The Zero-Knowledge Proof

Ryan Tineo

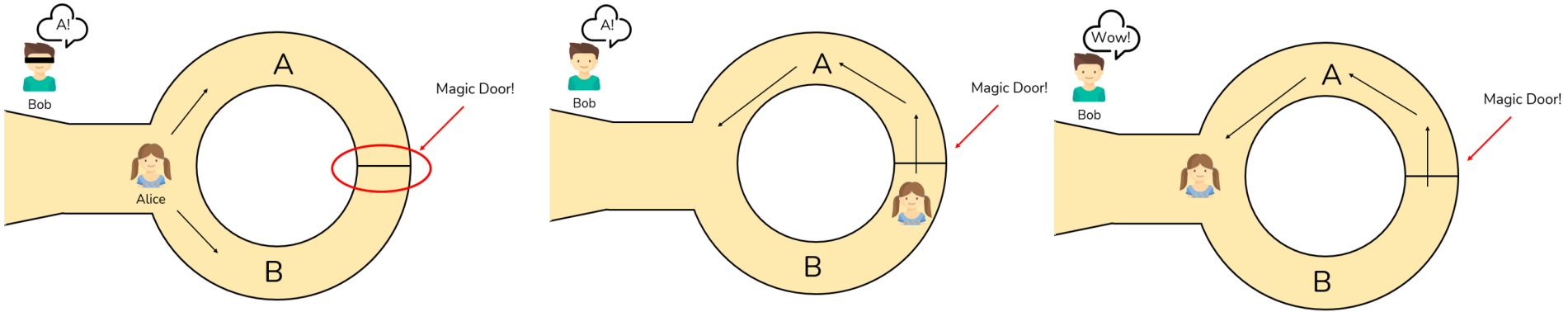
Why does the Zero-Knowledge Proof Matter?

- Major Applications in Digital Security
- Cryptographic method to cut down data sharing and retention to services
    - Everyday, millions of users browse the internet, accepting cookies, and sharing personal information in exchange for access to services and digital products
    - Causing users to become more at risk for security breaches and illicit use of their data

DEFINING A ZERO KNOWLEDGE PROOF

- Zero-knowledge proofs and techniques are mathematical methods to verify things **without sharing or revealing underlying data**
- Involves a **prover** and **verifier**
    - Prover must prove to the verifier that something is **true without revealing anything about why it's true**
- Example: A payment app (Venmo) checking whether you have sufficient funds to complete a transaction without finding out anything else about your actual balance

An Easy Way to Understand Zero-Knowledge Proofs: Cave Example



1. Bob closes his eyes and Alice Enters cave
2. Bob doesn't know which entrance Alice Chose, and her yells for Alice to exit from "A"
3. Alice knows the secret word and she can exit from "A," proving Alice knows the magic word to the verifier Bob

But what if she entered through A originally?

- Takeaway: The prover, had to demonstrate she knew the secret key to Bob, the verifier, without actually showing him the real password

We Don’t Trust Each Other

- The Zero-knowledge proof allows for increased trust amongst individuals
    - If I can prove that I’ve done something correctly to someone, without having to reveal any secrets, that person will trust me more

- In CS, a metaphorical “key” and “lockbox” in conjunction with mathematics are used for applications of zero-knowledge proofs.
    - In Cryptography:
        - If I wanted to send secret messages to somebody
        - I could encrypt a message using mathematics and prove to somebody that I know the key to the encryption
        - Proves that I have the mathematical ‘key’ to the mathematical ‘lockbox’ in question
        - In turn, this person could deem me as trustworthy

Thank you!

Sources

- https://www.google.com/url?sa=i&url=https%3A%2F%2Fmedium.com%2Fcoinmonks%2Fblockchain-zero-knowledge-proof-in-a-nutshell-f0684a669a68&psig=AOvVaw2-Q6zK9YTNVH5G-_ruDziv&ust=1651637913116000&source=images&cd=vfe&ved=0CAwQjRxqFwoTCLi2_p6vw_cCFQAAAAAdAAAAABAD
- https://www.wired.com/story/zero-knowledge-proofs/
- https://www.bbva.com/en/zero-knowledge-proof-how-to-maintain-privacy-in-a-data-based-world/
- https://link.springer.com/content/pdf/10.1007/BF00195207.pdf