ISSN: 2834-7706

Research Article

Journal of Mathematical Techniques and Computational Mathematics

Application of Zero-Knowledge Cryptography in Blockchain Technology: Guaranteeing Privacy and Data Integrity

Adiane Cueto Portuondo*, Dariel Gonzalez Robinson and Angel Alejandro Guerra Vilches

University of Sciences IT, Cuba

***Corresponding Author**
Adiane Cueto Portuondo, University of Sciences IT, Cuba.

Submitted: 2024, May 31; **Accepted**: 2024, Jun 21; **Published**: 2024, Jul 02

Citation: Portuondo, A. C., Robinson, D. G., Vilches, A. A. G. (2024). Application of Zero-Knowledge Cryptography in Blockchain Technology: Guaranteeing Privacy and Data Integrity. *J Math Techniques Comput Math, 3*(7), 01-06.

Abstract

This research work focuses on zero-knowledge cryptography and its application in blockchain technology. The theoretical foundations of zero-knowledge cryptography, its practical applications and limitations are addressed, and existing protocols applicable to blockchain are explored. The challenges of Privacy and confidentiality in the context of blockchain are discussed and how this type of cryptography can mitigate those challenges. Several Cryptographic protocols are examined and an example of Implementation through the zkLedger system is presented. Finally, several current challenges in this field are identified, including Computational efficiency, scalability and interoperability. The Studio aims to provide an updated vision of zero-knowledge cryptography applied to the blockchain, and to serve as a starting point for future investigations in this area.

Keywords: Zero-knowledge Cryptography, Blockchain, Application, Privacy, Confidentiality

1. Introduction

In recent years, the blockchain has emerged as one disruptive technology with wide applications in various industries. Its ability to provide an immutable and transparent register of transactions has been widely recognized. However, privacy and data confidentiality in the blockchain are significant challenges that require robust solutions.

In this context, zero-knowledge cryptography has emerged as a promising tool to address these challenges in the blockchain scope. Zero-knowledge cryptography allows parties to demonstrate that a claim is true without revealing additional information beyond the veracity of the claim itself. That's it implies that an entity can demonstrate knowledge of certain data without revealing the data itself, ensuring privacy and confidentiality.

The objective of this research work is to carry out a review of zero-knowledge cryptography used in the blockchain, analyzing its theoretical foundations, practical applications and limitations. Through a methodology based on a bibliographic review, the existing protocols will be explored, evaluating their efficiency and security in terms of privacy and confidentiality of the data, as well as the integrity of the records stored in it the blockchain.

The structure of the Work is divided into the following sections: first, the foundations of zero-knowledge cryptography will be presented, highlighting the concepts and techniques used A Next, the challenges of Privacy and confidentiality in the context of the blockchain will be addressed, and It will analyze how zero-knowledge cryptography can mitigate these challenges. Subsequently, zero-knowledge cryptography protocols used in the blockchain and an example of implementation will be examined. Other applications of this type of cryptography will be mentioned and finally the current challenges in this field will be discussed.

2. Content

2.1 Fundamentals of Zero-Knowledge Cryptography

Zero-knowledge cryptography is a field of study that allows parties to demonstrate that they possess knowledge of certain information without revealing that information itself. In other words, it allows the veracity of a statement to be demonstrated without revealing additional data beyond the statement itself. This property is of great importance Applications where privacy and confidentiality are fundamental.

Zero-knowledge proof systems (ZKP) are cryptographic techniques that allow a Prover to demonstrate knowledge about a specific fact or statement to a verifier without revealing additional information beyond the fact or statement itself. It mediates the generation of a test by the prover that meets a specific set of criteria, which The verifier can be used to verify the assertion and learn nothing more about the declaration. Consequently, ZKPs allow minimizing

and limiting access to data in distributed contexts, such as Internet services in general or cloud computing. (Implementation and Security Test of Zero-Knowledge protocols, 2023). Zero-knowledge cryptography is based on the concept of "a convincing deceiver", where one entity, called the verifier, can be convinced that another entity, called the prover, possesses certain information without learning anything more about it. That's it is achieved through the interaction between the verifier and the tester, where a series of tests is carried out. Challenges and answers that allow you to verify the validity of the Affirmation without revealing additional details.

Let's illustrate it with an example: Alice and Bob face a particular challenge, Bob is color blind and cannot differentiate the Colors red and green. However, Alice has in her hands two identical balls that differ only in color: one is red and the other is green. Alice's goal is to demonstrate to Bob that the balls are different, without revealing more information. The Tester is Alice and the Verifier is Bob.

1. Alice shows the two balls to Bob and explains that they are different, but Bob cannot tell them apart.
2. To start the demonstration, Alice asks Bob to put both balls behind her back and instructs him to sample one of the balls and then hide it again.
3. Then, Alice tells Bob that she has an option to either show the same ball she initially showed or change it to the other ball.
4. Each time Bob shows a new ball, Alice indicates it whether she changed the ball or not.
5. Alice continues guessing correctly if Bob changes the ball on each successive Turn.
6. As Alice continues to guess correctly, it becomes more and more likely that the balls are different.
7. Through this interaction and Alice's consecutive correct guesses, Bob becomes convinced that the balls are different without Alice having to explicitly reveal why.

Zero-knowledge tests have several main characteristics. First of all, the verifier cannot obtain anything useful from the protocol, which means that it cannot acquire sensitive information from it. Secondly, the verifier does not have the ability to impersonate the Tester that has been verified. That's it implies that messages exchanged during the protocol cannot be used to impersonate the tester being verified. Third, the probability that the verifier will accept a false statement as true is extremely low. Finally, the probability that the verifier will be convinced of a declaration that is true is very high [1].

Therefore, a zero-knowledge proof must meet three basic characteristics:

Completeness: If the Assertion is true, the verifier can be convinced of it by the prover.

Solidity: If what you want to prove is false, the verifier cannot be fooled

Zero Knowledge: The verifier will not be acquired additional information, except the Truth of the Assertion.

The first two attributes are required by any verification system; It is zero knowledge that is characterized by a ZKP method. These protocols are essential to guarantee privacy and security contexts such as cryptocurrencies and authentication in distributed systems [2]. These types of tests are divided into two types: interactive and non-interactive. Both involve a verifier and a tester, with the aim of the latter proving the veracity of a statement.

Non-interactive tests do not require interaction between the Tester and the verifier. The Tester presents a test that the verifier can analyze at any time to determine its validity. This process can be performed offline and does not require a shared communication channel to validate one test. Interactive testing involves an exchange of messages between the Tester and the Verifier. In this protocol, the prover attempts to “convince” the verifier of the veracity of a statement through an interactive game. These tests are probabilistic and require that the verifier be polynomially bounded. The prover, which is not generally computationally limited, must have a computational advantage over the verifier. These tests allow us to test statements that would not be possible with a non-interactive method, so They have greater expressive power. Typically, zero-knowledge protocols have one structure formed by 3 steps.

$$\begin{aligned} A \rightarrow B: &\quad witness \\ A \leftarrow B: &\quad challenge \\ A \rightarrow B: &\quad response \end{aligned}$$

Figure 1: Scheme of a zero-knowledge protocol [3]

In Figure 1, A has the role of Tester and B has the role of verifier. A provides a witness (witness) to B,

which computes from a secret random value. That's it allows each of the executions of the protocol to be different due to randomization and also establishes a series of questions that the tester (and only an honest tester) will be able to answer to "test" their knowledge and then challenge (send a challenge) to A, selecting one of these questions. Finally, A submits his answer to the challenge and B verifies that it is correct, repeating the entire process several times until the possibility that A is cheating is as low as B wishes. Both the witness and the response that A sent to B do not provide any additional information about the secret that A knows, beyond the assertion of his knowledge [3].

In the class of non-interactive tests, a particularly interesting concept for demonstrating the integrity of the results of large calculations is that of SNARK, that is, non-interactive and succinct knowledge argument. With this term, we denote a test System that is:
Succinct: the size of the test is very small compared to the size of the declaration or witness, say the size of the calculus is Yes.

No interactive: does not require rounds of interaction between the Demonstrator and the verifier.

Argument: We consider it safe only for Demonstrators that have limited computational resources, meaning that demonstrators with sufficient computational power can convince the verifier of one The statement is incorrect.

Solid knowledge: it is not possible for the demonstrator to construct a proof without knowing a certain witness called for the declaration; Formally, for any demonstrator capable of producing one valid test, there is an extractor capable of extracting a witness ("knowledge") for the declaration. SNARK systems can be equipped with a zero-knowledge property that allows the test to be performed without revealing anything about the intermediate steps. These schemas are the zk-SNARKs. (Nitulescu).

zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of knowledge) are publicly verifiable tests that demonstrate that the Prover has secret data (a witness) that satisfy a certain public NP relation (class of non-deterministic polynomial problems). The test does not reveal anything about the secret data other than its validity. zk-SNARKs have two key strengths:
Privacy and efficiency: zk-SNARKs allow a tester to demonstrate that he knows a valid solution to a problem without revealing the solution itself. This is useful in situations where you need to verify the validity of a solution without exposing confidential details. For example, in cryptocurrencies like Zcash, zk-SNARK is used to verify transactions without revealing the addresses of senders and receivers.

Compactness: zk-SNARKs generate very short and efficient tests in terms of computational size. This is it crucial for applications like blockchain, where Storage space and processing time are limited [4].

A (zk-)SNARK protocol (like any other non-interactive test system) is described by three algorithms that function as follows:
Gen is the setup algorithm, it generates a necessary crs string used later in the testing process and some vrs verification key, sometimes assumed to be secret only to the verifier. Normally it executes a trusted party.

Prove is the testing algorithm that takes as input the crs, the declaration u and a corresponding witness w and generates the test π. Verify is the algorithm that takes as input the Verification vrs key, the u statement and the π test, and returns 1 "accept" the test or 0 "reject" [6].

2.2 Privacy and Confidentiality Challenges in the Context of Blockchain

In the blockchain scope, privacy and confidentiality are fundamental. Although Blockchain provides transparency and traceability, it can also present challenges in protecting user privacy and the confidentiality of sensitive information. On a public blockchain, all transactions are visible, which can raise concerns about the exposure of personal data. Additionally, the wallet address used in one transaction can be linked to the identity of the user. On the other hand, confidentiality refers to the protection of sensitive information. Smart contracts on the blockchain can contain confidential information, and there is a risk that this information is visible to all participants in the blockchain. These challenges highlight the need for solutions that preserve privacy and confidentiality in the blockchain. Zero-knowledge cryptography can play an important role in this regard, allowing parties to prove the validity of certain information without revealing additional details.

The main method to allow private transactions on blockchain networks is zero-knowledge tests. The challenge with blockchains is the publicly verifiable nature of the technology, and the puzzle is how transactions can be recorded on the public ledger in a shared trusted method (because it is trustless, i.e. trust derived) computationally) which, however, does not reveal the specific details of the transaction. In the basic blockchain instantiation (e.g. Bitcoin), the public ledger tracks the sender address, the recipient address, and the transaction amount. With the disclosure of Transactions addresses and amounts, blockchain analytics companies and other parties have been able to piece together transactions and link overall asset ownership balances to real-life personal identities. In recent years, there has been a movement to implement private transactions on public and enterprise blockchains in which the sender address and addressee, as well as the transaction amount, are masked or protected on the public ledger and in the Consensus process. Privacy-protected transactions can be confidential (protecting the quantity being transferred), anonymous transactions (protecting the addresses that indicate who is transferring to whom), or both. Although Blockchain Addresses provide some privacy due to their nature (addresses are typically 32-character alphanumeric codes), if they are exchanged publicly between people or other forms of voluntary transmission, they may be traceable in certain ways [7].

2.3 Mitigation of Challenges through Zero-Knowledge Cryptography

Zero-knowledge cryptography has found application in the context of blockchain as a solution to mitigate the challenges of privacy and confidentiality. Zero-knowledge proof is a fundamental concept within zero-knowledge cryptography that has been implemented in transactions that use blockchain technology.

In this context, zero-knowledge proof allows transactions to be validated by an unrelated third party who does not know any of the parties involved or the legal nature of the transaction. In the blockchain registry, the existence of a transaction is recorded, but

the identity, nature or cause of the transaction is not revealed to those outside the Blocks chain [8].

This has a significant impact on the legal environment outside of the blockchain environment, especially on rights such as property. For example, in the case of a crypto contract for the transaction of immovable property, ownership can be transferred without revealing sensitive details through the implementation of zero-knowledge cryptography.

In particular, by combining blockchain technology with ZKP protocols, it is possible to create systems that provide both the transparency and security of a blockchain and the privacy and confidentiality of ZKPs. This is achieved by storing encrypted data on the blockchain and using ZKP protocols to demonstrate the property or validity of the data without revealing the actual data in Yes. ZKPs are already used in cryptocurrencies such as Zcash, which uses zk-SNARKs for transaction verification even after they are encrypted.

Zero-knowledge cryptography offers several benefits in terms of privacy and confidentiality in the context of blockchain. One of the benefits is the protection of identity. By using zero-knowledge testing, transactions can be verified without revealing the identity of the parties involved. That's it helps preserve the privacy of users and avoids linking activities outside the blockchain to their identity.

Another benefit is the preservation of confidentiality. Through this type of cryptography, it is possible to prove the validity of certain information without revealing additional details. That's it allows you to protect the confidentiality of sensitive information, such as commercial agreements or personal data, while verifying the integrity of the transaction.

2.4 Zero-Knowledge Cryptography Protocols used in the Blockchain

There are different zero-knowledge protocols that have in common to demonstrate that something is known without having to say exactly what it is that is known.

ZKP schemas can be divided into two Categories: interactive and non-interactive. Compared to interactives, no interactives do not require multiple interactive communications in the demonstration process, which prevents collusion attack while ensuring higher security. Especially in blockchain applications, no interactives can prevent transaction confirmations. caused by repeated interactions in the chain, which allows improving the Privacy of the applications without affecting the performance of the chain.

Currently, zkSNARK is considered an efficient implementation of non-interactive zero-knowledge proof, and many Excellent algorithms have been developed successfully, such as Groth16, PGHR13, among others. Compared to other algorithms, Groth16 has a minimum calculation for concise Verification and one test. Therefore, The ZKP based on Groth16 is widely applied in blockchain-based cryptocurrency systems such as Zcash, Filecoin, and others [9].

Zcash is a cryptocurrency based on Bitcoin code. another popular cryptocurrency. Its main characteristic that differentiates it from Bitcoin is privacy, resulting from the use of a special form of ZKP: the already presented zk-SNARKs. In fact, Zcash was considered one of the first widespread applications of zk-SNARK and allows all public transactions of the Zcash blockchain to be open encrypted, but in turn validated under the network's consensus. Monero is another cryptocurrency very focused on the privacy of transactions. Monero signs the Transactions with a technique called multisignature, where several participants are needed to sign and the identity of the Signers is hidden [3].

Zcash can be described as a cryptographic protocol on a government Blockchain to place personal information. Its function is almost identical to that of Bitcoin. Transaction validators are miners and full nodes. Zcash uses zero-knowledge proofs to encrypt all information and only allows approved parties to see said information using decryption keys. This could not be done on a government blockchain until now, as it would prevent miners from verifying whether transactions are valid if everything has been encrypted in the past (Overview and applications of zero knowledge proof [6].

Monero uses ring signatures to achieve confidentiality in its transactions. Ringo signatures consist of a ring composed of a set of public keys, in which one of them corresponds to the signer and the rest are unrelated, and a signature, generated with that ring of keys and that anyone who verifies it cannot determine which member of that Set is the signatory [3].

The Monero protocol signature system must fulfill three main properties: signer ambiguity, linkability and unforgeability. The First property establishes the Ambiguity of a signature, in the sense that it can be proven that the signer belongs to a group, but without revealing which member of this group he is. That's it is used to obfuscate the origins of the funds in each transaction. The second allows two different messages that were signed by the same private key to be related. This prevents double-spending, that is, the same currency cannot be spent more than once. The latter establishes that no attacker can forge a signature, preventing the theft of Monero funds by those who do not possess the appropriate private key.

Monero also uses ZKP concepts in another crucial aspect of its privacy: the concealment of transferred amounts (amount hiding). Most cryptocurrencies communicate this information in plain text. Monero en Cambio uses commitment schemes and range proofs to hide this information [3].

The notion of commitment is at the heart of almost any construction of cryptographic protocols. In this context, committing simply means that a jaguar in a protocol is able to choose a value from some (finite) Set and commits to his choice in such a way that he

can no longer change his mind.

A commitment scheme is a cryptographic primitive that consists of a two-stage interactive protocol between two parties called sender and receiver. Both parts are considered polynomially probabilistic. The first stage corresponds to the commit of a message my, which would be the equivalent of closing one box with a value inside. The second stage consists of revealing the message to the receiver, corresponding to revealing what is in the box. Formally a commitment scheme has to fulfill two properties: hiding and binding. Hiding means a dishonest receiver cannot obtain any information from the message during the commit stage. Binding meaning that a dishonest sender cannot reveal two different messages after the commit stage, that is, it cannot select a message m in the commit stage and then reveal another message m' in the reveal stage.

Range proofs are a type of zero-knowledge proofs that allow you to prove that a number is in a certain rank without needing to reveal that number [3].

2.5 Example of Implementation

zkLedger, developed by members of the MIT Media Lab, is a system that uses distributed ledger technology and zero-knowledge privacy to enable confidential and secure transactions on a shared ledger. The purpose is to be a system that can be easily audited, without compromising Privacy at any time. The System zkLedger is divided into three Principal components:

The consensus layer: This layer uses a distributed Consensus Algorithm, such as Proof of Stake (PoS) or Proof of Work (PoW), among others available, to ensure the integrity of the shared ledger and validate transactions.

The Privacy Layer: This layer uses zero-knowledge cryptography to protect the privacy of Transactions on the shared ledger. Transactions will be masked through the use of zero-knowledge cryptographic proofs, meaning that neither party is required to reveal their private information during the transaction.

The Application Layer: This layer handles application logic and smart contracts, allowing users to interact with the shared ledger and perform transactions in a secure and private environment.

In summary, zkLedger uses zero-knowledge cryptographic testing to hide private transaction information while maintaining the integrity and security of the shared ledger. That's what makes zkLedger It is an attractive option for blockchain applications that require enhanced privacy and security, such as Decentralized finance and digital identity solutions [10].

2.6 Other Applications

In electronic voting, to preserve the privacy of the voter, a zero-knowledge proof can be used. That's it allows the voter to demonstrate that her vote is valid to an authority without revealing the value of the vote [11]. These tests are useful for implementing secure electronic voting systems, as can be seen in the proposals where use of this technology is made [12,13]. In group firms [12]. In this focus there must be an authority that issues identities for group members, authorizes new members to join and can even revoke members. The use of group signatures allows a person to demonstrate that they are part of a group without needing to reveal their identity. . Since the votes are anonymous, it is crucial to ensure that no false votes are submitted or that a person votes more than once.

In the proposal, the use of digital signatures is combined with zero-knowledge tests [13].

This type is also used in remote authentication test The fundamental objective of remote authentication entities present from their origins vulnerability to identity theft fraud given the characteristics inherent to the process used In simpler and less secure protocols such as user-password, otherwise The necessary precautions are taken, a spy can capture the password and from that moment on imitate the legitimate user. Other protocols improve the situation by associating the password with something owned (two-factor authentication) or something inherent (biometric authentication). Another category includes challenge-response protocols in which an interactive dialogue is established between the verifier who poses challenges and the claimant who responds to them. Whatever the mechanism, the claimant tests your identity by waiting for you to possess a piece of secret information, yes. be exclusive or statistically associated with your person. However, in the majority of instances, proof of identity arises from the partial (or even total) exposure of your secret information. Even if secret information is partially exposed, an attacker can capture the parts to reconstruct enough information to commit identity fraud. This is the situation aggravated because in general the part of information revealed is variable and the number of authentication sessions progresses over time, thereby increasing the efficiency of this attack. Faced with these limitations, Authentication protocols were developed that, despite using secret information, they do not leak it during the test based on ZKP. The zero-knowledge property implies that a pretender who executes the protocol (even interacting with a malicious verifier) does not release any information (about its secret) and that this secret is not even computable in polynomial time from the public information it supplies. during the exchange. Therefore, her participation does not increase the risk of Imitation of Identity Fraud [3].

2.7 Current Challenges

The application of zero-knowledge cryptography in the context of blockchain poses significant challenges that must be addressed for its effective adoption. Among these challenges were computational efficiency, scalability and interoperability. Zero-knowledge cryptography protocols can be computationally expensive, so it is essential to investigate methods to improve efficiency and reduce computational load. As blockchain networks grow in size and complexity, scalability has become a crucial challenge. It is essential to explore scalable solutions that allow the efficient application of zero-knowledge cryptography in distributed

systems. In addition, integrate zero-knowledge cryptography with other protocols and systems in the Blockchain requires careful research to achieve this one Harmonization effective.

3. Conclusions

This research work has provided an updated vision of zero-knowledge cryptography and its application of blockchain technology. The theoretical foundations of zero knowledge cryptography, its practical applications and limitations have been addressed, and the existing protocols applicable to blockchain have been explored. Zero-knowledge cryptography has emerged as a promising tool to address the challenges of Privacy and confidentiality in the blockchain environment. Through its ability to allow parties to prove that an assertion is met without revealing additional information beyond the veracity of the assertion itself, zero-knowledge cryptography can help ensure privacy and confidentiality in transaction transactions. blockchain. Several zero-knowledge cryptography protocols applicable to the blockchain have been examined. These include interactive and non-interactive zero-knowledge protocols, with emphasis on those used in the cryptocurrencies Zcash and Monero. Furthermore, an example of implementation has been presented of zero-knowledge cryptography on the blockchain through the zkLedger System. This system uses zero-knowledge cryptography to allow confidential and secure transactions on a shared ledger, providing a practical example of how zero-knowledge cryptography can be used to improve privacy and security in blockchain applications. Finally, several current challenges have been identified in the application of zero knowledge cryptography in the blockchain, including computational efficiency, scalability and interoperability. These challenges underscore the need for continued research in this field to develop robust and efficient solutions that enable the effective adoption of zero-knowledge cryptography in blockchain technology [14].

References

1. Hernández Fernández, D. (2020). Zero knowledge proofs.
2. Moya, C. V., Bermejo Higuera, J. R., Bermejo Higuera, J., & Sicilia Montalvo, J. A. (2023). Implementation and Security Test of Zero-Knowledge Protocols on SSI Blockchain. Applied Sciences, 13(9), 5552.
3. Bukovits, Nicolás Axel. 2023. Zero knowledge proofs and their practical applications.
4. Petkus, M. (2019). Why and how zk-snark works. *arXiv preprint arXiv:1906.07221*.
5. Nitulescu, A. (2020). zk-SNARKs: A gentle introduction. *Ecole Normale Superieure*.
6. Hasan, J. (2019). Overview and applications of zero knowledge proof (ZKP). *International Journal of Computer Science and Network, 8*(5), 2277-5420.
7. Swan, M., Dos Santos, R. P., & Witte, F. (2020). *Quantum computing: physics, blockchains, and deep learning smart networks*.
8. Gutierrez, Eduardo de Celis. Fundamental rights and Blockchain technology. Fundamental rights and blockchain technology.
9. Digital identity verification and management system of blockchain-based verifiable certificate with the privacy protection of identity and behavior. Song, Zhiming, et al. 2022.
10. Fajardo, Wanden-Berghe. 2023. Blockchain and artificial intelligence in the accounting information system: the disruption of Triple Entry. 2023.
11. Cabarcas Jaramillo, D. Electronic voting and related cryptographic challenges.
12. Study and analysis of electronic voting schemas using anonymous digital signature protocols. Spurs, Gonzalo José Abad-Pérez. 2017
13. Development of a verifiable electronic voting system based on zero-knowledge tests. Garcia, Alfonso Camblr. 2021.
14. Pastor-Galindo, J., Nespoli, P., Mármol, F. G., & Pérez, G. M. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. *IEEE access, 8*, 10282-10304.