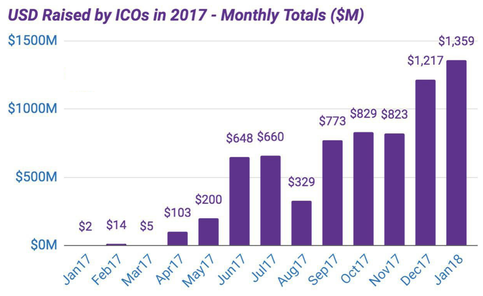
Blockchain: Regulation & Compliance

Jacqueline Garrahan, Applied Mathematics, Northeastern University, Clinical Quality and Mfg

Blockchain Regulatory Environment

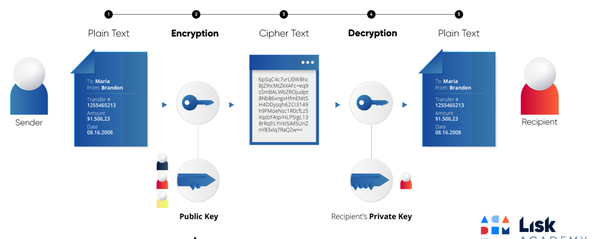
SEC Regulation



- Initial Coin Offerings (ICOs) are token launches used to rapidly raise capital[1]
- 80 firms subpoenaed by SEC March for violating securities laws
- However, the SEC has ruled Ethereum and Bitcoin are **NOT** securities
  - Projects may be classified as securities while platform is not

GDPR

"[...] Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an **identifiable natural person**."
- Recital 26, EU GDPR

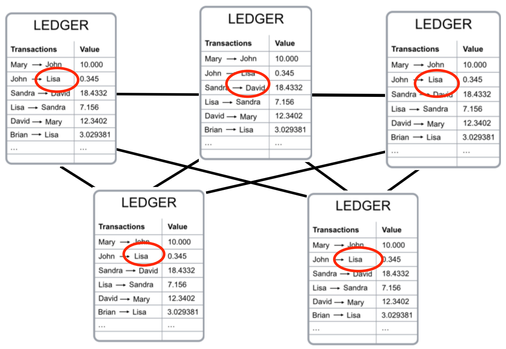


Visible to the entire network

Public keys are classified as pseudonymous data under GDPR

Because public keys can be considered identifiable data:

- Replications of a blockchain could be considered data sharing events
- Blockchain immutability is incompatible with the right to be forgotten



Government Organizations Using Blockchain

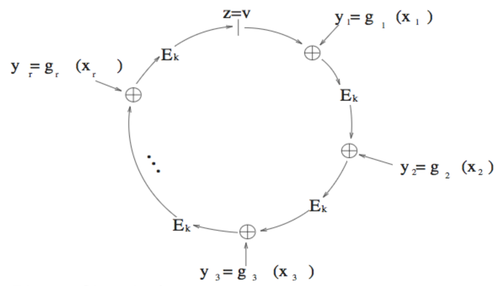
FEDERAL RESERVE BANK OF BOSTON™

- Global movement towards exploring blockchain technologies
- Applications include mitigating corruption, expanding financial inclusion, and managing digital identifications

Anonymous Blockchain Cryptosystems

Anonymous blockchain cryptosystems are compatible with GDPR

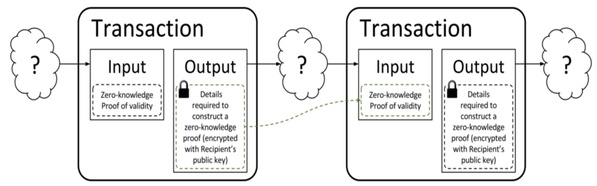
Ring Signatures



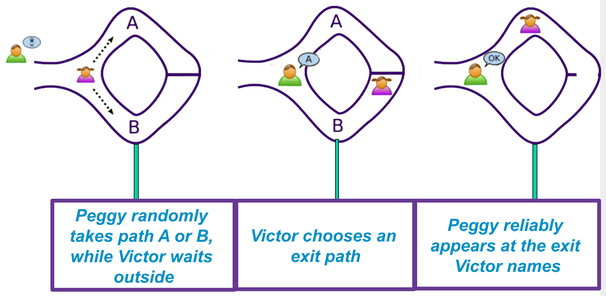
Rivest, Shamir, & Tauman ring signature scheme

- Digital signatures on transactions formed from keys of groups of users
- Unable to identify which individual initiated transaction
- Able to prove that a transaction came from the pool

Zero Knowledge Proofs



- Individual is able to prove knowledge of a secret without revealing that secret
- The contents of transactions may remain private



Sources:
Rivest, R., Shami, A., Tauman, Y. MIT. How to Leak a Secret.
https://tokeneconomy.co/%EF%B8%8F-token-economy-34-rip-ico-c893d45d3fd6
https://medium.com/@argongroup/on-zero-knowledge-proofs-in-blockchains-14c48cfd1dd1
https://cryptologie.net/article/193/schnorrs-signature-and-non-interactive-protocols/