Towards Solving the Blockchain Trilemma: An Exploration of Zero-Knowledge Proofs

Marc Principato
University of Bayreuth, marc.principato@fim-rc.de

Matthias Babel
University of Bayreuth, matthias.babel@fim-rc.de

Tobias Guggenberger
University of Bayreuth, tobias.guggenberger@fim-rc.de

Julius Kropp
University of Bayreuth, julius.kropp@fim-rc.de

Simon Mertel
University of Bayreuth, simon.mertel@fim-rc.de

Towards Solving the Blockchain Trilemma: An Exploration of Zero-knowledge Proofs

Completed Research Paper

Marc Principato
FIM Research Center for Information Management,
University of Bayreuth
Bayreuth, Germany
marc.principato@fim-rc.de

Matthias Babel
Branch Business & Information Systems Engineering of the Fraunhofer FIT
Bayreuth, Germany
matthias.babel@fit.fraunhofer.de

Tobias Guggenberger
FIM Research Center for Information Management, University of Bayreuth
Bayreuth, Germany
tobias.guggenberger@fim-rc.de

Julius Kropp
FIM Research Center for Information Management, University of Bayreuth
Bayreuth, Germany
julius.kropp@fim-rc.de

Simon Mertel
FIM Research Center for Information Management, University of Bayreuth
Bayreuth, Germany
simon.mertel@fim-rc.de

Abstract

Research on blockchain has found that the technology is no silver bullet compared to traditional data structures due to limitations regarding decentralization, security, and scalability. These limitations are summarized in the blockchain trilemma, which today represents the greatest barrier to blockchain adoption and applicability. To address these limitations, recent advancements by blockchain businesses have focused on a new cryptographic technique called "Zero-knowledge proofs". While these primitives have been around for some time and despite their potential significance on blockchains, not much is known in information systems research about them and their potential effects. Therefore, we employ a multivocal literature review to explore this new tool and find that although it has the potential to resolve the trilemma, it currently only solves it in certain dimensions, which necessitates further attention and research.

Keywords: Zero-knowledge Proof, Blockchain, Trilemma

Introduction

Since their emergence, blockchains have disrupted many industries by providing a new way of trustless data storage and data sharing (Lu 2019). Subsequently, many works have explored this new technology, its applications, benefits, and limitations. However, its main use case remains as a public infrastructure for various crypto assets, such as native cryptocurrencies like Bitcoin and Ether or various forms of tokens (e.g.,

ERC-20 and ERC-721) (Crosby et al. 2016). Today, blockchain is fundamentally researched, and it is well known that blockchains still provide no silver bullet for many applications (Iansiti et al. 2017).

One of the main theoretical constructs that emerged as a tool to illustrate this circumstance is the blockchain trilemma. The trilemma refers to the fact that the implementation of blockchains has to make a trade-off between decentralization, security, and scalability (Hafid et al. 2020). For example, public permissionless blockchains like Bitcoin allow anyone to actively participate and maintain the network. Thus, they are reasonably decentralized due to a large number of different participants and, thanks to the use of the Proof of Work consensus mechanism, are also secure against malicious attacks such as the Byzantine Fault (Nakamoto 2008). However, they suffer scalability limitations, resulting in longer transaction times and higher fees during periods of high demand (Zhou et al. 2020). Contrastingly, private permissioned blockchains, such as Hyperledger Fabric, allow only selected participants to join and further restrict the ability to maintain the network. This reduces the decentralization of the network while also reducing security through the use of less robust consensus mechanisms such as Proof of Authority, which are vulnerable to malicious attacks and, in some cases, are not even resilient to the unavailability of individual network participants, also known as Crash Fault Tolerant (Ekparinya et al. 2019). This reduces the complexity of adding new transactions to the ledger, resulting in higher transaction throughput and lower network latency for improved scalability (Guggenberger et al. 2022). These examples illustrate the tension that current blockchain solutions face and that two of the three dimensions are reachable, but not all three at the same time.

The focus on mainly two of the three dimensions of the trilemma ultimately limits the applicability of blockchain technology (Buterin 2021b). We find this, for example, with Ethereum, which experienced increased usability problems due to scalability limitations associated with the Ethereum virtual machine (EVM) (Chauhan et al. 2018). The EVM allows deploying decentralized applications on top of the blockchain, where increased demand for computational resources by its prominent application, CryptoKitties, started to paralyze the entire network (Smith 2022). The EOS blockchain aimed to overcome the scalability issues of Ethereum without compromising on the other features, yet leading to decreased decentralization, security issues, and ultimately the project's failure (Binance 2020; CoinMarketCap 2021). Therefore, to realize blockchain's transformative potential across industries and applications, it is imperative to explore innovative solutions that holistically address the trilemma, facilitating a more seamless integration of blockchain technology and, ultimately, mass adoption in many different applications.

Recent developments in the blockchain industry started to explore a cryptographic tool called "zero-knowledge proof" (ZKP) indicating that ZKPs might allow for blockchains to defy the limitations of the trilemma (Buterin 2021b, 2023; Titus 2022). Consequently, many projects are emerging, making use of ZKPs to address blockchain limitations (Chainlink 2022). For example, the “Aztec” protocol, developed by Aztec Network, claims to provide both scalability and security without compromising on decentralization by using an architecture based on two ZKPs (Aztec 2023). Further, Ethereum’s roadmap envisions the use of ZKPs to address its pressing scalability limitations without negatively affecting security and decentralization (Buterin 2020; Ethereum 2023a).

The foundational concept of zero-knowledge (ZK) and associated proofs have been around since 1985 in computer science (CS) (Goldwasser et al. 1985). While both blockchains and ZKPs originate from the field of CS and could have a significant impact on information systems (IS), there is currently a wider range of research on blockchains in IS research but hardly any on ZKPs. As a result, the application of blockchains is very well understood, but the phenomenon of the increasing use of ZKPs in this field remains unexplored. To the best of our knowledge, Sun et al. (2021) are the first and only ones that cover the topic with a concrete focus on applications. Although their work serves as a good summary, they remain rather broad and employ no scientific review method and thus do not provide an appropriate overview of the current state of knowledge. Consequently, there is a research gap with significant importance for IS research as ZKPs may enable blockchains to defy their applicational limitations, which are still constrained by the tension between decentralization, scalability, and security.

The goal of this study is to explore how ZKPs are used in blockchains by examining their impact on the trilemma dimensions and the reason for their current attention. This will be achieved by answering the following research question:

RQ – How and why are ZKPs applied to blockchains?

We employ a literature review for synthesizing and structuring the relevant knowledge about ZKPs from the field of CS and apply it to IS by using it to answer our research question and to assess how ZKPs impact the dimensions of the trilemma. Thereby, our aim is to introduce the technical topic of ZKPs from CS to IS for more application orientation in further ZKP research and to provide a foundational understating of their potential impact on blockchains. As such, this paper makes an important contribution to the field of IS research, highlighting the potential impact of ZKPs on blockchain technology. By exploring the origins and benefits of ZKPs in blockchain applications, we shed light on the common roots and interrelated development of both technologies. Our study indicates that the ability of ZKPs may assist in addressing limitations of blockchains by resolving trade-offs within the trilemma. Therefore, potentially allowing for achieving an ideal balance between the three dimensions. This calls for a comprehensive re-evaluation of the previous claims made in blockchain research. Ultimately, we argue that recent advances in ZKP technology have the potential to revolutionize the blockchain landscape, reshaping our understanding of what can be achieved in decentralized systems. Yet, further research is needed, especially concerning the application of ZKPs on the decentralization dimension of blockchains.

Background

Blockchain technology

The emergence of blockchains can be dated back to the publication of the Bitcoin whitepaper by the pseudonymous author Satoshi Nakamoto (Nakamoto 2008). The technology incorporates previously existing cryptographical concepts to form a distributed, synchronized, append-only ledger.

Each node in the blockchain network has an identical copy of the blockchain (i.e., ledger) in the initial position. If new transactions are made, they are signed by asymmetric encryption and sent to all nodes in the P2P network. A subset of nodes, called validators or miners, batches the raw transactions and their hash (i.e., the output of a cryptographic hash function) in a block (Nakamoto 2008). The transaction hashes get combined and hashed in a Merkle tree, which results in a "hash of hashes" that is a concatenation of all the individual transaction hashes and is called Merkle root (Merkle 1988; Nakamoto 2008). The Merkle root, the block's metadata, and the previous block hash will then be used as inputs to a hash function, which will output the header of the current block. This process concatenates the current block with the previous block (Nakamoto 2008). A consensus mechanism now decides who is authorized to create the new block and what requirements the block must fulfill (Butijn et al. 2020). The miner sends the new block to all nodes via the P2P network, where it is locally checked by each node against the requirements. If these are met, and the block is validated by the nodes, there is consensus, and the block is added to every individual ledger and, thus, the blockchain.

This mode of concept enables the blockchain to serve as a protocol for creating trust in a peer-to-peer network, on top of which many decentralized applications have emerged. One step further, Ethereum, with its distributed state machine, the EVM, enables arbitrary programs to run in a decentralized environment on top of the blockchain infrastructure. These programs are typically called "smart contracts" and are snippets of code that can receive function calls via transactions. A new contract state is calculated in a similar decentralized fashion by nodes locally verifying transactions and verifying the contracts' function execution.

Previous works have shown that the blockchain is no silver bullet and that its potential is limited by the inherent properties of the technology itself. The blockchain trilemma is a widely used concept in IS research that aims to describe this circumstance (Del Monte et al. 2020) and to provide a comprehensive understanding of the limitations, potentials, and trade-offs involved in practical blockchain applications (Guggenberger et al. 2022; Kannengießer et al. 2021). It highlights the challenges that arise from balancing the conflicting properties of a blockchain system for practical implementations.

The three competing goals that blockchain systems strive to achieve are security, scalability, and decentralization. The term "security" in the context of blockchain pertains to its capacity to thwart deceitful transactions and maintain the integrity and tamper-resistance of the data stored on the blockchain, according to Zhang et al. (2020). Meanwhile, "scalability" refers to the blockchain's capability to manage a significant volume of transactions while reducing the potential impact of storage and throughput

limitations that may cause bottlenecks (Chauhan et al. 2018). Lastly, "decentralization" pertains to the blockchain's ability to be dispersed among numerous nodes, which prohibits any single entity from exercising excessive control or influence over the system (Beck et al. 2017). The rule of the trilemma is that only two of these goals can be achieved simultaneously (Buterin 2021b). Therefore, the trilemma represents the current unsolved challenges of blockchain technology with regard to its usability and broad adoption. Limited scalability reduces user-friendliness and the potential of a blockchain platform to support a growing user base (Buterin 2021b).

In addition, there is a growing demand for privacy solutions for blockchains, with no solution in sight that is closely related to the blockchain trilemma's dimensions (Bernal Bernabe et al. 2019). Encrypting sensitive data seems like an obvious answer to this problem. However, if relevant data is encrypted, nodes cannot deterministically reach an agreement on the state of the blockchain, which leads to decreased security (Cachin and Vukolić 2017). Privacy can be achieved to some degree by restricting access to the ledger, as it is common in private blockchains (Ncube et al. 2020). However, achieving privacy without compromising on the trilemma's goals has been an ongoing research effort.

Zero-knowledge proofs

ZKPs are a cryptographic technique that allows a party (the prover) to prove to another party (the verifier) that a statement is true without revealing any additional information beyond the validity of the statement itself. ZKPs originated from the field of theoretical CS within the seminal paper of Goldwasser et al. (1985), who first introduced the concept of "zero-knowledge" and interactive proof systems. As such, a ZKP is defined as a proof system that conforms to the following three properties:

- *Completeness*
  If the statement to be proven is true, an honest verifier will always be convinced by a prover of its truth.
- *Soundness*
  No prover may (most probably) ever convince an honest verifier to try to prove a false statement.
- *Zero-knowledge*
  The proof does not reveal any additional information about the statement beyond its validity.

As outlined in the initial paper, the main reasons for research on ZKPs were use cases in other cryptographic primitives (Goldwasser et al. 1985). These proofs were initially envisioned as a solution to the problem of secure communication and authentication over unsecured networks and were used in identification protocols to interactively prove knowledge of a private key corresponding to a certain public key (Feige et al. 1988; Fiat and Shamir 1987; Schnorr 1990). Furthermore, Fiat and Shamir (1987) introduced a heuristic with the use of random oracles (in practice: hash functions) for transforming these ZKPs into signatures. While initially limited to interactive proof systems due to the need to repeatedly generate challenges by the verifier and according to responses by the prover, Blum et al. (1988) introduced the variant of non-interactive zero-knowledge proofs by using a common reference string. The reference string is a "source of randomness" shared between the prover and the verifier that contains random bits from which the challenges are predetermined, eliminating the need for interactivity (Blum et al. 1988). This mode of transforming interactive ZKPs into non-interactive ZKPs is commonly known today as the common reference string (CRS) model, which generalizes the generation of such a random string either with public parameters (Uniform Random String) or using secret parameters (Structured Reference String) (ZKProof 2022). Similarly, the Fiat-Shamir Transform can be used, but only on commit-challenge-prove ZKPs (i.e., Σ-Protocols), to replace the challenge with a random oracle (Random Oracle Model) (Bellare and Rogaway 1993). The generation of these initial parameters to construct a non-interactive ZKP is called setup. The parameters are used to calculate the non-interactive proof; If the parameters are secrets, homomorphic encryption is employed for the calculation to avoid revealing them.

Commitments are common building blocks of ZKPs, ensuring the integrity and confidentiality of the objects about which statements are to be proven (Bünz et al. 2018). These commitments provide a way to perform the ZKP-proving procedures on top of them, thereby proving knowledge of the value without revealing the value itself (ZKProof 2022). Most importantly, they offer two properties vital for the proving system (Alupotha et al. 2022; Poelstra 2016):

- *Perfectly hiding:* an adversary cannot learn anything about the committed value based on the

commitment alone, even if they have unlimited computational power. This ensures that the prover can commit to a value without revealing any information about it.

- *Computationally binding:* it is computationally infeasible to calculate a different value resulting in the same commitment, and therefore the prover cannot change their commitment retroactively.

By making ZKPs non-interactive, they have become more applicable to a wide range of use cases (Wu and Wang 2014). Most of the recent research on ZKPs, therefore, focuses on improving non-interactive ZKP schemes, leading to the development of the currently most popular protocols: succinct non-interactive arguments of knowledge (SNARKs) (Bitansky et al. 2012), Bulletproofs (Bünz et al. 2018), and scalable transparent arguments of knowledge (STARKs) (Eli Ben-Sasson et al. 2018). Bulletproofs and STARKs use building blocks, like Merkle commitments making use of hash functions (Eagen 2022) that enable them to generate the proofs without secrets and, therefore, do not need a trusted setup (Li et al. 2022).

Methodology

Research method selection

Given that there is an active and relevant CS and math-oriented research stream on ZKPs in blockchains, we conduct a literature review to identify, summarize, and synthesize this existing knowledge from an IS perspective. We thereby aim to transfer the knowledge to the field of IS, fill the research gap, and reveal the effect of ZKPs on blockchains to answer our research question. To achieve this, we make use of a systematic literature review (SLR), which is especially useful when aiming to synthesize and structure an existing body of knowledge in a field of inquiry (Webster and Watson 2002). However, SLRs typically only focus on academic literature (AL), such as peer-reviewed conferences and journals, and might exclude relevant literature from practitioners and other non-scholarly sources, commonly referred to as grey literature (GL) (Farace and Schöpfel 2010). This arguably reduces the quality of literature reviews, especially in CS-related areas of inquiry (Garousi et al. 2016, 2019; Kamei et al. 2021). Against this background, we chose to conduct a multivocal literature review (MLR), following the process of Garousi et al. (2019), because we see additional benefits in including grey literature, such as preventing publication bias (Kitchenham and Charters 2007). GL items come in handy when covering novel research fields and research fields in which developments are also driven by practitioners (Kamei et al. 2021). Since blockchains are decentralized and developments are often community-driven, we further argue that an MLR is an optimal method for our research endeavor that aims to cover exactly this interaction between practice-driven and scholarly advancements regarding the concept of ZKPs (Gramlich et al. 2023). The MLR process by Garousi et al. (2019) extends the well-established SLR process of Kitchenham and Charters (2007) for GL and thus provides a pre-defined approach for identifying relevant AL and GL to answer our research question.

Multivocal literature review

Following the approach of Kitchenham and Charters (2007), we started by developing a search string that enabled us to query items regarding our topic in scholarly databases. We initiated the development by collecting relevant and related terms via searches in GoogleScholar and Elicit.org for the terms "Cryptocurrency" and "Zero-knowledge" respectively. By constructing different search strings, we could obtain and test different base samples that also allowed us to obtain new terms for further developed strings. New variations of search strings resulting from new terms were hereby iteratively sample-tested regarding the quality of hits in databases and the inclusion rate of items. The resulting search string is:

(("Blockchain" OR "Cryptocurrency" OR "Token" OR "Decentralized Finance")
AND ("Zero-knowledge" OR "Zero knowledge")).

At the start of January 2023, we applied this string to query the following four well-established and reputable databases for AL: ACM Digital Library, AIS e-Library, IEEE Xplore, and Web of Science (Chen et al. 2010). Thereby, we obtained an initial set of 1106 items.

To refine the sample, we defined inclusion and exclusion criteria applied in the title, abstract, and full-text filters (Garousi et al. 2019; Kitchenham and Charters 2007). Items that (I1) explore the concept of ZK in blockchains, (I2) are published in peer-reviewed journals or conferences, (I3) and have accessible full-texts were included. We excluded items that (E1) do not contribute to the state of knowledge (i.e., only mention

the topic briefly) or (E2) are not written in English. Finally, we performed backward and forward searches to broaden our item set with relevant literature that is then evaluated in the same filter processes (Webster and Watson 2002). Our final set contains 30 AL items.

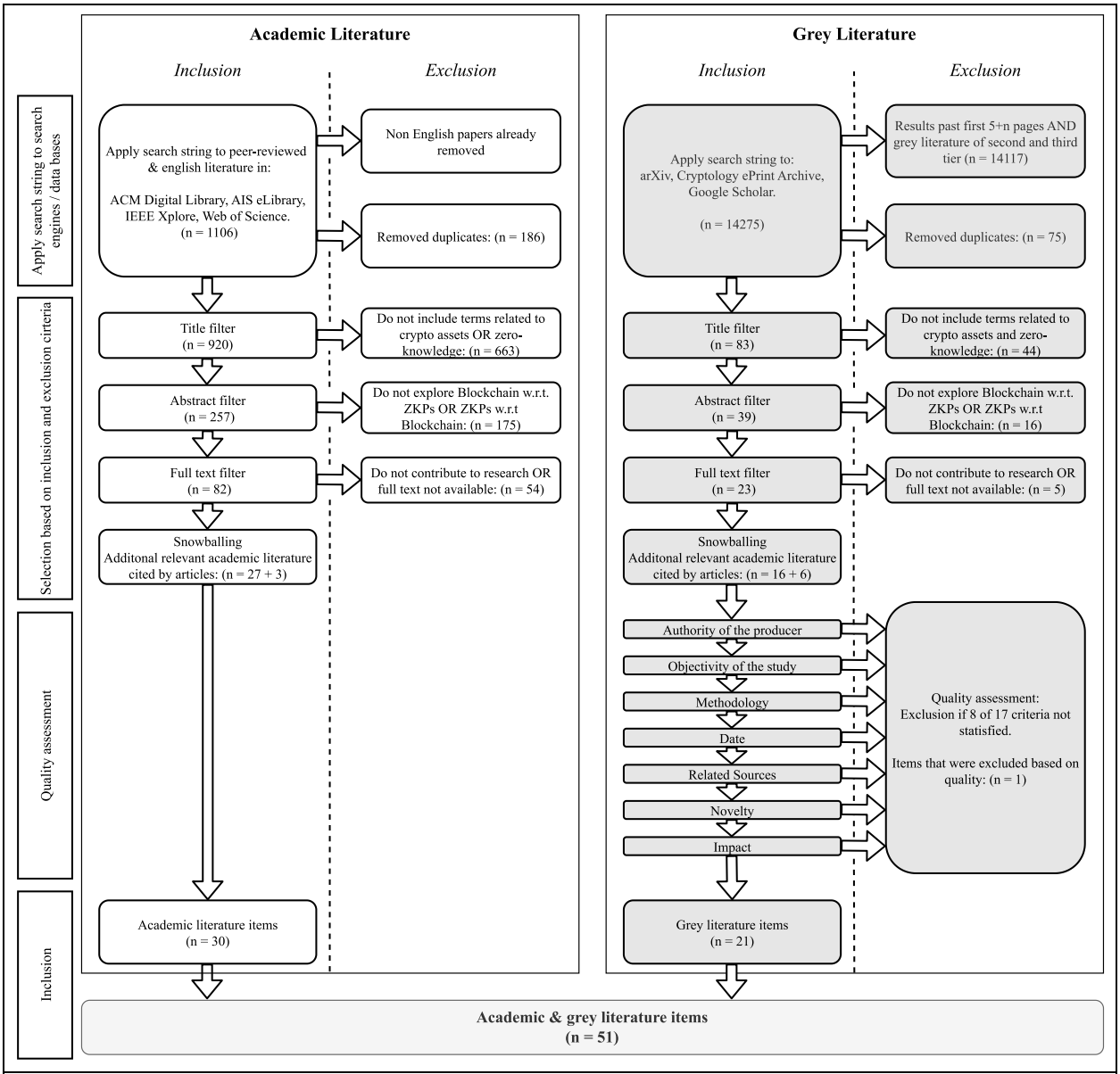

Figure 1: MLR item sampling and refining process

We also applied this search string to three established databases focusing on GL in this thematic area: arXiv, Cryptology ePrint Archive, and GoogleScholar. We, thus, obtained an initial GL set of 14,275 items. To manage such an extensive item set, we adopt the exhaustive stopping criteria proposed by Butijn et al. (2020): we include the first five pages of each database and incrementally preliminarily evaluate items on the following sites based on our inclusion and exclusion criteria until we reach a page n that contains more non-relevant items than relevant ones (i.e., >50% of the page). We included the hits in the 5+n pages and excluded items past 5+n pages. After the elimination of duplicates, the initial set comprises 158 GL items. There are three different tiers of grey literature based on the dimensions of "outlet control" and "credibility" (Garousi et al. 2019). To uphold high-quality standards while still enjoying the benefits of an MLR (Ogawa and Malen 1991), we chose to limit our identification to GL of the first tier. Items that (I1) can be assigned

to the first tier of GL (e.g., whitepapers, theses, working papers), (I2) explore the concept of ZK in blockchains, and (I3) have accessible full texts were included. Items were excluded if (E1) they do not contribute to the state of the knowledge or (E2) are not in English. After filtering as well as forward and backward searches, we obtained a set of 24 GL items. Since GL are usually not peer-reviewed and differ in quality, these items must undergo an assessment procedure (Garousi et al. 2019; Ogawa and Malen 1991). We assessed the items against the pre-defined quality criteria of Garousi et al. (2019). Items were excluded if they did not fulfill at least eight criteria. We thus obtain 21 final GL items and 51 items overall (30AL + 21GL). We have carefully analyzed these items in depth to identify cryptographic mechanisms, their respective evolution in recent years, and, finally, potential applications for blockchain technology.

Findings

While initial works started in 2013, ZKPs in blockchains have only recently gained traction from both practitioners and researchers. Our results indicate that the topic has become more significant for both academia and practice from 2018 on. It is particularly noticeable that journal articles about this topic were first published in 2019, while conference articles and grey literature started much earlier. Overall, it seems that conferences are the preferred venue for publishing academic research in this area. Contrary to AL, there is no clear preference for the item types of GL. Considering the publication dates of the items, the concept of ZKPs is currently gaining much attention and becoming a hot topic for practitioners and researchers alike.

Figure 2 provides a systematization of the research areas and artifacts in the field of cryptography and blockchain. Overall, we can differentiate research artifacts into a ZK-space and blockchain space based on whether they solely research ZKPs or if their focus lies on making them applicable to and integrating them in blockchains. On this basis, we analyze the influence of ZKPs on blockchain applications. Following the development of advanced algorithms and protocols over the past 40 years, we additionally have identified three epochs in this research area and organized the presentation of our findings accordingly. We begin with a brief introduction to the origins of ZKPs, tracing their development within the field of cryptographic research. We then examine research addressing privacy concerns associated with blockchain technology and explore the potential of ZKPs as a viable solution. Finally, we provide a comprehensive review of the literature, focusing on the application of ZKPs to improve scalability. This foundational knowledge then guides the subsequent discussion of this paper, where we evaluate our findings in the context of the blockchain trilemma and ultimately underpin the value of blockchain for future IS research on blockchains.

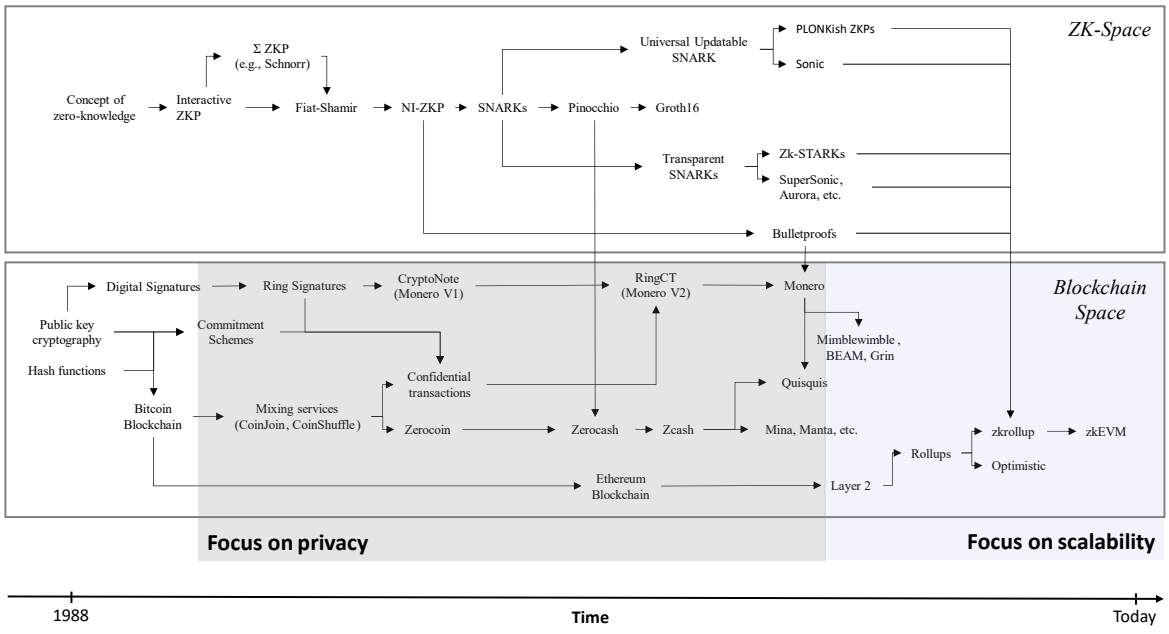

Figure 2: Development of ZKPs in blockchains

The genesis of ZKPs

The concept of ZK resulted from the work of Goldwasser et al. (1985), building on previous investigations into interactive proof systems. Although the first ZKP protocol, which was described in their paper, was of little practical significance, it made a groundbreaking theoretical contribution to the field of CS (Goldreich 2002). Building on these advancements, subsequent works sought to improve proving systems for more practical use by making them non-interactive, resulting in non-interactive ZKPs (Fiat and Shamir 1987). The Fiat-Shamir Transform emerged as a technique that converts interactive proof protocols into non-interactive zero-knowledge proofs. Thereby converting a multi-round proving process into a single computation for the user to output a proof. By making the proof non-interactive, the first practical ZKPs were then constructed using commitment schemes on private keys for authentication (Feige et al. 1988; Schnorr 1990). In follow-up works, research on foundational ZK demonstrated that ZKPs could be instantiated for sets of specific mathematical problems by using any commitment scheme (Ben-Or et al. 1988; Ben-Or et al. 1990; Goldreich et al. 1991). Until 2008 works on ZKPs have further continued to focus on improving the efficiency of schemes and constructing theoretical sound proofs for different scenarios and arbitrary computations (Gennaro et al. 2009; Goldreich 2002; Kilian and Petrank 1998).

The early focus of research on improving privacy in blockchains

We found that most of the (early) work on ZKP for blockchain systems was primarily aimed at addressing privacy concerns. In 2008 the concept of a blockchain emerged, together with its first implementation Bitcoin. After Bitcoin gained some public attention, initial security analyses of Bitcoin concluded that it sacrifices the privacy of its users by publishing transaction contents and addresses to the entire network, which allows for deanonymization attacks (Meiklejohn et al. 2013; Ron and Shamir 2013). Privacy in blockchain systems arises from the inherent transparency of public ledgers and has two key dimensions that can be addressed: Confidentiality, which refers to keeping the transaction contents private, and anonymity, which refers to keeping the identities of users hidden (Bünz et al. 2020). With Bitcoin supporting neither of these dimensions, research, especially in the early days of ZKP adoption in blockchains, entirely focused on enhancing privacy.

The influential reports of lacking privacy led to an immediate reaction from the Bitcoin development team, which introduced the first crypto mixer via a technique called "coin join" (Maxwell 2013a, 2013b). A mixer is a tool that shuffles transactions to protect the privacy of users by mixing funds from multiple sources, making it difficult to trace the original source. However, early mixers worked via a centralized party that may compromise the procedure or makes it very user-unfriendly, which leads to inappropriate use and subsequent danger of again falling victim to deanonymization attacks (Miers et al. 2013). The Zerocoin protocol was designed as a privacy extension for Bitcoin to circumvent this problem by implementing a decentralized mixing technique at the core blockchain protocol. This mixing technique works by introducing another currency (Zerocoin) on top of Bitcoin, which can be mined for burning a Bitcoin. A Zerocoin corresponds to a commitment to a serial number with a secret random value. The Zerocoin can then be traded in for a Bitcoin after a ZKP for an unspent serial number, and knowledge of the random value is generated. This burning/minting mixes transactions and breaks the link between the original Bitcoin and the newly minted one and thus also between sender and receiver, thereby enhancing anonymity (Miers et al. 2013). As such, the Zerocoin protocol presents the very first blockchain application in which ZKPs have been implemented.

In 2013, Parno et al. (2013) published "Pinocchio" and van Saberhagen (2013) published "CryptoNote". Pinocchio refers to a breakthrough of foundational ZKP research on SNARKs. However, it was designated as "nearly practical" due to significant inefficiency, which prevented its practical implementation (Parno et al. 2013). CryptoNote, on the other hand, refers to further developments in the blockchain space that aims to provide a solution to the drawback of Zerocoin, which uses ZKPs whose proof size makes practical use limited. CryptoNote also implements a mixing technique on the infrastructure level by making use of ring signatures for improved mixing and one-time addresses for increased anonymity. A ring signature is a type of digital signature that allows a user of a group to sign on behalf of the group without revealing which group member actually produced the signature (van Saberhagen 2013). The protocols' ZKPs are generated from the ring signature to prove the knowledge of a private key that can produce the respective ring signature and are more efficient than the ones from Zerocoin (van Saberhagen 2013). CryptoNote provided the foundation for the first version of Monero.

Both applications made use of application specific ZKPs. These proofs are designed to be optimized for specific use and can only be instantiated using specific cryptographic protocols, limiting them to certain types of applications (Chen et al. 2019). The most commonly used building block is the Σ-Protocol, a three-step protocol consisting of commitment, challenge, and response (Ganesh et al. 2019). The ZeroCoin protocol uses a specific variant of a Σ-Protocol, called the Schnorr protocol, allowing users to prove that they have a valid transaction without revealing the inputs and outputs of the transaction (Miers et al. 2013). This works by creating a commitment to the transaction and proving via a ZKP that the value in it corresponds to a valid input commitment registered on the chain (Jivanyan 2019; Miers et al. 2013). Commitment schemes find application in blockchain use cases to demonstrate knowledge of a committed value, which is essential in proving the validity of a transaction while keeping amounts confidential (Lu et al. 2019; Wang et al. 2019). In confidential cryptocurrencies, a commitment is used to prove the validity of the transaction (Jeong et al. 2022). The commitments, along with other relevant data, are included in a transaction to allow other nodes in the network to verify the transaction without disclosing any additional information beyond the transaction's validity (Bontekoe et al. 2022).

However, commitments can also be used to prove a wide variety of attributes if the necessary infrastructure to support claims is given and can be used for identity and access management via credentials and presentations (Heiss et al. 2022; Pauwels et al. 2022; Rathee et al. 2022). Further, cryptographic accumulators are such an infrastructure that supports making claims via commitments. They are a class of cryptographic primitives that allow for accumulating multiple inputs into a single output value while retaining the ability to prove that a particular input is a member of the set of accumulated values without revealing any of the other inputs (Bünz et al. 2018). In privacy-preserving blockchains, cryptographic accumulators are commonly used to store and prove the membership of encrypted values, such as confidential transaction amounts (Monero/Mimblewimble) (Poelstra 2016; van Saberhagen 2013) or commitment values (Zcash/Zcoin) (Ben Sasson et al. 2014a; Miers et al. 2013), while hiding the actual values from public view. The current state of the cryptographic accumulator can hereby be used as a commitment over which a proof of membership for a certain value can be performed (Chu et al. 2021). Accumulators, therefore, provide a way to keep track of the sent and received coins (i.e., the blockchain state) in a privacy-preserving manner, thereby preventing double spending in a blockchain (Campanelli et al. 2022).

In 2014 Ben-Sasson et al. (2014b) made a final breakthrough in practical SNARKs by improving the Pinocchio protocol for practical usage. They subsequently implemented it in Zerocash, an improvement of the Zerocoin protocol. Therefore, Zerocash is the very first application of SNARKs. It offers more functionality than Zerocoin and is orders of magnitudes faster and, thus, more suitable for a decentralized network (Ben Sasson et al. 2014a). The efficiency combined with the small proof size is the main factor for the usage of SNARKs, although a trusted setup is needed. The Zerocash protocol was then implemented into a cryptocurrency called "Zcash" (Hopwood et al. 2016). Like the development of Zerocash into Zcash, Monero developed from its origins in CryptoNote. Although mixing techniques provide a way to obfuscate the transaction graph, they are still susceptible to tracing analyses via heuristics based on transaction amounts. Therefore, the necessity of making the amounts private arises, which was first achieved in 2015 by the Bitcoin development team via "Confidential Transactions" (CT) on the Elements side-chain (Maxwell 2015; Poelstra et al. 2019). Building on these advancements, Noether et al. (2016) combined CT (confidentiality) with CryptoNote mixing (anonymity) in the RingCT scheme, which provided the foundation for achieving full privacy by combining confidentiality and anonymity and was implemented in the second version of Monero.

Propelled by the recent uses of ZKPs in blockchain applications, there have been various improvements in ZKP schemes such as more efficient SNARKs (Groth 2016), STARKs (Eli Ben-Sasson et al. 2018), and Bulletproofs (Bünz et al. 2018). Bulletproofs were specially tailored to blockchain applications by aiming to achieve a solution to the problem that ZKPs are either efficient but compromise decentralization due to trusted setups or decentralized but less efficient (Bünz et al. 2020). These new improvements have then been used in various blockchain solutions to improve the previous ZKPs. For example, Monero implemented Bulletproofs to replace their previous range-proof scheme, which was based on Borromean ring signatures and thus resulted in the Monero version that is still present today. Furthermore, improved mixers that make use of ZKPs, such as Tornado Cash, have emerged (Pertsev et al. 2019). SNARKs enable the generation of short, compressed proofs that can be efficiently verified, leading to a high-speed proving system. The compactness of the proofs is achieved through compression techniques, resulting in efficient

verification and making SNARKs well-suited for use cases where efficiency and scalability are critical (Bonneau et al. 2020). Therefore, SNARKs have been widely used as a fast verification tool for confidential and anonymous transactions in privacy-focused cryptocurrencies (Ben Sasson et al. 2014a). For example, Zcash uses the "Pinocchio" SNARK to allow for private transactions (Biryukov et al. 2019). Furthermore, SNARKs can be of use in smart contracts to provide off-chain verification of contract execution to reduce the computational burden on the blockchain as well as downscaling its storage space requirements (Eberhardt and Tai 2018; Kosba et al. 2016). However, the literature highlights that the main drawback of using standard SNARKs for applications in the blockchain realm is the re-introduction of trust in a central entity to perform the trusted setup, which produces the CRS and allows for this quick and efficient type of proofing scheme (Jivanyan 2019; Lai et al. 2019). Although this central entity can be decentralized from a single authority to multiple individuals by using a multi-party computation, trust in these participants is still required (Bünz et al. 2018). STARKs are ZKP schemes with a specific design that aims to address the issue of trusted setups and prove inefficiencies for large and complex computations. None of the methods we have examined employ SNARKs mainly due to their large proof size, which makes them less suitable for use in cryptocurrencies and blockchain applications (Guan et al. 2022; Li et al. 2022). Bulletproofs are the most novel of the commonly used schemes. They were created to offer a trade-off between the ZKP dilemma of a trusted setup, computational demands, and flexibility of use and are especially suited for secure and efficient range proofs with a focus on applications in blockchain settings (Bünz et al. 2018). Bulletproofs have been mainly used in more recent proposals and improvements for privacy-preserving blockchains as a replacement for SNARKs (Eagen 2022; Lai et al. 2019).

The recent focus of research on improving scalability of blockchain

Against the backdrop of the trilemma's constraints, developments in the blockchain industry have since focused on addressing the next challenge posed by the trilemma: Scalability. Most notably, the crypto industry is currently heavily increasing efforts to implement ZKPs, the most recent example being Ethereum with its move towards "Danksharding", a method that envisions the use of ZKPs as a tool to achieve scalability without compromising other goals of the trilemma (Buterin 2023). This movement is not arising in isolation but rather represents the most recent advancement in a broader industry shift. Other blockchain industry pioneers, including Polygon (2022), Starkware (2023), Loopring (2023), and many more, have also started exploring ZKPs to overcome scalability limitations (Chainlink 2022).

From 2016 on, foundational ZKP research has focused on improving schemes regarding their efficiency, resulting in very efficient proofs that are available for usage in blockchain applications. These proofs are in turn used in approaches of the blockchain space to address limitations of scalability. Yu et al. (2022) advance the payment channel system, which is also included in Bitcoin, with ZK in order to keep the members of the channel while ensuring a high transaction success rate. Bonneau et al. (2020) focus on improving scalability with the goal of implementing a succinct blockchain (called "Coda" and today known as "Mina") that can be verified even on mobile devices. Mina's use of recursive SNARKs allows for a constant-size proof that summarizes the entire blockchain's transaction history without needing to include all the transaction data in each new block. This proof is validated by network nodes, which can verify that the blockchain's history is valid without needing to store all the data. By compressing the blockchain in this way, Mina is able to maintain a constant blockchain size, which enables faster syncing times, lower storage requirements, and greater accessibility for network participants with limited resources (Bonneau et al. 2020). Eberhardt and Tai (2018) propose to move the verification of transactions off-chain and to only post proof of it to the blockchain, which keeps data private and enables higher throughput as it moves computational effort from the chain. This has been especially relevant for the second largest cryptocurrency, Ethereum, with its EVM. Per protocol rules, transactions and computations of the EVM are re-executed by all nodes to verify them. This severely limits Ethereum's scalability, allowing it to process only about 15 to 20 transactions per second (Ethereum 2023d).

The approach of replacing transactions with ZKPs gave rise to a promising scalability solution: Rollups – a concept that has originated from the Ethereum Community and Ethereum Foundation (Buterin 2021a). Rollups come in two flavors: Optimistic rollups, which employ game theory (fraud proofs) (Ethereum 2023b), and ZK-rollups, which employ computational integrity proofs on Merkle Trees via ZKPs (validity proofs) (Ozdemir et al. 2020). The origin of ZK-rollups can be traced back to a proposal by barryWhiteHat (2018), who first introduced the concept and its concrete mechanisms. A rollup works by aggregating transactions off-chain and only posting a hash with the respective ZKP of the new state after the transaction,

allowing for the verification of multiple transactions in only one. These validity proofs are usually generated off-chain to move intensive computation from the chain. In the Ethereum community, rollups are referred to as Layer 2 (L2) scaling solutions as they build on top of the pre-existing Layer 1 blockchain while adhering to the Layer 1 protocol. Depending on which type of rollup and where computations are outsourced to, there is an emerging ecosystem of different rollups, such as plain ZK-rollups, Optimistic rollups, Validium, Volition, and Plasma (Ethereum 2023d; Starkware 2020). Aside from rollups, there are further L2 scaling solutions, such as state channels and side-chains (Ethereum 2023d). However, these scaling solutions are limited and do not extend to general-purpose EVM code due to the challenges involved in efficiently verifying the correctness of more complex and universal computations on-chain (Buterin 2021a). The latest development in the crypto asset space now aims to tackle this challenge by designing "ZK-EVMs". Together with other scaling techniques, this is envisioned to bring high scalability for any computation on the Ethereum blockchain (Buterin 2020, 2021b). A ZK-EVM is the union of ZK-rollups and the EVM: it can be thought of like a general-purpose rollup for the entire EVM, where everything from transactions to smart contract function executions can be performed (Chainlink 2023). In other words: An EVM that supports executing arbitrary programs and only posting a ZKP of its execution to maintain blockchain security.

Discussion

The analysis of the literature allows us to uncover most of the significant milestones that have impacted the development of ZKPs for blockchains until today. There is a pattern emerging where ZKPs and blockchains developed independently from each other before 2013 but then converged to solve the blockchain privacy problem and, in 2020, the blockchain scalability problem. If we compare these developments with the body of literature that we analyzed in the literature review, we can see a significant gap in knowledge regarding the recent developments from 2020 onwards. While the works capture the first wave of privacy developments, they do not capture the scalability pattern. The body of literature has mentioned the topic of scalability through ZKPs only briefly, which does not stand in relation to the actual developments that have been made in this area. Almost all of these developments were driven by practice, for example, through the Ethereum Applied ZKP Team (Ethereum 2023c), STARKWARE (Starkware 2023), Polygon (Polygon 2022), Matterlabs (MatterLabs 2023), and other crypto industry players.

Articles about blockchain limitations commonly describe ZKPs as a solution to the privacy problem by ensuring anonymity (Capraz and Ozsoy 2021; Feng et al. 2019). However, as the analyzed literature demonstrates: One-time addresses and stealth addresses ensure anonymity, commitments ensure confidentiality, and ZKPs ensure integrity. It is important to recognize that the former primitives hide information, while the latter allows them to prove statements about the information without having to reveal the information in the first place. In essence, ZKPs do *not* ensure privacy by themselves. However, they ensure that the integrity of the ledger can be maintained while privacy is ensured via privacy-preserving primitives. ZKPs, therefore, offer a tool for resolving the conflict between the security and the decentralization dimensions of the trilemma and are used in conjunction with privacy-enhancing techniques.

Furthermore, most modern ZK proving schemes are highly optimized and compress computations into a concise representation that allows performing a ZKP verification much faster than the computation can be performed itself (Ben-Sasson et al. 2014b; Bünz et al. 2018). In blockchain systems, nodes verify the blockchain state by performing the computation in transactions locally and checking if the output matches the associated state, which means that traditional verification is linear in time-complexity. In a ZK-rollup, transactions are batched, simulated off-chain, and a ZKP is generated and posted on the blockchain to prove the integrity of the resulting state. Therefore, it reduces computational overhead on all nodes in the blockchain system (Jeong and Ahn 2021). Further, ZK-rollup proofs are smaller than the data, which would normally be posted to the blockchain, therefore, also occupying less storage space on nodes in the network (Bonneau et al. 2020). Overall, ZKPs thus can improve the scalability of blockchains in two essential points: computational complexity and storage space. Nevertheless, since this data aggregation and likewise the proof of its integrity take place off-chain, these processes do not benefit from the decentralization of the blockchain itself. In most cases, a single party or a small network of parties build the rollups (Ethereum 2023e), leading to another governance layer with a higher degree of centralization which is completely decoupled from the blockchain layer to which the proof is later posted. However, the verification could still be considered decentralized as proofs are verified by all nodes of the network.

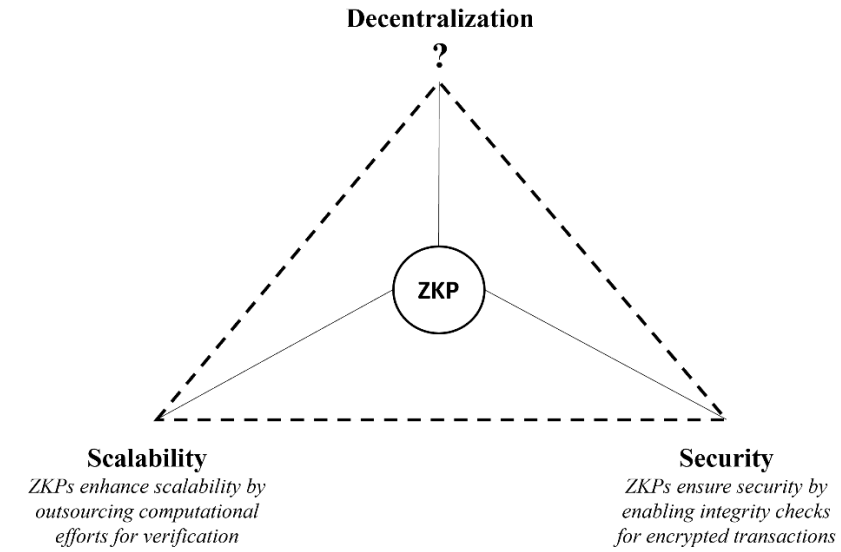

Figure 3: Blockchain-ZKP trilemma

Despite this remarkable progress, there still appears to be ample opportunity for future research on simultaneously satisfying all three dimensions of the blockchain trilemma: While our findings illustrate that ZKPs are addressing the scalability and security constraints of blockchains (see Figure 3), it is unclear how they impact the blockchains decentralization. Instead of impacting this aspect directly, ZKPs rather create another governance layer with a degree of decentralization that is decoupled from the blockchain itself, thus allowing the decentralization challenge to shift from the blockchain layer towards the ZKP layer. The major limitation in this layer is that there are currently not enough providers offering services (e.g., ZK-rollups), resulting in a lower degree of decentralization. To answer our research question: ZKPs are applied to blockchains using aforementioned primitives to increase scalability while upholding security; However, it is currently unclear how they directly impact blockchain decentralization. Therefore, we propose two ways for future research towards addressing this issue and finally resolving the blockchain trilemma: Increasing the number of ZK-service providers or coupling the ZK governance layer to the blockchain infrastructure. The former could be achieved via game-theoretic incentives, as it is common in decentralized finance, and the latter could be achieved by approaches where block producers of blockchains become ZK-service providers.

Conclusion

Inspired by a recent spike in Zero-Knowledge Proof (ZKP) projects initiated by the blockchain industry, we explore the use of ZKPs in blockchain applications and answer the question of their origins and benefits. Regarding the research question, we find that ZKPs and blockchains share a common origin, and their development is closely intertwined. The origin of ZKP research is mainly of practical nature, CS-oriented, and driven by blockchain-based businesses and communities that simultaneously explore and apply these new cryptographic tools in their projects and products.

Based on our research results, we propose that previous claims in blockchain research be re-evaluated comprehensively, considering the significant impact of ZKPs on the blockchain trilemma. We've noticed that ZKPs are presently being employed to enhance scalability while ensuring security and bringing a new level of privacy within blockchain systems. Looking ahead, there may be opportunities to decentralize the integration of ZKP-based applications in blockchains as well. A first step in this direction can be found in Ethereum's roadmap, which foresees the use of L2 blob transactions for data availability, as proposed in EIP-4844. Anticipating this evolution of ZKPs, as they might gain the ability to enable these attributes to coexist, they hold the potential to revolutionize the blockchain landscape and reshape our understanding of what is possible within decentralized systems.

Consequently, we urge the establishment of a dedicated IS research stream focused on ZKPs, as their substantial influence on blockchain applications has become increasingly apparent. With ZKPs playing a pivotal role in overcoming traditional blockchain limitations, they have also contributed to the emergence of new business models and opportunities within the crypto asset ecosystem. By fostering an IS research stream centered around ZKPs, we can support the development of a more robust body of knowledge in this area and accelerate innovation in the field. Especially the influence on the aspect of decentralization is currently highly relevant and insufficiently studied, providing an excellent opportunity for further research.

We hope that this initial exploration of ZKPs in blockchains will act as a catalyst for future research endeavors. By highlighting the need for further investigation into the potential of ZKPs, we aim to inspire the IS community and researchers to delve deeper into this emerging building block for decentralized systems. The rapid advancements in ZKP technology, combined with their substantial impact on blockchain applications, suggest that now is the time for the academic community to engage in rigorous research on this transformative cryptographic tool.

Acknowledgements

We gratefully acknowledge the Bavarian Ministry of Economic Affairs, Regional Development and Energy for their support of the project "Fraunhofer Blockchain Center (20-3066-2-6-14)" that made this paper possible.

References

Alupotha, J., Boyen, X., and Mckague, M. 2022. "Aggregable Confidential Transactions for Efficient Quantum-Safe Cryptocurrencies," *IEEE Access* (10), pp. 17722-17747 (doi: 10.1109/ACCESS.2022.3149605).

Aztec. 2023. *The Hybrid zkRollup*. *Aztec*, available at https://medium.com/aztec-protocol/aztec-the-hybrid-zkrollup-a90a197bf22e.

barryWhiteHat. 2018. "Roll Up," available at https://github.com/barryWhiteHat/roll_up.

Beck, R., Avital, M., Rossi, M., and Thatcher, J. B. 2017. "Blockchain Technology in Business and Information Systems Research," *Business & Information Systems Engineering* (59:6), pp. 381-384 (doi: 10.1007/s12599-017-0505-1).

Bellare, M., and Rogaway, P. 1993. "Random oracles are practical," in *Proceedings of the 1st ACM conference on Computer and communications security - CCS '93*, D. Denning, R. Pyle, R. Ganesan, R. Sandhu and V. Ashby (eds.), Fairfax, Virginia, United States. 03.11.1993 - 05.11.1993, New York, New York, USA: ACM Press, pp. 62-73 (doi: 10.1145/168588.168596).

Ben Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., and Virza, M. 2014a. "Zerocash: Decentralized Anonymous Payments from Bitcoin," San Jose, CA. 2014/05, IEEE, pp. 459-474 (doi: 10.1109/SP.2014.36).

Ben-Or, M., Goldreich, O., Goldwasser, S., Håstad, J., Kilian, J., Micali, S., and Rogaway, P. 1990. "Everything Provable is Provable in Zero-Knowledge," in *Advances in Cryptology — CRYPTO' 88*, S. Goldwasser (ed.), New York, NY: Springer New York, pp. 37-56 (doi: 10.1007/0-387-34799-2_4).

Ben-Or, M., Goldwasser, S., Kilian, J., and Widgerson, A. 1988. "Multi-prover interactive proofs: how to remove intractability," in *Proceedings of the twentieth annual ACM symposium on Theory of computing - STOC '88*, J. Simon (ed.), Chicago, Illinois, United States. 02.05.1988 - 04.05.1988, New York, New York, USA: ACM Press, pp. 113-131 (doi: 10.1145/62212.62223).

Ben-Sasson, E., Chiesa, A., Tromer, E., and Virza, M. 2014b. "Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture," in *Proceedings of the 23rd USENIX Conference on Security Symposium*, USA: USENIX Association, pp. 781-796.

Bernal Bernabe, J., Canovas, J. L., Hernandez-Ramos, J. L., Torres Moreno, R., and Skarmeta, A. 2019. "Privacy-Preserving Solutions for Blockchain: Review and Challenges," *IEEE Access* (7), pp. 164908-164940 (doi: 10.1109/ACCESS.2019.2950872).

Binance. 2020. "Binance Research Case Study: Is EOS Too Centralized? | Binance Blog," available at https://www.binance.com/en/blog/all/binance-research-case-study-is-eos-too-centralized--4214998246849004 25.

Biryukov, A., Feher, D., and Vitto, G. 2019. "Privacy Aspects and Subliminal Channels in Zcash," London, United Kingdom. 2019, Association for Computing Machinery, pp. 1813-1830 (doi: 10.1145/3319535.3345663).

Bitansky, N., Canetti, R., Chiesa, A., and Tromer, E. 2012. "From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again," in *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, S. Goldwasser (ed.), Cambridge Massachusetts. 08 01 2012 10 01 2012, New York, NY, USA: ACM, pp. 326-349 (doi: 10.1145/2090236.2090263).

Blum, M., Feldman, P., and Micali, S. 1988. "Non-interactive zero-knowledge and its applications," in *Proceedings of the twentieth annual ACM symposium on Theory of computing - STOC '88*, J. Simon (ed.), Chicago, Illinois, United States. 02.05.1988 - 04.05.1988, New York, New York, USA: ACM Press, pp. 103-112 (doi: 10.1145/62212.62222).

Bonneau, J., Meckler, I., Rao, V., and Shapiro, E. 2020. *Coda: Decentralized Cryptocurrency at Scale*, available at https://eprint.iacr.org/2020/352.

Bontekoe, T., Everts, M., and Peter, A. 2022. "Balancing privacy and accountability in digital payment methods using zk-SNARKs," 2022/08/22/24, pp. 1-10 (doi: 10.1109/PST55820.2022.9851987).

Bünz, B., Agrawal, S., Zamani, M., and Boneh, D. 2020. "Zether: Towards Privacy in a Smart Contract World," in *Financial Cryptography and Data Security*, J. Bonneau and N. Heninger (eds.), Cham: Springer International Publishing, pp. 423-443.

Bünz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., and Maxwell, G. 2018. "Bulletproofs: Short Proofs for Confidential Transactions and More," in *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 315-334 (doi: 10.1109/SP.2018.00020).

Buterin, V. 2020. "A rollup-centric ethereum roadmap," available at https://ethereum-magicians.org/t/a-rollup-centric-ethereum-roadmap/4698.

Buterin, V. 2021a. "An Incomplete Guide to Rollups," available at https://vitalik.ca/general/2021/01/05/rollup.html.

Buterin, V. 2021b. "The Limits to Blockchain Scalability," available at https://vitalik.ca/general/2021/05/23/scaling.html.

Buterin, V. 2023. "Proto-Danksharding FAQ," available at https://notes.ethereum.org/@vbuterin/proto_danksharding_faq.

Butijn, B.-J., Tamburri, D. A., and van Heuvel, W.-J. 2020. "Blockchains: a systematic multivocal literature review," *ACM Computing Surveys (CSUR)* (53:3), pp. 1-37.

Cachin, C., and Vukolić, M. 2017. "Blockchain Consensus Protocols in the Wild,"

Campanelli, M., Hall-Andersen, M., and Kamp, S. H. 2022. *Curve Trees: Practical and Transparent Zero-Knowledge Accumulators*, available at https://eprint.iacr.org/2022/756.

Capraz, S., and Ozsoy, A. 2021. "Personal Data Protection in Blockchain with Zero-Knowledge Proof," in *Blockchain Technology and Innovations in Business Processes*, S. Patnaik, T.-S. Wang, T. Shen and S. K. Panigrahi (eds.), Singapore: Springer Singapore, pp. 109-124 (doi: 10.1007/978-981-33-6470-7_7).

Chainlink. 2022. "Overview of Zero-Knowledge Blockchain Projects," *Chainlink Blog*.

Chainlink. 2023. "What Is a zkEVM?" *Chainlink Blog*.

Chauhan, A., Malviya, O. P., Verma, M., and Mor, T. S. 2018. "Blockchain and Scalability," in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C),* Lisbon. 16.07.2018 - 20.07.2018, IEEE, pp. 122-128 (doi: 10.1109/QRS-C.2018.00034).

Chen, L., Babar, M. A., and Zhang, H. 2010. "Towards an Evidence-Based Understanding of Electronic Data Sources," in *Proceedings of the 14th International Conference on Evaluation and Assessment in Software Engineering*, Swindon, GBR: BCS Learning & Development Ltd, pp. 135-138.

Chen, Y., Ma, X., Tang, C., and Au, M. H. 2019. *PGC: Pretty Good Decentralized Confidential Payment System with Auditability*, available at https://eprint.iacr.org/2019/319.

Chu, S., Xia, Y., and Zhang, Z. 2021. *Manta: a Plug and Play Private DeFi Stack*, available at https://eprint.iacr.org/2021/743.

CoinMarketCap. 2021. "Is EOS Dead? What Happened to the Ethereum Killer?" *CoinMarketCap*.

Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V., and others. 2016. "Blockchain technology: Beyond bitcoin," *Applied Innovation* (2:6-10), p. 71.

Del Monte, G., Pennino, D., and Pizzonia, M. 2020. "Scaling blockchains without giving up decentralization and security," in *Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems,* London United Kingdom. 25 09 2020 25 09 2020, New York, NY, USA: ACM, pp. 71-76 (doi: 10.1145/3410699.3413800).

Eagen, L. 2022. *μCash: Transparent Anonymous Transactions*, available at https://eprint.iacr.org/2022/1104.
Eberhardt, J., and Tai, S. 2018. "ZoKrates - Scalable Privacy-Preserving Off-Chain Computations," 2018/08/30/July-3, pp. 1084-1091 (doi: 10.1109/Cybermatics_2018.2018.00199).
Ekparinya, P., Gramoli, V., and Jourjon, G. 2019. "The attack of the clones against proof-of-authority," *arXiv preprint arXiv:1902.10244*.
Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. 2018. *Scalable, transparent, and post-quantum secure computational integrity*, available at https://eprint.iacr.org/2018/046.
Ethereum. 2023a. "Ethereum roadmap," available at https://ethereum.org/en/roadmap/.
Ethereum. 2023b. "Optimistic Rollups | ethereum.org," available at https://ethereum.org/en/developers/docs/scaling/optimistic-rollups/.
Ethereum. 2023c. "Privacy and Scaling Explorations," available at https://appliedzkp.org/.
Ethereum. 2023d. "Scaling | ethereum.org," available at https://ethereum.org/en/developers/docs/scaling/.
Ethereum. 2023e. "Zero-Knowledge rollups," available at https://ethereum.org/en/developers/docs/scaling/zk-rollups/.
Farace, D. J., and Schöpfel, J. 2010. *Grey Literature in Library and Information Studies*, DE GRUYTER SAUR.
Feige, U., Fiat, A., and Shamir, A. 1988. "Zero-knowledge proofs of identity," *Journal of Cryptology* (1:2), pp. 77-94 (doi: 10.1007/BF02351717).
Feng, Q., He, D., Zeadally, S., Khan, M. K., and Kumar, N. 2019. "A survey on privacy protection in blockchain system," *Journal of Network and Computer Applications* (126), pp. 45-58 (doi: 10.1016/j.jnca.2018.10.020).
Fiat, A., and Shamir, A. 1987. "How To Prove Yourself: Practical Solutions to Identification and Signature Problems," in *Advances in cryptology: CRYPTO '86, proceedings*, A. Odlyzko and U. o. California (eds.), Berlin: Springer, pp. 186-194 (doi: 10.1007/3-540-47721-7_12).
Ganesh, C., Orlandi, C., and Tschudi, D. 2019. "Proof-of-Stake Protocols for Privacy-Aware Blockchains," Y. Ishai and V. Rijmen (eds.). 2019, pp. 690-719 (doi: 10.1007/978-3-030-17653-2_23).
Garousi, V., Felderer, M., and Mäntylä, M. V. 2016. "The need for multivocal literature reviews in software engineering," S. Beecham, B. Kitchenham and S. G. MacDonell (eds.), Limerick Ireland. 01 06 2016 03 06 2016, New York, NY, USA: ACM, pp. 1-6 (doi: 10.1145/2915970.2916008).
Garousi, V., Felderer, M., and Mäntylä, M. V. 2019. "Guidelines for including grey literature and conducting multivocal literature reviews in software engineering," *Information and Software Technology* (106), pp. 101-121 (doi: 10.1016/j.infsof.2018.09.006).
Gennaro, R., Gentry, C., and Parno, B. 2009. *Non-Interactive Verifiable Computing: Outsourcing Computation to Untrusted Workers*, available at https://eprint.iacr.org/2009/547.
Goldreich, O. 2002. "Zero-Knowledge twenty years after its invention," *IACR Cryptol. ePrint Arch.* (2002), p. 186.
Goldreich, O., Micali, S., and Wigderson, A. 1991. "Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems," *Journal of the ACM* (38:3), pp. 690-728 (doi: 10.1145/116825.116852).
Goldwasser, S., Micali, S., and Rackoff, C. 1985. "The knowledge complexity of interactive proof-systems," in *Proceedings of the seventeenth annual ACM symposium on Theory of computing*, R. Sedgewick (ed.), Providence, Rhode Island, United States. 5/6/1985 - 5/8/1985, New York, New York, USA: ACM Digital Library, pp. 291-304 (doi: 10.1145/22145.22178).
Gramlich, V., Guggenberger, T., Principato, M., Schellinger, B., and Urbach, N. 2023. "A multivocal literature review of decentralized finance: Current knowledge and future research avenues," *Electronic Markets* (33:1) (doi: 10.1007/s12525-023-00637-4).
Groth, J. 2016. "On the Size of Pairing-Based Non-interactive Arguments," in *Advances in Cryptology – EUROCRYPT 2016*, M. Fischlin and J.-S. Coron (eds.), Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 305-326 (doi: 10.1007/978-3-662-49896-5_11).
Guan, Z., Wan, Z., Yang, Y., Zhou, Y., and Huang, B. 2022. "BlockMaze: An Efficient Privacy-Preserving Account-Model Blockchain Based on zk-SNARKs," *IEEE Transactions on Dependable and Secure Computing* (19:3), pp. 1446-1463 (doi: 10.1109/TDSC.2020.3025129).
Guggenberger, T., Sedlmeir, J., Fridgen, G., and Luckow, A. 2022. "An in-depth investigation of the performance characteristics of Hyperledger Fabric," *Computers & Industrial Engineering* (173), p. 108716 (doi: 10.1016/j.cie.2022.108716).

Hafid, A., Hafid, A. S., and Samih, M. 2020. "Scaling Blockchains: A Comprehensive Survey," *IEEE Access* (8), pp. 125244-125262 (doi: 10.1109/ACCESS.2020.3007251).
Heiss, J., Muth, R., Pallas, F., and Tai, S. 2022. "Non-Disclosing Credential On-chaining for Blockchain-based Decentralized Applications,"
Hopwood, D., Bowe, S., Hornby, T., and Wilcox, N. 2016. "Zcash protocol specification," *GitHub: San Francisco, CA, USA* (4), p. 220.
Iansiti, M., Lakhani, K. R., and others. 2017. "The truth about blockchain," *Harvard business review* (95:1), pp. 118-127.
Jeong, G., Lee, N., Kim, J., and Oh, H. 2022. *Azeroth: Auditable Zero-knowledge Transactions in Smart Contracts*, available at https://eprint.iacr.org/2022/211.
Jeong, S., and Ahn, B. 2021. "A Study of Universal Zero-Knowledge Proof Circuit-based Virtual Machines that Validate General Operations & Reduce Transaction Validation," *COMPUTER SCIENCE AND INFORMATION SYSTEMS* (18:2), pp. 481-497 (doi: 10.2298/CSIS200322006J).
Jivanyan, A. 2019. *Lelantus: A New Design for Anonymous and Confidential Cryptocurrencies*, available at https://eprint.iacr.org/2019/373.
Kamei, F., Pinto, G., Wiese, I., Ribeiro, M., and Soares, S. 2021. "What Evidence We Would Miss If We Do Not Use Grey Literature?" F. Lanubile (ed.), Bari Italy. 11 10 2021 15 10 2021, New York, NY, USA: ACM, pp. 1-11 (doi: 10.1145/3475716.3475777).
Kannengießer, N., Lins, S., Dehling, T., and Sunyaev, A. 2021. "Trade-offs between Distributed Ledger Technology Characteristics," *ACM Computing Surveys* (53:2), pp. 1-37 (doi: 10.1145/3379463).
Kilian, J., and Petrank, E. 1998. "An Efficient Noninteractive Zero-Knowledge Proof System for NP with General Assumptions," *Journal of Cryptology* (11:1), pp. 1-27 (doi: 10.1007/s001459900032).
Kitchenham, B., and Charters, S. 2007. "Guidelines for performing Systematic Literature Reviews in Software Engineering," (2).
Kosba, A., Miller, A., Shi, E., Wen, Z., and Papamanthou, C. 2016. "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," 2016/05/22/26, pp. 839-858 (doi: 10.1109/SP.2016.55).
Lai, R. W. F., Ronge, V., Ruffing, T., Schröder, D., Thyagarajan, S. A. K., and Wang, J. 2019. "Omniring: Scaling Private Payments Without Trusted Setup," London, United Kingdom. 2019, Association for Computing Machinery, pp. 31-48 (doi: 10.1145/3319535.3345655).
Li, Y., Zhang, Y. Y., Wang, M. M., Zhu, J. M., and Wang, X. L. 2022. "BMSC: A Novel Anonymous Trading Scheme Based on Zero-Knowledge Proof in Ethereum," Y. Wang, G. Zhu, Q. Han, L. Zhang, X. Song and Z. Lu (eds.). 2022, pp. 59-77 (doi: 10.1007/978-981-19-5209-8_5).
Loopring. 2023. "Loopring - zkRollup Layer2 for Trading and Payment,"
Lu, Y. 2019. "The blockchain: State-of-the-art and research challenges," *Journal of Industrial Information Integration* (15), pp. 80-90 (doi: 10.1016/j.jii.2019.04.002).
Lu, Z. M., Jiang, Z. L., Wu, Y. L., Wang, X., and Zhong, Y. T. 2019. "A Lattice-Based Anonymous Distributed E-Cash from Bitcoin," Y. Ishai and V. Rijmen (eds.). 2019, pp. 275-287 (doi: 10.1007/978-3-030-31919-9_16).
MatterLabs. 2023. "Matter Labs — an engineering team passionate about liberty, blockchain, and math.,"
Maxwell, G. 2013a. "CoinJoin: Bitcoin privacy for the real world," available at https://bitcointalk.org/?topic=279249.
Maxwell, G. 2013b. "I taint rich! (Raw txn fun and disrupting 'taint' analysis; >51kBTC linked!)," available at https://bitcointalk.org/?topic=139581.
Maxwell, G. 2015. "Confidential Transactions - Investigation," available at https://elementsproject.org/features/confidential-transactions/investigation.
Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., and Savage, S. 2013. "A fistful of bitcoins," in *Proceedings of the 2013 conference on Internet measurement conference*, K. Papagiannaki, K. Gummadi and C. Partridge (eds.), Barcelona Spain. 23 10 2013 25 10 2013, New York, NY, USA: ACM, pp. 127-140 (doi: 10.1145/2504730.2504747).
Merkle, R. C. 1988. "A digital signature based on a conventional encryption function," in *Advances in Cryptology—CRYPTO'87: Proceedings 7*, pp. 369-378.
Miers, I., Garman, C., Green, M., and Rubin, A. D. 2013. "Zerocoin: Anonymous Distributed E-Cash from Bitcoin," Berkeley, CA. 2013/05, IEEE, pp. 397-411 (doi: 10.1109/SP.2013.34).
Nakamoto, S. 2008. "Bitcoin whitepaper," *URL: https://bitcoin. org/bitcoin. pdf-(17.07. 2019)*.
Ncube, T., Dlodlo, N., and Terzoli, A. 2020. "Private Blockchain Networks: A Solution for Data Privacy," in *2020 2nd International Multidisciplinary Information Technology and Engineering Conference*

(IMITEC), Kimberley, South Africa. 25.11.2020 - 27.11.2020, IEEE, pp. 1-8 (doi: 10.1109/IMITEC50163.2020.9334132).
Noether, S., Mackenzie, A., and others. 2016. "Ring confidential transactions," *Ledger* (1), pp. 1-18.
Ogawa, R. T., and Malen, B. 1991. "Towards Rigor in Reviews of Multivocal Literatures: Applying the Exploratory Case Study Method," *Review of Educational Research* (61:3), pp. 265-286 (doi: 10.3102/00346543061003265).
Ozdemir, A., Wahby, R., Whitehat, B., and Boneh, D. 2020. "Scaling verifiable computation using efficient set accumulators," in *29th USENIX Security Symposium (USENIX Security 20)*, pp. 2075-2092.
Parno, B., Howell, J., Gentry, C., and Raykova, M. 2013. "Pinocchio: Nearly Practical Verifiable Computation," in *2013 IEEE Symposium on Security and Privacy (SP) Conference Dates Subject to Change,* Berkeley, CA. 5/19/2013 - 5/22/2013, IEEE, pp. 238-252 (doi: 10.1109/SP.2013.47).
Pauwels, P., Pirovich, J., Braunz, P., and Deeb, J. 2022. *zkKYC in DeFi: An approach for implementing the zkKYC solution concept in Decentralized Finance*, available at https://eprint.iacr.org/2022/321.
Pertsev, A., Semenov, R., and Storm, R. 2019. "Tornado Cash Privacy Solution Version 1.4,"
Poelstra, A. 2016. "Mimblewimble,"
Poelstra, A., Back, A., Friedenbach, M., Maxwell, G., and Wuille, P. 2019. "Confidential Assets," in *Financial Cryptography and Data Security*, A. Zohar, I. Eyal, V. Teague, J. Clark, A. Bracciali, F. Pintore and M. Sala (eds.), Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 43-63 (doi: 10.1007/978-3-662-58820-8_4).
Polygon. 2022. "Polygon's Zero Knowledge Strategy Explained," available at https://www.polygon.technology/blog/polygons-zero-knowledge-strategy-explained.
Rathee, D., Policharla, G. V., Xie, T., Cottone, R., and Song, D. 2022. *ZEBRA: Anonymous Credentials with Practical On-chain Verification and Applications to KYC in DeFi*, available at https://eprint.iacr.org/2022/1286.
Ron, D., and Shamir, A. 2013. "Quantitative Analysis of the Full Bitcoin Transaction Graph," in *Financial Cryptography and Data Security*, D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum and A.-R. Sadeghi (eds.), Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 6-24 (doi: 10.1007/978-3-642-39884-1_2).
Schnorr, C. P. 1990. "Efficient Identification and Signatures for Smart Cards," in *Advances in Cryptology — CRYPTO' 89 Proceedings*, G. Brassard (ed.), New York, NY: Springer New York, pp. 239-252 (doi: 10.1007/0-387-34805-0_22).
Smith, M. S. 2022. "The Spectacular Collapse of CryptoKitties, the First Big Blockchain Game," *IEEE Spectrum*.
Starkware. 2020. "Volition and the Emerging Data Availability spectrum," *Medium*.
Starkware. 2023. "STARKWARE," available at https://starkware.co/.
Sun, X., Yu, F. R., Zhang, P., Sun, Z., Xie, W., and Peng, X. 2021. "A Survey on Zero-Knowledge Proof in Blockchain," *IEEE Network* (35:4), pp. 198-205 (doi: 10.1109/MNET.011.2000473).
Titus, O. J. 2022. "Enforcing Scalability and Data Integrity on Blockchain with Zero-Knowledge Proof,"
van Saberhagen, N. 2013. "CryptoNote v 2.0,"
Wang, Z. Y., Pei, Q. Q., Liui, X. F., Ma, L. C., Li, H. Z., and Yu, S. 2019. "DAPS: A Decentralized Anonymous Payment Scheme with Supervision," Y. Ishai and V. Rijmen (eds.). 2019, pp. 537-550 (doi: 10.1007/978-3-030-38961-1_46).
Webster, J., and Watson, R. T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly* (26:2), pp. xiii-xxiii.
Wu, H., and Wang, F. 2014. "A survey of noninteractive zero knowledge proof system and its applications," *TheScientificWorldJournal* (2014), p. 560484 (doi: 10.1155/2014/560484).
Yu, M., M. Xu, D. Yu, X. Cheng, Q. Hu, and Z. Xiong. 2022. "zk-PCN: A Privacy-Preserving Payment Channel Network Using zk-SNARKs," 2022/11/11/13, pp. 57-64 (doi: 10.1109/IPCCC55026.2022.9894329).
Zhang, R., Xue, R., and Liu, L. 2020. "Security and Privacy on Blockchain," *ACM Computing Surveys* (52:3), pp. 1-34 (doi: 10.1145/3316481).
Zhou, Q., Huang, H., Zheng, Z., and Bian, J. 2020. "Solutions to Scalability of Blockchain: A Survey," *IEEE Access* (8), pp. 16440-16455 (doi: 10.1109/ACCESS.2020.2967218).
ZKProof. 2022. "ZKProof Community Reference," Version 0.3, available at https://docs.zkproof.org/reference.