SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A++' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF INFORMATION TECHNOLOGY

BLOCK CHAIN AND CRYPTOCURRENCY

IV YEAR - VII SEM

UNIT 5 – **CRYPTO CURRENCY REGULATION**

CRYPTO CURRENCY REGULATION

Why is blockchain identity a breakthrough?

- Distributed ledgers (blockchains) are tremendously secure, scalable, and reliable
- When applied to identity, a distributed ledger can solve the "root of trust" problem:

  How can there be a global source of identity that everyone trusts, but isn't owned or controlled by any
  one company or government?

- It enables true *self-sovereign* identity

PHIL WINDLEY'S

TECHNOMETRIA

WELCOME TO THE INTERNET OF MY THINGS

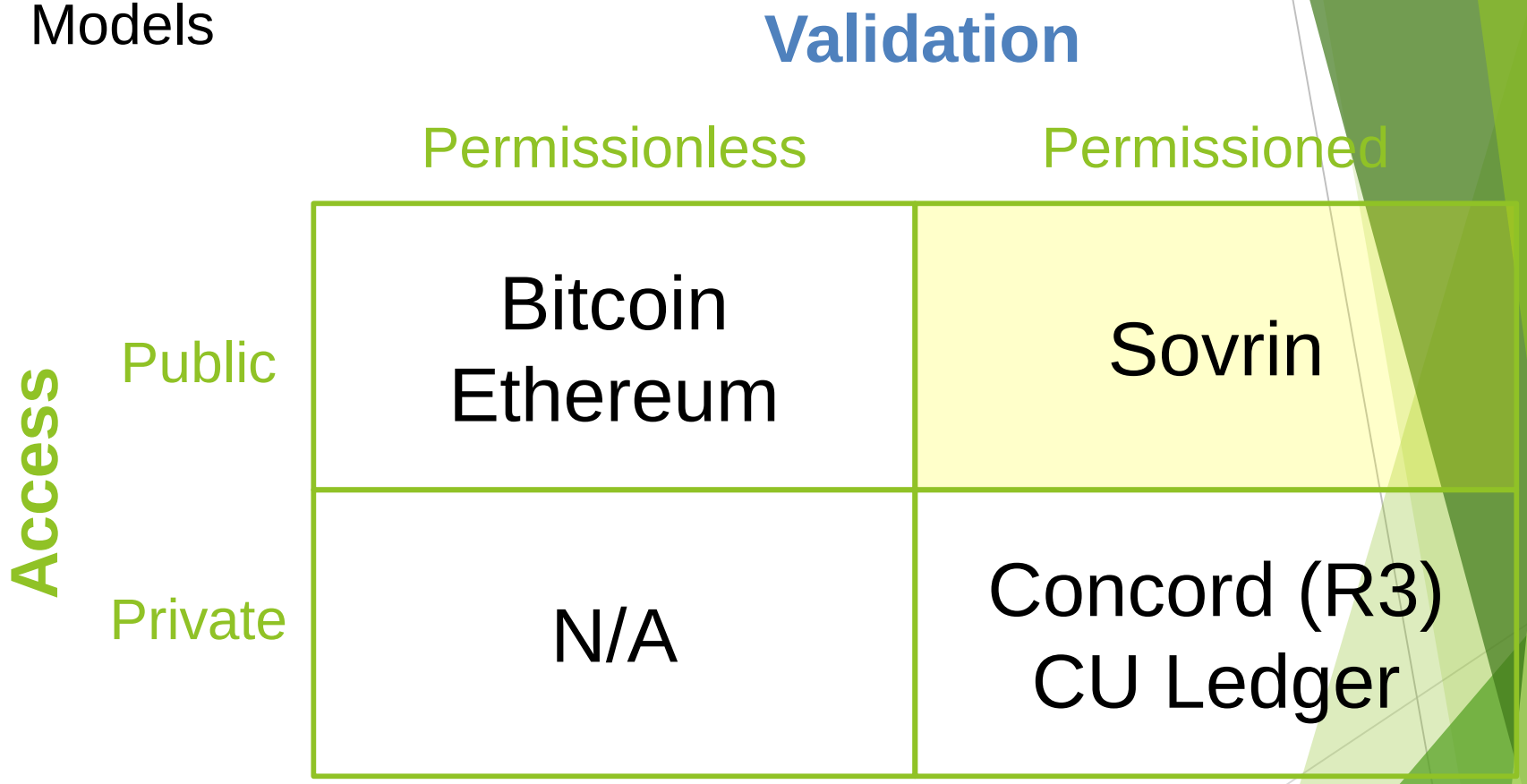
An Internet for Identity

Phil Windley // Mon Aug 29 14:30:00 2016 // BLOCKCHAIN DISTRIBUTED+LEDGER IDENTITY SELF+SOVEREIGN

Summary

Online services and interactions are being held back by the lack of identity systems that have the same virtues as the Internet. This post describes what we can expect from an Internet for identity.

Blockchain Models



So, on a “fit for purpose” identity ledger, what does a root identity record look like? And can it deliver both security AND privacy?

{ Key: “Value” }

{ DID: “DID Object” }

DIDs (Decentralized IDentifiers)

- Term originally coined by W3C Verifiable Claims Task Force
- Design goal: a globally unique identifier anyone can generate without a central authority
- Default choice: a UUID

```
did:76d0cdb7-9c75-4be5-8e5a-e2d7a35ce907
```

CIDs (Cryptographic IDentifiers)

- Term originally coined by OASIS XDI Technical Committee
- Design goal: a globally unique identifier anyone can generate—but with specified cryptographic properties
- Example: a base58 encoded Ed25519 key

```
cid-1:MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCABMC
```

Bridging the DID and CID Worldviews

- There are strong arguments for both
- We are currently seeking a consensus across the two camps
- But on this we all agree: there should be a single unified standard for the globally unique identifier of a DID object

{ Key: “Value” }

{ DID: “DID Object” }

DID Objects: The Fundamentals

1. JSON object
    1. Conformant with RFC 7159
2. Digitally signed
    1. JSON Web Signature (RFC 7515)
    2. JSON-LD signature
    3. JXD (JSON XDI Data) signature

DID Objects: The 4 Essential Elements

1. Identifier (reflexive)
2. Pointer(s) to sources of claims (attributes)
3. Cryptographic Proof of Ownership
4. Cryptographic Proof of Update

Proof of Ownership: Two Options

1. CID
   - Easy if already supported by the DLT
   - Extensible to different CID types
2. PEM (Privacy Enhanced Mail) format
   - Popular public key encoding format
   - RFCs 1421-1424

Proof of Update: Three Options

1. Self
2. M of N signatures (CID or PEM)
3. Smart signatures (Christopher Allen et al)

Binding DIDs to DLTs

- A DID binding defines the CRUD (Create, Read, Update, Delete) operations on a DID record for a specific DLT
- Can be defined for almost any DLT
  - Sovrin, Bitcoin, Ethereum
- **Caution:** storing DIDs on multiple DLTs introduces very complex source-of-authority problems

Four Rules for Respecting Privacy

1. Allow multiple DIDs for persona and pseudonym management
2. Avoid storing private attributes on a public ledger (even when encrypted)
3. Avoid correlation of off-ledger pointers
4. Use anonymous credentials (zero-knowledge proofs) whenever possible

Future Work: Please Join Us

- Watch for publication of DID Identifers and Objects specification
- Join us at one of the following events (all in San Francisco or Mountain View):
  - Rebooting the Web of Trust—Oct 19-21
  - Internet Identity Workshop—Oct 25-27
  - Verifiable Claims Task Force—Oct 27-28

Thank You