ZERO KNOWLEDGE PROOFS

by Marija Mikić

Zero Knowledge Proofs

Zero Knowledge proof is a cryptographic method by which we can prove that any information we have without revealing it: proof without knowledge (**Zero Knowledge Proof**).

The essence of Zero Knowledge proofs is that it is trivial to prove that one possesses knowledge of certain information by simply revealing it; the challenge is to prove such possession without revealing the information itself or any additional information.

*

You can find more information on these links:

[Link 1 >]
[Link 2 >]

Zero Knowledge Proofs

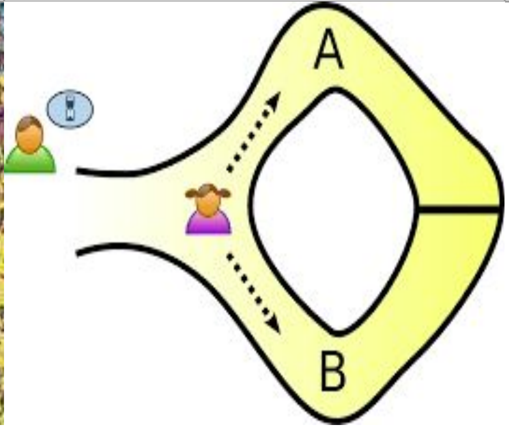
Zero knowledge proofs are not proofs in the mathematical sense of the word because there is a small probability, the **soundness error**, that a cheating prover can convince the verifier of a false statement. In other words: Zero-knowledge proofs are **probabilistic "proofs".**

History of zero-knowledge proofs:
Zero-knowledge proofs were first introduced in 1985 by Shafi Goldwasser, Silvio Micali and Charles Rackoff in their paper "The Knowledge Complexity of Interactive Proof-Systems”.

Although they were already discovered in the 1980s, they experienced their full bloom with the development of the blockchain.

There’s More 👉

Illustrative examples

➢ Where is Waldo?	➢ Ali Baba cave	➢ Color blind friend
		

*

You can find more information on these links:

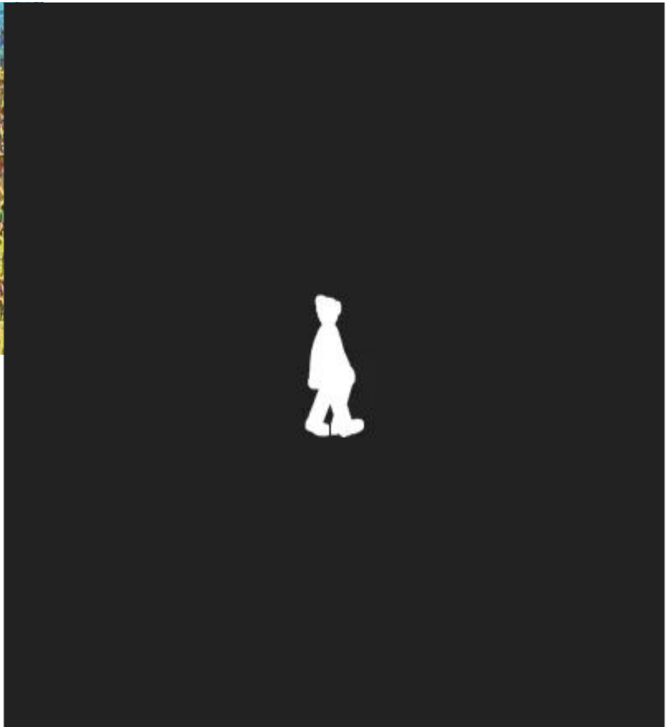
[Link 1 >]

[Link 2 >]

[Link 3>]

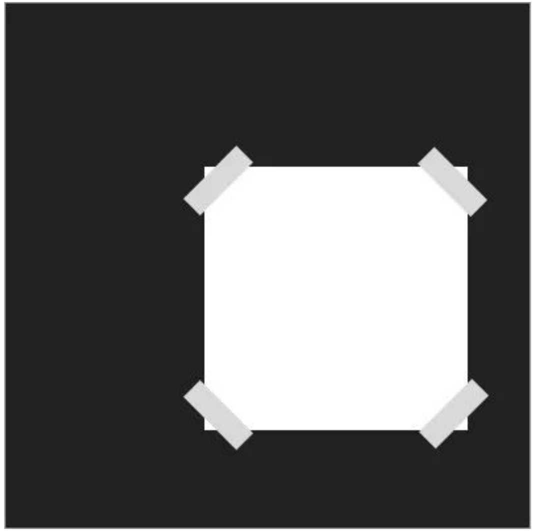
Illustrative examples

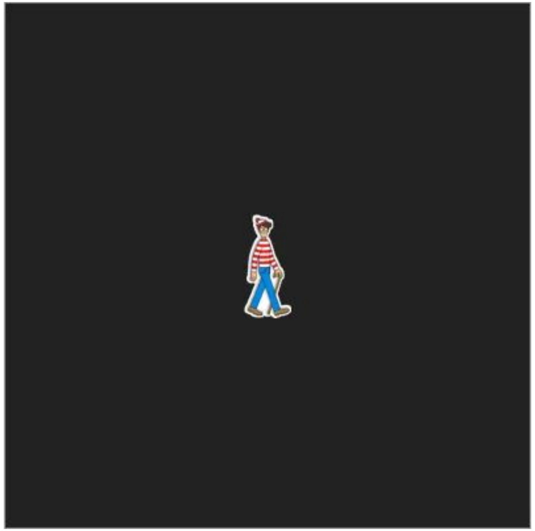
- ➢ Where is Waldo?



There's More 👉

Illustrative examples





There's More 👉

Illustrative examples

- ➢ Color blind friend

LOTO
MINIMUM 2 Millions€ à gagner
POUR CHAQUE GRILLE COCHEZ 5 NUMÉROS
2€
50 EURO

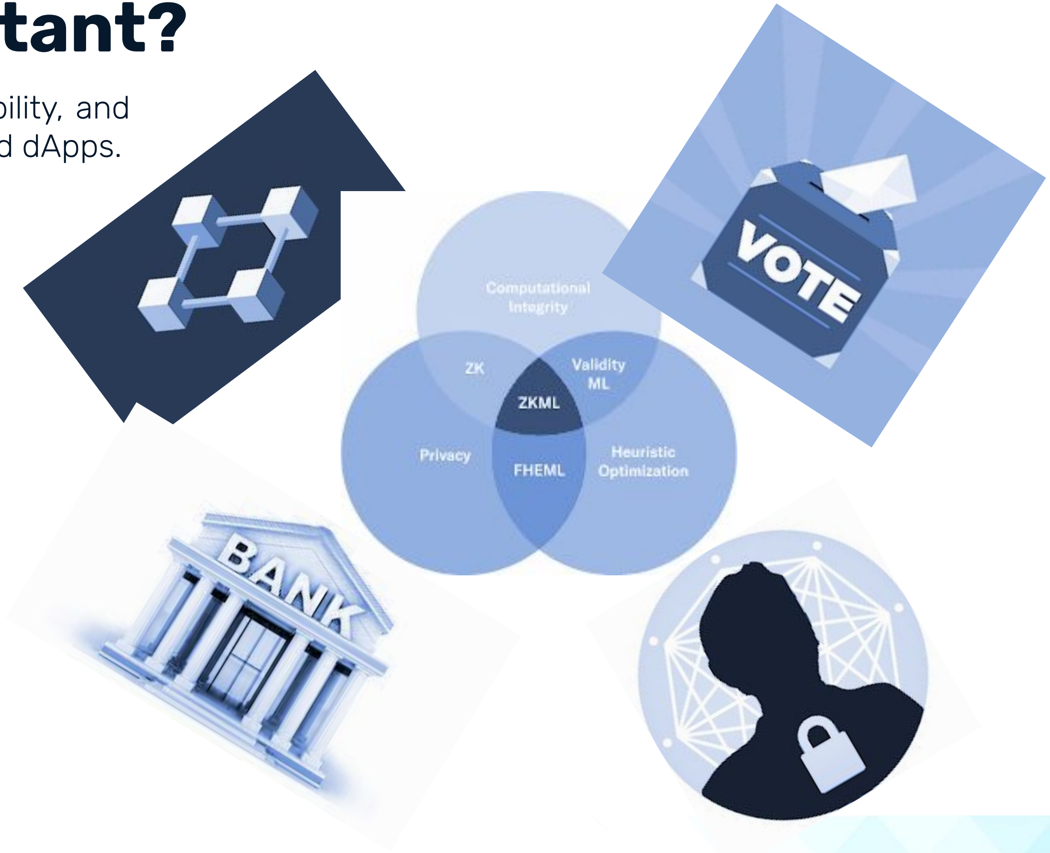
There's More 👉

Why ZKPs are so important?

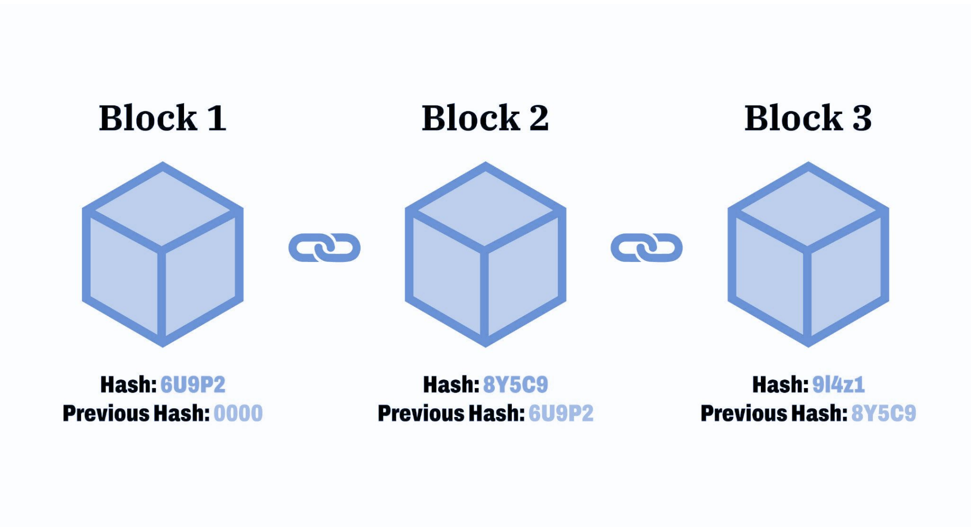
ZKP technology in Web3 enable better privacy, scalability, and security for all players and their projects, initiatives, and dApps.

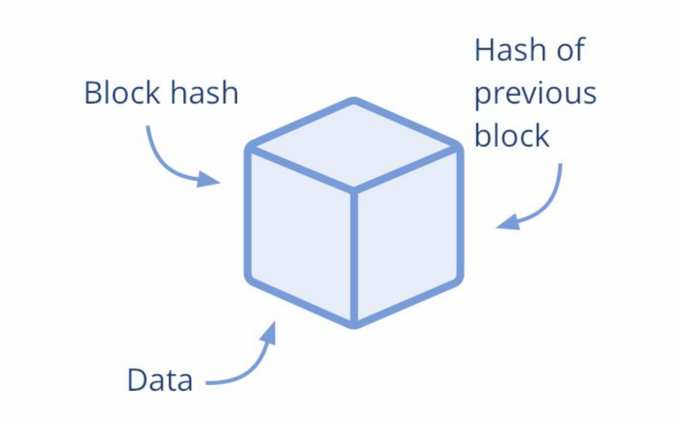
Some applications of ZKPs:

- ➔ ⛓️ **Blockchain (privacy and scaling);**
- ➔ 💰**Finance;**
- ➔ 📨**Online voting;**
- ➔ **DIDs;**
- ➔ 🔐**Authentication;**
- ➔ 💻**Machine learning.**



A little about Blockchain





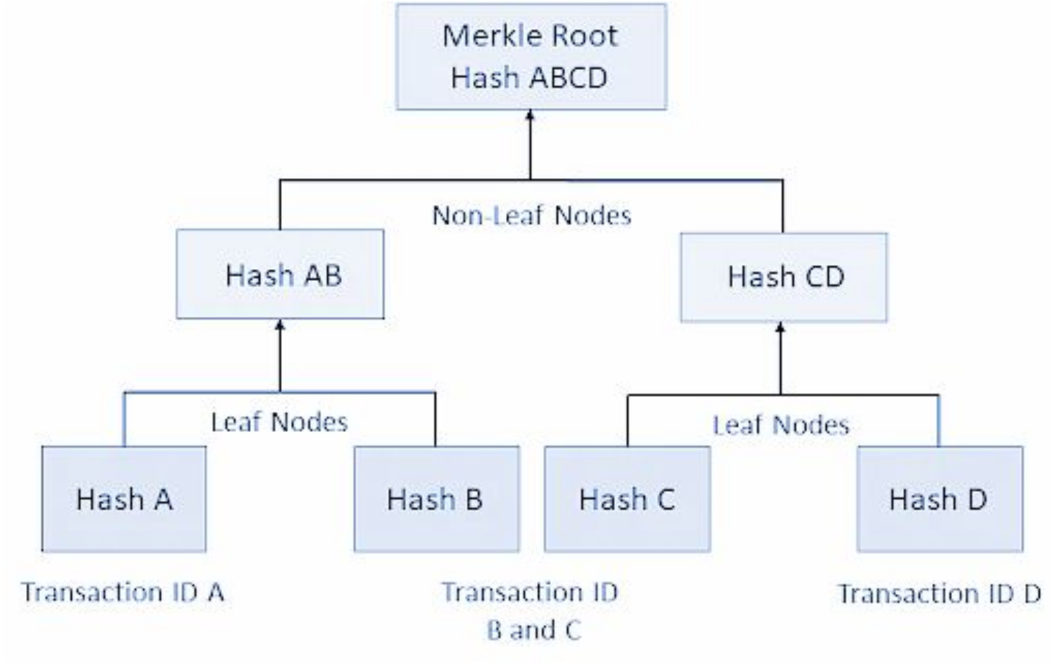
You can find more information on these links:

[Link 1 >]

[Link 2 >]

[Link 3>]

Merkle tree

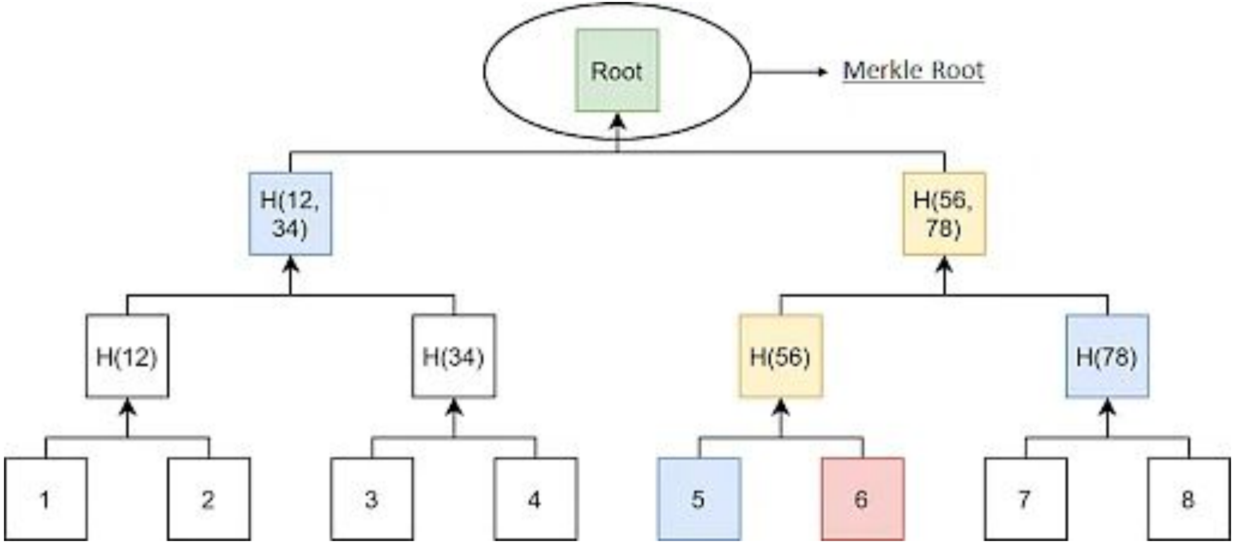


*

You can find more information on these links:

Link 1 >
Link 2 >

Merkle tree



There's More 👉

⛓ Blockchain (privacy)

Anonymous payments. Cryptocurrencies were intended to provide a means for users to conduct private, peer-to-peer transactions. But most cryptocurrency transactions are openly visible on public blockchains.

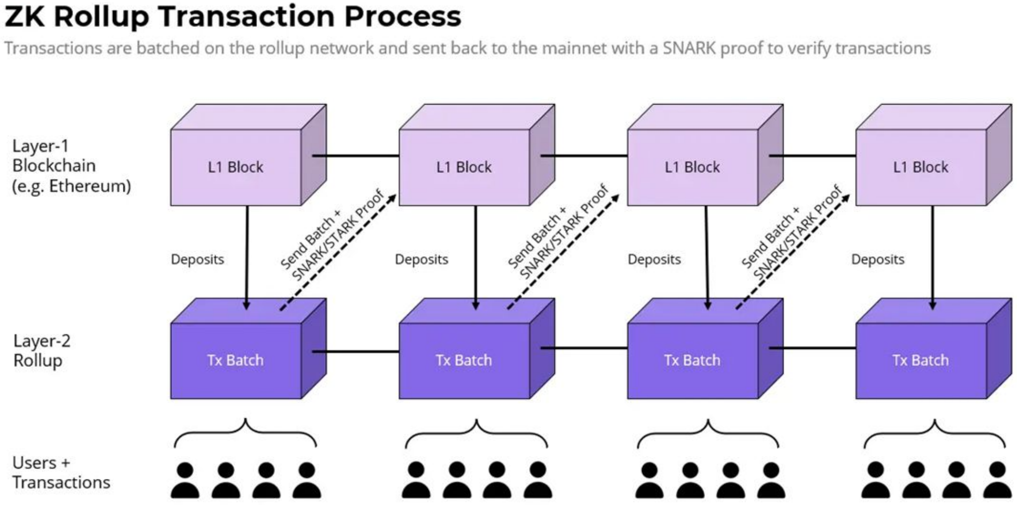
Privacy-focused blockchains, such as Zcash and Monero, shield transaction details, including sender/receiver addresses, asset type, quantity, and the transaction timeline.

There’s More 👉

⛓ Blockchain (scaling)

ZK-rollups. Zero-knowledge rollups (ZK-rollups) 'roll up' transactions into batches that are executed off-chain. Off-chain computation reduces the amount of data that has to be posted to the blockchain.

ZK-rollup operators submit a summary of the changes required to represent all the transactions in a batch rather than sending each transaction individually. They also produce validity proofs to prove the correctness of their changes.



ZK Rollup Transaction Process

Transactions are batched on the rollup network and sent back to the mainnet with a SNARK proof to verify transactions

You can find more information on these links:

[Link 1 >]
[Link 2 >]
[Link 3>]
[Link 4>]

💰 Finance

Zero knowledge range proof allows users to prove they have a secret number that lies in a known range.

For example, a credit applicant could prove that their salary sits within a certain range, without revealing the exact figure.

Similarly, it could prove that a payment amount is within a limit, but it does not show the exact amount.

There's More 👉

📨Online voting

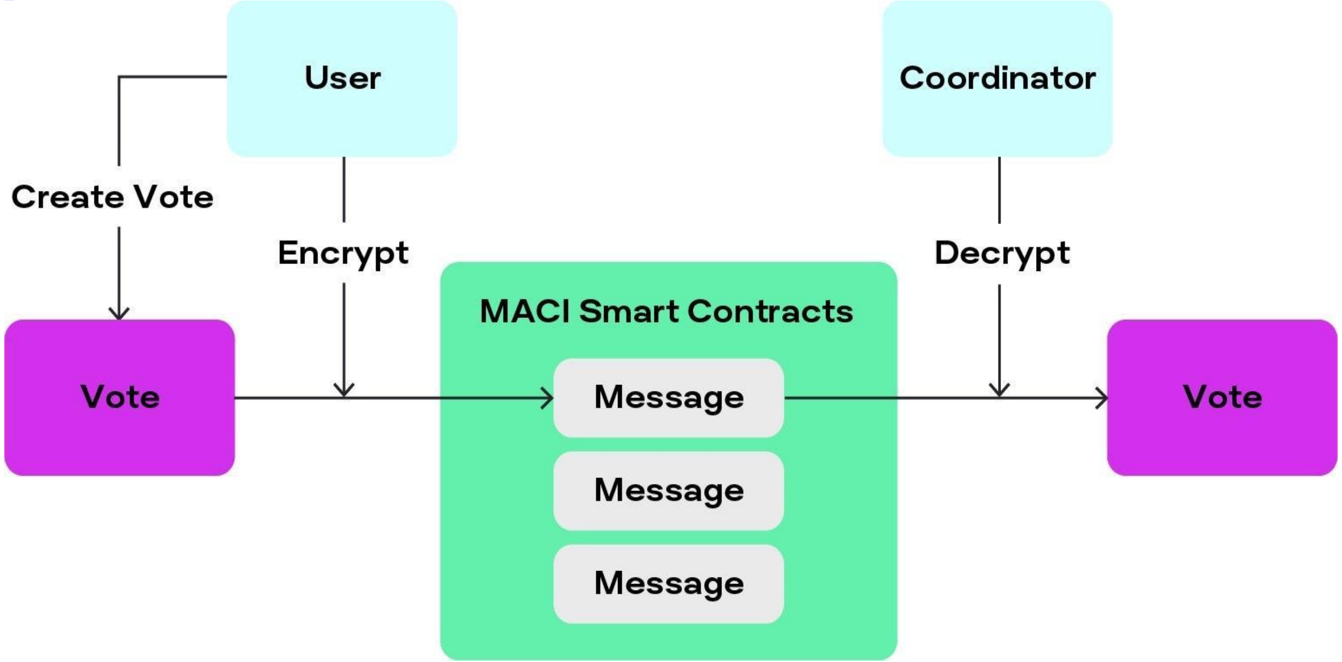
MACI (Minimum Anti-Collusion Infrastructure) are using zero-knowledge proofs to make on-chain voting resistant to bribery and collusion.

MACI is a set of smart contracts and scripts that allow a central administrator (called a "coordinator") to aggregate votes and tally results without revealing specifics on how each individual voted.

Even so, it is still possible to verify that the votes were counted properly, or confirm that a particular individual participated in the voting round.

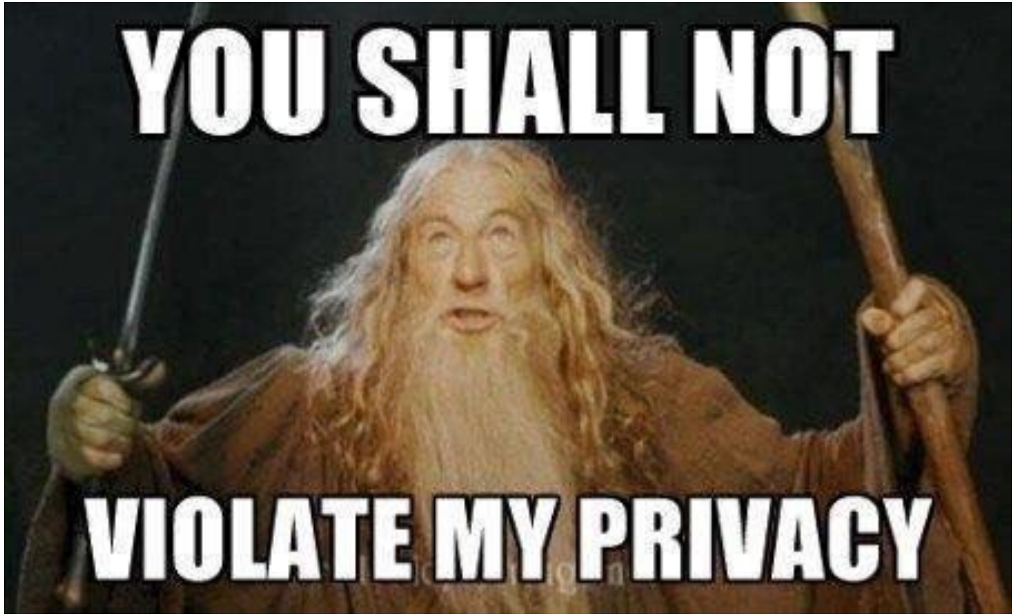
There's More 👉

📨Online voting



There's More 👉

📨Online voting



There's More 👉

👩 DIDs

Zero-knowledge proofs are particularly useful in the context of decentralized identity. Decentralized identity gives the individual the ability to control access to personal identifiers.

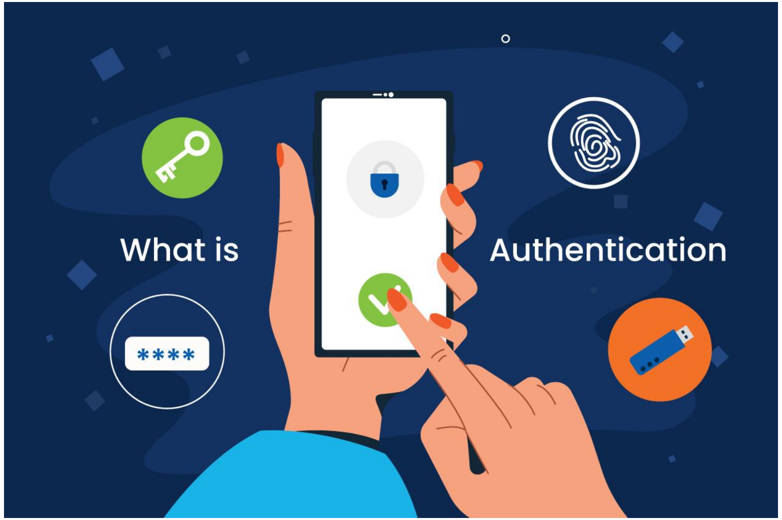
Proving your citizenship without revealing your tax ID or passport details is a good example of how zero-knowledge technology enables decentralized identity.

There's More 👉

🔐Authentication

Using online services requires proving your identity and right to access those platforms. This often requires providing personal information, like names, email addresses, birth dates, and so on. You may also need to memorize long passwords or risk losing access.

Zero-knowledge proofs, however, can simplify authentication for both platforms and users. Once a ZK-proof has been generated using public inputs and private inputs, the user can simply present it to authenticate their identity when they need to access the service.

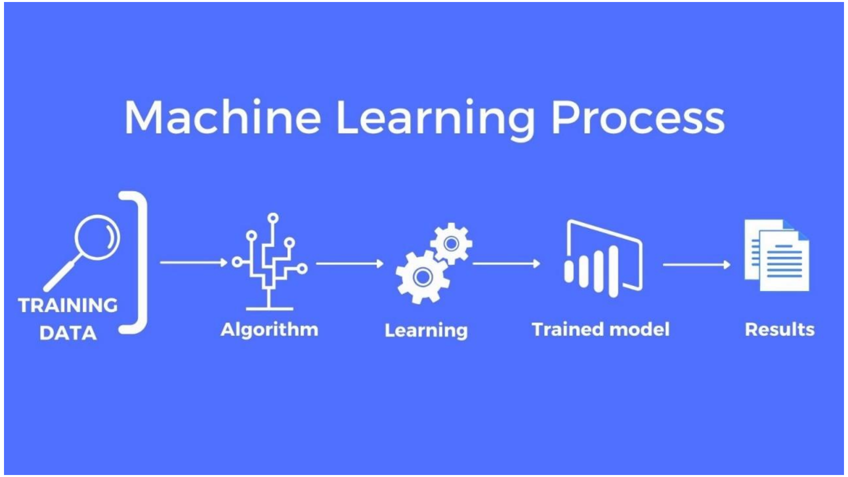


There's More 👉

💻Machine learning

The zero-knowledge property allow us to hide parts of the input or the model as well if need be.

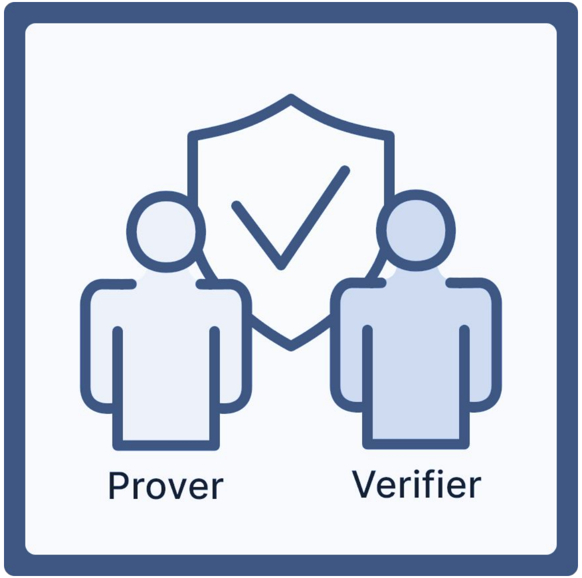
A good example of this would be applying a machine learning model on some sensitive data where a user would be able to know the result of model inference on their data without revealing their input to any third party (e.g., in the medical industry).

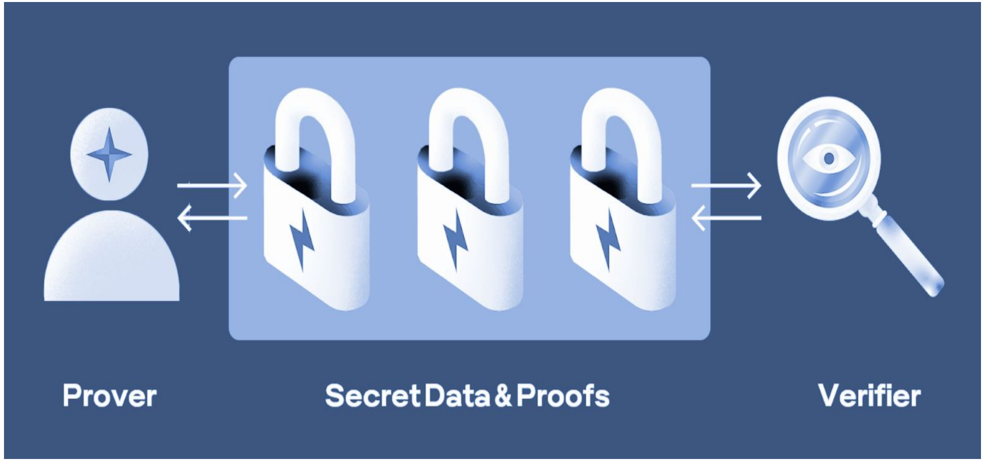


There's More 👉

How does ZKPs work?

In this method, there are two sides: the **prover** and the **verifier**. The prover can prove the verifier that the given statement is true, while the prover avoids conveying any additional information other than the fact that the statement is indeed true.





There's More 👉

Types of ZKPs

There are two main types of zero-knowledge proofs:

➔ **Interactive** Zero Knowledge Proofs;
➔ **Non-interactive** Zero Knowledge Proofs.

Types of Non-interactive Zero Knowledge Proofs:

➔ **ZK SNARKs -** Zero-Knowledge Succinct Non-Interactive Argument of Knowledge;
➔ **ZK STARKs -** Zero-Knowledge Scalable Transparent Arguments of Knowledge.

*

You can find more information on these links:

Link 1 >

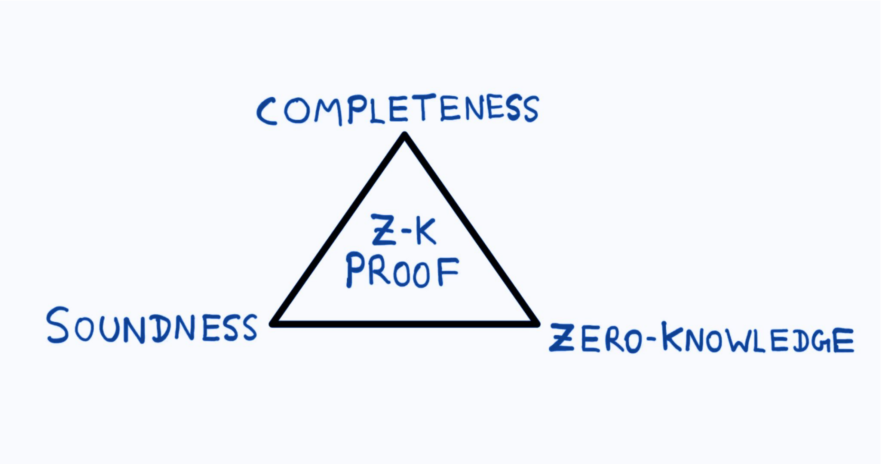
Completeness, soundness and ZK

A zero-knowledge proof must satisfy three properties (we can call it the holy trinity):

➢ **Completeness:** if the statement is true, an honest verifier must accept the proof if it is correct by an honest prover.

➢ **Soundness:** if the statement is false, there is a very low probability that the verifier will accept the proof.

➢ **Zero-knowledge:** if the statement is true, verifier will not learn anything other than the fact that the statement is true.



МАТЕМАТИЧКИ ФАКУЛТЕТ
У БЕОГРАДУ
1873

Thank you!