Journal of Open Innovation: Technology, Market, and Complexity

MDPI

Review

A Survey of Blockchain Applications in the FinTech Sector

Tara Renduchintala [1], Haneen Alfauri [2,*], Zebo Yang [2], Roberto Di Pietro [3] and Raj Jain [2]

[1] Electrical and Computer Engineering Department, University of Southern California, Los Angeles, CA 90007, USA
[2] Computer Science and Engineering Department, Washington University Saint Louis, St. Louis, MO 63130, USA
[3] Science and Engineering Department, Hamad Bin Khalifa University, Ar-Rayyan 5825, Qatar
* Correspondence: a.haneen@wustl.edu

Abstract: FinTech has proven its true potential in traditional financial offerings by delivering digital financial services to individuals worldwide. The pandemic has accelerated how people interact with financial services and has resulted in long-term changes to societies and economies. FinTech has expanded access to financial services and has made such changes possible. FinTech or Financial Technology refers to using new technologies for financial services. Artificial Intelligence, Blockchain, and cloud computing are a few technologies currently being applied to FinTech. In this paper, we consider FinTech, which partly uses blockchain technology. Blockchain technology plays a vital role in the financial sector as it ultimately lifts trust and the need for third-party verification by using consensus-based verification. This survey provides a comprehensive summary of the most relevant blockchain-based FinTech implementations and an overview of FinTech sectors and segments. For each segment, we provide a critique and a discussion on how each blockchain implementation contributes to solving the majority of problems faced by FinTech companies and researchers. This research aims to direct the future of financial solutions by providing an outline of the applications of blockchain technology and distributed ledger technology (DLT) for FinTech. We discuss various implementations, limitations, and challenges of blockchain-based FinTech applications. We conclude this work by exploring possible strengths, weaknesses, opportunities, and threats (SWOT) analysis and future research directions.

Keywords: blockchain; FinTech; payment services; deposits and lending; financial services; bitcoin; Ethereum; Hyperledger; smart contract; digital wallet

Citation: Renduchintala, T.; Alfauri, H.; Yang, Z.; Di Pietro, R.; Jain, R. A Survey of Blockchain Applications in the FinTech Sector. *J. Open Innov. Technol. Mark. Complex.* **2022**, *8*, 185. https://doi.org/10.3390/joitmc8040185

Received: 18 August 2022
Accepted: 25 September 2022
Published: 13 October 2022

1. Introduction

The economic disruption due to the pandemic has led to tremendous growth in digital financial services and e-commerce as social distancing has taken hold worldwide. According to the World Bank [1], there are 1.7 billion unbanked individuals worldwide; half of these include women in rural areas or out of the workforce. The toll of the COVID-19 pandemic highlighted the importance of the inclusion and serving of people currently outside financial systems [2].

According to the 2020 Global COVID-19 FinTech market rapid assessment study [3], a more significant push towards digitalization during the pandemic was seen in most types of FinTech firms, who reported strong growth in transaction numbers and volumes of 13% and 11%, respectively, for the first half of 2020 compared to the same period in 2019, which was before the pandemic.

FinTech improves activities in finance by using digital technologies. Applying digital methods to traditional financial activities eases the online demands brought by the pandemic. Yet, it still raises concerns about centralization, such as dictatorship, data monopoly, data tampering, and user privacy issues. Blockchain technology, the most practical

decentralized solution, has recently attracted much attention. It removes the need for third-party verification for transactions (i.e., the need for centralized exchanges).

In 2019, Gartner estimated that blockchain remains in the "Peak of Inflated Expectation" region, gaining a high interest from investors and consumers with a forecast to reach a plateau in "five to ten years". The report predicted that blockchains will undergo more mainstream adoption in 2023, thus leading to a generation of $3.1 trillion [4] in new business value by 2030.

This growth is partly due to multinational corporations and technology industry giants using blockchain to capture larger market shares.

The adoption of blockchain technology by FinTech companies is inevitable [5]. In 2021, the Gartner report [6] categorized decentralized finance in the "innovation trigger" region, meaning that the technology is subject to significant media and industry interest, with a high potential for technology breakthrough. Blockchain-based FinTech solutions can offer financial services at lower costs and a higher level of accessibility [7] when compared with traditional solutions.

Blockchain technology can provide decentralized, secure, and traceable storage, attracting massive industry investment. There are currently several blockchain applications that span a vast range of industries, including healthcare [8], IoT [9], security [10,11], data privacy [12], supply chain and goods tracing [13,14], the energy sector [15], product counterfeiting [16], etc. Among the various sectors interested in the blockchain industry, FinTech stands out and has become a prevalent topic with great promises.

Financial behaviors such as banking and trading have changed since the emergence of blockchain. Traditional financial institutions are pouring money into FinTech companies and startups to leverage innovation and gain a competitive advantage over their peers [17]. The FinTech industry incentivizes traditional banking institutions to develop their blockchain infrastructure to seize the market share of FinTech services.

Although there are high-level reviews of blockchain technology [18–21], a systematic comparison of blockchain platforms in the context of financial applications is still lacking. There is a considerable gap in investigating how blockchains and distributed ledger technologies are implemented and used for financial services on a technical level for various FinTech Segments. Other studies [22] have provided an overview of existing fintech platforms from a theoretical lens by presenting a plan for adopting fintech platforms. Others [23] have investigated digital finance from a business function perspective.

The authors in [24] investigated FinTech innovations (e.g., ML, blockchain, and alternative finance) and the related regulatory issues. Our paper is solely focused on laying out blockchain-based applications for FinTech segments.

This survey focuses on using blockchains to enhance the way financial services are offered to individuals and businesses by FinTech companies. We discuss how different companies leverage blockchains to realize their goal.

The contributions of this paper can be summarized as follows:

(1) This survey provides a thorough and detailed systematization and summary of the most relevant blockchain-based FinTech implementations.
(2) We provide an overview of various FinTech Sectors and segments. For each FinTech segment, we map the current blockchain applications and discuss how these implementations contribute to solving the vast majority of problems faced by FinTech companies and users.
(3) We also present detailed blockchain-based use-cases to illustrate how different blockchain applications are implemented for various financial services.
(4) We provide an overview of some critical challenges in implementing blockchains for FinTech and a summary of related research work.
(5) We provide a discussion and SWOT analysis to identify the strengths, weaknesses, opportunities, and threats in this field.

The rest of the paper is organized as follows. Section 2 provides an overview of the procedures and methodology that we followed in our research. Section 3 provides a brief background on blockchain architecture, highlights the most popular blockchain implementations' key characteristics, and introduces smart contracts that enable FinTech companies to provide low-cost, secure, and decentralized applications. Section 4 introduces the FinTech literature and discusses blockchains' interaction with banking and their applications within the main three segments of FinTech (Payments, Deposits and Lending, and Investment Management). Section 5 reviews the Payments segment. Section 6 reviews the Deposits and Lending segment. Section 7 discusses the FinTech Investment Management segment. Section 8 discusses key challenges facing blockchain implementations for FinTech, examines blockchain-based Defi, and provides a SWOT analysis to identify the field's strengths, weaknesses, opportunities, and threats.

To the best of our knowledge, this is the first mapping study of blockchain applications in solving the issues faced by the Fintech segments from a technical point of view.

2. Methodology

For a comprehensive review and analysis of blockchain applications in the FinTech sector, multiple survey processes and techniques were used to gather and examine information in academic and industry settings. In this section, we summarize the procedure that we followed in this survey.

The first step was choosing the databases (i.e., data sources) that will be used to extract academic articles and research papers. We compared the top three databases (Scopus, Google scholar, and Web of Science) used in this field. It was found that Google Scholar was able to find most of the citations in Social Sciences articles (94%), while Web of Science and Scopus found 35% and 43%, respectively [25]. Therefore, Google scholar was chosen as our search database. This is shown in step 1 of Figure 1. We conducted a literature review that included all available academic publications and practitioner-oriented papers on the topic of FinTech for the last seven years (2016–2022).

Our search terms for FinTech literature were ("FinTech" OR "Financial services" OR "Finance"), and our search terms for blockchain literature were ("Blockchains" OR "Distributed Ledger") and ("Application" OR "Service" OR "DApp" OR "Implementations"). This is shown in step 2 of Figure 1.

We conducted a systematic literature search on blockchain-based applications for FinTech. We identified potential papers and conducted a quality assessment and filtering to avoid sampling any poorly conducted studies whose biases may skew. The papers were selected based on three factors: the journal ranking, the number of citations since it is a good indication of the papers' popularity, and a manual assessment of their potential to solve the current issues faced by each segment. This is shown in step 3 of Figure 1.

Then, we conducted a systematic literature search on FinTech to gain a deeper understanding of the academic publications. During our literature search, we identified a possible research question. We found a considerable gap in investigating how blockchains and distributed ledger technologies are implemented and used for financial services on a technical level. This is shown in step 4 of Figure 1.

We then investigated the evolution of financial services and FinTech. Our study builds on prior work by Deloitte [26], where they categorized financial services segments and provided an overview of the characteristics of each of the segments. After defining the main three segments of financial services, we delve into a deeper search to find potential issues for each segment of the financial sector. This is shown in step 4 of Figure 1.

After identifying and filtering the most popular blockchain solutions, we spent an extensive amount of time working on mapping each blockchain technology within each segment, where we highlighted how each application solves an issue within the allocated segment. This is shown in step 5 of Figure 1.

Finally, based on the review and investigation in the Fintech literature, we examined blockchain-based Defi by establishing a SWOT analysis to identify the strengths, weaknesses, opportunities, and threats in this field. This is shown in step 6 of Figure 1.

Figure 1 summarizes the procedure that we followed in our survey.

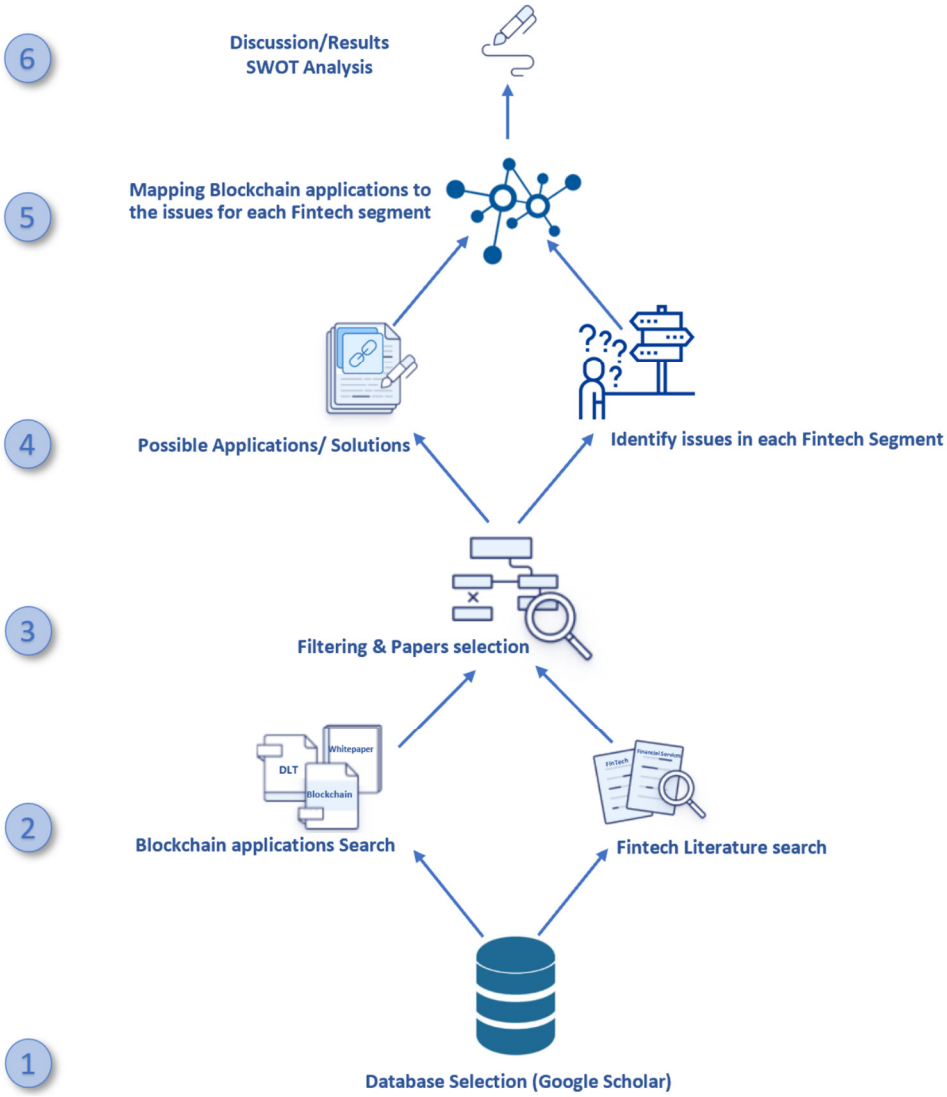

Figure 1. Procedures and methodology.

3. Blockchain Background

This section starts with an overview of blockchain architecture and smart contracts. A comparison of different open-source blockchain implementations for FinTech is provided. We aim to ensure the readers' familiarity with blockchain technology and its key characteristics crucial to FinTech.

3.1. Blockchain Architecture

A blockchain can be regarded as an append-only, shared, fault-tolerant, distributed database. A blockchain is immutable because all blocks are connected via hash functions. Any tamper of a block invalidates all the following blocks.

A chain is formed by connecting the blocks. Each block contains the hash value of the block before it (i.e., each block points to its previous block). The blocks consist of several time-stamped transactions collected from users' broadcasts. Each block also stores the time of creation. Each transaction is verified before its inclusion in a block.

By having the blocks linked to each other, an immutable data chain is prepared, whose copies can be safely kept on distributed network nodes. With a consensus protocol, a decentralized system can be achieved without a centralized authority controlling any data or mechanisms. When a node wants to carry out a transaction within the network, it broadcasts the transaction. Then, several nodes (i.e., Validators) check to ensure that the nodes involved and the transactions are valid, and then a block is made that consists of the valid transactions.

Once the new block is deemed valid, it is added to the database. If the block is not valid, the block is discarded. Therefore, it will not be added to the database. The transactions and the block are signed, so that future transaction revocation or repudiation is impossible. The transactions are bundled in a Merkle tree [27]. Each block contains the hash of the previous block in the chain. The very first block of the chain is called the genesis block.

By network structure, blockchains can be classified into four categories: public blockchains, private blockchains, consortium blockchains, and hybrid blockchains.

Public blockchains are fully decentralized, permissionless, and public, where everyone can participate. This ensures that there is no centralized entity that controls the network. Therefore, such a network has no single point of failure and no data monopoly. Bitcoin [28], Ethereum [29], Litecoin [30], and USDF [31] are popular examples of public blockchains. However, this type of blockchain suffers immensely from a scalability issue. Achieving a consensus among a large number of nodes is generally slow.

A private blockchain network implies that the nodes need to be granted access to the network and authenticated, hence "permissioned." For example, Hyperledger [32], Quorum [33], and R3 Corda [34] are all private blockchains. Many banks are shifting their financial services toward utilizing private blockchains for more secure, faster processing, with more transparent and lower-cost processes than traditional banking [35]. Although private blockchains can provide more granular control over who belongs to the network, they sacrifice some decentralization by introducing a network administrator to control access. Nonetheless, the distributed data among the participating parties are still traceable and immutable.

Private blockchains are highly scalable, the network size can be customized to match the need, and new nodes can be added to the network as required. However, a centralized identity and access management system is needed to implement access control to the network and the data.

A consortium blockchain is a semi-decentralized blockchain where two or more parties (e.g., financial institutions) manage the blockchain network. Banks and government entities usually utilize this type of blockchain. Examples of this blockchain are CargoSmart [36] and the Energy Web Foundation (EWF) [37].

A hybrid blockchain is a combination of private and public blockchains. Only a selected amount of information is allowed to go public while keeping the rest confidential. The idea of incorporating both types is to keep part of the information private while allowing more nodes to join the network for scalability. IBM Food Trust [38] is an example of a hybrid blockchain.

Note that private blockchains, consortium blockchains, and hybrid blockchains are permissioned blockchains that require authorized permissions to access networks and data.

3.2. Consensus Algorithms

Consensus algorithms are required in distributed ledgers (i.e., blockchains) to get all nodes in the system to agree on the content. When a node appends a block to the chain, the other nodes should also append the same block to maintain blockchain integrity.

For example, in the Proof-of-Work (PoW) algorithm, all nodes complete solving a mathematical puzzle. The puzzle selected by the Bitcoin community is to find a nonce that hashes below a specific value. Whoever solves it first and broadcasts their block has it

appended to the chain. The process of verifying the nonce is computationally cheap. Therefore, nodes can verify the new block and append it to their copy of the chain. In PoW, the incentive for mining transactions lies in economic payoffs. Numerous alternative consensus algorithms have been developed for blockchains, namely Proof of Work (PoW), Proof of Stake PoS [39], Istanbul Byzantine Fault Tolerant (IBFT), leader-free Byzantine consensus [40], implicit consensus [41], ELASTICO [42], Proof of Trust (PoT) [43], Delegated Byzantine Fault Tolerant (DBFT) [44], Proof of Participation and Fees (PoPF) [45], Proof of Vote (PoV) [46], Delegated Proof of Stake (DPoS) [47], and Delegated Proof-of-Private-Stake (DPoPS) [48].

In this subsection, we briefly discuss Proof-of-Work (PoW) [28], Proof of Stake PoS [39], Byzantine fault-tolerance (BFT) [49], and RAFT [50] to ensure the readers' familiarity with the consensus algorithms utilized in blockchain-based FinTech Applications.

Proof of Work (PoW): PoW [28] is the consensus algorithm adopted in the Bitcoin blockchain. Under PoW, nodes (called miners in Bitcoin) solve a computational task to generate a new block. The computational task is finding a value that, when hashed with SHA-256, results in a number beginning with a pre-specified number of zero bits.

The difficulty of the task and the average work required are exponential in the number of zero bits required. The block can be verified by executing a single hash and added to the chain. If most nodes add a block to their copy of the chain and then generate new blocks pointing to it, this indicates a consensus that it is the correct next member of the chain.

Assuming the majority of the nodes in the network are honest, PoW consensus is resistant to Sybil attack [51], in which an attacker can acquire multiple identities (i.e., nodes) in a distributed system and use them to gain a significant influence (consensus). PoW forces every node on the network, whether it is a malicious or honest node, to carry out an equal amount of computational power. This makes it very difficult for an attacker to alter a past block as they would have to redo the hash pointer of the block and all the subsequent blocks to catch up with and surpass the work of the honest nodes.

A big problem with PoW is that computation of the hash wastes too many computing resources. Many studies [52,53] worked on improving the original PoW mechanism. For example, SPECTRE [54] is a consensus protocol that allows a parallel block creation on the block direct acyclic graph (BlockDAG). This operation improves the transaction throughput and reduces the confirmation time of Bitcoin.

Bitcoin-NG (Next Generation) [55] is another example of a leader-election PoW consensus protocol. Bitcoin-NG introduces two types of blocks: key blocks and micro blocks. Key blocks are only used for the leader's election. Once a key block generated by a node is accepted, it becomes the leader. The micro block contains the packaged transaction data and ledger entries. Thus, transactions can be processed continually until the next leader is elected, significantly reducing transaction confirmation time and improving scalability.

The Greedy Heaviest-Observed Sub-Tree (GHOST) [56] consensus algorithm follows the heaviest sub-tree rule when appending blocks to the chain to eliminate double-spending [57] attacks on Bitcoin. This rule is more secure than the longest chain rule as it is independent of the size of the blocks or the block creation rate.

Proof of Stake (PoS): In PoS [39], validators are selected based on the number of coins that the validator stakes. The nodes having more stakes will have a higher opportunity to add the next block to the chain. A new leader is elected using random criteria based on the amount of stakes that a node (i.e., miner) possesses. Ouroboros [58] and Casper [59] are examples of PoS algorithms.

Ethereum 1.0 utilized the PoW consensus protocol. Later, in Ethereum 2.0, PoW was replaced by Proof of Stake (PoS) to increase the network's scalability and power efficiency.

Byzantine fault-tolerance (BFT): BFT [49] is called Byzantine as the algorithm can cope with some fraction of "Byzantine nodes"—nodes that are faulty and behave arbitrarily. They can lie or intentionally mislead other network nodes, delay message delivery, and cause disruption. Examples of BFT protocols are Trinity [60] and Exonum [61].

Reversible Addition-Fragmentation Chain-Transfer (RAFT): The RAFT algorithm [50] achieves consensus through an elected leader responsible for log replication to the followers, where followers blindly trust their leader. A follower node becomes a leader candidate if it receives no communication from its leader over an election timeout period. Quorum utilizes RAFT as its consensus algorithm.

Istanbul Byzantine Fault Tolerance (IBFT): IBFT[62] is a proof-of-authority Byzantine fault-tolerant consensus protocol. It uses a group of validators to ensure each proposed block's integrity. The majority (around 66%) of these validators must sign the block before it can be added to the chain. The group's leadership also rotates over time, ensuring that a faulty node cannot have long-term effects on the chain. Validators do not assume that all leaders are trustworthy or honest and do multiple rounds of voting to arrive at a consensus.

3.3. Smart Contract

A smart contract is an innovative way to trigger a "contract" program where the deposited cryptocurrency is transferred when a predetermined condition or set of conditions is met. Smart contracts are contractual clauses that have been converted into lines of code that can be run on top of a blockchain.

The purpose is to embed the contractual clauses into a blockchain such that they can be enforced automatically. Smart contracts reduce the risk of contract violation, decrease cost and increase trading efficiency [63].

Smart contracts adhere to the immutability of the blockchain, meaning that they cannot be altered once issued. Behaviors that violate the contract, such as financial fraud, can be avoided in some cases.

The elimination of a third party allows an automatic settlement of financial transactions, improving businesses' efficiency in addition to reducing turnaround time and removing the need for reconciliation between parties (i.e., cross-border banks) that speed up transactions and the settlement of trades for FinTech companies.

3.4. Digital Wallets

Digital wallets are financial applications that allow users to store public and private keys for their cryptocurrency transactions. Based on internet connectivity, blockchain-based wallets can be categorized into cold and hot wallets.

A hot wallet is always connected to the internet and cryptocurrency network. It is used for day-to-day transactions. Cold wallets are called "vaults." They are not connected to the internet and allow users to store cryptocurrencies with a higher level of security. Cold wallets are less convenient for active traders as they have to move the amount of cryptocurrency to a hot wallet or power on cold wallets and connect them to the internet to carry out transactions.

3.5. Blockchain Platforms Adopted in Financial Services

FinTech companies are shifting towards blockchain-based financial services for security, scalability, and efficiency compared with traditional financial services.

Table 1 summarizes the five main properties of blockchains critical to FinTech.

Table 1. Properties of blockchains.

Characteristics	Description
Decentralization	No longer need a third party to verify transactions on the blockchain. The network does the verification of these transactions using a consensus algorithm [64]
Security	Blockchains employ asymmetric-key crypto algorithms and hash functions. The chain stored in a distributed ledger makes it secure [65]
Data integrity	The chain ensures that all the blocks are connected where every block contains its hash and the previous block's hash and, therefore, cannot be changed. The network would detect any modification. The chain is thus an immutable ledger that cannot be manipulated [66]
Auditability	All transactions are recorded and distributed; therefore, they can be verified and traced, enabling transparency between nodes within the blockchain network[66].
Fast Settlement	Blockchain can settle cross-border money transfers faster than traditional methods by eliminating the need for intermediaries' verification and reducing the transaction processing time [66].

3.6. Description of Blockchain Platforms

In this subsection, we discuss and provide a comparative analysis of the current and most popular open-source blockchain implementations. We start with Bitcoin. Then we discuss Ethereum, Hyperledger Fabric, Quorum, and R3 Corda implementations.

3.6.1. Bitcoin

Bitcoin introduced the concept of blockchain to the world. It was created by Satoshi Nakamoto [28]. It has been popular since its introduction and has enlightened many derivatives worldwide.

It is a permissionless public ledger record, meaning that the ledger of all Bitcoin transactions is accessible publicly and distributed to nodes worldwide. Since its creation in 2008, many have argued that Bitcoin should be seen as a speculative commodity rather than just a cryptocurrency.

The symbols used for bitcoin are BTC or XBT. BTC is short for Bitcoin. These abbreviations come from the International Standards Organization (ISO), which maintains a list of internationally recognized currencies. The "X" indicates that the currency is not associated with a particular country. Many FinTech applications are built on the Bitcoin distributed ledger, where the transaction records can be easily verified. We discuss these implementations in detail later in this paper.

3.6.2. Ethereum

Ethereum was created as an alternative protocol to Bitcoin and allows for building decentralized applications, writing smart contracts, and managing digital assets. Ethereum is a permissionless, open-source blockchain platform [67]. Its smart contract implementation and development kits are the most popular blockchain platform for decentralized applications [68].

Ethereum has a native digital currency called Ether (ETH) that has three primary purposes: to settle transactions through the exchange of ETH and enable network operations by using ETH as currency to pay transaction fees and store value. Ethereum has the largest enterprise ecosystem in the world [68], with an active technical community of over 300,000 developers and infrastructure experts coordinated by the Enterprise Ethereum Alliance (EEA) [69], which is dedicated to promoting Ethereum adoption and comprises

the world's largest companies such as Microsoft, JP Morgan, Accenture, ING, Intel, and Cisco.

However, Ethereum has a few limitations in terms of scalability, smart contract volatility, lack of a clear monetary policy, and some uncertainty with Securities and Exchange Commission (SEC) regulations. The momentum of implementing Ethereum for financial services comes from the blockchain's smart contract capabilities and its heavy involvement in decentralized finance. Ethereum 1.0 utilized Proof of Work (PoW) as its consensus algorithm, resulting in around 40 transactions per second.

Later, Ethereum 2.0 [70] replaced PoW with Proof of Stake. Ethereum 2.0 has recently become the preferred platform for FinTech because it can handle up to 3000 transactions per second, which is faster and yet more efficient than Bitcoin or Ethereum 1.0.

3.6.3. Hyperledger Fabric

Hyperledger Fabric is an open-source consortium maintained under the Linux Foundation and has more than 200 members from various global companies, including financial services, for example, Visa-integrated Hyperledger Fabric for Business-to-Business (B2B) blockchain payments in 2018 [52]. Hyperledger Fabric enables blockchain adoption for industrial applications as well.

The Hyperledger Fabric is a permissioned, private blockchain platform where the participating nodes can transfer assets. The transactions are directed by Chaincode [71]. Chaincode is what executes the functionality of a smart contract within the Hyperledger Fabric framework. The execution of the Chaincode creates the interactions between the nodes and the shared ledger. All nodes within the network need to know and maintain the identity of the other nodes.

There are subnetworks within the larger Hyperledger network, called channels. Channels are restricted to a particular subset of the nodes. A channel can create its own ledger that only maintains a record of its transactions and digital assets and can only be accessed or viewed by nodes in that channel [35].

Hyperledger supports a Hardware Security Module (HSM) that is vital for managing and protecting the digital keys and its modular architecture, which supports plug-in components [32]. Hyperledger provides modified and unmodified PKCS #11 for key generation. PKCS #11 [72] is one of the Public-Key Cryptography Standards (PKCS).

Some implementations may suffer from a lack of transparency. This may lead to data monopoly or tampering, in addition to the limitation in terms of scalability [73].

3.6.4. Quorum

Quorum is a permissioned version of the Ethereum blockchain. It was developed by JP Morgan and was later acquired by ConsenSys. Since it is a permissioned blockchain, nodes must be verified before entering the Quorum network. The consensus algorithms used by Quorum are RAFT and IBFT in place of the PoW implementation of Ethereum 1.0 and Bitcoin. Privacy is preserved in Quorum as transactions are not visible to members of the larger network. This is similar to Hyperledger's channels, where some transactions can only be visible to a smaller group of network nodes maintained on a smaller, private ledger. Quorum is referred to as a free gas network, meaning that there is no "mining fee" for transactions, and there are no cryptocurrency costs associated with its transactions (i.e., Gas is set to zero) [74].

3.6.5. R3 Corda

R3 Corda is a private, permissioned, open-source software project that creates the Corda Network [21]. The main benefit of Corda is that it eases managing contracts and reaching agreements between parties, especially when there is not enough trust between the parties by using smart contracts. Unlike Hyperledger or Ethereum, to achieve

consensus, it uses the idea of notary pools. The details of this consensus method can be found in the introduction to the Corda Platform Whitepaper [75].

Corda focuses mainly on financial services to create a global independent network and therefore abstracts away many of the typical blockchain structure's components that cause time and computational overhead. However, the full functionality of the Corda blockchain platform can be achieved by utilizing the components provided by Hyperledger. In addition to the fast operational speeds provided by Corda, it also helps FinTech companies optimize inter-company cooperation's costs and efficiency, where data can be shared only among permissioned nodes.

Quorum provides the fastest transaction throughput compared with the other blockchains' original implementations. However, it is less flexible.

Ethereum provides security with limited scalability and is less efficient (i.e., low transactions per second) and thus does not apply to time-critical situations. Hyperledger fabric conducts transactions much faster than Ethereum. This is expected since the latter is based on a permissionless blockchain.

R3 Corda also has higher transaction rates than Ethereum 1.0 but has lower throughput than Hyperledger Fabric. As mentioned before, a Hyperledger Fabric with its "plug-n-play" components can be built to perform similarly to the Corda platform.

However, the highest transaction throughput was reported by Ethereum 2.0. There is no standard yet when it comes to blockchain performance measures. Experiments are limited by resources and often are focused on specific use cases. Therefore, these measurements are not necessarily accurate.

Table 2 provides a comparative summary of the key characteristics of the top five blockchain implementations.

Table 2. A comparison of the top five blockchain implementations.

Characteristics/Platforms	Ethereum	Hyperledger Fabric	Quorum	R3Corda	Bitcoin
Platform Description	A general platform for blockchain solutions	Business- to- Business centric blockchain modules [76]	Financial-focused DLT [77] (built on Ethereum)	Financial-focused DLT [77]	A general platform for blockchain solutions
Governance	Ethereum developers	Linux Foundation	ConsenSys	R3	Bitcoin developers
Blockchain Type	Private/Public	Private	Private	Private	Public
Access Type	Permissionless	Permissioned	Permissioned	Permissioned	Permissionless
Consensus Mechanism	PoW, PoS	Multiple	RAFTIBFT, PoA [78]	Own Implementations (NotaryNodes) [34]	PoW
Smart Contract	Yes	Yes	Yes	Yes	No
Digital Currency	Ethers and tokens through smart contracts	No native asset, Internal token [79]	None	Native token, XDC	BTCorXBT
Throughput (Transactions/Sec)	ETH1.040 [67] ETH2.03000 [70]	300 [76]	750 [77]	170 [80]	7–10

4. Fintech Background

This section discusses the difference between 'Decentralized Finance' (DeFi) and centralized finance (CeFi). Later we provide an overview of FinTech evolution.

It is important to differentiate between 'Decentralized Finance' (DeFi) and Centralized Finance (CeFi). Traditional finance fundamentally depends on the trust and confidence of the intermediaries that centralize financial functions and resources. It is usually referred to as centralized finance (CeFi). Decentralized finance (DeFi) emerged with the

promise of eliminating centralized governance and intermediaries, transforming traditional finance into a trustless and transparent protocol [81,82].

Three factors made DeFi possible [24]. First, Moore's law is the principle that the amount of data processing grows exponentially. Second, Kryder's law is the principle that the amount of data storage grows exponentially. Thirdly, there is an advancement in communications bandwidth with a decrease in cost. This allowed advancements in AI, blockchain and distributed Ledgers (DLT), Big data, and Clouds.

Fintech existed before blockchain technology, and the use of this term evolved with time [83]. This may prove confusing. Fintech can be used for CeFi [84,85], utilizing the evolution of traditional finance innovation using technologies such as instant messaging and cloud computing to provide financial services, while others [86] use the term to indicate the distributed technology (e.g., DLT, blockchains) used to provide DeFi services [87]. We shall use the latter meaning throughout our paper unless we indicate otherwise.

The development of FinTech experienced several different phases [88]. Although the roots of FinTech can be traced back to the 19th century, we see that the term only gained traction in the 21st century in concurrence with recent technological advances.

The first age of financial globalization is dated back to 1866, when trans-Atlantic cable was used for the first time to verify signatures in banking transactions operating between Paris and Lyon, France. In the late 1800s, consumers and merchants started to exchange goods using cards for the first time in history. Charga-Plate was an early predecessor of the credit card we know today. Charga-Plate is a small metal card. The transaction record was made using an imprinting machine by pressing an inked ribbon against the card with the embossed transaction information. In 1918, federal reserve banks established Fedwire Funds Service to transfer funds by connecting all Reserve Banks by telegraph using a Morse code system. In 1920, Keynes, in his famous book, "The Economic Consequences of the Peace" [89], published right after World War I, took the lead in highlighting the inter-linkage between finance and technology. In 1964, the Charg-It card was launched by John C. Beggins to be used in a two-block radius of Flatbush National Bank in Brooklyn, New York.

The second generation of FinTech, "FinTech 2.0," was marked by Barclays' introduction of the first ATM. In 1974, the Equal Credit Opportunity Act was signed by President Gerald Ford, prohibiting and punishing any creditor discrimination against consumers. The year 1982 marked the birth of the first online brokerage, "E-Trade," which allowed the execution of electronic trades by individual investors.

FinTech 2.0 aimed to seamlessly integrate and combine customers' financial needs in one place. Fintech 3.0 was born on the heels of the economic recession. The financial crisis of 2007–2008 started the disputable argument about who has the legitimacy to own and provide financial resources. The crisis deteriorated public perception of and trust in banks. The post-crisis strict regulations for FinTech 3.0 opened the market to new providers and allowed open banking, which allows third-party companies access to financial data.

Fintech 3.0 marked the emergence of Bitcoin, followed by other cryptocurrencies using distributed ledger technology (DLT). Distributed ledger technology is also called a shared ledger, where the recording of the transaction of assets is distributed across multiple nodes. Thus, distributed ledgers have no central data store or administration functionality. The challenges brought by the global pandemic in 2019 marked the beginning of FinTech 4.0 [90].

The COVID-19 pandemic increased the demands for digitization and decentralization. BigTech platforms (e.g., Meta, Google, Amazon) have increased significantly during the COVID-19 pandemic. These platforms have been able to reap the benefit of having a large number of users through online payments, credit, insurance, and digital wallets. Annual FinTech financing and investments by venture capitals, private equity, and cross-border mergers and acquisitions reached $210 billion by 2021 [91]. They had been doubling over the preceding years ($112 Billion by 2018). FinTech companies were brought about due to the surge of the technological age.

Technology companies spotted this need and have jumped in to provide the architecture, software, and services that enable these financial institutions to continue to provide the services on computer-based platforms [92]. There are currently over 8775 financial services startups in the North American region, 7385 in Europe, the Middle East, and Africa combined, and 4765 in the Asia–Pacific region [2]. FinTech companies have adopted many technologies, starting with Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), and Blockchain. Blockchain-based FinTech implementation and application are the focus of this survey paper.

Blockchain-based applications for the FinTech sector were motivated by the blockchain's decentralized potential for finance. In this paper, we study the three main categories of FinTech services [26]: Payments Services, Deposits and Lending, and finally, Investment Management Services. In this paper, these different services will be described as segments within the FinTech sector.

Figure 2 shows a sample of the current FinTech companies within their assigned FinTech Segment.

Figure 2. FinTech companies and segments.

The first segment is the Payments segment, which provides new and easier payment methods without centralized authorities. For this reason, the payments segment continues to be the largest segment of the FinTech space. The next most significant segment is the deposits and lending segment. With application processes and background checks already being done online, this was a big avenue in which technology companies could apply big data principles and find a way to streamline the loan and refinancing processes even further to make them more accessible. Following deposits and lending, the investment management space is the next most significant and certainly more blossoming (as of recent times) segment of the FinTech space. More novice investors are putting their money into apps that help them to make investment and trading decisions. Investment management companies allow the investing process to be more tangible and accessible and offer a friendly and straightforward user interface. Each segment can be further broken up and categorized by various companies' services, goals, and specializations.

For blockchain-based FinTech, it is crucial to understand what exact services a company is attempting to provide in order to understand the core components of these services. By understanding these components, one can formulate a plan to understand the requirements for the technology within this space.

4.1. Payments Segment

Payment is currently the most significant segment that is continually growing larger. A crucial reason for this growth is that access to mobile devices, data networks, and applications has allowed FinTech companies to lure traditional banking customers away from legacy banking platforms. These applications then enable users to interact directly with vendors, removing third-party brokers [26]. Companies focused on the payments segment are now driving innovation to increase blockchain-based applications' efficiency and accessibility [93].

This segment can be broken up into categories that specify what services they offer within the payment realm. Table 3 discusses the different payment segment categories [26] and briefly describes the services and companies in each category.

Table 3. Payments Segment Categories.

Subsegment	Services	Companies
Consumer Payments	Services and technologies that are focused on the payment between consumers and payment issuers	Doxo, Headnote, Affirm, Paypal, Stripe, Zelle, Ripple, Stellar
Financial Transaction Security	Companies that focus on security within financial transactions, such as securing transactions, authenticating users, and preventing overall fraud/theft	Venmo (a service of Paypal)
International Money Transfer	Companies that enable sending money (both personal and business) across countries	Remitly, Paypal, Ripple, SureRemit, Everex
Payment Backend and Infrastructure	Enabling payments by providing the infrastructure to payment issuers and acquirers	Circle, Stripe.
Point of Sale Payments	Focused on payment acquirers (businesses and	Square, Algorand, Pauni-X

	organizations) by providing the infrastructure as well as physical hardware for payment solutions

4.2. Deposits and Lending Segment

Deposits and lending is another huge segment in the FinTech space. The purpose of this segment is to simplify the traditional banking flow. This includes storing the money in the bank (i.e., deposits) and building interest on that money. It also incorporates companies that enable people or businesses to obtain loans (i.e., lending) and monitor/collect information about credit. We highlight the top three categories of the deposits and lending [26] segment and provide exemplary services and companies for each category in Table 4.

Table 4. Deposits And Lending Categorizes.

Subsegment	Services	Companies
Business Lending	Offering new ways for companies to assess their credit risk and raise financing for their debt	Credifi, Peer IQ, Celsius, Figure, Colendi
Consumer and Commercial Banking	Allowing businesses and consumers to interact with banking services more simply and easily.	J.P. Morgan & Co, Wells Fargo
Consumer Lending	Providing new ways for people to obtain loans and assess their credit risk	Salta, Tala, Avant, Celsius, Figure, Colendi

However, some FinTech companies can fit in more than one category based on their services. These companies attempt to simplify the loan process by finding different ways to assess credit risk. They provide various ways for companies to collect data and analytics to simplify the background checking process and shorten the turnover time of loan applications and loan grants/rejections. PeerIQ[94] is an example of a company that provides risk analytics and decision-making tools to help FinTech lending institutions to analyze, access, and manage lending risk.

4.3. Investment Management Segment

The Investment Management segment of the FinTech sector is mainly comprised of companies that attempt to invest in a simple automated process. These companies ease access to various securities for those less familiar with finance. Table 5 highlights different segments [26] of Investment Management companies. Example services and companies for each segment are provided. Still, most FinTech companies provide one or more services and, therefore, can fit within more than one category within the same segment. Table 5 highlights deposit and lending subsegments.

Table 5. Deposits and Lending Categorizes.

Subsegment	Services	Companies
Financial Research and Data	Businesses that enable people to make informed and better investment decisions by providing information services	Addepar
Institutional Investing	Directed towards managers (wealth/hedge fund)and other professional traders, these businesses help manage portfolios to optimize their return on investment	Wealthfront, Betterment

Retail Investing	Companies that enable investing insecurities with new methods and means. These services are targeted toward newer and younger investors.	Robinhood, Webull, Interactive Brokers

5. The Payments Sector

The payments sector consists of three segments: retail and consumer payments, point of sale payments, and international money transfers (remittances). This section discusses six FinTech companies (Stellar, Ripple, Algorand, Pundi-X, SureRemit, and Everex), two for each segment. We highlight how blockchain technology is leveraged to solve the sector's problems.

5.1. Retail and Consumer Payments

This subsection discusses two retail and consumer payments FinTech companies, Ripple and Stellar. With increased users in online shopping, ride-sharing, food delivery, etc., payment methods have now moved away from in-person exchanges of money and gravitated toward digitization.

Oliver Wyman, a leading international management consulting firm, proposed that the payments space has become key for a seamless shopping experience that provides a unique competitive advantage [95].

The ability to leverage blockchain allows customers to use cryptocurrency in their transactions and allows a faster transaction settlement due to the reduction of centralized verification.

Currently, many transaction fees are associated with traditional banking strategies within the FinTech space. With the rise in payment solutions, technology experts have been trying to leverage different mechanisms to alleviate these fees. For example, merchants send batches of authorized transactions to their payment processors. A payment processor allows merchants to handle customer transactions via various channels such as credit/debit cards or bank accounts.

For every transaction, the card issuer charges the merchant a fee, and the payments processor charges a fee to facilitate all of the background work to perform the transaction. Therefore, the merchant has to pay additional fees to accept a customer's payment. According to Square, the average cost for payment processing is about 2.87% to 4.35% per transaction [96].

Along with transaction fees, the intermediaries (i.e., payment processors) create time delays during the transaction. Each intermediary has to process and validate the transaction, then send it to the next intermediary to process. Each intermediary processing the transaction increases the transaction time. This is not only inefficient but also poses a risk for fraud.

Blockchain payment solutions can eradicate transaction fees, allowing customers and merchants to settle transactions without intermediaries. Most existing payment solutions attempt to find the path with the least intermediaries to reduce cost.

Most blockchain payment methods can remove transaction fees by using smart contracts to remove all the intermediaries and decrease the time spent at each intermediary.

Removing all intermediaries (e.g., permissionless blockchain) or reducing the number of intermediaries (e.g., permissioned blockchains) gets rid of high transaction fees and reduces transaction times.

Another challenge in this category is the transaction error rate and lack of transparency. Errors in transactions within payment processing occur for many reasons. Sometimes there can be issues with the physical condition of the card, whether or not there is money in the card holder's account or even the merchant's terminal. There can be a lack of authorization, a duplicate charge, or even an incorrect amount charged [97]. As the

transaction passes through so many intermediaries, it is problematic to localize the step where an error occurs and thus troublesome to recover the loss.

Blockchain allows the entirety of the transaction to be transparent and immutable. Therefore, if one of the transaction participants is fraudulent, it is evident and easy to localize the fraudulent transactions.

Furthermore, the consensus mechanism that governs most blockchain payment solutions ensures that errors are minimized or eliminated. A lack of traditional financial services is the main issue that small-to-medium businesses face.

That is because they are not connected to a large financial institution. This is quite common in countries that lack the infrastructure to support large financial institutions but have many small-to-medium banks. These small-to-medium banks lack the same services as their larger counterparts or cannot conduct currency conversion. Without some basic services, merchants have difficulty processing and conducting electronic payments.

Blockchain enables small-to-medium banks to operate internationally by connecting them to larger financial institutions and banks worldwide. This way, when paying with fiat money or cryptocurrency, the transaction can travel through many intermediaries within the blockchain network. Thus, small-to-medium businesses can conduct the same transactions that larger businesses can do with large banks. This has opened up commerce in many areas of the world.

5.1.1. RippleNet

RippleNet is a network of financial entities such as banks, payment providers, and other financial institutions [64]. RippleNet routes payments among the financial institutions on their network to settle transactions. The network itself is a decentralized global network that uses a Ripple-developed consensus protocol to validate account balances and transactions within the network. The network keeps track of all the transactions that occur and are publicly recorded and viewable. RippleNet uses Ripple Cryptocurrency, XRP. By having banks and payment providers within the network, Ripple removes the fragmentation within the payments processing landscape. Fragmentation results from the lack of interconnection between multiple securities markets. It can reduce the effectiveness of mass marketing techniques, erode brand loyalty, and result in customer orders being directed to markets that do not necessarily offer the best price.

Ripple's solutions have opened up many services for small-to-medium banks and merchants, especially in countries with little financial infrastructure. RippleNet's integration allows small banks and merchants to complete transactions.

Access to the network allows these previously challenged companies to complete cross-border transactions and allow different payment services locally. It also allows Ripple's financial partners to reach many customers that they would not have been able to reach before due to the lack of infrastructure.

5.1.2. Stellar Network

The Stellar Network is a peer-to-peer payments network that originates from the early iterations of the XRP Ledger developed by Ripple. Stellar's consensus protocol (SCP) utilizes smart contracts to carry out transactions [98].

It uses the Quorum blockchain to emphasize security and speed up transactions within the network by utilizing the slices. A Quorum slice is a subset of nodes on the network that a given node chooses to trust and depend on [99].

Stellar allows each node to choose what node is within its "trusted zone" (slice), enabling open participation and more jurisdiction over who is validating the transactions, leveraging the trust built through interpersonal interactions.

Interpersonal interaction is the communication that occurs between interdependent nodes that have some knowledge of each other. However, to reach a global consensus, there have to be intersections between Quorums—meaning that one node in the Quorum slice must also be in another Quorum slice to maintain the integrity of the network. This

allows the network to reach a consensus without relying on a centralized/closed system. Quorum slices allow transactions to be accepted quicker by the nodes in the Quorum, thus increasing the speed at which the transactions are carried out.

Since the protocol also allows an open network, there are many ways to decrease the number of intermediaries the money travels through, thus providing shorter options that decrease transaction fees. Quorum slices play a significant role in ensuring the security of each node and the validity of transactions. Table 6 compares and summarizes the solutions provided by RippleNet and Stellar Network.

Table 6. Retail And Consumer Payments Chart.

Problems Faced by Financial Institutions	Solutions Provided by Ripple's Blockchain	Solutions Provided by Stellar's Blockchain	Ripple's Current Implementation Issues	Stellar's Current Implementation Issues
High Transaction Fees and Time Delays	RippleNet finds the most efficient (time and cost) path through its network of banks to complete the transactions.	The Stellar consensus protocol utilizes Quorum slices to ensure that transactions can be validated in a matter of seconds with the least amount of fees possible.	Ripple charges quite a bit for transactions that take place on RippleNet. XRP can reduce transaction times, but they are still too high. Cross-border payments need to be faster.	Stellar charges fees in their native currency, Lumen, which has proven to be highly correlated with the price of Bitcoin [98]. Therefore, it can be volatile. If the transaction needs to be converted into multiple currencies, the transaction time can increase
Errors in Transactions	Blockchain implementation provides transparency through DLT by information redundancy and transaction immutability that is visible.	The Quorum Intersection ensures that a general consensus is made such that there are no errors in deductions from accounts.	-	Because of the consensus protocol, there have been cases of errors occurring when a transaction starts with insufficient funds or due to nodes being offline
Lack of Transparency	-	A decentralized, immutable blockchain system provides transparency.	Ripple is centralized as a majority of the nodes belong to Ripple. Thus, the possibility of complete transparency is not possible.	-
Lack of Traditional Financial Services (Small-to-Medium Banks)	RippleNet connects banks through its infrastructure so that small-to-medium banks can complete cross-border transactions.	Stellar connects banks across the world in a public manner. This means that anyone can join the Stellar network.	There may not be a bank in that country of interest that has enough money to complete large transactions as not many well-funded large banks are part of the RippleNet.	-

5.2. Point of Sale Payments

This segment focuses on the actual place and technology used when a consumer initiates transactions for goods and services provided by a merchant. Point of Sale payments can be online or in-person.

This facilitates the transactional process from customer to merchant. It can also provide order management, inventory tracking, and card payment processing services.

One of the main issues faced by the point-of-sale segment is the high fees. That is because the point of sale systems are often physical devices in stores that can vary from cheap to costly. Whether or not a merchant buys or rents their hardware and software, there is still a non-negligible upfront cost. On top of the existing system, most points of sale vendors charge payment processing fees. Some vendors will allow the merchant to work with a third-party credit processor or require the merchant to pay some fee per transaction.

Other vendors also enforce processing service fees. These fees accumulate over time, and the merchant loses quite a bit of profit to fees. To cover these fees or the cost of the point-of-sale system, merchants often charge the customer a fee for processing the transaction. A point of sale operating within a blockchain framework can prevent processing fees regarding payment. The payment is quickly processed on the network itself. In addition, blockchain provides transparency, so merchants and customers can see all fees associated with the transaction.

Another issue is scalability. Since the point of sale systems tend to have physical devices in stores or online payment systems, the ability to scale is somewhat limited. Merchants fear many taxes and fees associated with credit card providers in addition to the allowed transaction rate in a given time frame. Maintaining large amounts of information is another challenge. Currently, traditional point-of-sale systems are required to maintain several databases and store information of various parties they need to connect with.

The information that needs to be stored relating to customers, such as billing, ratings, and orders, can be stored on individual nodes within a blockchain. Additionally, inventory can be stored on nodes across the chain. Alternatively, the network can be built on top of a decentralized database that can be accessed by nodes when needed. Smart contracts can then trigger processes regarding incoming data and ensure that transactions between existing and new nodes are complete and valid. This ensures security, as there is no one centralized database that can be tampered with [100].

5.2.1. Algorand Blockchain

The Algorand blockchain is a payment solution with its point-of-sale implementation. Their application acts as a point of sale and communicates with a crypto wallet containing its currency ('Algo') through a transaction gateway. The Algorand process starts with an application that captures the transaction details and creates an unsigned transaction that is then sent to the transaction gateway. The transaction gateway forwards it to the wallet. The signing wallet receives the unsigned transaction and waits for approval from the consumer. The transaction gets signed and returned to the gateway if the consumer approves it.

The entire receipt is stored in an off-chain storage system—essentially recording the transaction in an immutable manner so it can be retrieved when needed [101]. The storage system eliminates the need for data to be managed by the point of sale system/application as it is stored on an off-chain system. That way, all the data can be managed and retrieved at any time. The Algorand blockchain uses a pure PoS consensus algorithm that requires minimal computation.

The Algorand blockchain can handle around 1000 transactions per second [102]. This increases efficiency, allows the blockchain to scale more rapidly, and significantly reduces settlement times.

Additionally, since the blockchain operates within its own network (from the point of sale application to the gateway into the wallet), there are no outside transaction fees associated with intermediaries in the transaction. The point of sale solution relies entirely on Algorand's currency, 'Algo.' Limiting to one currency poses a threat to scaling as it forces consumers to make an initial investment in Algos to carry out the transactions.

5.2.2. Pundi-X

Pundi-X is an end-to-end platform that allows consumers to use cryptocurrency at retail points of sale [103]. Consumers must have a mobile wallet to use the platform. The mobile wallet maintains the public key encryption behind a standard password-based system to be user-friendly.

The platform also allows for "physical" smart card information to be loaded by the mobile app and allows the currency to be used even without access to a smartphone. Although Visa and Mastercard have networks that enable using cryptocurrency as payment through conversion to a fiat currency, the issue is that not all locations worldwide have access to these services.

Pundi-X targets under-serviced countries where it allows merchants and users to begin to transact more digitally. Pundi-X is currently marketing in Indonesia, giving a hardware device to merchants in retail environments when a smartphone is available. Merchants can carry out their transactions on a smartphone-based application as well.

The merchant sets all the rates required for the transaction at about 1–2%. 65% of that fee is given to the merchant, while the rest is given to Pundi-X or the digital asset issuer. Though this does not eliminate third-party fees, merchants still control the fee being charged.

The merchant is also very aware of who is receiving the fees. With the rise of digital assets, the Pundi-X platform enables people to use some of their investments to pay for goods. Most cryptocurrencies can be used on the Pundi-X platform. The platform is open, allowing digital assets to be submitted and evaluated on the possibility of being used as currency.

This enables long-term scalability as it allows the platform to start incorporating popular digital assets and opens up accessibility to various regions of the world. Furthermore, Merchants can choose whether to accept their payments in fiat currency or a stablecoin. A stablecoin is a crypto asset that is backed one-to-one by the U.S. dollar or other fiat currencies. Therefore, if a consumer chooses to pay with a more volatile coin, the merchant controls the currency in which they receive that payment. This has been very interesting for institutional players as it allows consumers to trade crypto at the institutional level.

A volatile coin is a cryptocurrency whose value and price fluctuate heavily by investor and user sentiments, government regulations, and media hype. On the contrary, stablecoins are unaffected by market volatility.

Pundi-X allows customers to keep their investment in stablecoins that remain in the digital assets space whenever the markets become volatile instead of selling all cryptocurrencies and moving to cash until they return to trading actively.

An issue for scalability may arise as the ledger needs to maintain much more information than just a simple transaction, especially if it is being used to calculate inventory for a merchant. Therefore, this large data storage could affect scalability and transaction time. Additionally, scalability comes into question when it is realized that a physical offline device is needed to scale the platform's use as a whole. Therefore, since the XPOS machine is acting as a node, there will be slow growth when the adoption process is slow.

Figure 3 summarizes the issues faced by financial institutions within the point-of-sale subsegment. In Tables 7 and 8, we summarize the solutions provided by Algorand and PaundiX.

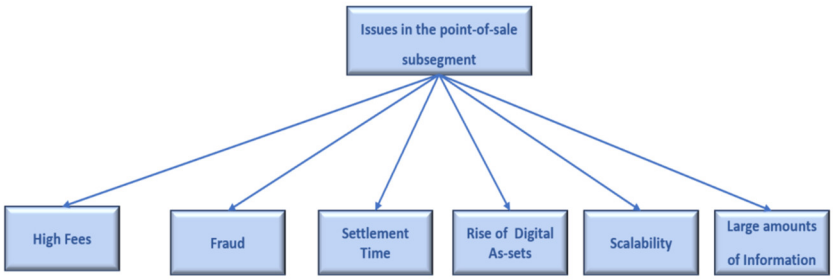

Figure 3. Issues faced by financial institutions within the point of sale subsegment.

Table 7. Point Of Sale Payments Chart.

Problems Faced by Financial Institutions	Solutions Provided by Algorand	Solutions Provided by PundiX XPOS	Algorand Blockchain Implementation Issues	PundiX XPOS Implementation Issues
High Fees	The fast transaction times incur fewer transaction fees. Thus, the high transaction fees associated with standard credit cards are avoided.	Merchant sets the fee rate (between 1–2%) and gets 65% of the service fee. The rest of the service fee is given to Pundi X or the digital asset issuer.	Since the transaction fee is 0.001 Algo/transaction, if the price of Algo increases, the transaction fee can also increase.	The merchants set the service fee rate, which can be between 1–2%; it is not standardized.
Settlement Time	Processes transactions within 5s such that the smart contracts execute and settle the transactions as fast as possible.	Transactions occur almost instantly– in less than half a second.	-	-
Fraud	Due to real-time settlement and immutable transactions, it is hard to initiate and complete fraudulent transactions.	The immutable transactions are recorded within the PundiX blockchain.	-	-
Rise of Digital Assets	-	Pundi Xwallet allows the management of digital assets and links with a card called XPass that can be used with XPOS machines. The Open Platform allows digital assets to be submitted to PundiX for use on the PundiX platform for scalability in terms of incorporating popular digital assets as payment. Merchants get paid in fiat currency or a stablecoin of their choice to avoid the risk of cryptocurrency volatility.	Users need to have a signing wallet linked to their Algorand account. The only crypto asset allowed to be used is Algo.	Users need to create an XWallet to use the XPOS terminals. To use the XPass, they must also link their card to the XWallet.

Table 8. Point Of Sale Payments Chart.

Problems Faced by Financial Institutions	Solutions Provided by Algorand	Solutions Provided by PundiX XPOS	Algorand Blockchain Implementation Issues	PundiX XPOS Implementation Issues
Scalability	The Algorand blockchain can process 1000transactions/second. This increases efficiency and the ability to carry out more transactions with security. It uses a Pure Proof of Stake consensus mechanism—meaning that the only factor that affects the block creator is the number of Algos held by the participant. This increases speed while maintaining decentralization.	The PundiX XPOS runs within the PundiX blockchain ecosystem. Therefore, the XPOS will scale with that of the blockchain as it acts as a node within the blockchain.	There have been issues with the consensus algorithm. When one node has too much stake—the other nodes cannot form a consensus.	Each XPOS terminal is a node. It has not been determined whether the PundiX blockchain can manage a large number of nodes.
Large Amounts of Information	Algorand implements off-chain storage,essentially a decentralized file storage system that encrypts the data and makes the content immutable. Open-source solutions such as Interplanetary File System or other commercial file systems can be used.	A receipt is printed at the terminal containing the transaction information maintained within the PundiX blockchain.	Blockchain transaction storage is limited, so a third party must act as an intermediary between the point of sale application and the blockchain. This can cause delays, errors, and efficiency loss.	One would need to use the PundiX interface to see the transactions made. A large amount of data storage can affect scalability and transaction time.

5.3. International Money Transfer (Remittance)

Blockchain has revolutionized cross-border payments. Several companies (such as Ripple, Everex, SureRemit, etc.) have capitalized on using blockchain for remittance.

This subsection discusses the current issues faced by the remittance international money transfer segment and reviews how Everex and SureRemit solve these issues. Currently, the remittance market is dominated by the Society of Worldwide Interbank Financial Telecommunication (SWIFT).

SWIFT is a network of banks that connects all corners of the world. For a transaction to be completed, the transaction must go through a clearing or settlement center before the transaction is cleared.

SWIFT itself does not settle the transaction. It simply confirms the consumer's transaction request. It is up to the banks to settle the transaction and relay the confirmation back to SWIFT so both sides can acknowledge the transaction's completion [104].

For a cross-border transaction to be executed, it has to pass through several banks because not all banks operate with a large variety of fiat currencies in other countries. Thus, a route between banks must be established to allow currencies to be exchanged into the desired receiving currency.

Blockchain can speed up the cross-border transaction time as a decentralized ledger. The transaction is settled almost as soon as the payment is made. By bypassing third-party intermediaries, sending money globally via blockchain reduces settlement time significantly.

Risk is another major issue while using international currency. The exchange rates for various fiat currencies change quite sporadically. Therefore, the long settlement time poses the risk of changing its value from when it is sent to when it is settled. Furthermore, most banks have a clause in their remittance contract that disclaims liability if the transaction remains incomplete. Thus, the risk is undertaken primarily by the person who initiates the transaction (the sender of the money).

A blockchain architecture mitigates the risk associated with currency exchange rates as the transactions are settled in real-time. Thus, the value sent is likely to be completed with minimal conversion rate changes. The lack of financial inclusion and infrastructure is another issue.

Finding a bank that operates with the desired country's currency would result in using many intermediary banks that increase the transaction's cost. Additionally, as some countries do not have the financial infrastructure, some people do not have bank accounts. Without a bank account, it is hard for money to exchange hands without physically handing the money to the desired recipient.

By using blockchain solutions, it does not matter whether or not the country has a bank connected to the rest of the world. It simply relies on the Internet and the conversion between cryptocurrency to the fiat currency of that country. Furthermore, some blockchain companies have taken an interest in the lack of infrastructure in underbanked populations and are finding ways for money to be exchanged and used within the country of that region. The cost of compliance is increasing due to the varying regulatory environments.

Compliance refers to the operational efficiency and reliability of the money being moved safely to the recipient. With the current SWIFT system, it is hard for the sender to track the transaction as it passes through many third-party financial institutions before it reaches the desired recipient. The transparency provided by the blockchain gives the sender the ability to track the transaction's path.

The interoperability between countries becomes another delay aspect when attempting to complete the transaction. Different countries require different amounts of information for transactions to be processed.

5.3.1. SureRemit

SureRemit [105] is a blockchain platform started by the makers of Suregifts. SureRemit provides cashless remittance services for cross-border businesses. The Remit token (RMT) can be used within the platform to pay bills and access vouchers. Customers can select the country to which they want the money to be sent, look for the category, and thus create a voucher that can be sent via text and email. These vouchers freeze the tokens. When the voucher is used, the merchant gets paid in their fiat currency or RMT [105].

The Remit Token is not subject to the volatility of exchange rates; therefore, what the sender sends is what the receiver will receive [106]. By utilizing vouchers sent over SMS and email, SureRemit breaks through the barriers created due to a lack of financial infrastructure. A customer does not need a bank account in the country of origin to pay and send vouchers. However, one drawback to using RMT vouchers when paying the merchant is that it is required for the merchant to be partnered with SureRemit. This creates an issue in places where merchants are not willing to partner with SureRemit. SureRemit leverages the Stellar platform and also partners with merchants to allow transactions to bypass different regulatory environments, as the RMT tokens can be converted into fiat currency via the Stellar platform. Furthermore, by using the SureRemit blockchain, the sender is cutting out banking intermediaries.

The minimal fees charged by SureRemit are very small compared to SWIFT fees for cross-border money transfers. Additionally, the transaction time is much faster, as Stellar transactions, on average, take 5 seconds to process without the need to interact with several intermediaries. Thus the risk associated with changing conversion rates does not pose a threat.

5.3.2. Everex

Everex aims to achieve financial inclusion of the underbanked [107] as it enables wallet-to-wallet interactions through its cryptocurrency "Cryptocash." Cryptocash is an Ethereum-based token. Each unit of Cryptocash is backed by the fiat currency it represents. Cryptocash balances are underwritten by third-party cash custodians that allow users to convert their fiat currency into Cryptocash. They then can exchange and transfer the Cryptocash via blockchain. This allows Everex to obtain its goal of financial inclusion and avoid the volatility of current, non-stablecoin cryptocurrencies. Since the Everex token is a "fiat"-pegged stablecoin, the money being transferred is equivalent to the same fiat currency that is being transferred—without needing to be converted multiple times into various currencies. This poses a risk because the conversion from eFiat (Cryptocash) to fiat is subject to conversion rates and can be volatile. Furthermore, for transactions to occur, Everex needs international trusted banking partners to provide a 1:1 conversion rate. This can limit geographical inclusion as it depends on the existing financial infrastructure. If a banking partner does not exist in a region, the eFiat money cannot be redeemed and converted into fiat money.

Summary: This section discusses how blockchains allow Stellar and Ripple to make payments promptly and cost-effectively. We highlighted that RippleNet and the Stellar Network differ in their use cases. The Ripple network was built to provide liquidity solutions to larger institutions, while Stellar's goal is to provide payment solutions on a smaller scale and facilitate global financial inclusion. The distributed ledger technology enables transparency of transactions and guarantees immutability, leaving a permanent record of transactions that have taken place. This opens up banking services to unbanked populations in certain countries. The Pundi-X and Algorand blockchain implementations leverage the blockchain architecture to have a point-of-sale system for underbanked and under-serviced populations, allowing sales for both merchant and consumer to be more accessible and less costly. The most common problems with remittance are the cost and time it takes for international transactions to complete. SureRemit and Everex solve these problems by utilizing the blockchain architecture and enabling nontraditional ways of sending money. They each approach the issue differently. However, both use the architecture to lower costs due to fees, reduce the time of the transaction, as well as to work around regulatory environments, and serve underbanked populations, which tend to be the main targets of remittance.

Tables 9 and 10 compare and summarize the solutions provided by SureRemit and Everex

Table 9. Remittance/International Money Transfer.

Issues Faced by Financial Institutions	Solutions Provided by SureRemit	Solutions Provided by Everex	SureRemit Blockchain Implementation Issues	Everex Blockchain Implementation Issues
Lack of Financial Inclusion	SureRemit does not need a bank account on the receiving side to use the voucher that is sent—the receiver simply needs a mobile phone to be able to use the voucher.	Everex partners with banks targeting underbanked populations and allows workers to send money home without paying high remittance fees.	Merchants must be partnered with SureRemit and accept tokens.	Everex needs to have licensed exchange partners in the country of receipt to exchange tokens into local currency.
Cost of Compliance Among Different Regulatory Environments	SureRemit leverages the Stellar platform and also acquires partner merchants to bypass different regulatory environments altogether by settling Remit tokens with fiat currency via Stellar.	-	The Token can only be used to make purchases with partner merchants. Therefore, the money cannot be used if a partner merchant does not accept the Remit token.	-
Interoperability	SureRemit has standardized the process regardless of country. The same information is required no matter where or with whom the transaction is placed.	Everex has trusted banking partners in the countries they interact with, thus promising a 1:1 conversion rate of their eFiat stablecoins.	-	For the stable coins to be redeemed in Fiat currency, Everex must have local banking partners that operate within that currency. Otherwise, the eFiat cannot be sent/redeemed.
Risk	RemitToken is not subject to the volatility of currency exchange rates. Immediate and continuous liquidity provided by Stellar allows for the issuance and trading of tokens immediately. Therefore, they are not subject to the risk of exchange rates.	The Everex Token is a dollar-pegged stablecoin, ensuring that the money being transferred is equivalent to the same fiat currency that is being transferred.	The stablecoins used by Everex when redeemed from eFiat to fiat are subject to conversion rates that can be volatile.	-

Table 10. Remittance/International Money Transfer.

Issues Faced by Financial Institutions	Solutions Provided by SureRemit	Solutions Provided by Everex	SureRemit Blockchain Implementation Issues	Everex Blockchain Implementation Issues
Fraud and Transparency	The blockchain ledger is publicly verifiable and immutable. It will confirm whether the correct parties sent and received the money.	The blockchain ledger is publicly verifiable and immutable. It will confirm whether the correct parties sent and received the money.	Remit Tokens are sent via a "voucher" outlining what the tokens are to be used for. This restricts the voucher from being used with only specific merchants.	-

Transaction/Settlement Time Delays.	Stellar transactions take 5 seconds to process using the Remit Token instead of fiat currency. There are no intermediaries when sending Tokens around the world.	Ethereum transactions take upwards of 1min to settle using the eFiat token. Since there are no intermediaries, the account is credited based on the speed of the Ethereum blockchain.	-	The Ethereum blockchain has longer transaction times than other platforms, which could cause an issue considering conversion rates.
Transaction Fees	By cutting out banking intermediaries, transaction fees are also removed. There is a 0–2% fee when sending using SureRemit, which is significantly less than the standard 7–14%.	The transaction fees are removed due to the transfer of eFiat stable coins bypassing banking intermediaries. Wallet-to-Wallet interactions have no fees associated with them.	-	-

6. Deposits and Lending

Deposits and Lending is a segment of the FinTech industry that relies on companies enabling people to obtain loans and monitor and collect information about their credit. This section focuses primarily on the Lending aspect of this segment as it has the largest application within the blockchain [26] and provides an overview of Colendi, Figure, and Celsius Fintech companies.

Blockchain can speed up verification processes by simplifying and breaking down barriers to obtaining a loan and even allowing other people to lend money without the risk of not knowing who they are lending to. Businesses and consumers can use blockchain-aided platforms to initiate transactions and loans guaranteed through the ledger's transparency and immutability.

Furthermore, blockchain has yet to reach a stage where it can support large business loans. Therefore, blockchain companies specializing in loans and deposits target many small businesses and personal loans. Small business and personal loan companies that utilize blockchain have leveraged the architecture in several ways.

Colendi uses blockchain to perform credit assessments, Figure uses blockchain to provide credit-based loans, and Celsius uses blockchain to provide crypto-based loans. However, within this segment, the problems that are encountered are relatively the same—the solution by each company is what differs.

One of the main issues in the small business and personal loans sector is the high fixed costs. Traditional loan approval is a lengthy process that involves several credit checks, background checks, paperwork, and other processes that often require the use of third-party intermediaries. These third-party intermediaries accrue costs that often have to be paid for by the customer who is taking the loan.

The fees are high, and often personal loans can be a significant barrier because the customer may not be able to afford them. Furthermore, the transaction fees from obtaining the loan and the administration fees associated with the loaner of the money also drive up the overall price of the loan—making the person or customer borrowing responsible for paying back a lot more than the amount that they require in the loan.

Blockchain has the capability of solving these problems by providing a clear and direct translation of the money. Creditworthiness can be tracked by transactions on the blockchain, providing an immutable and transparent account of the person's financial history. It reduces a lot of the third-party verification needed to approve a loan, thus cutting costs down significantly.

Another main challenge is the lack of information to make a credit decision. The bank's process of obtaining information about a person or company's financial history

and security to approve or reject the loan is lengthy. Due to the time required to conduct the investigation, many loans take a long time to process.

The information, though through a third party, is not always accurate. Depending on the accuracy, this can pose a risk for both the lender and the borrower. Therefore, there needs to be a transparent way to carry out checks. Blockchain can not only keep a ledger that ensures that financial transactions and trustworthiness can be seen by multiple parties but can also allow this data to be accessed in real-time. Therefore, no large hunt is needed to investigate whether or not the person or company is qualified for the loan. The information lies within the immutable ledger that is fully accessible.

Another component that blockchain allows for is reliance on cryptocurrency as an investment. Now, cryptocurrency can be an asset that is used to back certain loans. One of the largest pain points of loans is the time taken to approve the loan once requested. This is due to the immense amount of third parties that need to either provide information for the approval process or look over the loan application themselves. When evaluating collaterals, many people have to become involved in assessing the worth of the collateral to ensure that it can indeed cover the cost of the loan.

Furthermore, humans are involved heavily in the process. Therefore, time delays occur due to humans' limited capacity when processing documents. Blockchain architecture enables the possibility of speeding up the process by the utilization of smart contracts and by verifying information via the immutable ledger. Smart contracts allow for agreements to be executed automatically and efficiently, thus reducing the time it takes from one approval action to another.

Furthermore, it reduces costs as legal and administrative fees can be cut. The immutable ledger allows documents and information to be shared via the ledger, thus eliminating the need for an investigation, as it can be inquired of the ledger. All the information is available and easily accessed by those processing the loans. When loans are backed by cryptocurrency, the currency exists on the blockchain. Thus, it is evident that the applicant has collateral funds, reducing any time needed to understand and investigate whether or not the collateral can support the loan.

6.1. Colendi

Colendi is a credit-scoring FinTech company that leverages new sources of information about borrowers to provide new avenues of creditworthiness [108].

Colendi leverages the Ethereum blockchain and machine learning-based scoring technologies to evaluate user data segments; that is, the process of collecting data related to the transactions, smartphones, social media data, and more than a thousand pieces of personal information to generate a metric called Colendi Score.

This allows underserved and underbanked populations to have the ability to assess the population with less traditional information. Banks create scores dependent on their customers' records, so the potential borrower is not evaluated based on their characteristics. The customers' private data shows much more information than the bank can access. Thus Colendi's goal is to utilize the transparent property of blockchain to create a high standard of evaluation transparency combined with their machine learning algorithms to allow for a comprehensive understanding of the borrower's full potential.

The blockchain component of the Colendi platform has three main functions: identity management, collecting/storing data, and generating a credit score that can lead to a lending decision based on the stored data.

Due to its significant nature, the data storage combines blockchain and decentralized storage, Storj. The Colendi SDK allows users to interact with Storj without knowing the underlying technology.

The computation of scores is not done on the blockchain itself but rather by the Engima protocol, where data can be split across nodes and used for computation. The score is then relayed back and stored on the blockchain.

Colendi is opening up the opportunity for underbanked populations to gain access to micro-financed loans. If a user does not have enough data to secure a loan, Colendi offers the option for a borrower to stake Colendi tokens.

Though these tokens cannot be used as collateral against a loan, they provide a positive number when it comes to scoring. Furthermore, the data drawn upon goes beyond just traditional assets and bank history by including mobile data, social media data, and external data partners. All information is then stored in decentralized storage and drawn into the Engima protocol to create a score [109].

All of these processes on the blockchain significantly reduce costs as everything takes place within the Colendi network and does not have to go through several intermediaries.

Furthermore, this reduces time delays as these activities are triggered via smart contracts and are all within the Colendi network. Thus, no time delay is associated with processing information by third-party companies verifying the data. Furthermore, this data is secured as only the Colendi network can access the decentralized storage system.

All that lenders garner is the final score the Colendi protocol produces. The blockchain provides an integral abstracting layer that ensures the protection and confidentiality of the borrowers' data and information.

6.2. Figure

Figure is a FinTech company leveraging blockchain technology to speed up the loan application process. Figure has its own blockchain platform called Provenance. Provenance is used to store data within the blockchain to ensure that the data is accessible and untampered with.

The data is digitally signed and validated using smart contracts. This inherently reduces the need for third-party companies to verify the data, saving time and cost throughout the loan process. The transactions are granted by the administrator and need to be approved by the stakeholders.

The administrator is a key player in the blockchain as they create and review smart contracts held by the node to process transactions. They are also in charge of determining the cost of the transaction and the amount of stake that each node needs to hold. When a loan originator selects an offer from a consumer's application for a loan, they generate a "smart contract" that enables them to provide the amount required in the loan.

Once the loan is funded, the originator can either retain or sell the servicing, meaning that the originator has sold the rights to service the loan (i.e., collect the monthly principal and interest payments). The loan payments are collected through a remittance agent.

The administrator creates smart contracts related to the transactions by taking encrypted data from the member and transforming that information into encrypted data in the blockchain [110].

Banks on the Omnibus network, called Omnibus banks, are responsible for facilitating fiat settlement on the blockchain.

When fiat is used, the members check to ensure that the Omnibus bank account has enough money. The bank then generates a settlement token backed by the member's account. Then, the token is passed to the receiving member. This transaction is immutable and present on the blockchain such that it can be referenced later if needed. By performing all of the transactions on the blockchain, Figure cuts out all other intermediary fees, leaving only the origination fee as the primary fee on the blockchain. However, one caveat to using Figure for loans is that they default to traditional methods to determine creditworthiness, primarily a high credit score [111]. This does not open up Figure to those with no banking infrastructure or to those who do not have a good credit history.

However, since the data is stored on the ledger, the approval time for the application is much faster as the records within the ledger are trusted. Furthermore, smart contracts enable many functions within the entire loan process to be automated and reduce any overhead of maintenance by a person.

6.3. Celsius

Celsius is a FinTech lending platform that leverages blockchain technology to allow people to use cryptocurrencies as collateral for fiat loans. Many people are investing their money into digital assets due to cryptocurrency hype.

They hold onto their digital assets as they invest in cryptocurrency with a long-term mindset. Simply put, they are investing now for significant payoffs in the future.

However, although some businesses and companies allow the use of cryptocurrencies in transactions, crypto assets still do not have a lot of "real value." The only way to obtain value from them is to sell them—in which case, with such volatile prices, an investor does not know if the sale will be for profit or for a loss.

This is extremely important, as when people need cash instantly, they cannot always wait for the market to regulate such that their coins are valued higher. This often leads people to have to leverage real-world assets to obtain a loan from the bank.

Celsius now offers a platform where people can leverage their cryptocurrency as collateral to secure a loan in fiat currency. Rather than selling the cryptocurrency, members can leverage it while still holding onto that crypto portfolio to obtain future value [112]. They even take it one step further and allow members to accrue interest on their crypto assets, similar to how money in a bank accrues interest. When asset holders deposit coins on the Celsius Network, they can earn interest on their coin balances.

Celsius token (CEL) is the heart of the blockchain implementation of Celsius. These CEL tokens are Ethereum ERC-20 coins issued on the Ethereum network. Celsius uses these tokens so that the lending and borrowing model is transparent.

The Ethereum platform is leveraged by Celsius such that it can utilize the idea of smart contracts, leverage quick transaction times, and leave a traceable footprint that allows for trade transparency on coin exchanges.

Lenders in the Celsius network can be anyone who deposits crypto assets into the Celsius wallet. These assets are stored in a "Lending Stake Pool" Celsius account. These accounts then transfer the coins to coin exchanges. The lender's wallet then accrues interest in the form of Celsius tokens.

Lenders also can leverage their crypto assets in exchange for a fiat-based loan. In this instance, the user requests a loan and, in exchange, transfers crypto assets, which are locked. These crypto assets cannot be withdrawn until the loan is paid. The user then receives the fiat loan via a debit card or a direct bank transfer to a Celsius bank account. The payment plan and instructions are also issued at this time. Then, the user pays the loan installments like any other traditional loan. Once a loan is paid, the crypto assets are unlocked, and users may withdraw them as they please. However, if the user fails to pay, Celsius has the authority to sell the crypto assets in exchanges to recover the fiat value and reduce the loan amount. To borrow coins, a borrower deposits a fiat value into a custodian trader account owned by Celsius. To short the crypto asset, the borrower places a limit sell order. This sell order acts as a request that includes conditions of the trade (time and price) and a fee to access the assets.

While the borrower is requesting, the Celsius service checks to ensure the funds that are being requested are available based on the assets from lenders.

If the trade is approved by Celsius, then Celsius issues a sell order of the crypto asset on the exchanges to hold a short position on behalf of the borrower.

Once the crypto assets are sold, Celsius orders exchanges to purchase the crypto assets back. When the Celsius platform and the borrower make a profit off a short, the Celsius master account receives a percentage of that profit in addition to the fees accrued from holding the short position. The money received by the master account from the borrowers is in fiat. Still, the Celsius platform converts this fiat value into CEL tokens and then distributes it back to the lenders' wallets as a form of daily interest. The amount that is distributed back is contingent on a Proof of Stake consensus.

In other words, the more crypto assets the lender puts into the Celsius Network, the more interest in the form of CEL tokens they accrue.

Lenders then can buy and sell these CEL tokens on exchanges however they wish. Additionally, lenders can pay off their Celsius loans via CEL tokens.

By using the CEL token, not only is Celsius offering a very transparent and efficient method of making exchanges, but it also provides an excellent incentive for people to lend out their crypto assets and use them as collateral for fiat currency while still holding onto them such that they can realize their long-term investments.

The Celsius network leveraging blockchain eliminates any third-party cost as the loans are lent and borrowed within the Celsius platform, effectively making it a P2P loan.

This cuts out any loan application or approval process that requires anybody other than the borrower or lender, making the entire process faster.

It also significantly reduces transaction and administrative costs. The loan is also not based on credit, but it is contingent upon the amount of stake (i.e., the amount of crypto coin) held and put up as collateral.

However, these crypto assets, when used as collateral, are also subject to volatility. Therefore, if the crypto asset loses its value, the Celsius network will require more assets to be put up as collateral.

Furthermore, the transactions all take place on Ethereum, and the ability to use smart contracts enables all internal functions, such as checking the availability of funding or efficiently performing the transactions, significantly reducing the overhead that comes with administrative work for traditional loans.

Summary: Lending processes can be significantly more efficient when using blockchain, especially when the network leverages smart contracts to perform much of the functionality. The immutable ledger provides an accurate record that can later be referenced (or, in some cases, used) to ensure the validity and honesty of an entity and even be a marker of how responsible they are. All three companies, Colendi, Figure, and Celsius, utilize blockchain differently within the loan process. However, they address the pain points they all face and have leveraged the architecture to benefit their users.

Tables 11 and 12 compare and summarize the solutions provided by Colendi, Figure, and Celsius.

Table 11. Deposit and Lending Chart.

Categories	Credit Assessment		Credit-Based Loan		Crypto-Based Loan	
Problems Faced by Individuals and Small Businesses	**Colendi Solutions**	**Problems Facing Colendi**	**Figure Solutions**	**Problems Facing Figure**	**Celsius Solutions**	**Problems Facing Celsius**
High Fixed Costs (Administration Fees and Transaction Fees)	It uses blockchain to track and keep records of people's trustworthiness. There are fewer third parties to go through, so costs are reduced.	-	Figure only has an origination fee as all the other intermediary fees are cut out due to the loans being sold and obtained via the Provenance blockchain.	-	Celsius does not charge any fees, and the loans are lent and borrowed within the Celsius platform, making it a P2P loan.	Centralized network as the wallet is held and managed within Celsius's platform.
Lack of Information to Make Credit Decisions	It uses a decentralized scoring system that consists of the smartphone, social media data, and transaction logs showing repayment performance.	Due to the goal of serving the underbanked population, more people may get loans that they cannot pay off—which could hurt financial institutions.	-	A high credit score is needed. This is the only aspect Figure checks.	The loan is not based on credit but on the amount of crypto coins put up as collateral.	-

Table 12. Deposit and Lending Chart.

Categories	Credit Assessment		Credit-Based Loan		Crypto-Based Loan	
Problems Faced by Individuals and Small Businesses	**Colendi Solutions**	**Problems Facing Colendi**	**Figure Solutions**	**Problems Facing Figure**	**Celsius Solutions**	**Problems Facing Celsius**
Lack of Collateral	Allows borrowers without much collateral to stake Colendi tokens contributing to a positive score.	-	-	-	Celsius allows crypto assets to be used as collateral when trying to obtain a fiat loan.	Due to crypto asset volatility, Celsius requests more crypto assets as collateral for loans if the assets' value drops below a certain threshold.
Poor or Insufficient Credit	In underbanked populations, other data is drawn upon (see text) to determine creditworthiness.	-	-	Figure still does a soft credit pull and requires a decent line of credit to obtain a loan.	The loan is not based on credit but on the amount of crypto coins put up as collateral.	-
Time of Application Process to Approval/Rejection.	Colendi Token enables efficient and automatic fulfillment of agreements that reduce cost and time delays.	-	The immutable ledger allows administrators to trust the records held within the ledger, saving time during the process. The hash token enables smart contracts to automate many functions during the loan process.	-	Celsius uses a simple check via smart contracts on Ethereum, which is time-efficient	-

7. The Investment Sector

The investment sector uses a different approach when implementing blockchain-based solutions. Although blockchain can solve problems due to the traditional operating procedures of investing, the current focus is on investing in blockchain rather than using blockchain. Institutional and retail investors are investing in digital assets to obtain long-term profits.

Bitcoin and Ether are two of many digital assets on blockchain frameworks. Although Bitcoin and Ethereum entered a bear market as of the second quarter of 2022, there is still momentum for a long-term investment.

Investors are treating digital assets as an entity that holds value, not only as a technology that simplifies the ease of transaction as the other sectors do.

This section overviews five FinTech companies in the FinTech investment sector, Grayscale, Fidelity Digital Assets, Robinhood, Webull, and IBKR, and discusses the three main segments of this sector [26]: institutional investment, venture capital, and retail investing.

7.1. Institutional Investment

Before developments in regulatory requirements surrounding Bitcoin, trading and investing in digital assets by institutional investors were not as important as the other stocks and securities being traded.

This is due to the opaque rules and regulations. However, as Bitcoin became widespread, the use of digital assets in payments rose. Governments worldwide began to formulate rules and regulations around Bitcoin, making it fill a once gray area.

Bitcoin and digital assets appeared to hold their power for years, inspiring the buy-in of institutional investors due to their ability to hedge against inflation, economic depression, and the aging population. In other words, as fiat money was losing its value, Bitcoin could hold its value and be a safe investment for the period before 2020.

However, this anti-inflation concept was proven incorrect as of 2022. Countries such as Canada and Europe have Exchange-Traded Products (ETPs) that allow institutional investors to place money on stock exchanges backed by crypto assets. ETPs are an excellent way for investors to get involved with crypto without the need to handle the actual management of the assets themselves.

According to Fiona, many different institutional investors entered the market to capitalize on crypto opportunities. This was started by giant investment management firms noticing a growing interest in crypto. Many companies including Binance [113], FTX [114], Coinbase [115], and Grayscale Investments [67] emerged in the institutional investment sector. Merrill Lynch [116], Goldman Sachs [117], and Fidelity Digital Assets also joined [118]. This subsection provides an overview of Grayscale and Fidelity Digital Assets.

7.1.1. Grayscale Investments

Grayscale [67] is a digital currency asset manager offering various investment products. These investment products retain the value of their shares that reflect the actual performance of the digital assets that compose the product.

These products can either be single asset products or diversified asset products. In this scenario, Grayscale is not using blockchain to carry out the investment procedures. Still, it is using the cryptocurrency's value store to realize a profit for its investors. These products enable investors to gain exposure to digital currency asset classes without worrying about buying, storing, or safekeeping digital currencies.

The products are held in cold, offline storage with the Coinbase Custody Trust Company, which ensures the security of the assets. Furthermore, investors save money by investing in products rather than holding the assets by eliminating the expensive and time-consuming processes required to trade, acquire, secure, and keep the assets.

Grayscale enables the investor to bypass having to deal with different intermediaries when doing the trading as they handle those tasks themselves. Once again, it is worth noting that Grayscale is holding crypto assets to realize their value on the stock market rather than for the properties of the crypto assets due to being built on a blockchain. The assets are held in a cold storage wallet and not on any blockchain.

7.1.2. Fidelity Digital Assets

Fidelity Digital Assets [118] focuses on custody solutions for institutional investors who want to bypass the hassle of securing these assets. Therefore, the company found its market in offering trading and custody services that enable its investors to realize the true potential of their blockchain holdings without doing the trading themselves.

The assets are stored in cold storage. Thus, they are physically separated from the internet, making them highly secure. Furthermore, the trade execution services will leverage the same internal crossing engine, that is, when buy and sell orders are paired internally from two separate customers of the same stock at the same price. Like Grayscale, Fidelity Digital Assets does not harness the utility of blockchain as an entity but emphasizes the value of cryptocurrency to make a profit.

7.2. Venture Capital

Venture capitalists are utilizing crypto assets (i.e., cryptocurrencies, utility coins, and security tokens) to diversify their portfolios and create crypto-based funds that are used in investing in blockchain start-ups, initial coin offerings (ICO), and crypto assets. Venture capitalists funded start-up blockchain companies by issuing a certain number of tokens to be sold to the venture capital (VC) that has invested in them [119].

This type of investment is captivating because it gives VCs an early jump on stake within the company and because cryptocurrencies are liquid and can be seen as a tool to counter the effects of inflation. Crypto asset management products and services are becoming more accessible to the public. When investing in a typical company, VCs put in fiat money to obtain a long-term profit.

With cryptocurrencies, the profits need only be transferred into Bitcoin or Ether. Then, online services can convert that into fiat currency. Therefore, investors can realize gains and obtain them more easily using ICOs.

There are now several cryptocurrency venture capital firms, such as SPiCE [120], Pantera [121], and Blockchain Capital [122]. Each firm has a unique way of building portfolios and offering its investors various incentives, emphasizing that crypto assets are liquid assets that allow investors to realize their money sooner.

7.3. Retail Investing

Retail investing can be done by an individual who buys and sells securities, equity shares, commodity contracts, mutual funds, or exchange-traded funds (ETFs) through brokerage firms or retirement accounts (e.g., 401k accounts) or can be an institutional investor who invests the money of others on their behalf. Crypto markets entered a new era in 2017 due to the adoption of cryptocurrencies by retail investors [123].

However, they pulled out of markets after making profits and witnessing the volatility of Bitcoin—hoping to avoid losing the investment that they had made due to the high volatility. Because of the many exchanges now handling crypto trading, increased regulation, and price stabilization due to institutional investors providing liquidity to the market, retail investors have once again entered the crypto market.

There is speculation over whether or not this will be similar to 2017, where assets are held for the short term, or whether it will be similar to institutional investors making a long-term investment into crypto assets.

Brokerage platforms have been set up specifically for the crypto space to ease the transition of new investors into the market. Schwab [124], ETrade [125], Robinhood [126], Webull [127], Interactive Brokers (IBKR) [128], and Merrill Edge [129] are popular brokerage platforms. This section discusses Robinhood, Webull, and IBKR, which are used to exchange crypto.

7.3.1. Robinhood

Robinhood [126] has recently surged to become one of the most popular brokerage platforms in the United States, allowing trading stocks and ETFs in the crypto space. It has no fees associated with asset trading.

The main difference between putting fiat money into Crypto stocks instead of purchasing Crypto directly (say through a company such as CoinBase) is that the cryptocurrency bought in Robinhood cannot be taken out or converted into something else. Instead, to realize the value of the money, the crypto assets need to be converted back into fiat money. It is great for newcomers who are not entirely sure what cryptocurrency is to invest their money in a simple-to-use app that allows them to participate in cryptocurrency's rise and fall. It is not for large traders who want to make large volume trades or to expand their trading portfolio.

7.3.2. Webull

Webull's [127] marketing strategy depends upon providing research on and analysis of the market. Webull is a subsidiary of Fumi Technology, a multinational Chinese company.

Therefore, though it has similar trading capabilities as Robinhood—it seems better suited for more sophisticated investors as it has more in-depth analysis and metrics than Robinhood. Like Robinhood, once fiat money is converted into crypto assets, the only way to realize that value is to convert it back into fiat money. Webull's platform is for trading and exchanges, not for storing crypto assets.

7.3.3. Interactive Brokers

Interactive Brokers (IBKR) [128] is an American multinational brokerage firm. IBKR provides broad global market access. In September of 2021, IBKR added cryptocurrency trading to its offerings by allowing users to directly trade cryptocurrencies, including Bitcoin, Ethereum, Litecoin, Bitcoin Cash, and cryptocurrency exchange-traded funds (ETF).

Most retail investing companies are inevitably shifting towards utilizing blockchain technologies in their financial services.

Summary: For institutional and retail investing, crypto assets are held for their marginal value on the stock market. The assets are not used for their blockchain capabilities but for their value as a good investment. Crypto assets are used to hedge bets against inflation, diversify portfolios, and provide an easy way for those interested in crypto to become somewhat involved.

7.4. Non-Fungible Token

Non-fungible tokens (NFTs) are digital assets stored on a blockchain. They are typically correlated to the ownership of digital content (i.e., digital arts) such as photos, audio, videos, and in-game assets. Such ownership can be transferred through blockchain transactions, which means that NFTs can be sold and traded like cryptocurrencies. However, unlike cryptocurrencies, NFTs are uniquely identifiable (i.e., non-fungible). For example, a Bitcoin is identical (fungible) to another Bitcoin, but an NFT differs from another NFT.

NFT is believed to be a realistic solution for ownership proof for digital assets, even though its legitimation is still uncertain [130]. NFT ownership is not equivalent to legal rights such as copyright and intellectual property. One can still share or copy a digital file freely that is associated with an NFT. It is currently just a decentralized proof commonly recognized in the blockchain community and is granted value by trading with cryptocurrencies. OpenSea [131] is currently the largest marketplace for NFTs, where one can create, trade, and bid for NFTs via different kinds of cryptocurrencies.

The first NFT project, Etheria [132] (built on Ethereum), was launched in 2015. It consists of a total number of 33 × 33 tiles (a digital map based on tiles), among which 457 tiles are land and can be bought for ownership. While each tile was initially hardcoded to 1 ETH, some were bid to about 70 ETH when NFT started rapidly growing in 2020 [133].

The trading market of NFTs was more than $17 billion in 2021, about 210 times as much as in 2020, which was $82 million [134]. Recently, placing in-game items (e.g., avatars, virtual costumes, and properties) as NFTs on blockchain became a new trend and derived a set of Fintech applications called GameFi (i.e., game and decentralized finance) [135]. Online game players can earn in-game rewards (e.g., digital points, game items, and NFTs) by completing tasks in-game or competing with other players. Traditionally, in-game items have been traded via the digital points created by gaming companies, which are charged via fiat money. Items are centralized and owned by gaming companies. Even though there are third parties to trade in-game items in the real world, the commission fees and verification processes cost money and time.

Producing them as NFTs on blockchains makes them decentralized and owned by the players. They can be traded or sold through blockchains by their owners. Such use cases can also be seen in the metaverse, an emerging virtual reality technology trend named by Meta [136]. It creates a virtual world that combines physical and virtual societies, in which users create digital forms of art and property. NFTs can enable the ownership of such digital assets. The top GameFi projects based on their market capitalization can be found in [137]. NFTs are an important aspect of Web3.0, a popular idea for decentralization being discussed in the blockchain community. Web3.0 is envisioned as the new iteration of the World Wide Web (WWW), with Web1.0 characterized by static web pages (e.g., official websites) and Web2.0 featured by web-based platforms centering on user-created content (e.g., social media). Web3.0 incorporates decentralization and cryptocurrency, envisioning a decentralized internet with high-level data integrity (immutable data source) and user privacy (pseudonymity).

Like most blockchain-based infrastructure solutions, it emphasizes peer-to-peer user networks and tends to eliminate the need for trusted intermediaries. Some believe that Web3.0 is more secure, scalable, and pseudonymous, but some still are concerned about the harmful content that may inundate a decentralized web without censorship. Furthermore, pseudo-decentralization could mean a centralization or dictatorship of wealth and resources to a small group of rich and powerful people [138]. NFTs can be seen as a solution for digital asset ownership and a use case of Web3.0. They can be used to identify and claim ownership of all the digital data on the Internet, paving the way toward an ultimate decentralized data storage.

Note that NFTs only store the unique identification and the ownership of a digital asset on a blockchain, not the whole digital file. Whether Web3.0 will become a reality is yet to be known. Technical problems still need to be solved, such as the performance bottleneck of blockchain technologies, the blockchain storage explosion, and the lack of authoritative regulation. However, a new perspective for a peek into the future is always noteworthy and intriguing.

8. Results and Discussion

This section presents the challenges, results, and discussion for Fintech from the perspective of blockchain-based DeFi. We start with the challenges, conclude and compare each covered topic and implementation, and then give a general analysis and discussion on DeFi.

8.1. Challenges

Implementing blockchain technology for the financial sector brings many changes to business models, financial services, and operating processes. This section provides an overview of privacy and security issues, energy efficiency and sustainability issues, market volatility, and regulations issues.

Although blockchain and cryptocurrencies are widely discussed, they are much less understood. The lack of expertise and reputational risk are two of the many challenges facing banks when incorporating blockchain into their financial services.

Utilizing blockchain for FinTech poses security risks. The decentralized nature of blockchain necessarily allows any actor to write unaudited and even malicious smart contracts [138], where user funds can be lost through programming errors or stolen.

Most FinTech applications utilize permissioned blockchains that are subject to periodical audit by the governments to detect/prevent illegal activities (i.e., money laundering, blackmailing, and ransomware). Therefore, some governments require cryptocurrency exchanges and investing platforms to collect customers' personal information, i.e., know your customer (KYC) procedures [139], and comply with regulatory requirements.

This poses a lengthy process of ID card verification, face/biometric verification, and document verification (i.e., utility bills) as proof of address. Moreover, FinTech companies must ensure that their permissioned blockchain network has sufficient redundancy to

prevent network fragmentation. With transparency being one of the primary purposes of blockchains, privacy is a critical concern. Implementing blockchain for the FinTech sector is subject to data protection regulations, such as the General Data Protection Regulation (GDPR) [139], the Personal Information Protection and Electronic Documents Act (PIPEDA) [140], and the California Consumer Privacy Act (CCPA) [141].

These data protection laws and regulations hinder the adoption of blockchain for FinTech. For example, the immutability of recorded transactions violates GDPR's "right to be forgotten," where users have a personal right to withdraw and delete transactions and personal information. This includes any encrypted data [139].

Utilizing off-chain storage of personal data is a feature that could be useful for data privacy compliance. Data can be stored and maintained off the blockchain with only a hash of the personal data recorded on the ledger. However, this approach reduces the transparency benefit of blockchain.

Blockchain technology has inherent security properties by design. It is based on principles of cryptography, decentralization, and distributed ledger. Yet the implementation of blockchain still faces security issues.

As of today, most blockchains employ public-key cryptography for identification. Ideally, the private key should be only known to the user. However, many cryptocurrency exchanges store the users' private keys in online "hot wallets." There have been cases where hackers have stolen users' private keys in online wallets. As a result, lots of funds and digital assets were stolen. We have seen an attack on AscendEX hot wallet where the AscendEX crypto exchange lost $77.7 million [142].

The authors in [85] categorized the security risks and challenges mainly in smart contract vulnerabilities, infrastructural risk, and interdependence weaknesses. DApp developers must be wary when designing applications and choosing the infrastructure to which they deploy their applications. Choosing the infrastructure directly affects the peer-to-peer network throughput, which may lead to network congestion and cause honest transaction timeouts [85]. Implementing a new protocol on top of an old protocol may lead to complexities and interdependence weaknesses since the security of the new protocol is as good as the security of the old protocol.

Smart contracts still prove their value for FinTech applications by making financial processes and transactions cost- and time-efficient. However, implementing smart contracts for FinTech applications requires a precaution to eliminate the presence of vulnerabilities and avoid the misuse of intelligent contracts.

This includes conducting security code scanning and testing. Ethereum's Decentralized Autonomous Organization (DAO) attack is an example of a misconstructed smart contract. DAO suffered from vulnerabilities in its code base that allowed an attacker to retrieve approximately 3.6 million Ether from the DAO fund [143]. As of the second quarter of 2022, the market has entered a crypto winter [144].

The prices of all cryptocurrencies have entered the bear market and have been affected by a general market downturn. FinTech companies have shifted their focus to building for the long-term as the average bear market typically bottoms out around the 12-month mark and may fully rebound in two years.

Permissionless blockchains' energy efficiency and sustainability is a challenging problem that has a significant environmental effect and could prevent the widespread adoption of this technology. However, PoS and PoT were proposed as alternative solutions to the PoW consensus algorithm. Recent research works focus on PoW-based solutions. The authors in [145] propose an offline optimization solution to reduce energy consumption. Others have proposed Green-PoW [146] by utilizing the energy spent during block mining to elect a small number of miners that will exclusively mine the next block.

8.2. Comparative Results on the Reviewed Topics

Based on the review and investigation of the Fintech literature, we examined blockchain-based DeFi by establishing a SWOT analysis to identify the strengths, weaknesses, opportunities, and threats in this field.

This article reviews and categorizes DeFi applications into three sectors: (1) Payments, (2) Deposits and Lending, and (3) Investment Management. We give comprehensive overviews for each segment of service types and application examples. The payment sector facilitates user payment activities such as retail, point of sale, and money transfer in a decentralized manner. Deposits and lending enable loans and user credit management with fewer intermediary procedures. Investment management introduces cryptocurrency exchanges and their derivatives (e.g., NFT). Table 13 compares the three sectors to provide an overview of the reviewed topics.

Table 13. Overall comparison of the three sectors.

Sectors	Advantages	Disadvantages	Example Technologies
Payments	1. Avoid a significant amount of transaction fees, such as credit card fees. 2. Less or no intermediaries and thus less delay. 3. Less risk and fraud due to less or no intermediaries. 4. Transparent transactions. 5. Lower transaction error rate. 6. Easy to localize the fraudulent transactions. 7. Useful for undeveloped regions that lack financial infrastructure.	1. Lower transaction rates (transactions per second) compared to CeFi clouds. 2. User-unfriendly: current blockchain-based financial payments are intricate to most users. 3. Private key storage: user tends to lose their private keys if storing them offline, but online wallets are risky. 4. Hard to scale. 5. Potential high gas fee per transaction.	Retail and Consumer Payments: RippleNet, Stellar Network. Point of Sale Payments: Algorand Blockchain, Pundi-X. Money Transfer: SureRemit, Everex.
Deposits and Lending	1. Less intermediary fees due to fewer intermediary processes. 2. Less delay due to fewer audit procedures (audit can be reused). 3. Pseudonymous deposits and lending preserve privacy. 4. Transparent deposits and lending history. 5. An accurate record of lenders. 6. Undeniable loan and collateral (immutable ledger). 7. Easy to localize lending and collateral scams. 8. Fluidify cryptocurrency.	1. Hard to determine collateral and loan value due to unstable cryptocurrency prices. 2. User-unfriendly. 3. Private key storage problem. 4. High collateral requirements due to lack of trust in borrowers. 5. Hard to scale. 6. Fewer audits and censorships lead to higher risk for lenders.	Colendi, Figure, Celsius.
Investment Management	1. Pseudonymous investment. 2. Manifest values of digital assets such as cryptocurrency. 3. Flourish blockchain development. 4. More and more companies and organizations are accepting cryptocurrencies. 5. Easy to localize transaction scams. 6. A new financial product that reflects the market and economy. 7. NFTs to correlate to ownership of digital content.	1. Unstable cryptocurrency prices. 2. User-unfriendly. 3. Potential fraudulent transactions even if it is easy to localize. 4. Hard to undo the damage (when some crypto assets are lost, they are hard to recover). 5. Private key storage problem. 6. ICO and crypto scams due to too much hype.	Binance, FTX, Coinbase, Grayscale Investments, Merrill Lynch, Goldman Sachs, Fidelity Digital Assets.

8.3. General Analysis and Discussion on DeFi

The concepts of DeFi bring us the excitement of a fair, secure, and democratic finance solution with self-controlled assets and pseudonymous transactions. The invention of blockchain technology makes it realistic and tangible. While blockchain technology is undoubtedly the first option to implement DeFi at present, weaknesses and threats exist in both the technology and DeFi itself. For example, technically, blockchain transactions are slow compared to CeFi transactions (not considering the intermediary processes of CeFi). Even though Ethereum 2.0 promises 100,000 transactions per second [147], it is still not comparable to the million-grade requests per second of CeFi clouds.

Moreover, blockchains can help realize immutable and transparent data and transactions. However, the immutability of transactions is a double-edged sword. If a historical transaction or data turns out to be a mistake in the future, there is no direct way to correct it. Nonetheless, there are approaches to "update" transactions by appending new blocks with transactions that correct mistakes [148]. Still, it wastes storage space, and we know that data size is a critical problem of blockchain with the continuously increasing data chain, c.f., blockchain storage explosion [149].

Centralization is notorious, but it has its advantages, such as auditability, good censorship, and lower collateral requirements for lending because of the mutual trust between the centralized party and a regular customer. Trust in the centralized entities such as banks and governments has been successfully (to some extent) established in current society. People have been used to the dominating system of such centralization. On the other hand, financial solutions and regulations are slow to respond. Usually, they will only be updated after the damage has been done (e.g., huge scams or frauds), so DeFi may not be able to be widely adopted if CeFi is well-operative. Nonetheless, DeFi, which is more powerful and beneficial to users, has become an important alternative to CeFi.

Besides all the benefits we mentioned for DeFi, decentralization has general strengths and opportunities. For example, with decentralization, standardization can be automatically done in a decentralized fashion. For example, what the majority follows and agrees will automatically become the standard, which more new and young users will follow.

Such mechanisms are mainly used for consensus but can be extended to a blockchain-based standardization or regulation solution that supplements DeFi. Moreover, with decentralization, financial globalization can be better established over borderless financial activities, which can be achieved without a centralized organization such as SWTIF [150]. A cross-border transaction will no longer need to go through multiple entities before it goes to the receiver's account.

Finally, based on the above review and discussion, we implemented a SWOT analysis and concluded the outcomes in Table 14 (in terms of strength, opportunities, weakness, and threats). Such situational assessment helps to evaluate the strategic position of DeFi in the market and the research cycle, both internally (e.g., financial perspective) and externally (e.g., environment perspective).

Table 14. SWOT analysis on DeFi.

	Positive	**Negative**
Internal (Attributes of DeFi)	**Strengths**. 1. Immutability and transparency of data and transactions. 2. No central parties dominate the services. 3. Benefits of CeFi can also be applied to DeFi, e.g., accessible and inclusive online services. 4. Custody of self-assets. 5. Smart contracts execute strict agreements automatically.	**Weakness**. 1. Slow-responding financial solutions: usually only updated after damage (e.g., huge scams or frauds), so DeFi may not be widely adopted if CeFi is well-operative. 2. DeFi solutions are pseudonymous (not anonymous). 3. High collateral requirements, e.g., lending in DeFi.

	6. User-privacy preserving, e.g., applying decentralized identity to DeFi.	4. Key protection issue: user needs to secure their private key, but wallet providers are somewhat centralized.
External (Attributes of the environment, e.g., blockchains, regulations)	**Opportunities**. 1. Automatic standardization: standardization can be automatically done in a decentralized fashion (e.g., what the majority follows becomes the standard). 2. Globalization: borderless financial activities can be achieved without a centralized organization such as SWIFT. 3. Fast transactions in terms of fewer intermediary processes such as audition and verification. 4. Rich technical recourses, e.g., many open-source blockchain frameworks. 5. Pseudonymous to genuinely anonymous.	**Threats**. 1. Technical challenges in blockchains, for example, slow transactions and controversial consensus. 2. Expensive implementations and development of decentralized platforms. 3. Rigid and slow-responding financial regulations. 4. Immaturity, e.g., large-scale DeFi platforms, may suffer serious glitches. 5. Gas fee in blockchain transactions, even though there are fewer commission fees, blockchain processes usually require a gas fee per transaction.

9. Conclusions and Future Work

This survey provides a comprehensive overview of the three main segments of the FinTech sector: the payments segment, the deposits and lending segment, and the investment management segment.

To help and benefit future researchers, practitioners, and DApp developers to understand blockchain benefits and applications for FinTech, we provide a summary and a related discussion on the most popular blockchain applications and use cases for FinTech. In particular, we first laid out the foundation and architecture of blockchains, smart contracts, digital wallets, and consensus algorithms. Then, we introduced FinTech's background and how it came to the current fourth generation. Later, we identified the issues in each Fintech segment and mapped the blockchain-based applications with the issue within the allocated FinTech segment. Furthermore, we listed challenges and problems hindering blockchain development and implementation in FinTech.

In addition to reviewing the current stage of FinTech (from a DeFi perspective) and envisioning a blockchain-based DeFi future where centralized parties are utterly removed, we highlighted the current limitations of blockchain technology and pointed out how they could be solved in the future. Besides DeFi maintaining the self-custody user assets, we consider decentralized identity management valuable to the Fintech sector, where self-sovereign identities are achieved and have the potential to move blockchain from pseudonymous decentralization to true anonymity. As we know, cryptocurrency transactions are pseudonymous and are potentially vulnerable to mapping the public address of an account to the user's real identity by tracking blockchain activities.
Indeed, blockchain-based identity management can avoid such vulnerability and preserve user privacy by authentication that only reveals a minimal amount of the user's personal information. The combination of decentralized identity and DeFi is out of the scope of this article and remains as future work.

Author Contributions: Conceptualization, T.R. and H.A. Validation, Z.Y. Writing—original draft preparation, H.A. and T.R. Writing—review and editing, H.A. and Z.Y. Supervision, R.J. and R.D.P. Funding acquisition, R.J. and R.D.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by awards NPRP11S-0109-180242 from the QNRF-Qatar National Research, a member of The Qatar Foundation. The findings reported herein are solely the responsibility of the authors.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study, in the collection, analyses, or interpretation of data, in the writing of the manuscript, or in the decision to publish the results.

References

1. Demirguc-Kunt, A.; Klapper, L.; Singer, D.; Ansar, S.; Hess, J. The Global Findex Database 2017. In *Measuring Financial Inclusion and the FinTech Revolution*; World Bank: Washington, DC, USA, 2018. ISBN 1464812594.
2. Sahay, R.; Allmen, U.; Lahreche, A.; Khera, P.; Ogawa, O.; Bazarbash, M.; Beaton, K. *The Promise of Fintech: Financial Inclusion in the Post COVID-19 Era*; International Monetary Fund: Washington, DC, USA, 2020. ISBN 1513512242.
3. Ziegler, T.; Zhang, B.; Carvajal, A.; Barton, M.; Smit, H.; Wenzlaff, K.; Natarajan, H.; Ferri de Camargo Paes, F.; Suresh, K.; Forbes, H.; et al. The global COVID-19 finTech market rapid assessment study; CCAF, World Bank and World Economic Forum. 2020. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3770789 (accessed on January 2022).
4. Gartner. The CIO's guide to blockchain. 2022. Available online: https://www.gartner.com/smarterwithgartner/the-cios-guide-to-blockchain (accessed on September 2022).
5. Guo, Y.; Liang, C. Blockchain application and outlook in the banking industry. *Financ. Innov.* **2016**, *2*, 1–12. https://doi.org/10.1186/s40854-016-0034-9.
6. Gartner, Hype Cycle for Emerging Technologies, 2021. Available online: https://www.gartner.com/interactive/hc/4004623?ref=hp-wylo (accessed on December 2021).
7. Dorfleitner, D.; Braun, D. *Fintech, Digitalization, and Blockchain: Possible Applications for Green Finance, in the Rise of Green Finance in Europe*; Palgrave Macmillan: Cham, Switzerland, 2019; pp. 207–237. https://doi.org/10.1007/978-3-030-22510-0_9.
8. McGhin, T.; Choo, K.-K.R.; Liu, C.Z.; He, D. Blockchain in healthcare applications: Research challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *135*, 62–75. https://doi.org/10.1016/j.jnca.2019.02.027.
9. Novo, O. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet Things J.* **2018**, *5*, 1184–1195. https://doi.org/10.1109/JIOT.2018.2812239.
10. Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.-K.R. A systematic literature review of blockchain cyber security. *Digit. Commun. Networks* **2020**, *6*, 147–156. https://doi.org/10.1016/j.dcan.2019.01.005.
11. Al-Quraan, M.; Mohjazi, L.; Bariah, L.; Centeno, A.; Zoha, A.; Muhaidat, S.; Deb-bah, M.; Ali Imran, M. Edge-native intelligence for 6G communications driven by federated learning: A survey of trends and challenges. *arXiv* **2021**, arXiv:2111.07392. https://doi.org/10.48550/arXiv.2111.07392.
12. Xiao, Y.; Zhang, N.; Li, J.; Lou, W.; Hou, Y.T. PrivacyGuard: Enforcing private data usage control with blockchain and at-tested off-chain contract execution. In Proceedings of the European Symposium on Research in Computer Security, Online, 13 September 2020; Springer: Cham, Switzerland, 2020; pp. 610–629. https://doi.org/10.1007/978-3-030-59013-0_30.
13. Gayialis, S.P.; Kechagias, E.P.; Konstantakopoulos, G.D.; Papadopoulos, G.A.; Tatsiopoulos, I.P. An approach for creating a blockchain platform for labeling and tracing wines and spirits. In Proceedings of the IFIP International Conference on Advances in Production Management Systems, Nantes, France, 5–9 September 2021; Springer: Cham, Switzerland, 2021; pp. 81–89. https://doi.org/10.1007/978-3-030-85910-7_9.
14. Gayialis, S.P.; Kechagias, E.P.; Papadopoulos, G.A.; Masouras, D. A Review and Classification Framework of Traceability Approaches for Identifying Product Supply Chain Counterfeiting. *Sustainability* **2022**, *14*, 6666. https://doi.org/10.3390/su14116666.
15. Wang, Q.; Su, M. Integrating blockchain technology into the energy sector—from theory of blockchain to research and application of energy blockchain. *Comput. Sci. Rev.* **2020**, *37*, 100275. https://doi.org/10.1016/j.cosrev.2020.100275.
16. Gayialis, S.P.; Kechagias, E.; Papadopoulos, G.A.; Konstantakopoulos, G.D. Design of a blockchain-driven system for product counterfeiting restraint in the supply. In Proceedings of the IFIP International Conference on Advances in Production Management Systems, Austin, TX, USA, 1–5 September 2019.
17. Romānova, I.; Kudinska, M., Banking and Fintech: A challenge or opportunity? In *Contemporary Issues in Finance: Current Challenges from Across Europe*; Emerald Group Publishing Limited: Bingley, UK, 2016; ISBN 1786359070.
18. Mohammed, A.H.; Abdulateef, A.A.; Abdulateef, I.A. Hyperledger, Ethereum and blockchain technology: A short overview. In Proceedings of the 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 11–13 June 2021; pp. 1–6. https://doi.org/10.1109/HORA52670.2021.9461294.
19. Wang, G.; Zhang, S.; Yu, T.; Ning, Y. A Systematic Overview of Blockchain Research. *J. Syst. Sci. Inf.* **2021**, *9*, 205–238. https://doi.org/10.21078/JSSI-2021-205-34.
20. Moezkarimi, Z.; Nourmohammadi, R.; Zamani, S.; Abdollahei, F.; Golmirzaei, Z.; Arabsorkhi, A. An overview on technical characteristics of blockchain platforms. In Proceedings of the International Congress on High-Performance Computing and Big Data Analysis, Tehran, Iran, 23–25 April 2019; Springer: Cham, Switzerland. 2019; pp. 265–278. https://doi.org/10.1007/978-3-030-33495-6_20.
21. Kuo, T.-T.; Rojas, H.Z.; Ohno-Machado, L. Comparison of blockchain platforms: A systematic review and healthcare examples. *J. Am. Med. Inform. Assoc.* **2019**, *26*, 462–478; https://doi.org/1093/jamia/ocy185.

22. Ng, E.; Tan, B.; Sun, Y.; Meng, T. The strategic options of fintech platforms: An overview and research agenda. *Inf. Syst. J.* **2022**. https://doi.org/10.1111/isj.12388.
23. Gomber, P.; Koch, J.-A.; Siering, M. Digital Finance and FinTech: Current research and future research directions. *J. Bus. Econ.* **2017**, *87*, 537–580. https://doi.org/10.1007/s11573-017-0852-x.
24. Cai, C.; Marrone, M.; Linnenluecke, M.; Macquarie University Trends in FinTech Research and Practice: Examining the Intersection with the Information Systems Field. *Commun. Assoc. Inf. Syst.* **2022**, *50*, 803–834. https://doi.org/10.17705/1CAIS.05036.
25. Martín-Martín, A.; Orduna-Malea, E.; Thelwall, M.; Delgado-López-Cózar, E. December 3rd, 2019. Available online:https://blogs.lse.ac.uk/impactofsocialsciences/2019/12/03/google-scholar-web-of-science-and-scopus-which-is-best-for-me/ (accessed on 1 January 2022).
26. Deloitte. Fintech by the Numbers. 2022. Available online: https://www2.deloitte.com/tr/en/pages/financial-services/articles/fintech-by-the-numbers.html (accessed on 1 January 2022).
27. Bitcoin Wiki. Merkle Trees. 2022. Available online: https://en.bitcoin.it/wiki/Protocol_documentation#Merkle_Trees (accessed on 1 July 2022).
28. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. 2022. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 1 July 2022).
29. USDF Consortium. Introducing the USDF Consortium. 2022. Available online: https://www.usdfconsortium.com/ (accessed on 1 May 2022).
30. Litecoin. Litecoin Core Integration/Staging Tree. 2022. Available online: https://github.com/litecoin-project/litecoin (accessed on 1 July 2022).
31. Ethereum. Ethereum Whitepaper. 2022. Available online: https://ethereum.org/en/whitepaper/ (accessed on 1 June 2022).
32. Dhillon, V.; Metcalf, D.; Hooper, M. The Hyperledger project. In *Blockchain-Enabled Applications*; Apress: Berkeley, CA, USA, 2017; pp. 139–149. https://doi.org/10.1007/978-1-4842-3081-7_10.
33. ConsenSys. Quorum Whitepaper. 2022. Available online: https://github.com/ConsenSys/quorum/blob/master/docs/Quorum%20Whitepaper%20v0.2.pdf (accessed on 1 July 2022).
34. Corda. Consensus. 2022. Available online: https://docs.r3.com/en/platform/corda/4.7/open-source/key-concepts-consensus.html (accessed on 1 January 2022).
35. Maharjan, P.S. Performance Analysis of Blockchain Platforms. Master's Thesis, University of Nevada, Las Vegas, NV, USA, August 2018. https://doi.org/10.34917/14139888.
36. Morris, N. Five of Top 10 Container Shippers Join New Blockchain Consortium. 2022. Available online: https://www.ledgerinsights.com/container-shipping-blockchain-consortium-cargosmart/ (accessed on 1 May 2022).
37. Energyweb. We Build Operating Systems for Energy Grids. 2022. Available online: https://www.energyweb.org/ (accessed on).
38. IBM. IBM Food Trust: A New Era in the World's Food Supply. 2022. Available online: https://www.ibm.com/blockchain/solutions/food-trust (accessed on 1 May 2022).
39. Bitcointalk. Proof of Stake. 2011, Available online: https://bitcointalk.org/index.php?topic=27787.0 (accessed on 1 January 2022).
40. Crain, T.; Gramoli, V.; Larrea, M.; Raynal, M. DBFT: Efficient Byzantine Consensus with a Weak Coordinator and its Application to Consortium Blockchains. *arXiv* **2018**, arXiv:1702.03068.
41. Ren, Z.; Cong, K.; Pouwelse, J.; Erkin, Z. Implicit consensus: Blockchain with unbounded throughput. *arXiv* **2017**, arXiv:1705.11046.
42. Luu, L.; Narayanan, V.; Zheng, C.; Baweja, K.; Gilbert, S.; Saxena, P. A Secure Sharding Protocol for Open Blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 Oc-tober 2016; pp. 17–30. https://doi.org/10.1145/2976749.2978389.
43. Zou, J.; Ye, B.; Qu, L.; Wang, Y.; Orgun, M.A.; Li, L. A Proof-of-Trust Consensus Protocol for Enhancing Accountability in Crowdsourcing Services. *IEEE Trans. Serv. Comput*. **2018**, *12*, 429–445. https://doi.org/10.1109/TSC.2018.2823705.
44. Jeon, S.; Doh, I.; Chae, K. RMBC: Randomized mesh blockchain using DBFT consensus algorithm. In Proceedings of the 2018 International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 10–12 January 2018; pp. 712–717. https://doi.org/10.1109/ICOIN.2018.8343211.
45. Fu, X.; Wang, H.; Shi, P.; Mi, H. PoPF: A consensus algorithm for JCLedger. In Proceedings of the 2018 IEEE Symposium on Service-Oriented System Engineering (SOSE), Bamberg, Germany, 26–29 March 2018; pp. 204–209. https://doi.org/10.1109/SOSE.2018.00034.
46. Li, K.; Li, H.; Hou, H.; Li, K.; Chen, Y. Proof of Vote: A high-performance consensus protocol based on vote mechanism & consortium blockchain. In Proceedings of the 2017 IEEE 19th International Conference on High-Performance Computing and Communications, Bangkok, Thailand, 18–20 December 2017; pp. 466–473. https://doi.org/10.1109/HPCC-SmartCity-DSS.2017.61.
47. Bitshares. Delegated Proof of Stake (DPOS). 2022. Available online: https://how.bitshares.works/en/master/technology/dpos.html (accessed on 1 January 2022).
48. Chaumont, G.; Bugnot, P.; Hildreth, Z.; Giraux, B. DPoPS: Delegated Proof-of-Private-Stake, a DPoS Implementation under X-Cash, a Monero Based Hybrid-Privacy Coin, X-Cash Yellowpaper, 2019. 2022. Available online: https://3.122.229.24/whitepaper/XCASH_Yellowpaper_DPoPS.pdf (accessed on 1 January 2022).
49. Vukolić, M. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In Proceedings of the International Workshop on Open Problems in Network Security, Zurich, Switzerland, 29 October 2015; Springer: Cham, Switzerland, 2015; pp. 112–125. https://doi.org/10.1007/978-3-319-39028-4_9.

50. Ongaro, D.; Ousterhout, J. The Raft Consensus Algorithm, Lecture Notes CS 190, 2015. 2022. Available online: https://raft.github.io/slides/riconwest2013.pdf (accessed on 1 September 2022).
51. Douceur, J.R. The Sybil attack. In Proceedings of the International Workshop on Peer-to-Peer Systems, Cambridge, MA, USA, 7–8 March 2002; Springer: Berlin/Heidelberg, Germany, 2002; pp. 251–260.
52. Wang, J.; Wang, H. Monoxide: Scale-out blockchains with asynchronous consensus zones. In Proceedings of the 16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19), Boston, MA, USA, 26–28 February 2019; pp. 95–112; ISBN 978-1-931971-49-2.
53. Sompolinsky, Y.; Zohar, A. Secure high-rate transaction processing in bitcoin. In Proceedings of the International Conference on Financial Cryptography and Data Security, San Juan, Puerto Rico, 26–30 January 2015; Springer: Berlin/Heidelberg, Germany, 2015; pp. 507–527. https://doi.org/10.1007/978-3-662-47854-7_32.
54. Sompolinsky, Y.; Lewenberg, Y.; Zohar, A. Spectre: A fast and scalable cryptocurrency protocol; Cryptology ePrint Archive, Paper 2016/1159. 2016. Corpus ID: 20050445.
55. Eyal, I.; Gencer, A.E.; Sirer, E.G.; Renesse, R.V., {Bitcoin-NG}: A scalable blockchain protocol. In Proceedings of the 13th USENIX symposium on networked systems design and implementation (NSDI 16), Santa Clara, CA, USA, 16–18 March 2016; pp. 45–59; ISBN 978-1-931971-29-4.
56. Kovalchuk, L.; Kaidalov, D.; Shevtsov, O.; Nastenko, A.; Rodinko, M.; Oliynykov, R. Analysis of splitting attacks on Bitcoin and GHOST consensus protocols. In Proceedings of the 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Bucharest, Romania, 21–23 September 2017; pp. 978–982. https://doi.org/10.1109/IDAACS.2017.8095233.
57. Ramezan, G.; Leung, C.; Jane Wang, Z. A Strong Adaptive, Strategic Double-Spending Attack on Blockchains. 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), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1219–1227.
58. Kiayias, A.; Russell, A.; David, B.; Oliynykov, R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2017; Springer: Cham, Switzerland, 2017; pp. 357–388.
59. Bandara, E.; Shetty, S.; Mukkamala, R.; Liang, X.; Foytik, P.; Ranasinghe, N.; Zoysa, K. Casper: A blockchain-based system for efficient and secure customer credential verification. *J. Bank. Financ. Technol.* **2022**, *6*, 43–62.
60. Ramachandran, G.S.; Wright, K.-L.; Zheng, L.; Navaney, P.; Naveed, M.; Krishnamachari, B.; Dhaliwal, J. Trinity: A Byzantine fault-tolerant distributed publish-subscribe system with immutable blockchain-based persistence. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea, 14–17 May 2019; pp. 227–235. https://doi.org/10.1109/BLOC.2019.8751388.
61. Yanovich, Y.; Ivashchenko, I.; Ostrovsky, A.; Shevchenko, A.; Sidorov, A. Exonum: Byzantine fault-tolerant protocol for blockchains. *Bitfury* **2018**, 1–36, 408p.
62. Moniz, H., 2020. The Istanbul BFT consensus algorithm. *arXiv Prepr.* **2022**, arXiv:2002.03613.
63. Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, W.; Chen, X.; Weng, J.; Imran, M. An overview on smart contracts: Challenges, advances and platforms. *Future Gener. Comput. Syst.* **2020**, *105*, 475–491. https://doi.org/10.1016/j.future.2019.12.019.
64. Ripple. Business Impact, Powered by Crypto. 2022. Available online: https://ripple.com/ (accessed on 1 September 2022).
65. Zhang, R.; Xue, R.; Liu, L. Security and Privacy on Blockchain. *ACM Comput. Surv.* **2019**, *52*, 1–34. https://doi.org/10.1145/3316481.
66. Monrat, A.A.; Schelen, O.; Andersson, K. A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities. *IEEE Access* **2019**, *7*, 117134–117151. https://doi.org/10.1109/ACCESS.2019.2936094.
67. Grayscale. A Digital-Native Asset Manager for a Digital-Driven World. 2022. Available online: https://grayscale.com/ (accessed on 1 January 2022).
68. Consensys. 5 Reasons Why Enterprise Ethereum Is so Much More Than a Distributed Ledger Technology. 2022. Available online: https://consensys.net/enterprise-ethereum/best-blockchain-for-business/5-reasons-why-enterprise-ethereum-is-so-much-more-than-a-distributed-ledger-technology/ (accessed on 1 January 2022).
69. Gleim, B.; Bertani, T.; Cabelguen, J.; Towne, B.; Kohorn, D.; Polzer, G. Enterprise Ethereum Alliance Off-Chain Trusted Compute Specification v1. 0, Enterp. Ethereum Alliance, 2019. 2022. Available online: https://entethalliance.org/wp-content/uploads/2019/05/EEA_Off_Chain_Trusted_Compute_Specification_V0_1.pdf (accessed on 1 December 2021).
70. Ethereum. Upgrading Ethereum to Radical New Heights. 2022. Available online: https://ethereum.org/en/upgrades/ (accessed on 1 June 2022).
71. Foschini, L.; Gavagna, A.; Martuscelli, G.; Montanari, R. Hyperledger Fabric blockchain: Chaincode performance analysis. In Proceedings of the ICC 2020–2020 IEEE International Conference on Communications (ICC), Halifax, NS, Canada, 30 July–3 August 2020; pp. 1–6. https://doi.org/10.1109/Cybermatics_2018.2018.00216.
72. OASIS PKCS 11 TC. PKCS# 11 Cryptographic Token Interface Base Specification Version 2.40, 2015. 2022. Available online: https://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/os/pkcs11-base-v2.40-os.pdf (accessed on 1 August 2022).
73. Nasir, Q.; Qasse, I.A.; Abu Talib, M.; Nassif, A.B. Performance Analysis of Hyperledger Fabric Platforms. *Secur. Commun. Netw.* **2018**, *2018*, 3976093. https://doi.org/10.1155/2018/3976093.
74. Baliga, A.; Subhod, I.; Kamat, P.; Chatterjee, S. Performance evaluation of the Quorum blockchain platform. *arXiv* **2018**, arXiv:1809.03421.

75. Brown, R.G. The Corda Platform: An Introduction, 2018. 2022. Available online: https://www.corda.net/content/corda-platform-whitepaper.pdf. (accessed on 1 August 2022).
76. Business World. Which Platform Offers a Modular Architecture in Blockchain? 2022. Available online: https://www.businessworldit.com/blockchain-cryptocurrency/which-platform-offers-a-modular-blockchain-in-architecture/ (accessed on 1 August 2022).
77. Gupta, N. Why Hyperledger Fabric Will Win against R3 Corda and Quorum? 2022. Available online: https://akeo.tech/blog/blockchain-and-dlt/enterprise-blockchains-hyperledger-fabric-corda-quorum/ (accessed on 1 August 2022).
78. GoQuorum. Consensus Protocols, 2022. Available online: https://consensys.net/docs/goquorum/en/stable/concepts/consensus/ (accessed on 1 August 2022).
79. Hyperledger Fabric. Using FabToken. 2022. Available online: https://fabric-documentations.readthedocs.io/en/latest/token/FabToken.html (accessed on 1 August 2022).
80. Corda. Transactions Per Second (TPS). 2022. Available online: https://www.corda.net/blog/transactions-per-second-tps/ (accessed on 1 August 2022).
81. Zetzsche, D.A.; Arner, D.W.; Buckley, R.P. Decentralized Finance (DeFi). *SSRN Electron. J.* **2020**, *6*, 172–203. https://doi.org/10.2139/ssrn.3539194.
82. Werner, S.M.; Perez, D.; Gudgeon, L.; Klages-Mundt, A.; Harz, D.; Knottenbelt, W.J. SoK: Decentralized Finance (DeFi). *SSRN Electron. J.* **2021**, 1–19. https://doi.org/10.2139/ssrn.3782216.
83. Fernandez-Vazquez, S.; Rosillo, R.; De La Fuente, D.; Priore, P. Blockchain in FinTech: A Mapping Study. *Sustainability* **2019**, *11*, 6366. https://doi.org/10.3390/su11226366.
84. Harvey, C.R.; Ramachandran, A.; Santoro, J. DeFi and the Future of Finance. *SSRN Electron. J.* **2021**, *2020*. https://doi.org/10.2139/ssrn.3711777.
85. Amler, H.; Eckey, L.; Faust, S.; Kaiser, M.; Sandner, P.; Schlosser, B. DeFining DeFi: Challenges & Pathway. In Proceedings of the 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 27–30 September 2021. https://doi.org/10.48550/arXiv.2101.05589.
86. Available online: https://www.investopedia.com/terms/f/fintech.asp (accessed on 9 October 2022).
87. Caldarelli, G.; Ellul, J. The Blockchain Oracle Problem in Decentralized Finance—A Multivocal Approach. *Appl. Sci.* **2021**, *11*, 7572. https://doi.org/10.3390/app11167572.
88. Arner, D.W.; Barberis, J.; Buckley, R.P. The evolution of Fintech: A new post-crisis paradigm. *Geo. J. Int*. **2015**, *47*, 1271. https://doi.org/10.2139/SSRN.2676553.
89. Keynes, J. *The Economic Consequences of the Peace*; Routledge: London, UK, 2017. ISBN 1351304641.
90. Arner, D.; Buckley, R.; Charamba, K.; Sergeev, A.; Zetzsche, D. Governing Fintech 4.0: Bigtech, Platform Finance, and Sustainable Development. Fordham J. Corp. Fin. L. **2022**, *27*, 1.
91. KPMG. Pulse of Fintech H2 2021—Global. 2022. Available online: https://home.kpmg/xx/en/home/insights/2022/01/pulse-of-fintech-h2-2021-global.html (accessed on 1 August 2022).
92. Puschmann, T. Fintech. *Bus. Inf. Syst. Eng*. **2017**, *59*, 69–76.
93. Infosys. Fintech Revolution in Banking: Leading the Way to Digital. 2022. Available online: https://www.infosys.com/industries/financial-services/white-papers/Documents/fintech-revolution-banking.pdf (accessed on 1 August 2022).
94. PEERIQ. Data and Liquidity for Marketplace Lending. 2022. Available online: https://www.peeriq.com/ (accessed on 1 August 2022).
95. Wyman, O. Payments in Retail. 2022. Available online: https://www.oliverwyman.com/our-expertise/insights/2019/dec/retail-consumer-journal-vol-7/payments-in-retail.html (accessed on 1 August 2022).
96. Thompson, J. Credit card processing costs and fees explained. 2022. Available online: https://www.businessnewsdaily.com/16583-credit-card-processing-costs-fees-explained.html (accessed on 1 August 2022).
97. Gurus, C. Costly Payment Processing Errors and How to Avoid Them. 2022. Available online: https://www.chargebackgurus.com/blog/payment-processing-errors (accessed on 1 August 2022).
98. Grayscale Building Blocks. An introduction to Stellar Lumens. 2022. Available online: https://grayscale.com/wp-content/uploads/2021/10/grayscale-building-blocks-stellar-lumens-october-2021.pdf.pdf (accessed on 1 August 2022).
99. Stellar Development Foundation. Why Quorums matter and how Stellar approaches them. 2022. Available online: https://medium.com/stellar-developers-blog/why-quorums-matter-and-how-stellar-approaches-them-547336c1275 (accessed on 1 August 2022).
100. Takyar, A. How Can Blockchain Improve the Point of Sale Process? 2022. Available online: https://www.leewayhertz.com/how-blockchain-improve-point-of-sale-process/ (accessed on 1 August 2022).
101. Gieseke, E. Creating a Point-of-Sale Application with the Algorand Blockchain. 2022. Available online: https://developer.algorand.org/solutions/creating-point-sale-application-algorand-blockchain/ (accessed on 1 August 2022).
102. Algorand. Algorand Scalability. 2022. Available online: https://www.algorand.com/technology/scalability (accessed on 1 August 2022).
103. PundiX. PundiX Whitepaper. 2022. Available online: https://pundix.com/pdf/PundiX_Whitepaper_EN_Ver.pdf (accessed on 1 August 2022).

104. Qiu, T.; Zhang, R.; Gao, Y. Ripple vs. SWIFT: Transforming cross border remittance using blockchain technology. *Procedia Comput. Sci.* **2019**, *147*, 428–434. https://doi.org/10.1016/j.procs.2019.01.260.
105. SureRemit. SureRemit Whitepaper. 2022. Available online: https://www.allcryptowhitepapers.com/sureremit-whitepaper/ (accessed on 1 August 2022).
106. Mademanalex. Sureremit Global Non-Cash Remittance platform and Cryptocurrency. 2022. Available online: https://medium.com/@masauwuphone/sureremit-global-non-cash-remittance-platform-and-cryptocurrency-69f565b806a0 (accessed on 1 August 2022).
107. Norta, A.; Leiding, B.; Lane, A. Lowering financial inclusion barriers with a blockchain-based capital transfer system. In Proceedings of the IEEE INFOCOM 2019—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Paris, France, 29 April 2019–2 May 2019; pp. 319–324. https://doi.org/10.1109/INFCOMW.2019.8845177.
108. Colendi. 2022. Available online: https://www.colendi.com/ (accessed on 1 August 2022).
109. Colendi. Colendi Technical Paper. 2022. Available online: https://www.scribd.com/document/477004197/Colendi-technical-paper-EN (accessed on 1 August 2022).
110. Provenance. Provenance Whitepaper. 2022. Available online: https://bfi.uchicago.edu/wp-content/uploads/Provenance-Whitepaper.pdf (accessed on 1 August 2022).
111. Figure. Personal Loan FAQs. 2022. Available online: https://www.figure.com/faqs/personal-loan/ (accessed on 1 August 2022).
112. ErCelsius. Celsius Whitepaper. 2022. Available online: https://whitepaper.io/document/524/celsius-whitepap (accessed on 1 August 2022).
113. Binance. Binance Whitepaper. 2022. Available online: https://whitepaper.io/document/10/binance-whitepaper (accessed on 1 August 2022).
114. FTX. FTX Token Whitepaper. 2022. Available online: https://whitepaper.io/document/502/ftx-token-whitepaper (accessed on 1 August 2022).
115. Coinbase. Crypto Resources: What to Read, Watch, and Stream in Crypto. 2022. Available online: https://www.coinbase.com/learn/crypto-basics/essential-reading (accessed on 1 August 2022).
116. Merrill. 2022. Available online: https://www.ml.com/ (accessed on 1 August 2022).
117. Goldman Sachs, Goldman Sachs. 2022. Available online: https://www.goldmansachs.com/ (accessed on 1 August 2022).
118. Fidelity Digital Assets. The Institutional Standard for Digital Assets. 2022. Available online: https://www.fidelitydigitalassets.com/ (accessed on 1 August 2022).
119. Lin, L.; Nestarcova, D. Venture capital in the rise of crypto economy: Problems and prospects. *Berkeley Bus. L. J.* **2019**, *16*, 533.
120. SPiCE. SPiCE VC. 2022. Available online: https://spicevc.com/ (accessed on 1 August 2022).
121. Pantera Capital. First U.S. Institutional Asset Manager Focused Exclusively on Blockchain Technology. 2022. Available online: https://panteracapital.com/ (accessed on 1 August 2022).
122. Blockchain Capital. Blockchain Venture Pioneers. 2022. Available online: https://blockchain.capital/ (accessed on 1 August 2022).
123. Sharma, R. Retail Investors Are Back in Crypto Markets. 2022. Available online: https://www.investopedia.com/retail-investors-are-back-in-crypto-markets-5095407 (accessed on 1 August 2022).
124. Schwab. Charles Schwab. 2022. Available online: https://www.schwab.com/ (accessed on 1 August 2022).
125. ETRADE. ETRADE from Morgan Stanley. 2022. Available online: https://us.etrade.com/ (accessed on 1 August 2022).
126. Robinhood. Robinhood Markets. 2022. Available online: https://robinhood.com/us/en/ (accessed on 1 August 2022).
127. Webull. Webull Financial. 2022. Available online: https://www.webull.com/ (accessed on 1 August 2022).
128. Interactive Brokers. 2022. Available online: https://www.interactivebrokers.com/en/home.php (accessed on 1 August 2022).
129. Merrill Edge. 2022. Available online: https://www.merrilledge.com/ (accessed on 1 August 2022).
130. Brown, A. What Is An NFT—And Should You Buy One? 2022. Available online: https://www.forbes.com/sites/abrambrown/2021/02/26/what-is-an-nft-and-should-you-buy-one/?sh=2803b4ff24b2 (accessed on 1 August 2022).
131. OpenSea. Discover, Collect, and Sell Extraordinary NFTs. 2022. Available online: https://opensea.io/ (accessed on 1 August 2022).
132. Etheria. 2022. Available online: https://etheria.world/ (accessed on 1 August 2022).
133. Pymnts. NFTs Hit $17B in Trading in 2021, Up 21,000%. 2022. Available online: https://www.pymnts.com/nfts/2022/nfts-hit-17b-in-trading-in-2021-up-21000/ (accessed on 1 August 2022).
134. Deloitte. The new era for KYC processes. 2022. Available online: https://www2.deloitte.com/content/dam/Deloitte/fi/Documents/risk/The%20new%20era%20for%20KYC%20processes.pdf (accessed on 1 August 2022).
135. Kiong, L.V. *DeFi, NFT and GameFi Made Easy: A Beginner's Guide to Understanding and Investing in DeFi, NFT and GameFi Projects*; Publisher: Independently published, 2021; 155p. ISBN 8488549050.
136. Meta. 2022. Available online: https://about.facebook.com/ (accessed on 1 August 2022).
137. Crypto. Top GameFi Coins by Market Capitalization. 2022. Available online: https://crypto.com/price/categories/gamefi (accessed on 1 August 2022).
138. Kastrenakes, J. Jack Dorsey Says VCs Really Own Web3 (and Web3 Boosters Are Pretty Mad about It). 2022. Available online: https://www.theverge.com/2021/12/21/22848162/jack-dorsey-web3-criticism-a16z-ownership-venture-capital-twitter (accessed on 1 August 2022).
139. GDPR.EU. What is GDPR, the EU's New Data Protection Law? 2022. Available online: https://gdpr.eu/what-is-gdpr/ (accessed on 1 August 2022).

140. The Privacy Commissioner of Canada. The Personal Information Protection and Electronic Documents Act (PIPEDA). 2022. Available online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/ (accessed on 1 August 2022).
141. State of California Department of Justice. California Consumer Privacy Act (CCPA). 2022. Available online: https://oag.ca.gov/privacy/ccpa (accessed on 1 August 2022).
142. Pandey, S. AscendEX Reportedly Loses ~$78M after Its Hot Wallet is Compromised. 2022. Available online: https://ambcrypto.com/ascendex-loses-78m-after-its-hot-wallet-is-compromised/ (accessed on 1 August 2022).
143. Cryptopedia. What Was the DAO? 2022. Available online: https://www.gemini.com/cryptopedia/the-dao-hack-makerdao (accessed on 1 August 2022).
144. Golubova, A. Crypto Winter Impact: 50% Drop in the Number of Active Crypto Users, Says Bank of America. 2022. Available online: https://www.kitco.com/news/2022-07-04/Crypto-winter-impact-50-drop-in-the-number-of-active-crypto-users-says-Bank-of-America.html (accessed on 1 August 2022).
145. Lasla, N.; Al-Sahan, L.; Abdallah, M.; Younis, M. Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm. *Comput. Networks* **2022**, *214*, 109118. https://doi.org/10.1016/j.comnet.2022.109118.
146. Alofi, A.; Bokhari, M.; Bahsoon, R.; Hendley, B. Optimizing the Energy Consumption of Blockchain-based Systems Using Evolutionary Algorithms: A New Problem Formulation. *IEEE Trans. Sustain. Comput.* **2022**. https://doi.org/10.1109/TSUSC.2022.3160491.
147. Nairametrics. Ethereum to Process 100,000 Transactions per Second—Vitalik Buterin, Co-Founder. 2022. Available online: https://nairametrics.com/2022/07/22/ethereum-to-process-100000-transaction-per-second-vitalik-buterin-co-founder/ (accessed on 1 August 2022).
148. Blömer, J.; Bobolz, J.; Diemert, D.; Eidens, F. Updatable anonymous credentials and applications to incentive systems. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 11–15 November 2019; pp. 1671–1685. https://doi.org/10.1145/3319535.3354223.
149. Zhou, Q. Blockchain Storage Explosion: Problem, Analysis, and Solutions. 2022. Available online: https://medium.com/@qizhou_63115/blockchain-storage-explosion-problem-analysis-and-solutions-14ece07fe6a1 (accessed on 1 July 2022).
150. SWIFT. SWIFT—The Global Provider of Secure Financial Messaging Services. 2022. Available online: https://www.swift.com/ (accessed on 1 July 2022).