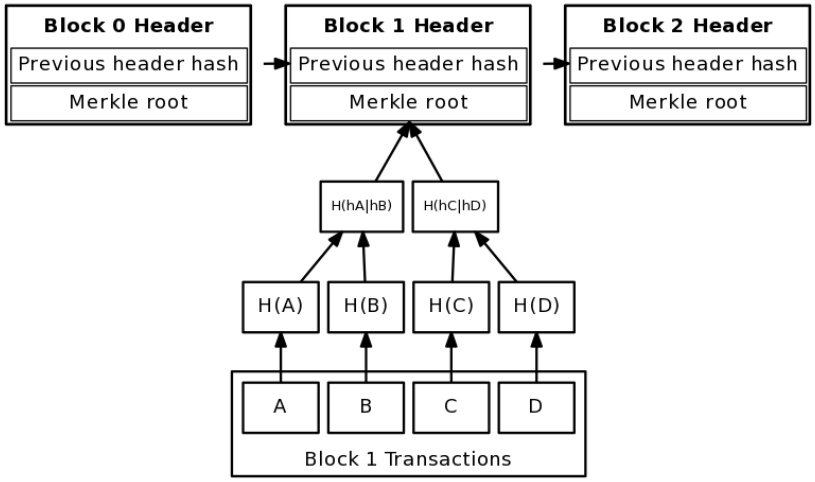

Figure 7. Merkle Tree in Blockchain Technology (https://yos.io/2016/05/19/merkle-trees-in-elixir/, accessed on 15 March 2022).

2.2.3. Digital Signature

Digital signatures based on asymmetric cryptography [62], are used to validate the *authenticity* and *integrity* of a digital message or asset. In cryptocurrencies, digital signatures can be used as a mean to prove the *ownership* of coins/tokens. The sender signs on the message due to his *private key* and the receiver uses the sender's *public key* to verify the validity of the digital signature.

ECDSA

The most popular digital signature used in the blockchain technology is the Elliptic Curve Digital Signature Algorithm (ECDSA), the elliptic curve analogue of the DSA [63]. This signature scheme was proposed by Scott Vanstone in 1992 [64]. It became popular and was accepted as the ISO 14888-3 standard in 1998 [65], the ANSI X9.62 standard in 1999 [51], and the IEEE 1363-2000 standard in 2000 [66].

Special Signatures

Bitcoin provides only pseudonymity, its transactions thus could be traceable and linkable, and thus users could be de-anonymized. In order to ensure the sender's privacy, a blockchain can implement a special signature algorithm, such as one-time signatures [67], ring signatures [52] or blind signatures [68]. By using *ring signatures*, one can sign a message on behalf of a group without revealing herself. Monero [69] combined the ideas of one-time signature and ring signature to create *one-time ring signatures*, in which private key can be used only once to generate a digital signature on behalf of a group. That blockchain also implemented Borromean (ring) signatures [70], an extension of ring signatures. Blind signatures [68] can be used to provide anonymity and inlinkability in case the transaction's owner and the signer are different parties. This signature scheme was implemented in BlindCoin [71]. Otherwise, multisignatures [72] can be used when a group of users commonly sign in a single document. In the blockchain technology, multisignatures can be used to increase to security of wallets. Multisignatures in [73] offers an aggregation of public keys that allows a smaller signature stored on the blockchain.

2.2.4. Accumulators

The cryptographic accumulator, formally introduced by Benaloh and de Mare in 1993 [74], is a one-way function that can prove the membership without revealing any individual member in the underlying set. Their construction is based on the RSA problem.

Another efficient construction of accumulators is based on cryptographic pairing [75], a bilinear map constructed over elliptic curves with low embedding degrees [76].

In the blockchain technology, a cryptographic accumulator can be used in building other cryptographic primitives, such as commitments and borromean ring signatures [70,77]. In fact, Zerocoin deployed an accumulator to eliminate trackable linkage in the Bitcoin blockchain, which would make transactions anonymous and more private [78].

2.2.5. Homomorphic Commitments

A cryptographic commitment scheme allows us to commit to a value while preserving its secrecy (with the ability to reveal it later) by publishing its hash value. A binding factor can be used when data size is small to prevent a brute-force attack. A commitment $Com(m, r)$ to message m and a blinding factor r has the following property:

- **Hiding**: one party wants to commit the message m without revealing the content of m itself.
- **Binding**: if one party makes a commitment to m, she/he cannot open it to a different message m'.

Pedersen Commmitment

Pedersen commitment [54] is a commitment scheme, which is binding under discrete logarithm assumption. Given an elliptic curve E defined over a finite field $GF(p)$. Assume that E has a group of point of large order q in which the discrete logarithm is hard, and two random public generators g and h. The commitment of a message m is a point c on the elliptic curve E that binding a message m and a random r to a point c on E. Pedersen commitment is defined as follows:

$$Com(m, r) = g^m h^r$$

It would be infeasible to calculate another pair m', r' that can produce the same commitment $Com(m)$. Pedersen commitment has additional property:

Additively homomorphic: if $m = m_1 + m_2$, and $r = r_1 + r_2$, then $Com(m, r) = Com(m_1, r_1) + Com(m_2, r_2)$.

Petersen commitment is used in cryptocurrencies such as Monero, Zcoin, Bytecoin, etc. to keep the amount of transactions confidential.

2.2.6. Zero-Knowledge Proofs

Zero-Knowledge Proofs (ZKP) [53] is a proof protocol between a prover and a verifier so that the verifier, after accepting the proof, learn nothing more than what she knows before receiving the proof from sender. Zcash [79] creators implemented and popularized zk_SNARKs [80], a zero-knowledge succinct non-interactive argument of knowledge protocol, aiming to provide perfect privacy for not only sender and but also the amount in transactions. Another ZKP protocol is used in blocchain is Bulletproofs [81], a non-interactive and aggregatable inner-product range proof, that allows proving that a committed value lie in a give range.

2.3. Smart Contracts

Smart contracts, first envisioned by Szabo in 1994 [55], are a complementary technology to blockchain. The following is a functionally recognized definition of smart contracts: Smart contracts are digital contracts that allow for decentralized consensus-based terms that are tamper-proof and often self-enforcing via automatic execution [82]. The primary purpose of smart contracts was to eliminate the need for centralized institutions to serve as authorizers or verifiers in transactions and to automate the whole financial process. The exact guarantees and features of smart contracts can vary across different blockchain technologies, but in general systems share a common goal of providing a robust system along with a safe general purpose language to allow payments on the platform to be

programmed for more complicated scenarios than a simple fund transfer. Typically they are implemented as high-level objects that co-exist on the blockchain with transactions and other data being stored on the blockchain. They could be made for one time use cases such as using a Hashed Timelock Contract (HTLC) [83] for an automated future payment as well as persistent and long-lived use cases such as Decentralised Exchanges [84] as well. Most implementations of smart contracts are designed for decentralised use cases in mind so that users can minimize their reliance on trusted-third parties, however they often will share the same pitfalls and vulnerabilities as the payments layer of the system.

2.3.1. Hashed Timelock Contracts

Secure escrows traditionally rely on a trusted third party to secure the funds and ensure that the funds are transferred to the recipient upon meeting preset criteria. Since blockchains are decentralised, there arose a need to invent a method to perform secure escrowing without a trusted third party and thus the Hashed Timelock Contract (HTLC) was invented [85,86]. It is one of the most important and widely used innovations in the blockchain space as it is often used to bridge tokens from one chain to another via cross-chain atomic swaps that facilitate secure funds transfer on two separate blockchains simultaneously.

The concept of a HTLC takes advantage of the security of a cryptographic hash as the main primitive that enables this innovation. They typically are composed of initial funds sent by the creator of the secure escrow, a hash of a secret, an expiry condition, and a recipient account. Knowledge of the secret in addition to a call to trigger the HTLC results in the funds being sent from the secure escrow to the recipient account. Depending on the scenario it will be appropriate for the hash of the secret to be generated either by the recipient or the sender. The expiry condition is typically a proxy for some future time, after which the secure escrow can be triggered to return funds to the original creator. These HTLCs can be chained in succession by the hash of the secret to give arise to much more complicated contingent payment structures.

2.3.2. Cross-Chain Swap

By using two HTLCs on two separate systems we can construct a cross-chain swap [87,88] that ensures that two parties swap one asset for another on two separate chains without the two blockchains building specific functionality for bridging across the two chains. In other words, it is a trustless swapping mechanism across two separate systems that does not require the systems to implement any bridging mechanism for the specific use case. When the HTLC is available as a primitive on both systems, as long as both parties can negotiate and agree on some conditions, swapping assets between systems is trivialized.

The overall construction of a swap is as follows:

1. Alice generates a secret and sends the hash of the secret to Bob out of band while negotiating the details for the secure escrows on both chains;
2. Alice generates an HTLC with her funds and the hash of the secret;
3. Bob generates an HTLC with his funds and the hash of the secret;
4. Alice reveals the secret to collect the funds from Bob's HTLC thereby revealing the secret to Bob who also collects the funds from Alice's HTLC;

During this process, no chain specific functionality was used on either blockchain, only each blockchain's internal HTLC primitive was invoked.

2.3.3. Bridges

A critical aspect of Fintech is the presence of massive legacy systems that cannot be converted overnight into a decentralized architecture. It will take considerable time and evolution for Fintech to implement blockchain. To address this issue, we have developed the notion of bridges, which may be utilized by private blockchain networks in conjunction with the HTLC and cross-chain exchange concepts. A blockchain bridge may be thought of as a link between disparate blockchains [89]. For instance, consider connecting a Hyperledger

Fabric ledger to the Ethereum network. The bridges operate as controllers, allowing them to disclose the ledger's data pieces based on their authorization. Bridges have been classified in a variety of ways depending on their purpose. The most often being: Trusted and Trustless bridges [90].

- *Trusted bridges*: These bridges are backed by a central authority that guarantees the integrity of the activities that pass over them. This means that users of this bridge must develop a relationship of trust with the entity that manages it. Multichain is an example of this sort of bridge.
- *Trustless Bridges*: These are bridges that are not controlled by a third party. Smart contracts or their own consensus algorithms regulate the bridge. Connext, cBridge, and Hop are a few examples.

3. Overview of Blockchain Platforms in Fintech

This section discusses the content necessary to respond to a handful of the research questions posed in Section 1.4. We begin by outlining all of the functional areas where blockchain can add value when combined with Fintech solutions. We next give a detailed classification of blockchain platforms using a multi-level methodology, highlighting both the common essential characteristics shared by all platforms and the fundamental dividing factor. Finally, we compare numerous projects to the classification's categories and provide their current status.

3.1. How Blockchain Transforms Fintech Industry?

The Fintech industry in the last decade has seen a large number of transformations due to the disruption in various technologies like Artificial Intelligence, Cloud computing and Blockchain. Specifically with blockchain, the amount of disruption spans across all the Fintech verticals. Below we list the core functional areas in which blockchain adds benefits.

3.1.1. Disintermediation

Conventional banking methods involve dependency on intermediaries at all levels. Every transaction requires a counter-party in order to process. This causes bottlenecks and systems prone to *single points of failure*. Disintermediation refers to the reduction of the use of intermediaries between producers and consumers. The essence of blockchain is to induce decentralization into this fintech workflow in effect eliminating the middleman. In a blockchain network, there is no single entity that controls the transactions. Depending on the chosen consensus mechanism, the network as a whole agrees upon the state changes in a trustless manner.

3.1.2. Immutability and Transparency

A principal challenge in the Fintech industry is the lack of visibility to the consumers. Consider any sector like Trade Finance or Cross-border payments, the consumer is walking blind with no intuition as to the fees structure or the resources available for usage. Transparency acts as pillar that can bridge gap between the customer and financial institutions. Blockchain is powerful in increasing transparency as no one party controls the information processed in the network and cannot be manipulated at the whim of an entity. Every transaction that updates the state is recorded by either all the network participants or the involved parties depending on the choice of architecture. The recorded state is immutable and cannot be prone to manipulation. This also simplifies auditing and regulatory requirements enabling observation of the flow of money in real-time.

3.1.3. Timeliness

Automation and instant execution of traditional contracts has been one of the focus areas for the past few years. Traditional financial contracts usually take 1–4 days for execution with the added manual intervention which can be as part of the remittance system or escrow or due to the requirement of physical presence for a signature. With the

introduction of smart contracts, we are able to achieve instant transactions along with the substitution of the escrow and use of digital signatures.

3.1.4. Cost Optimization

Time can always be attributed to money. The cutting down of middlemen, making the process visible to all and reducing the time evolves into the introduction of new business models with upgraded cost structures. The benefits around cost can be ascribed to the reduced infrastructure costs, operation costs, documentation costs and transaction costs. Several studies [91,92] suggest that around 20 billion USD cost savings can be observed in areas of cross-border payments, trade finance and regulatory compliance.

3.1.5. Privacy and Security

Fintechs in general deal with highly-sensitive data related to both individuals and enterprises. Fraud, security breaches and cyber-attacks are the top threats to the rise of Fintech. With most of the Fintech services going online enterprises collect tremendous amounts of data about customers and insights. Protecting and providing this data to the relevant parties in a secure manner is also a challenge. With the usage of cryptographic primitives imbibed in the blockchain infrastructure, the ability to make any data accessible to the authorized individuals without any leakage is easier.

3.2. Classification of Blockchain Platforms

There are several parts and aspects that make up a blockchain. It is as if these parts are Lego bricks that you can put together in different ways to make new technological advances. These components can be used to classify the many projects in this sector. In this Fintech-focused study, we first classify blockchains based on their permissioned or permissionless nature, and then, as illustrated in Figure 8, a further classification is based on specific characteristics. Based on the Taxonomy of blockchain systems defined in [93] and the different applications in the blockchain ecosystem that have been disrupted in recent years, we have formulated these characteristics. Below we define these characteristics on a high-level:

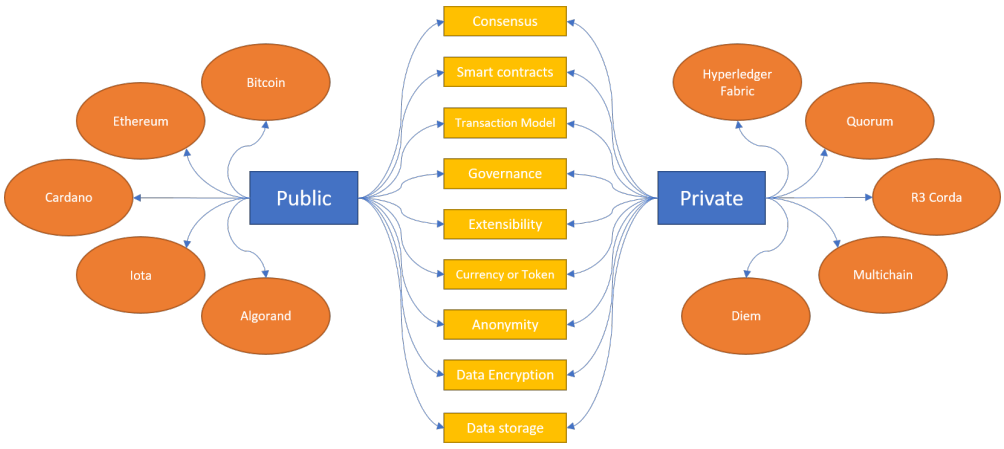

Figure 8. Classification of Blockchains.

Consensus: A blockchain is a distributed ledger system maintained by a network of nodes. As ledger data are changed, each of these parties must agree on the authenticity of the revisions. Consensus mechanisms for blockchain networks are composed of a set of rules and principles that facilitate agreement [94]. Each blockchain network has its own consensus algorithm. There are two extensively utilized consensus algorithms across major blockchain networks. The first is proof of work (POW) [20], which is employed in both the Bitcoin and Ethereum networks at the moment. POW requires participants to mine blocks and attach them to the chain once they are confirmed

as valid. These blocks must be provided in such a way that the block's hash begins with a certain number of zeros. The count is determined by a difficulty level that varies according to the network's congestion. As the difficulty of the block grows, the effort required to produce it can become exponentially more difficult. While proof of work enables an unbiased selection of miners, it comes with a slew of downsides. Specifically, the process of producing the block consumes a lot of energy, and the network is also vulnerable to 51 percent attacks [95]. Another extensively used algorithm is Proof of Stake (POS) [96]. Ethereum is expected to transition to a fully POS network in the last quarter of 2022. In POS, instead of miners, validators are chosen according on a consensus rule. By incorporating the network's transactions, the chosen validator offers the block for the current round. Other validators in the network can monitor and certify the correctness of the present validator's work. Even POS has drawbacks, such as the nothing at stake problem and long-range attack [97]. As a result, it is up to the network participants to decide which consensus to use based on the requirements of the product or platform.

Smart contracts: As mentioned in Section 2, smart contracts are rules that can be automatically enforced upon the fulfilment of specified criteria without the intervention of a third party. Each blockchain contains its own virtual computer, which each network participant must operate in order to analyse and process transactions. We can interface with the virtual machines using a low-level assembly language or a high-level language such as Solidity, which supports the Ethereum Virtual Machine (EVM). Thus, the support for smart contracts and the high-level language can also play a role in determining which blockchain network is most suited for a given use case.

Transaction Model: The transaction model defines the internal structure of the distributed ledger. This also influences how modifications to the ledger are stored in the ledger's memory. There are two widely used transaction models: Unspent Transaction Outputs (UTXO) and account-based. Each transaction in the UTXO model results in the production of additional outputs. These outputs are the only ones that can be used in subsequent transactions. For instance, suppose Alice owes Bob 30 BTC in Bitcoin. She can use an existing output tag of 40 BTC to send 30 BTC to Bob. The transaction's outputs would be a new output tag containing 30 BTC owned by Bob and 10 BTC held by Alice. Alice may use the ten bitcoins in any subsequent transactions. She is unable to use the earlier 40 BTC output tag because it is no longer valid. The same holds true for Bob. In contrast, the account model requires the system to keep a tree of accounts and their balances. Whenever a transaction between two accounts is issued, like in the preceding example, if the transaction is legitimate, meaning Alice has at least 30 BTC in her account balance and is permitted to handle the account, she can transfer it to Bob. On Bob's side, he should have an account at the address specified by Alice in the transaction. In this situation, there is no need to track any output tags. However, each model offers a number of distinct advantages and downsides.

Governance: On-chain governance and off-chain governance are two distinct types of blockchain governance [98]. On-chain governance refers to the decentralised enforcement of protocol rules and smart contracts. In these instances, governance norms will be referred to as Decentralized Autonomous Organizations (DAOs) [99]. Off-chain governance, on the other hand, refers to the rules and decision-making processes followed by the protocol's owners or the network's members as a whole. Off-chain governance methods on public blockchains include discussions on social media, online forums, conferences, and other events. In particular, governance systems in enterprise scenarios should incorporate both off-chain and on-chain components.

Extensibility: Due to the fact that blockchain is being used in the Fintech ecosystem, it must demonstrate durability, upgradeability, and maintainability features. This is commonly referred to as extensibility. Since the inception of blockchain technology, the majority of networks have encountered a variety of challenges, both in terms of

protocols and hacks. However, these same networks have overcome these obstacles. They have modernised the protocols. Issues with the codebase have been resolved. This capability is critical for a technology that is still in its infancy. Additionally, the presence of heterogeneous blockchains and DLT networks necessitates the establishment of communication between these systems. This interoperability situation adds complexity, yet it is a necessary condition for advancing the use of DLT in enterprise contexts.

Currency or Token: Numerous transactions are carried out on blockchains, which necessitates resource allocation by participants. In order to operate the network decentralised and equitably handle all transactions from all participants, the network must have incentive systems. These incentive mechanisms are reinforced by the use of either a system-wide native currency or a token that may be connected with ownership. Ether (ETH) is an example of a native currency, whereas ERC20 is an example of a token on the Ethereum network. The distinction is that actions within the virtual machine must be compensated in local currency, whilst certain apps are valued in ERC20.

Privacy: At all levels of the terrain, financial organisations are extremely concerned about privacy. With transparency being a primary purpose of blockchains, privacy is a critical concern. When it comes to financial services, privacy may be characterised in three ways from the user's perspective [100], including: transactional confidentiality, user anonymity, and unlinkability. Transactional confidentiality implies that no information about user transactions may be released without prior consent. Any malicious assaults on the system as a whole must nonetheless protect the system against user data leakage. Secondly, user anonymity requires that except for the user and the participating party in a given transaction, no other entity in the network should be aware of any specifics of the transaction, including the sender and receiver's identities. Finally, unlinkability implies that the inability of users to be associated with transactions. The ability to link a specific user to a transaction might result in the user's anonymity being compromised and all transactions related with the user being disclosed.

Security: On the other side, security needs might be classified similarly to privacy requirements. At the system level, it is required that the distributed ledger should be *immutable* and *reliable*, that is, the ledger should be consistent among network participants. No contradictions should occur as a result of the reconciliation, clearing, and settlement processes. It is also required that the system must provide a high *availability*. The majority of transactions are intended to have low latency and to complete without causing system disruption. At the transactional level, the transaction integrity must be maintained throughout the ledger's existence. In the Fintech sector, online transactions mostly include equity bonds, investments, and different high-risk assets. Thus, intentional falsification and forgery of transactions should be prohibited. Last but not least, preventing double-spending attacks on blockchain-based payment systems must be a desirable security feature.

Scalability: When it comes to blockchain performance, two critical variables are monitored: transaction throughput and confirmation delay. Centralized payment systems, such as banks, achieve a high level of optimization in terms of these two criteria. Whereas, blockchains confront significant issues in maintaining decentralisation. Scalability concerns extend deep into the system's numerous levels. This might be due to consensus constraints, the ledger state's structure, or reliance on external players, all of which result in confirmation delays. Thus, a project may be differentiated from others based on the solution chosen for a particular scalability challenge.

3.3. Comparison between Platforms

We have chosen many projects to review from both public and private blockchains that are highlighted in Table 4. These initiatives were chosen due to their inherent collaborations within Fintech sector.

Table 4. A Summary of Blockchain platforms and Applications.

Platform	Consensus	Transaction Model	Throughput	Private Transactions	Currency/Token	Applications
Bitcoin	Proof of work	UTXO	7 TPS	Shadow Addresses and Mixing	BTC	Payments
Ethereum	Proof of work	Account	15 TPS	ZK Proofs	ETH	Dapps
Cardano	Ouroboros Proof of stake	UTXO	257 TPS	ZK proofs	ADA	Dapps
IOTA	Fast Probabilistic Consensus	UTXO	1500 TPS	CoinMixing	IOTA	IoT devices
Algorand	Pure proof of stake	Account	1000 TPS	None	ALGO	Payments
Hyperledger Fabric	CFT & BFT	Account	3000 TPS	Channels & ZK proofs	None	Enterprise
R3 Corda	Validity & Uniqueness consensus	UTXO	15-1678 TPS	Inherent support	None	Enterprise
Quorum	RAFT and IBFT	Account	900 TPS	ZK proofs	ETH	Dapps
Multichain	PBFT	UTXO	1000 TPS	Streams	Custom	Enterprise
Diem	DiemBFT	Account	3 TPS	None	DIEM	Payments

3.3.1. Bitcoin

Bitcoin [20] is the first public blockchain that does not require users any permission to join the network. The consensus mechanism is based on proof-of-work. Miners use energy to validate transactions and construct new blocks. Miners receive rewards in the form of local currency BTC for successfully mining valid blocks. Scripting languages enable the inclusion of complicated transactions that go beyond money. Scalability is a bottleneck of Bitcoin network. At the moment, it only supports around seven (7) transactions per second. To anonymize transactions, coin mixing or tumblers, and shadow addresses can be utilised [101]. Mixing is a term that refers to a service that jumbles bitcoins in private pools and distributes them to the appropriate recipient anonymously. The term "shadow address" refers to a feature built into the protocol that generates a new address for the sender with each transaction. Payments are the most often utilised use case for Bitcoin.

3.3.2. Ethereum

Ethereum [21] is yet another permissionless blockchain. Similar to Bitcoin, Ethereum currently uses the proof-of-work consensus mechanism to achieve an agreement among participants in the network. The primary distinction is the inclusion of smart contracts and the use of an account-based storage approach. On top of Ethereum, smart contracts may be developed using a variety of high-level programming languages such as Solidity. The network achieves a throughput of roughly 15 transactions per seconds, which is somewhat faster than bitcoin. On this network, decentralised applications (Dapps) are extremely easy to develop. At the time of writing, there have been almost 3000 Dapps developed on Ethereum (https://www.stateofthedapps.com/stats, accessed on 15 March 2022). The native currency is Ether (ETH). For privacy, Zero-Knowledge proof contracts can be used to create private transactions. In order to avoid a high energy consumption by the proof-of-work consensus mechanism, Ethereum is scheduled for an upgrade to proof-of-stake mechanism in 2022.

3.3.3. Cardano

The project, dubbed "Ethereum Killer", orders and validates transactions using the Ouroboros protocol, a proof-of-stake consensus mechanism [102]. It employs a multi-layered approach, with the settlement layer in charge of currency conversion and the computation layer in charge of smart contract execution. As a result, the Cardano network may be easier to be upgraded compared to Bitcoin and Ethereum networks. For transactions, the network employs the UTXO concept. It is capable of scaling up to 257 transaction per second. For privacy, Cardano implemented Zero-Knowledge proofs, allowing private transactions. ADA is the network's native currency, which is used to incentivize validators. Cardano's road to acceptance is still long, since the network currently has just 62 decentralised applications (dapps), which is too small compared to Ethereum (https://cardanocrowd.com/dapps, accessed on 15 March 2022).

3.3.4. IOTA

Aimed at revolutionising the Internet of Things (IoT), IOTA [103] facilitates decentralised micro-payments between IoT devices. This network implements tangle, that is based on the Directed Acyclic Graph (DAG) data structure. There are no miners to validate transactions in the IOTA network, instead, it deploys a fast probabilistic consensus mechanism. Each node. issuing a new transaction, must approve two previous transactions. In the original design, IOTA also operates a coordinator node to achieve the consensus. It is thus criticized as a centralized network. It also did not offer smart contracts due to lack of absolute timestamp. Those issues were addressed in the IOTA's newest version, launched in April 2021. The system enables smart contracts by supporting EVM, all Solidity contracts can thus be implemented on IOTA. The network is capable of around 1500 transactions per second. Coin mixing is a technique used to conceal transactions. IOTA is the native currency used for rewards and payments in the network.

3.3.5. Algorand

A public blockchain that employs a variation of the proof-of-stake consensus mechanism known as Pure proof-of-stake [104]. ALGO is the currency that is dispersed throughout the network's validators. Payments-focused network capable of up to 1000 transactions per second with a five second finality. The Algorand network is built on a tiered structure, in which the first layer performs straightforward smart contracts pertaining to payments. The second layer is responsible for the execution of sophisticated smart contracts. The network was launched in 2019 and is funded by the Algorand Foundation, a non-profit organisation. Algorand is also planning to expand into the permissioned space with their enterprise blockchain platform.

3.3.6. Hyperledger Fabric

One of the most popular projects under the Hyperledger umbrella [22]. It is a permissioned distributed ledger that is well-suited for corporate use cases. Hyperledger Fabric enables the creation of smart contracts in the form of chaincode. Its design is very modular with many software components, minimizing the complexity of each component as well as the overall module-dependency network. The network does not have its own currency, and is able to perform approximately 3000 transactions per second. For privacy, Hyperledger Fabric establishes consortiums amongst members through the use of channels. There is also an option to have a private database contained within a node for the purpose of conducting private data transactions.

3.3.7. R3 Corda

The brainchild of the R3 Foundation [105], permits the creation of a privacy-focused permissioned blockchain in which organisations may deal directly with one another. This enables parties to conduct private transactions over the network. Similar to Bitcoin, it uses the UTXO concept for transactions. Additionally, legal contracts can be attached to transactions. Corda uses Kotlin, a cross-platform programming language to implement smart contracts. Due to the restriction on private transactions, throughput is limited to between 15 and 1678 transactions per second, depending on the participant structure. Corda implements two types of consensus mechanisms: *transaction validity* and *transaction uniqueness*. While the former requires contractual validity of the transaction and all its dependencies, the later prevents double-spends. In transaction validity, parties must first verify the relevant contract code and present all needed signatures. Otherwise, in transaction uniqueness, the parties must be assured that the transaction in issue is the sole consumer of all specified input. This procedure entails ensuring that no subsequent transaction consumes any of the agreed states.

3.3.8. Quorum

Quorum [106,107] is a private and permissioned network built on top of an Ethereum. It is based on the Go Ethereum client and utilises voting-based consensus. The unique feature of Quorum is that it can classify transactions as private or public based on an identity. As a result, the user initiating the transaction will have the option of making it private or public. One of Quorum's key goals is to maximise the usage of existing technologies rather than reinventing the wheel. Due to the fact that it is a fork of Ethereum, it supports EVM and smart contracts. Consensys bought Quorum from its original owner, JPMorgan Chase, in 2020. Currently, the network supports around 900 transactions per second, depending on configuration and setup.

3.3.9. Multichain

Mutlichain [23] is a Bitcoin core fork. It was created to facilitate the establishment of both public and private blockchain networks. Multichain provides several configuration options for configuring the network. Its primary purpose, as implied by its name, is to link and interoperate with several chains. Multichain implements privacy using streams. Participants can establish streams between themselves in order to share confidential data. The performance may thus be affected by the network settings and the amount of streams produced. Due to the fact that it is built on Bitcoin core, this protocol does not yet enable smart contracts and the chain operates using the UTXO transaction paradigm. Round-robin selection of validators for mining is used. During the initial setup process, custom native assets can be developed. At the moment, the network has a throughput of roughly 1000 transactions per second.

3.3.10. Diem

Diem [108] is a private permissioned blockchain network that is established with a small number of validators. DiemBFT is the consensus technique for validator election. The network is controlled by an entity called Association, which operates as a central authority. The Association account is primarily responsible for managing network memberships and setup. Diem made a significant contribution with the Move smart contract language. It contains several intrinsic safety attributes and tools that were created to facilitate the creation of secure smart contracts from the start. The objective was to make payments simple and flexible. Diem is the network's native currency. Except for the fact that the network is private, there are no intrinsic private transactions. According to a recent performance measurement on the testnet, Diem had a throughput of roughly 3 transactions per second, which is much slower than other blockchains. There has never been a mainnet from Diem till today. The project was formerly held by Meta before being acquired by Silvergate Capital (https://www.bloomberg.com/news/articles/2022-01-31/meta-backed-diem-association-confirms-asset-sale-to-silvergate, accessed on 15 March 2022). As a result, the project has been halted for an extended length of time with no updates.

4. Taxonomy of Use Cases

In this section, we will discuss the taxonomy of use cases in relation to fintech sectors and blockchain-related advancements. While each of the fintech verticals is self-contained inside its own domain, the use cases for blockchains are not, and they are having a ripple effect on other sectors. These use cases can serve as building blocks for developing new paradigms in financial services. We provide the Use cases alongside the fintech verticals in Figure 9 and indicate how each Use case can be applied to several verticals. Utility can refer to either technical architecture or commercial concepts. We expand on each of the use cases below in detail in this section.

		Fintech Ecosystem Verticals					
		Payments & Digital Banking	Digital Lending & Borrowing/Insurance	Investments & Capital Markets & Trade Finance	Infrastructure and Value-add services	Marketplaces	Crowdfunding
Taxonomy of usecase	Digital Identity	✓	✓	✓	✓	✓	✓
	Cryptocurrencies	✓					
	CBDCs and Stablecoins	✓	✓	✓			
	Decentralized exchanges		✓	✓			
	Decentralized finance		✓	✓			
	Decentralized oracles				✓		
	Decentralized storage system				✓		
	Node as a service				✓		
	Online marketplaces					✓	
	Supply chain finance			✓		✓	
	Governance			✓			✓
	Crowdfunding						✓

Figure 9. Use case Categories and Mapping.

4.1. Digital Identity

Blockchain technology can be used to issue digital identity and credentials such as birth certificates, driver licences, etc. in a secure and verifiable way. Indeed, in the simplest identity model, the organization which provides services will issues a digital credential that its users can use to access its service. This identity model requires a trust between user and the organization, typically established through a password-based authentication. This is a centralized and insecure approach to online interactions, and although multi-factor schemes enhance the security, but they add friction that reduce user adoption and productivity.

Federated identity, or third-party identity provider (IDP) model adds a third-party company or consortium to act as an "identity provider" (IDP) between users and the organization. The approach provides a single sign-on method, reducing the number of separate credentials users need to maintain. Although this identity model improves the user experience, it raises privacy concerns, where the IDPs can track and spy users' online activities. The digital credentials issued by an IDP also could not be used in privacy-focused industries, for example, a user can not use his Google credential to his banking service.

Blockchain-based digital identity, or self-sovereign identity (SSI), offers better privacy compared to the two above identity models. The self-sovereign identity community have worked on the validation of decentralized identity approaches to the critical password-based authentication problem. This decentralized framework not only improves the user experience, but also the security and privacy of users. It is pointed out in a Gartner's report in 2021 [109] that decentralized identity can mitigate risk associated with centralized identity solutions that continue suffering from many data breaches. Based on Hyperledger Indy [110], ATB Financial, Evernym, IBM, the Sovrin Foundation and Workday have come together in a joint multi-phase effort to conceive and incubate working examples of verifiable credentials (VC) for the purposes of awareness and education (https://www.ibm.com/blogs/blockchain/2018/10/decentralized-identity-an-alternative-to-password-based-authentication/, accessed on 15 March 2022). In practice, the European Union is creating an eIDAS compatible European Self-Sovereign Identity Framework (ESSIF) [111]. The ESSIF is based on the concept of decentralized identifiers (DIDs) and the European Blockchain Services Infrastructure (EBSI).

4.2. Payments

Payments, especially cross-border payments between individuals and SMEs in developing countries are facing high cost and long delays. Typically, each cross-border transaction is conducted across a network of corresponding banks or money transfer providers without a central clearing system. Transaction fees are high due to charges from payor's and payee's institutions; inter-bank, cross-border transfer. There is a significant amount of overhead and negotiation that is required to set up and facilitate transactions across two legal jurisdictions that is partially solved if parties are willing to agree to use decentralised platforms like Ethereum as an intermediary.

One primary issue with payments in the public blockchain space is that transactions are often, but not always entirely transparent with no privacy features. Typically there are four ways in which privacy is provided in this area:

1. Use an inherently privacy-preserving cryptocurrency;
2. Atomically swap to a privacy-preserving cryptocurrency and transact there;
3. Use a mixing service;
4. Use an on-chain privacy token/service

Given that a privacy-preserving ledger is designed to hide information from the public, atomically swapping to a privacy-preserving ledger is a non-trivial task. There are recent examples of such atomic swaps but they are still nascent in their adoption. Mixing services such as Coinjoin have a long history since before the DeFi space was well established but many keen observers have realised that its privacy-preserving mechanism was much more flawed than expected and do not provide the privacy-guarantees it was set out to achieve. The current most popular approach of achieve privacy in payments is through privacy enabling smart contracts such as Tornado Cash [112] which users exchange base currency for a variable denomination token that represents the user's claim on the Tornado Cash reserves. The token exchange happens over a zero-knowledge protocol on the relevant blockchain that closely follows and was inspired by ZCash's design [113].

Apart from the privacy issues, using payments in decentralized context introduces a new conceptual model. The traditional four-party payment model covers four main entities involved in transactions, including: (i) the customer making a purchase; (ii) the issuer, who holds the customer's funds and has issued the payments instrument (typically card) being used; (iii) the merchant accepting the payment; and (iv) the acquirer, the merchant's bank, who holds the merchant's account, ensures that the merchant has the necessary facilities, such as point-of-sale (POS) hardware, and initiates the processing of transactions.

Figure 10 depicts the main entities involved in the four-party payment model. In practice, an online payment must include another party, so-called card scheme, e.g., Visa, Mastercard, etc. The card scheme facilitates the communication between the acquirer and the issuer. They pair up the card information received by the acquirer with the relevant bank, enabling the acquirer to get the payment authorised.

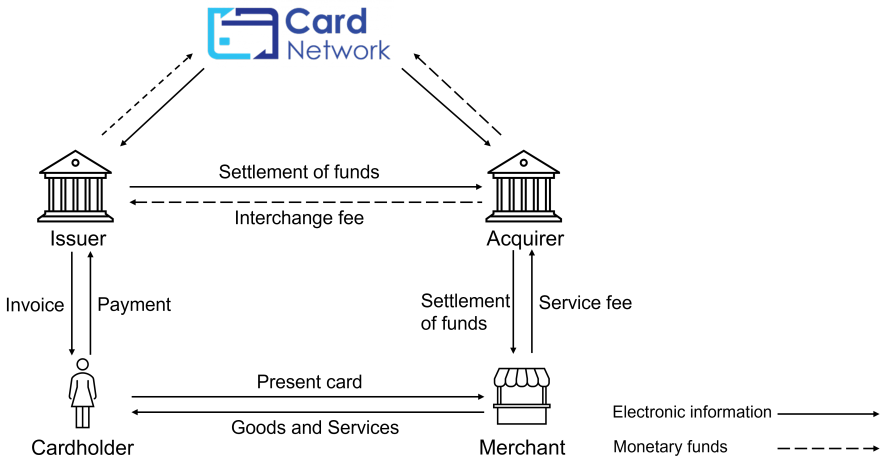

Figure 10. Four Party Payment Model.

Different from the four-party model, transactions on the blockchain are analogous to cash payments in that they are transmitted directly from payer to payee (Person-to-Person) without the need for an intermediary. This payment model when performed online introduces the following advantages:

- Reduce transaction fees
- Faster transactions, especially transactions performed across different countries

- Offer transparency and tractability
- Indisputable and immutable after finality

4.3. Digital Currencies

The invention of digital currencies has brought about the pressure of innovation in the fields of Banking, Payments, and Investments. To be considered a currency by the definition in economics, it must meet the following requirements [114]: *be a unit of account, a medium of trade, and a store of wealth*. Digital currencies are a form of money that are expressed as a string of bits transmitted as a message via a network that validates the message's validity using a variety of processes. Four classes of digital currencies exist: Cryptocurrencies, Stablecoins, Platform-based digital currencies(PBDC), and Central bank digital currencies(CBDC). Each variety has distinct benefits and drawbacks. To begin, cryptocurrencies are digital assets established on public and open blockchains that may be utilized similarly to traditional currency. There is no central authority in charge of currency supervision or regulation. The code is the law, and it establishes the laws governing the money. There are around 15,000 cryptocurrencies in existence as of December 2021, with a market valuation of $2.28 trillion USD [115]. The most well-known of these cryptocurrencies are Bitcoin and Ethereum. Although they are decentralized, allowing the blockchain's capabilities, their price volatility and market changes as shown in Figure 11 earn them a high level of public suspicion as a secure payment mechanism.

Stablecoins are an innovation that has emerged as a result of the aforementioned concern. Stablecoins are digital currencies that are tied to other assets such as cryptocurrencies, fiat currency, or commodities traded on exchanges. Typically, each stablecoin is backed by a collateralized reserve asset. Various approaches might be used to back stablecoins with other assets. As with Tether(USDT) [116], it might be a one-to-one mapping, where each USDT is backed by a genuine US dollar. As with Dai by Maker [117], it might be collateralized by a basket of cryptocurrencies. As price stability becomes an ever growing quality that investors seek out, some cryptocurrencies like Terra have opted to research and engineer price stability mechanisms built into the protocol inspired by government fiscal policy. Stablecoins have been compared to payment systems like as Venmo and Paypal [118]. The fees levied by these systems are significantly greater than the transaction fees offered by certain networks, such as Binance Smart Chain (BSC) [119]. Stablecoins can also be used as a bridge currency between cryptocurrency and fiat economies. Stablecoins have been critical in providing liquidity for both domestic and international payments. Stablecoins now have a market value of $183.37 billion USD as of 3 March 2022 (https://coincodex.com/cryptocurrencies/sector/stablecoins/, accessed on 15 March 2022).

Platform-based digital currencies (PBDCs) [120] are another type of currency that is exclusive to certain internet platforms such as Meta [121] and Amazon [122]. There may be a variety of defined procedures for users to acquire and trade this currency. These mechanisms vary according to business models. They are not linked to or denominated in national currencies. PBDC is a highly centralized with stringent restrictions on how the currencies may be utilized. The platform retains control, and users are not permitted to utilize these currencies outside of the platform.

Central bank digital currency (CBDC) is a digital version of a sovereign currency issued by the monetary authority of a state [123]. CBDCs can be classified as Wholesale CBDCs or Retail CBDCs [124]. Retail CBDC is a digital version of currency that is mostly utilized for personal and consumer transactions. Retail CBDC may improve user access and usability, lower the cost of e-commerce and cross-border payments. CBDC wholesale is a new infrastructure for inter-bank settlements, such as payments between banks and other companies with a direct link with the central bank. CBDC on a wholesale basis can help enhance inter-bank payment settlement, as well as mitigate the risks and costs associated with cross-border payment transactions. The design of CBDC should consider the following non-exhaustive key characteristics [125]: privacy, resilience, universal access

and security. It could support and credibly instill confidence in a thriving and competitive digital economy in a way private platforms may not be able; presenting a new compelling option. Since 2016, many central banks have been doing research in order to develop an effective CBDC prototype [124]. The state of efforts on designing CBDCs throughout the world is depicted in Figure 12. Not every effort is directed towards blockchain-based CBDCs. With its e-CNY initiative, the People's Bank of China is putting CBDC to the test [126]. The e-CNY is a prototype initiative that is being implemented in 10 regions around China. It was presented in February 2022 at the Olympic Games sites in Beijing and Zhangjiakou. An additional CBDC effort worth highlighting is Project Hamilton [127]. It is a digital currency initiative initiated by the Massachusetts Institute of Technology's Media Lab in partnership with the Federal Reserve Bank of Boston to construct a hypothetical CBDC (https://www.atlanticcouncil.org/cbdctracker/, accessed on 3 March 2022).

Figure 11. Bitcoin Price and Volatility (https://www.buybitcoinworldwide.com/volatility-index/, accessed on 3 March 2022).

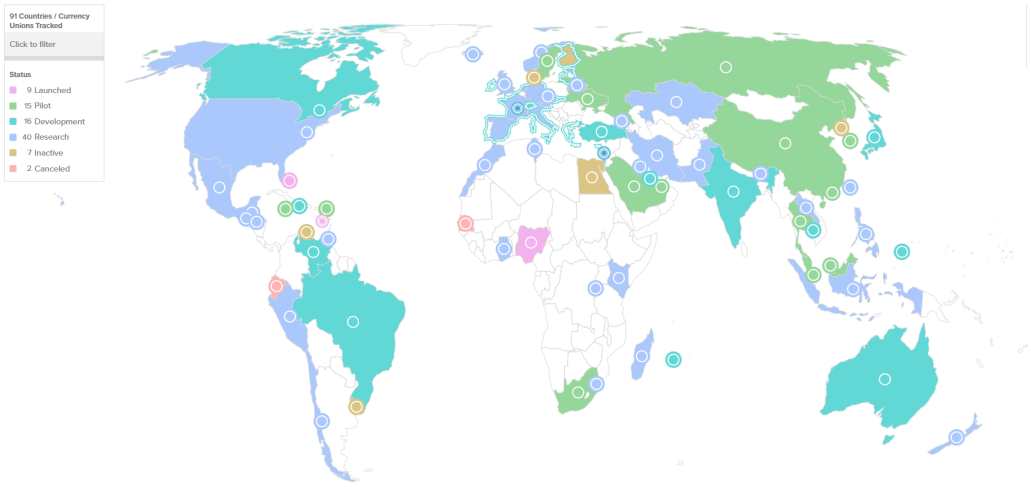

Figure 12. CBDC Tracker.

4.4. Investing

4.4.1. Decentralised Exchanges

A critical challenge that cryptocurrencies faced early on was the issue of centralised exchanges. Many pointed out and rightly criticized that how could the technology which constantly touted its decentralisation could be truly called as such if it relied on centralised

entities in order to purchase and sell. Thus many open discussions were held to solicit ideas from the community on how to build decentralised exchanges (DEXs). Overtime, it became abundantly clear that the issue was non-trivial. Some of the first iterations of DEXs resembled a mere replication of the traditional order book model [128] that most people who have a investment account would be familiar with. There would be two sides of the order book, a collection of bids of buyers willing to purchase a set amount at a set price, and a collection of asks of sellers willing to sell a set amount at a set price. An order would go through if either a buy or seller were willing to take the price set by the bids and asks. However, given the nature of transaction creation in the blockchain space, pending transactions would be totally transparent and be open to frontrunning, a typically illegal trading strategy that involves in exploiting and scalping the market to raise or decrease prices in the scalper's favour to the disadvantage of an honest buyer or seller.

Since it became clear that market makers would take advantage of this attribute of blockchains, an automated market making (AMM) mechanism [129] was introduced so that the decentralised exchange would be working with arbitrageurs to bring correct prices and benefits to the transacting parties rather than working against them. The first proposal for such a mechanism was called the constant product mechanism [130] which spawned numerous derivatives that are common place in liquidity pool and DEXs today. Uniswap [131], Sushiswap [132] and Balancer [133] are the three well-known protocols in the DEX ecosystem.

4.4.2. Decentralised Finance

Current consumers in the conventional financial ecosystem are unaware of the majority of accessible products and are unfamiliar with the laws governing these assets. Decentralized Finance (DeFi), often known as the lego of finance, provides the end user with the transparency, control, and accessibility that centralized finance lacks. Asset exchanges, loans, leveraged trading, decentralized governance, stablecoins, options, and derivatives are just a few of the items that fall under the DeFi umbrella. The previous subsection's discussion of decentralized exchanges falls within the DeFi taxonomy as well. Figure 13 illustrates the DeFi services and the market mechanisms introduced due to the underlying distributed database. We have already covered the concepts of Stablecoins and Decentralized Exchanges in the previous subsections. Below we define few other notable products under DeFi:

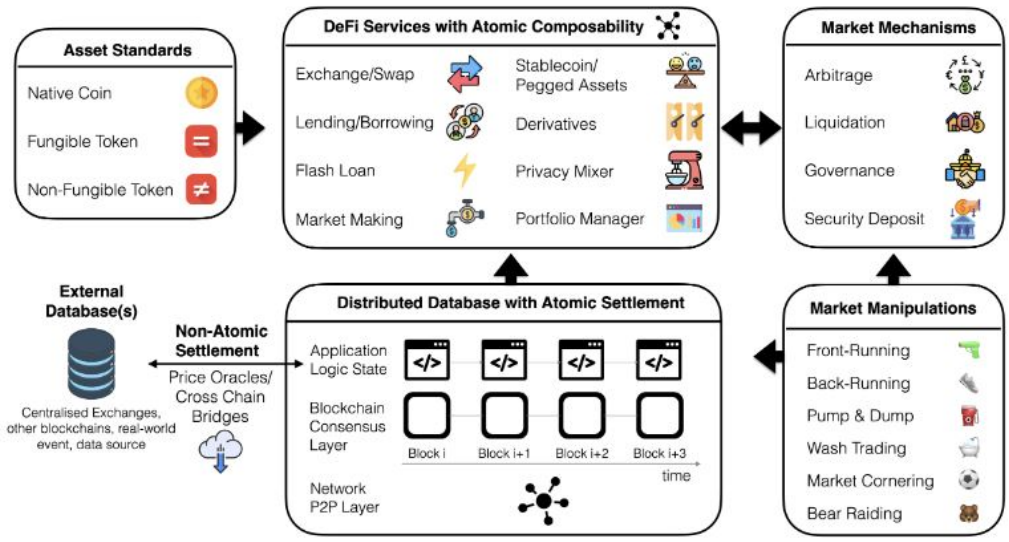

Figure 13. High-level DeFi Components [134].

Protocols for Loanable Funds (PLFs) Protocol Loanable Funds (PLFs) or Lending /Borrowing Protocols can be used to describe the way deposited funds in smart contracts are pooled and made accessible on distributed-ledger marketplaces for lending and borrowing. These PLFs can be further classified into over-collateralized loans and flash loans [135]. Over-collateralized loans in which collateral is needed to get a loan on an asset. The catch being the collateral is worth more than the loan itself. To compensate for the volatility of assets, the added value is often employed. In contrast, there is no collateral required for a flash loan. Flash loans [136] are those in which the loan is initiated to help bootstrap a chain of transactions that ensures repayment by the borrower in an atomic bundle of transactions. Compound [137], Aave [138], and dYdX [139] are three well-known protocols in the PLF market. Four factors differentiate these three protocols [140]: interest rate model, interest disbursement, governance token and the amount interest deducted to be place in reserve. The reserve component is there to be used during times of illiquidity.

Derivatives DeFi derivatives are smart contract-based services. Essentially, these are financial contracts that generate revenue dependent on the performance of the underlying assets. Assets may contain a combination of bonds, currencies, and interest rates. Synthetix [141], Nexus Mutual [142], and Erasure [143] are all popular protocols in the derivatives market. As of February 2021, the crypto derivatives market makes up for 57% of monthly volume [144].

4.5. Infrastructure/Value-Add Services

4.5.1. Decentralized Oracles

Blockchain networks are like closed circuits. All the data that smart contracts can be associated with is located and maintained by the nodes of the network. There is no way in-built into the protocol, as to how smart contracts can interact with external data as part of certain computations. Oracles are entities external to a blockchain network that can pipe information into the network as shown in Figure 14. The information can be relied upon based on the proofs submitted along with the data. Oracles have been classified based on different factors [145–147]: infrastructure architecture, data source, purpose of the oracle and based on design patterns. Depending on the choice of the oracle type, multiple protocols have been proposed [148–156].

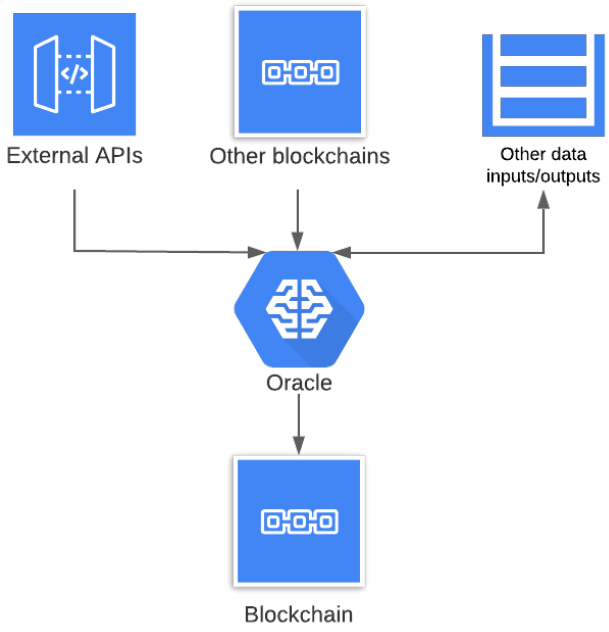

Figure 14. Blockchain and Oracles.

The induction of decentralization into Fintech space will bring in lot of dependencies on the existing legacy infrastructure. With the limitation of connectivity to external systems in blockchain, oracles will definitely play a key role. A secure, dependent, inexpensive and decentralized protocol for an oracle will become a basic need for this community.

4.5.2. Decentralized Storage

The internet generates massive amounts of data that is then served to the users from all over the world using multitude of services like cloud storage, peer-to-peer networks, intranet servers etc. When it comes to storage and retrieval of financial data it is crucial to maintain security, latency and availability at all times. Reliance on a centralized system will always have a backdoor through which an adversary can easily access and manipulate the data. Another evident issue with cloud storage is the concentration of few technology companies that have the capacity to build massive data centers. Due to this restriction, the cost around storage within these known servers increases with the space and availability requirements. Recently, with the inclusion of General Data Protection Regulation (GDPR) restrictions in some countries, the regulations around how and where to store the data are also changed. Data privacy is becoming a basic intuition needed when thinking about storage services.

Decentralized storage [157–159] is an option that can overcome the above mentioned constraints and is gaining momentum with the influx of blockchain use-cases. This enables trustless storage and allows for splitting the data and replicating the data across the world along multiple servers. These servers could be like a standalone user machine that is connected over a network with some pre-allocated hard disk space. The control of the data is not with the service provider anymore, rather with the user itself. Based on the persistence or incentive mechanisms used for data, different storage solutions have been proposed [160–166]. Below we present three popular storage systems on a high-level:

Filecoin: Filecoin [167] was created in 2017 by Protocol Labs, the team responsible for the InterPlanetary File System's inception (IPFS). IPFS is a decentralized peer-to-peer file system that enables the storage and distribution of data between peers. Filecoin is positioned on top of IPFS. It makes use of IPFS for storage. Filecoin's consensus process is known as *Proof of storage*. Consensus consists of two components: *proof of replication*, which requires miners to establish that they are storing legitimate data; and *proof of space time*, which requires miners to demonstrate that they are storing valid data for over certain period. The other component is evidence for the existence of space and time. The miners in this example exhibit the data's durability. They demonstrate how long they have been storing the data in this stage. Miners are compensated with FIL coins for storing data and mining proofs in the network. When saving data, there is no built-in encryption technique. Additionally, unlike other storage technologies, the data are not fragmented among different nodes. The files are stored on a single IPFS backend node as entire units. In 2020, Filecoin launched their mainnet.

Storj: Storj [164] is a decentralised cloud storage platform that was founded in 2014 leveraging Bitcoin. In 2017, Storj moved to Ethereum. Storj is currently on version V3, which was introduced in 2019. The Storj network is made up of three primary components: Storage Nodes—Servers that offer the ability to rent out extra hard drive capacity. Uplinks—Clients install the service on their PCs and use it to securely upload and download data. Satellites—Traffic mediators between uplinks and storage nodes. They segment and stripe the data for storage on the nodes. Additionally, the data may be copied across numerous nodes. Occasionally, if the data are too small, the satellites will store the data segments themselves. To retrieve and see data, clients must give the private key used to create the data upload. STORJ is the network's preferred method of payment. Users are rewarded for paying in STORJ since it enables them to get payment. The total quantity of STORJ tokens is 500 million.

Sia: Sia [161,168] is a cloud storage company that operates on a decentralised model. Its architecture is comprised of several components and roles. On a high-level, storage providers and hosts in the Sia network engage into a Sia File contract with storage renters. The contract may include expiration and other stipulations. Hosts are responsible for storing data and submitting evidence of storage to the blockchain on a regular basis. The data are distributed in fragments across different nodes on the network to increase reliability. Hosts need to buy in the storage, this allows for penalizing the hosts when they go offline. Compared to Storj, Sia has limited number of nodes. The blockchain stores only proofs. The hosts maintain the real data. Renters can validate the data's veracity using the proofs. Renters pay the hosts for the storage service, depending on the payment option chosen. Apart from the storage network, Sia just released *Skynet*, a layer 2 solution. Skynet operates as an application layer, allowing for the deployment of decentralised applications that interface with Sia storage. Siacoin is the token used in this network for rewards and payments.

4.5.3. Node-as-a-Service

In the Fintech ecosystem, even in centralized infrastructure settings, cloud service providers such as Amazon, Azure, or Google are relied upon. They generally do not host servers on their own, as this entails a significant amount of engineering effort in terms of upkeep. In the blockchain scenario, the network is composed of several types of nodes based on the server's capability. The majority of procedures fall into one of three categories: *Archive Node*—A node that maintains a history of data on the blockchain dating all the way back to the network's genesis block. *Full Node*—A node that may purge data on a periodic basis and rely on the Archive node to verify the legacy data. *Light Node*—A client-facing node that does not store data but communicates with the Full Node to calculate and deliver blocks to the Full Node for storage. Light nodes keep extremely low data due to the fact that their infrastructure may consist of devices such as mobile phones. The user interface of any network of decentralized apps will communicate with the nodes to obtain data from the blockchain. Depending on the storage capacity, experience, and level of control required for the application, clients can either self-host or use a *node-as-a-service (NaaS)* provider. By utilizing a NaaS service, the duty for maintaining the node is eliminated. The client is not concerned about storage, bandwidth, or technical effort. Although customers of this type of service must never reveal their private keys. Users can interact with their data using an API given by the NaaS provider. Numerous services have existed since the concept of NaaS was born. Alchemy [169], Ankr [170], BlockDaemon [171], and Chainstack [172] are just a few of the most well-known applications in this domain. They offer a variety of service kinds depending on their business models.

4.6. Online Marketplaces and Supply Chains

4.6.1. Online Marketplaces

Historically, markets had four objectives: *Match-making*—the process of connecting buyers and sellers; *transaction settlement*—depending on the goods or services exchanged between a buyer and seller, settlement may include payment or the exchange of another good or service; *service delivery*—the end result of a transaction settlement is the delivery of the product to the buyer; and *dispute resolution*—the crux of marketplaces is to provide a mechanism for resolving disputes between buyers and sellers. Since the dawn of the internet, centralized marketplaces have existed. The majority of these businesses rely on reputation as their trust mechanism, which presents a significant barrier to entry for new merchants or consumers. Additionally, there are several middlemen who exert influence over the marketplaces and operate in the system's favor. An example of this, is when an intermediary constantly connects with the highest bidding seller in order to benefit from the deal. Client privacy is not maintained in the centralized scenario as information is with a central entity. Payments could become a problem as well when interacting with sellers and buyers across border. Finally, there is the issue of terminating the marketplace, which

is not difficult to do when everything is controlled by a small number of intermediaries. Figure 15 lists the major differences between centralized and decentralized marketplaces. Decentralized marketplaces are another intriguing application of blockchain technology. Figure 16 depicts a prototype architecture and the players that can engage in each of the marketplace's fundamental operations. The usage of smart contracts in this design highlights how each function may be decentralized and facilitated by blockchain technology. Additionally, the network as a whole is not controlled by a single intermediary. A simple example for blockchain based marketplace is where a seller uploads the good information on to a smart contract and a buyer will have transparent interaction as to the purchase using the data shown and the infrastructure itself can be used for payments.

Marketplace Feature	Blockchain-Based Decentralized Marketplace	Traditional E-Marketplace
Trust through contract enforcement	Distributed validation, including proof-of-work mechanisms or proof-of-stake mechanisms. The network enforces the contract between seller and buyer. The network validates reputation ratings, including reviews and feedback mechanisms.	Third parties (such as a bank, certifying authority, promissory note, transfer systems, or other forms of contractual mechanisms). Usually controlled by the firm. Potential for significant alteration.
Transaction time	Can be instantaneous due to fast network validation. Delays can be mitigated using proof-of-stake/ proof-by-consensus algorithms.	Promissory note, letter of credit, or acceptance of credits that can take a long time.
Value	The network can reward participants with tokens or by accepting third-party tokens.	Banking systems (such as national exchanges, currency, and underwriters).
Privacy and security	Identity is not disclosed on the network. Tracking transactions can be facilitated, though with difficulty. Transaction details can be hidden behind layers of encryption. Cost of tampering with the network's validation mechanism is high.[a]	Identity fully disclosed in the marketplace. As secure as the network's components.

[a] To break the network's validation, an attacker would have to be able to control >50% of the network's hash power, involving a huge economic cost in case of proof-of-work validation mechanisms.
For proof-of-stake or proof-by-consensus mechanisms, tampering with the network's validation represents an economic disincentive.

Figure 15. Marketplace Comparison [173].

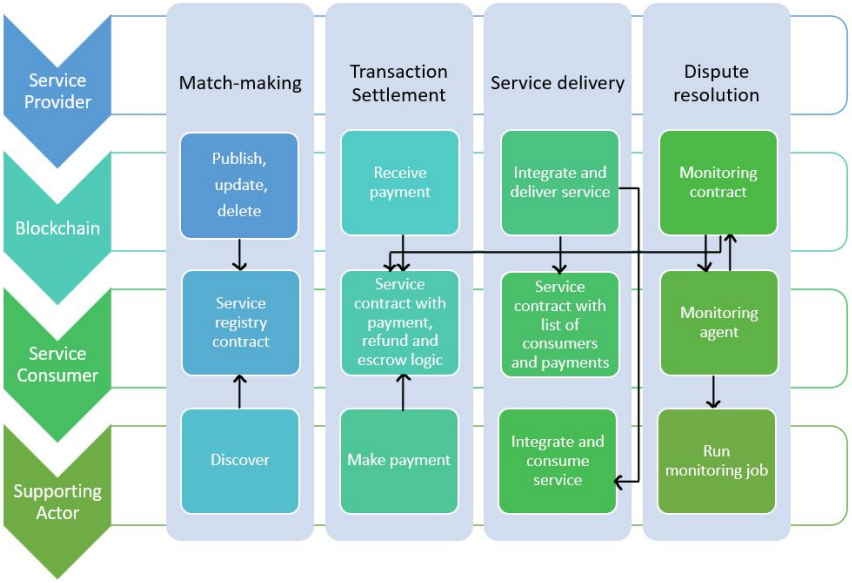

Figure 16. Roles and Functionalities of a Decentralized Marketplace [174].

Different sorts of marketplaces exist. There are two notable use cases for marketplaces in terms of decentralized options:

Prediction Marketplaces This is a fascinating application of markets. This is a market for the purchase and sale of future contracts on binary events. They are often arranged so that they charge between $0 and $1 depending on the result of an event. Both good and bad consequences can be bought into by participants. Additionally, blockchain has several benefits in this circumstance. The first is opposition to censorship. There is no regulation that could be instituted by organizations. The other significant advantage is that it is accessible to individuals. Anybody may create a market and participate as a buyer or vendor. Oracles, as described previously, serve a critical role in linking the marketplace to the conclusion of non-blockchain events. In this example, Augur [154] and Gnosis [175] are two major initiatives.

Data Marketplaces The current generation is based on the exchange of massive volumes of data. This interaction might take place between individuals, between individuals and devices, or between devices and devices. A decentralized data marketplace may foster openness, integrity, and privacy, all of which are critical in this circumstance. Numerous prototypes [176–178] for data marketplaces are being developed, the majority of which will include Internet of Things (IoT) devices.

4.6.2. Supply Chain Finance

The 2008 global financial crisis exposed numerous vulnerabilities in supply chains and associated capital management. During this time period, interest in Supply Chain Finance (SCF) began to grow. SCF [179] is the process of optimizing financial structures and processes within the supply chain ecosystem. The optimization process is primarily concerned with managing the working capital and liquidity associated with corporate institutions' supply chain procedures. The basic flow of SCF is depicted in Figure 17, along with the parties involved. SCF enables risk management by facilitating the management of cash flows between customers, suppliers, and service providers.

As illustrated in Figure 17, there is a high degree of reliance on intermediates such as SCP Platform and lead financial institutions. This is where the application of blockchain technology becomes apparent. The incorporation of Blockchain technology into the SCF workflow benefits significantly in two ways [180,181]: it eliminates information asymmetry and enables traceable and tamper-proof systems to detect irregularities and anti-counterfeit challenges. Without the requirement for an intermediary, all components such as cash flows, information flows, payment exchanges, and invoice exchanges can be enabled on blockchain. Table 5 summarizes several well-known ventures, their underlying platform, and some of the specifics of their objectives, business strategies, and participants.

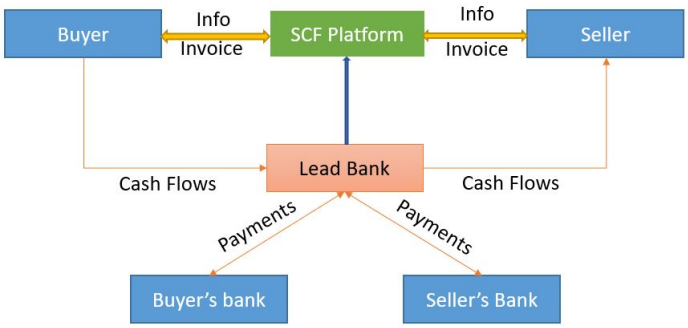

Figure 17. Workflow of SCF.

Table 5. A Summary of SCF Blockchain companies.

Company	Platform	Summary
Contour [182]	R3 Corda	Rebranded from Voltron, targetted towards letters of credit usecase. Revenue model will include monthly subscription fees and transaction fees in the platform. Participants in the network currently include: Bangkok Bank, BNP Paribas, CTBC, Citi, ING, HSBC, SEB, and Standard Chartered.
Skuchain [183]	Hyperledger Fabric	Provides end-to-end solution for supply chain finance and not restricted to a particular usecase. Firms pay subscription and transaction fees for using the platform. Currently, the platform is operating across countries including USA, Asia, Europe etc., It is fully interoperable with Corda and Ethereum.
eTradeConnect [184]	Hyperledger Fabric	Operated by the Hong Kong Trade Finance Platform Company Limited. Offers multiple products for SCF including purchase order and invoice creation, pre-shipment trade finance and post-shipment trade finance. Current participants include various banks from Australia, Hong Kong and Asia.
komgo [185]	Quorum blockchain	Around 150 companies are using this platform. Along with SCF solutions this platform also offers Know-Your-Customer(KYC) and certification feature. They generate revenue through subscription fees and professional services charges for activities like integration.
Marco Polo [186]	R3 Corda	Is a network for SCF consisting of over 30 banks globally. The platform is compatible with APIs and legacy systems allowing banks to easily integrate. Marco Polo operates following a license and transaction fee model.
UAE Trade Connect [187]	Hyperledger Fabric	8 banks participated in the product launch. UAE Trade Connect addresses several of the issues with duplicate and fraudulent invoice financing that have posed considerable problems to banks in the industry.It will generate revenue by charging banks for each transaction that they verify.
We.trade [188]	Hyperledger Fabric	Through a license fee and transaction fee model, we.trade currently has a number of products that are live, including: Auto-Settlement: automation of payment based on pre-agreed conditions; Bank Payment Undertaking (BPU): confirmation of buyer's bank to make a payment to the seller; BPU Financing: a financing option for the seller based on the BPU; and Invoice Financing: a financing option for the seller based on a single sales invoice.

4.7. Corporate Governance

Corporate governance [189,190] is primarily concerned with the administration of an organization's economic and social objectives. Engagement of stakeholders is critical in this scenario. Although corporate governance has existed for a long period of time, it continues to face numerous fundamental issues. To begin, businesses can profit from short-term fluctuations in share prices and accounting methods. Several instances include violations of ethics, lack of openness, and conflicts of interest. For shareholders, issues arise around accountability and ownership transfer, which are frequently associated with expensive costs. In terms of decision-making, present procedures rely heavily on manual processes, making it easier for actors to be persuaded and collude in order to commit systemic malpractices. This is where blockchain enters the fray. Blockchain has completely transformed the field of governance. Multiple governance mechanisms have been established at various levels of the blockchain architecture, which enables corporate governance structures to be executed on these platforms. As indicated in Figure 18, governance can be achieved at the application level through the use of smart contracts and at the protocol level through the use of access control. We have discussed in detail the access control techniques at the protocol level in

Section 1.2 and some of the platforms that implement these mechanisms in Section 3.3 under classification of blockchain platforms. Below we cover on the application level options.

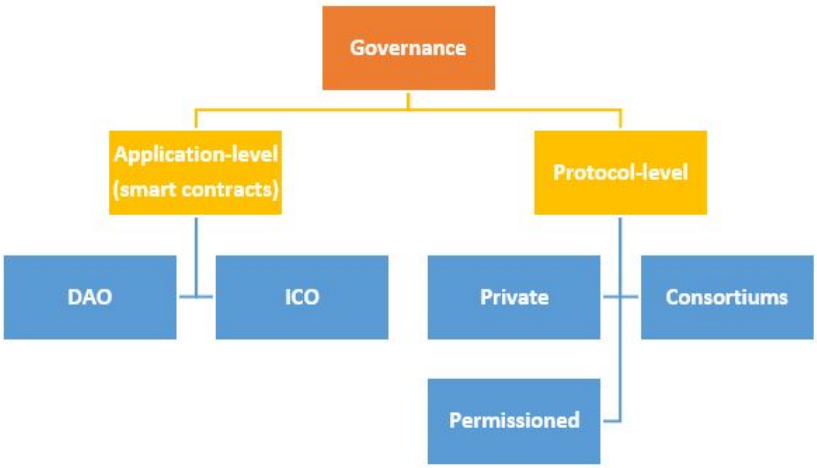

Figure 18. Blockchain and Governance.

Initial Coin Offerings (ICOs): Initial coin offerings (ICOs) are a method of issuing assets on the blockchain as tokens. These assets can be used to raise funds from investors or to distribute shares among an organization's stakeholders and management. The initial coin offering (ICO) was created as a decentralized alternative to the first public offering (IPO). Table 6 summarizes a number of the analogies that may be made between ICOs and initial public offerings. Due to the intrinsic advantages allowed by the usage of the blockchain layer, ICOs primarily facilitate more transparency in terms of ownership and real-time accounting.ICO tokens can be classified into multiple types which include the following: *Security tokens*—Tokens that represent an organization's shares and are issued as an investment vehicle. They are regulated similarly to conventional securities. *Utility tokens*—Rather than ownership in the organization, these tokens provide owners with preferential treatment and access to certain specified items. The goods could be software packages or a platform for software as a service. *Payment tokens*—These are intrinsically valuable tokens, comparable to cash, that can be used to purchase and sell goods and services. Figure 19 illustrates a few initiatives for each type of token (https://medium.com/swlh/types-of-tokens-the-four-mistakes-beginner-crypto-investors-make-a76b53be5406, accessed on 3 March 2022).

Table 6. IPO vs. ICO [191].

	IPO	**ICO**
Legal status	Detailed regulation	No regulation or insufficient one
Securities type	Stocks and bonds	Tokens that may have features of particular types of securities or being vouchers or having no additional attributes at all
Risk level	Moderate	High (for the company and investors)
Accessibility	For large enterprises, For investors	May be used by almost any company. Anyone who have internet access can become an investor
Costs	High	Moderate or low

Figure 19. Types of Tokens.

Decentralized Autonomous Organizations (DAOs): DAOs [192,193], which were first proposed in 2016, are governance structures that can incorporate not only mechanisms for participant financing maintenance, but also code-formulated and automated governance rules into the system via software code. One of the primary uses of smart contracts is to enable the implementation of DAOs. By utilizing their tokens, investors and shareholders can participate in significant decisions. Additionally, these decision-making procedures can be achieved through the use of voting or auction systems. DAOs can be configured to provide a variety of functionalities, depending on the business model of the organization. A word that is often used in conjunction with DAOs is Decentralized Autonomous Corporation (DAC) [99], which is used to refer to corporate governance. While DAOs are more akin to public blockchain scenarios, DACs are more akin to shareholder dividends. With the growing interest in DAOs, a trend known as DAO as a service has emerged. These systems enable the automated construction of DAOs on blockchains with customized functionality. Users that lack the necessary skills or experience in terms of smart contract development can use these platforms to immediately construct their own DAOs. They can create DAOs by modifying existing DAOs. Aragon [194], DAOStack [195], and Colony [196] are the primary platforms in this. The following Table 7 summarizes a few high-level details about these initiatives.

Table 7. Comparison between DAOs.

Platform	Launch	DAOs	Token	Market Cap	Features
Aragon	Oct 2018	1700	ANT	$ 3 billion USD	• Tool to create and participate in DAOs • Large network of DAOs • Non profit organization to distribute network tokens • A system to resolve disputes
DAOStack	Apr 2019	22	GEN	$ 1.6 million USD	• Holographic consensus mechanism • Asset management services • Modular smart contract framework • Javascript development environment • Friendly user interface
Colony	Jan 2022	-	CLNY	-	• Mainnet launched very recently • Reputation mechanism • Token creation and distribution • Gasless transactions • Lazy consensus

4.8. Crowdfunding

Crowdfunding is another area in which substantial sums of money are transferred. In general, crowdfunding [197] is the process through which an individual, a group of individuals, or an organization solicits cash for a specific cause via an internet platform. Michael Sullivan coined the word crowdsourcing for his fundavlog project (https://socialmediaweek.org/blog/2011/12/a-social-history-of-crowdfunding/, accessed on 25 February 2022). Globally, crowdsourcing generated approximately $5.5 billion USD in 2017 and $10.2 billion USD in 2018. According to the Global Crowdfunding market study 2022 (https://www.marketwatch.com/press-release/crowdfunding-market-by-growth-opportunities-2022---top-key-players-analysis-by-demand-status-industry-size-and-share-forecast-with-covid-19-impact-analysis-on-regional-trends-2024-2022-03-07), accessed on 25 February 2022, it is predicted to grow at a continuous rate of 18 percent, reaching $124.85 billion USD in revenue. According to the report, a significant driver is the rising use of social media platforms for free fund raising efforts and the increased accessibility to cash enabled by technological innovations such as blockchain. Numerous market models [198] have been employed throughout crowdfunding's history. Certain models are investment vehicles, which implies that investors can anticipate receiving a portion of the earnings generated. Other models include non-investing, which refers to non-profit endeavours that cannot be anticipated to generate a profit for investors. The four most often used business models in crowdfunding are as follows: *Lending-based Crowdfunding*—This funding strategy entails lenders and borrowers as participants. They can communicate directly with one another, eliminating the need for an intermediary. This is an investing model in which the lenders' loans will be repaid. LendingClub [199] is a good illustration of this strategy. *Donation-based Crowdfunding*—This is a non-investment paradigm in which individuals can raise money for a cause by using online platforms. Individuals interested in assisting social initiatives can use GoFundMe [200] to create a crowdfunding request and raise funds. *Equity-based Crowdfunding*—Intended mostly for small businesses and start-ups willing to distribute a portion of their ownership to investors as equity. AngelList [201] is an illustration of this model. A non-profit organization that connects entrepreneurs and angel investors. Finally, *Reward-based Crowdfunding* is a viable option. As the name implies, the platform will provide some type of compensation in exchange for the funds. The benefits may be proportional to the amount contributed: the more the contribution, the greater the reward. Kickstarter [202] is a fine example of this model. Individuals that contribute to a project can be set up to get rewards at multiple tiers, and the project creator can choose the reward model.

Traditional crowdfunding sites charge a fee for connecting fundraisers with investors or donors. These platforms operate as intermediates, and due to the centralized control, numerous scams are possible. In 2005, amid Hurricane Katrina's aftermath, more than 2400 malicious websites defrauded donors of millions of dollars [203]. To avoid these types of scams and ensure the crowdfunding process is conducted transparently, blockchain technology can be used as the technology provider. There is no middleman, and the platform is entirely governed by code. Anti-fraud, anti-tampering, and a decentralized ledger system are all characteristics that would be incorporated [204]. Additionally, the platform can connect worldwide players regardless of the underlying local currency. There are 181 cryptocurrency-based crowdfunders worldwide (https://tracxn.com/d/trending-themes/Startups-in-Crypto-Crowdfunding, accessed on 3 March 2022). Table 8 summarizes the top five projects.

Table 8. Top 5 Blockchain Crowdfunding Platforms.

Name	Launch Year	Summary
RealBlocks [205]	2015	RealBlocks is a decentralized platform built on distributed ledger technology which enables retail and institutional investors to invest in real estate projects. Tokenizes the physical assets and thus allows retail investors to own a part of the project.
Meridio [206]	2017	Meridio is an online crowdfunding platform for real estate investments. The SaaS solution uses blockchain based technology to convert individual properties into digital shares. Investors can directly connect with landlords by circumventing all traditional intermediaries and co-own properties. The company claims to verify all investors and properties registered on the platform.
QuantmRE [207]	2017	QuantmRE is an online crowdfunding platform based on blockchain technology. It enables property owners/investors to create a portfolio of assets, receive investments from other investors, and more. It enables homeowners to gain additional value of their homes by enabling others to invest in it. Investors can purchase tokens to begin the process.
Gitcoin [208]	2017	On-demand requirement for open source software development. Features of gitcoin are fund issues, tip developers, project search, gith hub integrations, and hackathons. It allows freelancers to work on Python, Rust, Ruby, JavaScript, Solidity, HTML, CSS, and Design.
Brickblock [209]	2016	Brickblock claims to be creating an investment platform that allows individuals to invest directly into ETFs and real estate funds using their cryptocurrency balances. The goal of the project is to create a system that facilitates cross-border investments and access to capital markets round the clock. Enabled by smart contracts, the platform will allow routine dispersion of dividends, reduce entry barriers in terms of paperwork and foreign exchange, and function relatively transparently.
RealtyBits [210]	2018	It is one of the decentralized crowdfunding platforms that allow investing in American commercial real estate. Real estate investment funds are raised via verified investors. It uses RBX tokens to raise its fund and make investments.

5. Open Research Challenges

Until now, we have talked about the benefits, advantages, and many use cases that can arise from the properties of blockchain. Despite this, the blockchain/DLT ecosystem still faces a number of outstanding research topics and problems. With the proliferation of applications in both the public and private sectors, these issues are only going to becoming more difficult to solve. Scalability, security, and decentralization were the three pillars of the Blockchain Trilemma [211,212] when it was first proposed. The blockchain trilemma basically argues that we must make trade-offs while choosing one of the three primary aspects of blockchain. However, with the expansion of use cases, we can now add other categories to this framework and no longer have a Trilemma. These concerns can be broken down into a number of categories, as shown in Figure 20. All of these topics are covered in depth in this section.

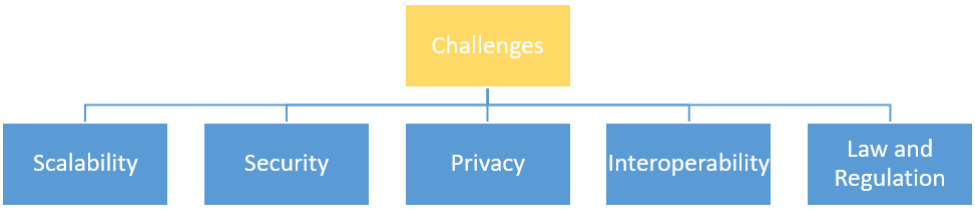

Figure 20. Challenges in Blockchain/DLT ecosystem.

5.1. Scalability

Scalability [213,214] is a primary objective when involving Fintech. The network must be scalable and self-sustaining in terms of transaction volume. Visa currently processes approximately 1700 transactions per second. In comparison, Bitcoin and Ethereum currently handle 7 and 15 transactions per second, respectively. This is the polar opposite of what the existing financial system requires. According to the architecture of the blockchain platform, we can evaluate scalability limitations at several levels, as seen in Figure 21.

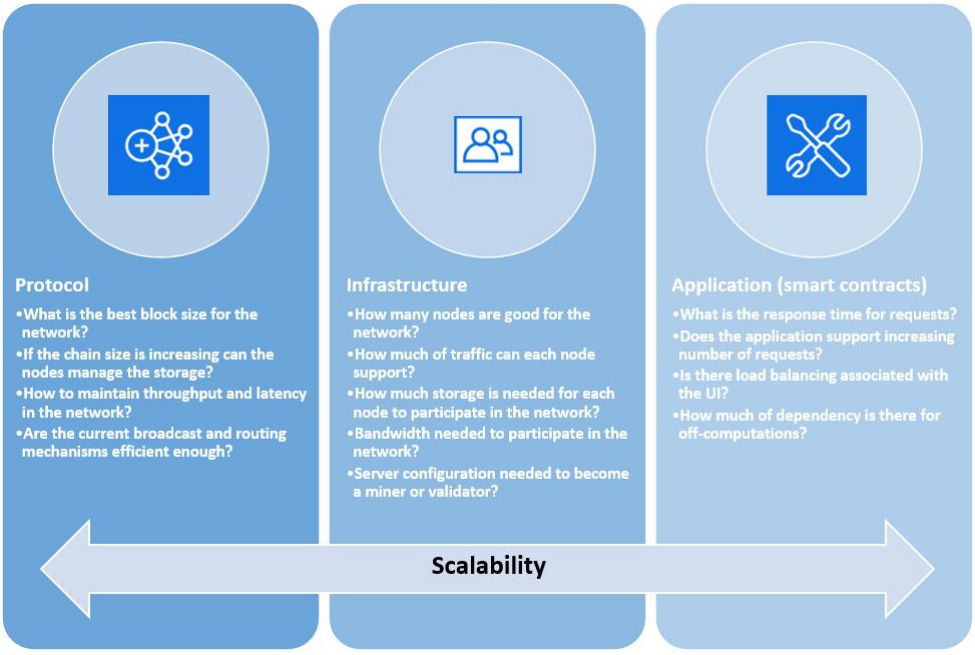

Figure 21. Open Research in Scalability.

To begin, we shall consider protocol-level difficulties. Because the block size is currently limited, if the network experiences an increase in transactions, either the block generation rate (which is determined by the consensus method) or the block size must be increased. Increasing the block size incurs additional processing node overhead and is dependent on network bandwidth. In any situation, the chain size would grow in lockstep with the number of transactions in the network, increasing the required storage capacity on the node. On the other hand, decreasing the block size results in more forks as blocks are generated more quickly. The other constraint is latency. Latency is the time difference between the input and output; a short latency is always preferred. For example, due to the consensus constraints imposed by bitcoin, it takes at least six blocks to confirm a transaction, which means it has been accepted by all miners and is on the longest chain. This will obstruct network scalability once more.

Increasing the number of nodes at the infrastructure level, as in centralized networks, is not a possibility. Increasing nodes stabilizes performance for POW mechanisms, but degrades performance for BFT mechanisms. In terms of chain size, bitcoin now requires

more than 100 GB of storage and this will continue to grow over time. Miners and validators must have access to this type of storage capacity. They must take into account the network speed in order to process gossip-protocols efficiently.

Finally, at the application level, depending on the frameworks used for the user interface, requests from the front-end must be managed in such a way that the program does not become unresponsive as the number of requests grows. For managing incoming data requests, multiple load balancing approaches should be considered. The second concern is nodes' reliance on off-chain computation. If nodes in the network are unable to do sophisticated computations, reliance on off-chain data rises, potentially increasing delay. Several open research questions (ORQ) in this functional area include the following:

ORQ1: How should we design scalable protocols from the ground up when developing a blockchain-based financial services platform?

ORQ2: Which characteristics (block size, network size, etc.) should be used to ensure that a network maintains consistent throughput and latency?

ORQ3: What is the optimal throughput and latency required for a financial application to run on blockchain?

ORQ4: How much centralization should be permitted (if scalability is increased) while using blockchain in enterprise scenarios?

ORQ5: On which layer of the architecture should we place a premium on scalability? Is it Layer 1 (at the protocol-level) or Layer 2?

ORQ6: Is reliance on multi-layered architectures a disadvantage, or is it more beneficial for the community to host a variety of applications?

5.2. Interoperability

With the proliferation of blockchain platforms and the variety of implementations inside these platforms, there is still a communication gap between them. Many of these platforms are application-specific, which contributes to the communication difficulty. Interoperability refers to a platform's capacity to communicate and exchange data with other platforms. As a result, the interoperability challenges can also be mapped as a trilemma [215], as illustrated in Figure 22. A trade-off must be made between the three variables—trustlessness, extensibility, and generalizability—to determine which two qualities are crucial for the network. The term *trustlessness* relates to ensuring that the underlying domains keep the same level of security. *Extensibility* is a term that refers to the capacity to accommodate numerous domains. The capacity to support cross-domain applications is referred to as *generalizability*.

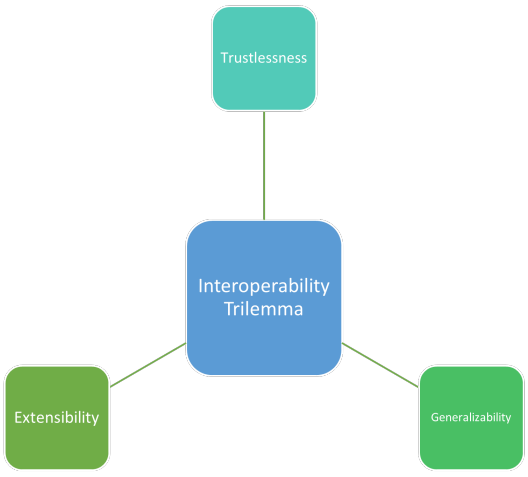

Figure 22. Interoperability Trilemma.

The following are some of the open research questions (ORQ) in this field. **ORQ1–ORQ4** are questions about communication between platforms with varying degrees of trust. **ORQ5** and **ORQ6** address platform-specific concerns. **ORQ7–ORQ9** raise concerns about accessibility and usability.

ORQ1: How do we transfer data between platforms while maintaining an identical level of privacy and security?

ORQ2: How can we ensure that data are valid across platforms?

ORQ3: What safeguards and protocols should be used when communicating between public and private/consortium blockchains?

ORQ4: What are the dangers associated with implementing interoperability between platforms with varying degrees of trust?

ORQ5: If the platform is application-specific, for example, supply chain blockchain, how do you transfer data in a way that other platforms can interpret it?

ORQ6: Using financial services as an example, how do you model the value of assets across numerous platforms?

ORQ7: From a programming standpoint, how can we execute a smart contract developed for one platform on another?

ORQ8: How can developers compete in terms of becoming familiar with the semantics of many platforms that use different languages?

ORQ9: In terms of usability and accessibility, is the end-user experience consistent across platforms?

5.3. Security

As any computer system, blockchain systems, built on distributed networks could be vulnerable to cyber-attacks. As shown in Figure 23, security threats to a blockchain could be classified in the three following groups:

1. **Threats to protocols**: A security breach in this group would impact the system integrity. Depending on protocols that drive system and network behaviors, hackers could be able to fork the blockchain, perform unauthorized transactions, double-spending, violate the privacy, etc. Threat targets include the following:
    - **Consensus mechanisms**: The integrity of an blockchain relies on the assumption that the majority of miners are honest in mining and in maintaining the network. In the proof-of-work (PoW), if there is a chance that the majority of the miners are colluding together, these miners would be capable of compromising the integrity of the transactions. An successful attack against consensus mechanism provably the most harmful to the system. The study of effective and secure consensus mechanisms is still a open problem.
    - **Cryptographic algorithms**: While blockchain can provide the tamper-proof of transactions due to the use of cryptographic hash functions, attackers are still able to exploit other vulnerabilities. A collision in the hash functions could allow a malicious adversary to replace or modify the input data without changing its digest. A signature forgery could lead to unauthorized transactions. A security breach in other asymmetric cryptographic algorithms, such as ring signatures, zero-knowledge proofs or homomorphic commitment will result in loosing confidentiality and privacy. Last but not least, practical quantum computers would break all cryptosystems based on integer factorization and discrete-logarithm.
    - **Smart contracts**: Since smart contracts are encoded as a part of a "creation" transaction, and written on the blockchain, it is difficult to update. In case a vulnerability is exploited in a smart contract, a malicious adversary could gain profit without respecting agreements between related parties.

- **Virtual machine**: As this platform provides an execution environment for smart contracts, vulnerabilities exploited also allow a malicious adversary to gain profit without an agreement from related parties in the smart contracts.

2. **Threats to networks**: Various kind of attacks against networking services exist. For instance, Ethereum suffered a DoS attack in 2016 (https://blog.ethereum.org/2016/09/22/ethereum-network-currently-undergoing-dos-attack/, accessed on 2 February 2022). In Dos attacks, an attacker will flush data to a node. This may make the node cannot process normal transactions, that is, aims at the availability of a system. Other network attacks could be carried out on the node routing table or note identity. Designing and provisioning a secure blockchain-based Fintech system against network attacks is crucial.
3. **Threats to data on the blockchain**: Users' addresses, data transactions, digital wallets, smart contracts, etc. are visible to all participants on the blockchain system to some extent. A blockchain-based system must provide security features to the data, including its *integrity*, *confidentiality* and *availability*. Loosing private key is a significant security concern of participants on the blockchain as without his private key, a participant will have no longer control on his digital assets on the blockchain. Loosing could be caused by a carelessness or by a compromised device holding the digital wallet. How could we design a user-friendly, but digital wallet?

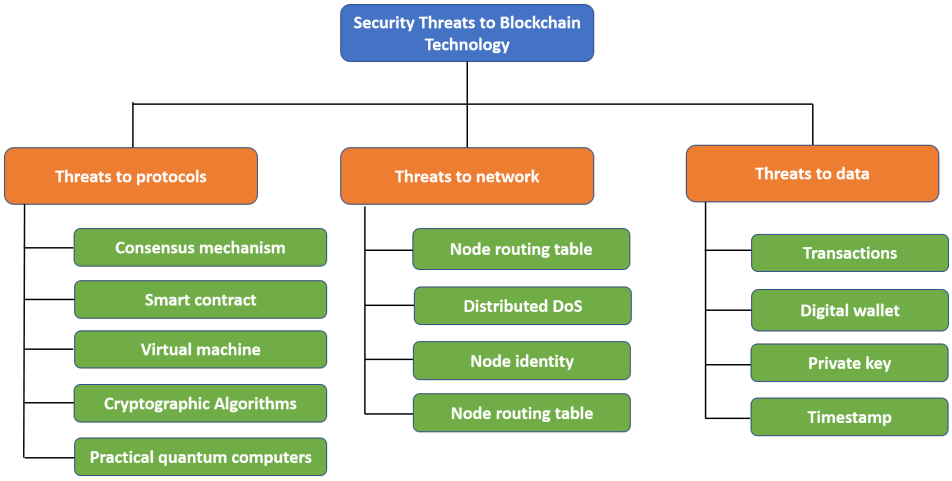

Figure 23. Security Threats to Blockchain Systems.

The following are some of the open research questions (ORQ) for the security in blockchain systems. While the first two questions are related to public blockchains, the last three questions are for private blockchains.

ORQ1: How can a public blockchain network detect false network identities to prevent Sybil attacks?

ORQ2: How can a public blockchain network provide the confidentiality of blockchain's data?

ORQ3: How do we provide the same level of security in a private blockchain compared to the public blockchain networks with a higher level of decentralization?

ORQ4: How does a private blockchain network provide a secure access control?

ORQ5: How can we prevent double-spending in private blockchains, where transactions are not publicly verified?

5.4. Privacy

The term *privacy* refers to the fact that transactions on the blockchain do not reveal the sender, receiver, or even the content (e.g., amount) of the transaction. For enterprise

blockchains, which are typically permissioned, there is a greater emphasis on privacy, as corporations value the ability to keep their business activities private. On the other hand, public blockchains emphasize openness as a key characteristic that enables auditability. However, users still value the ability to keep information that is non-relevant to the transaction private, such as their identity. Numerous privacy protocols, like as Zcash [79] and Monero [77], have developed a variety of (non-)cryptographic techniques for entirely anonymizing transactions, such as ring signatures, homomorphic commitments, zero-knowledge proofs, etc. Certain protocols require users to interact with networks via specific anonymizing communication protocols such as Tor [216]. By now, privacy remains subject to numerous research obstacles. There are two main concerns around privacy for users: identity privacy and transaction privacy. The term *identity privacy* refers to the practice of maintaining related participants' information without disclosing it to unauthorised third parties. The term *transaction privacy* relates to the specifics of the data or quantity transmitted between network users.

On the one hand, cryptographic protocols are able to provide computationally perfect privacy as long as the private keys remain secret. On the other hand, in order to comply with regulations in Fintech industry, for example, Anti-Money Laundering and Financing of Terrorism (AML-CFT), when required, the transactions' information must be revealed to authorized agencies. Solving this dilemma is still open to the research community.

In terms of privacy, there are two major considerations:

De-anonymization De-anonymization [217] is the process of evaluating a network by monitoring transactions between accounts and deducing information about account data. This can be accomplished by performing a static analysis of the network information included in a blockchain.

Transaction Fingerprinting By doing cluster analysis on the user information on a network, transaction behaviors can be retrieved. Numerous attributed, such as random time interval (RTI), hour of the day (HOD), time of the hour (TOH), time of the day (TOD), coin flow (CF), and input/output balance (IOB), are available to consider the transaction information [218].

The following are some of the open research questions (ORQ) in this field.

ORQ1: Many contracts performed in a business context is done in confidence. How can we implement private smart contracts?

ORQ2: How can we perform an KYC/AML compliance in blockchain-based Fintech applications whilst offering users and transactions privacy?

ORQ3: How can blockchain-based Fintech applications comply with privacy requirements such as the right to be forgotten, or other data rights under the GDPR framework?

ORQ4: The current cryptographic primitives being used to ensure privacy such as Zero-Knowledge Proofs or special signatures are not suitable for use in a tap-pay user experience. Can we design efficient cryptographic algorithms for low resource devices?

5.5. Law and Regulation

Dealing with legal and regulatory frameworks is a critical challenge when incorporating innovative technologies into financial services. In general, it takes a long time to develop solid and reliable legal and regulatory policies. This is especially critical when traditional systems are being disrupted by innovations such as blockchain. It is necessary to set new standards guiding the rules and regulations governing technology. The key selling point of blockchain is that it eliminates a large number of intermediates, which means that the structures that these intermediaries had influence over will no longer exist. As a result, it is critical for Fintech to include legal and regulatory study alongside technical issues. The following are possible classifications for open research challenges in this area:

Inter-Continental

- Due to the fact that blockchain applications span multiple countries, legal and regulatory requirements within those countries may become ineffective.
- Financial services have a tendency to migrate to less restrictive jurisdictions when they are prohibited in one. If there are no legal safeguards in place for these scenarios, it will be hard to manage hostile activity.
- At the moment, the majority of designs being offered are being tested in siloed environments, which do not fully simulate working with many entities.
- When it comes to payments, states and governments must collaborate to develop shared regulatory sandboxes in which new technologies can be tested. Particularly for use cases such as cross-border payments, it is critical to thoroughly examine the risks associated with employing blockchain as the underlying technology.

National

- Numerous usecases for blockchain are being evaluated within country-specific regulatory domains, but again, this is limited to usecase-specific circumstances.
- Users must be assured of the stability of the system under consideration. This is because the majority of blockchain applications entail high-value transactions.
- Priority should be directed to educating the public on both the benefits and risks. For instance, when customers register with centralized exchanges, are they aware that their private keys are not in their control?

Domain-Specific

- When code becomes law, it is critical to understand how difficulties should be handled when the semantics of code are not specified and learned uniformly by all.
- Within specified areas, a mechanism for incorporating legal documents into the code should exist. R3 Corda is the more well-known protocol that implements this concept. However, this should be consistent across platforms.
- Multiple protocols may be working to improve processes within a single domain, and we have identified interoperability as a critical topic of research. If the platforms are distinct, how are compliance and regulatory challenges addressed? Is there a standardized legal template to which all of these platforms can relate is a critical research subject that has to be addressed.

The following are some of the open research questions (ORQ) in this field.

ORQ1: Can smart contracts' compliance and adherence with local regulations be validated?

ORQ2: How can compliance and regulatory challenges be handled across different platforms that are bridged together?

ORQ3: How should legal disputes be handled if a platform spans across jurisdictions that have legally divergent consequences?

6. Conclusions

The fintech ecosystem is always evolving into new regimes. Blockchain/DLT is here to stay and is gradually permeating all facets of society. We have discussed in depth all of the fundamental principles necessary for comprehending the technology underlying blockchains. We established a taxonomy of blockchain platforms based on the categories of distributed ledger technologies and the most widely used platforms within each group. We then have extensively covered the use cases for each of the Fintech ecosystem's verticals. These use cases are prevalent in public blockchain ecosystems and are upending established financial transaction protocols. As said previously, blockchain also has a slew of challenges due to the fact that it is still in its infancy, at least in enterprise contexts. We discussed open research problems related to all parts of blockchain and Fintech.

As a result of our study, we hope to reorient Fintech firms toward the critical obstacles that remain unsolved in Blockchain for Fintech applications. Due to the fact that this

involves financial services and has the potential to cause irreversible damage both nationally and internationally across multiple industries, we must pay close attention to performance, security, and privacy concerns. In terms of performance, we should strive to create a system that is more efficient than the current system. That is a significant improvement over the current state of blockchain technology. Criminal activity and hacking should be regulated, which has been a primary objective of financial regulators. With the addition of blockchain, it remains to be seen if this provides a more robust regulatory framework or creates further loopholes for bad actors. Finally, we need to instill customer confidence in blockchain technology, which is another difficult task given the prevalence of security and privacy concerns across key blockchain platforms.

This work will present an overview of the Fintech ecosystem and the topics that can be investigated as a result of the new digital advances brought forth by blockchain. On the other hand, fintech players such as Visa, Mastercard, and large financial institutions are already conducting research and have made their findings public. In our future study, we intend to examine these works and develop a conceptual understanding of the objectives pursued by these entities. Additionally, we would like to bridge the divide between the public and enterprise blockchain ecosystems and envision the common ground between the two scenarios, as well as how this would work under legal and regulatory constraints.

Author Contributions: Conceptualization, K.N., H.D. and D.-P.L.; methodology, K.N., H.D. and D.-P.L.; writing—original draft preparation, K.N.; writing—review and editing, H.D. and D.-P.L.; supervision, D.-P.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available in article.

Conflicts of Interest: The views expressed in this paper are solely those of the authors, and no responsibility for them should be attributed to the Bank of Canada.

References

1. Statista. Investments into Fintech Companies Globally 2010–2021. 2022. Available online: https://www.statista.com/statistics/719385/investments-into-fintech-companies-globally/ (accessed on 25 February 2022).
2. Insider, B. Overview of the Fintech Industry: Stats, Trends, and Companies in the Ecosystem Market Research Report. 2022. Available online: https://www.businessinsider.com/fintech-ecosystem-report (accessed on 15 March 2022).
3. Lee, I.; Shin, Y.J. Fintech: Ecosystem, business models, investment decisions, and challenges. *Bus. Horiz.* **2018**, *61*, 35–46. [CrossRef]
4. Franco-Riquelme, J.N.; Rubalcaba, L. Innovation and SDGs through Social Media Analysis: Messages from FinTech Firms. *J. Open Innov. Technol. Mark. Complex.* **2021**, *7*, 165. [CrossRef]
5. Gomber, P.; Kauffman, R.J.; Parker, C.; Weber, B.W. On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *J. Manag. Inf. Syst.* **2018**, *35*, 220–265. [CrossRef]
6. Jakšič, M.; Marinč, M. Relationship banking and information technology: The role of artificial intelligence and FinTech. *Risk Manag.* **2019**, *21*, 1–18. [CrossRef]
7. Belanche, D.; Casaló, L.V.; Flavián, C. Artificial Intelligence in FinTech: Understanding robo-advisors adoption among customers. *Ind. Manag. Data Syst.* **2019**, *119*, 1411–1430. [CrossRef]
8. Ashta, A.; Herrmann, H. Artificial intelligence and fintech: An overview of opportunities and risks for banking, investments, and microfinance. *Strateg. Chang.* **2021**, *30*, 211–222. [CrossRef]
9. Meng, S.; He, X.; Tian, X. Research on Fintech development issues based on embedded cloud computing and big data analysis. *Microprocess. Microsystems* **2021**, *83*, 103977. [CrossRef]
10. Trelewicz, J.Q. Big data and big money: The role of data in the financial sector. *It Prof.* **2017**, *19*, 8–10. [CrossRef]
11. Pant, S.K. Fintech: Emerging Trends. *Telecom Bus. Rev.* **2020**, *13*, 47–52.
12. Tan, S.; Yang, Y.; Leopold, C.; Robeller, C.; Weber, U. Augmented Reality and Virtual Reality: New Tools for Architectural Visualization and Design. In *Research Culture in Architecture*; Walter De Gruyter: Berlin, Germany, 2019; pp. 301–310.
13. Fernandez-Vazquez, S.; Rosillo, R.; De La Fuente, D.; Priore, P. Blockchain in FinTech: A mapping study. *Sustainability* **2019**, *11*, 6366. [CrossRef]
14. Imerman, M.B.; Fabozzi, F.J. Cashing in on innovation: A taxonomy of FinTech. *J. Asset Manag.* **2020**, *21*, 167–177. [CrossRef]

15. Sardana, V.; Singhania, S. Digital technology in the realm of banking: A review of literature. *Int. J. Res. Financ. Manag.* **2018**, *1*, 28–32.
16. BusinessWire. 2022. Available online: https://www.businesswire.com/news/home/20220218005233/en/Global-Digital-Payment-Market-is-Expected-to-Grow-at-a-CAGR-of-over-20.5-During-2022-2030---ResearchAndMarkets.com (accessed on 7 March 2022).
17. Federal Reserve Bank of St Louis. 2022. Available online: https://www.stlouisfed.org/education/tools-for-enhancing-the-stock-market-game-invest-it-forward/episode-1-understanding-capital-markets (accessed on 7 March 2022).
18. Biery, M.E. What Is Digital Lending and How Can Community Banks, Credit Unions Benefit. 2018. Available online: https://www.abrigo.com/blog/what-is-digital-lending-and-how-can-community-banks-credit-unions-benefit/ (accessed on 3 March 2022).
19. Arner, D.W.; Barberis, J.; Buckley, R.P. *FinTech and RegTech in a Nutshell, and the Future in a Sandbox*; CFA Institute Research Foundation: Charlottesville, VA, USA, 2017; Volume 3, pp. 1–20.
20. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Technical Report. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 3 March 2022).
21. Wood, G. *Ethereum: A Secure Decentralised Generalised Transaction Ledger*; Technical Report; Ethereum & ETHCore: New York, NY, USA, 2016; Volume 151, pp. 1–32.
22. Foundation, L. Hyperledger Fabric. 2015. Available online: https://hyperledger-fabric.readthedocs.io (accessed on 15 March 2022).
23. Greenspan, G. MultiChain Private Blockchain—White Paper. 2015. Available online: https://www.multichain.com/white-paper/ (accessed on 15 March 2022).
24. Lee, S.H.; Lee, D.W. Review on Fintech Industry in Oversea. In Proceedings of the Conference on Circuits, Control, Communication, Electricity, Electronics, Energy, System, Signal and Simulation, Ho Chi Minh City, Vietnam, 12–19 October 2016.
25. Hendershott, T.; Zhang, X.; Zhao, J.L.; Zheng, Z. FinTech as a game changer: Overview of research frontiers. *Inf. Syst. Res.* **2021**, *32*, 1–17. [CrossRef]
26. Suryono, R.R.; Budi, I.; Purwandari, B. Challenges and trends of financial technology (Fintech): A systematic literature review. *Information* **2020**, *11*, 590. [CrossRef]
27. Li, B.; Xu, Z. Insights into financial technology (FinTech): A bibliometric and visual study. *Financ. Innov.* **2021**, *7*, 1–28. [CrossRef]
28. Bollaert, H.; Lopez-de Silanes, F.; Schwienbacher, A. Fintech and access to finance. *J. Corp. Financ.* **2021**, *68*, 101941. [CrossRef]
29. Takeda, A.; Ito, Y. A review of FinTech research. *Int. J. Technol. Manag.* **2021**, *86*, 67–88. [CrossRef]
30. Sangwan, V.; Prakash, P.; Singh, S. Financial technology: A review of extant literature. *Stud. Econ. Financ.* **2019**, *37*, 71–88. [CrossRef]
31. Knewtson, H.S.; Rosenbaum, Z.A. Toward understanding FinTech and its industry. *Manag. Financ.* **2020**, *46*, 1043–1060. [CrossRef]
32. Milian, E.Z.; Spinola, M.D.M.; de Carvalho, M.M. Fintechs: A literature review and research agenda. *Electron. Commer. Res. Appl.* **2019**, *34*, 100833. [CrossRef]
33. Xu, M.; Chen, X.; Kou, G. A systematic review of blockchain. *Financ. Innov.* **2019**, *5*, 1–14. [CrossRef]
34. Ali, O.; Ally, M.; Dwivedi, Y. The state of play of blockchain technology in the financial services sector: A systematic literature review. *Int. J. Inf. Manag.* **2020**, *54*, 102199. [CrossRef]
35. Rabbani, M.R.; Khan, S.; Thalassinos, E.I. FinTech, Blockchain and Islamic Finance: An Extensive Literature Review. *Int. J. Econ. Bus. Adm.* **2020**, *VIII*, 65–86.
36. Cao, S.; Cao, Y.; Wang, X.; Lu, Y. A review of researches on blockchain. In Proceedings of the Wuhan International Conference on e-Business, Wuhan, China, 29–28 May 2017.
37. Da Luz, M.A.; de Oliveira, K.S.F. The Use of Blockchain in Financial Area: A Systematic Mapping Study. In *Proceedings of the Anais do XVI Simpósio Brasileiro de Sistemas de Informação*; SBC: São Bernardo do Camp, Brazil, 2020.
38. Frizzo-Barker, J.; Chow-White, P.A.; Adams, P.R.; Mentanko, J.; Ha, D.; Green, S. Blockchain as a disruptive technology for business: A systematic review. *Int. J. Inf. Manag.* **2020**, *51*, 102029. [CrossRef]
39. Pal, A.; Tiwari, C.K.; Behl, A. Blockchain technology in financial services: A comprehensive review of the literature. *J. Glob. Oper. Strateg. Sourc.* **2021**, *14*, 61–80. [CrossRef]
40. Trivedi, S.; Mehta, K.; Sharma, R. Systematic Literature Review on Application of Blockchain Technology in E-Finance and Financial Services. *J. Technol. Manag. Innov.* **2021**, *16*, 89–102. [CrossRef]
41. Gamage, H.; Weerasinghe, H.; Dias, N. A survey on blockchain technology concepts, applications, and issues. *SN Comput. Sci.* **2020**, *1*, 1–15. [CrossRef]
42. Gan, Q.; Lau, R.Y.K.; Hong, J. A critical review of blockchain applications to banking and finance: A qualitative thematic analysis approach. *Technol. Anal. Strateg. Manag.* **2021**, 1–17. [CrossRef]
43. Osmani, M.; El-Haddadeh, R.; Hindi, N.; Janssen, M.; Weerakkody, V. Blockchain for next generation services in banking and finance: Cost, benefit, risk and opportunity analysis. *J. Enterp. Inf. Manag.* **2021**, *34*, 884–899. [CrossRef]
44. Gorkhali, A.; Chowdhury, R. Blockchain and the Evolving Financial Market: A Literature Review. *J. Ind. Integr. Manag.* **2021**, 1–35. [CrossRef]
45. Maiti, M.; Ghosh, U. Next generation Internet of Things in fintech ecosystem. *IEEE Internet Things J.* **2021**. [CrossRef]

46. Maiti, M.; Kotliarov, I.; Lipatnikov, V. A future triple entry accounting framework using blockchain technology. *Blockchain Res. Appl.* **2021**, *2*, 100037. [CrossRef]
47. Javaid, M.; Haleem, A.; Singh, R.P.; Khan, S.; Suman, R. Blockchain technology applications for Industry 4.0: A literature-based review. *Blockchain Res. Appl.* **2021**, *2*, 100027. [CrossRef]
48. Chondrogiannis, E.; Andronikou, V.; Karanastasis, E.; Litke, A.; Varvarigou, T. Using blockchain and semantic web technologies for the implementation of smart contracts between individuals and health insurance organizations. *Blockchain Res. Appl.* **2022**, *3*, 100049. [CrossRef]
49. Six, N.; Herbaut, N.; Salinesi, C. Blockchain software patterns for the design of decentralized applications: A systematic literature review. *Blockchain Res. Appl.* **2022**, *3*, 100061. [CrossRef]
50. NIST-FIPS. *FIPS Publication 180-2: Secure Hash Standard*; Technical Report; Federal Information Processing Standard Publication: Gaithersburg, MD, USA, 2002.
51. America National Standard Institute. *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*; ANSI: San Fransisco, CA, USA, 1998.
52. Rivest, R.L.; Shamir, A.; Tauman, Y. *How to Leak a Secret*; Springer: Berlin/Heidelberg, Germany, 2001; pp. 552–565.
53. Blum, M.; Feldman, P.; Micali, S. Non-Interactive Zero-Knowledge and Its Applications. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing (STOC '88)*; Association for Computing Machinery: New York, NY, USA, 1988; pp. 103–112. [CrossRef]
54. Pedersen, T.P. Non-interactive and information-theoretic secure verifiable secret sharing. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 11–15 August 1991; pp. 129–140.
55. Szabo, N. Formalizing and securing relationships on public networks. *First Monday* **1997**, *2*. [CrossRef]
56. Bosselaers, A.; Preneel, B. *Integrity Primitives for Secure Information Systems: Final Ripe Report of Race Integrity Primitives Evaluation*; Number 1007; Springer Science & Business Media: New York, NY, USA, 1995.
57. Dobbertin, H.; Bosselaers, A.; Preneel, B. RIPEMD-160: A strengthened version of RIPEMD. In *Proceedings of the International Workshop on Fast Software Encryption*; Springer: Cambridge, UK, 1996; pp. 71–82.
58. Litecoin. Litecoin—Open Source P2P Digital Currency. Technical Report. 2011. Available online: https://litecoin.org/ (accessed on 30 November 2012).
59. Percival, C.; Josefsson, S. The Scrypt Password-Based Key Derivation Function. 2016. Available online: http://tools.ietf.org/html/josefsson-scrypt-kdf-00.txt (accessed on 7 March 2022).
60. Biryukov, A.; Khovratovich, D. Equihash: Asymmetric proof-of-work based on the generalized birthday problem. *Ledger* **2017**, *2*, 1–30. [CrossRef]
61. Merkle, R.C. A digital signature based on a conventional encryption function. In Proceedings of the Conference on the Theory and Application of Cryptographic Techniques, Santa Barbara, CA, USA, 16–20 August 1987; pp. 369–378.
62. Diffie, W.; Hellman, M. New Directions in Cryptography. *IEEE Trans. Inf. Theor.* **2006**, *22*, 644–654. [CrossRef]
63. National Institute of Standards and Technology. *Digital Signature Standard*; NIST: Washington, DC, USA, 1994.
64. Vanstone, S. Responses to NIST's Proposal. *Commun. ACM* **1992**, *35*, 50–52.
65. International Standard Organization. Information Technology—Security Techniques—Cryptographic Techniques Based on Elliptic Curves—Part 2: Digital Signatures. 2002. Available online: https://www.iso.org/standard/31076.html (accessed on 7 March 2022).
66. IEEE Computer Society. *IEEE Std 1363-2000*; IEEE Standard Specifications for Public-Key Cryptography; IEEE Computer Society: Washington, DC, USA, 2000; pp. 1–228. [CrossRef]
67. Lamport, L. *Constructing Digital Signatures from a One Way Function*; Technical Report CSL-98; IEEE: New York, NY, USA, 1979; This paper was published by IEEE in the Proceedings of HICSS-43 in January 2010.
68. Chaum, D. Blind signatures for untraceable payments. In *Advances in Cryptology*; Springer: Santa Barbara, CA, USA, 1983; pp. 199–203.
69. Van Saberhagen, N. CryptoNote v 2.0; Technical Report. 2013. Available online: https://bytecoin.org/old/whitepaper.pdf (accessed on 7 March 2022).
70. Maxwell, G.; Poelstra, A. Borromean ring signatures. *Comput. Sci.* **2015**, *8*, 2019.
71. Valenta, L.; Rowan, B. Blindcoin: Blinded, accountable mixes for bitcoin. In Proceedings of the International Conference on Financial Cryptography and Data Security, San Juan, Puerto Rico, 26–30 January 2015; pp. 112–126.
72. Itakura, K.; Nakamura, K. *A Public-Key Cryptosystem Suitable for Digital Multisignatures*; NEC Research & Development: Kanagawa, Japan, 1983; pp. 1–8.
73. Le, D.P.; Yang, G.; Ghorbani, A. A new multisignature scheme with public key aggregation for blockchain. In Proceedings of the 2019 17th International Conference on Privacy, Security and Trust (PST), Fredericton, NB, Canada, 26–28 August 2019; pp. 1–7.
74. Benaloh, J.; Mare, M.D. One-way accumulators: A decentralized alternative to digital signatures. In *Proceedings of the Workshop on the Theory and Application of of Cryptographic Techniques*; Springer: Lofthus, Norway, 1993; pp. 274–285.
75. Nguyen, L. Accumulators from bilinear pairings and applications. In Proceedings of the Cryptographers' Track at the RSA Conference, San Francisco, CA, USA, 14–18 February 2005; pp. 275–292.
76. Boxall, J.; El Mrabet, N.; Laguillaumie, F.; Le, D.P. A Variant of Miller's Formula and Algorithm. In *Proceedings of the 4th International Conference on Pairing-Based Cryptography (Pairing'10)*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 417–434.

77. Sun, S.F.; Au, M.H.; Liu, J.K.; Yuen, T.H. Ringct 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero. In Proceedings of the European Symposium on Research in Computer Security, Oslo, Norway, 11–15 September 2017; pp. 456–474.
78. Miers, I.; Garman, C.; Green, M.; Rubin, A.D. Zerocoin: Anonymous distributed e-cash from bitcoin. In Proceedings of the 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 19–22 May 2013; pp. 397–411.
79. Sasson, E.B.; Chiesa, A.; Garman, C.; Green, M.; Miers, I.; Tromer, E.; Virza, M. Zerocash: Decentralized Anonymous Payments from Bitcoin. In Proceedings of the Symposium on Security and Privacy, Berkeley, CA, USA, 18–21 May 2014.
80. Ben-Sasson, E.; Chiesa, A.; Riabzev, M.; Spooner, N.; Virza, M.; Ward, N.P. Aurora: Transparent succinct arguments for R1CS. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, 19–23 May 2019; pp. 103–128.
81. Bünz, B.; Bootle, J.; Boneh, D.; Poelstra, A.; Wuille, P.; Maxwell, G. Bulletproofs: Short proofs for confidential transactions and more. In Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), Berkeley, CA, USA, 21–23 May 2018; pp. 315–334.
82. Cong, L.W.; He, Z. Blockchain disruption and smart contracts. *Rev. Financ. Stud.* **2019**, *32*, 1754–1797. [CrossRef]
83. Dcunha, S.; Patel, S.; Sawant, S.; Kulkarni, V.; Shirole, M. Blockchain Interoperability Using Hash Time Locks. In Proceedings of the Fifth International Conference on Microelectronics, Computing and Communication Systems, Ranchi, India, 12–13 May 2021; pp. 475–487.
84. Han, J.; Huang, S.; Zhong, Z. Trust in DeFi: An Empirical Study of the Decentralized Exchange. 2021. Available online: https://ssrn.com/abstract=3896461 (accessed on 7 March 2022).
85. Poon, J.; Dryja, T. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. *White Paper*, 14 January 2016. Available online: https://lightning.network/lightning-network-paper.pdf (accessed on 7 March 2022).
86. Besedin, S.; Mitrokhin, A. Decentralized Escrow Whitepaper. Technical Report. 2017. Available online: https://descrow.com/images/WP_en.pdf (accessed on 7 March 2022).
87. Goldfeder, S.; Bonneau, J.; Gennaro, R.; Narayanan, A. Escrow protocols for cryptocurrencies: How to buy physical goods using bitcoin. In Proceedings of the International Conference on Financial Cryptography and Data Security, Sliema, Malta, 3–7 April 2017; pp. 321–339.
88. Herlihy, M. Atomic cross-chain swaps. In Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing, Egham, UK, 23–27 July 2018; pp. 245–254.
89. Hardjono, T. Blockchain gateways, bridges and delegated hash-locks. *arXiv* **2021**, arXiv:2102.03933.
90. Blockchain Bridges. 2022. Available online: https://ethereum.org/en/bridges/ (accessed on 3 March 2022).
91. Kfoury, B. The Role of Blockchain in Reducing the Cost of Financial Transactions in the Retail Industry. Technical Report. 2021. Available online: http://ceur-ws.org/Vol-2889/PAPER_02.pdf (accessed on 15 March 2022).
92. Mori, T. Financial technology: Blockchain and securities settlement. *J. Secur. Oper. Custody* **2016**, *8*, 208–227.
93. Tasca, P.; Tessone, C.J. Taxonomy of blockchain technologies. Principles of identification and classification. *arXiv* **2017**, arXiv:1708.04872.
94. Zhang, C.; Wu, C.; Wang, X. Overview of Blockchain consensus mechanism. In Proceedings of the 2020 2nd International Conference on Big Data Engineering, Shanghai, China, 29–31 May 2020; pp. 7–12.
95. Vukolić, M. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. In *Open Problems in Network Security. iNetSec 2015. Lecture Notes in Computer Science*; Camenisch, J., Kesdoğan, D., Eds.; Springer: Cham, Switzerland, 2015; Volume 9591._9. [CrossRef]
96. Saleh, F. Blockchain without waste: Proof-of-stake. *Rev. Financ. Stud.* **2021**, *34*, 1156–1190. [CrossRef]
97. Nair, P.R.; Dorai, D.R. Evaluation of performance and security of proof of work and proof of stake using blockchain. In Proceedings of the 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Virtual, 4–6 February 2021; pp. 279–283.
98. Reijers, W.; Wuisman, I.; Mannan, M.; De Filippi, P.; Wray, C.; Rae-Looi, V.; Cubillos Vélez, A.; Orgad, L. Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies. *Topoi* **2021**, *40*, 821–831. [CrossRef]
99. Chohan, U.W. The Decentralized Autonomous Organization and Governance Issues. 2017. Available online: https://ssrn.com/abstract=3082055 (accessed on 7 March 2022).
100. Zhang, R.; Xue, R.; Liu, L. Security and privacy on blockchain. *ACM Comput. Surv. (CSUR)* **2019**, *52*, 1–34. [CrossRef]
101. Chen, X.; Hasan, M.A.; Wu, X.; Skums, P.; Feizollahi, M.J.; Ouellet, M.; Sevigny, E.L.; Maimon, D.; Wu, Y. Characteristics of bitcoin transactions on cryptomarkets. In Proceedings of the International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Atlanta, GA, USA, 14–17 July 2019; pp. 261–276.
102. Guides, T.S. Why Cardano ADA Deserves Your Attention—Cardano Cryptocurrency Strategy. 2018. Available online: https://tradingstrategyguides.com/cardano-cryptocurrency-strategy/ (accessed on 7 March 2022).
103. Silvano, W.F.; Marcelino, R. Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. *Future Gener. Comput. Syst.* **2020**, *112*, 307–319. [CrossRef]
104. Chen, J.; Micali, S. Algorand: A secure and efficient distributed ledger. *Theor. Comput. Sci.* **2019**, *777*, 155–183. [CrossRef]
105. Brown, R.G.; Carlyle, J.; Grigg, I.; Hearn, M. Corda: An introduction. *R3 CEV* **2016**, *1*, 14.

106. Baliga, A.; Subhod, I.; Kamat, P.; Chatterjee, S. Performance evaluation of the quorum blockchain platform. *arXiv* **2018**, arXiv:1809.03421.
107. Consensys. Quorum Blockchain. 2022. Available online: https://github.com/ConsenSys/quorum (accessed on 15 March 2022).
108. Diem. Diem Blockchain. 2022. Available online: https://www.diem.com/en-us/ (accessed on 15 March 2022).
109. Kelley, M.; Mahdi, D. *Innovation Insight for Decentralized Identity and Verifiable Claims*; Technical Report; Gartner Research: Stamford, CT, USA, 2021.
110. Foundation, H. *Decentralized ID and Access Management (DIAM) for IoT Networks*; Technical Report; Linux Foundation: San Francisco, CA, USA, 2021.
111. Lyons, T.; Courcelas, L.; Timsit, K. *Blockchain and Digital Identity*; Technical Report; The European Union Blockchain Observatory & Forum: Washington, DC, USA, 2019.
112. Pertsev, A.; Semenov, R.; Storm, R. Tornado Cash Privacy Solution Version 1.4. 2019. Available online: https://tornado.cash/Tornado.cash_whitepaper_v1.4.pdf (accessed on 15 March 2022).
113. Hopwood, D.; Bowe, S.; Hornby, T.; Wilcox, N. *Zcash Protocol Specification*; GitHub: San Francisco, CA, USA, 2016; p. 1.
114. Ali, R.; Barrdear, J.; Clews, R.; Southgate, J. The economics of digital currencies. *Bank Engl. Q. Bull.* **2014**, *54*, 276–286.
115. Allen, F.; Gu, X.; Jagtiani, J. Fintech, Cryptocurrencies, and CBDC: Financial Structural Transformation in China. *J. Int. Money Financ.* **2022**, *124*, 102625. [CrossRef]
116. Calcaterra, C.; Kaal, W.A.; Rao, V. Stable cryptocurrencies: First order principles. *Stan. J. Blockchain L. Pol'y* **2020**, *3*, 62. [CrossRef]
117. Bogoni, G. Cryptocurrencies Stabilization Systems: A Focus on the MakerDAO Case. 2019. Available online: https://www.politesi.polimi.it/handle/10589/152447?mode=full (accessed on 15 March 2022).
118. Acker, A.; Murthy, D. What is Venmo? A descriptive analysis of social features in the mobile payment platform. *Telemat. Inform.* **2020**, *52*, 101429. [CrossRef]
119. Tsepeleva, R.; Korkhov, V. Implementation of the Cross-Blockchain Interacting Protocol. In *Computational Science and Its Applications—ICCSA 2021. Lecture Notes in Computer Science*; Springer: Cham, Switzerland, 2021; Volume 12952._4. [CrossRef]
120. Fung, B.; Halaburda, H. Understanding platform-based digital currencies. *Bank Can. Rev.* **2014**, *2014*, 12–20.
121. Meta. 2022. Available online: https://about.facebook.com/meta/ (accessed on 6 March 2022).
122. Amazon. 2022. Available online: https://www.aboutamazon.com/ (accessed on 6 March 2022).
123. Kiff, M.J.; Alwazir, J.; Davidovic, S.; Farias, A.; Khan, M.A.; Khiaonarong, M.T.; Malaika, M.; Monroe, M.H.K.; Sugimoto, N.; Tourpe, H.; et al. A Survey of Research on Retail Central Bank Digital Currency. 1 July 2020. Available online: https://ssrn.com/abstract=3639760 (accessed on 15 March 2022). http://dx.doi.org/10.2139/ssrn.3639760.
124. Zhang, T.; Huang, Z. Blockchain and central bank digital currency. *ICT Express* **2021**. [CrossRef]
125. Bank of International Settlements. 2022. Available online: https://www.bis.org/publ/othp33.pdf (accessed on 14 March 2022).
126. Atlantic Council. 2022. Available online: https://www.atlanticcouncil.org/blogs/econographics/a-report-card-on-chinas-central-bank-digital-currency-the-e-cny/ (accessed on 6 March 2022).
127. MIT Media Lab. 2022. Available online: https://dci.mit.edu/project-hamilton-building-a-hypothetical-cbdc (accessed on 7 March 2022).
128. Liu, Y.; Vogel, S.; Zhang, Y. Electronic trading in OTC markets vs. centralized exchange. In Proceedings of the Finance Meeting EUROFIDAI-AFFI, Paris, France, 20 December 2018.
129. Xu, J.; Paruch, K.; Cousaert, S.; Feng, Y. Sok: Decentralized exchanges (dex) with automated market maker (AMM) protocols. *arXiv* **2021**, arXiv:2103.12732.
130. Capponi, A.; Jia, R. The adoption of blockchain-based decentralized exchanges. *arXiv* **2021**, arXiv:2103.08842.
131. Uniswap. 2022. Available online: https://uniswap.org/ (accessed on 7 March 2022).
132. Sushiswap. 2022. Available online: https://www.sushi.com/ (accessed on 7 March 2022).
133. Balancer. 2022. Available online: https://balancer.fi/ (accessed on 7 March 2022).
134. Qin, K.; Zhou, L.; Afonin, Y.; Lazzaretti, L.; Gervais, A. CeFi vs. DeFi–Comparing Centralized to Decentralized Finance. *arXiv* **2021**, arXiv:2106.08157.
135. Werner, S.M.; Perez, D.; Gudgeon, L.; Klages-Mundt, A.; Harz, D.; Knottenbelt, W.J. Sok: Decentralized finance (defi). *arXiv* **2021**, arXiv:2101.08778.
136. Qin, K.; Zhou, L.; Livshits, B.; Gervais, A. Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit. In *Financial Cryptography and Data Security. FC 2021. Lecture Notes in Computer Science*; Borisov, N., Diaz, C., Eds.; Springer: Berlin/Heidelberg, Germany, 2021; Volume 12674._1. [CrossRef]
137. Compound. 2022. Available online: https://compound.finance/ (accessed on 7 March 2022).
138. Aave. 2022. Available online: https://aave.com/ (accessed on 7 March 2022).
139. dYdX. 2022. Available online: https://dydx.exchange/ (accessed on 7 March 2022).
140. Gudgeon, L.; Werner, S.; Perez, D.; Knottenbelt, W.J. Defi protocols for loanable funds: Interest rates, liquidity and market efficiency. In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies, New York, NY, USA, 21–23 October 2020; pp. 92–112.
141. Synthetix. 2022. Available online: https://synthetix.io/ (accessed on 7 March 2022).
142. Nexus. 2022. Available online: https://nexusmutual.io/ (accessed on 7 March 2022).
143. Erasure. 2022. Available online: https://erasure.world/ (accessed on 7 March 2022).

144. jumpcrypto.com. 2022. Available online: https://jumpcrypto.com/state-of-crypto-derivatives-market/ (accessed on 7 March 2022).
145. Beniiche, A. A study of blockchain oracles. *arXiv* **2020**, arXiv:2004.07140.
146. Egberts, A. The Oracle Problem—An Analysis of how Blockchain Oracles Undermine the Advantages of Decentralized Ledger Systems. 13 December 2017. Available online: https://ssrn.com/abstract=3382343 (accessed on 7 March 2022). http://dx.doi.org/10.2139/ssrn.3382343.
147. Pasdar, A.; Dong, Z.; Lee, Y.C. Blockchain Oracle Design Patterns. *arXiv* **2021**, arXiv:2106.09349.
148. Zhang, F.; Maram, D.; Malvai, H.; Goldfeder, S.; Juels, A. Deco: Liberating web data using decentralized oracles for tls. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, 9–13 November 2020; pp. 1919–1938.
149. Liu, B.; Szalachowski, P.; Zhou, J. A First Look into DeFi Oracles. In Proceedings of the 2021 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), London, UK, 23–26 August 2021; pp. 39–48. doi:10.1109/DAPPS52256.2021.00010. [CrossRef]
150. Adler, J.; Berryhill, R.; Veneris, A.; Poulos, Z.; Veira, N.; Kastania, A. Astraea: A Decentralized Blockchain Oracle. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Dalian, China, 20–21 October 2018; pp. 1145–1152. doi:10.1109/Cybermatics_2018.2018.00207. [CrossRef]
151. Goel, N.; Filos-Ratsikas, A.; Faltings, B. Decentralized Oracles via Peer-Prediction in the Presence of Lying Incentives. 2019. Available online: https://arisfilosratsikas.com/papers/decentralized_oracles.pdf (accessed on 7 March 2022).
152. Merlini, M.; Veira, N.; Berryhill, R.; Veneris, A. On Public Decentralized Ledger Oracles via a Paired-Question Protocol. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea, 14–17 May 2019; pp. 337–344. doi:10.1109/BLOC.2019.8751484. [CrossRef]
153. Cai, Y.; Fragkos, G.; Tsiropoulou, E.E.; Veneris, A. 2020 A Truth-Inducing Sybil Resistant Decentralized Blockchain Oracle. In Proceedings of the 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 28–30 September 2020; pp. 128–135. doi:10.1109/BRAINS49436.2020.9223272. [CrossRef]
154. Peterson, J.; Krug, J.; Zoltu, M.; Williams, A.K.; Alexander, S. Augur: A decentralized oracle and prediction market platform. *arXiv* **2015**, arXiv:1501.01042.
155. De Pedro, A.S.; Levi, D.; Cuende, L.I. Witnet: A decentralized oracle network protocol. *arXiv* **2017**, arXiv:1711.09756.
156. Breidenbach, L.; Cachin, C.; Chan, B.; Coventry, A.; Ellis, S.; Juels, A.; Koushanfar, F.; Miller, A.; Magauran, B.; Moroz, D.; et al. Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks. 2021. Available online: https://research.chain.link/whitepaper-v2.pdf (accessed on 7 March 2022).
157. Benisi, N.Z.; Aminian, M.; Javadi, B. Blockchain-based decentralized storage networks: A survey. *J. Netw. Comput. Appl.* **2020**, *162*, 102656.
158. Casino, F.; Politou, E.; Alepis, E.; Patsakis, C. Immutability and decentralized storage: An analysis of emerging threats. *IEEE Access* **2019**, *8*, 4737–4744. [CrossRef]
159. Shah, M.; Shaikh, M.; Mishra, V.; Tuscano, G. Decentralized Cloud Storage Using Blockchain. In Proceedings of the 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), Tirunelveli, India, 16–18 April 2020; pp. 384–389.10.1109/ICOEI48184.2020.9143004. [CrossRef]
160. Lakshman, A.; Malik, P. Cassandra: A decentralized structured storage system. *ACM SIGOPS Oper. Syst. Rev.* **2010**, *44*, 35–40. [CrossRef]
161. Vorick, D.; Champine, L. Sia: Simple decentralized storage. *Retrieved May* **2014**, *8*, 2018.
162. Churyumov, A. Byteball: A Decentralized System for Storage and Transfer of Value. 2016. Available online: https://byteball.org/Byteball.pdf (accessed on 7 March 2022).
163. Haeberlen, A.; Mislove, A.; Druschel, P. Glacier: Highly durable, decentralized storage despite massive correlated failures. In Proceedings of the 2nd Conference on Symposium on Networked Systems Design & Implementation, Boston, MA, USA, 2–4 May 2005; Volume 2, pp. 143–158.
164. Wilkinson, S.; Lowry, J.; Boshevski, T. *Metadisk a Blockchain-Based Decentralized File Storage Application*; Technical Report, hal; Storj Labs Inc.: Atlanta, GA, USA, 2014; pp. 1–11. Available online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.692.8781&rep=rep1&type=pdf (accessed on 7 March 2022).
165. Ali, S.; Wang, G.; White, B.; Cottrell, R.L. A Blockchain-Based Decentralized Data Storage and Access Framework for PingER. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security And Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 1303–1308. doi:10.1109/TrustCom/BigDataSE.2018.00179. [CrossRef]
166. Ruj, S.; Rahman, M.S.; Basu, A.; Kiyomoto, S. BlockStore: A Secure Decentralized Storage Framework on Blockchain. In Proceedings of the 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), Krakow, Poland, 16–18 May 2018; pp. 1096–1103. doi:10.1109/AINA.2018.00157. [CrossRef]
167. Filecoin. 2022. Available online: https://filecoin.io/ (accessed on 7 March 2022).
168. Medium. 2022. Available online: https://blog.sia.tech/a-deep-dive-into-skynet-a0fa037feea (accessed on 7 March 2022).
169. Alchemy. 2022. Available online: https://www.alchemy.com/ (accessed on 7 March 2022).

170. Ankr. 2022. Available online: https://www.ankr.com/ (accessed on 7 March 2022).
171. BlockDaemon. 2022. Available online: https://blockdaemon.com/ (accessed on 7 March 2022).
172. ChainStack. 2022. Available online: https://chainstack.com/ (accessed on 7 March 2022).
173. Subramanian, H. Decentralized blockchain-based electronic marketplaces. *Commun. ACM* **2017**, *61*, 78–84. [CrossRef]
174. Klems, M.; Eberhardt, J.; Tai, S.; Härtlein, S.; Buchholz, S.; Tidjani, A. Trustless Intermediation in Blockchain-Based Decentralized Service Marketplaces. In *Service-Oriented Computing. ICSOC 2017. Lecture Notes in Computer Science*; Maximilien, M., Vallecillo, A., Wang, J., Oriol, M., Eds.; Springer: Cham, Switzerland, 2017; Volume 10601._53. [CrossRef]
175. Gnosis. 2022. Available online: https://gnosis.io/ (accessed on 7 March 2022).
176. Lawrenz, S.; Sharma, P.; Rausch, A. Blockchain technology as an approach for data marketplaces. In Proceedings of the 2019 International Conference on Blockchain Technology, Atlanta, GA, USA, 14–17 July 2019; pp. 55–59.
177. Banerjee, P.; Ruj, S. Blockchain Enabled Data Marketplace—Design and Challenges. *arXiv* **2018**, arXiv:1811.11462.
178. Xu, R.; Ramachandran, G.S.; Chen, Y.; Krishnamachari, B. BlendSM-DDM: BLockchain-ENabled Secure Microservices for Decentralized Data Marketplaces. In Proceedings of the 2019 IEEE International Smart Cities Conference (ISC2), Casablanca, Morocco, 14–17 October 2019; pp. 14–17. doi: 10.1109/ISC246665.2019.9071766. [CrossRef]
179. Vousinas, G. Supply chain finance: Definition, modern aspects and research challenges ahead. In *Supply Chain Finance: Risk Management, Resilience and Supplier Management*; Tate, W., Bals, L., Ellram, L., Eds.; Kogan Page: London, UK, 2019; pp. 63–95. Available online: https://www.researchgate.net/publication/327981053_Supply_chain_finance_definition_modern_aspects_and_research_challenges_ahead (accessed on 7 March 2022).
180. Wang, R.; Wu, Y. Application of Blockchain Technology in Supply Chain Finance of Beibu Gulf Region. *Math. Probl. Eng.* **2021**, *2021*, 5556424. [CrossRef]
181. Yaksick, R. Overcoming Supply Chain Finance Challenges Via Blockchain Technology. In *Disruptive Innovation in Business and Finance in the Digital World (International Finance Review, Vol. 20)*; Choi, J.J., Ozkan, B., Eds.; Emerald Publishing Limited: Bingley, UK, 2019; pp. 87–100. [CrossRef]
182. Contour. 2022. Available online: https://contour.network/ (accessed on 7 March 2022).
183. Skuchain. 2022. Available online: https://www.skuchain.com/ (accessed on 7 March 2022).
184. Etradeconnect. 2022. Available online: https://www.etradeconnect.net/ (accessed on 7 March 2022).
185. Kongo. 2022. Available online: https://www.komgo.io/ (accessed on 7 March 2022).
186. Marco Polo. 2022. Available online: https://marcopolonetwork.com/ (accessed on 7 March 2022).
187. UAE Trade Connect. 2022. Available online: https://avanzainnovations.com/blog/portfolio/utc/ (accessed on 7 March 2022).
188. We.trade. 2022. Available online: https://we-trade.com/ (accessed on 7 March 2022).
189. Singh, H.; Jain, G.; Munjal, A.; Rakesh, S. Blockchain technology in corporate governance: Disrupting chain reaction or not? *Corp. Gov. Int. J. Bus. Soc.* **2019**, *20*, 67–86. [CrossRef]
190. Yermack, D. Corporate governance and blockchains. *Rev. Financ.* **2017**, *21*, 7–31. [CrossRef]
191. Wiśniewska, A. The initial coin offering—Challenges and opportunities. *Copernic. J. Financ. Account.* **2018**, *7*, 99–110. [CrossRef]
192. Jentzsch, C. Decentralized Autonomous Organization to Automate Governance. *White Paper*, November 2016. Available online: https://lawofthelevel.lexblogplatformthree.com/wp-content/uploads/sites/187/2017/07/WhitePaper-1.pdf (accessed on 7 March 2022).
193. Fenwick, M.; Vermeulen, E.P. Technology and corporate governance: Blockchain, crypto, and artificial intelligence. *Tex. J. Bus. L.* **2019**, *48*, 1. [CrossRef]
194. Aragon. 2022. Available online: https://aragon.org/ (accessed on 7 March 2022).
195. DAOStack. 2022. Available online: https://daostack.io/ (accessed on 7 March 2022).
196. Colony. 2022. Available online: https://colony.io/ (accessed on 7 March 2022).
197. Oguama, L. Fintech Credit Market—Crowdfunding: An Evaluation of Market Models. 20 September 2020. Available online: https://ssrn.com/abstract=3696044 (accessed on 7 March 2022).
198. Shneor, R.; Zhao, L.; Flåten, B.T. (Eds.) *Advances in Crowdfunding*; Springer International Publishing: Berlin, Germany, 2020. [CrossRef]
199. LendingClub. 2022. Available online: https://www.lendingclub.com/ (accessed on 7 March 2022).
200. GoFundMe. 2022. Available online: https://www.gofundme.com/ (accessed on 7 March 2022).
201. AngelList. 2022. Available online: https://angel.co/ (accessed on 7 March 2022).
202. Kickstarter. 2022. Available online: https://www.kickstarter.com/ (accessed on 7 March 2022).
203. Lacasse, R.; Lambert, B.; Roy, N.; Sylvain, J.; Nadeau, F. A digital tsunami: FinTech and crowdfunding. In Proceedings of the International Scientific Conference on Digital Intelligence, Quebec City, QC, Canada, 4–6 April 2016; pp. 1–5.
204. Baber, H. Blockchain-Based Crowdfunding. In *Blockchain Technology for Industry 4.0. Blockchain Technologies*; Rosa Righi, R., Alberti, A., Singh, M., Eds.; Springer: Singapore, 2020. [CrossRef]
205. RealBlocks. 2022. Available online: https://www.realblocks.com/home (accessed on 7 March 2022).
206. Meridio. 2022. Available online: https://medium.com/@Meridio (accessed on 7 March 2022).
207. QuantmRE. 2022. Available online: https://www.quantmre.com/ (accessed on 7 March 2022).
208. Gitcoin. 2022. Available online: https://gitcoin.co/ (accessed on 7 March 2022).
209. Brickblock. 2022. Available online: https://www.brickblock.io/ (accessed on 7 March 2022).

210. RealtyBits. 2022. Available online: https://www.realtybits.com/ (accessed on 7 March 2022).
211. Zhou, Q.; Huang, H.; Zheng, Z.; Bian, J. Solutions to scalability of blockchain: A survey. *IEEE Access* **2020**, *8*, 16440–16455. [CrossRef]
212. Medium. 2022. Available online: https://aakash-111.medium.com/the-scalability-trilemma-in-blockchain-75fb57f646df (accessed on 7 March 2022).
213. Nasir, M.H.; Arshad, J.; Khan, M.M.; Fatima, M.; Salah, K.; Jayaraman, R. Scalable blockchains—A systematic review. *Future Gener. Comput. Syst.* **2022**, *126*, 136–162. [CrossRef]
214. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
215. Medium. 2022. Available online: https://blog.connext.network/the-interoperability-trilemma-657c2cf69f17 (accessed on 7 March 2022).
216. Goldberg, I. On the security of the Tor authentication protocol. In Proceedings of the International Workshop On Privacy Enhancing Technologies, Cambridge, UK, 28–30 June 2006; pp. 316–331.
217. Feng, Q.; He, D.; Zeadally, S.; Khan, M.K.; Kumar, N. A survey on privacy protection in blockchain system. *J. Netw. Comput. Appl.* **2019**, *126*, 45–58. [CrossRef]
218. Androulaki, E.; Karame, G.O.; Roeschlin, M.; Scherer, T.; Capkun, S. Evaluating user privacy in bitcoin. In Proceedings of the International Conference on Financial Cryptography and Data Security, Okinawa, Japan, 1–5 April 2013; pp. 34–51.