Information Technology and Management Science
ISSN 2255-9094 (online)
2023, vol. 26, pp. 27–34
https://doi.org/10.7250/itms-2023-0004
https://itms-journals.rtu.lv

1862
RIGA TECHNICAL UNIVERSITY

Cross-Chain Bridges: A Potential Solution to Standardising Distributed Ledger Technology in Payment Systems

Vadims Zilnieks[1*], Ingars Erins[2]
[1,2]*Faculty of Computer Science and Information Technology, Riga Technical University, Riga, Latvia*

***Abstract* – Despite standardisation initiatives, the modern financial landscape continues to be characterised by heterogeneous payment systems. This issue persists even with the emergence of distributed ledger technology in the market. Independent groups of developers are producing their own permissioned blockchain solutions without clear directions for standardisation that could be associated to the lack of a clear position from central banks and regulatory organisations regarding these technologies. The unresolved problem of transaction finality in distributed ledgers adds to the difficulty of reconciling separate distributed platforms. One potential solution is the implementation of cross-chain bridges, which can establish connections between platforms and potentially enable seamless experiences for end users and applications. The paper discusses the advantages and issues associated with these bridges.**

***Keywords* – Blockchain, cross-chain bridge, distributed ledger.**

I. Introduction

Starting with the automation of bank-to-bank transactions using electronic communications, payment systems have reached their current modern landscape. Clearing houses, real-time settlements, or instant transfers, all these systems are regulated by institutions prescribed by law, such as central banks or national regulatory.

The year of 2008 marked the first decentralized electronic payment system creation, Bitcoin [1]. It was a crucial moment for the industry. Considering the open-source nature of the project, numerous software clones were developed, and alternative projects as well. All of these were based on the principle of operating without central regulation. Trust is established through cryptography and specific proofs of transaction validity [2]. Data are maintained in a shared distributed database, commonly known as a blockchain or distributed ledger (DL). The consistency of this ledger, depending on the algorithm used, is ensured to be immutable. In the case of Bitcoin, this was achieved through proof-of-work, when consistency of the ledger is provided by complexity of finding solution of one-directed function [2]. The ledger remains consistent unless a participant receives the majority of the total computational power required to produce an alternative blockchain more valuable than the current one and replacing it [2].

Ethereum [3], made as a successor, introduced among other features such as the capability to execute programming code on Turing-complete languages, leading to the concept of "smart contracts". Through these digital contracts, it opened the way for new financial products, such as currencies on a unified platform, and after a period of community development, services like foreign exchanges and decentralised finances [4].

The financial industry has been researching blockchains for the period and continues to do so. Notable commercial blockchain projects include the Linux Foundation's Hyperledger [5], Consensys Quorum [6], and R3 Corda [7]. Some proprietary DL were adapted from public ones, while others were custom-built. These projects did not follow strictly the principles of Bitcoin and its derivative projects; they were designed with control over operations and operators. However, even these blockchains have advantages such as:

- Trusted and immutable transaction chain: provides historical records that are easy to audit at any given time, without requiring access to a private institution's database;
- Instant settlement: the automation of the reconciliation process;
- Availability and consistency: a participant can initiate a transaction without the receiver being online. The receiver gets the transaction information automatically once it is back and updates the information.

Standards play an important role in modern finances. A good example is ISO 20022 for financial messaging, which offers a wide range of standards for payments, cash management, security operations, and more. These documents are well-structured, easily verified by XML schemas, and can be efficiently processed by back-office applications. Notable technical committees include Cross-Border Payments and Reporting Plus (CBPR+), Real-Time Gross Settlement (RTGS), and Central Liquidity Management (CLM) [8].

In public blockchain projects, there is not a single leader dictating standards, and a similar scenario persists in the private blockchain sector. Currently, there are no established standards

[*] Corresponding author. E-mail: vadims.zilnieks@edu.rtu.lv
Article received 30.09.2023; accepted 8.11.2023

for distributed ledger technology (DLT) that could be utilized for the financial industry. SWIFT, the primary orchestrating organisation in banking, has not announced any; however, there is a report by SWIFT and Accenture discussing the potential future of payments in the context of distributed ledgers [9].

In addition to the above, the Central Bank Digital Currencies (CBDC) are worth mentioning. These are mostly developed at the national level, without the technical standardization. Examples include the digital Euro [10], digital Yuan [11], and a stable coin offered by the Australian National Bank [12]. "Stable coins" refer to electronic money on various platforms, usually in the form of cryptographic tokens pegged to a real-world currency and controlled by a trusted organisation. They are not as volatile as independent cryptocurrencies.

The current landscape of distributed ledgers presents a collection of independent domains. This fragmentation is one reason why ideas about the interconnection of DLs appeared in the last five years. Another motivation behind this trend is the issue of distributed ledger scalability.

The paper aims to systematise knowledge in the field of cross-chain bridges with a focus on financial application. The authors will attempt to present advantages and disadvantages of cross-chain bridges in their current variations.

Related works include systematic reviews of knowledge such as the paper by McCorry et al. [13], which addresses bridges and scalability issues; Robinson's survey of cross-chain protocols [14]; and Sung-shin Lee et al. review of security issues relating to cross-chain bridges [15]. As a source of information on available protocols, white papers of cross-chain bridge projects were utilised. These include the significant paper by Wood, which discusses the challenges in the current blockchain environment with a focus on scalability and interconnectivity through the Polkadot project [16], as well as technical documentation of Rainbow Bridge [17], DeBridge [18], and Cosmos [19].

Section II provides information on atomic swaps and payment channels. Section III discusses the fundamentals of tokens. The concept of cross-chain bridges, along with variations in topology, is presented in Section IV. Section V explores issues related to forks. The application of bridges in commercial projects is discussed in Section VI. Security issues are examined in Section VII. The paper ends with a final section that presents conclusions and directions for future research.

II. Atomic Swaps and Payment Channels

The method for connecting two heterogeneous distributed platforms involves the use of a smart contract with a fund-locking feature for a specific duration and an encrypted secret, known as an "atomic swap" [20]. The specific contract is called a Hash Time-Lock Contract (HTLC). The operational principle is shown in Fig. 1. A secret phrase or pre-image is transferred to counterparty, unlocking the transaction on the target platform, and the initiator does the same on the target platform. If one or both parties fail to fulfil their obligations, the contract is terminated after a predetermined period, ensuring security through the secret and the time constraint.

One advantage of this approach is its easy implementation on many blockchain platforms, even those without Turing-complete contracts, such as Bitcoin. Disadvantages include:

- Contract deployment: every new deal requires a new contract to be added to the ledger;
- Online requirement: both parties must be online and actively monitor the transaction;
- Potential freezing of funds: If one party fails to complete an obligation (e.g., intentionally), the funds of the counterparty will be frozen for the duration of the time-lock period.

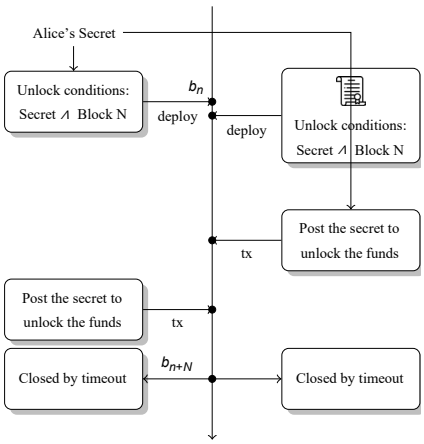

Fig. 1. Hash time-lock contract.

Despite these issues, the HTLC was highlighted as an example of cross-border payments between two DLs in a SWIFT report [9]. HTLCs are utilised in what are termed "payment channels", where funds are locked as a deposit for micro-transactions between two or more parties. These transactions are made off-chain, meaning they are not recorded on the main blockchain. Only the final result of the operation gets posted to the blockchain. Examples include the Lightning Network [21] and Raiden [22].

III. Token Basics

To understand the concept of cross-chain bridges, it is important to be familiarized with specific notations. While it is possible to transfer the embedded value units of each platform (like ethers in Ethereum), most use cases primarily utilise standardised tokens.

A token is a type of smart contract, mostly based on standard templates like ERC-20 or ERC-775 (using Ethereum terminology). These contracts come with inherited methods, such as "approve" and "transfer". The "approve" method allows a specific token amount to be marked for withdrawal by a certain participant, while the "transfer" method makes the actual movement of tokenized funds. Additionally, there are specialised contracts for tokens with mintable and/or burnable capabilities. This indicates that such tokens can be created ("minted") and, if needed, removed from circulation ("burned").

A wrapped token is a contract that creates an equivalent representation of a token from another platform. This equivalent does not exist on the current platform, however, can be used as if it does. A classic example of this is Wrapped Bitcoin (wBTC) on the Ethereum platform.

IV. Cross-chain Bridge

The concept of a protocol bridging two DLs has been under research in the past five years [13]–[16]. This research was largely motivated by the "blockchain trilemma" [23], which declares that only two out of the three core attributes can be achieved simultaneously: decentralisation, security, and scalability.

As decentralisation and security cannot be compromised for financial purposes, scalability is the primary challenge to address [24]. Possible solution search has two main directions: layer 2 solutions [25], [26] and cross-chain bridges. The term "layer 2" refers to a blockchain that operates independently of the main blockchain, however, remains connected to it via a gateway smart contract. Some argue that the contract connecting layer 1 and layer 2 functions as a cross-chain bridge. In that case, a cross-chain bridge can be defined as an abstract entity linking two or more independent DLs, whether they belong to the same platform or not.

Additional ledgers can, in theory, enhance the scalability of global networks. It is hard to imagine the scenario where all global financial institutions are connected to a single peer-to-peer network, attempting to achieve consensus at more than 10 000 transactions per second (tps)[2]. In such a context, it would be more efficient to have regional clusters, each with their own consensus mechanisms for high-frequency transactions. These groups could then be interconnected through bridges, producing less frequent transactions between them.

Key points for the desired solution include:

- Automation of transactions;
- Security of operations;
- Cost-effectiveness of the process.

There are several methods for the cross-bridge communication:

A. Protocol Integration

The scheme is illustrated in Fig. 2. A participant in the source blockchain intends to send a transaction to an account on the target blockchain. This is made by authorising a token transfer on the source platform, followed by a deposit operation on the source smart contract (bridge contract). The bridge contract on the target side then receives this information and must verify the transaction validity [14].

If the contract can utilise the logic of the source protocol, it acts as a "light client", validating both the Merkle proof and the block. Light client uses a set of algorithms for validating the blockchain without access to a full dataset. This approach is termed Simplified Payment Verification [27]. In contrast, full clients have a complete copy of the blockchain to perform important tasks like producing new blocks.

To verify the block validity, a partial version of the source blockchain is required. This can be executed within another smart contract that stores block headers.

A central component in the scheme is the "relayer", shown in the middle of the figure. The relayers connect to both platforms, transmitting information between them. This design eliminates the need for every participant on the source platform to also be a client of the target platform. Upon successful validation, new wrapped tokens are minted and transferred to the recipient. An example of this approach is the Rainbow Bridge [28].

The primary advantage of this approach is its transparency in both design and result. A contracted light client implements the functions of a standard client, utilising the same algorithms for block and transaction validation. It can be effectively tested. However, a drawback is the storage requirement for block headers, which can be expensive to maintain on the blockchain. This challenge can be partially solved by keeping only the minimal sequence of blocks necessary, depending on the external platform protocol.

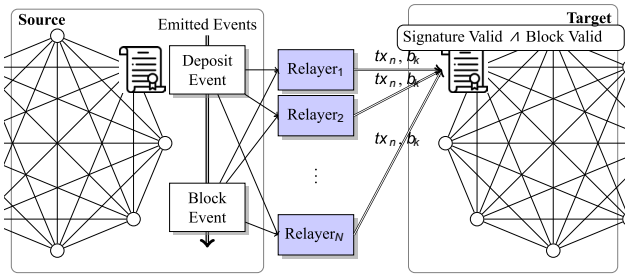

Fig. 2. Light client model.

B. Reduced Information Flow

Continuous block posting can be expensive, depending on the fee structure of the target network. A more efficient approach might involve sending only selected checkpoint blocks, based on the platform validation protocol, or only blocks containing bridged transactions. This system utilises a pool of validators who must approve and sign the source transaction. The bridge contract on the target then checks if the number of signers exceeds a predetermined threshold before

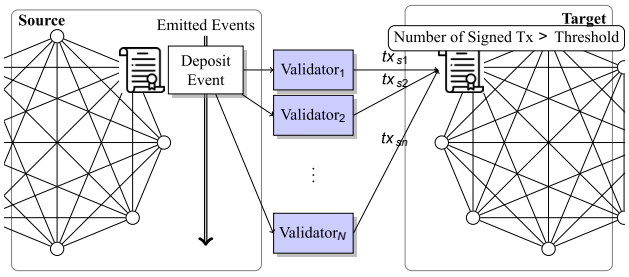

Fig. 3. Validators.

[2] Based on statistics from SWIFT: https://www.swift.com/about-us/discover-swift/fin-traffic-figures/swift-fin-traffic-document-centre

processing the transaction (see Fig. 3). This method eliminates the need for storing a copy of the external blockchain. While the previous approach relies on trust in relayers, this method requires trust in the validators. The transaction flow is decreased since there is

no need to transfer additional information like blocks' headers or cryptographic proofs. However, each validator still must post signed transaction.

To further optimise this process and consolidate it into a single transaction, a specific consensus model among validators can be adopted. Based on this consensus, validators will generate an approved transaction once they reach an agreement. This approach has similarities to validation in the Casper FFG protocol of Ethereum 2.0 [29], and PBFT-based protocols such as QBFT [30], and LibreBFT [31].

C. Zero-knowledge Flow

Another strategy to minimise data flow between interconnected platforms adopts zero-knowledge (ZK) proofs. This technique is implemented in Ethereum's zk-rollups [26]. Instead of transferring full transaction data, the information about transactions is condensed using ZK proofs. This provides proof that the transaction existed and was committed without needing the full dataset. The example of the scheme is shown in Fig. 4.

ZK proofs come with their own set of benefits and drawbacks. They reduce the amount of data transferred between

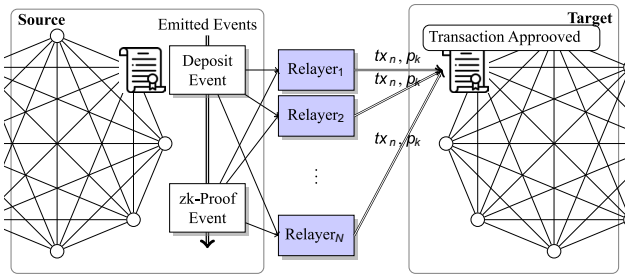

Fig. 4. Zero-knowledge model.

platforms; however, the validation of ZK proofs can be resource-intensive for smart contracts. This includes both mathematical computations and additional algorithmic segments needed for proofing [32]. If the platform verifier tools lack built-in decoding algorithms for a specific ZK solution, then that algorithm must be developed using the platform development kit, and the resulting smart contracts might require significant resources, leading to higher fees.

V. Forks

The validation of cross-chain transfers is just one aspect. Another important concept is "finality", which determines when a transaction can be considered finished. Different consensus mechanisms handle finality in various ways.

In proof-of-work (PoW) protocol [2], for instance, finality is probabilistic. Hypothetically, if a node is able to gain a majority of the computational power, it could create an alternative blockchain and replace the existing one. However, as the blockchain grows, this risk decreases. To achieve the accepted finality in PoW, a common approach is to wait for *N* subsequent blocks after a transaction's inclusion in the blockchain.

Other consensus mechanisms, like proof-of-stake (PoS) [33], achieve finality through staking. Here, the guarantee of finality is based on the amount of the stake and the potential penalties for malicious actors. In protocols like Ethereum 2.0 Casper FFG [26], finality is based on epoch checkpoints. Other projects can utilise voting for every block as a checkpoint, making transactions almost instantly final.

Forks in DL can be categorised into two main types: soft and hard. A soft fork is a logical state-splitting situation that appears as part of the distributed consensus process. For bridges, soft forks can be managed using artificial delays in block and/or transaction transfers between platforms. When dealing with probabilistic finality, a smart contract can introduce a "waiting" period for *N* blocks before initiating the next action, ensuring a more consistent state of data. In contrast, hard forks typically provide deeper structural changes [2].

Hard forks in the context of blockchain can be compared to version updates in traditional payment systems, such as the TARGET Instant Payment System (TIPS) releases [34]. In centralised systems, all participants must transition to the updated protocol version to continue operations. On the other hand, in decentralised systems, an upgrade functions similarly to a soft fork. It divides the blockchain. Participants operating on the previous version can persist and act like previously. Some notable examples of this include Litecoin [35] and Ethereum Classic [36].

Addressing the issues of hard forks is crucial for designing cross-chain bridges. That can introduce complexities in the logic of bridge contracts, as shown by marked links in the state machine (Fig. 5). Specifically, the links affected by hard forks

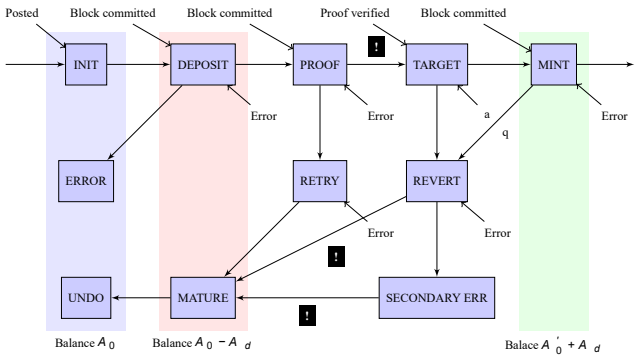

Fig. 5. State machine of bridge operations.

need vigilant observation. Several strategies can be applied to mitigate the risks associated with these forks:

- Announcement in private DLs: for private networks, hard forks are announced. This allows bridge developers to prepare for the impending changes, similar to the protocol in traditional payment systems.
- Updatable contracts: some contracts are designed to be upgradable, allowing developers to change the contract

code without migrating state. OpenZeppelin provides libraries and standards that support this feature [37].

- Proxy contracts: this approach involves a main contract that delegates calls to other contract implementations, allowing for logic to be changed by switching the delegate [38].
- Decoupling contract logic: by breaking up a contract into modular parts, it is possible to update only certain components without affecting the whole system [38].

VI. Bridges for Commercial Projects

Private blockchains offer a specific landscape compared to their public counterparts, primarily due to the absence of the trustless component. In private networks, financial institutions trust certified entities, mirroring the trust structures in centralised payment systems. This opens the door for alternative consensus mechanisms, like proof-of-authority (PoA) [39], to replace commonly used protocols like PoW or PoS. As a result, finality, a challenge in most public blockchains, becomes less impactive in a private environment. PoA permits only authorised participants to create new blocks. If there is more than one such authority, the first to sign will produce the new block [39].

Furthermore, transaction costs in private networks are structured differently. Instead of being dictated by competition, as in public blockchains, fees in private blockchains are typically lower. This offers some flexibility, ensuring that the process of data transfer and the volume of transactions in bridging operations do not constrain so much.

However, private blockchains introduce their own set of challenges. A group of private platforms, such as Hyperledger or Corda, do not operate on virtual machines like Ethereum Virtual Machine (EVM). This can create challenges when attempting to establish bridges with them and EVM-based networks like Quorum [6] and Besu [5].

The state machine that represents the cross-chain transfer is shown in Fig. 5. The states and transitions are detailed in Table I.

The total duration required for a cross-chain operation is influenced by several factors, each contributing a specific duration to the overall process:

- Source blockchain commitment: this is the time taken for the source blockchain to register or commit the cross-chain transaction ("Deposit" state in Fig. 5).
- Finality duration: this refers to the period required for the transaction to achieve finality. In other words, it is the time taken to ensure that the transaction will not be reversed or changed.
- Relay latency: this concatenates the time taken by the relay mechanism (or the relayer) to recognise and relay the transaction from the source blockchain to the target blockchain.
- Target contract execution: once the transaction has been relayed, the target blockchain must execute the necessary actions, such as minting new tokens or unlocking existing ones ("Target" state in Fig. 5).

Depending on the specific bridging model and its complexity, additional durations may need to be included. For instance, if the process involves submitting cryptographic proofs, validations, or any other additional steps, the time taken for each of these actions must also be added to get the complete operation duration.

Considering instantaneous finality of PoA, the total execution time of a cross-chain transaction will summarise the block generation times of both the involved platforms and the synchronisation duration of the middle agents. This shows that, in an ideal scenario, a cross-chain operation could take 2-3 times longer than a transaction made on a single distributed ledger.

TABLE I
Cross-Chain Bridge State Machine

State	Description	Success Condition	On Success	On Error
INIT	Transaction initiated by user's application	Hash of transaction returned	DEPOSIT	ERROR
ERROR	Transaction not sent; balance unchanged	-	-	-
DEPOSIT	Token deposit to the source bridge contract	Block mined (Event)	PROOF	RETRY
RETRY	User can retry deposit	Deposit successfully made	PROOF	WITHDRAWAL
WITHDRAWAL	User initiates deposit maturity	Block mined	UNDO	
UNDO	Transaction reversed; deposit returned	Block mined	-	-
PROOF	Awaiting proof of the transaction	No errors and proof relayed	TARGET	RETRY
RETRY	Attempt to post proof until accepted	No errors and proof relayed	TARGET	WITHDRAWAL
TARGET	Checking the transaction and proof on target bridge	Transaction relayed, proof correct, and block valid	MINT	REVERT
REVERT	Transfer is reverted to source	Refund is relayed to the source	WITHDRAWAL	SECONDARY ERROR
SECONDARY ERROR	Manual intervention required. User must use tools to return transaction, possibly with proof and error code	Refund is relayed to the source	WITHDRAWAL	
MINT	Awaiting final transaction	Block mined	Finish	REVERT

This abstract duration, however, is not comparable to traditional cross-border payment methods, such as those routed through the SWIFT network. The latter, characterised by its multiple actions involving intermediary correspondent banks,

can prolong transactions to durations of days or even weeks. These delays are caused by the nature of intermediaries, each having its own operational hours and processing times.

Cross-chain transactions appear rapid, moving more closely to the speed and efficiency of instant payment systems such as the TIPS operational within the Eurozone. However, TIPS functionality is geographically restricted, and, for instance, there currently is not a direct integration with the US instant payment mechanisms [40].

This presents a great advantage for blockchain-based systems. Let us consider a scenario: A commercial bank in Latvia, participating in a future European DL payment system (perhaps even CBDC "digital Euro"), can seamlessly proceed a payment to a US bank. This transaction, made via a bridge to platforms like Corda, can be completed in seconds. The process would involve the Euro amount being temporarily locked in the European bridge contract, followed by a transfer of wrapped Euros to the recipient bank in the US.

Such a capability accelerates cross-border transactions and removes geographic barriers. With regard to such advantages, it is not hard to see why blockchain and cross-chain bridges can represent the future of global financial transactions.

VII. Middle Agents and Security Issues

Centralising functionalities or tasks can introduce security issues, especially in decentralised systems where the core element is trustlessness [15]. Relayers or other middle agents in cross-chain bridges play a pivotal role and introduce potential vulnerabilities.

Relayers, by design, act as the conductor between two blockchains in many bridge implementations. If not designed securely, relayers can exploit flaws in smart contracts or validation mechanisms to own locked funds or disrupt the bridging process [14], [15].

To counterbalance the power of relayers and validators, some systems introduce independent entities known as watchdogs or fishermen [13], [16]. Their primary role is to monitor the relayer' actions and ensure they are acting in the network best interests. In the event of malicious behaviour, these entities can report the activity, and in return, receive a reward. However, this mechanism is not ideal. If malicious actions are infrequent, these watchdog entities might not be motivated enough to continuously monitor, especially if they are not being compensated. Also, their effectiveness can be low if there are only a few watchdogs. If these entities go offline or are compromised, malicious activities might go unchecked.

In cross-chain bridges that connect multiple platforms, there appears the possibility of mixing wrapped tokens from various chains. These tokens, while theoretically representing the same asset, might originate from different platforms, making it challenging to differentiate or trace them. This is an open question [15].

Regular audits of bridge contracts are essential. Expert auditors can identify vulnerabilities in the smart contract code, ensuring a higher level of security. Though audits do not guarantee absolute security, they significantly reduce the risk of known issues [13].

While these approaches can mitigate the risks, they might not offer full-proof solutions. Therefore, constant monitoring and audits are crucial in the rapidly growing area of DLT.

VIII. Conclusions

The evolution of payment systems has always been closely tied to the formulation and adoption of international standards. This process is illustrated in the implementation of ISO 20022 formats with CLM, RTGS, and CBPR+ initiatives.

Distributed ledger technology presents a bias from this pattern. In the absence of universal standards, financial groups are making individualized research and developing unique projects, whether based on open-source foundations or proprietary designs. This individualistic approach has produced the modern landscape of standalone projects.

The global trend of central bank digital currencies further complicates the landscape, enlarging the diversity of digital platforms and systems.

It is becoming clear that the future of financial systems will be anchored in a heterogeneous environment. To ensure effective operations within this environment, the mentioned systems must be seamlessly interconnected. While atomic swaps offer one solution, their ability for automation remains limited.

Cross-chain bridges appear to be the more promising technology. Following an observable pattern of DLT, public initiatives often present solutions, which are later adapted by the financial industry. This trend is seen in how Ethereum's infrastructure has been implemented for private payment systems. Similarly, public bridge projects, either in their original form or with some modifications, may find application in commercial use.

Unlike their public counterparts, private bridges have specific advantages. The elimination of the need for a trustless model simplifies operations. Moreover, removing the proof-of-work protocol and its probabilistic finality accelerates the bridging process.

These advantages come with the security challenges, questions around relayers and validators, the maintenance of smart contracts, and the handling of forks remain pressing.

Despite these challenges, the perspectives of cross-chain bridges are promising. We posit that this technology will play a central role in shaping the global payment systems of the future, preserving the benefits of distributed ledgers while ensuring more scalability and efficiency.

Future directions include the monitoring of existing and new trustless cross-chain bridge projects, which are a primary source for private project implementations. Additionally, efforts are directed towards forecasting the potential standardisation of cross-chain bridges and searching for the most efficient models of financial asset interoperability with a focus on security and scalability.

Abbreviations:

CBDC - Central Bank Digital Currency
CBPR+ - Cross-Border Payments and Reporting Plus
CLM - Central Liquidity Management
DL - Distributed Ledger
DLT - Distributed Ledger Technology
EVM - Ethereum Virtual Machine
HTLC - Hash Time-Lock Contract
PoA - Proof of Authority
PoS - Proof of Stake
PoW - Proof of Work
RTGS - Real-Time Gross Settlement
SWIFT - Society for Worldwide Interbank Financial Telecommunication
TARGET - Trans-European Automated Real-time Gross Settlement Express Transfer System
TIPS - TARGET Instant Payment System
ZK – Zero-knowledge

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009. [Online]. Available: https://bitcoin.org/bitcoin.pdf. Accessed on: Sep. 17, 2023.
[2] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *IEEE P2P 2013 Proceedings*, Trento, Italy, Sep. 2013, pp. 1–10. https://doi.org/10.1109/P2P.2013.6688704
[3] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, 2014. [Online]. Available: https://gavwood.com/paper.pdf
[4] D. A. Zetzsche, D. W. Arner, and R. P. Buckley, "Decentralized finance (DeFi)," *Journal of Financial Regulation*, vol. 6, no. 2, pp. 172–203, Sep. 2020. https://doi.org/10.1093/jfr/fjaa010
[5] Hyperledger, "Hyperledger Besu Ethereum client," 2022. [Online]. Available: https://besu.hyperledger.org/en/stable/. Accessed on: Sep. 17, 2023.
[6] Consensys, "A trusted, open source foundation for your blockchain solution," 2023. [Online]. Available: https://consensys.net/quorum/. Accessed on: Sep. 17, 2023.
[7] R3, "Capitalize on the new digital economy – Transact openly and securely, at scale," 2023. [Online]. Available: https://r3.com/products/corda/. Accessed on: Sep. 17, 2023.
[8] International Organization for Standardization, "Technical committees," 2023. [Online]. Available: https://www.iso.org/technical-committees.html. Accessed on: Sep. 17, 2023.
[9] SWIFT, "Exploring central bank digital currencies: How they could work for international payments," 2021. [Online]. Available: https://www.paymentscardsandmobile.com/wp-content/uploads/2021/05/Exploring-CBDC-for-International-Payments.pdf
[10] European Central Bank, "Progress on the investigation phase of a digital euro – Third report," 2023. [Online]. Available: https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov230424_progress.en.pdf. Accessed on: Sep. 17, 2023.
[11] C. Mu, "Theories and practice of exploring China's e-CNY," in *Data, Digitalization, Decentialized Finance and Central Bank Digital Currencies: The Future of Banking and Money*, A. Dombret and P. S. Kenadjian, Eds. Berlin, Boston: De Gruyter, 2023, pp. 179–190. https://doi.org/10.1515/9783111002736-013
[12] National Australia Bank, "NAB completes world-first with cross-border stablecoin transaction," 2023. [Online]. Available: https://news.nab.com.au/news_room/nab-completes-world-first-with-cross-border-stablecoin-transaction/. Accessed on: Sep. 17, 2023.
[13] P. McCorry, C. Buckland, B. Yee, and D. Song, "SoK: Validating bridges as a scaling solution for blockchains," Cryptology ePrint Archive, Paper 2021/1589, 2021. [Online]. Available: https://eprint.iacr.org/2021/1589. Accessed on: Sep. 17, 2023.
[14] P. Robinson, "Survey of crosschain communications protocols," *Computer Networks*, vol. 200, Dec. 2021, Art. no. 108488. https://doi.org/10.1016/j.comnet.2021.108488
[15] L. Sung-Shine, A. Murashkin, M. Derka, and J. Gorzny, "SoK: Not quite water under the bridge: Review of cross-chain bridge hacks," in *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Dubai, United Arab Emirates, May 2023, pp. 1–14. https://doi.org/10.1109/ICBC56567.2023.10174993
[16] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," *White Paper*, vol. 21, no. 2327, 2016, Art. no. 4662. [Online]. Available: https://assets.polkadot.network/Polkadot-whitepaper.pdf
[17] Near Foundation, "ETH-NEAR rainbow bridge," 2020. [Online]. Available: https://near.org/blog/eth-near-rainbow-bridge/. Accessed on: Sep. 17, 2023.
[18] deBridge, "deDocs: Protocol overview," 2023. [Online]. Available: https://docs.debridge.finance/the-core-protocol/protocol-overview. Accessed on: Sep. 17, 2023.
[19] J. Kwon and E. Buchman, "A network of distributed ledgers," 2019. [Online]. Available: https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md. Accessed on: Sep. 17, 2023.
[20] M. Herlihy, "Atomic cross-chain swaps," in *Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing*, Jul. 2018, pp. 245–254. https://doi.org/10.1145/3212734.3212736
[21] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," 2016. [Online]. Available: https://lightning.network/lightning-network-paper.pdf. Accessed on: Sep. 17, 2023.
[22] Raiden Network, "What is the Raiden Network?" 2020. [Online]. Available: https://raiden.network/101.html. Accessed on: Sep. 17, 2023.
[23] V. Buterin, "The Ethereum trilemma," 2023. [Online]. Available: https://vitalik.ca/general/2021/04/07/sharding.html. Accessed on: Sep. 17, 2023.
[24] C. Smith, "Scaling," 2023. [Online]. Available: https://ethereum.org/en/developers/docs/scaling/. Accessed on: Sep. 17, 2023.
[25] Ethereum Foundation, "Optimistic rollups," 2023. [Online]. Available: https://ethereum.org/en/developers/docs/scaling/optimistic-rollups/. Accessed on: Sep. 17, 2023.
[26] Ethereum Foundation, "Zero-knowledge rollups," 2023. [Online]. Available: https://ethereum.org/en/developers/docs/scaling/zk-rollups/. Accessed on: Sep. 17, 2023.
[27] Bitcoin Wiki, "Simplified payment verification," 2023. [Online]. Available: https://wiki.bitcoinsv.io/index.php/Simplified_Payment_Verification. Accessed on: Sep. 17, 2023.
[28] Aurora, "How the rainbow bridge works," 2021. [Online]. Available: https://aurora.dev/blog/2021-how-the-rainbow-bridge-works. Accessed on: Sep. 17, 2023.
[29] V. Buterin and V. Griffith, "Casper the friendly finality gadget," arXiv:1710.09437, Jan. 2019. https://doi.org/10.48550/arXiv.1710.09437
[30] Enterprise Ethereum Alliance, "QBFT blockchain consensus protocol specification v1," 2023. [Online]. Available: https://entethalliance.org/specs/qbft/. Accessed on: Sep. 17, 2023.
[31] LibraBFT Team, "State machine replication in the Libra blockchain," 2020. [Online]. Available: https://developers.diem.com/papers/diem-consensus-state-machine-replication-in-the-diem-blockchain/2020-04-09.pdf
[32] Y. Bespalov, A. Garoffolo, L. Kovalchuk, H. Nelasa, and R. Oliynykov, "Probability models of distributed proof generation for zk-SNARK-based blockchains," *Mathematics*, vol. 9, no. 23, Nov. 2021, Art. no. 3016. https://doi.org/10.3390/math9233016
[33] L. Pennella, "Proof-of-stake (PoS)," 2023. [Online]. Available: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/. Accessed on: Sep. 17, 2023.
[34] European Central Bank, "TIPS changes and new releases for professional use," 2023. [Online]. Available: https://www.ecb.europa.eu/paym/target/tips/profuse/html/index.en.html. Accessed on: Sep. 17, 2023.
[35] Litecoin, "The future of money," 2023. [Online]. Available: https://litecoin.com/. Accessed on: Sep. 17, 2023.
[36] Ethereum Classic, "The original Ethereum," 2023. [Online]. Available: https://ethereumclassic.org/. Accessed on: Sep. 17, 2023.

[37] OpenZeppelin, "Writing upgradeable contracts," 2023. [Online]. Available: https://docs.openzeppelin.com/upgrades-plugins/1.x/writing-upgradeable. Accessed: Sep. 17, 2023.
[38] M. Hajizadeh, "Upgrading smart contracts," 2023. [Online]. Available: https://ethereum.org/en/developers/docs/smart-contracts/upgrading/. Accessed: Sep. 17, 2023.
[39] P. Szilagyi, "EIP 225: Clique proof-of-authority consensus protocol," 2017. [Online]. Available: https://eips.ethereum.org/EIPS/eip-225. Accessed: Sep. 17, 2023.
[40] Federal Reserve, "FedNow service participants and service providers," 2023. [Online]. Available: https://www.frbservices.org/financial-services/fednow/organizations. Accessed: Sep. 17, 2023.

Vadims Zilnieks obtained a Master's degree in Computer Science from Riga Technical University in 2004 and a professional Master's degree in Finance from the BA School of Business and Finance in 2014. Currently, he is engaged in a Ph.D. at Riga Technical University. Vadims also contributes as an expert in payments and settlements at a Latvian commercial bank. Merging academic rigour with industry insights, he delves deep into optimising instant payment strategies within the realm of Distributed Ledger Technology.
E-mail: vadims.zilnieks@edu.rtu.lv
ORCID iD: https://orcid.org/0009-0005-5149-1107

Ingars Erins acquired both his Master's and Ph.D. degree from Riga Technical University. From 2014 to 2017, he worked as an Associate Professor. Since 2017, he has been holding the position of Professor at the Department of Artificial Intelligence and Systems Engineering. In 2018, he embraced the role of a Senior Researcher. His research predominantly orbits around AI-centric solutions and avant-garde computing paradigms.
E-mail: ingars.erins@rtu.lv
ORCID iD: https://orcid.org/0000-0003-0138-2277