OUTLINE:

- ➢ Topic motivation
- ➢ Introducción: Proof VS ZKP
- ➢ ZKP Roots
- ➢ Types of ZKP and examples
- ➢ Inherent Properties
- ➢ Pros & Cons
- ➢ Most popular Interactive / Non-interactive ZKPs
- ➢ Applications
- ➢ Conclusions

INFORMATION:

Topic motivation:

- How do you think elections are shown to be done correctly without showing publicly the votes of each citizen? (For privacy)
- How do you think certain banks know that a customer who is asking for a loan has sufficient balance in his bank account to repay the loan, without seeing his balance? (For privacy reasons).

All of them done through a ZKP: A certain type of proof that reveals absolutely no information to the ones who ask for the proof of some statement, the verifiers. // A certain type of proof in which no information is revealed at all to the ones who ask for the proof of some statement, the verifiers.

Introduction: Proof VS ZKP *(Logic vs Probabilistic demonstration)*

- Proof: The type of proof we all know. Convincing steps through logic that can be verified. Basis of mathematics. The way to know if something is absolutely true. (Triangle angle 180 illustration)
- ZKP: Authentication and validation protocol (and not encryption) between prover and verifier (The one who asks for some proof and the one who proves it) in which the prover demonstrates the verifier the truth of a statement without revealing the content.
- Key differences: No info revealed throughout the zk-proof which wasn´t known before and the type of demonstration, which is probabilistic.
- Probabilistic demonstration: Considering an statement to be proven if after successive tests it has been assured that the probability of guessing it by luck is close to 0

When was ZKP born?

Back then, in 1985 the ZKP protocol was born within a paper of its inventors who were Goldwasser, Micali, and Rackoff; later they received the “Nobel Prize” of computer science, called Gödel Prize.

The introduction of this brand new method proposed a paradigm shift. Although all of its features were already invented they put them all together and made a huge advance in how something can be validated without sharing any information. This is kind of similar to what RSA did, it changed the way of interchanging messages (mainly keys) no matter how insecure is the channel in which they are sent.

Types of ZKP and examples (Interactive VS Non Interactive):

- **Interactive**: Prover must complete a series of actions to convince the verifier about a specific fact. And must do this for each specific verifier. These actions associated with the concepts deal with mathematical probability.
  EXAMPLE (Could do it interactively at presentation with a volunteer):

  Suppose you (the prover) have a color-blind friend (the verifier) that cannot distinguish a green and a red ball from each other (have zero knowledge about whether the balls are different colors). You need to prove that the colors of the balls are different but your friend needs something more than your words to be convinced. A ZKP method for this problem would be like this:

  - Your friend takes the balls and lets you see which ball is in which hand.
  - Then, they either switch the balls between their hands or not behind their back.
  - They then present the balls to you and ask you whether they switched the balls or not. As you can distinguish the green ball from the red one, you can easily give the correct answer.
  - Your friend is not convinced. You have a 50% chance to correctly guess whether they switched the balls or not and the balls can still be the same color.
  - However, if they repeat this several times, eventually, the probability of you correctly guessing whether they switched the balls or not each time would be very low. This enables your friend to verify that the balls are different colors without *knowing* the actual colors of the balls.

- **Non-Interactive**: ∄ interaction between prover and verifier. This type of proof is created by the prover in such a way that anyone can verify. May need specific software (for better mechanism).
  EXAMPLE:

1. Alice wants to prove to Bob that she knows a value such that $y = g^a$ to base g.
2. Alice picks random value v from the set of values Z, and computes $t = g^v$.

3. Alice computes c = H(g, y, t) where H() is a hash function.
4. Alice computes d = v – c·a.
5. Bob or anyone can then check if $t = g^d \cdot y^c$.

Fiat–Shamir heuristic allows us to replace interactive step 3 with non-interactive random oracle access, but in practice, Hash function is used.

In Interactive ZKP, Bob would have picked random value c from set Z and sends it to Alice.

As shown in examples, ZKP requires 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. If this is not the case, then the prover will eventually be proven wrong by the verifier's test with a higher degree of probability. This is consequence of *ZKP Inherent Properties*:

Inherent Properties (Completeness, Soundness, Zero-Knowledge)

Completeness:: " Verification + Privacy preservation"

- The goal is achieved ie: the prover assures to have let the verifier verified the truth about its statement, without knowing no more than its truth value (true or false)

Soundness: "Lying resistance"

- Anti-Cheaters factor: a dishonest prover(cheater) could still prove a false statement (formal fallacy) with a success probability ≅ 0 (soundness error).

There are ways to minimize this soundness error based on implementation aspects, such as incrementing the number of choices and procedure iterations.

Zero-Knowledge: "The icing on the cake**"**

- If the statement is true, the verifier learns only whether the statement is true or false.

Pros & Cons:

PROS:

- Computational secure
  Resistant to brute force attacks.
- Quantum secure
  Actual ZKP protocols are not susceptible to known attacks involving quantum algorithms.
- Mantain's users' privacy
  The most admired quality of ZKPs is its protection of users' privacy. It never requires sensitive data-sharing, making it incredibly private overall.
- Scalability
  You don't need a huge infrastructure to provide the advantages of ZKP, so it can be used in a wide variety of applications. It does not require the prover or verifier to be online all the time.
- Simplicity
  Software knowledge is not required for ZKP to operate, but can provide better solutions that have an influence on our daily lives.

- Safety
  If it is known that a certain company uses ZKPs and asks their customers for personal information, they can deny giving it as ZKPs do not require data sharing and could be used for fraudulent actions.

CONS:

- Security flaws
  Security flaws might appear based on the influence of soundness error.
- Not efficient
  Lots of tries which require high demand of computational power.
- Very weak to information recovery once it has been lost

Most popular Interactive / Non-interactive ZKPs:

- Succinct Non-Interactive ARguments of Knowledge (SNARK)
- Scalable Transparent ARgument of Knowledge (STARK)
- Verifiable Polynomial Delegation (VPD)
- Succinct Non-interactive ARGuments (SNARG)

ZKP System	Publication year	Protocol	Transparent	Universal	Plausibly Post-Quantum Secure	Programming Paradigm
Pinocchio	2013	zk-SNARK	No	No	No	Procedural
Zilch	2021	zk-STARK	Yes	Yes	Yes	Object-Oriented

*See extended table, with information of protocols between 2013 until 2021 at: https://en.wikipedia.org/wiki/Zero-knowledge_proof#Zero-Knowledge_Proof_protocols
*A transparent protocol is one that does not require any trusted setup and uses public randomness. A universal protocol is one that does not require a separate trusted setup for each circuit. Finally, a plausibly post-quantum protocol is one that is not susceptible to known attacks involving quantum algorithms.

Applications

Zero-knowledge proofs can be used to protect data privacy in a diverse set of cryptography use cases, such as:

- Blockchain: Although blockchain is a revolutionary technology and has brought many brand new features, one that is usually highly mentioned is that it maintains total privacy and protects user's anonymity, but that's not completely true when ZKPs are not used. There are many cases in which some drug dealers or criminals have been tracked by the police because the public blockchains always keep track of any transaction. In this sense ZKP can bring up better performance in terms of privacy.

- Finance: For instance the clients in the ING bank can demonstrate that their secret number falls inside a predetermined range by using ZKPs. An applicant for a mortgage, for example, might demonstrate that their income is within the acceptable range without disclosing their exact pay.

- Online voting: ZKPs provide voters the option of casting an anonymous poll and checking if their vote was counted in the final total.

- Authentication: ZKPs can be used to authenticate users without requiring them to exchange confidential information such as passwords.

- Machine learning: ZKPs can let the owner of a machine learning algorithm convince the people of the model's outcomes without disclosing any details about the ML model itself.

Conclusions

Among all the current methodologies to carry out verification protocols, ZKP has made a name for itself, standing out for its innovative and self sufficient manner to be carried through. Although over the last years the solution to the problem of data integrity and user authentication had greatly been solved, with the advent of new technologies such as Blockchain, AI and Big Data as a whole, new vulnerabilities have been encountered leading to the raise of a new type of approach which is rather innovative to say least , compared to the rest in the field of cybersecurity. ZKP heuristics lie over the mathematical field of probability and have a clear and powerful intention: guaranteeing authentication (already solved issue) while retaining the user's involved information confidential (constraint under which the issue wasn't yet solved). In other words, the implementation of ZKP has offered its users a system which is characterized by confidentiality, authentication and data integrity and not less important, solid security against the potential biggest threat in the industry… Quantum Computing.

Bibliography:

https://youtu.be/fOGdb1CTu5c

https://youtu.be/5ovdoxnfFVc

https://www.leewayhertz.com/zero-knowledge-proof-and-blockchain/

https://research.aimultiple.com/zero-knowledge-proofs/#easy-footnote-bottom-1-30650

https://www.coinbureau.com/adoption/applications-zero-knowledge-proofs/

https://www.geeksforgeeks.org/non-interactive-zero-knowledge-proof/

https://en.wikipedia.org/wiki/Zero-knowledge_proof

https://www.quantamagazine.org/how-to-prove-you-know-a-secret-without-giving-it-away-20221011/ (History & Alice-Bob Hamiltonian circuit example)

https://hal.archives-ouvertes.fr/hal-02150062/file/main.pdf

https://link.springer.com/content/pdf/10.1007/978-3-540-85174-5_30.pdf

https://www.usenix.org/system/files/sec21-weng.pdf

https://medium.com/predict/what-is-zero-knowledge-proof-and-its-role-in-blockchain-870fa1664fba

https://www.blockchain-council.org/blockchain/zero-knowledge-proof-protocol/

https://blockheadtechnologies.com/zero-knowledge-proofs-a-powerful-addition-to-blockchain/

https://ieeexplore.ieee.org/document/9410618