Cross-chain Transaction Validation using Lock-and-Key Method for Multi-System Blockchain

Gaurav Kumar*, Samarthi Lahiri†, Amit Dua‡, Gagangeet Singh Aujla§
*Computer Science and Information Systems, BITS Pilani, Pilani, India
§Department of Computer Science, Durham University, UK
Emails: f20200145@pilani.bits-pilani.ac.in, h20210273@pilani.bits-pilani.ac.in, amit.dua@pilani.bits-pilani.ac.in, gagangeet.s.aujla@durham.ac.uk

***Abstract*—Blockchains have profoundly impacted finance and administration, but there are several issues with the current blockchain platforms, including a lack of system interoperability. Currently used blockchain application platforms only work within their networks. Although the underlying concept of all blockchain networks is mainly similar, it involves centralised third-party mediators to transact from other blockchain networks. The current third-party intermediates establish security and trust by keeping track of "account balances" and attesting to the validity of transactions in a centralised ledger. The lack of sufficient inter-blockchain connectivity hinders the mainstream adoption of blockchain. Blockchain technology may be a solid solution for many systems if it grows and works with other systems. For the multi-system blockchain concept to materialise, a mechanism that would connect and communicate with the blockchain systems of various entities in a distributed manner (without any intermediary) while maintaining the property of trust and integrity established by individual blockchains is required. Several methods for verifying cross-chain transactions have been explored in this paper among various blockchains. The efficient verification of cross-chain transactions faces many difficulties, and current research has yet to scratch the surface. In addition to summarising and categorising these strategies, the report also suggests a novel mechanism that gets beyond the existing drawbacks.**

***Index Terms*—Blockchain, interoperability, inter-blockchain connectivity, transaction, trust, integrity, multi-system blockchain**

I. Introduction

Blockchain is envisioned as a decentralised setting powered by distributed ledger technology [1], [2]. However, it is not a cumulative environment. Many blockchains are available, but their ecosystems are separate from one another [3], [4]. Because each chain was developed with a particular use case in mind, it has its unique strengths, weaknesses, and degrees of decentralisation [5]. For instance, a blockchain's level of decentralisation and security may be compromised if its objective is to boost transaction throughput. Blockchains cannot communicate with one another since they are mainly isolated from one another [6]. Thus, the strength of one chain nor the advantages of another chain can be used to compensate for the weaknesses of one link. Due to this isolation, the potential and value of the blockchain industry are fragmented, which worsens the user experience and prevents industry growth [7]. Cross-chain technologies may be helpful here. It is the crucial component needed to increase communication across blockchains. Cross-chain architecture, which enables two or more blockchains to trade off their effectiveness, decentralisation, feature set, and security, facilitates interoperability [8]. This can improve the chain's efficiency, reduce fragmentation, and facilitate the movement of users and features between other blockchains [9]. As more companies, startups, and big businesses use blockchain technology, they realise that no blockchain protocol can exist or function at its best in complete exclusivity [10]. As an analogy, email services could be considered, which would be rendered almost useless if they didn't allow inter-communication between different mail service providers. The same interoperability phenomena also contribute to operating system effectiveness. The same is true for blockchain ecosystems: interoperability, or the capability to efficiently transport data and exchange information between any blockchain, is crucial. By developing and deploying interoperable blockchain platforms, cross-chain technology aims to improve blockchain communication [11]. As the blockchain sector expands, new blockchain protocols are being developed, each with a unique strategy, new consensus techniques, and a new set of capabilities to host multiple applications [12]. However, they cannot scale to the next level because of the isolation required by blockchain's underlying architecture [13]. As a result, they all expand simultaneously and are unable to scale. As a result, various ecosystems are produced that cannot coexist. Because it has the potential to encourage interoperability between blockchains, cross-chain technology is significant [14]. Interoperability between blockchains is necessary to get around the constraints of blockchain protocols and achieve higher scalability, quicker block times, and more robust security [15]. Interoperability will also lower the operational costs related to blockchain technology [16]. The list of blockchain limitations caused by inadequate or nonexistent interoperability is below.

- Bitcoin users cannot use their digital assets within the Ethereum DeFi ecosystem since there is no direct compatibility between Bitcoin and Ethereum [18].
- Consumers cannot convert BTC to ETH without using a centralised cryptocurrency exchange due to a lack of compatibility [19].
- Although USDT is supported by both Ethereum and Binance Smart Chain, it cannot be sent directly from the Ethereum blockchain to Binance Smart Chain, or any other blockchain [20].

TABLE I: Comparative Analysis of Commercial Projects

Source Information	Cosmos	Metronome	Republic	BarterDex
Architecture	A common hub blockchain connects a large number of different blockchains	Employs a single chain architecture	Order matching protocol that deploys a smart contract on the Ethereum network that organises nodes in a network topology that makes attacking unfeasible	BarterDex combines order matching, transaction clearing, and liquidity provisioning
Methodology for cross-chain transaction	Uses IBCBlockCommitTx and IBCPacketTx transactions to transfer data between two blockchains	Destroys tokens in a way that can be verified using a straightforward proof-of-exit receipt	Uses the Shamir Secret Sharing Scheme to split up transactions into a vast number of pieces, the majority of which must be put back together again in order to reconstruct the original sequence	Enables order matching to enable cross-chain conversion of tokens and coins, including Simple Payment Verification(SPV)[17], Electrum and other Bitcoin protocol coins
Limitations	Can only enable zone-to-zone interoperability; other third-party blockchains are not supported	When scaled to a higher volume of transactions, inefficient	Supports only Ethereum-to-x and x-to-Ethereum transactions	Does not consider the existence of duplicate NFTs

- Blockchain researchers intend to integrate Blockchain into the conventional banking system. The goal of blockchain researchers is to incorporate blockchain technology into the current banking system. The creation of an effective solution will be hampered by the lack of interoperability, though, because if two banks use different blockchains, it would be challenging, if not impossible, to perform transactions between their bank accounts. Blockchain in the financial sector would result in a less connected system and a more fragmented without interoperability [21].

II. Literature Review

Both academic and commercial research has been done on cross-chain transaction techniques.

A. Commercial Projects

The following is a summary of commercial projects that are underway at the moment:

- **Cosmos:** Cosmos uses a state-of-the-art design with numerous autonomous blockchains called zones. However, Cosmos Hub is the name of the first zone. Other zones can be connected to the hub to extend its range. Hubs can keep up with the status of each zone. This is because zones always send block commits to the hub and vice versa. However, zones do not know the state of other zones. Additionally, two Merkle trees (IAVL Merkle Tree and Simple Merkle Tree) are kept up to date. A Simple-Tree is unbalanced and tracks a fixed list of elements. IAVLTree provides persistent storage of key-value pairs for the application state and enables rapid generation of deterministic Merkle root hashes. Inter-blockchain communication (IBC) occurs when the hub and zones communicate. IBCBlockCommitTx and IBCPacketTx are two different types of transactions that make up the IBC protocol. Using IBCBlockCommitTx, the blockchain can indicate the latest block hash to any observer. IBCPacketTx enables blockchain to indicate to observers that the sender sent a particular packet. By splitting the IBC mechanism into two different transactions, the receiving chain's native fee market mechanism can control which packets are committed (i.e., acknowledged) but not sent. The ability to control the number of outgoing packets a side chain is allowed is not limited. [22]
- **Metronome:** When a cross-chain transaction starts, the metronome ends with a receipt and discards the token from the source chain in a presentable way. The target blockchain can then use the receipt (simple Merkle proof) [23].
- **Republic:** As a new way of cross-chain transactions, the Republic protocol builds a dark pool of his DEX based on Ethereum using atomic swaps. By adopting Shamir secret sharing technology, the inside and outside of cross-chain transactions and the types of assets cannot be discovered from separated nodes. Transactions are split into many fragments, most of which must be recombined to reconstruct the order. Additionally, it leverages Registrar Ethereum smart contracts. This places nodes in a network topology that makes it impossible for an attacker to find a connected node for a particular transaction [24].
- **Barter DEX:** His BarterDEX, a Komodo project, uses liquidity nodes for order matching, atomic swaps, and peer-to-peer protocols for trading partner negotiation and settlement. BarterDEX uses an atomic swap protocol with two players. A liquidity taker (Alice) and a liquidity provider (Bob). Alice initiates an atomic swap and must pay her dexfee, which is 1/777th of the transaction amount. Liquidity providers also require deposits to ensure the completion of the protocol. It, therefore, acts as a market maker on the Komodo platform and provides liquidity for cross-chain trading [25].

B. Academic Projects

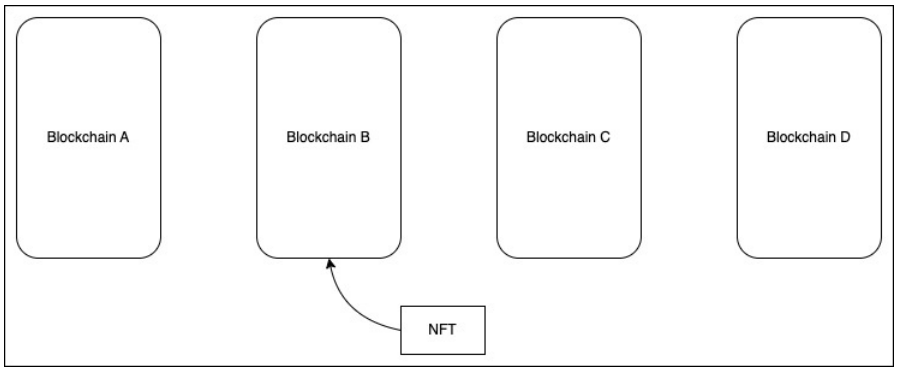
On the academic side, Token Atomic Swap Technology (TAST) has published several white papers incrementally improving various cross-chain transaction technologies.

- TAST's purpose is to explore various techniques within blockchain interoperability platforms to allow assets to move freely between many blockchains in real time without the risk of losing money. TAST also aims to

TABLE II: Comparative Analysis of Academic Projects

Source Information	**Michael Borkowski, TAST (2014)**	**Borkowski et al., TAST (2019)**
Research topic	Examines various methods for achieving blockchain interoperability and builds a model of what a perfect cross-chain token should look like. Examples of projects that support cross-chain transactions in part include Metronome, BarterDex, etc.	A claim-first cross-chain transaction paradigm and a cross-blockchain proof challenge.
Findings	A number of commercial projects, including Metronome and BarterDex, exist that only partially support cross-chain transactions.	Demonstrates that it is impossible to compute a full-scale cross-chain transaction verification in real-world circumstances. Additionally, it simulates a cross-chain claim-first transaction model that uses eventual consistency rather than immediate consistency.
Limitations	Lacks a specific mathematical model for cross-chain transactions.	Cannot be extended to NFTs

Fig. 1: The NFT is written onto one of the blockchains (Blockchain B in this case).



create an interoperable platform by launching a cross-blockchain token called PAN [26].

- The cross-blockchain proof problem states that data recorded on one blockchain cannot be verifiably recognized on another blockchain. TAST has shown through the rooted blockchain lemma that cross-blockchain proofs are not viable for practical reasons. They also introduced a new type of asset transfer called Claims First Transfer. For this type of transaction, the CLAIM transaction is reserved first. This will ensure that assets exist on both blockchains at the same time. However, a valid billing transaction contains data that allows anyone to create his corresponding SPEND transaction. This behaviour is also facilitated by defining rewards for booking SPEND transactions. The only way the system could lead to eventual discrepancies is not to post a SPEND transaction, but this is not believed to be a realistic scenario due to the large number of willing nodes participating. It also mitigates various challenges, such as double spending and double breaking [27].

III. Proposed Solution

Existing approaches for cross-blockchain transaction validation have a significant downside. SPV-based solutions succeed with fungible goods (like bitcoin tokens) but fail with non-fungible ones (such as NFTs). Non-fungible items cannot be kept from being duplicated across different blockchains.

First, all the blockchains under consideration would be linked so that each acts as a notifier and a listener, according to the scenario. Now when an NFT is published on one blockchain (let us say blockchain B), this NFT would first be verified on blockchain B. Once this NFT has been successfully published onto blockchain B, this blockchain would now act as a notifier and notify all the other blockchains, which would act as listeners, about this NFT (Fig. 1).

Blockchain B announces this NFT to other blockchains by sending a hash containing only enough information to prove that this NFT exists on Blockchain B. This hash is verified on every other blockchain and written to the ledger. This hash acts as a lock in the lock-and-key mechanism. Because when a user tries to publish the same NFT on another blockchain, the hash already present on that blockchain (which, in this case, acts as a lock) informs the chain that the NFT exists on another blockchain. Validation for that transaction fails and guarantees that the transaction will fail (Fig.2).

Now, if an NFT of blockchain B needs to be transferred to another blockchain D, that NFT is first burned on blockchain B. Burning an NFT produces two hashes: One acts as a lock on Blockchain B, and the other is used as a key to unlock the lock already present on Blockchain D (Fig. 3). The hash that acts as the key contains the rest of the information that is not present in the lock hash. This combined lock and key hashes contain all the information about the NFT.

When this key hash is written to blockchain D, it is checked against the lock hash that already exists on blockchain D. The key hash unlocks the lock hash, both are burned, and a new hash containing all the information about the NFT is generated and written to blockchain D. Note that the lock hash and key

Fig. 2: Blockchain B notifies all the other blockchains that are linked to it. The hash which is written onto the other blockchains contains only enough information to prove the existence of that NFT (This will act as a lock).

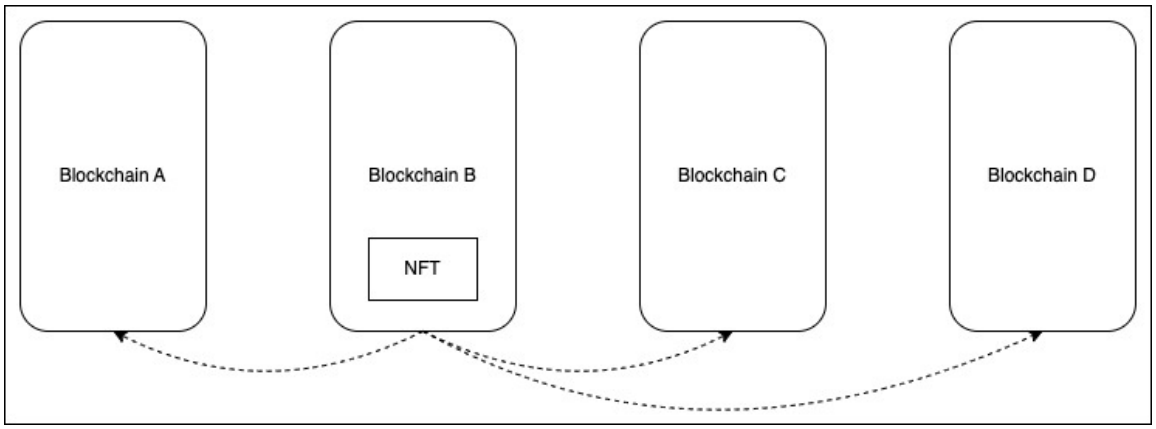


Fig. 3: When the NFT needs to be transferred from one Blockchain to another, it will be burned from blockchain B and two hashes would be generated: one which would now act as a lock on blockchain B, and another which would be used to as a key to unlock the lock which is already the present on blockchain D

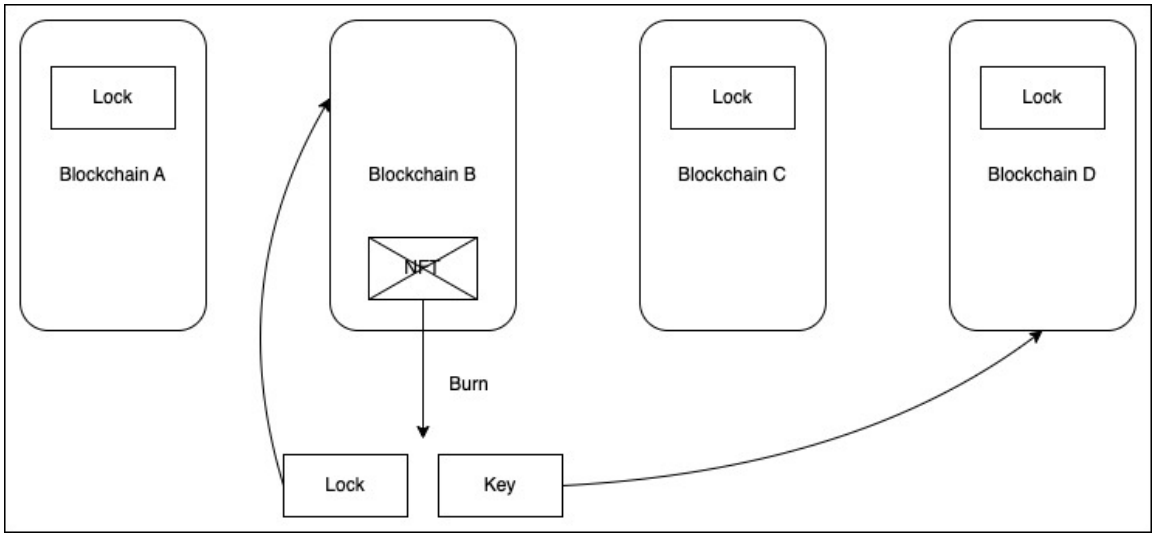
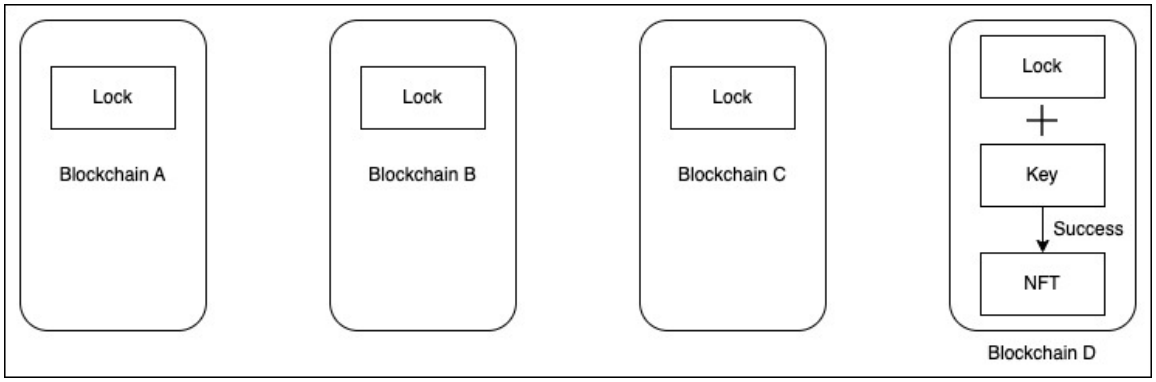


Fig. 4: The key will be matched with the lock on blockchain D. If they both match, the NFT will be written onto blockchain D.



hash are interdependent and do not have independent values (Fig. 4).

This entire process is much more efficient and secure than SPVs and other similar processes, as we never send all the information about an NFT at once. At every step, we always pass information in fragments between blockchains. These fragments have no meaning or value independently of each other.

IV. Results

Halo-2 [28] is the method suggested to demonstrate to a blockchain that a token has been burned. The inner product argument, a polynomial commitment mechanism used in Halo 2, eliminates the requirement for a trusted setup, unlike other Zero-knowledge proofs like Zk-SNARKS [29].

The burning of a token should be verified by a program P_B on a blockchain B. P_B can now be converted to a PLONKish circuit [30] L which can further be converted into a polynomial $g(x)$ where x belongs to a group H. The polynomial commitment scheme for a polynomial $g(x)$, where x belongs to group G, works as follows: A vector $\mathbf{V}$, which is a vector of random group elements and a vector $\mathbf{b}$ consisting of the coefficients of $g(x)$ are taken. The Pedersen [31] vector commitment P is calculated for H to the coefficients of $g(x)$.

$$P =< \mathbf{b}, \mathbf{H} >= Commit(g(x)) \tag{1}$$

A power vector of x, $\mathbf{b}$ also exists:

$$\mathbf{c} = (1, x, x^2, ..x^n) \tag{2}$$

In this setup, it is to be proven that vector b evaluates to u at point x, or in other words, the inner product of $\mathbf{b}$ and $\mathbf{c}$ would result in u.

$$u =< \mathbf{b}, \mathbf{c} > \tag{3}$$

Here P and u are related as:

$$P =< \mathbf{b}, \mathbf{H} > +[r]J \tag{4}$$

Where J is a vector of random group elements representing a shift.

Since Halo-2 is a recursive protocol, the Pedersen vector commitment P_k for the k^{th} iteration ranging from 1 to $log(n)$ is given by:

$$P_k = P + [v]W[32] \tag{5}$$

Where W is a random sample from a group H.

All blockchains henceforth mentioned are assumed to be probabilistic interactive Turing machines. Let there be n blockchains $B_1, B_2, ...B_n$. At the k^{th} round, $\mathbf{b}$, $\mathbf{c}$ and $\mathbf{H}$ are split into lo and hi halves. A random challenge v_k is introduced, and the vectors are compressed by adding the left and right halves separated by v_k:

$$\mathbf{b}^{(k-1)} = v_k.\mathbf{b}_{lo}^{(k)} + v_k^{-1}.\mathbf{a}_{hi}^{(k)} \tag{6}$$

$$\mathbf{c}^{(k-1)} = v_k^{-1}.\mathbf{c}_{lo}^{(k)} + v_k.\mathbf{c}_{hi}^{(k)} \tag{7}$$

$$\mathbf{H}^{(k-1)} = [v_k^{-1}]\mathbf{H}_{lo}^{(k)} + [v_k]\mathbf{H}_{hi}^{(k)} \tag{8}$$

Equation P_{k-1} can be written as, using the compressed vectors:

$$P_{k-1} =< \mathbf{b}^{(k-1)}, \mathbf{H}^{(k-1)} > + [< \mathbf{b}^{(k-1)}, \mathbf{c}^{(k-1)} >]W \tag{9}$$

Expressing the compressed P_{k-1} equation in terms of the original vectors, the following is obtained:

$$\begin{aligned} P_{k-1} =< v_k.\mathbf{b}_{lo}^{(k)} + v_k^{-1}.\mathbf{b}_{hi}^{(k)}, \\ [v_k^{-1}]\mathbf{H}_{lo}^{(k)} + [v_k]\mathbf{H}_{hi}^{(k)} > +[< v_k.\mathbf{b}_{lo}^{(k)} + \\ v_k^{-1}.\mathbf{b}_{hi}^{(k)}, v_k^{-1}.\mathbf{c}_{lo}^{(k)} + v_k.\mathbf{c}_{hi}^{(k)} >]W \end{aligned} \tag{10}$$

Breaking this down into simpler products:

$$\begin{aligned} P_{k-1} =< \mathbf{b}_{lo}, \mathbf{H}_{lo} > + < \mathbf{b}_{hi}, \mathbf{H}_{hi} > + \\ v_k^2 < \mathbf{b}_{lo}, \mathbf{H}_{hi} > + v_k^{-2} < \mathbf{b}_{hi}, \mathbf{H}_{lo} > + \\ [< \mathbf{b}_{lo}, \mathbf{c}_{lo} > + < \mathbf{b}_{hi}, \mathbf{c}_{hi} >]W + \\ [v_k^2 < b_{lo}, c_{hi} > + v_k^{-2} < \mathbf{b}_{hi}, \mathbf{c}_{lo} >]W \\ = P_k + [v_k^2]F_k + [u_k^{-2}]S_k \end{aligned} \tag{11}$$

P_{k-1} is the sum of P_k and the cross-terms F_k, and S_k(with coefficients from the round challenge v_k).

Creation of a token:
Arithmetization of the programme P, which confirms the burning of a token on a blockchain, would be required to create a token T in a blockchain B_i. The resulting arithmetic circuit can then be encoded into a polynomial $g(x)$, where x is a member of an arbitrary finite group H. The host B_i delivers (G), which acts as the lock for the tokens after $f(x)$ has been obtained.

Cross-chain transaction of a token:
The token is burned after a cross-chain transaction is started from the host blockchain Bi to a target blockchain Bt. The prover delivers L and R to the verifier, who can verify the token burn to the target blockchain with a communication complexity of $2k + 1 = O(k)$ terms[28]. A new token is minted onto the target blockchain where the successful verification has already occurred after this unlocks the lock and releases the lock.

V. Conclusion

In conclusion, our system has no known security flaws, is quantum-secure, and state-of-the-art enough to support any number of blockchains, independent of their underlying architecture. Additionally, it is decentralised and independent of third parties. Our method also expands cross-chain transactions to hitherto unexplored NFTs, solving the issue of having numerous chains with identical NFTs of the same physical item. Currently, NFTs that have already been copied on many chains are incompatible with our concept. Additionally, submitting locks to numerous blockchains can be expensive. Incentives that make blocking transactions more profitable as well as strategies for getting rid of redundant NFTs may be the subject of future research.

REFERENCES

[1] S. Meunier, "Chapter 3 - blockchain 101: What is blockchain and how does this revolutionary technology work?" in *Transforming Climate Finance and Green Investment with Blockchains*, A. Marke, Ed. Academic Press, 2018, pp. 23–34. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128144473000033

[2] G. S. Aujla, M. Singh, A. Bose, N. Kumar, G. Han, and R. Buyya, "Blocksdn: Blockchain-as-a-service for software defined networking in smart city applications," *IEEE Network*, vol. 34, no. 2, pp. 83–91, 2020.

[3] I. A. Qasse, M. Abu Talib, and Q. Nasir, "Inter blockchain communication: A survey," in *Proceedings of the ArabWIC 6th Annual International Conference Research Track*, ser. ArabWIC 2019. New York, NY, USA: Association for Computing Machinery, 2019. [Online]. Available: https://doi.org/10.1145/3333165.3333167

[4] C. Qiu, G. S. Aujla, J. Jiang, W. Wen, and P. Zhang, "Rendering secure and trustworthy edge intelligence in 5g-enabled iiot using proof of learning consensus protocol," *IEEE Transactions on Industrial Informatics*, 2022.

[5] J. S. Czepluch, N. Z. Lollike, and S. O. Malone, "The use of block chain technology in different application domains," *The IT University of Copenhagen, Copenhagen*, 2015.

[6] L. Kan, Y. Wei, A. Hafiz Muhammad, W. Siyuan, L. C. Gao, and H. Kai, "A multiple blockchains architecture on inter-blockchain communication," in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 2018, pp. 139–145.

[7] Y. Chen and C. Bellavitis, "Decentralized finance: Blockchain technology and the quest for an open financial system," *Stevens Institute of Technology School of Business Research Paper*, 2019. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3418557

[8] B. Pillai, Z. Hóu, K. Biswas, and V. Bui, "Blockchain interoperability: Performance and security trade-offs," 2018.

[9] B. Pillai, K. Biswas, and V. Muthukkumarasamy, "Cross-chain interoperability among blockchain-based systems using transactions," *The Knowledge Engineering Review*, vol. 35, p. e23, 2020.

[10] Y. Pang, "A new consensus protocol for blockchain interoperability architecture," *IEEE Access*, vol. 8, pp. 153 719–153 730, 2020.

[11] G. Wang, "Sok: Exploring blockchains interoperability," Cryptology ePrint Archive, Paper 2021/537, 2021, https://eprint.iacr.org/2021/537. [Online]. Available: https://eprint.iacr.org/2021/537

[12] W. Mougayar, *The business blockchain: promise, practice, and application of the next Internet technology*. John Wiley & Sons, 2016.

[13] U. Demirbaga and G. S. Aujla, "Mapchain: A blockchain-based verifiable healthcare service management in iot-based big data ecosystem," *IEEE Transactions on Network and Service Management*, 2022.

[14] S. Schulte, M. Sigwart, P. Frauenthaler, and M. Borkowski, "Towards blockchain interoperability," in *Business Process Management: Blockchain and Central and Eastern Europe Forum*, C. Di Ciccio, R. Gabryelczyk, L. García-Bañuelos, T. Hernaus, R. Hull, M. Indihar Štemberger, A. Kő, and M. Staples, Eds. Cham: Springer International Publishing, 2019, pp. 3–10.

[15] G. S. Aujla and A. Jindal, "A decoupled blockchain approach for edge-envisioned iot-based healthcare monitoring," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 491–499, 2020.

[16] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, and K.-K. R. Choo, "Sidechain technologies in blockchain networks: An examination and state-of-the-art review," *Journal of Network and Computer Applications*, vol. 149, p. 102471, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804519303315

[17] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf," 2008.

[18] G. Caldarelli, "Wrapping trust for interoperability: A preliminary study of wrapped tokens," *Information*, vol. 13, no. 1, 2022. [Online]. Available: https://www.mdpi.com/2078-2489/13/1/6

[19] T. Koens and E. Poll, "Assessing interoperability solutions for distributed ledgers," *Pervasive and Mobile Computing*, vol. 59, p. 101079, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574119218306266

[20] K. Qin, L. Zhou, Y. Afonin, L. Lazzaretti, and A. Gervais, "Cefi vs. defi–comparing centralized to decentralized finance," *arXiv preprint arXiv:2106.08157*, 2021.

[21] A. Lohachab, S. Garg, B. Kang, M. B. Amin, J. Lee, S. Chen, and X. Xu, "Towards interconnected blockchains: A comprehensive review of the role of interoperability among disparate blockchains," *ACM Comput. Surv.*, vol. 54, no. 7, jul 2021. [Online]. Available: https://doi.org/10.1145/3460287

[22] E. B. Jae Kwon. (2022) Cosmos whitepaper. [Online]. Available: https://v1.cosmos.network/resources/whitepaper

[23] Metronome. (2018) Metronome whitepaper. [Online]. Available: https://whitepaper.io/document/351/metronome-whitepaper

[24] L. W. Taiyang Zhang. (2017) Republic whitepaper. [Online]. Available: https://republicprotocol.github.io/whitepaper/republic-whitepaper.pdf

[25] Komodo. (2017) Barterdex. [Online]. Available: https://github.com/SuperNETorg/komodo/wiki/barterDEX-Whitepaper-v2

[26] C. R. S. S. Michael Borkowski, Daniel McDonald. (2014) Towards atomic cross-chain token transfers: State of the art and open questions within tast. [Online]. Available: https://dsg.tuwien.ac.at/tast/pub/tast-white-paper-1.pdf

[27] M. Borkowski, M. Sigwart, P. Frauenthaler, T. Hukkinen, and S. Schulte, "Dextt: Deterministic cross-blockchain token transfers," vol. 7, 2019, Article, p. 111030 – 111042, cited by: 34; All Open Access, Gold Open Access, Green Open Access. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85075927829&doi=10.1109%2fACCESS.2019.2934707&partnerID=40&md5=4f849d9d4bf5e4deb0b69a282a7b9603

[28] S. Bowe, J. Grigg, and D. Hopwood, "Recursive proof composition without a trusted setup," Cryptology ePrint Archive, Paper 2019/1021, 2019, https://eprint.iacr.org/2019/1021. [Online]. Available: https://eprint.iacr.org/2019/1021

[29] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Succinct non-interactive zero knowledge for a von neumann architecture," Cryptology ePrint Archive, Paper 2013/879, 2013, https://eprint.iacr.org/2013/879. [Online]. Available: https://eprint.iacr.org/2013/879

[30] A. Gabizon, Z. J. Williamson, and O. Ciobotaru, "Plonk: Permutations over lagrange-bases for oecumenical noninteractive arguments of knowledge," Cryptology ePrint Archive, Paper 2019/953, 2019, https://eprint.iacr.org/2019/953. [Online]. Available: https://eprint.iacr.org/2019/953

[31] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Advances in Cryptology — CRYPTO '91*, J. Feigenbaum, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1992, pp. 129–140.

[32] D. Labs. (2017, 23, August) Zcash: Halo 2 and snarks without trusted setups. [Online]. Available: https://www.youtube.com/watch?v=KdkVTEHUxgo