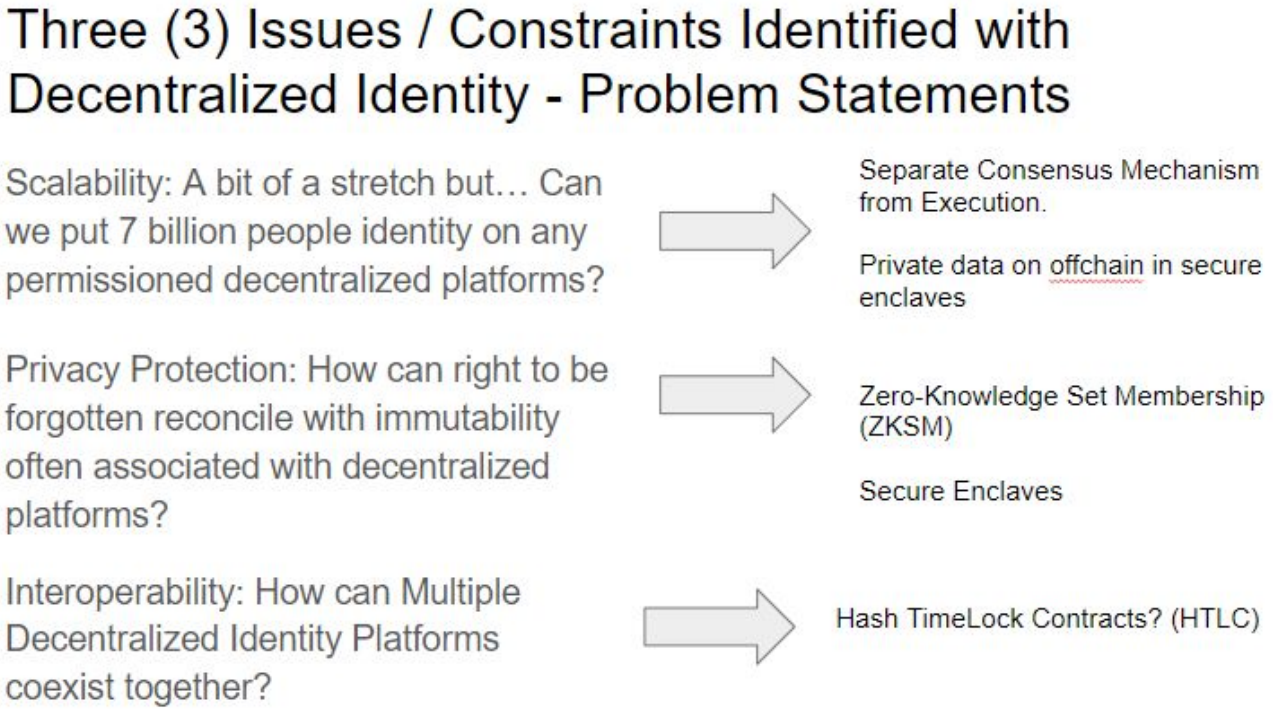
Byzantine Agreement Protocols for Large-Scale Decentralized Identity Management

Nathan Ming Kun Aw

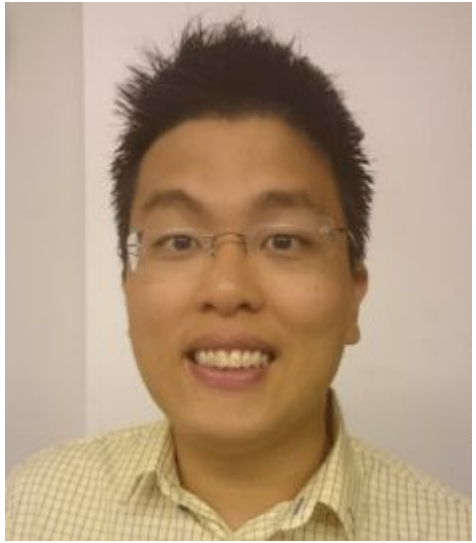
For The Decentralized Internet Infrastructure Research Group (DINRG) at the IETF 104, Prague
March 2019

In the last DIN IETF in Bangkok in 2018, I shared on how decentralized identities (“Self Sovereign Identities”) could help address the issue of data breaches and the challenges and constraints



SOURCE:https://datatracker.ietf.org/meeting/103/materials/slides-103-dinrg-decentralized-identity-01

Brief Introduction - Nathan Aw (Ming Kun Aw)



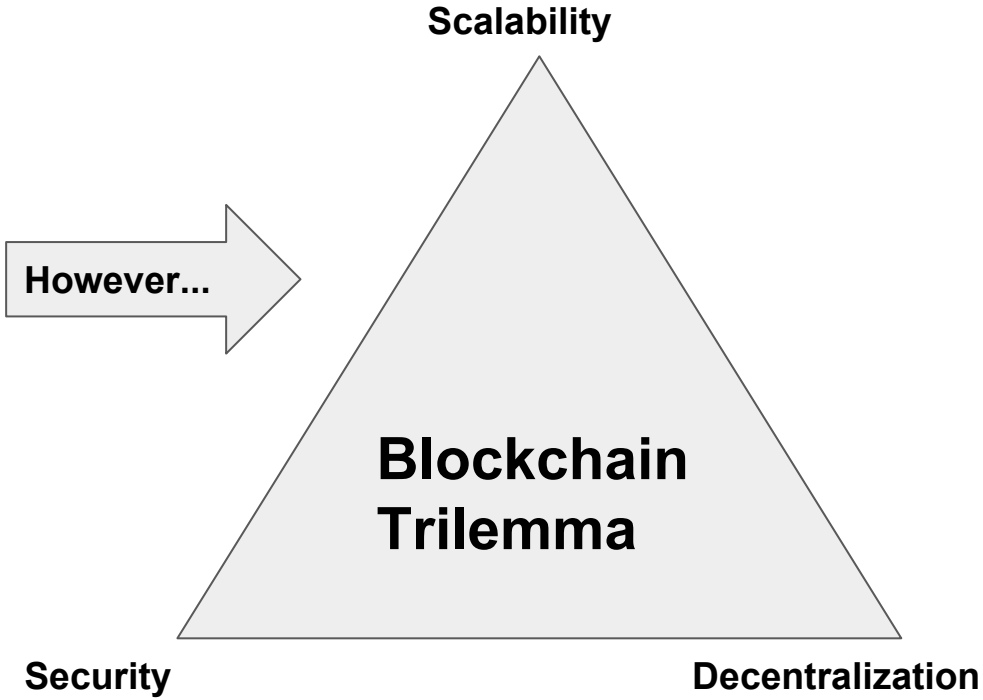
- Blockchain Research Engineer with a Leading Financial Institution in Singapore/ASEAN
- Previously worked at Fortune 500 companies - Oracle and Accenture
- Sit on the ERC725 Alliance - ERC 725 is a proposed standard for blockchain(ethereum)-based identity
- A Hyperledger Technical Ambassador for ASEAN and part of the Global Hyperledger Speakers Bureau
- Conduct multiple technical meetups in Asia in the area of decentralized identity and blockchain interoperability
- Sit on the IEEE Blockchain Editorial Board to advance ideas relating to blockchain
- Specific research interests in decentralized identity and interoperability within decentralized systems

REFERENCES:

https://www.hyperledger.org/news/speakersbureau
https://erc725alliance.org/
https://www.hyperledger.org/community/technical-ambassador
https://www.meetup.com/BlockChain-Dapps-Technology/events/254556114/
https://www.hyperledger.org/blog/2017/12/05/developer-showcase-series-nathan-aw-ntt-data
https://www.meetup.com/Hyperledger-HK/events/248011521/
https://www.meetup.com/Hyperledger-HK/events/248011521/
https://blockchain.ieee.org/newsletter/editorial-board

For Any Large-Scale, Cross Border Decentralized Identity Management, Three (3) Attributes Are Necessary

1. Sufficiently Decentralized (i.e., Borderless)
2. Scalable on a Planetary Scale
3. And… Secure

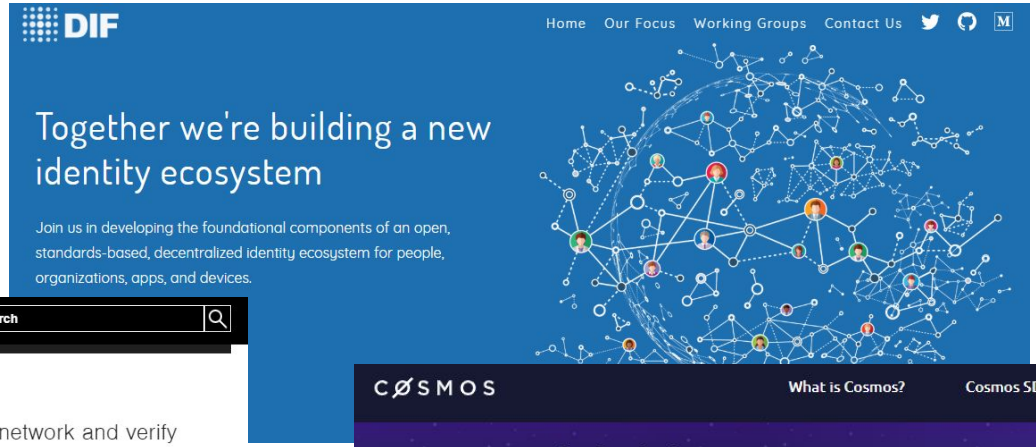


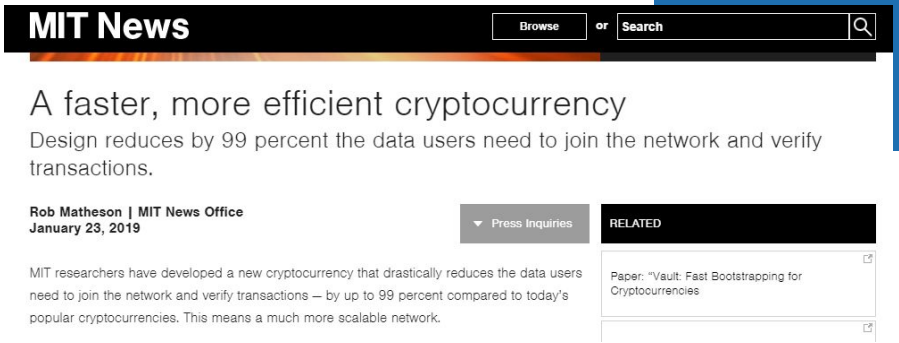
The Blockchain Trilemma

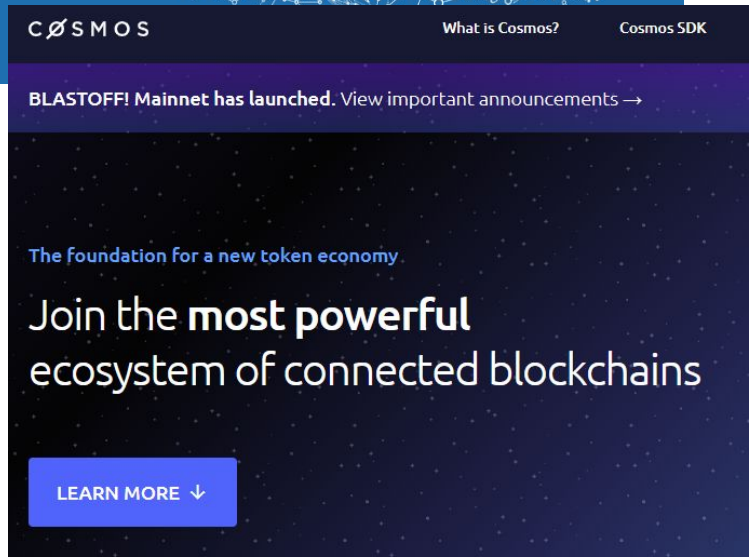
https://steemit.com/cryptocurrency/@adalhi/what-is-algorand-is-it-the-new-cardano

Meanwhile, many promising developments...

Algorand
THE BORDERLESS ECONOMY

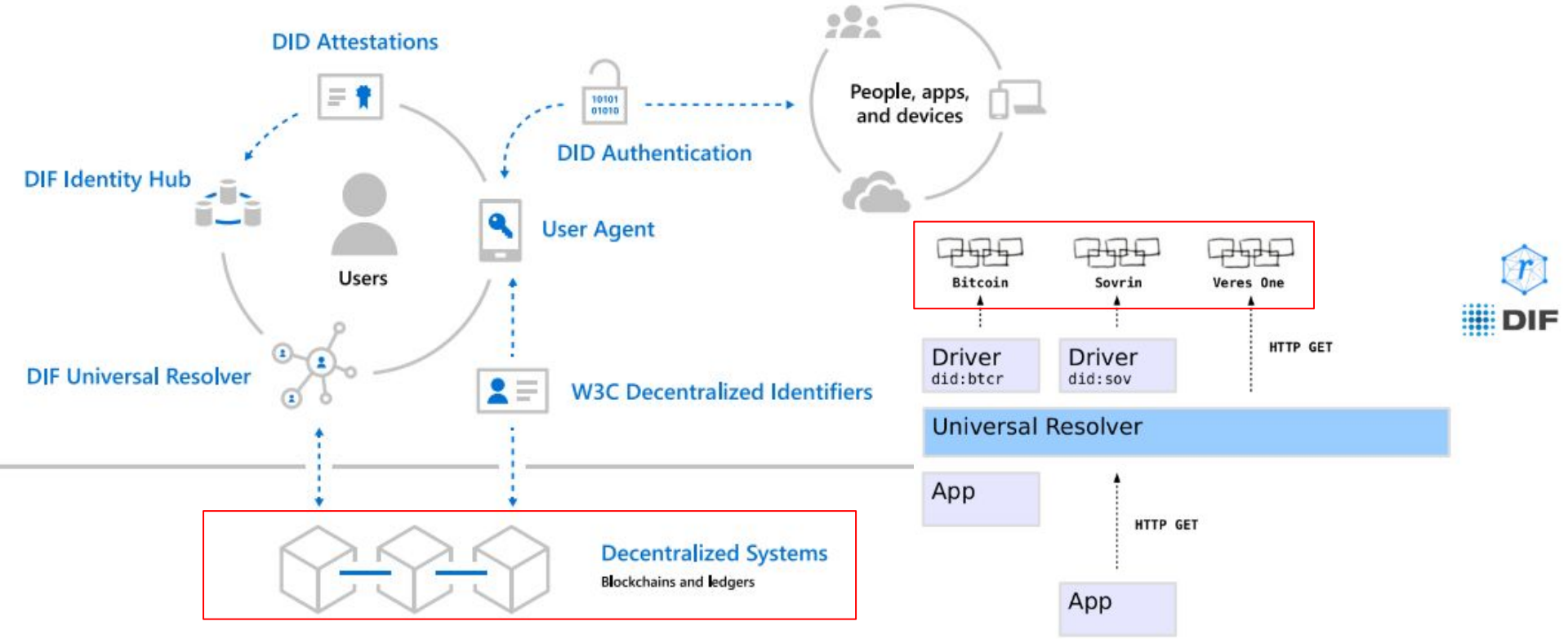






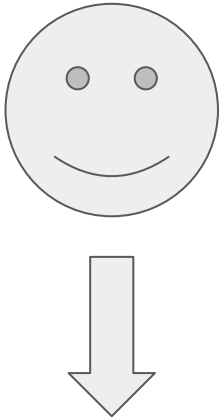
https://www.algorand.com/
https://cardanodocs.com/cardano/proof-of-stake/
http://news.mit.edu/2019/vault-faster-more-efficient-cryptocurrency-0124
https://eprint.iacr.org/2016/889.pdf
https://cosmos.network/

A Sample View of a Decentralized Identity Ecosystem



SOURCE: https://azure.microsoft.com/en-us/overview/decentralized-identity/ ; https://w3c-ccg.github.io/did-primer/

Decentralized Identifiers (DIDs)



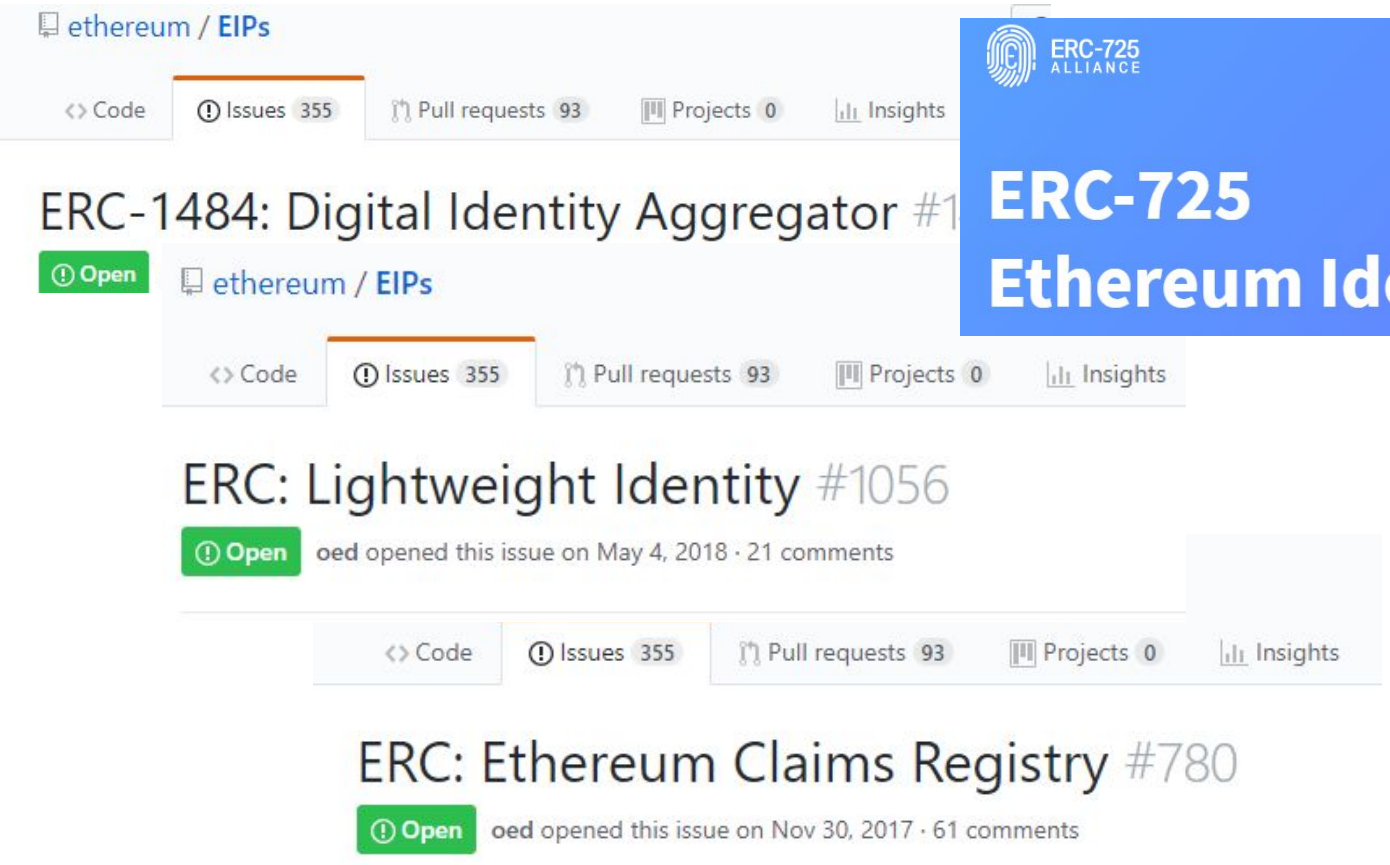
A user can have one or more DIDs, based on open standards.

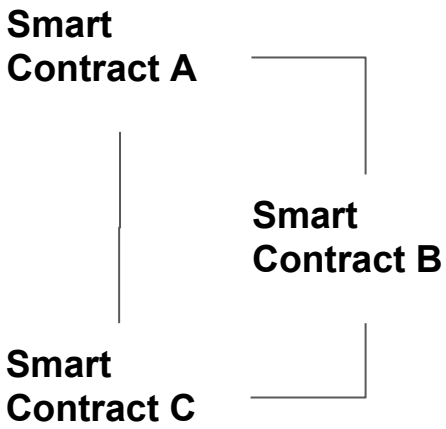
"At a superficial level, a decentralized identifier (DID) is simply a new type of globally unique identifier. But at a deeper level, DIDs are the core component of an entirely new layer of decentralized digital identity and public key infrastructure (PKI) for the Internet. This decentralized public key infrastructure (DPKI) could have as much impact on global cybersecurity and cyberprivacy as the development of the SSL/TLS protocol for encrypted Web traffic (now the largest PKI in the world)."

SOURCE: https://w3c-ccg.github.io/did-primer/

Figure 1 urn:uuid:fe0cde11-59d2-4621-887f-23013499f905

How Ethereum approaches DIDs





Scalability is Crucial - Many ways to achieve same goals with different tradeoffs

Pure (Traditional) Proof of Stake (PoS)	The creator of a new block is chosen in a pseudo-random way, depending on the user's coins at stake.
Delegated Proof of Stake (DPoS)	Users vote to elect a number of witnesses and and the top tier of witnesses (who have collected the most votes) earn the right to validate transactions.
Practical Byzantine Fault Tolerance	3F + 1

Byzantine Agreement *

A Byzantine Agreement protocol called BA, in which users are privately and pseudo-randomly selected to participate in a committee to execute one step of the protocol. The privately selected committee members then broadcast a message which includes their proof of selection, followed by a consensus procedure. This creates a more scalable system than Proof of Work based coins, since the transaction confirmations are much more efficient.*

SOURCE: https://inst.eecs.berkeley.edu/~cs261/fa18/scribe/Algorand.pdf

Algorand (“Byzantine Agreement”) Overview

Challenges

Avoid Sybil attacks, where an adversary creates many pseudonyms to influence the Byzantine agreement protocol

Must scale to millions of users

Resilient to denial-of-service attacks, and continue to operate even if an adversary disconnects some of the users

Techniques

Weighted users. To prevent Sybil attacks, Algorand assigns a weight to each user. BA⋆ is designed to guarantee consensus as long as a weighted fraction (a constant greater than 2/3) of the users are honest.

Consensus by committee. BA⋆ achieves scalability by choosing a committee—a small set of representatives randomly selected from the total set of users—to run each step of its protocol.

Cryptographic sortition. To prevent an adversary from targeting committee members, BA⋆ selects committee members in a private and non-interactive way.

SOURCE: https://inst.eecs.berkeley.edu/~cs261/fa18/scribe/Algorand.pdf; https://web.eecs.umich.edu/~manosk/assets/slides/w18/algorand.pdf

Cryptographic Sortition

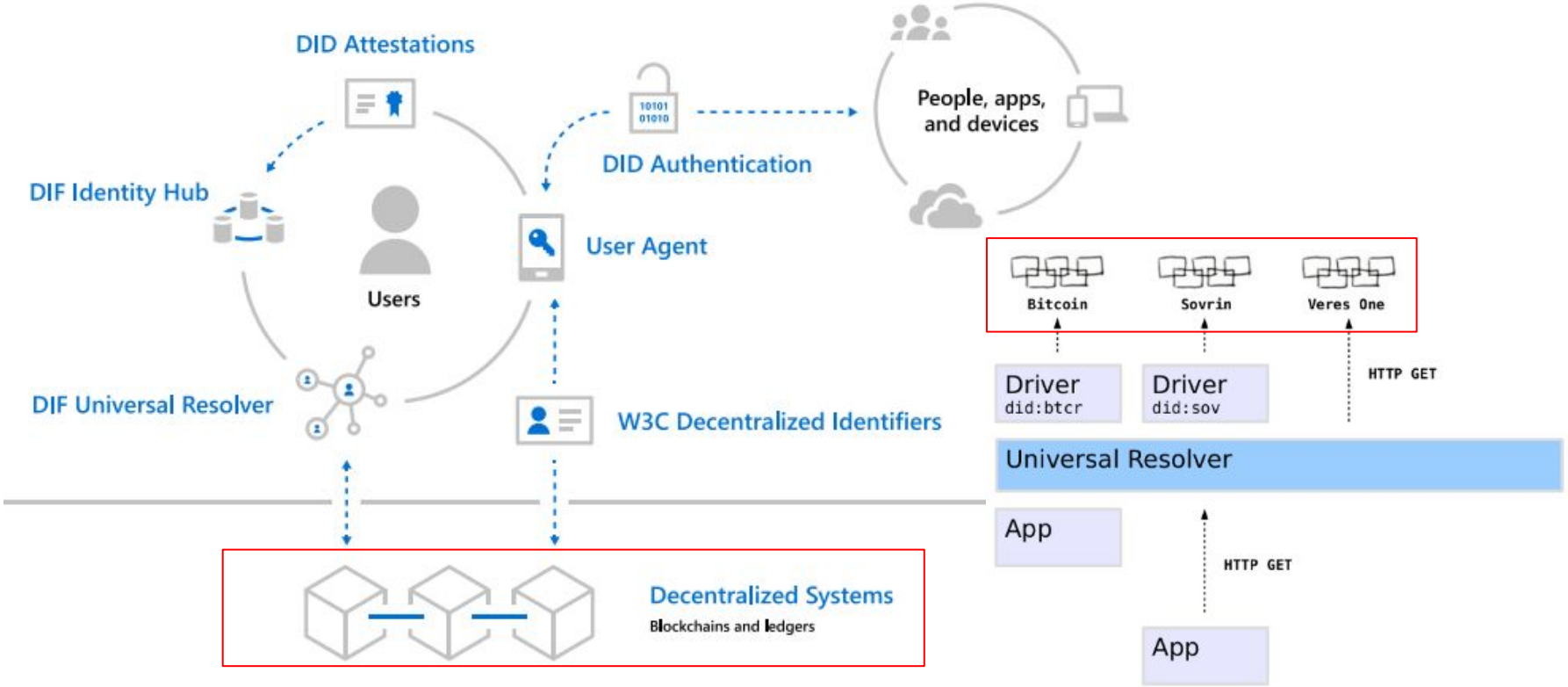
Goal: **Local and non-interactive** way to select subset of users

Implemented using **Verifiable Random Functions (VRF)**:

Hash is **pseudo-random** and is **distributed uniformly between [0, $2^{hashlen}$-1]**

https://web.eecs.umich.edu/~manosk/assets/slides/w18/algorand.pdf

Byzantine Agreement -- The Foundational Layer



SOURCE: https://azure.microsoft.com/en-us/overview/decentralized-identity/ ; https://w3c-ccg.github.io/did-primer/

3 Committee Selection

Committees are selected via **Cryptographic Sortition**; that is, a cryptographic procedure for randomly selecting a representative set of voters.
The procedure has three important properties:

1. It must select users to join the committee with probability proportional to their weights (as measured by their **stake** in the system – the percentage of all Algorand coins owned by that user)
2. Committees must be unpredictable. This is crucial so that an adversary cannot target the committee members until after they are revealed by broadcasting their votes (at which point the committee is already disbanded).
3. Committee members must be able to privately check whether they are selected, and also be able to provide a checkable proof for others to verify the selection.

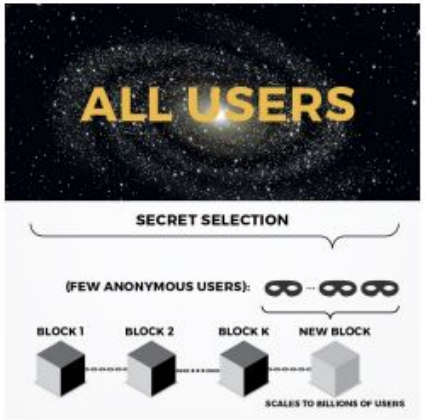


Figure 1: Illustration of committee selection (*Source: Algorand homepage* [1])

Verifiable Random Functions

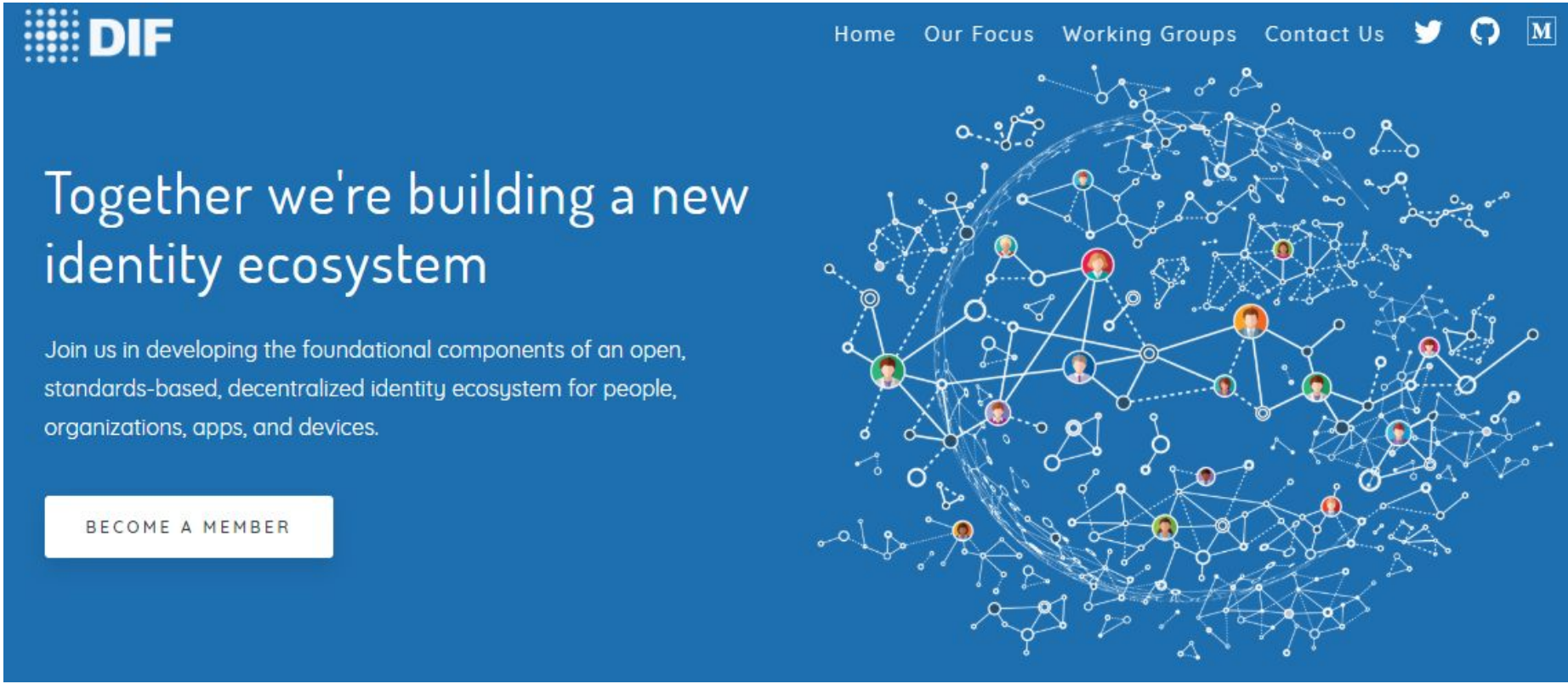
A Verifiable Random Function, or VRF, is a pseudo-random function computed based on a secret key, whose output can be publicly verified to be correct without compromising the secret key.

For a given input x, and parameterized by a private key, the Verifiable Random Function can be expressed as

$$VRF_{s_k}(x) \rightarrow (hash,\ proof)$$

where the hash is deterministic, and unpredictable to anyone without knowledge of s_k. Given the hash, p_k, and the proof, any user can check that the hash does in fact correspond to value x.

https://inst.eecs.berkeley.edu/~cs261/fa18/scribe/Algorand.pdf



https://identity.foundation/

Contact Details

nathan.mk.aw@gmail.com

https://www.linkedin.com/in/awnathan