# Blockchain

Security and Digital Identity

# Contents

- Digital Signatures and Anonymity
- Public and Private Keys
- Trustless Asset Management
- Tor and the Silk Road

# Digital Signatures and Anonymity

# Recap: Digital Signatures

- Public and Private Keys
  - Each can decrypt what the other encrypts
- A digital signatures combines a digital item with proof of private key ownership
- To create a digital signature
  - Hash the digital item
  - Encrypt the hash with the **private** key
- To validate a digital signature
  - Decrypt the encrypted hash with the public key
  - The decrypted hash should be the hash of the digital item
- https://sectigostore.com/blog/ecdsa-vs-rsa-everything-you-need-to-know/

# Anonymity and the Blockchain

- Bitcoin is pseudonymous, not anonymous
- Data mining is possible and there are commercial tools to support the activity (e.g. https://www.chainalysis.com/)
- There are privacy mechanisms (tumblers, mixers)
- Some blockchains are anonymous (Monero, Zcash)
- Selective anonymity hurts fungibility

# Attestations

- The act of showing, or evidence showing that something is true
- Fundamental building block for digital identity blockchain use cases
- Ideal is that attestations can be produced on request, but cannot be associated with your profile without your involvement/permission
- Blockchain as certificate authority
- Does not need one entry per attestation (http://www.blockcerts.org)
- Does not need a blockchain, except for updates
- Data does not need to be stored on chain

# Shamir’s Secret Sharing

- Say we have a secret, “p4ssw0rd”, and wish to securely distribute it between M parties
- We could split the alphanumeric string in M parts (e.g., M=2: “p4ss”, “w0rd”)
- But every part is required to recover the secret
- Enter Shamir’s Secret Sharing *
- With SSS, we can split secret into N of M parts, such that only N parts are required to retrieve the secret, and the secret’s entropy is not reduced if any of of the parts are compromised (up to the threshold)
- Usage: social recovery, estate management, secure seed phrase storage

* https://cryptography.fandom.com/wiki/Shamir%27s_Secret_Sharing

# Self-Sovereign Identity

- Your on-chain identity, backed by ownership of a private key
- Must be secure and recoverable
- Must be able to cope with Identity Theft
- Your digital identity might some day own your house, your savings
- uPort pattern of proxy identity ownership shows promise (UPDATE: never achieved)
- Social Recovery Patterns with Shamir’s Secret Sharing a useful approach
- https://www.coindesk.com/path-self-sovereign-identity/

# 10 Principles for Self Sovereign Identity

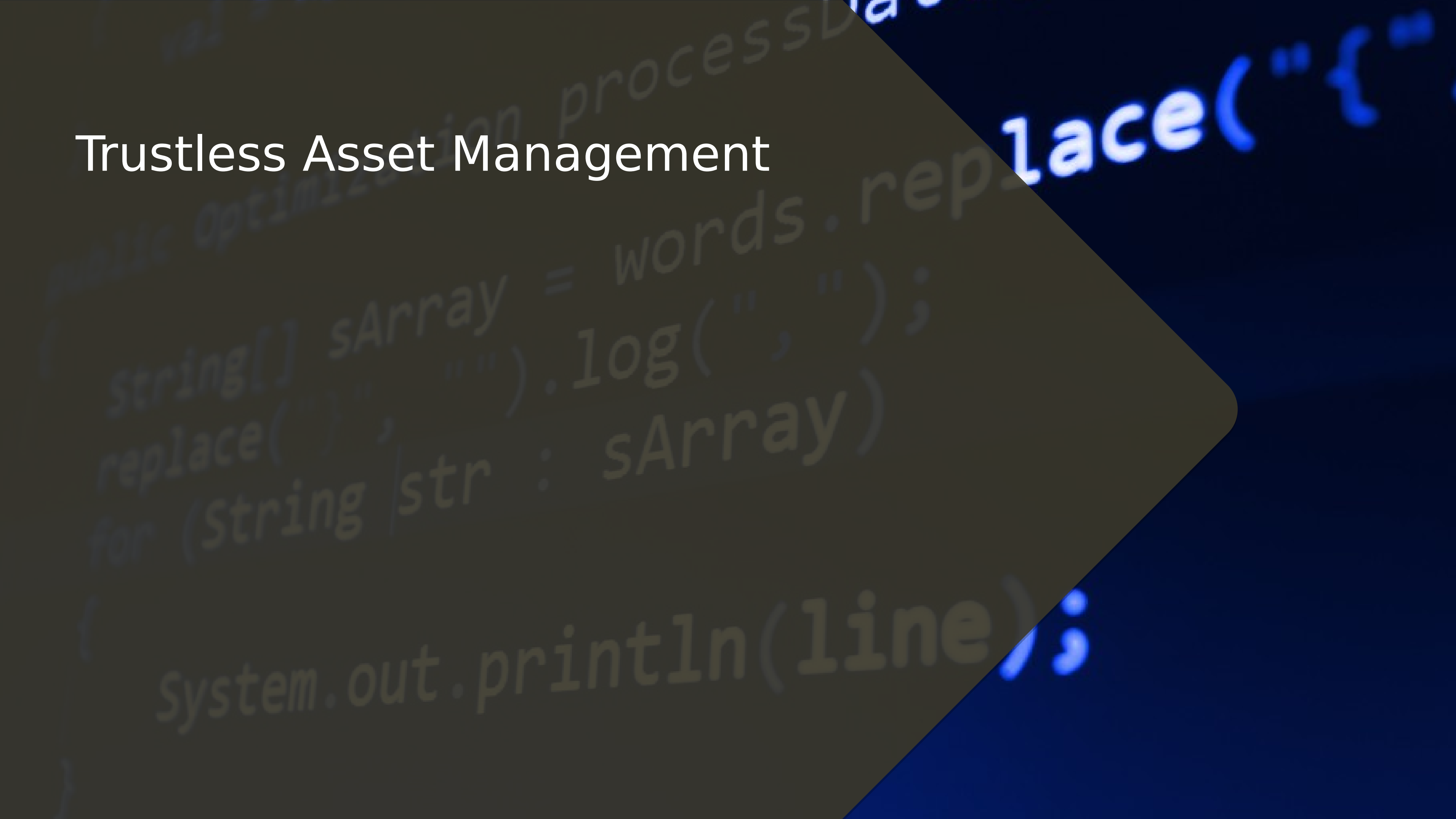
- Existence (independent of others)
- Control (controlled by the user)
- Access (user must have access to data)
- Transparency (open source algorithms and platforms)
- Persistence (must be long lived – right to be forgotten)
- Portability (must be global, not owned by third party)
- Interoperability (must be capable of integrating with other systems)
- Consent (users must agree to use of their identity)
- Minimalisation (data protection, only reveals what is necessary)
- Protection (rights of the users over the network – censorship resistance)

https://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

# Biometrics

- Identification, not authentication
- Biometrics are convenient identification, not authentication
- Your DNA, fingerprints and your IRIS patterns are all readily available
- Apple TouchID is 1 in 50,000, Apple FaceID is 1 in 1,000,000
- Biometric systems are not as secure as passwords (which have their own security issues)
    - https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands
- Biometrics cannot be your private key

# Trustless Asset Management



# Atomic Swaps

- Alice creates a bitcoin transaction that gives Bob 1 BTC
  - To access the outputs requires Bob’s signature and a secret (hash lock)
- Alice sends Bob the hash of her secret
- Bob creates a Litecoin transaction that gives Alice 140 LTC
  - To receive the transaction output requires Alice’s signature and the secret
- Bob and Alice swap transactions
- Alice signs the Litecoin transaction, providing the secret and broadcasts it
- The secret is now known (it’s visible on the Litecoin chain)
- Bob now has the secret and can sign the bitcoin transaction
- 
- If Alice doesn’t sign the transaction, the swap doesn’t happen

# Atomic Swaps II

1. Alice: I’ll give you (*Bob 0x address*) **10 ALICE** tokens if you can produce the value, **x**, behind this hash, **H(x)** *in the next 1000 blocks*
2. Bob: I’ll give you (*Alice 0x address*) **100 BOB** tokens if **you** can produce the value behind that hash, **x** (I have no idea what it is, lol) *in the next 1000 blocks*
3. Alice: Sure, I’ll take that. *Claims **100 BOB** tokens, revealing **x** to do so
4. Bob: Thank you, now I know x. *Claims **10 ALICE** tokens using **x** that Alice revealed

- Bob and Alice have now atomically swapped tokens. Atomic, because if one operation fails, everything fails, so both parts happen as one successful operation
- If your chains have the same hashing algorithm, you can run this across chains!

# Tokenisation of Assets

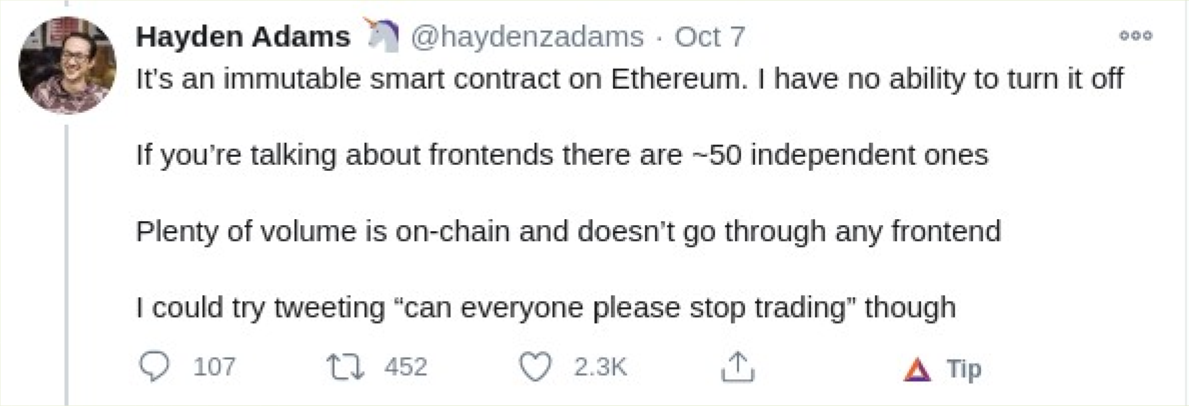
- Tokenisation of assets is foundation of large number of blockchains use cases
  - Land Registry on the blockchain
  - Stocks/Shares on the blockchain
  - Property on the blockchain (own 0.005% of a house)
  - Fund Management on the blockchain
- Trustless because the asset ownership is directly controlled by the private key, not a third party (that you would have to trust)
- Note: typically real-world assets are controlled by an entity compliant with regulations, and asset seizure/reversion is usually possible

# Decentralised Exchanges

- Still requires a third party to provide the marketplace for trades
  - But look at UNISWAP (IPFS available website, open front end interfaces, contracts running on Ethereum with governance using UNI token)
- Core difference is exchange does not control funds at any point
- Every trade is a transaction (slower than CEX), but liquidity providers can profit from trades using their liquidity.

https://app.uniswap.org/#/swap

https://uniswap.org/blog/ipfs-uniswap-interface/



**Hayden Adams** @haydenzadams · Oct 7

It's an immutable smart contract on Ethereum. I have no ability to turn it off

If you're talking about frontends there are ~50 independent ones

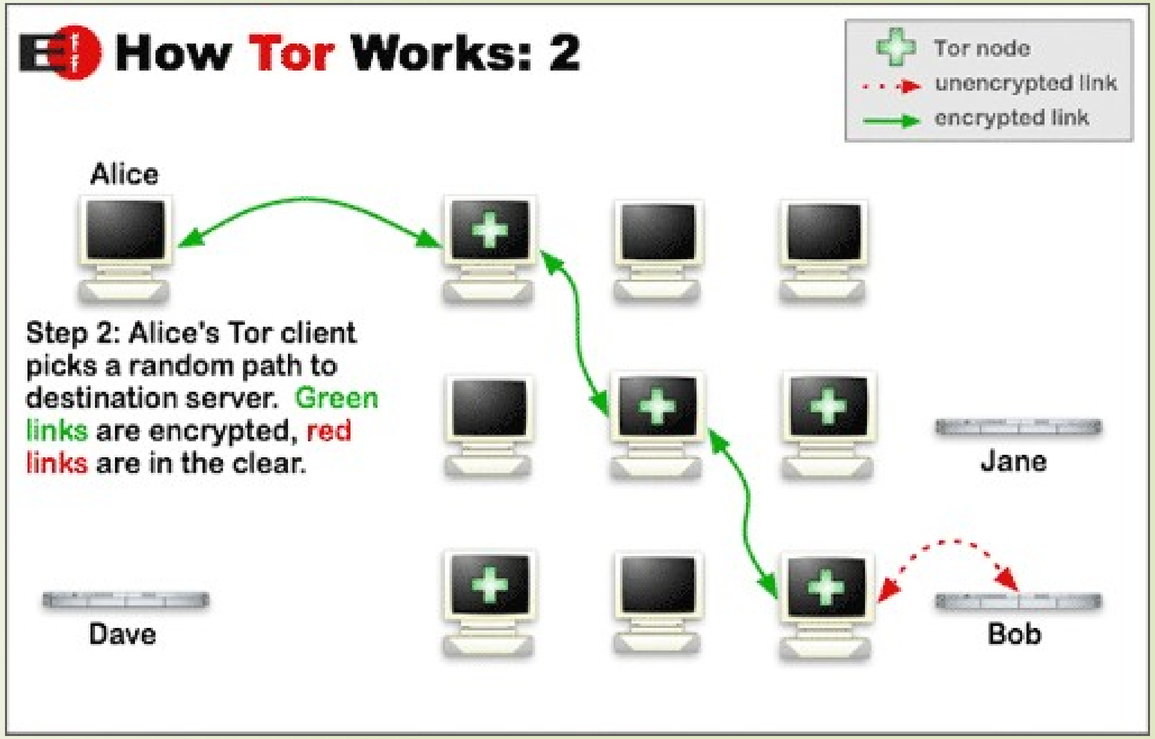
Plenty of volume is on-chain and doesn't go through any frontend

I could try tweeting "can everyone please stop trading" though

# Tor and the Silk Road

# Tor

- Developed 1990s by US Naval Research Lab
- “The Onion Router”
- Used to defeat traffic analysis
- Privacy and security tool
- Used by activists, journalists, dissidents and the dark web
- Not all servers are operated by privacy enthusiasts, some are hosted by nation states...



Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

# The Dark Web

- Accessible through TOR browser
- Anonymous hosting of websites (40,000 .onion addresses)
- Not the same as the Deep Web
- Hosts the dark web markets (e.g. http://silkroad7rn2puhj.onion/)
- July 2017 AlphaBay closed down by FBI
- AlphaBay users moved to Hansa Market (run by Dutch police, servers in Lithuania)
- Cryptocurrencies common on dark web with Monero gaining popularity
- https://www.theverge.com/2020/11/6/21552339/us-goverment-seizes-1-billion-bitcoin-profits-silk-road-wallet-individual-x

# Silk Road and Ross Ullbricht

- Created by Ross Ullbricht (Dread Pirate Roberts), currently serving life in prison
- Launched Feb 2011, closed Oct 2013 (SR2 started 6 Nov 2013)
- Site did $200m in business, DPR had $18m worth of BTC when arrested
- Silk Road BTC sold in government auctions 2014, 2015 ($334 per BTC)
- Tim Draper bought 30,000 BTC ($632) and completed the sale in 2017
- Some BTC (~$1.5m) later stolen by two FBI agents investigating case

- https://arstechnica.com/tech-policy/2015/05/sunk-how-ross-ulbricht-ended-up-in-prison-for-life/

# Summary

- Digital Signatures link data to ownership of a private key
- Bitcoin is pseudonymous, not anonymous
- Attestations are a key component in building claims on top of a digital identity
- Biometrics are username, not password
- Atomic swaps are powerful cross chain communication mechanism
- A trustless asset is one which does not require a third party