WHAT IS ZERO KNOWLEDGE PROOF AND ITS ROLE IN BLOCKCHAIN?

Talk to our Consultant

Listen to the article

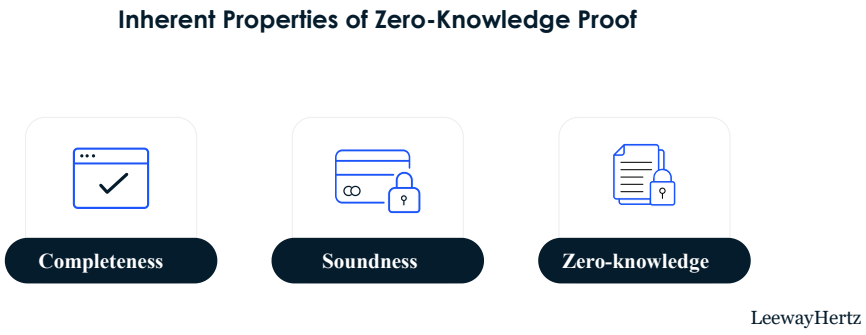
With the advancement of technology, the scope of fraudulent activities has also risen with time. Hence, maintaining security protocols is one of the major tasks in the process of transactions. While blockchain has come up as one of the promising innovations, we need additional security standards for maintaining security in transactions. In such circumstances, Zero Knowledge Proof or ZKP is a good option.

Cryptography has been associated with blockchain right from its inception. However, the combination of blockchain and cryptography has attracted people's attention recently after ZKP was introduced. Cryptographic techniques are used to secure the transaction fully on a blockchain platform. In other words, the amalgamation of blockchain and cryptography has given a secured mode of financial transactions.

What is Zero-Knowledge Proof?

Zero-Knowledge Proof is a cryptographic technique where no information is revealed during a transaction except for the interchange of some value known to both the prover and verifiers (the two ends of the process). The idea behind zero-knowledge proof is that a user can prove to another user that they know an absolute value without actually revealing any other or extra information.

ZKPs have the following three inherent properties:



- **Completeness**
  The completeness property notes that the transaction is verified, and the prover is permitted for processing the transaction ahead. When the transaction statement is true, the verifier has the authority to permit the prover for the input he requested earlier.
- **Soundness**
  The soundness property notes that the transaction is correct and not a part of any fraudulent case. It means that if the transaction situation is otherwise and the statement is wrong, the verifier cannot be convinced in any case. In this situation, the verifier cannot certify the prover or permit the prover's request for the inputs.
- **Zero-knowledge**
  The verifier cannot have any information other than the current statement and the statement's authenticity being true or false. Any other information and private data of various parties will be hidden.

At the top level, creating a Zero-Knowledge Proof requires the verifier's questioning of the prover to go through a series of actions that can be performed when the prover knows all the required information correctly. The prover will eventually be proven wrong by the verifier's test with a higher degree of probability.

What are the two fundamental types of Zero-Knowledge Proof?

The two fundamental types of ZKPs include the following:

- **Interactive ZKP**
  The actions associated with the concepts deal with mathematical probability. In interactive ZKP, a prover needs to convince a specific verifier and repeat this process for each verifier. In interactive ZKPs, the prover must complete a series of actions to convince the verifier about a specific fact.
- **Non-Interactive ZKP**
  Non-interactive ZKPs don't have any voluntary interaction between the verifier and the prover. In non-interactive ZKP, a prover creates proof that anyone can verify, and the verification process can also be moved to a later stage. For a better mechanism of non-interactive ZKPs, they need specific software.

Let's now understand the concept of ZKP and its usage with technology. One prominent usage of Zero-Knowledge proof is Zcash. Zcash is the initial application of zk-SNARKs and the fundamental form of Zero-Knowledge cryptography.

Now we need to understand what is zk-SNARKs. zk-SNARKs is an acronym for Zero-Knowledge Succinct Non-Interactive Argument of Knowledge. zk-SNARKs is a technology that uses non-interactive ZKP.

zk-SNARKs works on the following three algorithms.

- **Key Generator**
  A key generator establishes a parameter to generate a key pair. Here, a trusted source can delete the private information after generating a private or public key pair. Then, another key pair is generated using the public information. Of this pair, one would be used for proving and another for verifying.
- **Prover**
  The prover gets proving key and needs to prove his knowledge. He will receive and verify the private key and then shall forward the statement.
- **Verifier**
  The verifier will get the input from the prover and will validate the statement's authenticity.

Zk-SNARKS need to maintain the following four properties too.

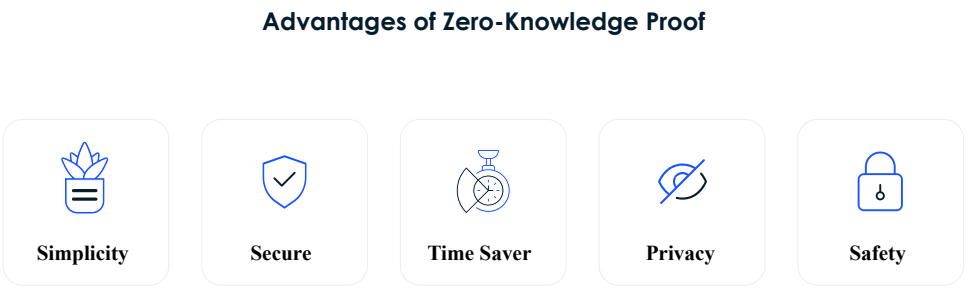
- The verifier won't learn anything other than the statement. If there is a challenge that needs to be succinct, it should need only a few milliseconds for execution.
- Non-interactive: the process should be non-interactive.

- The proof should follow the principle of soundness, having zero-knowledge encryption.
- Prover and verifier cannot carry on with the process without a trusted witness.

What are the various use cases of Zero-Knowledge Proof on the blockchain?

- **Messengers on blockchain**
  Although messengers we have nowadays promised to be encrypted, unencrypted blockchain can be the next big thing in the technological world. With the guarantee of an un-encrypted yet robust solution, ZKPs and blockchain can co-create a value-added messenger platform secured for one and all.
- **Next-gen file system controls**
  ZKPs can help in adding multiple layers of security to files, logins. As a result, ZKPs can present notable obstacles for hackers or manipulators to alter and retrieve the data.
- **Protection of storage**
  ZKPs include a security protocol with the information included in the storage unit. The access channels have formidable safeguards that create a highly secure and seamless environment.
- **Transferring private blockchain transactions**
  The most notable concern in private blockchain transactions is numerous loopholes evident in conventional procedures. The productive integration of ZKP with private blockchain transactions can create a powerful hacker-proof process.
- **Data Security**
  Organizations that control sensitive data, such as banks and hospitals, must keep them free from third-party access. ZKPs and blockchain together can make accessing data impossible.

What are the advantages of Zero-Knowledge Proof?



LeewayHertz

Advantages of Zero-Knowledge Proof:

- **Simplicity**
  Simplicity is probably the most noted attribute of ZKPs. It does not require any software knowledge to operate but can offer superior solutions that impact our daily lives. Moreover, as it is completely un-encrypted yet highly secure, it can offer the best of both worlds seamlessly.
- **Secure**
  ZKPs are extremely secure when it comes to sharing information. So, a user can use it with confidence while not having to master the codes or analytics to understand its basics.
- **Time saver**
  ZKPs shorten the time required in blockchain transactions, offering value to users in a noble manner.
- **Privacy**
  Safeguarding the privacy of its users is the most appreciated characteristic of ZKPs. It never requires sensitive data-sharing and hence is supremely private in general.
- **Safety**
  Users of ZKPs are aware of the need for ZKPs to share data, and they can stay away from any company that needs access to personal information without a valid reason.

Applications of Zero-Knowledge Proof

Apart from some blockchains such as ZCash, ZKPs are also used in private transactions that do not reveal monetary data and receiver and sender information. The decentralized Oracle networks that provide smart contracts off-chain data can also leverage ZKPs some facts about off-chain data without actually exposing on-chain information.

DECO, a privacy-controlled oracle protocol within the Chainlink's network, uses ZKPs in the blockchain. DECO guarantees that data will remain private and tamper-proof by extending HTTPS/TLS, the most basic data transfer protocols. DECO uses the most modern version of TLS, needs no special hardware, and

works in a backward-compatible manner, without any server-side changes. So, DECO-enabled chainlink oracle nodes can check the proof of data sourced from trusted servers without revealing on-chain data. DECO-like smart contracts enable banking and financial institutions to offer undercollateralized loans, where the borrower has proven creditworthiness. The borrowers can generate the credentials depending on records from authoritative sources without revealing sensitive personal or professional data.

Decentralized Identity protocols such as CanDID are a platform powered by ZKP where users can retrieve their information and credentials without relying on a third party. These credentials are signed by issuers who can authoritatively connect claims with users, including citizenship, occupation, educational qualification etc. DECO allows an existing web server as the issuer with key-sharing management to back up accounts and privacy- a hidden form of Sybil resistance depending on definitive unique identifiers, such as Social Security Numbers (SSNs).

By providing a way to monetize the proprietary and sensitive datasets, DECO helps traditional institutions and data providers confidentially. Instead of posting all data on-chain, these service providers can use attestations accessed from ZKPs to prove facts about the data that will be published. It creates a new market for data providers to monetize and increase their dataset revenue with zero data leakage.

Endnote

ZKPs have a great potential in saving costs as well as preserving the privacy of the users. Moreover, it is easy to use, and the technologies that support ZKPs are also superbly efficient. By leveraging on the latest-generation ZKP, you can benefit hugely without having to spend a lot of money. To know more about ZKPs, consult with our enterprise-level ZKP experts today.