**Zero Knowledge Projects: A Rising Trend in Blockchain Technology**

Zero knowledge projects that are based over zero knowledge proof methodology are becoming noticeable in the current scenario. It is due to the ability to protect the details of the data from third parties, while securely completing the transactions. Though, it seems as a new-age mathematics over blockchain, but was actually introduced in the eighth decade of the twentieth century; which was much earlier than the base technology.

Blockchain is a peer-to-peer technology that removes the dependency on a centralized system while increasing transactions' security, reliability, and immutability. But despite its applicability to multiple use cases, blockchain is facing significant reluctance from financial institutions due to scalability and privacy concerns.

Transferring assets on the blockchain requires a network address instead of sharing the sender and receiver's names. But this does not cancel out the functionality of tracing the details of the two nodes, thus, breaching essential information regarding the transaction during the validation process. Here comes zero knowledge proof, or ZKP, which is now being stated as the perfect solution to the problem.

**The Mechanism of Zero Knowledge Proof (ZKP)**

ZKP is an advanced technology of decentralized transactions based on a prover and verifier that encapsulates the secrecy of transactional value while maintaining scalability. The fundamental formulation is that the exclusivity of the asset is never disclosed among the nodes. Here the prover puts the statement, which is to be validated by the verifier for authenticity, without getting any knowledge about the information in the transaction.

The experts have derived a few case studies to simplify the concept and explain the outcome of zero knowledge proof. Let’s understand some of them.

1. **Candy Boxes with Bob & Alice:** There are a few boxes with dissimilar number of candies in each. They are locked, and Bob & Alice have put a mark on one of which they own the lock-key. In this situation, if both of them put a mark on the same box, it is deducible that they have the same number of candies. While if the mark is on different boxes, they can only verify that the other person does owns a package but with an unknown number of candies.
2. **The Ali Baba Cave:** Here the cave has two doors that open with a code word from inside. Peggy and Victor are two friends standing beside the cave Peggy is supposed to know the code, while Victor has to verify whether she knows it. Peggy enters from one door, and Victor calls her to return from a specific door (A or B). It is a complicated case to find out if Peggy really knows the code word because Victor might call the same door name from which she has entered. But with multiple attempts the verifier can authenticate the truth. There is a lesser probability that Victor calls the same path every time from where she entered and returned easily, even if the code is unknown to her.
3. **Color-blind Person With Two Balls:** Another similar example is of a color-blind person and two different color balls. Now to find out if the balls are of the same or different colors, this color-blind person will ask another person with normal-eyesight. To verify his statement, the color-blind person will take the balls in his hand, switch them (or not as per choice) at his back, and ask the other person if he changed the balls. By multiple verifications, the chance of falsification by the prover reduces. If the other person is also color-blind, he has 50% chance of guessing the right color each time.

**Characteristics Followed in The Technology**

Here we can figure out three main properties of ZKP that get fulfilled in each transaction between the prover and the verifier.

1. **Zero Knowledge:** The technology itself ensures that the verifier can never interpret the details about the payments other than verifying that the statement is true.
2. **Completeness:** True statement by an honest prover will convenience an honest verifier.
3. **Soundness:** False statements by the prover will have a negligible probability of acceptance by the verifier.

**Where Can We Implement This System**

Zero knowledge proof technology has proven to be a systematic, safe, and authentic mechanism to support blockchain transactions with its add-on benefits. The tech start-ups in this sector have begun to approach it and find marketable solutions that grab the attention of the stakeholders. Here are some of the prominent applications of ZKP technology.

1. **Messaging:** This is one of the most conventional usages of ZKP, as it allows an encrypted format of sending and receiving messages between two parties without any traces of compromised information.
2. **Private Blockchain Transaction:** ZKP is considered a trusted protocol to manage private transactions when it is required to provide a cover from any third party which is intended in leaking the data. The system ensures to protect the privacy of the transaction.
3. **Authorization & Documentation:** It can be useful in sharing authorized data, such as documents, with complete security. Here the data is transmitted in an encrypted format with zero possibility of a breach.
4. **File System Control:** With multiple layers of protection, the ZKP technology can hide the detail of documents, user details, and login details as well.
5. **Voting Systems:** A highly demanded application of blockchain technology is in the democratic voting system in an organization. It could be nothing better than introducing ZKP technology into this, which can assure the voters to uphold their privacy concerns regarding the choices they make.
6. **Protecting Transaction Details:** It provides additional security to each block containing financial data, and only the block requested by the verifier gets decrypted.
7. **Storage:** It is a useful application for storage units that protect sensitive information while securing access channels.

**Types of Zero Knowledge Proofs**

ZKP is divided into two categories depending on its applicability.

* **Interactive ZKP:** This methodology requires continuous interaction between the prover and the verifier to validate the transaction. It requires sufficient analysis by the verifier to authenticate the statement of the prover.
* **Non-Interactive ZKP:** Here, the claims set by the prover are provisioned at once to the verifier and do not require rigorous interactions. The system implies necessary tools to determine the truth of the statement.

**Concept of ZK-SNARKs and ZK-STARKs**

The non-interactive ZKP is implemented in two different formats by the enterprises.

* **Zk-SNARKs**

It stands for Zero Knowledge Succinct Non-Interactive Argument of Knowledge. The method requires a trusted setup of the public blockchain. It ensures the privacy of data, minimal proof size for quick verification, single transaction for validation, and prevention from bad actors that have limited computational powers.

* **Zk-STARKs**

STARK is implemented with hash functions instead of computational soundness. It stands for Zero Knowledge Scalable Transparent Arguments of Knowledge. It is a lesser preferred system, although works viably to maintain off-chain scalability and transparency without needing a trusted setup.

**Zero Knowledge Projects: Few Examples**

ZKP is prominently accepted by companies that have readily applied the technology in a full-fledged format and are continuously exploring its usability to generate enhanced experience. ZCash and ING are organizations that have applied zk-SNARKs to provide reliable solutions. Here is a brief on some of the currently running zero knowledge projects.

1. **ZCash:**

ZCash or Zero Cash is a popular example of ZKP technology implementation that clearly ensures scalability and privacy in the transactions performed between the sender and receiver while keeping the data intact.

1. **ING:**

ING is a banking organization from the Netherlands and probably among the first to adopt an advanced version of the ZKP blockchain, known as a zero knowledge range proof system. The primary feature is the ability to generate mortgage value by proving to have a sufficient salary in the account but disclosing the actual value of the funds.

1. **Mina:**

It is a protocol that produces blocks as small as 22kb in size and allows projects to implement it with full smart contract systems.

1. **DECO:**

This is an oracle protocol by Chainlink network that uses ZKP to maintain data privacy. They have managed to secure HTTPS/TLS and use an advanced version without needing external hardware. So, the nodes under Chainlink verify the data from the trusted senders. It is even applicable in financial sectors for offering loans to an individual without revealing personal data. CanDID is another ZKP-based decentralized identity protocol that enables users to generate their credentials without the need for any third party.

1. **NuCypher:**

The non-interactive ZKP is applicable to verify the correctness of re-encryption. It is a network security protocol that creates re-encryption or proxy encryption to the public key. The purpose is to provide extra protection to an encrypted document that needs to be shared along with the private key. Now with a proxy encryption, the receiver has to open it with his private key, while the sender need not share his private key.

1. **StarkWare:**

The company follows a unique path of zk-STARKs technology rather than the conventional zk-SNARKs. It offers data privacy with scalability in a transparent system that does not require a trusted setup. The company also has designed software and hardware support for optimum results.

**Take Away: Is Zero Knowledge Proof Beneficial?**

ZKP is undoubtedly an advanced state of blockchain with reasonable acceptance in essential sectors like security and finance. The technology involves easy developmental procedures while maintaining the required validity features to ensure the transaction's authenticity. It offers some significant advantages like data privacy and scalability, which are discussed above.

But a major drawback of ZKP is the need for excessive computational procedures to minimize the probability validating false statement. Therefore, it becomes a bit costlier and time-consuming process, and yet not offering surety of authenticity. Many technologists have even shown concern related to transactional data, which may get lost if the sender forgets them.

But it is in the initial stage of development and implementation zero knowledge projects in blockchain technology. With the application of decentralized transaction systems in multiple scenarios, ZKP has a major role to play soon.