697: Innovation and Cryptoventures

Zero Knowledge Proofs

Campbell R. Harvey

Duke University and NBER

Voting

How is a voting blockchain feasible if the government can see how everyone votes?

- The answer is a zero knowledge proof
- This means that you provide cryptographic proof that you are a valid owner of a voting token – yet you do not have to reveal who you are.

Billiard balls

- Imagine your friend is color-blind.

- You have two billiard balls; one is red, one is yellow, but they are otherwise identical.

- To your friend, they seem completely identical, and he is skeptical that they are actually distinguishable. You want to prove to him that they are in fact differently-colored. On the other hand, you do not want him to learn which is red and which is yellow.

http://mathoverflow.net/questions/22624/example-of-a-good-zero-knowledge-proof

Billiard balls

Proof system:

- You give the two balls to your friend so that he is holding one in each hand.
- You can see the balls at this point, but you don't tell him which is which.
- Your friend then puts both hands behind his back. Next, he either switches the balls between his hands, or leaves them be.
- Finally, he brings them out from behind his back. You now have to "guess" whether or not he switched the balls.

http://mathoverflow.net/questions/22624/example-of-a-good-zero-knowledge-proof

Billiard balls

Proof system:

- By looking at their colors, you can determine whether or not he switched them. If they were the same color, there is no way you could guess correctly with probability higher than 1/2.
- If you and your friend repeats this T times (for large T), your friend should become convinced that the balls are indeed differently colored; otherwise, the probability that you would have succeeded at identifying all the switch/non-switches is at most $(1/2)^T$
- Furthermore, the proof is "zero-knowledge" because your friend never learns which ball is yellow and which is red; indeed, he gains no knowledge about how to distinguish the balls.

http://mathoverflow.net/questions/22624/example-of-a-good-zero-knowledge-proof

Terminology

Key idea:

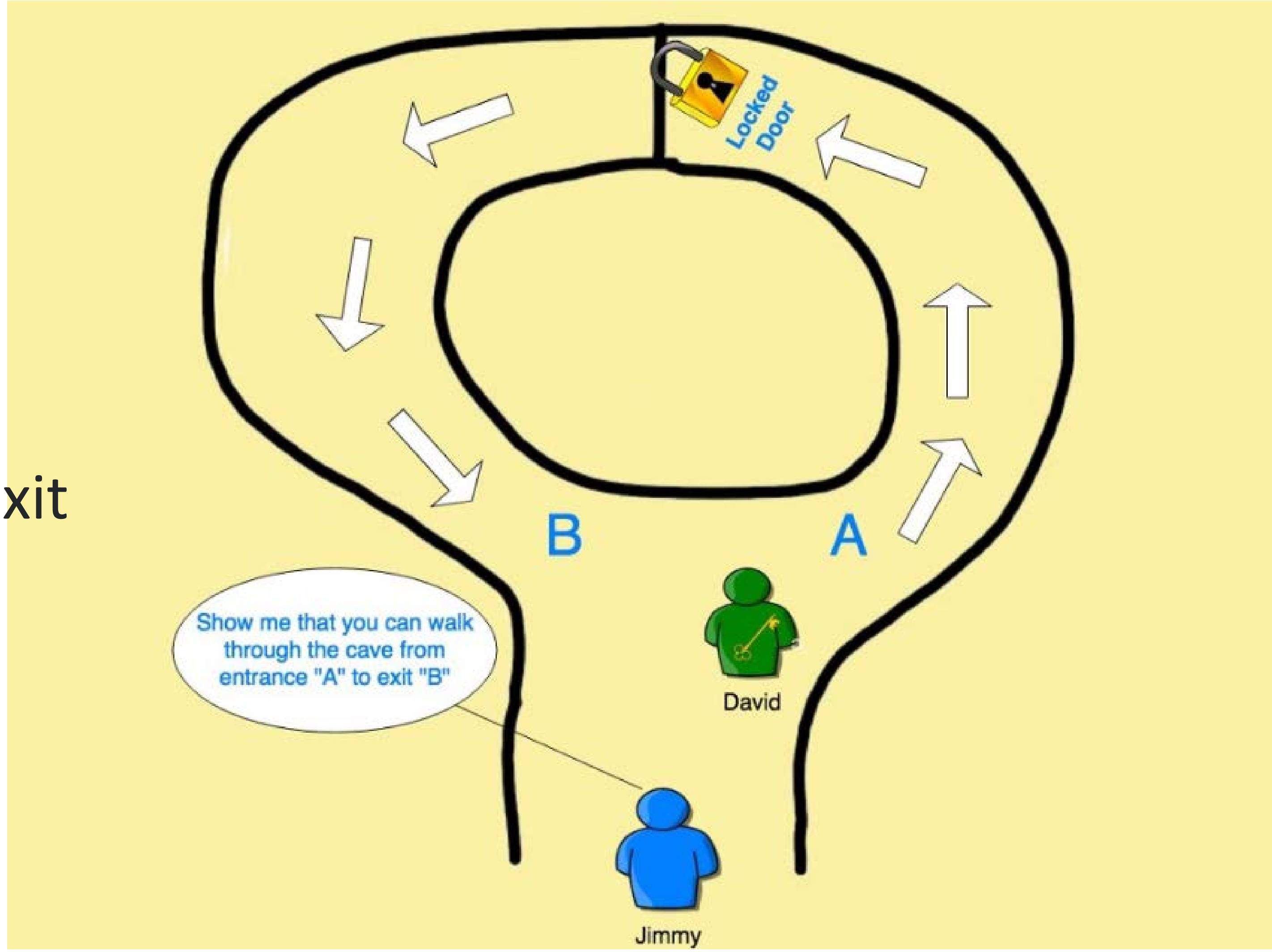
- Zero knowledge proof is the ability to prove a secret without revealing what the secret is
- Sometimes called zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge)

https://medium.com/coinmonks/blockchain-zero-knowledge-proof-in-a-nutshell-f0684a669a68

Another application

Secret key:

- Prove I can unlock with code without revealing the code
- If I can enter cave via A and exit via B, I have proved this


Locked Door
B
A
Show me that you can walk through the cave from entrance "A" to exit "B"
David
Jimmy

https://medium.com/coinmonks/blockchain-zero-knowledge-proof-in-a-nutshell-f0684a669a68

Blockchain applications

Transaction:

- User A may make a request to send to user B some money. Blockchain needs to figure out whether A has the money
- Blockchain doesn't need to know who is spending the money – only that they have the money to spend.

https://medium.com/coinmonks/blockchain-zero-knowledge-proof-in-a-nutshell-f0684a669a68

ZCash

Contrasts with bitcoin:

- ZCash extends the protocol and software underlying Bitcoin by adding new, privacy-preserving payments. In doing so it forms a new protocol that, while using some of the same technology and software as Bitcoin, is distinct from it.
- This new protocol has both anonymous coins, dubbed ***zcoins***, and non-anonymous ones, which, for purposes of disambiguation, we call ***basecoins***. In contrast to Bitcoin's transactions, payment transactions using the ZCash protocol do not contain any public information about the payment's origin, destination, or amount; instead, the correctness of the transaction is demonstrated via the use of a zero-knowledge proof.
- Users can convert from basecoins to zcoins, send zcoins to other users, and split or merge zcoins they own in any way that preserves the total value. Users may also convert zcoins back into basecoins, though in principle this is not necessary: all transactions can be made in terms of zcoins.

http://zerocash-project.org/

Other cryptos

Many involved:

- Hyperledger Ursa is an implementation of Zero-Knowledge Proof (December 4, 2018). See post.
- Ernst and Young ZKP prototype on Ethereum blockchain, November 7, 2018
- List of resources https://ethresear.ch/t/zero-knowledge-proofs-starter-pack/4519

https://www.hyperledger.org/blog/2018/12/04/welcome-hyperledger-ursa https://cointelegraph.com/news/eth-zero-proof-prototype-models-has-ernst-young-done-what-ethereum-could-not