Multi-Chain Architecture for Blockchain Networks

Kristián Košťál*
Institute of Computer Engineering and Applied Informatics
Faculty of Informatics and Information Technologies
Slovak University of Technology in Bratislava
Ilkovičova 2, 842 16 Bratislava, Slovakia
kristian.kostal@stuba.sk

Abstract

This paper focuses on interoperability between blockchain networks, whether existing or new. The issue of interoperability is a very current topic and is the subject of research by many articles or institutions. The current trend in the articles is to address interoperability only between homogeneous networks, i.e. the so-called Sharding, and not at all dealing with interoperability between different networks. The second trend is to focus on two specific blockchain networks and interconnect them as efficiently as possible. However, both of these trends are flawed, as a large number of new heterogeneous networks have recently emerged, which are incompatible with each other, so that all processes take place in isolation. If they want to communicate with another network, this is almost impossible because there is no standard for interlock blockchain communication. The only option is to exchange assets within the exchange, but this is only a scenario for cryptocurrencies and not for other use cases. Based on the research, an architecture is proposed that uses an API to connect existing blockchain networks and allows communication between any blockchain. From this blockchain it is possible to derive other blockchains that are scalable. The architecture has been implemented and experimental verification has shown scalability up to 18,000 transactions per second.

Categories and Subject Descriptors

C.2.1 [**Networks**]: Network Architecture and Design—*distributed networks*; C.2.4 [**Networks**]: Distributed Systems—*distributed applications, distributed databases*; D.2.12 [**Software Engineering**]: Interoperability; H.2.4 [**Database Management**]: Systems—*distributed databases*

Keywords

blockchain, cross-chain, multi-chain, atomic swaps, interoperability

*Recommended by thesis supervisor: Prof. Ivan Kotuliak To be defended at Faculty of Informatics and Information Technologies, Slovak University of Technology in Bratislava in September 2020.

1. Introduction

We live in a digital age. The Internet is used for everyday communication, bill payments, shopping, charity support or just for fun. Among them, blockchain technology creates another digital dimension and offers new business opportunities.

A key feature is storing data and transactions that change it in block strings. It acts as a distributed database that processes an ever-growing list of transactions for which no authority owns the data. Thanks to this function, the blockchain is extremely resistant to unauthorized modifications to the stored data. The financial sector was therefore the largest supporter. Publicly, the most perceived blockchain applications are cryptocurrencies [8, 24]. Even some of the most dominant regulators in the United States, such as Commodity Futures Trading Commission (CFTC) and Securities and Exchange Commission (SEC), see the positive potential of this technology.

In addition to its use in cryptocurrencies transactions, the benefits of blockchains, such as decentralized information verification and tamper resistance, have been noticed by various sectors [20, 21, 10]. Important applications include the value register, the valuable website and value ecosystem services. Related application industries include logistics, financial systems, medical records, data collection and verification in Internet of Things (IoT), supply chain management, stock or option trading, social networking software, electronic patient records, micropayments / mobile payment systems , asset transactions and distribution of digital products. People hope that blockchains will be able to play the role of trusted machines in the operation of these systems. Keeping a detailed record of related information and resolving information asymmetry problems (where one party to an economic transaction owns more related information than the other party) will allow a reliable record to be created. In the cases used above, a large amount of information will need to be recorded on the blockchain [14].

We will need more robust blockchain networks than are used today to store large amounts of data. This robustness will mainly face problems with scalability, speed of transactions and also privacy challenges [28, 25]. The problem is also in the blockchain community, as there are many more initiatives aimed at creating new blockchains or cryptocurrencies than at developing possible connections and means of communication between existing blockchain networks. For such a solution we need interoperability [11, 22] between today's blockchains and that is the main focus of this work.

2. State of the Art

Blockchain is, simply put, the technology of distributed ledger book (DLT). Blockchain is a decentralized distributed database, which is stored as a chain of blocks, that are cryptographically ordered. The blocks contain transactions between addresses of users. All of this happens in a peer-to-peer network. There exist more kinds of blockchain technology: public, private, consortium. Furthermore, these can be divided by two groups: permissionless, permissioned. When we talk about interoperability, we think communication between two distinct blockchains by any means. Therefore, we need to analyze the options and techniques to achieve inter-operable ledgers.

2.1 Cross-chain

We can understand cross-chain technology as a bridge connecting more blockchains. Its main application is the implementation of atomic cross-chain swaps between different blockchains, asset conversion or inter-block communication [4]. There are obvious obstacles to the distribution of value between blockchains. The cross-chain is a complex distributed coordination task. It needs not only a separate authentication capability for blockchain nodes, but also decentralized input, as well as data acquisition and authentication beyond the blockchain [26]. Cross-chain technologies currently include [3]:

- **Notary schemes** - one side decides to take any action on chain B when a specific event on chain A occurs. Means that a group of trusted parties comes to Byzantine-Fault Toleracne (BFT) consensus over the state of the ledger according to some action on another ledger. The notaries usually exist on separate ledger that they manage to ensure interoperability between two or more ledgers [16]. This is technologically one of the simplest solution to accomplish interoperability goal under its trust model. The model assumes that less than some fraction of the notaries act in Byzantine way [3];
- **Sidechains / Relays** - one chain is capable of reading and validating events on other chains. Technique that allows chains to act based on events from another ledger with the help of a smart contract. They are a more direct approach for chain interoperability without trusted intermediate participants as opposed to notary schemes [3]. They usually need copies of block headers from the other chain. These block headers usually contain Merkle Root tree hash by which any transaction can be proven to be contained in the block from the other chain [16]. Relay schemes are quite powerful because they allow for asset portability, atomic swaps or other more complex use case without restrictions [3]. The drawback is that the underlying blockchains one in case of one-way and both in case of two-way relays needs to support such smart contracts;
- **Hash-locking** - transactions on two chains have the same activation, usually a disclosure of some value. A technique where operations on two interoperating chains are set up in a way that they have the same trigger which is usually a revelation of the pre-image of a particular hash [3]. Hash-locking is simpler compared to relay schemes in which some copy of one ledger must be stored on another ledger because hash-locking only require an exchange of a single hash between two ledgers thus requires significant less exchange of data to achieve interoperability. The primary focus of hash-locking is to allow atomic swaps between ledgers without requiring a third party as it is with notary schemes [16]. The key drawback of hash-locking is that the underlying blockchain must support a special type of smart contracts, called Hash-TimeLock Contracts.

These are three main techniques. Moreover, we can define 4 potential use-cases for interoperability of blockchains as laid out in [3] and [16]:

- **asset portability** - transfer asset from one blockchain to another;
- **atomic swap** - swap asset between two blockchains in atomic way;
- **cross-chain oracles** - are used to read data from outside of blockchain so it can be act upon them;
- **cross-chain asset encumbrance** - lock up assets within one ledger based on locking conditions dependent on another ledger.

The techniques and use-cases are summarized in Table 1.

2.2 Related Work

There exist more solutions which try to make interoperabilty between blockchains. The nowadays state of the art solutions in this research area, according to my analysis and best knowledge, are Cosmos [17] and Polkadot [27]. They are both trying to solve similar problems, concretely introducing interconnection between any blockchain network with the help of centralized Cosmos's Hub (or Polkadot's Relay Chain). To the best of my knowledge they are now more focusing on homogeneous (similar in format of contracts, accounts and consensus) blockchains based on their own engines (Tendermint in Cosmos and Substrate[1] in Polkadot).

Other solutions are also suffering the same issue and a lot of more ones. Blocknet [6] focuses only on solving problems with cryptocurrency assets, concretely making a fully decentralized exchange. BTC Relay [5] concentrates only on one kind of interconnection, specifically connecting Ethereum and Bitcoin blockchains. Corda [12] is not blockchain in its fundamentals. It has some attributes of blockchain technology but tries to solve all problems only with notary schemes. Even if Corda was blockchain, it would not be able to make a connection between existing blockchain networks because Corda needs to have specifically implemented systems to be able to communicate with each other. InfiniteChain [14] introduces only sidechains to one blockchain network to make it more private, faster, scalable and distribute high data volumes. Thus it cannot connect more existing blockchain networks. Interledger Protocol (ILP) [13] is a protocol for communication between any ledgers, not only oriented into blockchains but also to ledgers held by existing banks. However, as the ILP uses Hash Timed Locks, it mandates that all sides of communication implement contracts. The Hyperledger Quilt [15], side by side with

[1] a framework for building decentralised systems; `https://www.parity.io/substrate/`

Table 1: Cross-chain Techniques and Their Use Cases

	Hash-locking	Notary schemes	Sidechains / Relays
Atomic swaps	Yes	Yes	Yes (only 2-way)
Asset portability	No	Yes (requires long-term notary trust)	Yes
Cross-chain oracles	No	Yes	Yes
Asset encumbrance	No	Yes (requires long-term notary trust)	Yes

Ripple, is just a real implementation of Interledger protocol into blockchain technology, so it also shares the same drawbacks as ILP. Lightning Network [23] is comparable to InfiniteChain but it is not a sidechain. A sidechain counts on its own blockchain. This network is, with the help of a two-way peg, coupled to the existing blockchain. On the other hand, the Lightning network consists of native Bitcoin 2-of-2 multi-sig transactions. The cross-chain communication with Lightning Network works as long as all the chains support the same hash function to use for the hash lock. Nodes cooperating in the Lightning Network have to be always online in order to send and receive payments, and this lowers the security as cold wallets cannot be used. Rootstock [18] is the next example of sidechain, but it has a significant disadvantage, that it is suited only for Bitcoin blockchain. Despite that, its only use is to make faster transactions with the help of Simplified Payment Verification[2]. TAST project [1] is still in development and not finished, but their approach with tokens in all blockchains requires that each blockchain has smart contracts functionality to create the tokens. Moreover, in order to function, all wallet balances and movable tokens must be in all participating blockchains. This can radically higher storage demands. Wanchain [19], with the help of Ethereum smart contracts, makes an interconnection between different Decentralized Apps (DApps), but for now, it works only with Ethereum-based blockchains. XClaim [31] is not a universal solution for blockchain interoperability. By far, it was implemented only between Bitcoin and Ethereum. The drawbacks are the need to have at least one smart contracts compatible blockchain, for each pair of blockchains you need to implement specific smart contract only for that pair, and the whole trust in transactions is based on a vault, which locks the funds.

2.3 Summary

A number of competing projects presented here aimed at creating a unified platform for inter-blockchain communication appeared. However, despite the large number of use cases and attempts to address them, the underlying problem of interblockchain communication has not been clearly defined, nor have the related challenges or the existing research [29] been studied. The lack of generality and dependence on the specific implementation of blockchains are disadvantages known to the vast majority of existing solutions. All blockchain solutions work on their "sand" and are not interested in communication between a huge number of blockchains and the interconnection of existing solutions. None of the options described above support plug-in connection of existing blockchains. Only some of the solutions may comply with some government regulations or may communicate with standard databases. In addition, some of the designs add additional overheads to already slow and unpredictable blockchain networks, which only limits functionality. So there are many gaps in interoperability that need to be addressed.

[2]https://en.bitcoinwiki.org/wiki/Simplified_Payment_Verification

3. Research Goals

According to the references and analyzed solutions, we certainly see room for improved interoperability between existing blockchain networks not only specialized in cryptocurrencies, but also databases or perhaps government and state technologies.

All our research is focused on the use of modern blockchain techniques and related technologies in combination with our knowledge of networking and architecture. Summary of the main goals:

- Introduce a new **multi-chain blockchain architecture** to connect two or more different blockchains to allow interoperability between them.
- Enable **attach existing blockchains** in an almost plug & play manner without the need to implement specific requirements on their part.
- Introduce **real-world asset backing mechanism** in token-driven blockchain, e.g. a gold-protected token as a store of value to prevent volatility.

In all three theses, it is important to think about security and, where necessary, ensure that assets can be exchanged between blockchains (for example, in the case of cryptocurrency volatility, redeeming an asset from the real world with a more stable value) and ensuring that this problem can be solved without a centralized third party, e.g. an exchange. The standard approach to atomic swaps between blockchain chains is currently hashed time-locked contracts and smart contracts, which function as two-way relays.

4. Architecture Design

In the proposal to solve the described problems we have two parts. The first is a unique double blockchain technology, where one is public and contains regular transactions, and the second is private, which stores information about the real coverage of the assets from the first blockchain, such as gold. The second part of the design is in the whole network ecosystem for new blockchains and also for existing ones. We decided to think of the blockchain as a color, so each blockchain has its own color assigned to it. That's why we present the color blockchain. The network is controlled by colors grouped into color spaces. The network topology is logically structured as a network of clearly colored networks, as shown in the Figure 1.

4.1 Double-blockchain

For double blockchain purposes, we will use authorized blockchains, authentication will only be possible through the authentication block, and the token register in the authentication subsystem will remain private. The validation block is the connection point between the public and private blockchain. The authentication block can be an application interface (API) or a smart contract. This option represents the detail of the implementation, both cases should work without problems, but the API is an option that can be implemented faster. In order to be able to verify the token validity status in a trouble-free manner, i.e. validation will take place after the transaction is signed without significant delay in the speed of the transaction, we will need a fast scalable consensus algorithm. The ideal consensus algorithm seems to be the Practical Byzantine-Fault Tolerance (PBFT) used in Hyperledger Fabric, which can reach more than 20,000 transactions per second (TPS) [9]. However, to complement the results of the mentioned article, their testing was performed on Fabric 1.2 and only with a critical path, not with complete nodes. According to the authors, the results will be about 25-30 % lower for complete nodes. Double-blockchain is an exact solution to my goal number three.

4.2 Color Blockchain

An architecture is proposed to solve interoperability problems between current blockchain networks. The proposed design introduces a multi-chain architecture for new, as well as existing blockchains. We called the architecture color blockchain. We do not provide any details or instructions regarding implementation, they are up to the developers. Examples of such details are the use of Merkle trees, specific consensus algorithms, cryptography, keys, and other blockchain bases that are inherited from the blockchains on which applications are built. Some basic concepts of architecture are given here.

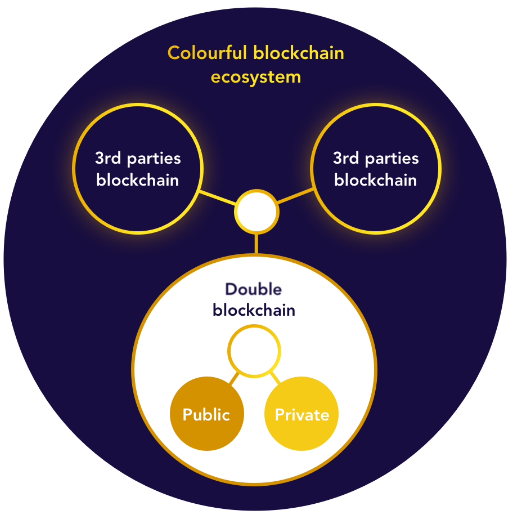

Figure 1: Color blockchain network.

4.2.1 Problem with "Too Large" Data

The coexistence of color blockchains can lead to a huge number of generated blocks during the life of the network. To relieve the pressure on the required performance and storage, we need the Epoch concept based on light clients [30] and Merklix tree[3].

4.2.2 Participation in Colors and Color Space

Each block belongs to exactly one color. This color belongs to the color space, and there is a tree hierarchy of color spaces.
Nodes participating in a particular color usually process only blocks of that color. They can (but are not obliged - depending on the rules in the color space) also process blocks belonging to the nearest / smallest color space to which they belong. Zero color blocks in color spaces are mainly used for color space management and inter-colored communication.

4.2.3 Color Blockchain Custom Network

The color blockchain network is a complete blockchain technology that can handle thousands of individual blockchains and a wide range of configurations. As part of the introduction, the network will create two custom blockchain implementations on the network: Color Blockchain and Color Verification Double Blockchain. Both of these blockchains can be realized in separate color spaces as individual colors. This color space can have a special customized set of rules that validates the properties of tokens in one color using properties in another color.

4.2.4 Smart Smart Contracts

Smart contract design allows to use color blockchain as a robust execution environment with pluggable environments and contract configuration. Smart Contract Execution Engine isolates the execution of smart contracts in a quarantine environment, and therefore protects the network from malicious behavior and increases security [7].

Finally, the key features of the architecture are:

- Blockchain colors - the color blockchain network is designed from the ground up based on the idea of partial blockchains. It can be divided into separate sub-blockchains with their own rules and behavior.
- Enormous readiness - the networks is designed to allow a huge number of operations in terms of throughput and overall capacity thanks to its concept of distributed processing and blockchain snapshots.
- Double-blockchain - in the center of color blockchain is the concept of double blockchain transaction verification. This can be applied to support mechanisms, e.g. gold-covered assets, cryptocurrency-covered assets, etc.

[3] `https://www.deadalnix.me/2016/11/06/using-merklix-tree-to-shard-block-validation/`

- Attaching existing blockchains - the only prerequisite for communicating with existing blockchains is the API. The API can be provided directly by the target blockchain, some API service for blockchains, or the developer can build it himself.

These are the key concepts of architecture. If they work, the whole architecture works like a monolith. Colors are the basic thing about an architecture that provides information about transactions, interoperability, but also makes the system easier to understand. The second feature concerns scalability. Slow blockchains already exist, but fast blockchains with a very high number of transactions per second are, as the overview shows, very current and academia and industry are trying to reach new milestones. Double-blockchain is a very innovative feature that shows other use cases where blockchain can be used. This technology can be selected for any combination of blockchain technologies (public, private). The combination of existing blockchains and distributed ledger technologies, i.e. Heterogeneous interoperability is the highest priority in this work and also a current research topic in the field of inter-blockchain communication.

5. Experimental Verification

We decided to implement a smaller grain of the proposed solution to see the key aspects of the architecture and to demonstrate the key concepts behind the design in a simple way.

5.1 Experimental Methodology

For experimental purposes, we implemented the topology shown in the Figure 2. The decision about colors and color spaces was random without special significance. We have grouped related blockchains with respect to their consensus algorithm used, but note that this is only current choice for experiments.

In this experimental topology, we use APIs provided from blockchains. However, if the blockchain does not provide its own API, we must use some service that the API will create or make available. For this service we use CryptoAPIs [4], which is an infrastructure layer that provides APIs, WebHooks and Web Sockets for some of the existing blockchain protocols, e.g. Litecoin, Bitcoin, Dash, Dogecoin and more.

The blockchains selected for testing were the public testing networks Bitcoin, Ethereum and Eos. These three existing blockchain networks are sufficient to demonstrate functionality and communication with existing blockchains. Color blockchain uses the Tendermint core [2].

All experiments were performed on Amazon EC2 instances of type *m5n.4xlarge*, where we ran the tests with 4, 8, 16 and 32 instances. Each was a validator for the core network and some were validators and vaults for existing blockchains and double-blockchain. We repeated each test 100 times and the results shown here are the median values.

The scenario was to verify the speed of transactions within the color blockchain network. When we compare it with the Tendermint from which this blockchain is built, we

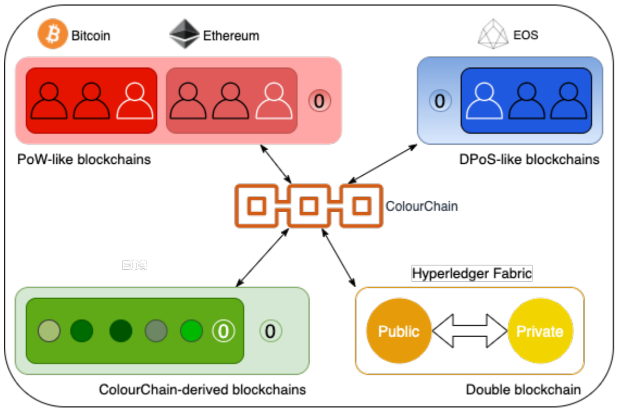

Figure 2: Experimental topology.

get very similar results, almost 20,000 TPS. The results are shown in the Figure 3.

5.2 Summary

This chapter described the verification of the proposed architecture. The verification started with the setting up of networks and processes, which also served as a basic verification for defined transactions and blocks. Verification with experimental implementation followed. Both selected methods are independent of each other and confirm the functionality of parts of the proposed architecture. In the experimental case, we verified the design by implementing part of the architecture and the sample network using several different blockchains. We divided this case into two scenarios. One where we focused on double blockchain technology to point out its speed and minimal impact on extension when verifying gold support for each transaction. The test showed minimal differences in times with and without validation, the only case where the difference was more seen, i.e. 831 ms, was with 50,000 transactions, but so many transactions usually do not occur in one blockchain network at once. In the second scenario, we verified the partially implemented color blockchain architecture using three existing blockchain networks, a double-blockchain, and six color blockchain-derived blockchains. In addition, there were APIs to connect to existing blockchains. The results in this scenario show that our network is high-speed and its slowdown is only affected by the length of the verification time in the source and destination blockchain. Subsequently, we verified the scalability on blockchains derived from color blockchain, which are not significantly slowed down by block time, and here it turned out that the entire color blockchain network managed up to 18,000 TPS. During the network latency and throughput test scenarios, we monitored the impact of our implementation and use of consensus algorithms on network properties. Measurements were performed in a real geographically distributed environment to indicate network operation if deployed. The real environment was set so that its properties do not affect the quality. In all experiments, we verified that the color blockchain network has a minimal impact on the quality of services provided.

6. Conclusion

In this work, we presented a solution to problems with the interoperability of various blockchain networks. Our architecture supports atomic swaps between existing block-

[4] https://cryptoapis.io/products/blockchain-apis/

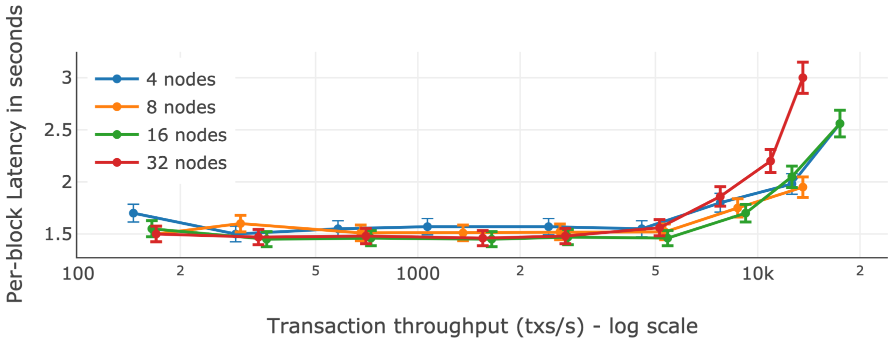

Figure 3: Delay vs. throughput in a testing environment.

chain networks using vaults and collateralization. There are also notary schemes. The current literature has shown that we cannot implement blockchain interoperability without a trusted third party [29]. However, in our solution, validators in a trusted third party come from participating blockchains, so even though our transmission chain is called "centralized," if we use nodes from existing networks where they are trusted, they will also be trusted in the color blockchain.

The results of verifications confirmed the functionality of the proposed architecture and the fulfillment of the defined goals. We introduced a new multi-chain blockchain architecture for interoperability that has proven itself, so the first goal is complete. The second goal is also achieved thanks to the API for existing blockchains and the introduction of colors and color spaces. We tested the connection of three different blockchains to our network; linking a new blockchain is a process that takes a few seconds, because the only requirement is to map the functions of the target blockchain to color blockchain. The third goal is achieved using double blockchain technology. In addition, atomic swaps are achieved in the architecture using smart contracts (i.e. relay schemes) and automatic locks between accounts via a transmission chain (i.e. notary scheme), but the system is also ready for hash locks, this will only be an implementation detail.

Acknowledgements. This research was supported by the Ministry of Education, Science, Research and Sport of the Slovak Republic, Incentives for Research and Development, Grant No.: 2018/14427:1-26C0. This publication was created thanks to support under the Operational Program Integrated infrastructure for the project: Research in the field of blockchain technology with connection to online payment services, ITMS 313022U641, co-financed by the European Regional Development Fund. It was also partially supported by the grants APVV-15-0731, KEGA 011STU-4/2017, and VEGA 1/0836/16. The author would like to thank for financial contribution from the STU Grant scheme for Support of Young Researchers.

References

[1] M. Borkowski, D. Mcdonald, C. Ritzer, and S. Schulte. Towards Atomic Cross-Chain Token Transfers: State of the Art and Open Questions within TAST. Technical report, TU Wien, Vienna, Austria, 2018.

[2] E. Buchman, J. Kwon, and Z. Milosevic. The latest gossip on BFT consensus. *arXiv*, 1807(4938):14, jul 2018.

[3] V. Buterin. Chain Interoperability. *R3 Research Paper*, 2016.

[4] Z.-d. CHEN, Z. YU, Z.-b. DUAN, and K. HU. Inter-Blockchain Communication. In *Proceedings of the 2nd International Conference on Computer Science and Technology (CST 2017)*, pages 448–454, Guilin, China, 2017. DEStech Publications.

[5] L. Coleman. BTC Relay Bridges BTC With Ethereum, Allowing BTC Verification For Smart Contracts, 2016.

[6] A. Culwick and D. Metcalf. The Blocknet Design Specification. Technical report, 2018.

[7] G. G. Dagher, C. L. Adhikari, and T. Enderson. Towards Secure Interoperability between Heterogeneous Blockchains using Smart Contracts. In *Future Technologies Conference (FTC) 2017*, pages 73–81, Vancouver, Canada, 2017. Science and Information Conferences.

[8] I. Eyal. Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities. *Computer*, 50(9):38–49, 2017.

[9] C. Gorenflo, S. Lee, L. Golab, and S. Keshav. FastFabric: Scaling Hyperledger Fabric to 20,000 Transactions per Second. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 455–463. IEEE, 2019.

[10] Y. Guo and C. Liang. Blockchain application and outlook in the banking industry. *Financial Innovation*, 2(24):1–12, dec 2016.

[11] T. Hardjono, A. Lipton, and A. Pentland. Towards a Design Philosophy for Interoperable Blockchain Systems. *arXiv*, 1805(5934):27, may 2018.

[12] M. Hearn. Corda: A distributed ledger. Technical report, 2016.

[13] A. Hope-Bailie and S. Thomas. Interledger: Creating a Standard for Payments. In *Proceedings of the 25th International Conference Companion on World Wide Web - WWW '16 Companion*, pages 281–282, New York, New York, USA, 2016. ACM Press.

[14] G.-H. Hwang, P.-H. Chen, C.-H. Lu, C. Chiu, H.-C. Lin, and A.-J. Jheng. InfiniteChain: A Multi-chain Architecture with Distributed Auditing of Sidechains for Public Blockchains. In S. Chen, H. Wang, and L.-J. Zhang, editors, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 10974 LNCS, pages 47–60. Springer International Publishing, Cham, jun 2018.

[15] Hyperledger Inc. Hyperledger Gets Cozy With Quilt, 2017.

[16] T. Koens and E. Poll. Assessing interoperability solutions for distributed ledgers. *Pervasive and Mobile Computing*, 59(101079):1–10, oct 2019.

[17] J. Kwon and E. Buchman. Cosmos: A Network of Distributed Ledgers. Technical report, 2018.

[18] S. Lerner. Drivechains, Sidechains and Hybrid 2-way Peg Designs. Technical report, RSK Labs Ltd., 2016.

[19] J. Lu, B. Yang, Z. Liang, Y. Zhang, S. Demmon, E. Swartz, and L. Lu. Wanchain: Building Super Financial Markets for the New Digital Economy. Technical report, 2017.

[20] M. Mettler. Blockchain technology in healthcare: The revolution starts here. In *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 1–3. IEEE, sep 2016.

[21] Q. K. Nguyen. Blockchain - A Financial Technology for Future

Sustainable Development. In *2016 3rd International Conference on Green Technology and Sustainable Development (GTSD)*, pages 51–54. IEEE, nov 2016.

[22] L. Pawczuk, J. M. Nielsen, P. K. H. Sin, and N. Hewett. Inclusive Deployment of Blockchain for Supply Chains: Part 6-A Framework for Blockchain Interoperability In Collaboration with Deloitte. Technical report, Deloitte, 2020.

[23] J. Poon and T. Dryja. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Technical report, 2016.

[24] M. Swan. *Blockchain : blueprint for a new economy*. O'Reilly Media, 1 edition, 2015.

[25] S. Underwood. Blockchain beyond bitcoin. *Communications of the ACM*, 59(11):15–17, oct 2016.

[26] H. Wang, Y. Cen, and X. Li. Blockchain Router. In *Proceedings of the 6th International Conference on Informatics, Environment, Energy and Applications - IEEA '17*, pages 94–97, New York, New York, USA, 2017. ACM Press.

[27] G. Wood. POLKADOT: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORK. Technical report, 2017.

[28] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander. Where Is Current Research on Blockchain Technology?âĂŤA Systematic Review. *PLOS ONE*, 11(10):163–189, oct 2016.

[29] A. Zamyatin, M. Al-Bassam, D. Zindros, E. Kokoris-Kogias, P. Moreno-Sanchez, A. Kiayias, and W. J. Knottenbelt. SoK: Communication Across Distributed Ledgers. Technical report, Cryptology ePrint Archive, 2019.

[30] A. Zamyatin, Z. Avarikioti, D. Perez, and W. J. Knottenbelt. TxChain: Efficient Cryptocurrency Light Clients via Contingent Transaction Aggregation. Technical report, Cryptology ePrint Archive, 2020.

[31] A. Zamyatin, D. Harz, J. Lind, P. Panayiotou, A. Gervais, and W. Knottenbelt. XCLAIM: Trustless, Interoperable, Cryptocurrency-Backed Assets. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 193–210. IEEE, may 2019.

Selected Papers by the Author

K. Košťál, P. Helebrandt, M. Belluš, M. Ries, and I. Kotuliak. Management and Monitoring of IoT Devices Using Blockchain. *Sensors*, vol. 19, no. 4, p. 856, Feb. 2019.

K. Košťál, T. Krupa, M. Gembec, I. Veres, M. Ries, and I. Kotuliak. On Transition between PoW and PoS. In *Proceedings of 2018 International Symposium ELMAR: 60th International symposium.*, pages 207–210, Zadar, Croatia, 2018. IEEE Press.

V. Valaštín, K. Košťál, R. Bencel, and I. Kotuliak. Blockchain Based Car-Sharing Platform. In *Proceedings of ELMAR-2019: 61st International symposium.*, pages 5–8, Zadar, Croatia, 2019. IEEE Press.

K. Košťál, R. Bencel, M. Ries, and I. Kotuliak. Blockchain E-Voting Done Right: Privacy and Transparency with Public Blockchain. In *2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS)*, pages 592–592. Beijing, China, 2019. IEEE Press