Towards Blockchain Interoperability

Stefan Schulte[1(✉)], Marten Sigwart[1], Philipp Frauenthaler[1], and Michael Borkowski[2]

[1] Distributed Systems Group, TU Wien, Vienna, Austria
{s.schulte,m.sigwart,p.frauenthaler}@infosys.tuwien.ac.at
https://www.dsg.tuwien.ac.at
[2] Institute of Flight Guidance, German Aerospace Center (DLR), Brunswick, Germany
michael.borkowski@dlr.de
https://www.dlr.de

Abstract. In recent years, distributed ledger technologies like blockchains have gained much popularity both within industry and research. Today, blockchains do not only act as the underlying technology for cryptocurrencies like Bitcoin, but have also been identified as a potentially disruptive technology in many different fields, e.g., supply chain tracking and healthcare. The widespread attention for blockchains has led to manifold research and development activities. As a result, today's blockchain landscape is heavily fragmented, with different, incompatible technologies being available to potential users. Since interoperability between different blockchains is usually not foreseen in existing protocols and standards, functionalities like sending tokens from one participant to another, or invoking and executing smart contracts can only be carried out within a single blockchain.

In this paper, we discuss the need for blockchain interoperability and how it could help to stimulate a paradigm shift from today's closed blockchains to an open system where devices and users can interact with each other across the boundaries of blockchains. For this, we consider the areas of cross-blockchain token transfers, as well as cross-blockchain smart contract invocation and interaction.

Keywords: Blockchain · Interoperability · Distributed ledger

1 Introduction

Originally, blockchains have been primarily perceived as the underlying technological means to realize monetary transactions in a fully decentralized way, thus enabling cryptocurrencies. While blockchains of the first generation like the one established by Bitcoin [1] provide the means to store data and to enact transactions in a distributed ledger, second-generation blockchains like Ethereum [2] enable the execution of almost arbitrary software functionalities within the blockchain, using so-called *smart contracts* [3]. For this, second-generation blockchains

C. Di Ciccio et al. (Eds.): BPM 2019 Blockchain and CEE Forum, LNBIP 361, pp. 3–10, 2019.
https://doi.org/10.1007/978-3-030-30429-4_1

provide quasi Turing-complete scripting languages like *Solidity*, and an according execution environment like the *Ethereum Virtual Machine* (EVM) [4].

Because of their capabilities, blockchains have the potential for wide-spread application in many different areas. These areas range from generic industrial applications to more specific use cases in Business Process Management (BPM) [5,6], anti-counterfeiting [7], or healthcare [8]. In brief, blockchains might be applied in any scenario where it is useful to execute transactions and store data in a tamper-proof and fully decentralized manner without being dependent on a centralized third party.

Naturally, different use cases have different requirements and thus demand different capabilities of blockchains. As a result, research and development in the blockchain field often focus on the creation of entirely new blockchains and cryptocurrencies, or on altering major blockchains like Bitcoin to satisfy additional requirements [9]. This leads to incompatible novel technologies.

The constant increase in the number of independent, unconnected blockchain technologies causes significant fragmentation of the research and development field since (industrial) users and developers have to choose which cryptocurrency and which blockchain to use for each use case scenario. Choosing novel, innovative blockchains enables users and developers to utilize new features and to take advantage of state of the art technology. However, the risk of security breaches potentially leading to a total loss of funds in novel blockchain networks is substantially higher than in established ones, due to a higher likelihood of bugs and the smaller user base in the beginning [10]. On the other hand, choosing mature, well-known blockchains reduces the risk of losses, since these blockchains are more likely to have been analyzed in-depth [11], but novel features remain unavailable.

Therefore, providing means to bridge the gaps between different blockchain technologies would evidently have a large impact since users could select and combine blockchains based on their current demands while not being locked-in to one particular technology. However, the ways in which different blockchains could potentially interact with each other remain mostly unexplored. Most importantly, today, the following functionalities can only be carried out within a single blockchain:

- Sending tokens from one participant to another
- Executing smart contracts saved in a blockchain
- Guaranteeing validity of data stored in a blockchain

In this paper, we further discuss the need for blockchain interoperability, and potential solution approaches. We consider blockchain interoperability on different levels, namely cross-blockchain token transfers (Sect. 2) and cross-blockchain smart contract invocation and interaction (Sect. 3).

2 Cross-Blockchain Token Transfers

2.1 State of the Art

Following their original purpose to serve as the underlying technology for cryptocurrencies, the most obvious research question in the field of blockchain interoperability is surely "How can we transfer tokens between different blockchains?". Today, tokens like cryptocurrency coins can only be used in one particular blockchain. Therefore, one promising research direction is to establish approaches for transferring tokens between different blockchains, i.e., from a source blockchain to a target blockchain. To achieve this, according token transactions need to be autonomously synchronized between the involved blockchains in a decentralized manner. The solution needs to prevent double spending and the faking of transactions in order to avoid tokens being created on the target blockchain without first being destroyed on the source blockchain. Since it is difficult to fully replicate the state of one blockchain within another blockchain [12], efficient mechanisms are necessary that allow the verification of events taking place on one blockchain from within another blockchain without relying on a third party.

One of the earliest contributions in the field of blockchain interoperability is the idea of a trustless cryptocurrency exchange realized in the form of atomic cross-chain swaps (also simply labeled as "atomic swaps"). Atomic swaps enable users of different cryptocurrencies to swap their assets in an atomic and trustless manner, e.g., Alice sends one Bitcoin to Bob on the Bitcoin blockchain and Bob sends 50 Ether to Alice on the Ethereum blockchain. In recent years, atomic swaps have received attention from industry and academia likewise. For instance, the approach is being adapted by platforms like Komodo's BarterDex [13] to enable the decentralized exchange of cryptocurrencies. In academia, work has focused on approaches to extend the protocol to more than two users and on the best ways to match users seeking to perform atomic swaps [14]. However, atomic swaps do not enable the transfer of a token from one blockchain to another in a sense that a certain amount of assets is destroyed on the source blockchain and the same amount is (re-)created on the destination blockchain, e.g., transfer a token T from Bitcoin to Ethereum such that T can be used on Ethereum after the successful completion of the transfer. As the name implies, atomic swaps provide not transfers, but exchanges of tokens across the boundaries of blockchains. Therefore, atomic swaps always need a counterparty willing to exchange tokens. An indirect way to exchange tokens is offered by online marketplaces. So far, however, this requires the existence of a trusted, centralized entity, which counteracts the decentralized nature of blockchains, and can therefore only be seen as an intermediate step towards full decentralization.

2.2 Research Directions

Despite the existing first attempts to decentralized solutions using atomic swaps, research in the field of cross-blockchain token transfers is still limited. In par-

ticular, so far, no practical solution exists that enables the transfer of a single token between different blockchains.

Ideally, a cross-blockchain token enables users to freely choose on which blockchain they want to hold their assets. Users should not be tied to particular blockchains and should be able to hold different denominations of a token on multiple blockchains at the same time. If a new blockchain technology emerges and offers novel features, users should be able to transfer their tokens to this new blockchain taking advantage of the novel capabilities. Finally, the distribution of assets across the participating blockchains could give an indication about the significance of a particular blockchain.

In general, when transferring tokens between blockchains, it needs to be ensured that the total amount of tokens remains the same, i.e., it must not be possible to create tokens out of nothing, since this would effectively lead to uncontrolled inflation. In [15], we present a first prototype that uses reward-incentivized third-party witnesses to propagate token transfers across an ecosystem of blockchains hence enabling a first kind of cross-blockchain token. This prototype synchronizes balances of the cross-chain token across all participating blockchains. However, this first prototype poses a couple of limitations. First, the synchronization of any balance change across all blockchains leads to excessive synchronization cost. The more blockchains are supported by the protocol, the higher the synchronization cost become. Second, the devised approach provides no means of adding a new blockchain later on. Since every blockchain stores the current balance of each wallet, these balances must also be synchronized with a new blockchain. This leads inevitably to the open question how all existing balances can be transferred to a new blockchain without relying on a trusted third party. Third, in order to verify digital signatures, all blockchains must support the same implementations of the required cryptographic primitives. Fourth, the proposed approach does not allow to determine the significance of individual blockchains (e.g., how much assets are stored on each blockchain), since each blockchain stores the same wallet balances.

Since it is not possible to fully replicate one blockchain within another blockchain [12], solutions are necessary to provide enough information to the target blockchain so that it can prove or be otherwise certain that the transferred amount of tokens has actually been destroyed on the source blockchain and can thus securely be created on the target blockchain. Since this information has to come from an external source, two strategies are promising. Either, (a) the provided information acts as a cryptographic proof that can be verified by the target blockchain to prove that the tokens were actually destroyed on the source blockchain, or (b) the target blockchain relies on information provided by oracles [16], to attest whether or not the tokens have actually been destroyed.

For (a), several limitations have to be tackled to make such a proof-based strategy work in praxis. In particular, proof construction and validation have to be efficient for the benefits of a cross-blockchain token transfer to outweigh the associated cost. For (b), since this approach relies on third parties or oracles to provide valid information, the challenges lie in aligning incentives in such a

way that the third parties are always inclined to behave honestly, and designing the system so that it is difficult or near impossible for malicious actors to perform manipulations. Note that these challenges are not specific to strategy (b), but rather are inherent challenges of blockchain technologies. For instance, 51% attacks are theoretically possible, but with the right incentive structure and consensus algorithm very difficult to do in practice for most of today's major blockchains.

In addition, different blockchains employ different consensus mechanisms, block sizes, confirmation times, hashing algorithms, and network models. Further, not all blockchains provide the same level of scripting capabilities, e.g., Ethereum's scripting language is quasi Turing-complete, whereas other languages like Script, which is employed by Bitcoin, are more limited. Hence, a major research challenge is to develop a solution for secure cross-blockchain token transfers that accounts for this diversity. Finally, special cases like potential blockchain forks need to be addressed by a solution, since blocks in forks are usually valid, but are not (or not yet) confirmed by the majority of participants.

3 Cross-Blockchain Smart Contract Interaction

3.1 State of the Art

With smart contracts being in the focus of most currently discussed application areas of blockchain technologies, the second quite obvious dimension of blockchain interoperability leads to the research question "Which possibilities exist to enable invocations of smart contracts across blockchains and therefore to realize cross-blockchain applications?".

Multiple projects aim to tackle the problem of general blockchain interoperability in contrast to the more specific use case of cross-blockchain token transfers discussed above. General interoperability is largely concerned with generic communication between blockchains, i.e., the passing of arbitrary information from one blockchain to another in a decentralized and trustless way. The ability to establish generic communication between blockchains would in turn enable cross-blockchain smart contract interaction or even cross-blockchain smart contracts. The latter describe smart contracts which do not only interact with each other, but which run on different blockchains, and could be transferred from one blockchain to another.

In [17], Jin et al. elaborate on different blockchain interoperation schemes such as an active mode and a passive mode. In terms of the passive mode, a blockchain monitors transactions or events occurring on another blockchain, whereas a blockchain in active mode first sends information to another blockchain, and then waits for the feedback from this blockchain. Furthermore, different challenges in realizing interoperability are discussed, e.g., guaranteeing atomicity, efficiency, and maintenance of security. Jin et al. further discuss possible concepts for establishing interoperability on different layers. More precisely, they discuss ideas and challenges in the terms of unifying data structures, network

communication, consensus mechanisms, cross-chain contracts, and blockchain applications.

A more generic multi-blockchain framework is proposed by PolkaDot [18]. PolkaDot aims to provide a platform for blockchain interoperability managed by a central relay blockchain which validates transactions taking place on so-called parachains. Parachains are blockchains which can be more or less specialized for specific applications and purposes. The aim of the relay blockchain is to enable interchain communication of parachains by a message-passing protocol and to let parachains pool their security, thus lowering the entry barriers for new blockchain projects. While the initial PolkaDot whitepaper mentions basic ideas about how the interaction of parachains with the relay blockchain might take place, no details are given about the actual validation process taking place on the relay blockchain. Further, the project seems to be in an early stage of development, and only individual parts have been prototyped so far. Also, the planned parachains have to comply to specific interfaces in order to interact with the relay blockchain. Existing blockchains like Ethereum will have to be integrated via so-called bridge blockchains.

Cosmos [19] is another project aiming to bring generic interoperability capabilities for blockchains to the industry. Similarly to PolkaDot, interoperability in Cosmos takes place between multiple blockchains called zones. Cosmos zones all run on the Proof-of-Stake consensus mechanism Tendermint. One zone, called the Cosmos hub, acts as a central communication blockchain between the other zones. The Cosmos hub keeps track of all committed block headers occurring in the other zones and likewise the zones keep track of the blocks of the hub. Via Merkle proofs, zones can prove to each other the existence of messages on their respective blockchains, this way enabling interchain communication. Similar to PolkaDot, one drawback of Cosmos is that it does not enable interoperability between existing blockchains out of the box. Instead, all zones have to implement the same consensus mechanism. While it is planned to also integrate existing blockchains like Ethereum via specific adapter zones, no details how this could be achieved are provided so far.

3.2 Research Directions

As it can be seen from the discussion above, generic blockchain interoperability is a highly active research field, however, so far, tangible progress is slow. Hence, cross-blockchain smart contract interaction is currently not possible in an efficient and trustless manner.

The basic prerequisite to establish cross-blockchain smart contract interaction is to establish an inter-blockchain communication protocol which can be used to exchange arbitrary data between blockchains in a decentralized and trustless way. Cross-blockchain token transfers as discussed above constitute a specific use case of inter-blockchain communication, since the existence of a particular piece of information (i.e., the transaction destroying tokens) on the source blockchain needs to be proven on the target blockchain. Hence, the same challenges and constraints that apply to cross-blockchain token transfers also apply

to generic inter-blockchain communication and therefore cross-blockchain smart contract interaction.

Therefore, a major research challenge is to generalize research results and solutions developed for cross-chain token transfers in order to allow the reliable verification of arbitrary data from one blockchain on another. Ideally, a protocol is developed, where generic information can be passed between multiple blockchains, comparable to the transport layer of the Internet. Once such a protocol exists, further research will be required to determine the efficient usage of this protocol, e.g., whether communication happens synchronously or asynchronously, via request and reply patterns, etc. Similar to cross-blockchain token transfers, in order to develop a solution capable of running on multiple different blockchains, a wide diversity of different systems needs to be taken into account, i.e., different consensus mechanisms, confirmation times, block sizes, header sizes, network models, the frequency of forks, scripting languages, etc.

4 Conclusions

The peculiar properties of blockchain technologies have lead to activities aiming at the application of blockchains in many different areas. To account for the diverse requirements of these application areas, existing blockchain protocols are adapted or completely new protocols are presented for new use cases. This has lead to today's widely fragmented blockchain landscape. Hence, solutions for blockchain interoperability are needed, e.g., the possibility to transfer tokens from one blockchain to another, or to achieve interoperability between smart contracts on different blockchains.

Within this paper, we have discussed the current state of the art in these areas and have given some thoughts about possible research directions. Our own concrete research in this area is currently aiming at cross-blockchain token transfers, which we see as a first step into the direction of more generic inter-blockchain communication. This, in turn, would enable more complex scenarios, such as cross-blockchain smart contracts.

Acknowledgments. The work presented in this paper has received funding from Pantos GmbH[1] within the TAST research project.

References

1. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. Whitepaper (2008)
2. Buterin, V.: A Next Generation Smart Contract & Decentralized Application Platform (2013) Whitepaper, Ethereum Foundation
3. Tschorsch, F., Scheuermann, B.: Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Commun. Surv. Tutor. **18**(3), 2084–2123 (2016)
4. Dannen, C.: Introducing Ethereum and Solidity. Apress (2017)

[1] https://pantos.io/.

5. Prybila, C., Schulte, S., Hochreiner, C., Weber, I.: Runtime Verification for Business Processes Utilizing the Bitcoin Blockchain. Futur. Gener. Comput. Syst. (2019, in press)
6. Mendling, J., et al.: Blockchains for business process management - challenges and opportunities. ACM Trans. Manag. Inf. Syst. **9**(1), 4 (2018)
7. Lu, D., et al.: Reducing automotive counterfeiting using blockchain: benefits and challenges. In: 2019 IEEE International Conference on Decentralized Applications and Infrastructures, pp. 39–48 (2019)
8. Li, M., Xia, L., Seneviratne, O.: Leveraging standards based ontological concepts in distributed ledgers: a healthcare smart contract example. In: 2019 IEEE International Conference on Decentralized Applications and Infrastructures, pp. 152–157 (2019)
9. Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K.: Where is current research on blockchain technology?-A systematic review. PLOS ONE **11**(10), e0163477 (2016)
10. Nofer, M., Gomber, P., Hinz, O., Schiereck, D.: Blockchain. Bus. Inf. Syst. Eng. **59**(3), 183–187 (2017)
11. Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q.: A survey on the security of blockchain systems. Future Gener. Comput. Syst. (2017, in press)
12. Borkowski, M., Ritzer, C., McDonald, D., Schulte, S.: Caught in chains: claim-first transactions for cross-blockchain asset transfers. Technische Universität Wien, Whitepaper (2018)
13. Komodo Platform: Blockchain Interoperability: Cross-Chain Smart Contracts (2018). https://komodoplatform.com/interoperability-cross-chain-smart-contracts/. Accessed 26 Apr 2019
14. Herlihy, M.: Atomic cross-chain swaps. In: 2018 ACM Symposium on Principles of Distributed Systems. ACM, pp. 245–254 (2018)
15. Borkowski, M., Sigwart, M., Frauenthaler, P., Hukkinen, T., Schulte, S.: DeXTT: decentralized cross-chain token transfers. arXiv:1905.06204 (2019)
16. Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., Santamaria, V.: Blockchain and smart contracts for insurance: is the technology mature enough? Future Internet **10**(2), 20 (2018)
17. Jin, H., Dai, X., Xiao, J.: Towards a novel architecture for enabling interoperability amongst multiple blockchains. In: 38th International Conference on Distributed Computing Systems, pp. 1203–1211 (2018)
18. Wood, G.: Polkadot Whitepaper (2019). https://polkadot.network/PolkaDotPaper.pdf. Accessed 26 Apr 2019
19. Kwon, J., Buchman, E.: Cosmos Whitepaper (2019). https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md. Accessed 26 Apr 2019