sustainability

MDPI

Review

Blockchain Interoperability: Towards a Sustainable Payment System

Debasis Mohanty [1], Divya Anand [1,*], Hani Moaiteq Aljahdali [2] and Santos Gracia Villar [3,4]

[1] School of Computer Science and Engineering, Lovely Professional University, Phagwara 144411, India; debasis.41900381@lpu.in
[2] Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 37848, Saudi Arabia; hmaljahdali@kau.edu.sa
[3] Higher Polytechnic School/Industrial Organization Engineering, Universidad Europea del Atlántico, Isabel Torres 21, 39011 Santander, Spain; santos.gracia@uneatlantico.es
[4] Project Department, Universidade Internacional do Cuanza Bairro Kaluanda, Cuito EN 250, Bié, Angola
* Correspondence: divyaanand.y@gmail.com

Abstract: The highly fragmented blockchain and cryptocurrency ecosystem necessitates interoperability mechanisms as a requirement for blockchain-technology acceptance. The immediate implication of interchain interoperability is automatic swapping between cryptocurrencies. We performed a systematic review of the existing literature on Blockchain interoperability and atomic cross-chain transactions. We investigated different blockchain interoperability approaches, including industrial solutions, categorized them and identified the key mechanisms used, and list several example projects for each category. We focused on the atomic transactions between blockchain, a process also known as atomic swap. Furthermore, we studied recent implementations along with architectural approaches for atomic swap and deduced research issues and challenges in cross-chain interoperability and atomic swap. Atomic swap can instantly transfer tokens and significantly reduce the associated costs without using any centralized authority, and thus facilitates the development of a sustainable payment system for wider financial inclusion.

Keywords: blockchain; interoperability; atomic; swap; P2P; cryptocurrency; exchange

Citation: Mohanty, D.; Anand, D.; Aljahdali, H.M.; Villar, S.G. Blockchain Interoperability: Towards a Sustainable Payment System. *Sustainability* **2022**, *14*, 913. https://doi.org/10.3390/su14020913

Academic Editor: Nicu Bizon

Received: 7 October 2021
Accepted: 9 December 2021
Published: 14 January 2022

1. Introduction

The idea of a chain of blocks called Blockchain was put forward by Satoshi Nakamoto in 2008 [1]. Nakamoto implemented the concept in a peer-to-peer decentralized cryptocurrency called Bitcoin. Blockchain is an immutable, append-only decentralized distributed ledger system that addresses the byzantine fault tolerance problem in centralized ledger systems. The development of Blockchain technology can be divided into four stages [2]. Blockchain 1.0 has cryptocurrency application, Blockchain 2.0 provides smart contracts whereas Blockchain 3.0 develops distributed applications (dapps) that cater to several fields beyond financial applications or asset transfers. Blockchain 4.0 includes industry 4.0 applications. The common use case of blockchain 1.0 is the electronic payment system or cryptocurrency. Different terminologies that refer to Blockchain 2.0 include Bitcoin 2.0, Bitcoin 2.0 protocols, smart contracts, smart property, etc. Ethereum Smart contracts [3], Hyperledger Fabric [4], and R3's Corda [5] are examples of Blockchain 2.0. Common-use cases of Blockchain 3.0 include dapps for sectors such as governance, IoT, healthcare, supply chain, smart city, and many other non-financial applications. Blockchain 4.0 is focused on distributed ledger technology and real-life blockchain applications for industry 4.0 applications. Blockchain is currently used in several industries, in financial instruments, maintaining public/private records, health records, tangible assets, or intangible assets [6]. Figure 1 represents the evolution of blockchain.

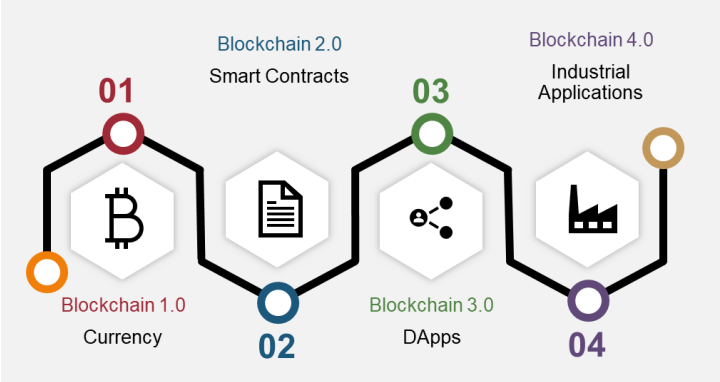

Figure 1. Evolution of Blockchain.

Due to the wide array of applications of distributed ledger technologies, different organizations have developed their version of Blockchain systems, catering to their need. This led to the in-house development of different blockchain projects using different protocols and architectures. These projects use different technologies, consensus protocols catering to specific use cases or applications. Such a large number of projects have made the development highly fragmented with very little or no interoperability between different blockchain projects. For the wide acceptance of these blockchain-based applications, they need to communicate with other blockchain applications, that are hosted on different blockchain networks. This will create a new system of communication between different isolated blockchain networks, thereby laying a foundation for the concept of interoperability between blockchain networks [7].

Blockchain Interoperability is defined according to the National Institute of Standards and Technology (NIST) as: "a composition of distinguishable blockchain systems, each representing a unique distributed data ledger, where atomic transaction execution may span multiple heterogeneous blockchain systems, and where data recorded in one blockchain are reachable, verifiable, and referable by another possibly foreign transaction in a semantically compatible manner [8]".

Currently, there is no standard way that different blockchain systems talk with each other and the Internet. The initial solution to blockchain interoperability is provided by Oracles. A blockchain oracle is any device or entity that connects a deterministic blockchain with off-chain data. Oracles provide an interface between smart contracts that live on the blockchain and any external data they need access to. Examples of blockchain oracle projects are Chainlink [9] and Augur [10]. Oracles have several problems:

1. Blockchains themselves cannot access off-chain data and vice versa.
2. Using centralized oracles nullifies the advantages of decentralization.
3. Security risks are associated with Oracles.

Blockchain interoperable protocols can be categorized into cross-chain and cross-blockchain protocols. Cross-chain protocols provide communication between homogenous blockchains, whereas cross-blockchain interoperability protocols facilitate communication between heterogeneous blockchains. An example of a cross-chain protocol is communication between Polygon and Avalanche. An example of a cross-blockchain protocol is communication between Bitcoin and Ethereum. The cross-blockchain protocol design is difficult as both the source and target of blockchain systems may differ in the hashing scheme, consensus algorithm, block size, execution environment, and network design. It is not impossible, but it is difficult, to identify and verify data recorded in one chain from another chain just by examining the information exchanged between them. Cross Blockchain token transfer involves several challenges such as [11] (i) how to issue tokens on the blockchains, ways to disable tokens when they are leaving the blockchain, (ii) rebalancing of tokens across blockchain to maintain liquidity, (iii) which blockchain features are required for cross chain transfer and (iv) which blockchain is suitable for cross-blockchain transfer (v) realiza-

tion of cross-chain transfer despite lack of Turing-complete smart contracts. Crypto tokens, the most common application of blockchain technology, are a type of cryptocurrency that represents a digital asset that is stored in a blockchain.

The first and most popular use of blockchain is a cryptocurrency such as bitcoin. Following the success of bitcoin, many alternative cryptocurrency projects have been developed, each with its cryptocurrency. Besides, more and more companies have launched initial coin offerings to fund their businesses. It is quite likely that the number of cryptocurrencies in circulation will only increase in subsequent years. Such a large number of circulated cryptocurrencies will make mechanisms for interexchange essential requirements for the future. Therefore, it becomes necessary to develop interoperability solutions that will aid interoperability between cryptocurrencies. One of the solutions that is widely used in the exchange of cryptocurrency is the trusted exchange scheme Coinbase [12]. This has disadvantages such as 1. trusted exchange can become compromised due to hacking, 2. privacy issues, and 3. loss of funds if the exchange is compromised. Most recently, in 2021, Bilaxy crypto exchange lost nearly $21 M after its hot wallet was hacked [13]. The number of cryptocurrencies worldwide has increased from 66 in 2013 to more than 7500 in 2021 [14]. The immediate implication of blockchain interoperability will be the quick and automatic exchange of cryptocurrencies between parties or groups, called atomic swaps. The advantages of such atomic swaps are peer-to-peer transfer, a low cost of exchange, decentralization, and increased security compared to exchanges. The major disadvantages include complexity and privacy issues.

Atomic swaps can be performed on-chain or off-chain. Decred is the first cryptocurrency that began supporting on-chain atomic swap between Decred, Bitcoin, and Litecoin in September 2017 [15,16]. Off-chain atomic swap is performed by opening a payment channel between both parties. The first such off-chain atomic swap using the lightning network occurred between Bitcoin and Litecoin in November 2017 [17]. Recently, atomic swap has become the most important functionality among crypto players [18,19]. Most crypto wallets, including Liquality [20], support atomic-swap functionality. Generalized atomic swapping protocol development for P2P crypto exchange is an area that has a lot of research potential. Designing a blockchain interoperability mechanism involves understanding the underlying system architecture, operations, interoperability principles, and best practices. In this survey, we reviewed blockchain interoperability solutions, including interoperability between cryptocurrencies with a focus on cross-chain atomic swap protocols.

The contributions of the paper are:

- Providing an overview of existing blockchain interoperability solutions and their classification,
- Survey of cross-chain atomic swap protocols and interoperable application design architecture
- Considering challenges and design issues for interchain technologies

The remainder of the paper is organized as follows: Section 2 provides a brief review of existing blockchain interoperability solutions, Section 3 is a comprehensive survey on cross-chain atomic swaps, protocols, and architectures, Section 4 discusses issues, challenges, opportunities, and concluding remarks.

2. Technologies for Blockchain Interoperability

A comprehensive literature survey on blockchain interoperability is provided by Belchior et al. [21]. The authors broadly categorized blockchain interoperability solutions into the following three categories: Cryptocurrency-directed Approaches, Blockchain Engines, and Blockchain Connectors. The three broad categories are divided into subcategories. Authors in [22] categorized inter-blockchain communications into four distinct groups, as follows: sidechains, blockchain routers, smart contracts, and industrial solutions. Robinson [23] organized cross-chain solutions into three categories value, namely, swap, cross-chain messaging, and state pinning techniques. Wang [24] discussed the current state of blockchain interoperability and broadly categorized blockchain interoperability solutions as chain-based, bridge-based, and dapp-based interoperability. In this section, we discuss the underlying technologies for cross-blockchain transactions. We categorize them

into notary schemes, sidechain-based solutions, Blockchain routers, Hashed time locks, and Industrial solutions. Many projects implement a combination of mentioned blockchain interoperability technologies. Figure 2 shows the blockchain interoperability solution types and example projects. We classify cross-chain transactions as a special application and included them in the subsequent section.

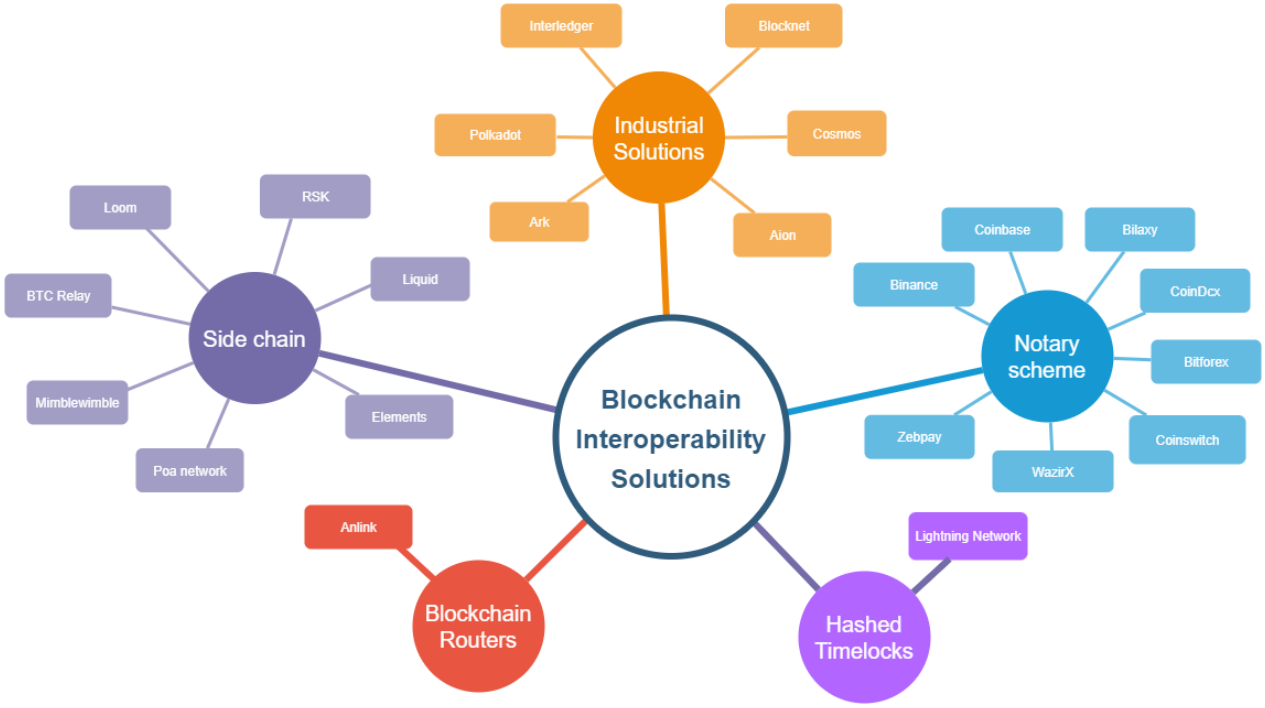

Figure 2. Blockchain Interoperability solutions and example projects.

2.1. Sidechains

The sidechain has three important components, including the mainchain, sidechain, and cross-chain communication protocol. A sidechain is a mechanism in which two existing blockchains interoperate [25]. One blockchain is called the mainchain and the other is called the sidechain. The mainchain maintains a ledger of assets and is connected to the sidechain with a cross-chain communication protocol. Sidechains act as a two-way peg, with a mechanism to transfer assets between the mainchain and sidechain [26]. Figure 3 shows the side chain connected with the mainchain. BTC Relay [27] is the first project that introduced the concept of relay and sidechain. BTC relay uses a technique called simplified payment verification (SPV). Many lightweight clients use SPV to cryptographically verify if transactions in a blockchain are included without downloading the entire chain. A chain of block headers showing proof of work is held by an SPV client. Merkle tree validation can be achieved with a limited number of inputs and calculations until the root hash. Example projects that use the sidechain technology are Loom [28], Elements [29], Liquid [30], Mimblewimble [31], Poa network [32] and RSK [33].

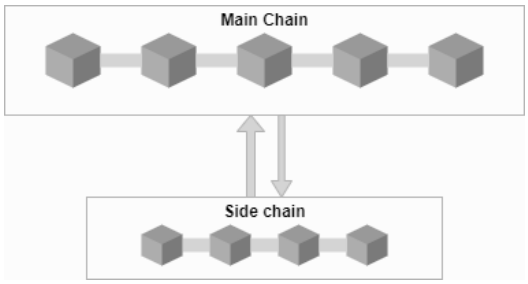

Figure 3. Sidechain.

2.2. Notary Schemes

In this scheme, transactions are dependent on a third-party notary. The trust deficit between both the parties of the transaction is managed by a trusted exchange called a notary. Both the parties trust the exchange. The notary can be a centralized exchange or can be a network of exchanges. The operation of notary schemes is solely dependent on the honesty of the notary. However, notary schemes are simple and easy to implement. Another drawback of the scheme is that the presence of a centralized element though a group of notaries decentralizes the scheme. Currently available notary schemes are centralized cryptocurrency exchanges such as Binance [34], Coinbase [12], Bilaxy [35], BitForex [36], WazirX [37], Zebpay [38], CoinDcx [39], Coinswitch [40].

2.3. Blockchain Routers

The concept of blockchain routers was first introduced by Wang et al. [41] in 2017. Blockchain routers facilitate inter-blockchain communication between different blockchain networks. The design of blockchain routers is inspired by the role of routers over the Internet. In blockchain router network architecture, the different blockchain networks such as bitcoin, Ethereum, etc., are regarded as terminal parts called sub-chains in the routing network. Sub-chains cannot directly communication with each other, and they can only communicate with a blockchain router. Inter sub-chain communication is made possible through the blockchain router following a cross-chain communication protocol. A blockchain maintains all information registered on sub-chains. The blockchain router enables inter sub-chain communication and establishes trust bridge cross-chains. The authors introduced four distinct participants in blockchain router architecture as a validator, connector, surveillant, and nominator. The blockchain router uses a practical byzantine fault tolerance algorithm. Blockchain routers can implement different algorithms based on business logic and user requirements. The Anlink blockchain network [42] uses Ann-router to provide interoperability across blockchains.

2.4. Industrial Solutions

Industrial solutions are blockchain systems that are developed to cater to specific utilities. A few prominent industrial projects include COSMOS [43], Polkadot [44] and Interledger [45]. COSMOS consists of a network of independent blockchains called zones. Zones use a tendermint consensus protocol. The first zone in a COSMOS network is called a hub. Hub and zones communicate by an inter-blockchain protocol. Interzone token transfer undergoes the COSMOS hub. The COSMOS hub monitors the total amount of tokens held by each zone. Cosmos allows developers to build both permissionless and permissioned blockchains. Polkadot is a heterogeneous multi-chain translation architecture. It enables customized sidechains to connect with a public blockchain. Different blockchains can exchange messages in a secure and trustless manner with Polkadot. Polkadot defines three types of blockchain classes as Parachains, Relay chains, and bridges. The token used in Polkadot is called a dot. Polkadot implements nominated proof-of-stake consensus protocol. Ark [46] creates an ecosystem allowing interoperability by using ARK smart bridge technology. ARK smart bridges make connections between standalone blockchains.

Other examples of major industrial blockchain interoperability solutions are Blocknet [47] and Aion [48].

2.5. Hashed Time Locks

In a two-party transaction, the parties publish a contract in which they take ownership of the asset of the other party. This hashed timelock contract [49] stores a pair (h, t) and guarantees that if the contract receives the corresponding secret s, $h = H(s)$, before time t has passed, the contract is activated, transferring ownership of the asset to the counterparty irreversibly. The asset is returned to the original owner if the contract does not obtain the matching secret before time t has passed. Hash locking is also useful for cross-chain atomic swaps, and HTLC is used to facilitate transactions routable through several payment channels. The amount of time within which either party must redeem assets is not fixed and varies between chains. The approach is potentially atomic, and sufficient time should be set aside for the second party to redeem funds after the owner or first-party has taken action. Otherwise, the first party will refuse to reveal s, and all funds will be returned. The Lightning Network [50] uses the hashed timelock, allowing the transaction to be performed off-chain. Table 1 shows blockchain interoperability projects and their features.

Table 1. Blockchain interoperability projects and their features.

Type	Blockchain Interoperability Project	Consensus Algorithm	Summary
Sidechain	BTC Relay	Proof of Work	First functional sidechain project Allows Ethereum contracts to securely verify Bitcoin transactions without any intermediaries Uses simplified payment verification (SPV) Mainchain is Bitcoin
	Mimblewimble	Proof of Work (Cuckoo Cycle)	Provides increased privacy and higher scalability Does not support scripts Mainchain is Bitcoin
	Poa network	Proof of Authority	Public sidechain of Ethereum Mainchain is Ethereum Rely on preselected validators Improves scalability
	RSK	Proof of Work	Enable execution of smart contracts Faster transactions and better scalability Mainchain is Bitcoin Bitcoins transferred to RSK become "Smart Bitcoins" (RBTC)
Blockchain Router	Anlink	Delegated Stake-Practical Byzantine Fault Tolerance	Ann-router provides connection, communication, and trust between chains Ann-Router can analyze communication data package Can send messages to sub-chain through Cross Blockchain Communication Protocol according to the Routing table dynamically maintained by itself

Table 1. *Cont.*

Type	Blockchain Interoperability Project	Consensus Algorithm	Summary
Industrial Solutions	COSMOS	Tendermint	COSMOS consists of a network of independent blockchains called zones The first zone in COSMOS network is called the hub Hub and zones communicate by inter blockchain protocol Interzone token transfer go through the COSMOS hub
	Polkadot	Nominated Proof of Stake	Defines three types of blockchain classes as Parachains, Relay chains, and bridges The token used in Polkadot is called dot Patachains participate in the Polkadot network Relay Chain serves as a connector to different parachains (or individual blockchains) through a system of bridges Includes three distinct node types (validators, collators, and fishermen)
Hashed Time locks	Lightening Network	Payment Channel	Uses the hashed time lock allowing transaction to be performed off-chain Used as a payment channel

3. Atomic Swaps

The major application of Blockchain is in performing monetary transactions in a decentralized way, without the use of any trusted third party. Several cryptocurrencies have been developed based on blockchain. Using exchanges to trade different bitcoins has disadvantages including being susceptible to hacking, exposure to privacy issues, and loss of funds for parties. In an atomic cross-chain swap, multiple parties exchange assets across multiple blockchains without using any intermediaries such as exchanges.

Imagine that Alice possesses x bitcoins and wants to trade it for y ethers. Bob has ethers in excess of y and is willing to trade ethers for bitcoins at the exchange rate. Here, both Alice and Bob hold their coins in different crypto networks. Alice and Bob can trade their tokens through a centralized exchange, such as Coinbase [12]. In the atomic swap, Alice and Bob, having different coins, exchange their coins without a trusted third party or centralized exchange. Figure 4 shows illustrates this transfer. In ideal conditions, the simple non-atomic protocol is that Alice sends her coins to Bob and Bob sends his coins to Alice. However, Bob can deviate from the protocol and choose not to send his coins, thus having both the amounts of coins. In an atomic swap, the transfer is atomic as it guarantees no loss of any asset. Atomic cross-chain swaps ensure atomicity, which is described as an all or nothing property, in which all or none of the transactions are performed. In the bitcoin forum, Nolan [51] describes atomic transfers between two parties on separate blockchains.

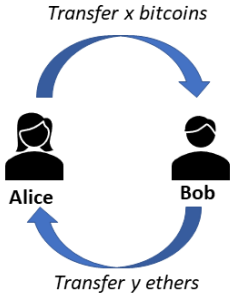

Figure 4. Two Party Swap.

The atomic swap guarantees the following 3 conditions [52]:

- if all parties conform to the protocol, then all swaps take place,
- if some coalition deviates from the protocol, then no conforming party ends up worse off, and
- no coalition has an incentive to deviate from the protocol. Atomic swaps can have applications in fields such as software versioning control, stocks, and commodity market clearing.

The atomic swap involves an exchange of assets at the limits of the blockchains. Atomic swap does not involve the destruction and recreation of assets from one blockchain to another, rather, an exchange of tokens takes place at the boundaries of the blockchain. Therefore, one requirement of atomic swap is the presence of an opposite party willing to exchange the tokens [53]. The cross-chain transaction can be considered as a special case of inter-blockchain communication, which involves information exchange between two blockchains without any central third party. Cross-blockchain communication facilitates cross-blockchain smart contract interaction as well as execution and transfer of smart contracts on different blockchains. As the cross-chain transaction is a form of inter-blockchain communication, the constraints and challenges that apply to inter-blockchain communication also apply to cross-chain transactions as well as cross-chain smart contract interaction.

In a swap, either party bears the risk of the other party defaulting in the transaction. Atomic swaps are a form of swap that guarantee the exchange of assets or tokens in their entirety. Herlihy [52] formalized the atomic-swap protocol between 3 parties in terms of a directed graph. Atomic swap is formalized as a digraph $D = (V, A)$, where each vertex in V represents a party and each edge A represents an asset transfer from the edge's head to its tail through shared blockchain. In the graphical representation of the atomic swap a subset of the vertices called leaders generate hashlock secrets and the rest of the vertices are called followers. The author describes the atomic swap as a cooperative game where an alliance member follows a common strategy. The outcome of the parties can be one of the following five states: freeride, discount, deal, no deal and underwater. A deal is the preferred state, whereas states such as freeride, discount, no deal can be accepted states as they in some way aid some conforming parties even if the protocol fails. Herlihy defined the requirements for a swap protocol to be uniform and in a strong Nash-equilibrium strategy. If a swap protocol is uniform and has a solid Nash equilibrium strategy, it is considered atomic. If, and only if, D is strongly connected, the author demonstrates that a uniform swap protocol for D is atomic. The author proposed a 2P protocol for atomic swap, with different actions/operations for leaders and followers phase wise. An analysis of the is presented, made using a simple pebble game.

The approaches used in [51,52] provide smart contract execution with hashed time locks for an atomic transaction. Using the protocol of Nolan [51], the atomic swap problem between Alice and Bob can be solved with the following steps, where Alice is the initiator of the transaction.

The contributions of the paper are:

1. Alice generates a secret s and a hashlock $h = H(s)$;
2. Alice uses the h to create a smart contract that locks x bitcoins and publishes it to the bitcoin network. If Bob produces s such that $h = H(s)$, the contract will allocate x bitcoins to Bob. The smart contract is also locked with timelock t_1, which means Bob must provide the secret s within time t_1 or Alice will receive an x bitcoin refund.
3. Since the contract is published in the bitcoin network, Bob can verify the authenticity of the contract.
4. Bob learns h from the contract Alice has created. He creates a smart contract and locks y ethers using h. The contract is locked with time lock t_2 with $t_2 < t_1$. The contract will refund Bob if Alice is unable to provide secret s within t_2. He then publishes his smart contract.

5. Alice checks the validity of Bob's contract and provides s within time t_2 to unlock Bob's contract. Alice received y ethers; the secret s is revealed to Bob. Bob provides the secret s to Alice's smart contract within time t_1 and receives x bitcoins.

The protocol requires the condition $t_1 > t_2$ so that Bob has enough time to provide the secret and receive the amount of coins.

Zakhari et al. [54] established two drawbacks in the protocol.

1. If Bob does not provide the secret by t_1 due to crash or network failure, he will not receive x bitcoins and Alice is refunded with x bitcoins, thus violating the atomic property.
2. The protocol necessitates the publication of smart contracts in a specific order. The sequential publication of smart contracts in atomic swaps with several participants raises the swap's latency proportionally to the number of contracts sequentially published.

Zakhari et al. [54] generalized an atomic swap as an atomic cross-chain commitment protocol. An atomic cross-chain commitment protocol is a trustless variation of a 2 phase commitment protocol used in distributed transactions. According to an atomic cross-chain commitment protocol, smart contracts in atomic cross-chain transactions can either all be redeemed, or all refunded. A redemption commitment scheme and a refund commitment scheme are two mutually incompatible commitment schemes in the atomic cross-chain commitment protocol. Based on the framework, the authors proposed an atomic-cross-chain commitment centralized trusted witness and atomic cross-chain commitment permissionless witness network. The authors used a multi-signature scheme instead of a hash timelock. Authors in [55] provided implementation-related shortcomings of HTLC and overcome them by extending the protocol with a multi-signature scheme. Using multisig transactions, the authors aimed to provide greater capabilities for cross-chain communications, without the provision of any extra trust. The protocol performs an atomic swap between a blockchain that supports scripting or smart contracts and one that supports multisig instead of HTLCs.

Cross-chain transactions may have off-chain executions and the transaction–representation directed graph might not be strongly connected [56]. The authors in the paper put forth a uniform 3-phase protocol for general cross-chain transactions with sequenced and off-chain steps in which a few parties confirm. Authors showed that the 3-party exchange requires that the mediator party has control of the incoming assets as well as outgoing assets. The proposed method transfers the transaction graph to an equivalent transaction graph to address the off-chain steps in tractions. The authors proposed a 3-phase protocol that complies with uniformity requirements and introduced a new property, terms as end-to-end, for transactions with off-chain steps. The property states that if the source parties pay, the sink parties are eventually paid. In equivalent transactions, the set of vertices remain the same and for each party, the net gain for each party must be the same for both the transactions. The proposed protocol strengthens the uniformity requirement by adding a third constraint as the protocol must be end-to-end. The authors demonstrated their Java-based synthesis tool XCHAIN to analyze the input graph and to construct contracts in the Solidity programming language.

Authors in [57] drafted two distributed commitment protocols and prove their working both analytically and experimentally. The first protocol, called Synchronous cross-Blockchain transactions protocol (SBP), strongly enforces ACID properties. The protocol provides strong consistency, but it has high latency. The strong consistent 2-phase commit protocol is suitable for financial transactions. The authors also proposed another protocol called the Redo-Log-Based Blockchain Protocol (RBP). RBP has the characteristic of low delay but supports a weak form of consistency called eventual consistency. The major challenge to blockchain interoperability is due to cross blockchain proof problem which states that it is not possible to verify on one blockchain A whether some particular data are recorded in another blockchain B [11]. The natural approach in inter blockchain transfer, also called spend-first, is to first mark the assets to be transferred on the source blockchain

as spent assets and claim the agreed-upon assets in the destination blockchain. The spend-first approach cannot eliminate double-spending due to the cross-blockchain proof problem. Borkowski et al. proposed a cross-blockchain asset-transfer protocol, using claim-first transactions [58]. The approach posts the claim transaction in the destination blockchain and allows others to create a valid spend transaction for the claim. The party that posts a valid spend transaction for the published claim transaction is rewarded. Cross-blockchain proof for the verification of data in one blockchain from another blockchain requires checking the whole blockchain to the start of the blockchain from the genesis block. A reverse form of the spend-first transaction, called a claim-first transaction, does not require verifying the spend transaction. The implementation challenges for the claim first transaction are managed using proof of Intent for sender authorization, recorded balances for the parties, the addition of the validity time-frame for double-spending, a time-period identifier for double destruction, and a proper rewarding mechanism for witnesses.

Liu et al. [59] provided further insight into blockchain interoperability by incorporating the dimension of programmability. The authors proposed a HyperService platform that allows interoperability and programmability between non-homogenous blockchain networks. The platform utilized the concept of cross-chain execution of decentralized apps or dapps. To ensure the correctness of the cross-chain dapps, the authors proposed a blockchain neutral Unified State Model (USM) to define cross-chain dapps and a high-level programming language, HSL, to write the inter-blockchain apps complying with the USM programming model. A generic blockchain interoperability protocol called the Universal Inter-blockchain Protocol (UIP) has been proposed, which is capable of securely executing complex cross-chain operations that involve smart contracts deployed on heterogeneous blockchains. HyperService has four architectural components, dapp clients interact with the HyperService; and a Verifiable Execution system (VESes) compiles the high-level dapp programs sent by dapp clients into runtime executables for the Hyperservice. Both VESes and dapp clients comply as per UIP. The UIP contains the Network Status Blockchain (NSB), which provides an objective and unified view of the dapp execution status, and ISCs arbitrate the correctness or violation of dapp executions in a trustless manner using NSB inputs.

Borkowski et al., in [60], proposed a cross-blockchain protocol called DeXTT to transfer a token on any blockchain in which transactions are autonomously synchronized in a decentralized manner. The protocol uses a pan-blockchain token called PBT, which is recognized and synchronized across wallets in all participating blockchains. The protocol accepts that eventual consistency for data synchronization as a strong consistency requirement cannot be achieved due to the cross-blockchain proof problem [11]. Dziembowski et al. [61] highlighted that the use of smart contracts for digital0asset transfer is costly, as each transaction requires validation from miners and the miners need to be paid commission. A zero-knowledge contingent payments (ZKCP) protocol [62] is very cheap compared to smart-contract execution, since it allows the contract to evaluate a hash function on a short input. The limitation of the ZKCP protocol is that it places a heavy computational burden on both parties. The protocol proposed in [61] has two advantages, cost minimization for smart contract execution and avoiding expensive cryptographic tools such as zero-knowledge proof. The authors note that the proof of misconduct can be short and that its verification involves fewer cryptographic operations. To discourage the sending party from cheating and to counter denial of service attacks, the protocol imposes a penalty. The protocol is efficient and includes low-cost construction for implementing "Claim and Refund" [63] functionality. Robinson et al. [64] proposed a General Purpose Atomic Cross-chain Transactions (GPACT) protocol, which facilitates the execution of a call execution tree that spans contracts on multiple blockchains. The protocol can run on Ethereum Virtual Machine (EVM) compatible blockchain platforms. For non-Ethereum blockchain platforms, the protocol requires validators who translate and validate the translated event data. Blockchain platforms that support smart-contract execution are desirable for cross-chain transfer mechanisms. However, widely used blockchain platforms such as Bitcoins

either do not support smart-contract execution or provide very limited support. A solution for the execution of smart contracts on legacy blockchain systems is proposed in [65].

All the major atomic cross-chain interoperability swap protocols discussed [51,52,54,57] do not address privacy issue as they rely on on-chain implementation of transactions through the execution of smart contracts. Andrew Poelstra [66] presented, for the first time, a scheme called scriptless scripts to provide privacy as well as efficiency and fungibility to bitcoin. The scriptless script concept was used primarily in Mimblewimble [31] platform which does not use scripting to execute transactions. Using Schnorr signatures, the scriptless scripts allows smart contracts to be executed off-chain. A scriptless cross-chain transaction has advantages such as better throughput and efficiency, privacy, and fungibility. G. Malavolta et al. [67] suggested a scriptless solution using ECDSA signatures to create a safe and privacy-preserving payment channel network. Its use in atomic swaps was also realized by the authors. Shlomovits et al. in [68] proposed a scriptless protocol for cross-chain atomic swapping using the gradual release of secrets. Deshpande et al. [69] formalized the notion of privacy for atomic-swap protocols. The authors proposed a privacy-preserving cross-chain atomic swap protocol, which, in addition to correctness and soundness, provides privacy, anonymity, and confidentiality to an atomic swap. The authors utilized the atomic release of secrets for conditional exchange with script-less scripts using adapter signature [67,70].

Inter-chain exchange requires the verification of transactions in a source chain from a target chain. This can be achieved using blockchain relays [71]. Relays, in principle, replicate a source blockchain's state within a destination blockchain, allowing the destination blockchain to verify the existence of specific pieces of state on the source blockchain. The source blockchain is replicated in a completely decentralized manner, which eliminates the need for trust in a centralized body. An atomic swap protocol, R-SWAP using relays and adapters for cross-chain swap has been proposed by Lys et al. [72] The authors formalized the blockchain relay and adapters and evaluated the performance of R-SWAP, using use-cases of permissionless-permissionless and permissioned-permissionless blockchain systems. The use of a relay increases the operational cost as verification requires both storage and calculation. The authors in [73] proposed another blockchain relay scheme that reduced cost by 92%, when evaluated with Ethereum-based blockchain.

The inherent characteristics of blockchain do not allow cross-smart contract calls. As a result, a smart contract, running on the source chain cannot contact another smart contract running on the target chain, receive the result from the target chain, and then return to the source chain to resume execution [53,74]. Nissl [75] pointed out the major challenge in blockchain interoperability, recognising that a transaction that is processed in a blockchain cannot be moved from the same blockchain. The author proposed a framework for executing smart contracts across blockchains. Argument passing, returning values, increased scalability, and recursive smart contract calls between different blockchains are also supported by the proposed method. Two smart contracts are needed for a smart contract interaction: a distribution contract on the source chain and an invocation contract on the target chain. Intermediaries, who serve as brokers and transfer information between the source and target chains, and validators, who validate the information forwarded by intermediaries, are included in the technique. The smart contract interaction scheme uses six phases, including the register, offer, execution, forwarding, verification, and finalization phases. To eliminate intermediaries with malicious intent, the approach uses an imposition of penalties as well as voting mechanisms. Honest validators are nominated using a delegated Proof of Stake protocol. Fynn et al. [76] conceptualized an inter blockchain move operation that allows smart contracts to migrate from a source blockchain to a destination blockchain using the programming model. The two-step process locks the smart contract in the source blockchain and recreates the smart contract in the target blockchain. The authors implemented and evaluated the move protocol using Ethereum [3] and Burrow [77] blockchains. The move protocol requires both of the blockchains to support 3 criteria: support for smart contracts, same execution environments (e.g., Virtual

machines), and a way to prove state variables (e.g., Merkel trees). ChainIDE is an IDE designed specifically for smart contract developers [78]. The authors addressed the need for developers to be empowered when developing smart contracts for various blockchain protocols. Inter-smart contract communication between smart contracts running in different blockchain networks was not considered by the authors.

In [79] the author described blockchain technology as a software system with two layers, namely, application and implementation. The application layer relates to user interfaces whereas the implementation layer deals manages the rest of the elements, including physical infrastructure, network, protocols, code, etc. To simplify the design of blockchain applications, the authors in [80–82] added further layers to the blockchain system. Figure 5 shows blockchain layers [82,83]. Layer 2 protocols provide secure, scalable, and cost-effective off-chain transactions [82]. The Layer Two Atomic Cross-Blockchain Function Calls (LTACFC) protocol proposed by Robinson et al. [83] offers synchronous, inter-contract, and atomic cross-blockchain function calls. Unlike the layer one cross-blockchain function calls, the layer two protocol does not require any modification in blockchain platform software. The atomic nature of the protocol ensures all or none of the states updates. Using hosted relay nodes, signed block headers passed from the source blockchain to the destination blockchain. To handle sections of a cross-blockchain function call, an instance of cross-blockchain control contracts is used. The protocol requires multiple signed block headers to be sent to each blockchain wherever required. LTACFC defines five types of functions such as start, segment, root, signal, and clean that are used in a Cross blockchain control contract. The performance overhead and security analysis of the protocol is also performed by the authors.

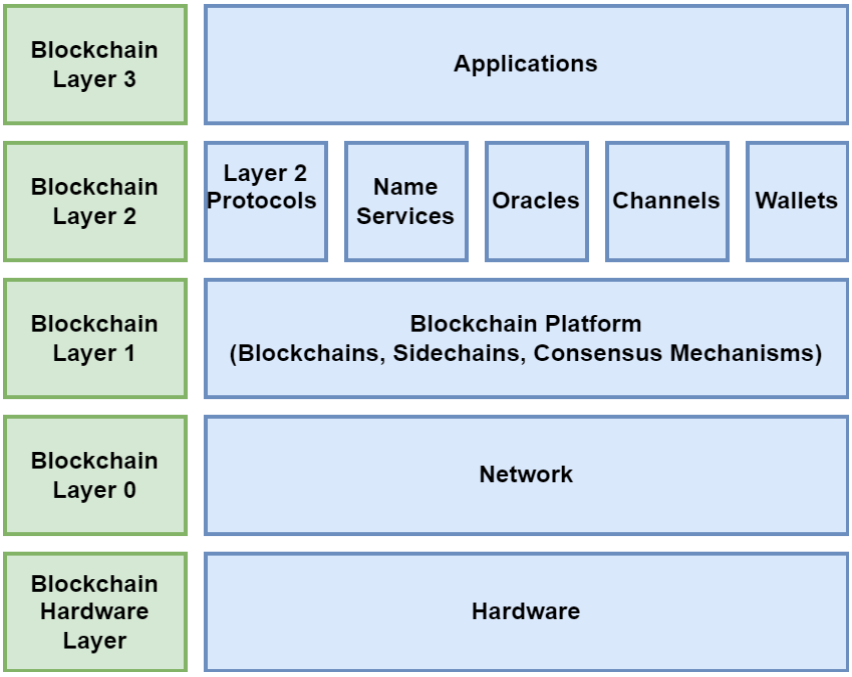

Figure 5. Blockchain Layers.

Authors in [7] proposed a new architecture for blockchain interoperability. The blockchain interoperability architecture contains 5 layers, namely, the data layer, network layer, consensus layer, contract layer, and application layer. Five considerations such as atomicity, efficiency, security, universality, and friendliness to address blockchain interoperability are discussed. Providing atomicity, efficiency, security, tolerance to diversity, developer friendliness are the challenges for implementing cross-blockchain interoperability.

The primary purpose of using blockchain is to provide tamper-proof data transfer. The cross-blockchain protocol developed needs to follow the security aspects of blockchain.

So, there is a need to develop cross-blockchain technologies that are also aligned with the security that the blockchain system provides. Pillai et al. [84] proposed an application layer-based cross-communication model for blockchain systems. The authors proposed a user-driven, application-level 2-stage model for cross-communication between blockchains, using transactions. In the information query stage, the recipient can request blocks from a client and verify the blocks. To make this step reliable, a consensus is required. In the second stage, also called state changes, the system is updated by data addition using transaction, verification, and validation. In the proposed approach, the authors made several assumptions. In the early form of the model, the authors did not consider any adverse condition that might arise due to security issues. The design of atomic cross-chain swap protocols for specific source and target cryptocurrencies is provided in [85,86]. The author in [85] proposed an atomic-swap protocol to complete transactions between Bitcoin and Monero using a scriptless approach. Another scriptless atomic swap between Bitcoin and Monero using adapter signature is proposed by P. Hoenisch et al. [86]. Table 2 shows the atomic cross-chain protocols and architectural approaches and their major contributions.

Atomic swaps can be used for cryptocurrency trading between parties operating in different cryptocurrency networks in a decentralized way. Traditional payment systems such as Visa and Paypal handle 1667 and 193 transactions per second (tps) on average, respectively [87]. In comparison to traditional payment systems, Bitcoin and Ethereum can only handle only 7 and 15 tps on average, respectively. Table 3 lists some of the major cryptocurrencies, average transactions per second achieved and smart contract execution as well as dapp support. Solana supports 50,000 tps, whereas Ripple supports 1500 tps. A higher value of tps characterize Solana and Ripple as suitable blockchain platforms for use as cryptocurrencies. Higher tps will also reduce the transaction cost. The highest number of crypto tokens have been launched based on the Ethereum platform. The next version of Ethereum, Ethereum 2.0 will be launched in 2022. Ethereum 2.0 will use a technique known as sharding, to significantly boost transaction speeds, with the potential to scale to 100,000 transactions per second or more. Atomic swap can be utilized to scale the payment network alongside a network of instantly confirmed micropayment channels [50,88]. The atomic swap will allow for a sustainable payment system for greater financial inclusion, by allowing tokens to be transferred quickly and at a lower cost without the use of a centralized authority. Besides, crypto-economics may regulate human behavior using incentive design, in order to tackle a variety of sustainability issues [89,90].

Table 2. Atomic swap protocols and architecture.

Author(s)	Year	Major Contribution(s)
P. Robinson et al. [64]	2021	GPACT protocol which facilitate a call execution tree that spans contracts on multiple blockchains Works with EVM-compatible blockchain platforms For non-EVM, requires validators
L. Lys et al. [72]	2021	Formalization of blockchain relay and adapter R-SWAP protocol using blockchain relays and adapters Protocol evaluation using Permissioned and Permissionless blockchains
P. Hoenisch et al. [86]	2021	Atomic swap protocol between Bitcoin and Monero Uses adapter signature
J. Gugger [85]	2020	Atomic swap protocol between Bitcoin and Monero Can be generalized to other cryptocurrencies Scriptless approach
P. Robinson et al. [83]	2020	Layer 2 atomic cross-chain function calls protocol Multiple signed block headers transfer between blockchains 5 types of function calls

Table 2. *Cont.*

Author(s)	Year	Major Contribution(s)
E. Fynn et al. [76]	2020	Smart contract migration (move operation) across blockchains
B. Pillai et al. [84]	2020	An application layer based cross-chain communication model
M. Nissl et al. [75]	2020	Framework for invoking smart contracts across blockchains
N. Shadab et al. [56]	2020	3P three-party exchange protocol Transforms the exchange into an equivalent transaction graph and execution
A. Deshpande et al. [69]	2020	Scriptless script-based protocol Addresses the privacy issues
O. Shlomovits et al. [68]	2020	Scriptless script-based protocol Gradual release of secrets
V. Zakhary et al. [54]	2019	Generalization of atomic cross-chain commitment protocol Centralized trusted witness and permissionless witness network protocol version
M. Borkowski et al. [60]	2019	DeXTT protocol accepting eventual consistency for data synchronization
J. Zie et al. [55]	2019	Multi-signature based atomic swap protocol
Z. Liu et al. [59]	2019	Platform for blockchain interoperability and programmability Cross-chain execution of dapps
H. Jin et al. [7]	2018	Five layered blockchain interoperability architecture, properties, challenges
M. Borkowski [58]	2018	Protocol based of claim first transaction
S. Dziembowski et al. [61]	2018	Efficient and low-cost FairSwap protocol compared to costly smart contract execution Proof of misbehavior and imposition of penalty for cheaters
M. Herlihy [52]	2018	Formalization of atomic swap and representation in terms of a directed graph Outcome of the atomic swap into any of the 5 states 2P atomic swap protocol and its analysis
T. Nolan [51]	2013	Implementation of Atomic swap protocol using HTLC

Table 3. Cryptocurrencies and transactions per second.

Cryptocurrency	Transactions per Second (TPS)	Support for Smart Contract	Support for Dapps
Bitcoin	7	Limited	No
Ethereum	15	Yes	Yes
Ripple (XRP)	1500	No (to support in future)	No
Bitcoin Cash	300	Limited	No
EOS	1000+	Yes	Yes
Litecoin (LTC)	50	Yes (recently)	No
Stellar	1000+	Limited	No
Cardano (ADA)	250	Yes	Yes
Tron (TRX)	1000+	Yes	Yes
Solana	50,000	Yes	Yes
Monero (XMR)	1000	No	No
Avalanche	4500	Yes	Yes

4. Discussion and Conclusions

4.1. Conclusions

Blockchain is a disruptive technology that has the potential to change the way digital assets are exchanged between parties. Blockchain interoperability has become a requirement for blockchain acceptance, and atomic cryptocurrency exchange between parties is an immediate consequence of blockchain interoperability. Atomic exchange protocols for cryptocurrencies, based on diverse blockchain platforms, are difficult to design if not impossible. Support for programmability, smart contract execution, and dapp-development aid in the development of atomic cross-chain transaction protocols. The programmability may induce security concerns as cryptocurrencies such as Monero do not provide any form of smart-contract support, thus providing more security and privacy. Off-chain atomic swaps that uses scriptless scripts tend to provide better privacy and performance compared to on-chain swap. On the other hand, blockchain platform programmability opens the door for the design of the diversely distributed application as newer platforms such as Cardano, Solana, and Avalanche, all extend their programmability support. Atomic swap can facilitate the development of a sustainable payment system for greater financial inclusion by allowing tokens to be transferred quickly and at a lower cost without the use of a central authority. In addition to this, crypto-economics has the potential to influence human behavior through incentive design, so as to address several sustainability challenges.

4.2. Theoretical Implication

The future of blockchain technology as well as its applications in terms of cryptocurrencies depends on the effectiveness, efficiency, and usability of blockchain interoperability solutions. Several projects are in motion to cater to interoperability between blockchain systems. Industrial solutions such as Cosmos, Interledger, and Polkadot require further stability for wide acceptance. In the future, even if a few such projects become successful and adopted, it will remain to be seen how such projects can interoperate. Therefore, there is a greater need for standards and APIs and similar developments for large-scale interoperability between blockchain platforms. The cryptocurrency ecosystem is not legally supported in many countries. Future applications of interchain interoperability depend on regulatory framework support. Moreover, transactions specifically catering to banking, financial and reality-like industries require proper legal and governance mechanisms at the level of individual cryptocurrencies as well as at interoperability mechanisms. The primary goal of atomic swap protocols is blockchain interoperability, yet the protocols can have greater application in many other fields involving various transactions. For the success of cryptocurrency along with interoperability, scalability is an important factor. Scalability for cryptocurrency transactions also requires that the atomic-swap protocols have highly scalable operation comparable to online digital transaction systems such as Visa. Another factor that can dictate their use is the cost of implementation of the atomic swap. Higher costs of implementation compared to traditional systems can make atomic swap a non-viable option.

Centralized payment systems including Visa are successful and widely used. Decentralized ledger-using inter-blockchain protocols cannot run parallelly, requiring another method by which to transfer money. Atomic-swap protocols must have the ability to operate with the centralized environment. For this interoperability mechanism systems between centralized and decentralized approaches need to be developed. Moreover, the centralized exchange has an advantage over decentralized inter-blockchain swapping in terms of convenience and wide acceptability. So, the development of a hybrid approach using the best elements of both schemes can be useful for many applications. Figure 6 summarizes the research issues in a cross-chain atomic swap protocol design.

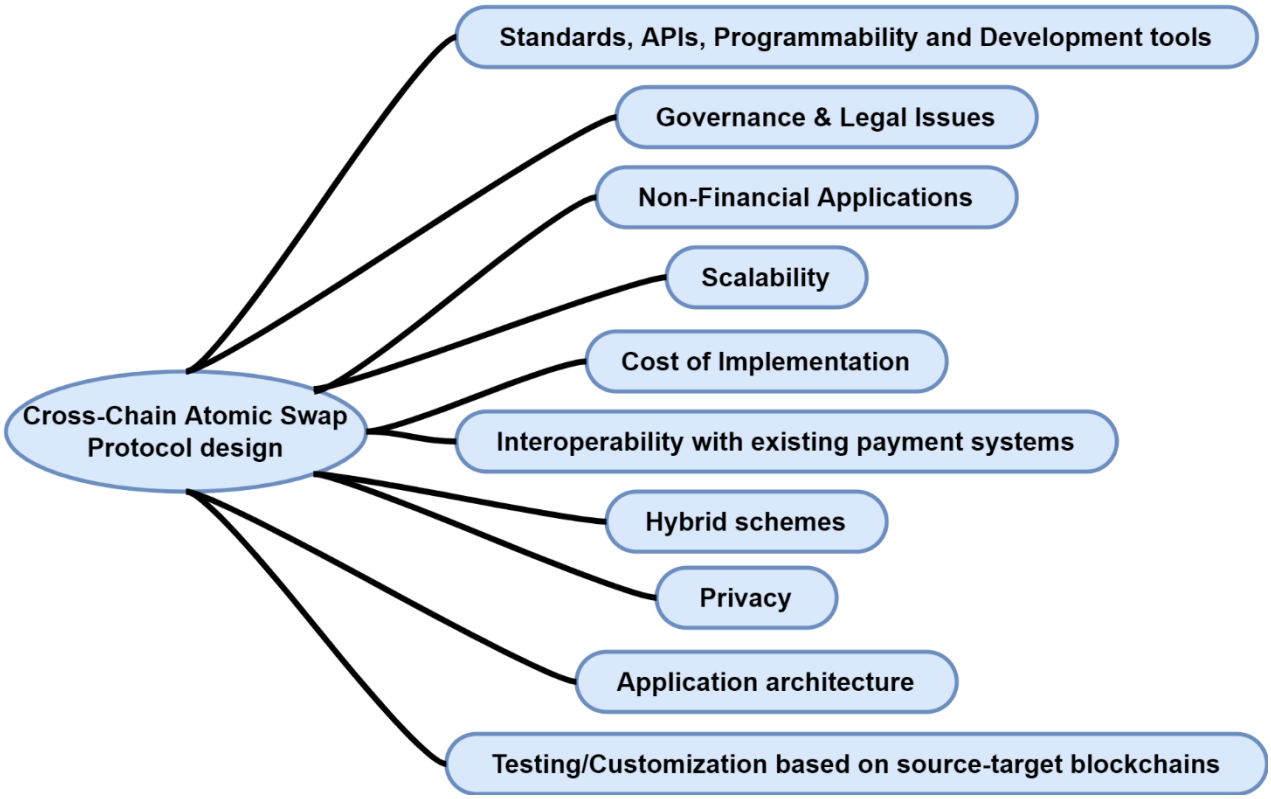

Figure 6. Cross-chain atomic swap protocol design research issues.

4.3. Practical Implication

Most blockchain platforms support programming, so they can be used to implement atomic-swap protocols using smart contracts. As we have discussed, implementing the swap protocol in layer 2 has advantages in terms of programmability. One striking feature of distributed-ledger technology is immutability, but this property has affected the privacy of the atomic swap protocols. Most protocols have not addressed the privacy and anonymity of a swap. The execution of transactions off-chain preserves the privacy of transactions, as used in two of the protocols. The atomic swap protocols discussed have a common limitation, as they require a specific party who wants to exchange the cryptocurrency. To achieve wide adaptability, it is essential to develop applications that are interoperable across different blockchain platforms. This requires the development of standards, APIs, and better development tools, which will make the development of methods for cross-chain application easy. Cross-chain interoperability also requires better modeling in terms of layered application architecture. Lastly, there is a need for better cross-chain applications, catering to financial, banking, transportation, and other potential sectors with a specific protocol development tailored to the corresponding industry. Atomic-swap protocols need to be validated with specific source-target cryptocurrency exchanges and should be customized accordingly. Furthermore, atomic swap protocols for specific source-target cryptocurrencies can be generalized and validated for other cryptocurrencies. By allowing tokens to be transferred swiftly and at a cheaper cost, without the use of a centralized authority, atomic swap will facilitate the development of a sustainable payment system for greater financial inclusion.

4.4. Limitations and Future Research

We investigated blockchain interoperability approaches and with a specific focus on interchain transactions. In this study, we reviewed only a few industrial blockchain interoperability projects and greater focus was directed to atomic-swap protocols. In this study,

we did not taken into account any change in the regulatory framework and government policy regarding blockchain technology and its applications.

We provided important suggestions in relation to the issues identified, as well as a discussion on the challenges of inter-chain swap. Discussions of shortcomings and future research directions on interchain atomic swap protocols are listed. Future research requires the vulnerability testing of existing interchain-swapping protocols. We expect the current review to provide valuable insight into the research directions of atomic cross-chain swaps, and that it will be helpful for researchers interested in blockchain interoperability.

Author Contributions: Conceptualization, D.A., D.M., H.M.A. and S.G.V.; formal analysis, D.A. and D.M.; investigation, D.M. and H.M.A.; resources, H.M.A.; writing—original draft preparation, D.A., D.M. and H.M.A.; writing—review and editing, D.A., D.M. and H.M.A.; validation S.G.V.; project administration S.G.V.; supervision, D.A., H.M.A. and S.G.V. All authors have read and agreed to the published version of the manuscript.

Funding: This project was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, under grant No. (D64-830-1443). The authors, therefore, gratefully acknowledge DSR technical and financial support.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This project was supported by the Deanship of Scientific Re-search (DSR), King Abdulaziz University, Jeddah, under grant No. (D64-830-1443). The authors, therefore, gratefully acknowledge DSR technical and financial support.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 26 December 2020).
2. Bodkhe, U.; Tanwar, S.; Parekh, K.; Khanpara, P.; Tyagi, S.; Kumar, N.; Alazab, M. Blockchain for Industry 4.0: A comprehensive review. *IEEE Access* **2020**, *8*, 79764–79800. [CrossRef]
3. Buterin, V. A Next Generation Smart Contract & Decentralized Application Platform. 2014. Available online: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (accessed on 6 January 2021).
4. About the Hyperledger Architecture Working Group. Hyperledger architecture. *Hyperledger. Org.* **2017**, *1*, 15.
5. Brown, R.G. The Corda Platform: An Introduction. 2018. Available online: https://www.corda.net/content/corda-platform-whitepaper.pdf (accessed on 6 January 2021).
6. Bitcoin Series 24: The Mega-Master Blockchain List—Ledra Capital. Available online: http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list (accessed on 6 January 2021).
7. Jin, H.; Xiao, J.; Dai, X. Towards A Novel Architecture for Enabling Interoperability Amongst Multiple Blockchains. In Proceedings of the 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), Vienna, Austria, 2–6 July 2018; pp. 1203–1211.
8. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. Blockchain Technology Overview. 2018. Available online: https://nvlpubs.nist.gov/nistpubs/ir/2018/nist.ir.8202.pdf (accessed on 7 January 2021).
9. Ellis, S.; Juels, A.; Nazarov, S. ChainLink A Decentralized Oracle Network. 2017. Available online: https://research.chain.link/whitepaper-v1.pdf (accessed on 6 January 2021).
10. Peterson, J.; Krug, J.; Zoltu, M.; Williams, A.K.; Alexander, S. Augur: A Decentralized Oracle and Prediction Market Platform (v2.0). 2018. Available online: https://arxiv.org/pdf/1501.01042.pdf (accessed on 6 May 2021).
11. Borkowski, M.; Mcdonald, D.; Ritzer, C.; Schulte, S. Towards Atomic Cross-Chain Token Transfers: State of the Art and Open Questions within TAST. 2018. Available online: https://dsg.tuwien.ac.at/projects/tast/pub/tast-white-paper-1.pdf (accessed on 6 March 2021).
12. Coinbase—Buy & Sell Bitcoin, Ethereum, and More with Trust. Available online: https://www.coinbase.com/ (accessed on 2 January 2021).
13. Crypto Exchange Bilaxy Loses $21M in Hack | PYMNTS.com. Available online: https://www.pymnts.com/cryptocurrency/2021/crypto-exchange-bilaxy-loses-21m-in-hack/ (accessed on 5 November 2021).

14. Number of Crypto Coins 2013-2021 | Statista. Available online: https://www.statista.com/statistics/863917/number-crypto-coins-tokens/ (accessed on 5 November 2021).
15. Decred Adds Atomic Swap Support for Exchange-Free Cryptocurrency Trading Nasdaq. Available online: https://www.nasdaq.com/articles/decred-adds-atomic-swap-support-for-exchange-free-cryptocurrency-trading-2017-09-20 (accessed on 5 November 2021).
16. GitHub-Decred/Atomicswap: On-Chain Atomic Swaps for Decred and Other Cryptocurrencies. Available online: https://github.com/decred/atomicswap (accessed on 5 November 2021).
17. First BTC-LTC Lightning Network Swap Completed, Huge Potential. Available online: https://cointelegraph.com/news/first-btc-ltc-lightning-network-swap-completed-huge-potential (accessed on 6 November 2021).
18. XMR. Developer Announces Bitcoin to Monero Atomic Swap Capabilities—Privacy Bitcoin News. Available online: https://news.bitcoin.com/xmr-developer-announces-bitcoin-to-monero-atomic-swap-capabilities/ (accessed on 6 November 2021).
19. COMIT. Network Launches Monero-Bitcoin Atomic Swaps on Mainnet-AMBCrypto. Available online: https://ambcrypto.com/comit-network-launches-monero-bitcoin-atomic-swaps-on-mainnet/ (accessed on 3 November 2021).
20. Liquality. Available online: https://liquality.io/ (accessed on 5 November 2021).
21. Belchior, R.; Vasconcelos, A.; Guerreiro, S.; Correia, M. A Survey on Blockchain Interoperability: Past, Present, and Future Trends. *ACM Comput. Surv.* **2020**, *54*, 1–41. [CrossRef]
22. Qasse, I.A.; Talib, M.A.; Nasir, Q. Inter Blockchain Communication: A Survey. In Proceedings of the ArabWIC 6th Annual International Conference Research Track, Rabat, Morocco, 7–9 March 2019. [CrossRef]
23. Robinson, P. Survey of crosschain communications protocols. *Comput. Netw.* **2021**, *200*, 108488. [CrossRef]
24. Wang, G. SoK: Exploring Blockchains Interoperability. *IACR Cryptol. Eprint Arch.* **2021**, *2021*, 537.
25. Back, A.; Corallo, M.; Dashjr, L.; Friedenbach, M.; Maxwell, G.; Miller, A.; Poelstra, A.; Timón, J.; Wuille, P. Enabling Blockchain Innovations with Pegged Sidechains. 2014. Available online: https://blockstream.com/sidechains.pdf (accessed on 6 January 2021).
26. Singh, A.; Click, K.; Parizi, R.M.; Zhang, Q.; Dehghantanha, A.; Choo, K.K.R. Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *J. Netw. Comput. Appl.* **2020**, *149*, 102471. [CrossRef]
27. GitHub-Ethereum/Btcrelay: Ethereum Contract for Bitcoin SPV: Live on. Available online: https://github.com/ethereum/btcrelay (accessed on 6 January 2021).
28. Loom Network—Production-Ready, Multichain Interop Platform for Serious Dapp Developers. Available online: https://loomx.io/ (accessed on 7 January 2021).
29. Elements | Elementsproject.org. Available online: https://elementsproject.org/ (accessed on 6 January 2021).
30. Liquid Network: Sidechain for Traders | Blockstream. Available online: https://blockstream.com/liquid/ (accessed on 17 January 2021).
31. Poelstra, A. Mimblewimble. 2016. Available online: https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.pdf (accessed on 16 January 2021).
32. Welcome to POA-POA. Available online: https://www.poa.network/ (accessed on 16 January 2021).
33. Lerner, S.D. RSK Rootstock Platform White Paper. 2019. Available online: https://www.rsk.co/Whitepapers/RSK-White-Paper-Updated.pdf (accessed on 17 March 2021).
34. Buy/Sell Bitcoin, Ether and Altcoins | Cryptocurrency Exchange | Binance. Available online: https://www.binance.com/en (accessed on 17 January 2021).
35. Bilaxy. Available online: https://bilaxy.com/ (accessed on 17 January 2021).
36. BitForex | The World's Leading One-Stop Digital Asset Service Platform. Available online: https://www.bitforex.com/ (accessed on 17 January 2021).
37. Buy Bitcoin, Cryptocurrency at India's Largest Exchange | Trading Platform | WazirX. Available online: https://wazirx.com/ (accessed on 17 January 2021).
38. Buy Bitcoin and Cryptocurrency at India's Leading Exchange | ZebPay. Available online: https://zebpay.com/in/ (accessed on 17 January 2021).
39. CoinDCX-Crypto Exchange | Buy, Sell and Trade Bitcoins & Top Altcoins. Available online: https://coindcx.com/ (accessed on 17 January 2021).
40. CoinSwitch Kuber-Cryptocurrency Exchange in India. Available online: https://coinswitch.co/ (accessed on 17 January 2021).
41. Wang, H.; Cen, Y.; Li, X. Blockchain Router: A Cross-Chain Communication Protocol. In Proceedings of the 6th International Conference on Informatics, Environment, Energy and Applications, New York, NY, USA, 29–31 March 2017; pp. 94–97.
42. Anlink Blockchain Network Whitepaper V 1.0. 2017. Available online: https://alicliimg.clewm.net/049/389/1389049/1484820492640c2baf37ea3e4f9fd77bd52c2a1e9bbbe1484820484.pdf (accessed on 17 January 2021).
43. Whitepaper-Resources-Cosmos Network. Available online: https://v1.cosmos.network/resources/whitepaper (accessed on 17 January 2021).
44. Wood, G. Polkadot: Vision For A Heterogeneous Multi-Chain Framework. 2016. Available online: https://polkadot.network/PolkaDotPaper.pdf (accessed on 17 January 2021).
45. Thomas, S.; Schwartz, E. A Protocol for Interledger Payments. 2015. Available online: https://interledger.org/interledger.pdf (accessed on 18 January 2021).
46. ARK Ecosystem Whitepaper Version 2.1.0. 2019. Available online: https://ark.io/Whitepaper.pdf (accessed on 20 January 2021).

47. Culwick, A.; Metcalf, D. The Blocknet Design Specification. 2018. Available online: https://blocknet.co/whitepaper/Blocknet_Whitepaper.pdf (accessed on 7 September 2021).
48. Aion Whitepaper-Whitepaper.io. Available online: https://whitepaper.io/document/31/aion-whitepaper (accessed on 26 January 2021).
49. Hash Time Locked Contracts-Bitcoin Wiki. Available online: https://en.bitcoin.it/wiki/Hash_Time_Locked_Contracts (accessed on 26 January 2021).
50. Poon, J.; Dryja, T. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. 2016. Available online: https://lightning.network/lightning-network-paper.pdf (accessed on 28 January 2021).
51. Nolan, T. Alt Chains and Atomic Transfers. Available online: https://bitcointalk.org/index.php?topic=193281.msg2224949#msg2224949 (accessed on 6 February 2021).
52. Herlihy, M. Atomic Cross-Chain Swaps. In Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing, New York, NY, USA, 23–27 July 2018; pp. 245–254.
53. Schulte, S.; Sigwart, M.; Frauenthaler, P.; Borkowski, M. Towards Blockchain Interoperability. In Proceedings of the 17th International Conference on Business Process Management: Blockchain and Central and Eastern Europe Forum, Wien, Österreich, 1–6 September 2019.
54. Zakhary, V.; Agrawal, D.; El Abbadi, A. Atomic commitment across blockchains. *Proc. VLDB Endow.* **2020**, *13*, 1319–1331. [CrossRef]
55. Zié, J.-Y.; Deneuville, J.-C.; Briffaut, J.; Nguyen, B. Extending Atomic Chain Swaps. ESORICS 2019, Data Privacy Management, Cryptocurrencies and Blockchain Technology. In Proceedings of the ESORICS 2019 International Workshops, DPM 2019 and CBT 2019, Luxembourg, 26–27 September 2019. [CrossRef]
56. Shadab, N.; Houshmand, F.; Lesani, M. Cross-chain Transactions. In Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2–6 May 2020. [CrossRef]
57. Zhao, D.; Li, T. Distributed Cross-Blockchain Transactions. *arXiv* **2020**, arXiv:2002.11771.
58. Borkowski, M.; Ritzer, C.; Mcdonald, D.; Schulte, S. Caught in Chains: Claim-First Transactions for Cross-Blockchain Asset Transfers. 2018. Available online: https://dsg.tuwien.ac.at/projects/tast/pub/tast-white-paper-2.pdf (accessed on 11 April 2021).
59. Liu, Z.; Xiang, Y.; Shi, J.; Gao, P.; Wang, H.; Xiao, X.; Wen, B.; Hu, Y.-C. HyperService: Interoperability and Programmability Across Heterogeneous Blockchains. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), London, UK, 11–15 November 2019; p. 18.
60. Borkowski, M.; Sigwart, M.; Frauenthaler, P.; Hukkinen, T.; Schulte, S. Dextt: Deterministic Cross-Blockchain Token Transfers. *IEEE Access* **2019**, *7*, 111030–111042. [CrossRef]
61. Dziembowski, S.; Eckey, L.; Faust, S. Fairswap: How to fairly exchange digital goods. In Proceedings of the ACM Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018; pp. 967–984.
62. Zero Knowledge Contingent Payment-Bitcoin Wiki. Available online: https://en.bitcoin.it/wiki/Zero_Knowledge_Contingent_Payment (accessed on 16 March 2021).
63. Bentov, I.; Kumaresan, R. How to use Bitcoin to design fair protocols. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8617, pp. 421–439.
64. Robinson, P.; Ramesh, R. General purpose atomic crosschain transactions. In Proceedings of the IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2021, Sydney, Australia, 3–6 May 2021.
65. Wüst, K.; Diana, L.; Kostiainen, K.; Karame, G.; Matetic, S.; Capkun, S. Bitcontracts: Supporting Smart Contracts in Legacy Blockchains. In Proceedings of the 2021 Network and Distributed System Security Symposium. Virtual: Internet Society, San Diego, CA, USA, 21–25 February 2021. [CrossRef]
66. Poelstra, A. Scriptless Scripts. 2017. Available online: https://download.wpsoftware.net/bitcoin/wizardry/mw-slides/2017-05-milan-meetup/slides.pdf (accessed on 16 March 2021).
67. Malavolta, G.; Moreno-Sanchez, P.; Schneidewind, C.; Kate, A.; Maffei, M. Anonymous Multi-Hop Locks for Blockchain Scalability and Interoperability. In Proceedings of the Network and Distributed Systems Security (NDSS) Symposium, San Diego, CA, USA, 24–27 February 2019.
68. Shlomovits, O.; Leiba, O. Jugglingswap: Scriptless Atomic Cross-Chain Swaps. *arXiv* **2020**, arXiv:2007.14423.
69. Deshpande, A.; Herlihy, M. Privacy-preserving cross-chain atomic swaps. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Berlin/Heidelberg, Germany, 2020; Volume 12063, pp. 540–549.
70. Gibson, A. Flipping the Scriptless Script on Schnorr—Joinmarket.me Archive. Available online: https://joinmarket.me/blog/blog/flipping-the-scriptless-script-on-schnorr/ (accessed on 6 May 2021).
71. Buterin, V. Chain Interoperability. 2016. Available online: https://www.r3.com/wp-content/uploads/2017/06/chain_interoperability_r3.pdf (accessed on 6 May 2021).
72. Lys, L.; Micoulet, A.; Potop-Butucaru, M. R-SWAP: Relay Based Atomic Cross-Chain Swap Protocol. In Proceedings of the 6th International Symposium, ALGOCLOUD 2021, Lisbon, Portugal, 6–7 September 2021; pp. 18–37. [CrossRef]
73. Frauenthaler, P.; Sigwart, M.; Spanring, C.; Schulte, S. Testimonium: A Cost-Efficient Blockchain Relay. 2020. Available online: https://arxiv.org/pdf/2002.12837.pdf (accessed on 18 August 2021).

74. Miraz, M.H.; Donald, D.C. Atomic Cross-chain Swaps: Development, Trajectory and Potential of Non-monetary Digital Token Swap Facilities. *Ann. Emerg. Technol. Comput.* **2019**, *3*, 42–50. [CrossRef]
75. Nissl, M.; Sallinger, E.; Schulte, S.; Borkowski, M. Towards Cross-Blockchain Smart Contracts. 2020. Available online: https://www.dsg.tuwien.ac.at/projects/tast/pub/tast-white-paper-10.pdf (accessed on 6 May 2021).
76. Fynn, E.; Bessani, A.; Pedone, F. Smart Contracts on the Move. In Proceedings of the 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), London, UK, 23–26 August 2021; pp. 233–244.
77. GitHub-Hyperledger/Burrow. Available online: https://github.com/hyperledger/burrow (accessed on 6 May 2021).
78. Qiu, H.; Wu, X.; Zhang, S.; Leung, V.C.M.; Cai, W. ChainIDE: A cloud-based integrated development environment for cross-blockchain smart contracts. In Proceedings of the International Conference on Cloud Computing Technology and Science (CloudCom), Sydney, Australia, 11–13 December 2019; pp. 317–319.
79. Drescher, D. Thinking in Layers and Aspects. In *Blockchain Basics*; Apress: New York, NY, USA, 2017; pp. 3–7.
80. Understanding Blockchain is Way Easier if You Think of It as an Onion. Available online: https://thenextweb.com/news/understanding-blockchain-easier-onion-layer (accessed on 6 May 2021).
81. Layer 2 Blockchain Technology: Everything You Need to Know | Lucidity. Available online: https://golucidity.com/layer-2-blockchain-technology/ (accessed on 6 May 2021).
82. Gudgeon, L.; Moreno-Sanchez, P.; Roos, S.; Mccorry, P.; Gervais, A. SoK: Layer-Two Blockchain Protocols. In *International Conference on Financial Cryptography and Data Security*; Springer: Cham, Switzerland, 2020; Volume 12059, pp. 201–226. [CrossRef]
83. Robinson, P.; Ramesh, R. Layer 2 Atomic Cross-Blockchain Function Calls. 2020. Available online: https://arxiv.org/pdf/2005.09790.pdf (accessed on 6 May 2021).
84. Pillai, B.; Biswas, K.; Muthukkumarasamy, V. Cross-chain interoperability among blockchain-based systems using transactions. *Knowl. Eng. Rev.* **2020**, *35*, 35. [CrossRef]
85. Gugger, J. Bitcoin-Monero Cross-chain Atomic Swap. *IACR Cryptol. ePrint Arch.* **2020**, *2020*, 1126.
86. Hoenisch, P.; Soriano Del Pino, L. Atomic Swaps between Bitcoin and Monero. *arXiv* **2021**, arXiv:2101.12332.
87. Mechkaroska, D.; Dimitrova, V.; Popovska-Mitrovikj, A. Analysis of the Possibilities for Improvement of BlockChain Technology. In Proceedings of the 2018 26th Telecommunications Forum, Belgrade, Serbia, 20–21 November 2018.
88. Decker, C.; Wattenhofer, R. A fast and scalable payment network with bitcoin duplex micropayment channels. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Berlin/Heidelberg, Germany, 2015; Volume 9212, pp. 3–18.
89. Brekke, J.K.; Alsindi, W.Z. Cryptoeconomics. *Internet Policy Rev.* **2021**, *10*, 1–9. [CrossRef]
90. Kim, M.S.; Chung, J.Y. Sustainable Growth and Token Economy Design: The Case of Steemit. *Sustainability* **2018**, *11*, 167. [CrossRef]