Evolution of Zero-Knowledge Proof (ZKP) and its role in blockchain applications for ensuring data privacy

1Liz George, 2Dr.Jubilant J Kizhakkethottam
1Asst.Professor, 2Professor
1St.Joseph's College of Engineering and Technology,
2Saintgits College of Engineering & Technology

Abstract - **Last decade has witnessed a flourish in blockchain applications on account of the transparency, immutability and data privacy it offers. It allows users to act anonymously and perform transactions with high-end security. Counter measures to prevent various attacks that compromises the privacy of blockchain applications and improvising existing privacy mechanisms is the main concern in this area. Zero Knowledge proof is a cryptographic technique which has the potential to revolutionize the way data is collected, used and transacted with. It allows the user to hide the information that he possess but still able to prove its validity to others, thereby opens far-reaching prospects in the privacy preservation mechanism of blockchain applications. This paper gives an insight about the various Zero Knowledge Proof protocols like NIZKP, ZKRP, zk-SNARK, Bulletproof etc. that have evolved over time, and its role in privacy management in the era of blockchain.**

keywords - **blockchain, zero knowledge proof, privacy, cryptography**

I. Introduction

The encryption scheme, 'zero knowledge proof' which is widely popular in terms of the privacy and anonymity it offers, was first proposed in the 1980s by MIT researchers Shafi Goldwasser, Silvio Micali and Charles Rackoff, while working on problems related to interactive proof systems. These are theoretical systems where a first party (called a 'Prover') exchanges messages with a second party ('Verifier') to convince the Verifier that some mathematical statement is true. [1] The prover even though in possession of infinite computational resources, cannot be trusted, while the verifier has limited computation power but is expected to be always honest. Messages are exchanged between the verifier and prover until the verifier has the answer to the problem and is "convinced" that it is correct.

Most work in the area of interactive proof systems focused on the soundness of the proof system, where a malicious prover attempts to 'trick' a verifier into believing a false statement. It completely neglected the scenario where in the verifier is not trust worth, which in turn might lead to information leakage. 'Zero Knowledge Proof' was proposed by Goldwasser et.al as a solution to the information leakage problem where the prover can prove statements, without revealing any information to the verifier. [2]

II. PRELIMINARY ASPECTS REGARDING ZKP

2.1 Properties of ZKP Protocol

There are three properties that every zero-knowledge protocol must satisfy [3].Stated informally, they are:

- Completeness: If the statement is true, the honest verifier (who follows the protocol properly) will be convinced of this fact by an honest prover.
- Soundness: If the statement is false, no cheating prover can convince the honest verifier that it is true, except with some
 small probability. This guarantees the security for the Verifier against a malicious Prover
- Zero-knowledge: If the statement is true, no verifier learns anything, except the fact that the statement is true.

Completeness and soundness are properties of interactive proof systems. The addition of the third property "zero-knowledge" turns the verification process into a zero-knowledge proof.

2.2 General structure of ZKP

The general structure of a zero-knowledge proof consists of three sequential actions between the prover A and the verifier B called commitment, challenge, and response.

- Commitment: A commits to a particular value and transfers the commitment to B
- Challenge: B chooses a random challenge and sends it to A
- Response: A calculates the response to the challenge and sends it back to B.

The received response allows B to check that A really knows the secret. The procedure can be repeated as many times as you want, until B is convinced that A knows the correct answers rather than the probability that A makes guesses, proving that A knowns the secret.

A very simple example presenting the idea of ZKP is 'The Ali Baba Cave'. [4] [5] In this, Peggy (the prover) knows the secret word used to open a magic door in a cave. The cave is circular shape, with the entrance on one side and the magic door blocking the opposite side. Peggy wants to convince Victor (verifier) that she knowns the secret, but she is not willing to disclose the secret word. They devise a scheme by which Peggy can prove that she knows the word without telling it to Victor. They named the 2 paths of the cave reaching to the magic door as A and B. Peggy goes into a random path of the cave without letting Victor knowing which path she chose. Standing at the entrance to the cave, Victor calls out the path name he wants Peggy to come out from. If Peggy indeed knows about the secret password, she can obey every time the process is repeated.

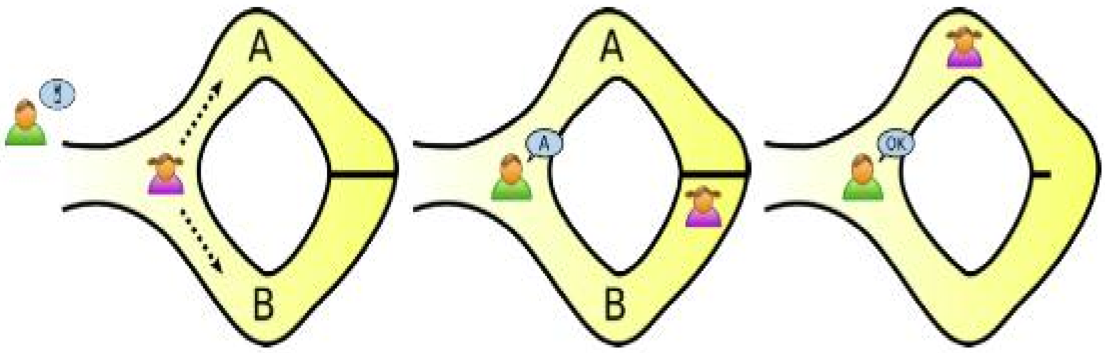

Fig:1

III. CLASSIFICATION OF ZKP

There are two types of ZKP. They are:

- Interactive zero-knowledge proof
- Non-interactive zero-knowledge proof

3.1 Interactive zero-knowledge proof

Interactive zero-knowledge proof performs a series of actions under the mechanism of mathematical probability to convince the verifier of a particular fact. Here prover can prove the fact to the verifier without disclosing it. Interactive zero-knowledge proof is limited in transferability. This means that people other than verifier are unable to verify the outcome of the demonstration. Also the repeated interaction involved in ZKP makes it unfeasible for a distributed network.

3.2 Non-Interactive Zero-Knowledge Proof

Non-interactive zero-knowledge proof excludes the series of interaction between the prover and the verifier. In this, the prover will send only one message to the verifier, restricting the collision in the channel. This system is widely used in the construction of various types of cryptographic protocols and encryption algorithms.

IV. RESEARCH PROGRESS IN NIZKP

A typical ZKP involves successive exchange of messages in the form of challenges and responses, which can be infeasible due to possible connection failures during the protocol. NIZK proof system based on the Common Reference String (CSR) model was proposed in the year 1988 by [6] to deal with this problem. Non-interactive zero knowledge proof consists of three entities: a prover, a verifier and a uniformly selected reference string. Both the prover and verifier get access to the same string, provided by a trusted third party. A message is sent by a prover to verifier, which can be better used in the construction of cryptographic protocols. In a NIZKP, all of the challenges of a typical ZKP are condensed into a single package sent in a single message which leads to the optimization of the time necessary for the exchange of messages. The introduction of NIZKP instigated further research in this area, resulting in development of NIZKP of NP problems, construction of public key encryption and signature schemes, where reference string may be incorporated in the public key.

Later Gorth et al. [7] suggested application of NIZKP to specific problems, improving the efficiency and practicability of NIZKP, thereby creating a new line of research in this area.

4.1 Basic Concepts

NIZK proof systems exist for every NP language. [8]
A language L is said to be a NP language if it is possible to define it using a polynomial-time computable relation R: a statement x is in L iff there exists a small witness w such that R(x,w) = true

Let R be an efficiently computable binary relation. Let (x,w) ∈ R where x is the statement and w the witness and L be the language consisting of statements in R. An argument system for R consists of K the key generation algorithm, the prover P and the verifier V. The common reference string σ. Is produced as the output of key generation algorithm. The prover accepts the input (σ,x,w) and produces a proof or argument π, if (x,w) ∈ R. The verifier takes as input (σ,x,π) and outputs 1 if the proof is acceptable or 0 otherwise.

Later, in the same year de Santis et al. proposed NIZK with pre-processing. Non-Interactive Zero-Knowledge Proof-Systems with Pre-processing have a pre-processing stage and a communication stage [9]:

1. Pre-processing stage: In this stage the prover A, chooses an n-bit theorem T_o and proves interactively and in zero-knowledge
to the verifier B, that the theorem To is true.

2. Communication stage: Prover, A proves to the verifier B any NP theorem of length not bigger than n^c, for some fixed positive
constant c < 1. This proof is unidirectional (from A to B) and zero-knowledge as B is only confirmed of the validity of the
theorem, doesn't have any additional knowledge of the theorem proved.

The prover and the verifier are allowed to interact in a preamble phase that depends only on the parameters for the problem (before the prover and the verifier see the actual statement that the prover needs to prove). This model is a stronger one, since the prover and the verifier can use the preamble phase to generate a common random string. [10]

4.2 Zero-Knowledge Range Proofs

The first practical construction of zero Knowledge range proofs was proposed by Boudot in 2001 [11] .ZKRP holds the same three properties as ZKP, which are completeness, soundness and zero-knowledge Zero Knowledge Range Proofs (ZKRP) allows to validate that a determined piece of private information belongs to a numeric interval. This property can be used to ensure compliance, while preserving a client's privacy [12].ZKRP can have wide range of applications like, allowing the user to maintain anonymity, by providing range proofs for relevant attributes like income and age while availing loan, to electronic voting where the user is able to prove that he is in the eligible age range to cast a vote

4.3 zk-SNARK

The acronym zk-SNARK stands for "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge" is a variation of NIZKP with no interaction between the prover and verifier. A 2012 article by Bitansky et al. introduced this protocol [13] which provides the computational backbone of the Zcash blockchain protocol.

Both zk-SNARKs and NIZKs require a one-time trusted setup of public parameters and guarantees completeness, proof of knowledge, and zero knowledge. The difference lies in efficiency. In zk-SNARKs proof size is reduced considerably, which was a concerning factor for complex applications which uses NIZKP.In a NIZK, the proof length and verification time depend on the NP language being proved. For instance, for the language of circuit satisfiability, the proof length and verification time in are linear in the circuit size. But the proof length in a zk-SNARK depends only on the security parameter, and verification time depends only on the instance size (and security parameter), but not on the circuit or witness size. Thus, zk-SNARKs can be thought of as "succinct NIZKs", having short proofs and fast verification times.

Confidentiality of system parameters is the main concern in SNARKs. The parameters should be generated in a trusted way. Anyone with access to the parameters can create false proofs and convince the verifier, violating soundness of the system. In view of defending the cryptanalytic efforts, latest researches have proposed zk-SNARK based on lattice assumptions [14] , which are believed to be post-quantum secure. Sonic, a zk-SNARK implementation uses a universal and repeatedly updatable structured reference string that scales linearly in size, provides constant size proofs. Marginal decrease in cost is guaranteed in the context of batch verification [15].

4.4 Bullet proofs

Bulletproof a non-interactive zero- knowledge proof protocol with very short proofs and without a trusted setup was released in 2017 [16] . The proof size is only logarithmic in the witness size. They are suitable as range proofs on committed values. Bulletproof use the Fiat-Shamir heuristic in order to become non-interactive and uses the discrete logarithm concepts for security. This leads to bulletproof increasing in size only logarithmically with the number of outputs and size of the range's proof. Not restricting itself to range proofs, Bulletproofs can also be used to prove generic statements, making them suitable for providing privacy to DTL [17].

4.5 zk-STARK

In 2018, the zk-STARK (zero-knowledge Scalable Transparent ARgument of Knowledge) protocol was introduced [18] , an efficient version of zk-SNARK with no need for trusted setup (transparent).It is considered to be potentially faster to generate and cheaper depending on the implementation. Zk-STARK do not require an initial trusted setup because they rely on cryptography through collision-resistant hash functions. This gave way to the elimination of computationally expensive number-theoretic assumptions of zk-SNARKs that are inclined to attack by quantum computers. The supreme feature of zk-STARK is its scalability, as it can move computations and storage off-chain. But one major disadvantage is that the size of the proofs is bigger when compared to zk-SNARK.

V. ZKP AND BLOCKCHAIN

The Distributed Ledger and Blockchain are two thriving technologies whose scope has expanded to a wide variety of application, as it helps to generate consensus among parties that do not fully trust each other, eliminating the need for trusted third party. In public blockchain the transactions can be viewed by everyone in the network as it is broadcasted to all participants. This is an issue, if transactions contain privacy sensitive information. ZKP provides a solution to this issue, by only making available the information that a valid transaction has taken place, hiding details regarding the sender, recipient and type/quantity of asset transferred.

ZKP allows an entity called prover to convince another entity verifier that a statement is true without revealing further information about the statement. In blockchain, the above feature of ZKP can be utilized to perform valid transactions, adhering to the constraints specified by smart contracts without compromising privacy.zk-SNARKs, with its very short proofs and verification times can be used as transaction data, hiding all the private details which can be later verified by a smart contract [19].

Cryptocurrency transactions can be effectively validated using Zero-knowledge proofs without revealing the details like, which wallet a payment came from, where it was sent, or how much currency is involved. One of the most popular techniques is zk-SNARKS which is effectively implemented by the cryptocurrency ZCash to ensure transaction privacy. Later developments came in this field in the form of BlockMaze [20] , providing an efficient privacy-preserving mechanism for transactions in account-model blockchain. There could be other use cases also, such as proving one's age without sharing date-of-birth or proving one's identity without sharing details of their identity proof, etc. Bulletproofs provides an efficient way for maintaining data privacy of transactions. Latest researches have proposed Shellproof which adopts the design of bulletproofs and provides the same efficiency with half the computational cost [21].

Interactive ZKP is not suitable for Blockchain applications, as, the prover and the verifier needs to communicate many rounds to prove the challenge/statement, because the validating nodes may not be able to agree upon how to choose a challenge.

While ZKP used with blockchain does solve the problem of data privacy and security for cryptocurrency use cases, the current implementations require significant computational power to generate the zero knowledge proofs. As complexity of the problem to be solved increases, the proof generation, which involves executing arithmetic circuits in the range of 106 to 1012, becomes more compute intensive. Therefore, efficient and modular ZKP implementations are the need of the hour.

CONCLUSION

The inherent privacy and authentication properties of Zero Knowledge proofs make them a suitable approach to construct cryptographic protocols. Focusing on optimizing their efficiency for specific problems and applications and making particular improvements in various different parameter scenarios research on zero-knowledge proof systems has been progressively improving. The introduction of block chain technology and later the implementation of private block chains have accelerated the research works associated with this area. The main objective was to reduce the proof size which was achieved through the implementation of zk-SNARKS, Bullet Proofs and later zk-STARKS. The smart contracts in block chain applications can use zk-SNARKs for privacy management but with the cost of a new trusted setup for each contract. Bullet proofs are suitable for implementing private smart contracts, as it avoids the trusted setup and guarantees small proofs. Supersonic [22] , a latest breakthrough in the SNARK, guarantees very small proof size (around 25 times smaller) and comparable verification times. It is expected to boost the collaboration of blockchain in financial sector, ensuring secure and fully compliant transfer of financial assets and their verification. Latest research in this area is the construction of post-quantum zero knowledge proofs which are quantum-resistant [23].

REFERENCES

[1] M. S. S Goldwasser, "Private coins versus public coins in interactive proof systems," in *Proceedings of the eighteenth annual ACM symposium on Theory of computing*, 1986.

[2] S. C. S.Goldwasser, "The Knowledge Complexity of interactive Proof Systems," in *Proceedings of the17th ACM Symposium on Theory of Computing*, 1985.

[3] Oded Goldreich , Yair Oren, "Definitions and Properties of Zero-Knowledge," *Journal of Cryptology,* pp. 1-32, 1994.

[4] J.-J. Uisquater, L. C. Guillou and T. A. Berson, "How to explain zero-knowledge protocols to your children," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).*

[5] B. M. Li Feng, "A survey on zero-knowledge proofs," *Advances in Computers,* p. 25–69, 2014.

[6] F. P. S. Blum M, "Non-interactive zero-knowledge and its applications," in *Proceedings of the Annual ACM Symposium on Theory of Computing*, 1988.

[7] O. R. A. Groth J, "Perfect Non-Interactive Zero Knowledge for NP," in *Lecture Notes in Computer Science* , 2006.

[8] S. M. W. Oded Goldreich, "Proofs that yield nothing but their validity and a methodology of cryptographic protocol design," in *27th Annual Symposium on Foundations of Computer Science*, 1986.

[9] S. M. a. G. P. A. de Santis, "Noninteractive zero- knowledge with preprocessing," *Advances in Cryptology— CRYPTO '88,* p. 269–282, 1988.

[10] R. R. Yael Tauman Kalai, "Succinct Non-Interactive Zero-Knowledge Proofs with Preprocessing for LOGSNP," in *47th Annual IEEE Symposium on Foundations of Computer Science*, 2006.

[11] B. F, "Efficient proofs that a committed number lies in an interval," *Lecture Notes in Computer Science,* vol. 1807, p. 431–444, 2000.

[12] T. K. C. V. W. A. K. E Morais, "A survey on zero knowledge range proofs and applications," *SN Applied Sciences,* 2019.

[13] R. C. C. T. Nir Bitansky, "From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again," in *Proceedings of 3rd innovations in Theoritical Computer Science Conference*, 2012.

[14] M. M. N. O. Rosario Gennaro, "Lattice-Based zk-SNARKs from Square Span Programs," in *ACM SIGSAC Conference on Computer and Communications Security*, 2018.

[15] S. B. K. M. Mary Maller, "Sonic: Zero-Knowledge SNARKs from Linear-Size Universal and Updatable Structured Reference Strings," in *ACM SIGSAC Conference on Computer and Communications*, 2019.

[16] J. B. D. B. P. P. W. G. M. Benedikt Bunz, "Bulletproofs: Short Proofs for Confidential Transactions and More," in *Proceedings - IEEE Symposium on Security and Privacy*, 2018.

[17] P. I. K. L. Zhang, "Adding Confidential Transactions to Cryptocurrency IOTA with Bulletproofs," in *International Conference on Network and System Security* , 2018.

[18] I. B. Y. H. M. R. Eli Ben-Sasson, "Scalable, transparent, and post-quantum secure computational integrity," 2018.

[19] A. M. Pinto, "An Introduction to the Use of zk-SNARKs in Blockchains," in *Mathematical Research for Blockchain Economy*, 2020.

[20] Z. W. Y. Y. Y. Z. B. H. Zhangshuang Guan, "BlockMaze: An Efficient Privacy-Preserving Account-Model Blockchain Based on zk-SNARKs," *IEEE Transactions on Dependable and Secure Computing* , 2020.

[21] C. X. Q. Z. Xianfeng Li, "Shellproof: More Efficient Zero-Knowledge Proofs for Confidential Transactions in Blockchain," in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2020.

[22] B. F. S. Benedikt Bünz, "Transparent SNARKs from DARK Compilers," in *International Conference on the Theory and Applications of Cryptographic Techniques* , 2020.

[23] T. Z. Thomas Vidick, "Classical zero-knowledge arguments for quantum computations," *Quantum,* vol. 4, p. 266, 2020.