big data and cognitive computing

MDPI

Article

Proposal of Decentralized P2P Service Model for Transfer between Blockchain-Based Heterogeneous Cryptocurrencies and CBDCs

Keundug Park [1] and Heung-Youl Youm [2,*]

[1] AI&Blockchain Research Center, Seoul University of Foreign Studies, Seoul 60745, Republic of Korea
[2] Department of Information Security Engineering, Soonchunhyang University, Asan 31538, Republic of Korea
* Correspondence: hyyoum@sch.ac.kr

Abstract: This paper proposes a solution to the transfer problem between blockchain-based heterogeneous cryptocurrencies and CBDCs, with research derived from an analysis of the existing literature. Interoperability between heterogeneous blockchains has been an obstacle to service diversity and user convenience. Many types of cryptocurrencies are currently trading on the market, and many countries are researching and testing central bank digital currencies (CBDCs). In this paper, existing interoperability studies and solutions between heterogeneous blockchains and differences from the proposed service model are described. To enhance digital financial services and improve user convenience, transfer between heterogeneous cryptocurrencies, transfer between heterogeneous CBDCs, and transfer between cryptocurrency and CBDC should be required. This paper proposes an interoperable architecture between heterogeneous blockchains, and a decentralized peer-to-peer (P2P) service model based on the interoperable architecture for transferring between blockchain-based heterogeneous cryptocurrencies and CBDCs. Security threats to the proposed service model are identified and security requirements to prevent the identified security threats are specified. The mentioned security threats and security requirements should be considered when implementing the proposed service model.

Keywords: blockchain; cryptocurrency; central bank digital currency; virtual asset; transfer; payment; blockchain interoperability; decentralized finance

Citation: Park, K.; Youm, H.-Y. Proposal of Decentralized P2P Service Model for Transfer between Blockchain-Based Heterogeneous Cryptocurrencies and CBDCs. *Big Data Cogn. Comput.* **2022**, *6*, 159. https://doi.org/10.3390/bdcc6040159

Academic Editors: Peter R.J. Trim, Yang-Im Lee and Min Chen

Received: 7 November 2022
Accepted: 15 December 2022
Published: 19 December 2022

1. Introduction

About ten thousand cryptocurrencies are being traded on cryptocurrency exchanges [1], and about one hundred countries are exploring central bank digital currencies (CBDCs) in one form or another. For example, some countries are researching, some are testing, and some have already distributed CBDCs to the public [2–4]. To enhance digital financial services and improve user convenience, transfer between heterogeneous cryptocurrencies, transfer between heterogeneous CBDCs, and further transfer between cryptocurrency and CBDC should be required.

However, due to the lack of interoperability between heterogeneous blockchains, there is a problem related to the transfer between blockchain-based heterogeneous cryptocurrencies (e.g., Bitcoin [5], Ether [6], etc.) and CBDCs (e.g., US CBDC, UK CDBC, Korean CBDC, Chinese CBDC, etc.). For example, it is difficult to transfer between a Bitcoin wallet and an Ether wallet, between a US CBDC wallet and a Korean CBDC wallet, or between a Bitcoin wallet and a US CBDC wallet. Existing studies to address the lack of interoperability between heterogeneous blockchains have progressed towards centralized architectures where intermediaries handle ledger data sharing between blockchains. The sharing of ledger data that records the transaction history of cryptocurrencies and CBDCs is an essential operation for the interoperability between heterogeneous blockchains.

This paper proposes a decentralized peer-to-peer (P2P) service model for transferring between blockchain-based heterogeneous cryptocurrencies and CBDCs. The proposed service model provides a solution for transferring between blockchain-based heterogeneous cryptocurrencies and CBDCs without centralized intermediaries, such as cryptocurrency exchanges, banks, transfer service providers, and so on.

The contribution of this paper is as follows: to the best of our knowledge, there has been no previous study on a decentralized P2P service model for transferring between blockchain-based heterogeneous cryptocurrencies and CBDCs, and the proposed service model, based on an interoperable architecture that shares ledger data without intermediaries between heterogeneous blockchains, provides a solution for transferring between blockchain-based heterogeneous cryptocurrencies and CBDCs. The proposed decentralized P2P service model improves user convenience and ledger data security compared to the existing centralized service model.

This paper is organized into the following sections. Section 1 introduces cryptocurrency market trends and CBDC-related activities. Section 2 proposes an interoperable architecture to share ledger data without intermediaries between heterogeneous blockchains. Section 3 describes related studies including a problem with the transfer between blockchain-based heterogeneous cryptocurrencies and CBDCs. Section 4 proposes a decentralized P2P transfer service model to solve the problem identified in Section 3. Section 5 identifies security threats to the proposed service model and specifies security requirements to counter those security threats. Section 6 discusses the results and concludes the paper.

2. Interoperable Architecture between Heterogeneous Blockchains

This section proposes an interoperable architecture to share ledger data without intermediaries between heterogeneous blockchains. Interoperability between heterogeneous blockchains should be required to transfer between blockchain-based heterogeneous cryptocurrencies and CBDCs.

The proposed interoperable architecture is based on the proposed service model in Section 4 for sharing ledger data between heterogeneous blockchains. The proposed interoperable architecture is a decentralized architecture without intermediaries, whereas existing interoperable architectures, such as the inter-blockchain communication (IBC) protocol and the heterogeneous multi-chain framework described in Section 3.2, are centralized architectures with intermediaries.

In Figure 1, the blockchain-based interoperable management system (BIMS) maintains the registered information of blockchains and distributes common operations (COPs) to the contact nodes running on the blockchains. The BIMS does not store and maintain the ledger data from blockchain-1 and blockchain-2. Blockchain-1 and blockchain-2 can directly share ledger structure and ledger data through contact node-1 and contact node-2. The registered information of the blockchains includes the names of the blockchains, names of the consensus algorithms, names of the cryptocurrencies, IP addresses of the contact nodes, and more. The contact nodes running on the heterogeneous blockchains share data between the heterogeneous blockchains by common operations.

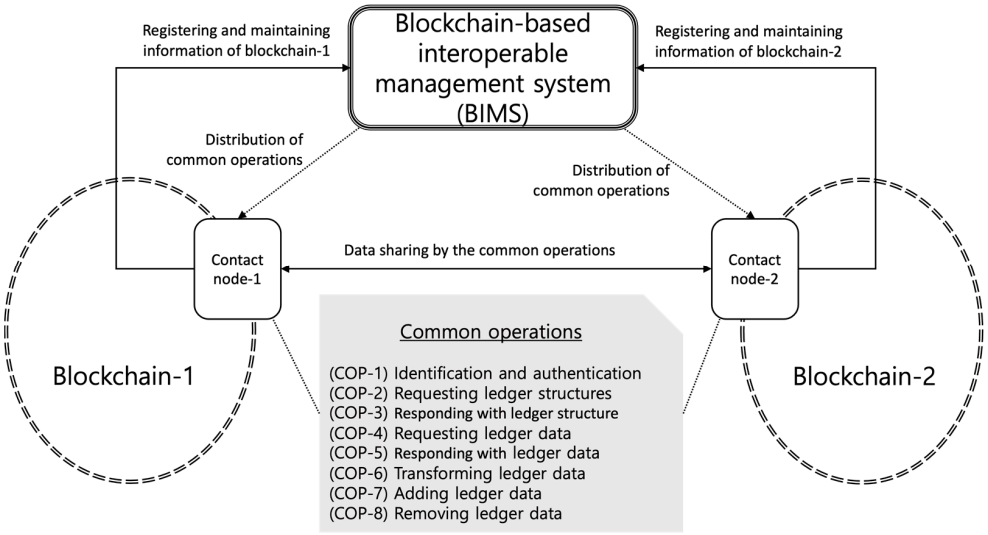

Figure 1. The interoperable architecture between heterogeneous blockchains.

The common operations are described as follows:

- (COP-1) Identification and authentication: operation for mutual identification and authentication between heterogeneous blockchains;
- (COP-2) Requesting ledger structures: operation to request the ledger structures of other blockchains;
- (COP-3) Responding with ledger structure: operation to provide the ledger structure of one's own blockchain in response to operation '(COP-2) Requesting ledger structures';
- (COP-4) Requesting ledger data: operation to request ledger data from other blockchains;
- (COP-5) Responding with ledger data: operation to provide the ledger data of one's own blockchain in response to operation '(COP-4) Requesting ledger data';
- (COP-6) Transforming ledger data: operation of converting (e.g., processing, combining, etc.) ledger data provided from other blockchains according to the ledger structure and data format of one's own blockchain;
- (COP-7) Adding ledger data: operation to add the data converted (e.g., processed, combined, etc.) by operation '(COP-6) Transforming ledger data' to the ledger of one's own blockchain;
- (COP-8) Removing ledger data: operation to delete ledger data provided from other blockchains.

In Figure 2, the ledger data sharing process based on the interoperable architecture between heterogeneous blockchains is described as follows:

1. Contact node-1 and contact node-2 register the information (e.g., the names of blockchains, names of the consensus algorithms, names of the cryptocurrencies, the IP addresses of the contact nodes, etc.) of blockchain-1 and blockchain-2 with the BIMS;
2. BIMS distributes the common operations to contact node-1 and contact node-2;
3. Contact node-1 and contact node-2 identify and authenticate each other by COP-1;
4. Contact node-1 requests contact node-2 for the ledger structure of blockchain-2 by the COP-2;
5. Blockchain-2 provides its own ledger structure to contact node-2;
6. Contact node-2 responds to contact node-1 with the ledger structure of blockchain-2 by COP-3;
7. Contact node-1 requests contact node-2 for the ledger data of blockchain-2 by COP-4;
8. Blockchain-2 provides its own ledger data to contact node-2;
9. Contact node-2 responds to contact node-1 with the ledger data of blockchain-2 by COP-5;

10. Contact node-1 transforms the ledger data of blockchain-2 by COP-6, and then contact node-1 stores the transformed ledger data to blockchain-1 by COP-7. Contact node-1 removes the transformed ledger data and the ledger data of blockchain-2 by COP-8.

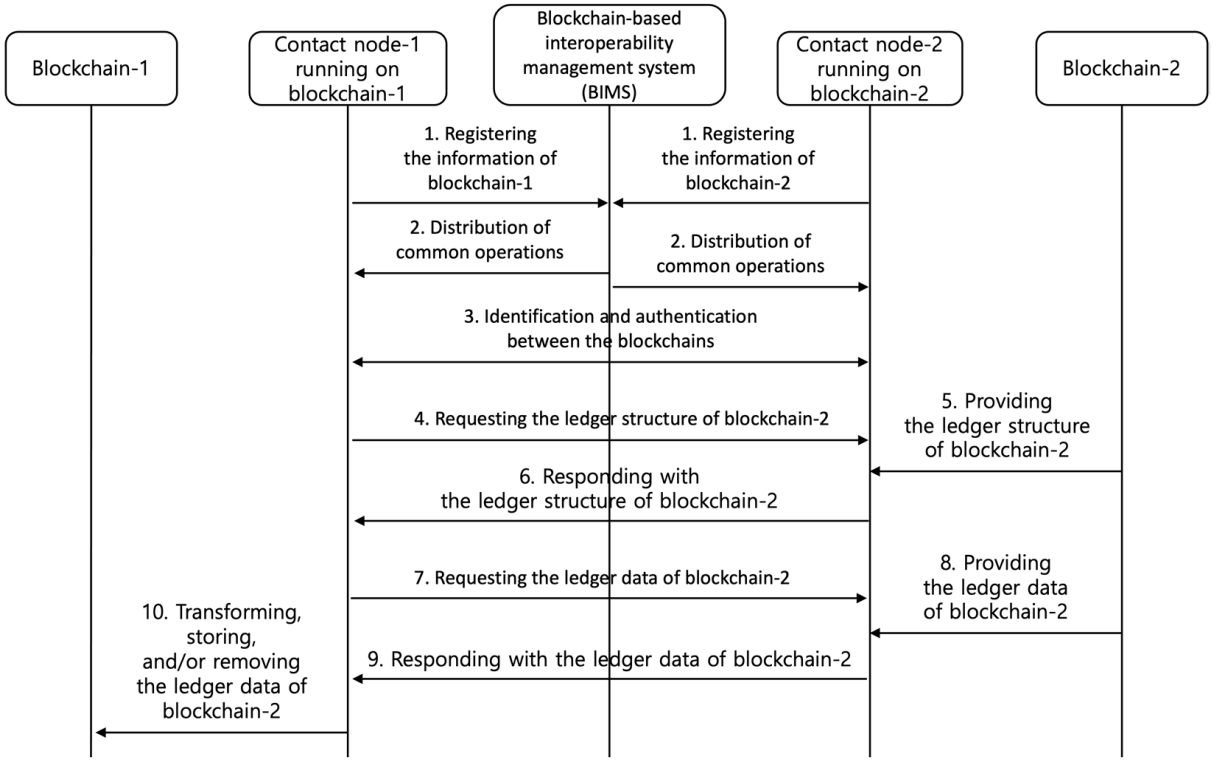

Figure 2. The ledger data sharing process based on the interoperable architecture between heterogeneous blockchains.

3. Related Studies

This section describes the problem with the transfer between blockchain-based heterogeneous cryptocurrencies and CBDCs and examines other studies related to the problem.

3.1. Problem with the Transfer between Blockchain-Based Heterogeneous Cryptocurrencies and CBDCs

It is easy for users to transfer cryptocurrencies within the same blockchain (e.g., Bitcoin blockchain [7], etc.). For example, when an originator with a Bitcoin wallet wants to transfer to a beneficiary with a Bitcoin wallet, the originator can easily transfer Bitcoins to the beneficiary using the beneficiary's wallet addresses within the Bitcoin blockchain.

However, it is difficult for users to transfer cryptocurrencies between heterogeneous blockchains (e.g., a transfer between Bitcoin blockchain and Ethereum, etc.). For example, when an originator with a Bitcoin wallet wants to transfer to a beneficiary with an Ether wallet, the originator cannot transfer Bitcoins to the beneficiary using the beneficiary's wallet addresses within the Ethereum. This problem is due to the lack of interoperability between heterogeneous blockchains. Due to the nature of blockchain, transfer between blockchain-based heterogeneous CBDCs has the same problem as cryptocurrency. Additionally, transfer between blockchain-based cryptocurrencies and CBDCs encounters the same problem.

3.2. Other Approaches for the Transfer between Blockchain-Based Heterogeneous Cryptocurrencies and CBDCs

Several organizations and studies have made proposals to solve the problem mentioned in Section 3.1, but their proposals differ from the proposed service model in terms of concept and concreteness.

The inter-blockchain communication (IBC) protocol is proposed in [8]. The Cosmos is a network of independent parallel blockchains with a Tendermint [9] consensus algorithm, such as the practical byzantine fault tolerance (PBFT [10]) consensus algorithm. The Cosmos Hub will be the first blockchain in the Cosmos network. Many other blockchains are connected by the Cosmos Hub using the IBC protocol. The Cosmos Hub can track many token types and record the total number of tokens for each connected blockchain. All inter-blockchain coin transfers go through the Cosmos Hub, allowing tokens to be transferred from one blockchain to another without a liquid exchange between blockchains. The Cosmos Hub is an intermediary that connects heterogeneous blockchains.

The heterogeneous multi-chain framework Polkadot is proposed in [11]. Polkadot is a sharded blockchain, meaning it connects several blockchains together in a single network, allowing them to process transactions in parallel and exchange data between blockchains [12]. Polkadot allows any type of data to be sent between any type of blockchains [12]. Polkadot is an intermediary connecting heterogeneous blockchains, which is very similar to the Cosmos Hub.

The hub-and-spoke payment route called universal payment channels (UPC) is proposed in [13]. UPC can be used to support digital currency transfers of funds across different networks through payment channels. UPC hub can be useful in the context of CBDCs to support cross-border payment flows between CBDCs that may run on different blockchains [13]. UPC hub can also play an important role between private stablecoins [14] and public CBDCs by providing permissioned access for whitelisted stablecoins to be interoperable with CBDCs. The UPC hub concept that emerged would connect different blockchains by establishing dedicated payment channels between them—whether that means connecting CBDC blockchains between countries or connecting CBDC blockchains with vetted private stablecoin blockchains [15]. UPC hub is an intermediary that connects heterogeneous blockchains for CBDCs and stablecoins.

The blockchain implementation method for interoperability between CBDCs is proposed in [16]. This paper focuses on a blockchain system and management method, based on the ISO/IEC 11179 metadata registries (MDR) [17], for exchanges between CBDCs that records transactions between registered CBDCs. Furthermore, this paper describes implementing the blockchain system and experiment with the operation method, measuring the block generation time of blockchains using the proposed method.

The blockchain interoperability towards a sustainable payment system is proposed in [18]. This paper investigates different blockchain interoperability approaches, including industrial solutions, categorizing them, identifying the key mechanisms used, and listing several example projects for each category. As examples of the underlying technologies for cross-blockchain transactions, this paper describes the notary schemes such as centralized cryptocurrency exchanges (e.g., Coinbase [19], Binance [20], etc.), the sidechain-based solutions, the blockchain routers, the hashed time locks, and the industrial solutions (e.g., Cosmos Hub [8], Polkadot [11], etc.).

The formation and development of Von Hayek's theory of private money is analyzed in [21]. This paper concludes that when the national currency is replaced by digital currency, due to the international nature of digital currencies, both developing and developed economies will be vulnerable to 'digital dollarisation'. Moreover, this paper describes how governments can ask central banks to use a CBDC, which is preferable to a national currency for forecasting, computation, and accounting.

The main objective of this paper is to propose an interoperable architecture between heterogeneous blockchains without intermediaries, and a new decentralized P2P transfer service model based on the proposed interoperable architecture between blockchain-based heterogeneous cryptocurrencies and CBDCs.

4. Decentralized P2P Transfer Service Model and the Service Scenarios

This section proposes a decentralized P2P service model based on an interoperable architecture for transferring between blockchain-based heterogeneous cryptocurrencies and CBDCs to solve the transfer problem mentioned in Section 3.1.

4.1. Service Model

The decentralized P2P service model, based on the interoperable architecture for transferring between blockchain-based heterogeneous cryptocurrencies and CBDCs, includes transfer between cryptocurrencies, transfer between cryptocurrency and CBDC, and transfer between CBDCs. In the proposed service model, the transfer agent is an entity that receives cryptocurrency and CBDC from the originator and sends another cryptocurrency and CBDC to the beneficiary. Any entity can be a candidate for the transfer agent.

In Figure 3, cryptocurrency-1 (e.g., Bitcoin) is transferred from the originator's wallet to the transfer agent's wallet-1 on blockchain-1. Contact node-1, running on blockchain-1, directly provides the ledger data for the transfer of cryptocurrency-1 to contact node-2, running on blockchain-2, without any intermediaries (see Figure 2). Cryptocurrency-2 (e.g., Ether) is transferred from the transfer agent's wallet-2 to the beneficiary's wallet on blockchain-2.

In Figure 4, cryptocurrency-1 (e.g., Bitcoin) is transferred from the originator's wallet to the transfer agent's wallet-1 on blockchain-1. Contact node-1, running on blockchain-1, directly provides the ledger data for the transfer of cryptocurrency-1 to contact node-2, running on blockchain-2, without any intermediaries (see Figure 2). CBDC-1 (e.g., Korean CBDC) is transferred from the transfer agent's wallet-2 to the beneficiary's wallet on blockchain-2.

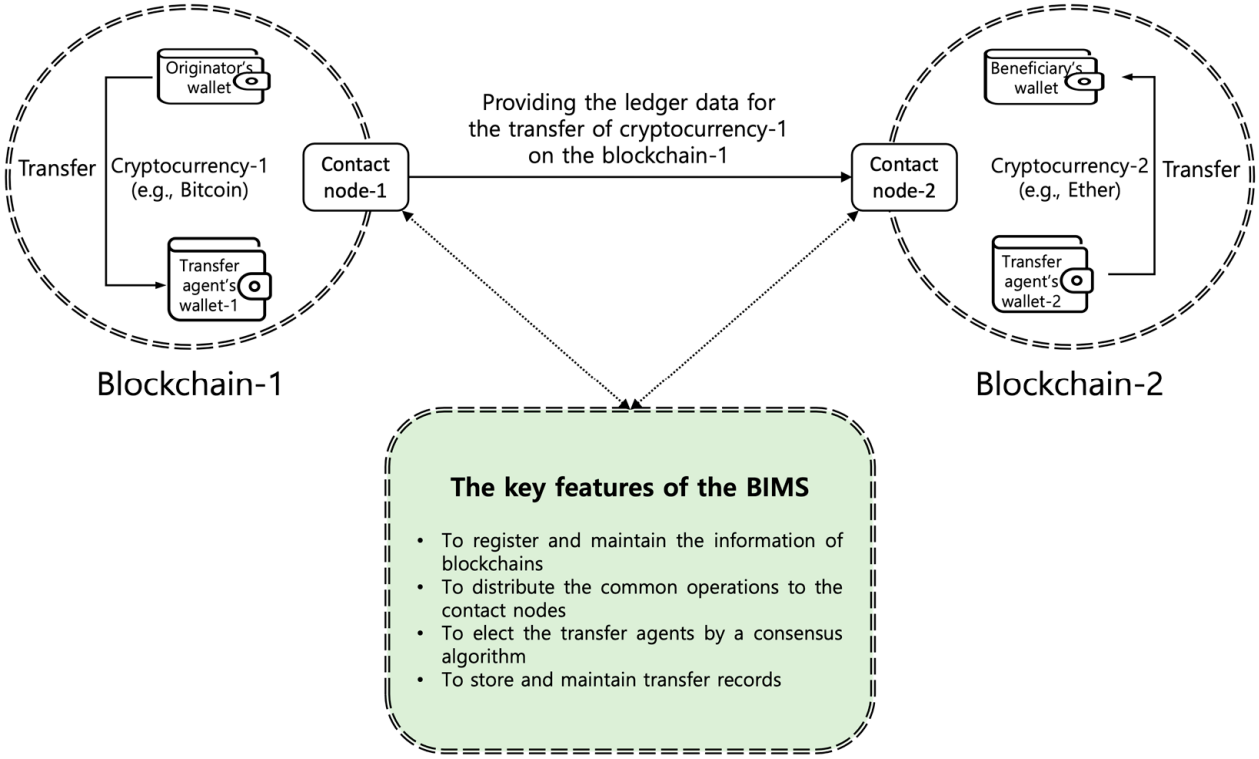

Figure 3. The service model for the transfer between cryptocurrency-1 and cryptocurrency-2.

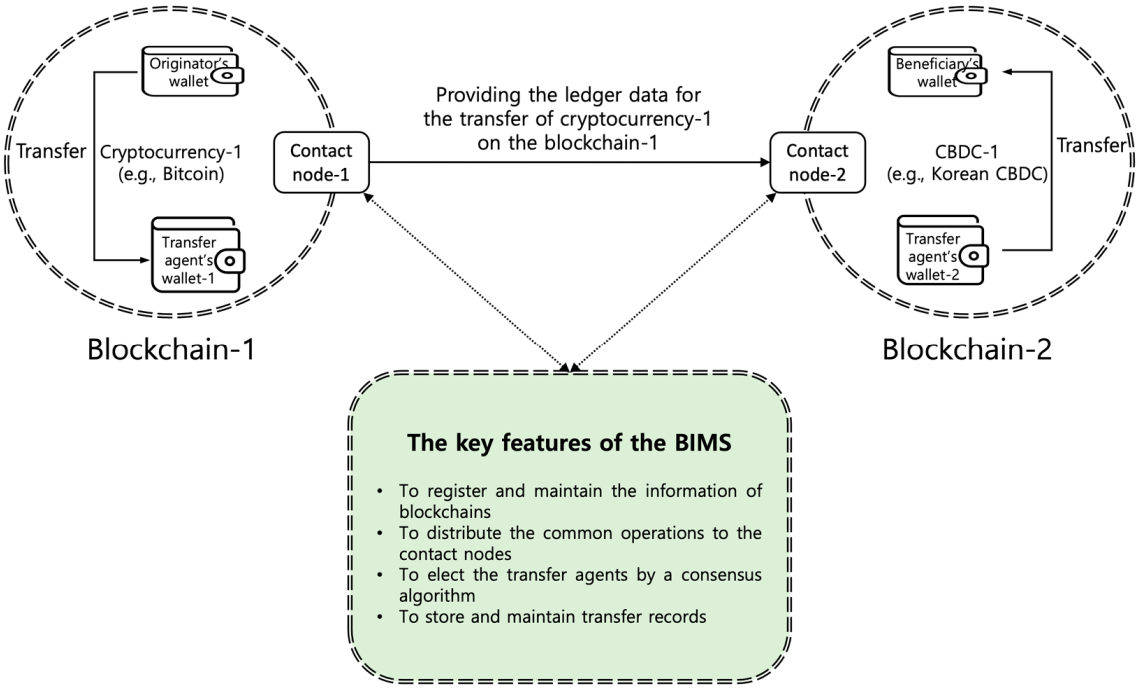

Figure 4. The service model for the transfer between cryptocurrency-1 and CBDC-1.

In Figure 5, CBDC-1 (e.g., Korean CBDC) is transferred from the originator's wallet to the transfer agent's wallet-1 on blockchain-1. Contact node-1, running on blockchain-1, directly provides the ledger data for the transfer of CBDC-1 to contact node-2, running on blockchain-2, without any intermediaries (see Figure 2). CBDC-2 (e.g., US CBDC) is transferred from the transfer agent's wallet-2 to the beneficiary's wallet on blockchain-2.

The key features of BIMS are included in Figures 3–5. BIMS registers and maintains the information of the blockchains (e.g., the names of the blockchains, names of the consensus algorithms, names of the cryptocurrencies, IP addresses of the contact nodes, etc.), and distributes common operations (COPs) to the contact nodes running on the registered blockchains. The transfer agents are elected by a consensus algorithm. The transfer records are stored and maintained.

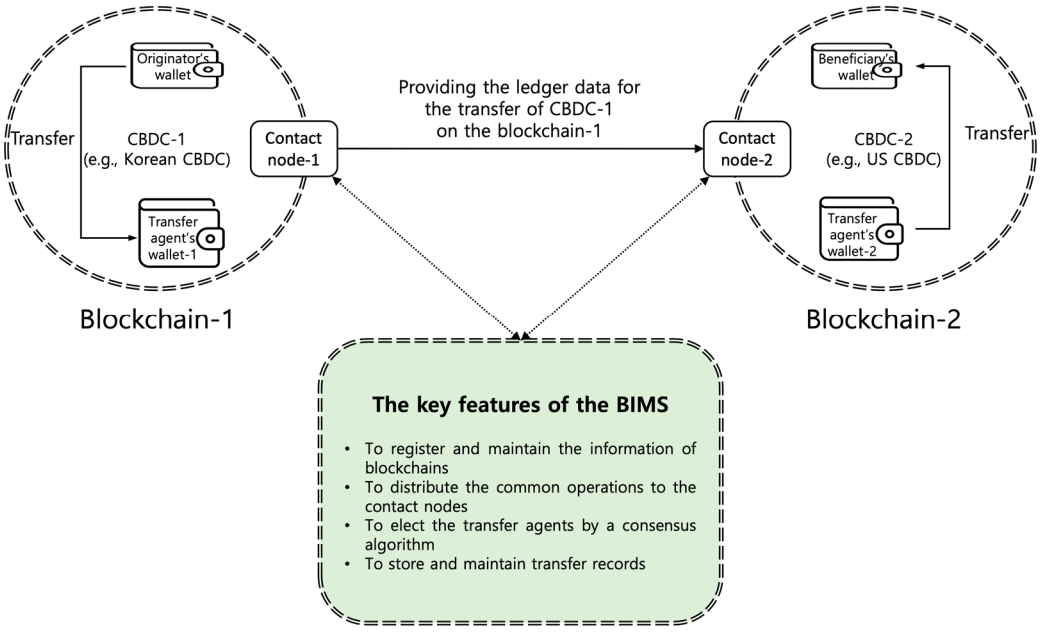

Figure 5. The service model for the transfer between CBDC-1 and CBDC-2.

4.2. Service Scenarios and Data Flow

The service scenarios include the transfer between cryptocurrency-1 and cryptocurrency-2, the transfer between cryptocurrency-1 and CBDC-1, and the transfer between CBDC-1 and CBDC-2. The service scenario for the transfer between cryptocurrency-1 and CBDC-1 and the service scenario for the transfer between CBDC-1 and CBDC-2 are very similar to the service scenario for the transfer between cryptocurrency-1 and cryptocurrency-2.

In Figure 6, the service scenario for the transfer between the cryptocurrency-1 and cryptocurrency-2 is describes as follows:

1. BIMS elects transfer agents with wallets on blockchain-1 and blockchain-2 by a consensus algorithm;
2. Cryptocurrency-1 is transferred from the originator's wallet to the transfer agent's wallet on blockchain-1. In the transfer between CBDC-1 and CBDC-2, CBDC-1 is transferred from the originator's wallet to the transfer agent's wallet on blockchain-1. This process is performed by the originator;
3. The ledger for the cryptocurrency-1 transfer from the originator's wallet to the transfer agent's wallet is stored in the blockchain-1. The ledger data include the transfer date, the originator's wallet address, the transfer agent's wallet address, cryptocurrency-1 amount, and the fee amount for blockchain-1. In the transfer between CBDC-1 and CBDC-2, the ledger for the CBDC-1 transfer from the originator's wallet to the transfer agent's wallet is stored in blockchain-1. The ledger data include the transfer date, the originator's wallet address, the transfer agent's wallet address, CBDC-1 amount, and the fee amount for blockchain-1;
4. The record for the cryptocurrency-1 transfer from the originator's wallet to the transfer agent's wallet is stored in BIMS. Examples of the record data include the transfer date, the originator's wallet address, the beneficiary's wallet address, the amount of cryptocurrency-1, the fee amount for blockchain-1, and the fee amount for the transfer agent of blockchain-1. In the transfer between CBDC-1 and CBDC-2, the record for the CBDC-1 transfer from the originator's wallet to the transfer agent's wallet is stored in BIMS. Examples of the record data include the transfer date, the originator's wallet address, the beneficiary's wallet address, the amount of CBDC-1, the fee amount for blockchain-1, and the fee amount for the transfer agent of blockchain-1;
5. Contact node-1, running on blockchain-1, directly provides the ledger data to contact node-2, running on blockchain-2, without any intermediaries. The ledger data are for the cryptocurrency-1 transfer from the originator's wallet to the transfer agent's wallet on blockchain-1. In the transfer between CBDC-1 and CBDC-2, the ledger data are for the CBDC-1 transfer from the originator's wallet to the transfer agent's wallet on blockchain-1;
6. Cryptocurrency-2 equal to the amount of cryptocurrency-1 is transferred from the transfer agent's wallet to the beneficiary's wallet on blockchain-2. In the transfer between CBDC-1 and CBDC-2, CBDC-2 equal to the amount of CBDC-1 is transferred from the transfer agent's wallet to the beneficiary's wallet on blockchain-2. In the transfer between cryptocurrency-1 and CBDC-1, CBDC-1 equal to the amount of cryptocurrency-1 is transferred from the transfer agent's wallet to the beneficiary's wallet on blockchain-2. This process is performed by the transfer agent or an application that can use the transfer agent's private key;
7. The ledger for the cryptocurrency-2 transfer from the transfer agent's wallet to the beneficiary's wallet is stored in blockchain-2. For example, the ledger data include the transfer date, the transfer agent's wallet address, the beneficiary's wallet address, the cryptocurrency-2 amount, and the fee amount for blockchain-2. In the transfer between CBDC-1 and CBDC-2, the ledger for the CBDC-2 transfer from the transfer agent's wallet to the beneficiary's wallet is stored in blockchain-2. Examples of ledger data include the transfer date, the transfer agent's wallet address, the beneficiary's wallet address, the CBDC-2 amount, and the fee amount for the blockchain-2. In the transfer between cryptocurrency-1 and CBDC-1, the ledger for the CBDC-1 transfer

from the transfer agent's wallet to the beneficiary's wallet is stored in blockchain-2. For example, the ledger data include the transfer date, the transfer agent's wallet address, the beneficiary's wallet address, the CBDC-1 amount, and the fee amount for the blockchain-2;

8. The record for the cryptocurrency-2 transfer from the transfer agent's wallet to the beneficiary's wallet is stored in BIMS. Examples of the record data include the transfer date, the transfer agent's wallet address, the beneficiary's wallet address, the cryptocurrency-2 amount, the fee amount for the blockchain-2, and the fee amount for the transfer agent of blockchain-2. In the transfer between CBDC-1 and CBDC-2, the record for the CBDC-2 transfer from the transfer agent's wallet to the beneficiary's wallet is stored in BIMS. Examples of the record data include the transfer date, the transfer agent's wallet address, the beneficiary's wallet address, the CBDC-2 amount, the fee amount for the blockchain-2, and the fee amount for the transfer agent of the blockchain-2. In the transfer between cryptocurrency-1 and CBDC-1, the record for the CBDC-1 transfer from the transfer agent's wallet to the beneficiary's wallet is stored in BIMS. Examples of the record data include the transfer date, the transfer agent's wallet address, the beneficiary's wallet address, the CBDC-1 amount, the fee amount for the blockchain-2, and the fee amount for the transfer agent of blockchain-2.

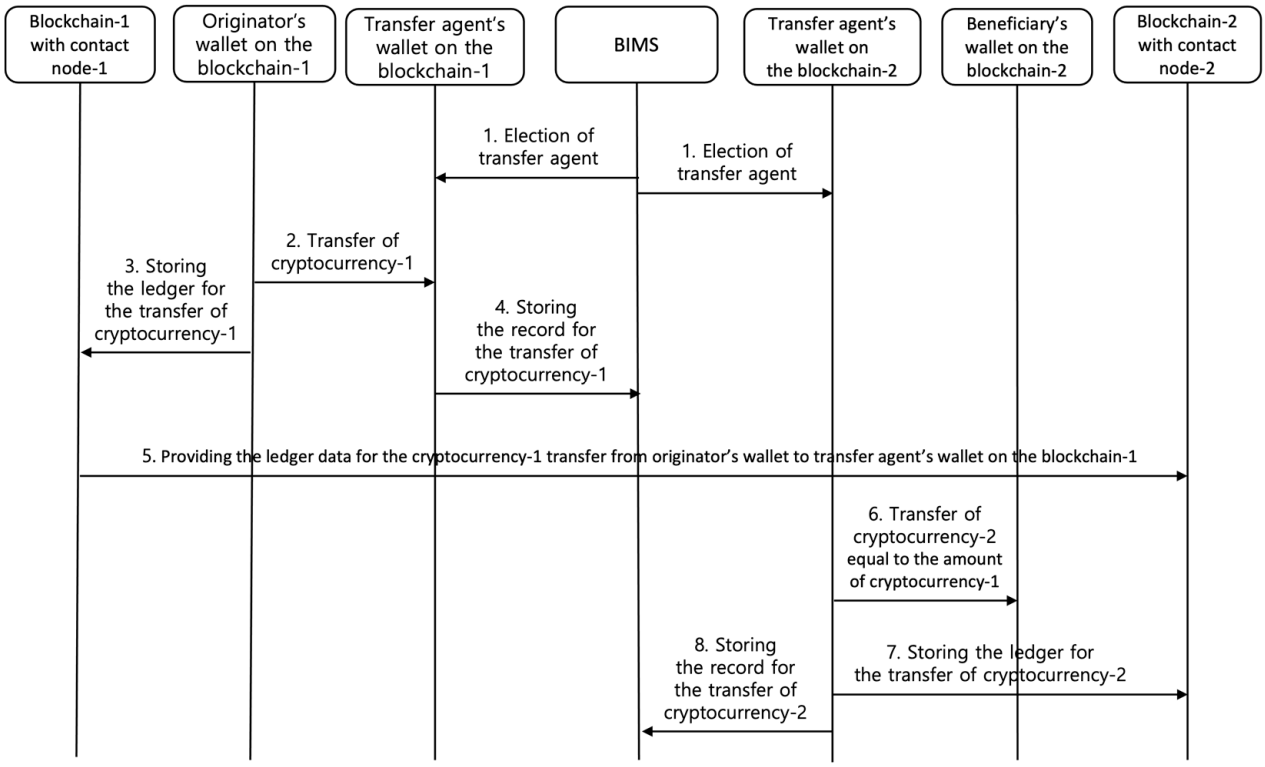

Figure 6. The service scenario for the transfer between the cryptocurrency-1 and cryptocurrency-2.

5. Security Threats and Requirements

Security threats (STs) to the proposed service model for the transfer between cryptocurrencies and CBDCs are identified and security requirements (SRs) countering the security threats are specified in this section.

5.1. Security Threats

Security threats to the proposed service model for the transfer between blockchain-based heterogeneous cryptocurrencies and CBDCs are identified as follows:

- (ST-1) Breach of contract by originator's transfer agents: If the originator's transfer agents and the beneficiary's transfer agents are not the same entity (for example, see

Figure 3), the originator's transfer agents may not pay the transfer amount excluding the transfer fee to the beneficiary's transfer agents. This threat may lead to the beneficiary's transfer agents not transferring the cryptocurrencies and CBDCs to the beneficiary. As a result, the transfer between cryptocurrencies and CBDCs will fail;

- (ST-2) Ledger data leakage during transmission between contact nodes: The ledger data can be leaked during transmission between the contact nodes running on heterogeneous blockchains. The leaked ledger data can be misused to steal cryptocurrencies and CBDCs;
- (ST-3) Massive ledger data leakage from blockchains: The massive ledger data can be leaked from blockchains registered with BIMS. The contact nodes running on blockchains which is registered with BIMS can request massive ledger data from the contact nodes running on other blockchains registered with BIMS. The leaked massive ledger data can be misused to track cryptocurrencies and CBDCs transfers. This threat can cause privacy issues related to the originators and beneficiaries;
- (ST-4) Monopoly by specific transfer agents: The transfer between cryptocurrencies and CBDCs can be monopolized by specific transfer agents. This threat can allow transfer agents that monopolize transfers to control transfers between cryptocurrencies and CBDCs. Ultimately, this threat can force the originators and beneficiaries to pay higher transfer fees;
- (ST-5) Data request by unauthorized blockchains: The contact nodes running on a blockchain which is not registered with BIMS can request ledger data from the contact nodes running on a blockchain registered with BIMS. The ledger data obtained from the blockchains registered with BIMS can be misused to steal cryptocurrencies and CBDCs.

The security threats are specific to the proposed service model for the transfer between cryptocurrencies and CBDCs, not to the general IT services.

5.2. Security Requirements

Security requirements countering the security threats identified in Section 5.1 are specified as follows:

- (SR-1) Stablecoin deposit: The proposed service model should allow the originator's transfer agents to deposit stablecoins equal to the amount of transfer prior to the transfer. As soon as the transfer from the originator's wallet to the transfer agent's wallet occurs, the stablecoins are automatically held in escrow by the smart contract [22,23] for the beneficiary's transfer agents. The smart contract runs on blockchains for stablecoins, such as Tether coin (USDT) on Ethereum;
- (SR-2) Data encryption in transmission: The proposed service model should provide safe cryptographic protocol (e.g., TLS) [24,25] to prevent ledger data leakage during transmission between the contact nodes running on heterogeneous blockchains. The ledger data should be protected with the cryptographic protocol in the transmission;
- (SR-3) Minimization of the amount of retrieved ledger data: The proposed service model should allow the contact nodes to minimize the amount of ledger data retrieved from the blockchains. More specifically, this can be implemented by narrowing the query conditions to seek ledger data;
- (SR-4) Election of transfer agents by a consensus algorithm: The proposed service model should elect the transfer agents by a consensus algorithm prior to the transfer. The elected originator's transfer agent and beneficiary's transfer agent may or may not be the same. Depending on the type of transfer (e.g., transfer between Bitcoin and Ether, transfer between Bitcoin and Korean CBDC, transfer between Korean CBDC and US CBDC, etc.), the transfer agents should be elected in consideration of the transfer agent's properties (e.g., wallet type, stablecoin deposit amount, transfer fee, etc.);
- (SR-5) Identification and authentication between the contact nodes: The proposed service model should provide an identification and authentication mechanism between

contact nodes. The contact nodes running on heterogeneous blockchains should identify and authenticate each other before sharing ledger data.

In Table 1, SR-1 (stablecoin deposit) can prevent ST-1 (breach of contract by originator's transfer agents). This means that if the originator's transfer agent does not pay the transfer amount, excluding the transfer fee to the beneficiary's transfer agent, the stablecoins deposited by the originator's transfer agent are automatically paid to the beneficiary's transfer agent by the smart contract. SR-2 (data encryption in transmission) can prevent ST-2 (ledger data leakage during transmission between contact nodes). This means that although the ledger data are leaked during transmission between the contact nodes running on heterogeneous blockchains, it is difficult to use the leaked ledger data encrypted with a cryptographic algorithm. SR-3 (minimization of the amount of retrieved ledger data) can prevent ST-3 (massive ledger data leakage from blockchains). This means that it is possible to prevent leakage of massive ledger data from blockchains by narrowing down the query conditions to seek ledger data in the contact nodes. SR-4 (election of transfer agents by a consensus algorithm) can prevent the ST-4 (monopoly by specific transfer agents). This means that the monopoly of specific transfer agents can be prevented by electing transfer agents based on the consensus algorithm for each transfer. SR-5 (identification and authentication between the contact nodes) can prevent ST-5 (data request by unauthorized blockchains). This means that the contact nodes running on blockchains which are not registered with BIMS cannot request ledger data from the contact nodes running on blockchains registered with BIMS, in accordance with the results of mutual authentication between contact nodes.

Table 1. Relationship between security threats and security requirements.

	SR-1 (Stablecoin Deposit)	**SR-2 (Data Encryption in Transmission)**	**SR-3 (Minimization of the Amount of Retrieved Ledger Data)**	**SR-4 (Election of Transfer Agents by a Consensus Algorithm)**	**SR-5 (Identification and Authentication between the Contact Nodes)**
ST-1 (breach of contract by originator's transfer agents)	O				
ST-2 (ledger data leakage during transmission between contact nodes)		O			
ST-3 (massive ledger data leakage from blockchains)			O		
ST-4 (monopoly by specific transfer agents)				O	
ST-5 (data request by unauthorized blockchains)					O

(Note: ST = security threat; SR = security requirement).

6. Discussion and Conclusions

The main objective of this paper is to propose an interoperable architecture between heterogeneous blockchains, and a new decentralized P2P service model for the transfer between blockchain-based heterogeneous cryptocurrencies and CBDCs. The experimental evaluation of the proposed service model could be done as future work.

This paper identifies potential security threats to the proposed service model and describes security requirements to prevent the identified security threats. The proposed service model should be implemented to meet the security requirements.

The interoperable architecture enables the exchange of transaction ledger data of cryptocurrency and CBDC without intermediaries between heterogeneous blockchains. This enables cryptocurrency and CBDC to be transferred by decentralized transfer agents, even if the originator's blockchain and the beneficiary's blockchain are different.

The service scenario in Figure 6 demonstrates that the transfer between an originator and a beneficiary with heterogeneous cryptocurrency and CBDC can be processed very conveniently and usefully. This is because the originator does not have to consider what the beneficiary's wallet type is. Thus, the proposed service model based on the proposed interoperable architecture solves the transfer problem between heterogeneous blockchain-based cryptocurrencies and CBDCs.

There are several advantages of the proposed service model: (1) The proposed interoperable architecture allows the sharing of ledger data between heterogeneous blockchains without intermediaries. (2) BIMS provides the common operations for sharing ledger data between the blockchains, rather than storing and maintaining the ledger data retrieved from the blockchains. (3) The proposed service model allows the transfer between cryptocurrencies, between cryptocurrency and CBDC, and between CBDCs without cryptocurrency exchanges and banks.

There are several reasons why BIMS service provider and transfer users would be interested in accepting the proposed service model: (1) The originator can directly transfer cryptocurrencies and CBDCs regardless of the beneficiary's wallet type. (2) The originator does not need to exchange the cryptocurrency and CBDC to be transferred for the same cryptocurrency and CBDC as the beneficiary's wallet type. (3) Transfer fees to be paid by the originators and beneficiaries are lower than the centralized organization, such as cryptocurrency exchanges, banks, transfer service providers and so on. (4) BIMS service providers are not burdened with storing and maintaining the ledger data retrieved from other blockchains for interoperability.

The proposed interoperable architecture will be developed as an international standard by ITU-T (International Telecommunication Unit) SG17, and the proposed service model will be developed as Korean ICT standard by TTA (Telecommunications Technology Association) PG1006. Private companies will be able to implement the proposed service model based on the interoperable architecture as a decentralized P2P transfer system by technology transfer in the future.

Author Contributions: Conceptualization, K.P.; methodology, K.P.; validation, K.P. and H.-Y.Y.; formal analysis, K.P.; investigation, K.P.; writing—original draft preparation, K.P.; writing—review and editing, K.P. and H.-Y.Y.; supervision, H.-Y.Y.; project administration, H.-Y.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This research was implemented as part of the project "Standardization Lab. for Next-generation Cybersecurity" (Project Number: 2021-0-00112) supported by MSIT (the Ministry of Science and ICT) and IITP (Institute of Information & Communications Technology Planning & Evaluation).

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

References

1. CoinMarketCap. Today's Cryptocurrency Prices by Market Cap. Available online: https://coinmarketcap.com (accessed on 20 October 2022).
2. International Monetary Fund (IMF). The Future of Money: Gearing up for Central Bank Digital Currency. Available online: https://www.imf.org/en/News/Articles/2022/02/09/sp020922-the-future-of-money-gearing-up-for-central-bank-digital-currency (accessed on 20 October 2022).
3. The Federal Reserve System. Money and Payments: The U.S. Dollar in the Age of Digital Transformation. Available online: https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf (accessed on 20 October 2022).
4. Zhang, T.; Huang, Z. Blockchain and central bank digital currency. *ICT Express* **2022**, *8*, 264–270. Available online: https://www.sciencedirect.com/science/article/pii/S2405959521001399 (accessed on 20 October 2022). [CrossRef]
5. Nakamoto, S. Bitcoin: A Peer-To-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 20 October 2022).
6. Ethereum. Ethereum White paper. Available online: https://ethereum.org/en/whitepaper/ (accessed on 20 October 2022).
7. Blockchain.com. Bitcoin Explorer. Available online: https://www.blockchain.com/explorer?view=btc (accessed on 22 October 2022).
8. Kwon, J.; Buchman, E. Cosmos Whitepaper. Available online: https://v1.cosmos.network/resources/whitepaper (accessed on 24 October 2022).
9. Tendermint. Tendermint Core Documentation. Available online: https://docs.tendermint.com (accessed on 24 October 2022).
10. Castro, M.; Liskov, B. Practical Byzantine Fault Tolerance. Available online: https://pmg.csail.mit.edu/papers/osdi99.pdf (accessed on 24 October 2022).
11. Wood, G. Polkadot: Vision for a Heterogeneous Multi-Chain Framework Draft 1. Available online: https://polkadot.network/PolkaDotPaper.pdf (accessed on 24 October 2022).
12. Wood, G. An Introduction to Polkadot. Available online: https://polkadot.network/Polkadot-lightpaper.pdf (accessed on 24 October 2022).
13. Christodorescu, M.; English, E.; Gu, W.C.; Kreissman, D.; Kumaresan, R.; Minaei, M.; Raghuraman, S.; Sheffield, C.; Wijeyekoon, A.; Zamani, M. Universal Payment Channels: An Interoperability Platform for Digital Currencies. Available online: https://arxiv.org/pdf/2109.12194v2.pdf (accessed on 24 October 2022).
14. Arner, D.; Auer, R.; Frost, J. Stablecoins: Risks, Potential and Regulation. Available online: https://www.bis.org/publ/work905.pdf (accessed on 24 October 2022).
15. Gu, C. Making Digital Currency Interoperable, Visa Shares New Thinking on Cross-Chain Interoperability. Available online: https://usa.visa.com/visa-everywhere/blog/bdp/2021/09/29/making-digital-currency-1632954547520.html (accessed on 24 October 2022).
16. Jung, H.; Jeong, D. Blockchain Implementation Method for Interoperability between CBDCs. *Future Internet* **2021**, *13*, 133. [CrossRef]
17. International Organization for Standardization (ISO). *ISO/IEC 11179-1:2015*; Information Technology—Metadata Registries (MDR)—Part 1: Framework. ISO: Geneva, Switzerland, 2015.
18. Mohanty, D.; Anand, D.; Aljahdali, H.M.; Villar, S.G. Blockchain Interoperability: Towards a Sustainable Payment System. *Sustainability* **2022**, *14*, 913. [CrossRef]
19. Coinbase. Coinbase—Buy & Sell Bitcoin, Ethereum, and More with Trust. Available online: https://www.coinbase.com/ (accessed on 26 October 2022).
20. Binance. Buy/Sell Bitcoin, Ether and Altcoins | Cryptocurrency Exchange | Binance. Available online: https://www.binance.com/en (accessed on 26 October 2022).
21. Mikhaylov, A.Y. Development of Friedrich von Hayek's theory of private money and economic implications for digital currencies. *Terra Econ.* **2021**, *19*, 1. [CrossRef]
22. 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. [CrossRef]
23. Negara, E.S.; Hidayanto, A.N.; Andryani, R.; Syaputra, R. Survey of Smart Contract Framework and Its Application. *Information* **2021**, *12*, 257. [CrossRef]
24. OpenSSL Software Foundation. Vulnerabilities. Available online: https://www.openssl.org/news/vulnerabilities.html (accessed on 5 November 2022).
25. Internet Engineering Task Force (IETF). The Transport Layer Security (TLS) Protocol Version 1.3. Available online: https://tools.ietf.org/html/rfc8446 (accessed on 5 November 2022).