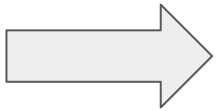
Decentralized Identity - What Lies Ahead of Us: The Open (Interesting) Research Issues

Nathan Aw Ming Kun

For The Decentralized Internet Infrastructure Research Group (DINRG) at the IETF 103, Bangkok on Nov 18

Three (3) Issues / Constraints Identified with Decentralized Identity - Problem Statements

Scalability: A bit of a stretch but… Can we put 7 billion people identity on any permissioned decentralized platforms?



Separate Consensus Mechanism from Execution.

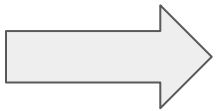
Private data on offchain in secure enclaves

Privacy Protection: How can right to be forgotten reconcile with immutability often associated with decentralized platforms?

Zero-Knowledge Set Membership (ZKSM)

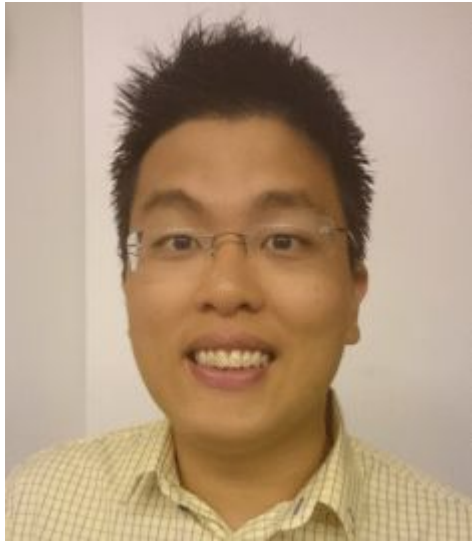
Secure Enclaves

Interoperability: How can Multiple Decentralized Identity Platforms coexist together?



Hash TimeLock Contracts? (HTLC)

Brief Introduction - Nathan Aw (Ming Kun Aw)



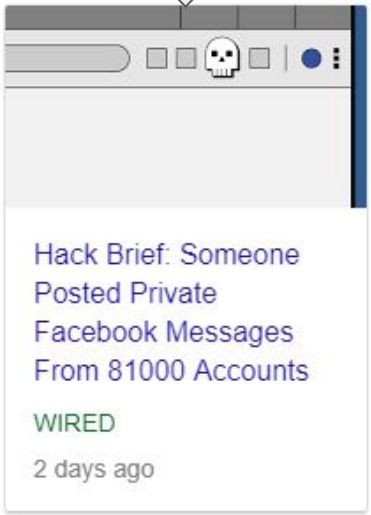
- Blockchain Engineer with a Leading Financial Institution in Singapore/ASEAN
- Previously worked at Fortune 500 companies - Oracle and Accenture
- Sit on the ERC725 Alliance - ERC 725 is a proposed standard for blockchain(ethereum)-based identity
- A Hyperledger Technical Ambassador for ASEAN and part 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

Background, Challenges and Constraints

Problem Statement: Missing Identity Layer



Is the solution a more secure centralized system?

Perhaps not….

Enter Decentralized Identity or Self Sovereign Identity

SOURCE:
https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog

What is digital identity?

- A Social Construct and with a Context
- Who you are (Nathan Aw), who you present yourself to be (e.g. Blockchain Engineer), who others perceive you to be (A Geek)
- Some Contexts can be people, family, groups, organizations, institutions
- Most importantly, identity has an identifier context

Identifiers in Context

- Nathanmkaw is a Twitter handle, nathanawmk is a GitHub handle, someone@wiley.com grants access to Wiley (using SAML?).
- NRIC (Singapore ID Card)
- Passport Number
- Singapore Airlines Krisflyer Frequent Flyer number
- Hotel Loyalty Number
- Many others….

What problems are we solving?

Problem Statement: There is **no standard** that makes it easy for users to assert their verifiable qualifications to a service provider

(e.g. my loyalty card number is X, I have an account at Bank Y, I am over the age of 21, I am a Singapore Citizen, I am a Blockchain Engineer, etc.).

Result: manual input and **fraud**

What problems are we solving?

Problem Statement: With existing attribute exchange architectures (like SAML, OpenID Connect, etc.), users, and their verifiable claims, do not independently exist from service providers. This means users can't easily change their service provider without losing or fragmenting their digital identity.

Result: vendor lock-in, identity fragility (duplication, confusion, and inaccuracy), reduced competition in the marketplace, and reduced privacy for all stakeholders.

Other Challenges

Problem: There is no interoperable standard capable of expressing verifiable claims that cuts across industries (e.g., finance, retail, education, and healthcare).
Result: industry-specific solutions that are costly, inefficient, proprietary, and inhibit users' ability to manage their digital identities in a cohesive way.

Summary: users cannot control their own identities and information, leading to a lack of security, vendor lock-in, and industry specific solutions.

Decentralized Identifiers (DID)

- Developed at Rebooting-the-Web-of-Trust workshop and W3C Credentials CG
- Persistent, dereference-able, cryptographically verifiable identifiers
- Registered in a blockchain or other decentralized network
- **did:sov:3k9dg356wdcj5gf2k9bw8kfg7a**
- Modular specification using “methods”:
- **did:sov**, **did:btcr**, **did:v1**, **did:uport**, ...
- Can be pairwise unique for each relationship
- Resolution: DID → DID Document
  - Set of public keys
  - Set of service endpoints

Method	DID Prefix
Sovrin	did:sov:
Bitcoin	did:btcr:
uPort	did:uport:
VeresOne	did:v1:
IPFS	did:ipid:
IPDB	did:ipdb:
Blockstack	did:stack

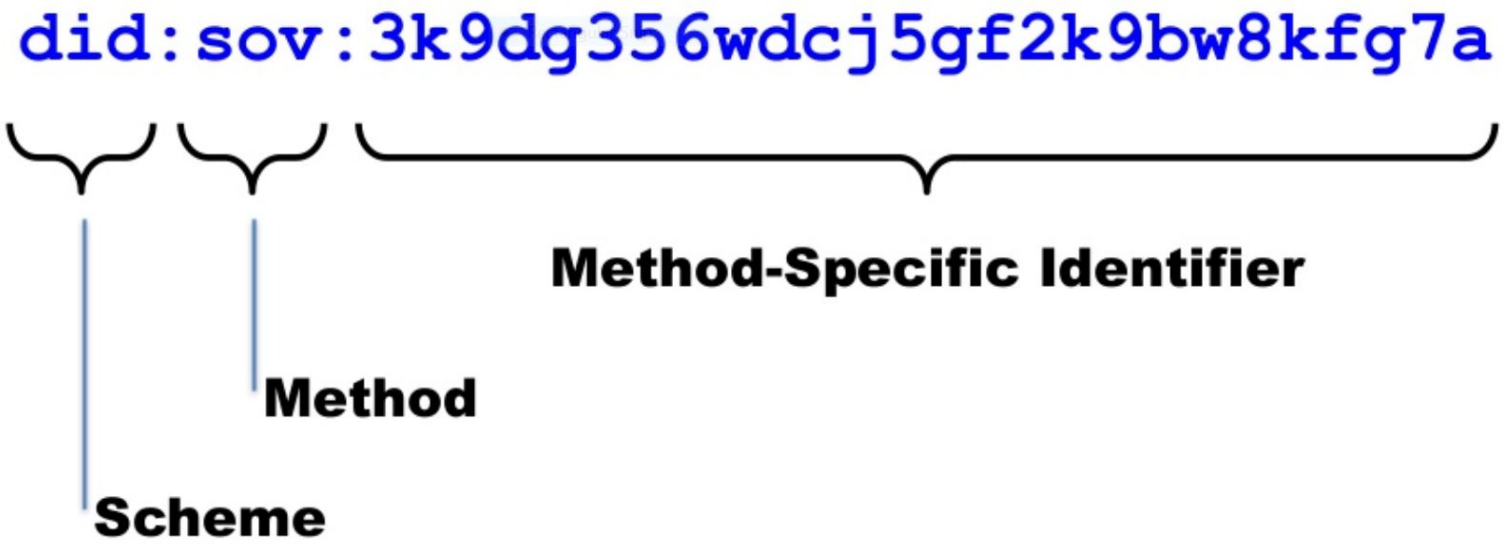
https://www.w3.org/2018/vocabws/presentations/Sabadello.pdf

Sample DID Document

- Example DID Document:


```
{
  "@context": "https://w3id.org/did/v1"
  "id": "did:btcr:xkrn-xzcr-qqlv-j6sl",
  "service": [
    {
      "type": "agent",
      "serviceEndpoint": "https://azure.microsoft.com/dif/hub/did:btcr:xkrn-xzcr-qqlv-j6sl"
    },
    {
      "type": "xdi",
      "serviceEndpoint": "https://xdi03-at.danubeclouds.com/cl/+!:did:btcr:xkrn-xzcr-qqlv-j6sl"
    }
  ],
  "authentication": {
    "type": "EdDsaSASignatureAuthentication2018",
    "publicKey": [
      "did:btcr:xkrn-xzcr-qqlv-j6sl#key-1"
    ]
  },
  "publicKey": [
    {
      "id": "did:btcr:xkrn-xzcr-qqlv-j6sl",
      "type": "Secp256k1VerificationKey2018",
      "publicKeyHex": "024a63c4362772b0fafc51ac02470dae3f8da8a05d90bae9e1ef3f5243180120dd"
    }
  ]
}
```

What does a DID look like?



Each ID has a public and private key

Some Definitions

Claim: an assertion made about a subject (of a linked data triple)

Credential: (aka Presentation) A set of one or more claims made by the issuer. A verifiable credential is a credential that is tamper-evident and that has authorship that can be cryptographically verified. Verifiable credentials can be used to build verifiable presentations, which can also be cryptographically verified.

Verification: The process that cryptographically demonstrates the authenticity of a verifiable credential or a verifiable presentation.

Decentralized Identifier: A globally unique identifier that does not require a centralized registration authority because it is registered with distributed ledger technology or other form of decentralized network.

Definitions from Verifiable Claims Data Model and Decentralized Identifiers 1.0

Connection between Verifiable Claims and DID?

- DID can exist without verification
- Verifiable Credentials are identifier-agnostic
- But, VC can VERIFY a DID
- The combination can afford certain things, such as cryptographic security (via a hyperledge, aka blockchain technology)

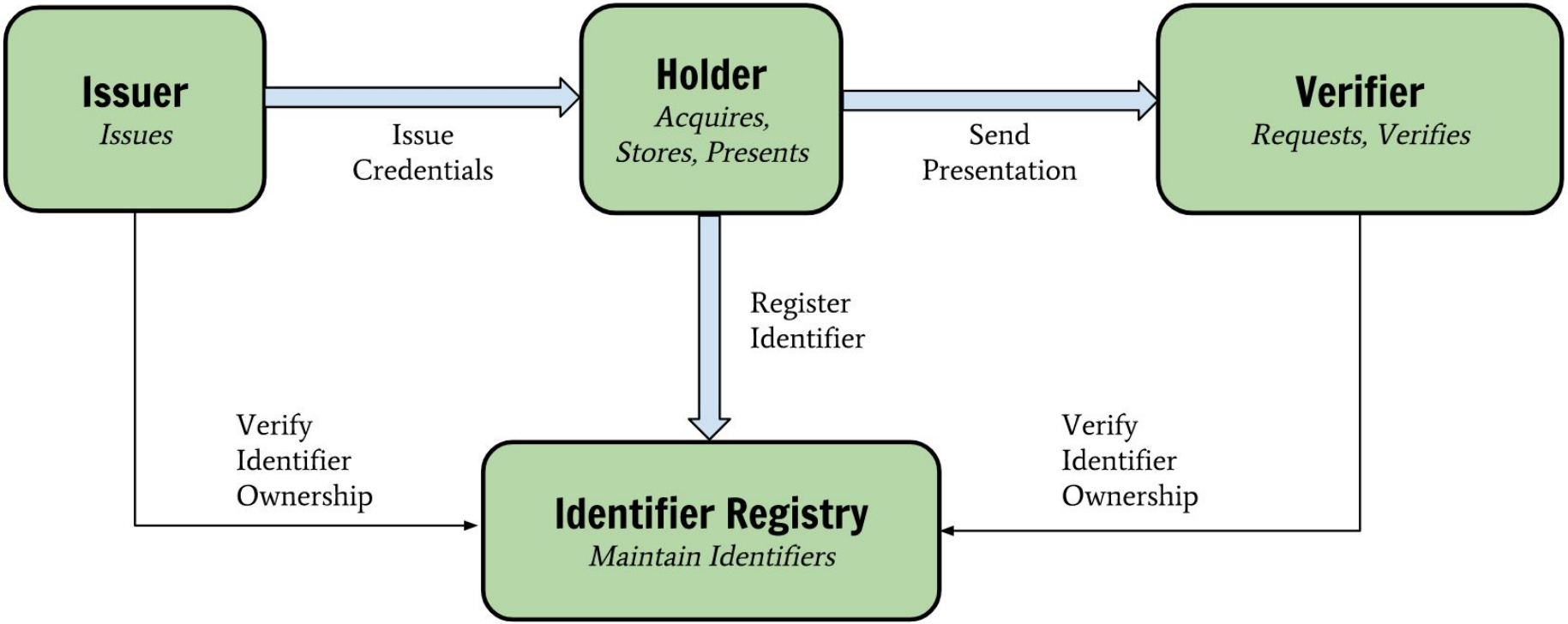
How does it work?

DID infrastructure can be thought of as a global key-value database in which the database is all DID-compatible blockchains, distributed ledgers, or decentralized networks. It is a virtual DB of DID Documents.

What is in a DID Document?

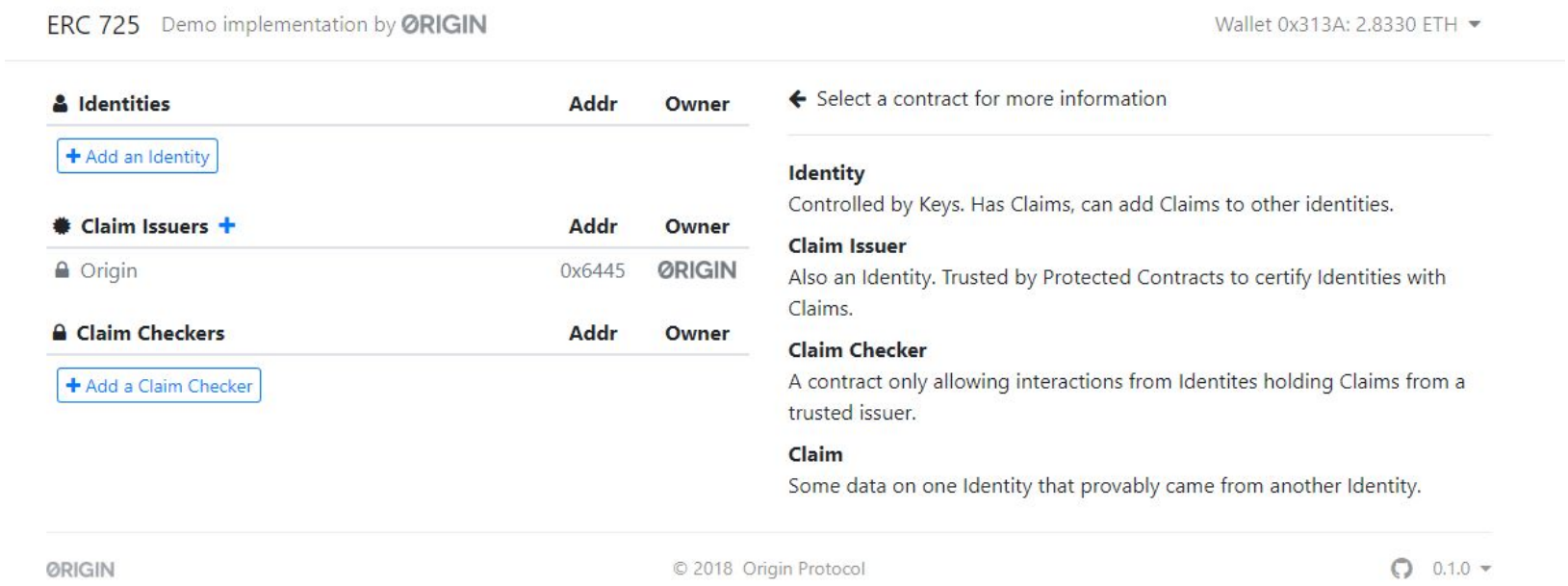
- DID
- Cryptographic material (e.g. public keys)
- Cryptographic protocols
- Service endpoints for interaction with subject
- Timestamps
- JSON-LD signature (optional)

W3C Verifiable Credentials

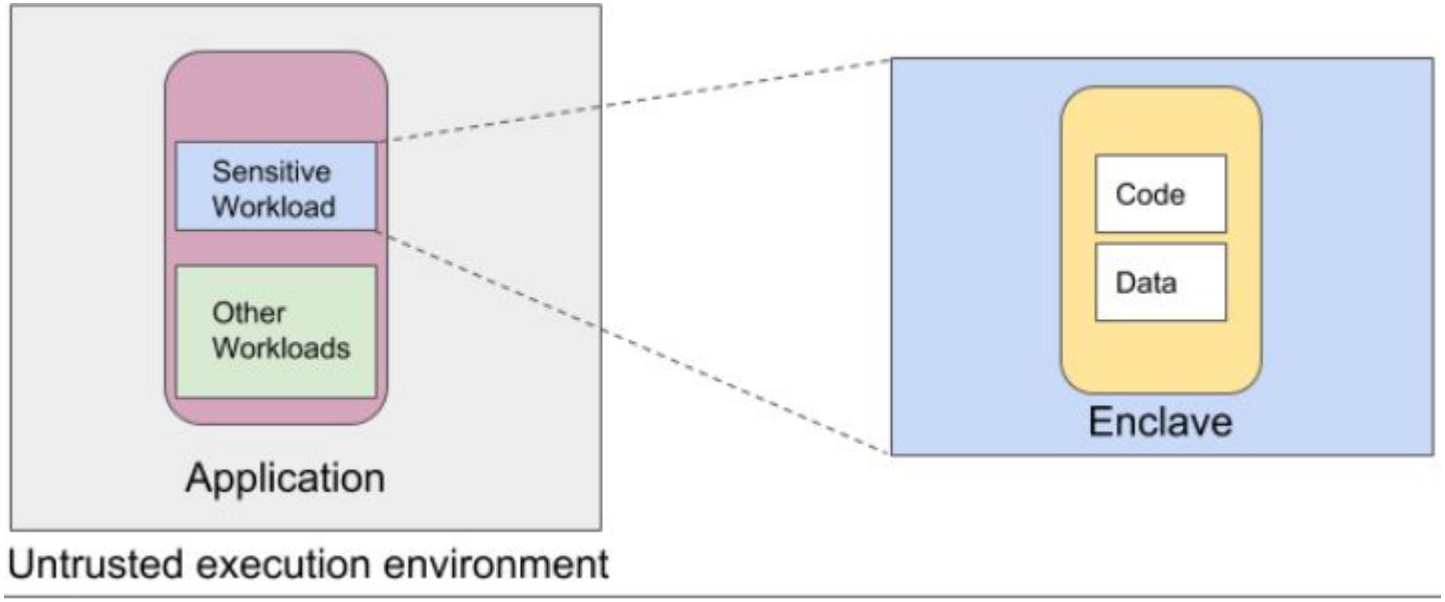


An ERC725 Demo Implementation

https://playground.originprotocol.com/#/



Exploring the Usage of Secure Enclaves to Enable Privacy Protection. E.g. Google Asylo



https://github.com/google/asylo

Explore how Zero Knowledge Proofs can be leveraged to limit exposure of our PII during attestation, thereby achieving GDPR

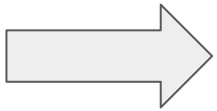
Definition of Zero-Knowledge Proof

Enable a **Prover** to convince a **Verifier** of the validity of a statement

- Yields nothing beyond validity of the statement
- Incorporates randomness
- Is probabilistic
  - Does not provide absolute certainty

Three (3) Issues / Constraints Identified with Decentralized Identity - Problem Statements

Scalability: A bit of a stretch but… Can we put 7 billion people identity on any permissioned decentralized platforms?



Separate Consensus Mechanism from Execution.

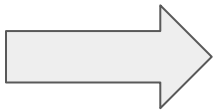
Private data on offchain in secure enclaves

Privacy Protection: How can right to be forgotten reconcile with immutability often associated with decentralized platforms?

Zero-Knowledge Set Membership (ZKSM)

Secure Enclaves

Interoperability: How can Multiple Decentralized Identity Platforms coexist together?



Hash TimeLock Contracts? (HTLC)

Contact Details

nathan.mk.aw@gmail.com

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