
digital X
TM
Data Ownership and Privacy on the Blockchain

Identity, Data ownership and privacy on the blockchain

1. Centralized Data Systems
2. Data ownership and Digital Identity
3. Data Privacy on the Blockchain
4. Zero Knowledge Proofs

Data ownership on centralized platforms

- The internet was created to facilitate the sharing of free information amongst it's users.
- Initially, open web services such as forums and discussion boards dominated the use of the internet
- Where we are now: Major centralized conglomerate corporations such as facebook and google claim ownership of data you (sometimes unwittingly) provided
    - The internet's unparallelled data sharing capabilities are now mainly being used for the benefit of large private entities
    - Facebook - Cambridge analytica, Equifax, constant new scandals involving the improper handling or collection of private information

- The decentralized web revolution enabled by blockchain technology allows the internet to work for the benefit of the network users once again
    - Allows data to be shared from multiple sources, allowing value to flow directly back to the users of the network
    - While still allowing the users to actually be in control of their data

Case Study: Golden State Killer's Personal Data

- The golden state killer was a serial killer in the 1970-1980s
  - Murdered 12 people
  - Case was unsolved until early 2018 when law enforcement arrested Joseph James DeAngelo for the crimes he commited 30+ years ago

- Found using very old DNA evidence from a crime scene
  - Police checked killers DNA against online DNA database 23andme
  - A relative of the killer had uploaded DNA to centralized online DNA database 23andme and triggered a partial match
  - This relative was questioned and that led them to arrest Joseph DeAngelo
  - Raises concerns about the sovereignty of genetic data
  - Another example of a centralized data aggregation service that will claim ownership to data you provided, and then share that with whoever it pleases.

Decentralized Genomic Data

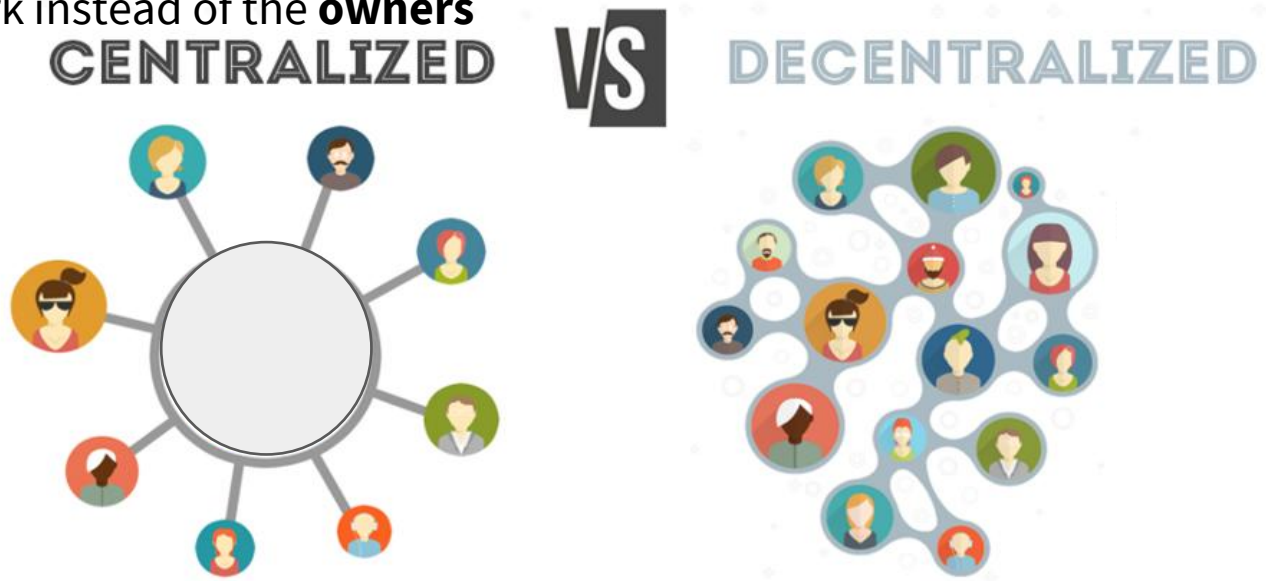
Case Study: Shivom

- Current blockchain based decentralized genomic database
- Allows each user to upload genetic data and selectively give levels of access to who the user decides
- User can authorize selective access to their health/genetic data by their health insurance company or doctor on a case by case basis to improve the quality of their services
- The **user** the beneficiary of the value of increased data sharing facilitated by the network

SHIVOM

Decentralized network benefits

- Centralized web services have repeatedly abused the trust placed in them to responsibly handle our personal information
- Centralized web services hoard their users data and use it to their own private benefit
- Decentralized web services allow a user sovereign control over their information
  - User selectively chooses what is committed to the blockchain
  - Users can approve who can access that data on a case by case basis
- Decentralized networks can be created that create value for the **users** of the network instead of the **owners**



Proving Data Ownership and Permissions

- Decentralized networks facilitated by blockchain technology enable a way to prove data ownership and create custom permissioned access to the data
- For these identity claims and permission levels to be reliable, a system for proving digital identity is desired
    - We want proof of identity beyond that someone has access to a certain private key
    - This digital Identity system should be available for people to verify some information about a users identity easily, without having to provide access to that identifying personal data to everyone who wants to verify that.

- Currently use public/private key pairs to prove ownership and often identity.
    - This is difficult to use for non-tech literate people
    - If a key is lost, there is no way to recover that
    - Keys can be stolen
- We need a stronger identity system

Digital Identity

Existing Digital Identity platorms

1. OpenID/OAuth - commonly used single sign on service.
2. Still trusting a centralized service with your data

Decentralised Digital Identity

- ERC725/735: A proposal for a self sovereign identity standard on the ethereum blockchain
- uPort
- identity.foundation

ERC725/735

Self Sovereign Identity Standard for Ethereum

- Proposed by Fabian Vogelstellar
  - creator of Mist, metamask, web.js and the ERC20 standard
- Decentralised solution to proving identity
- Simple smart contract based standard
- Each user is in control of who can see their own identifying claims
- Identity can be proved using any mutually trusted 3rd party verifier

ERC725/735 In Practice

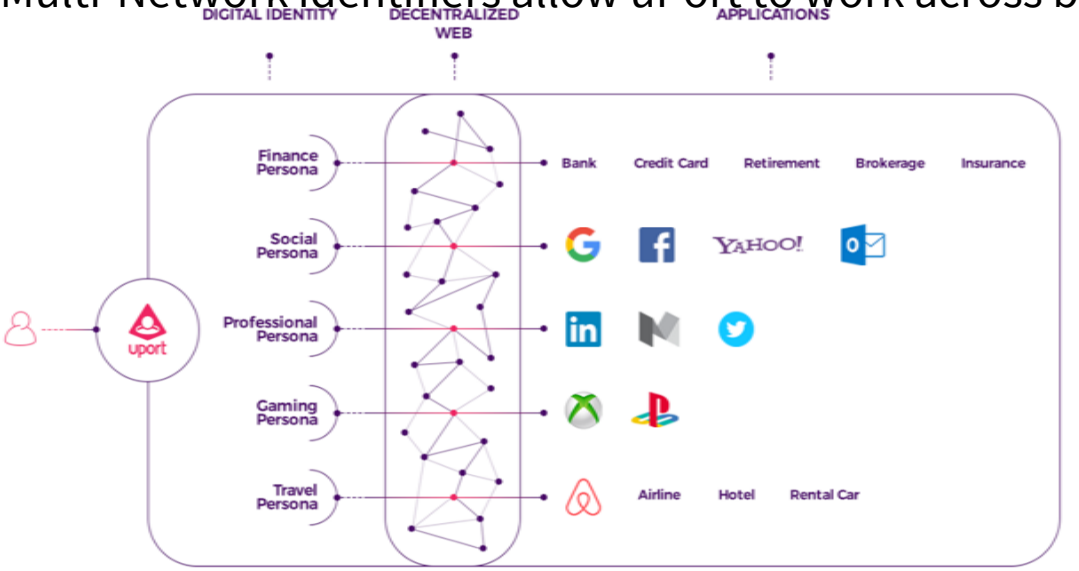
How would you use a decentralised identity service

1. Deploy your personal identity smart contract which will hold all your identity claims
2. Verify some information with an identity verification service
3. Update your personal identity smart contract with the verified claim by the identity verification service
4. Access a decentralized service that needs you to prove your identity, (such as a decentralized exchange that may need KYC/AML proof checks) and will will recognizes claims from your identity verification service
5. Decentralised service checks your identity contract for expected claim
6. If the claim is found, the identity verification is complete

uPort

Open Identity Infrastructure for the ethereum community

- A toolkit for identity verification
- Supports multiple identity personas
- Development of entire toolkit of wallet, single sign on provider, SDK and identity claim issuance and proofs
- Takes more complex approach to creating an open identity system compared to the fairly simple ERC725/735 smart contract
- MNID: Multi-Network Identifiers allow uPort to work across blockchains

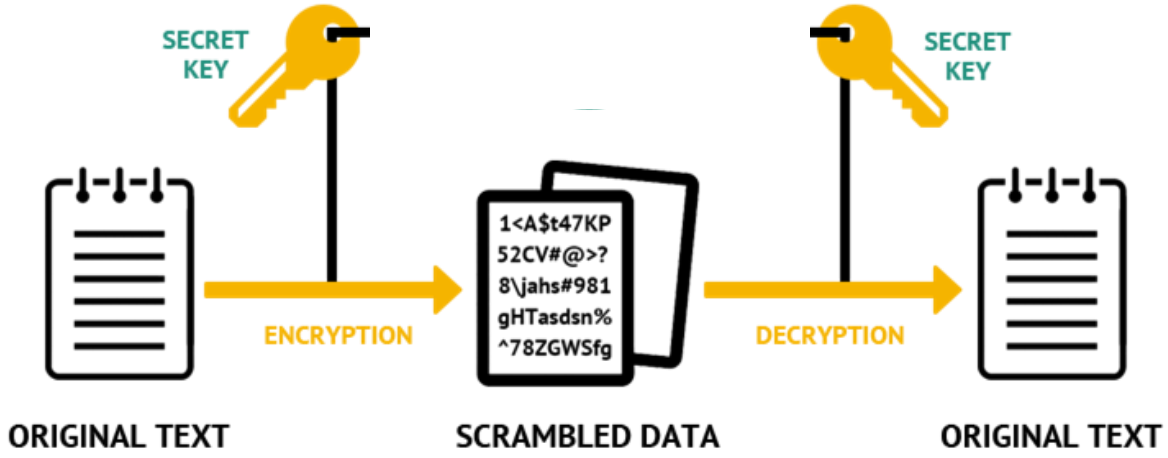


Identity.foundation

Privacy on the blockchain

Private and confidential transactions on the blockchain

- Transaction privacy should be a major concern with any blockchain application, not just financial and banking
  - E.g. identity verification claims and any other actual important information ideally will be private
- One simple way is to only pass encrypted data onto the blockchain.
  - This is adequate if you can ensure that nobody will ever leak the encryption key
  - Storing large amounts of data on the blockchain is cost prohibitive



Privacy on the blockchain

Methods to secure data on the blockchain

- Hash functions used extensively throughout blockchain technology
- Hash functions are a one way function used to transform data into something unrecognizable
- Possible to commit hashes of data to the blockchain instead of the data
  - Reference any data by it's hash function
  - Keeps amount of data required to be stored on the blockchain down
- This is fine if all you need is data authenticity verification

Privacy on the blockchain

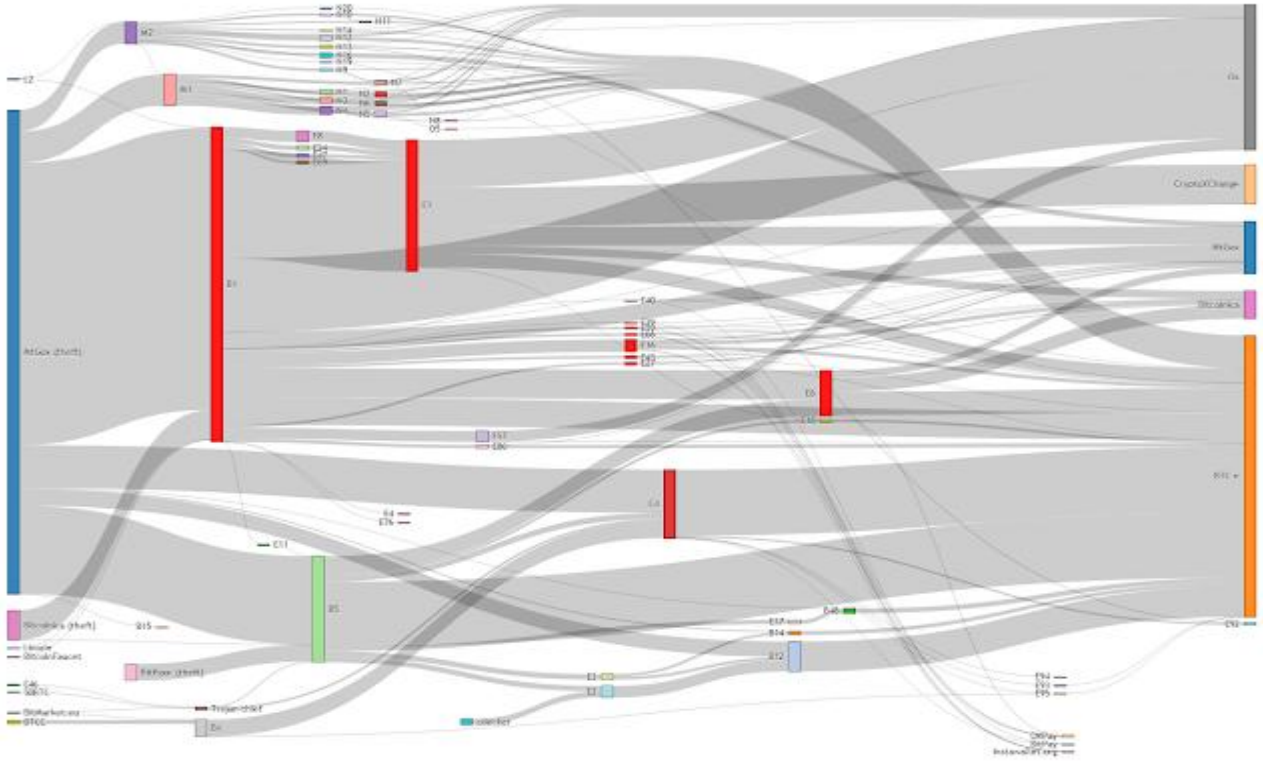
How Private is my data on the Blockchain?

- Not private enough!
- Many attempted methods used to obscure identifying blockchain data
- Hierarchical Deterministic (HD) wallets
  - Encouraged single use addresses
- Coin Mixing
  - Enable an arbitrary level of obfuscation about the origin of funds, provided you have the time, fresh liquidity and transaction fees to keep mixing the coins
- Ring signatures
- More traditional money laundering methods
  - Exchanging assets on unregulated exchanges
  - Transferring assets to and from shared liquidity pools

Case Study: The stolen MTGOX Bitcoins

MTGOX Hack

- MTGOX was the world's biggest cryptocurrency exchange at the time
- In 2013 MTGOX shut down after announcing a hack and loss of 850 000 BTC
  - Worth ~$8B today
- Company WizSec started tracking the stolen BTC on the blockchain



Zero Knowledge Proofs

What are Zero Knowledge Proofs?

- Zero Knowledge proof is when a prover can prove a statements validity without revealing any underlying information about it
  - Uses cutting edge cryptographic tools

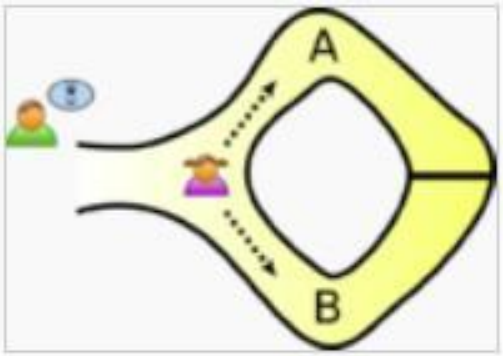
- How Zero Knowledge Proofs can be used:
  - Prove details about your finances without revealing any actual figures
  - Prove that you live in a certain area without revealing you address
  - Prove that a certain transaction is valid without revealing any details about it
  - Prove you know your password without revealing it

- How can that possibly work?!

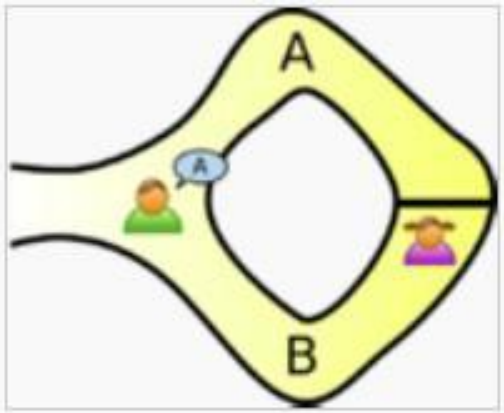
The Cave

Zero Knowledge Proof Thought Experiment

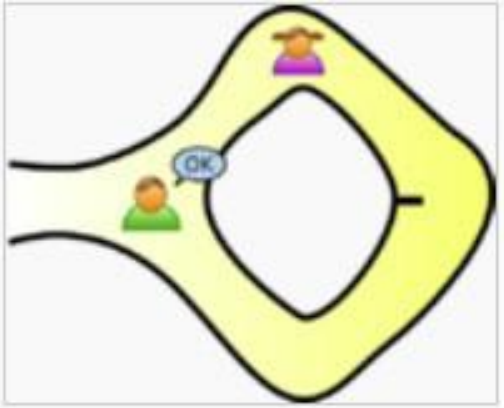
- Imagine a circular cave with a locked door around the other side
- Door will only open if a magic phrase is said
- Peggy wants to prove to Victor that she knows the phrase
- But without revealing the phrase!



Peggy randomly takes either path A or B, while Victor waits outside



Victor chooses an exit path

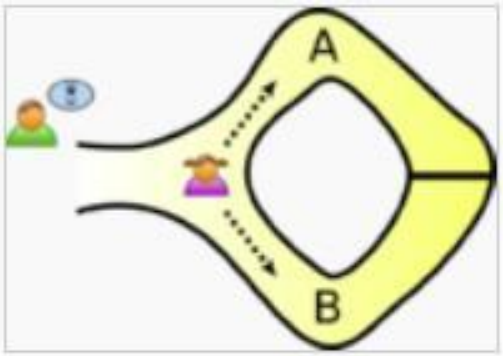


Peggy reliably appears at the exit Victor names

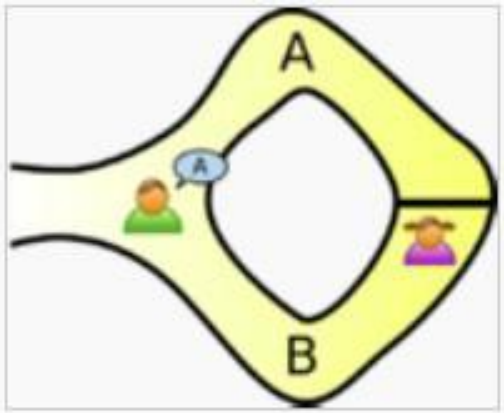
The Cave

Zero Knowledge Proof Thought Experiment

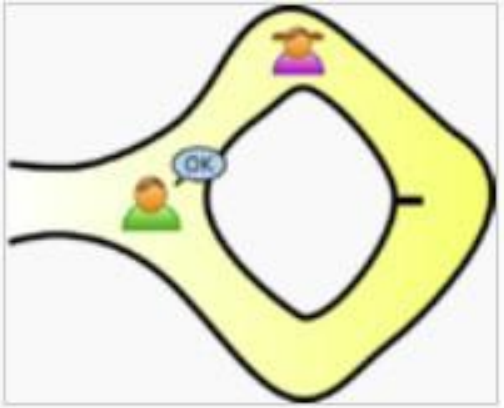
1. Victor waits outside cave so he can't see which path peggy takes
2. Peggy enters cave and walks around the other side
3. Victor announces a side he wants Peggy to return from
4. Peggy returns from the right side



Peggy randomly takes either path A or B, while Victor waits outside



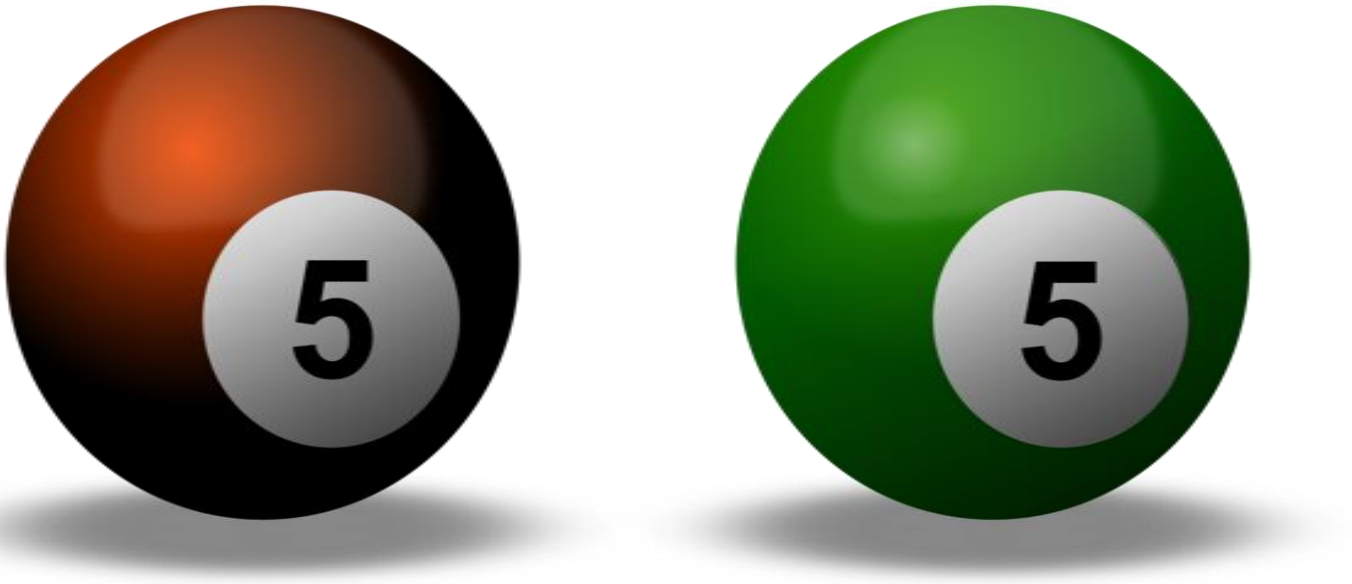
Victor chooses an exit path



Peggy reliably appears at the exit Victor names

The Two Balls

- Two Balls, one red, one green
- I am colourblind, and to me they look identical
- My friend Paul wants to prove to me that they aren't identical and he can tell them apart
- Doesn't want to reveal which colour is which or any other information apart from the fact he can distinguish between these apparently identical balls



The Two Balls

1. Put both balls behind my back and then I reveal only one ball
2. I put the balls behind my back again and again reveal only one ball
3. I ask the prover, Paul if I switched the balls when they were behind my back
4. Paul, being able to tell the two balls apart, can answer this correctly
5. This gives a 50% confidence that Paul is telling the truth
6. Repeat n times for desired amount of trust

Zero Knowledge proof confidence

Number of trials	Chance of Fraud	Confidence of Statement
1	50%	50%
2	25%	75%
3	12.5%	87.5%
4	6.25	93.75%
5	3.13	96.87%
6	1.56	98.44%
7	0.78	99.22%
10	0.09	99.91%
15	0.003%	99.997%
20	0.000095%	99.999905%
50	1 in 11 billion	99.9999999999999%

zk-SNARKs: Zero-Knowledge Succinct, Non-interactive Arguments of Knowledge

What is a zk-SNARK?

- Argument of knowledge
  - Not technically a proof because of the probabilistic nature
- Succinct:
  - Must be small and computationally easy to verify
- Non-interactive:
  - The prover and the verifier dont both need to be online at the same time

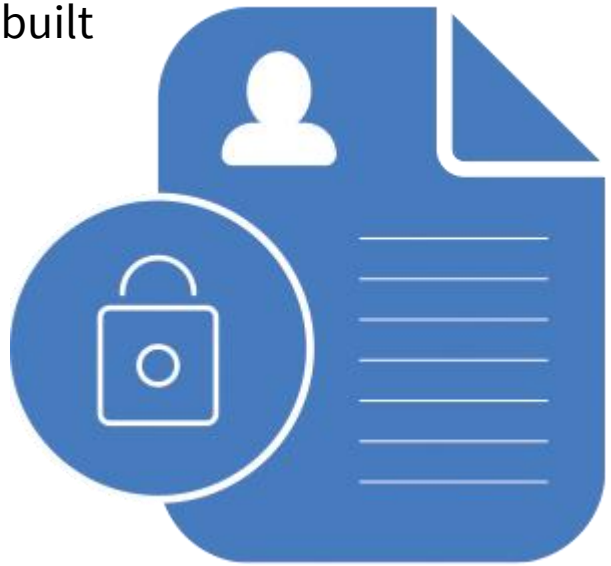
Available for use on the Ethereum main net as of the Byzantium hard fork in late 2017

Completely Private Blockchains

Private, turing complete EVM state changes

- Private, turing complete state changes in the EVM
  - Entire state change data is private, similar to how each transaction data is private in cash
  - Can still prove that transactions and therefore state changes are valid

- Fast, completely private blockchain that anonymizes all computation data using zero knowledge proof technology is still yet to be built



Case Study: Zcash

Zcash/Zerocash is a cryptocurrency that facilitates private account balances using Zero Knowledge Proofs

The whole blockchain uses zero knowledge proofs at its core protocol layer to enable completely private transactions

- Bitcoin blockchain: Contains list of each coin transfer since inception
  - You can prove ownership of a coin by tracking a chain of valid transfers visible on the blockchain
  - However this means ultimately that the bitcoins can easily be tracked
- Zcash blockchain: Stores proofs that each transfer is valid
  - Blockchain contains a chain of proofs that transactions are valid instead of transaction data itself
  - Analyzing the blockchain you cannot get any knowledge about where any of the coins are stored

Private Elections using zero knowledge proofs

Electronic Voting: A perfect use-case for a zero knowledge proof blockchain

- Electronic Voting has many obstacles to achieving the same trustworthy set-up as paper ballots
  - Paper ballots can be recounted and the tally confirmed
  - Paper ballots can be easily private
  - Paper ballots can be made impractical to counterfeit

- A zero knowledge proof blockchain can solve all of these problems
  - Votes can be made completely private even to those directly handling them
  - The winner and total vote tally can be confirmed by anybody
  - Counterfeit voting can be eliminated through blockchain technology identity solutions

DigitalX Ltd

Financial and technical services for the blockchain marketplace.

Perth | New York