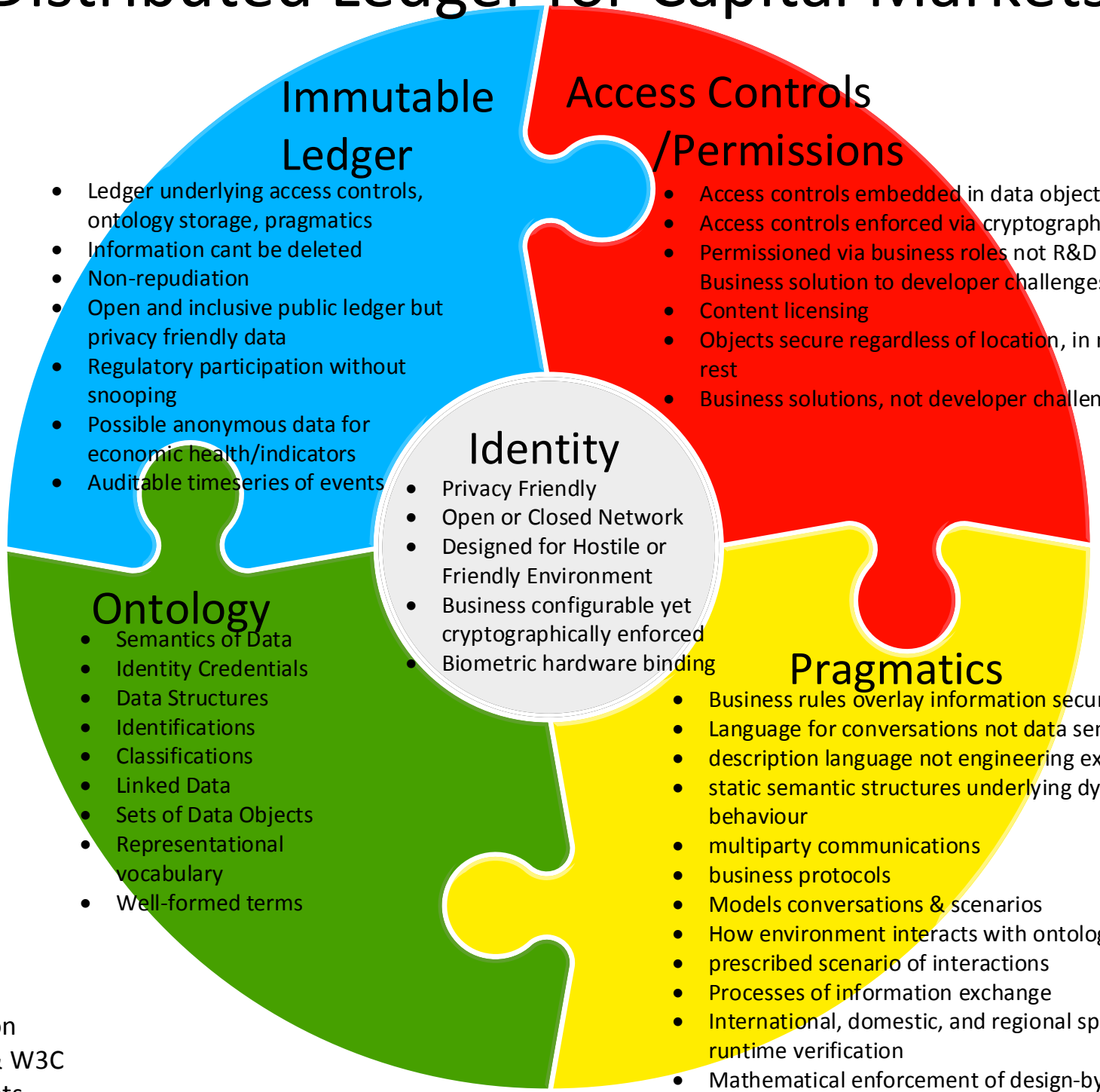
Distributed Ledger for Capital Markets



Immutable Ledger

- Ledger underlying access controls, ontology storage, pragmatics
- Information cant be deleted
- Non-repudiation
- Open and inclusive public ledger but privacy friendly data
- Regulatory participation without snooping
- Possible anonymous data for economic health/indicators
- Auditable timeseries of events

Access Controls /Permissions

- Access controls embedded in data objects
- Access controls enforced via cryptography
- Permissioned via business roles not R&D programmers. Business solution to developer challenges.
- Content licensing
- Objects secure regardless of location, in motion, or at rest
- Business solutions, not developer challenges

Identity

- Privacy Friendly
- Open or Closed Network
- Designed for Hostile or Friendly Environment
- Business configurable yet cryptographically enforced
- Biometric hardware binding

Ontology

- Semantics of Data
- Identity Credentials
- Data Structures
- Identifications
- Classifications
- Linked Data
- Sets of Data Objects
- Representational vocabulary
- Well-formed terms

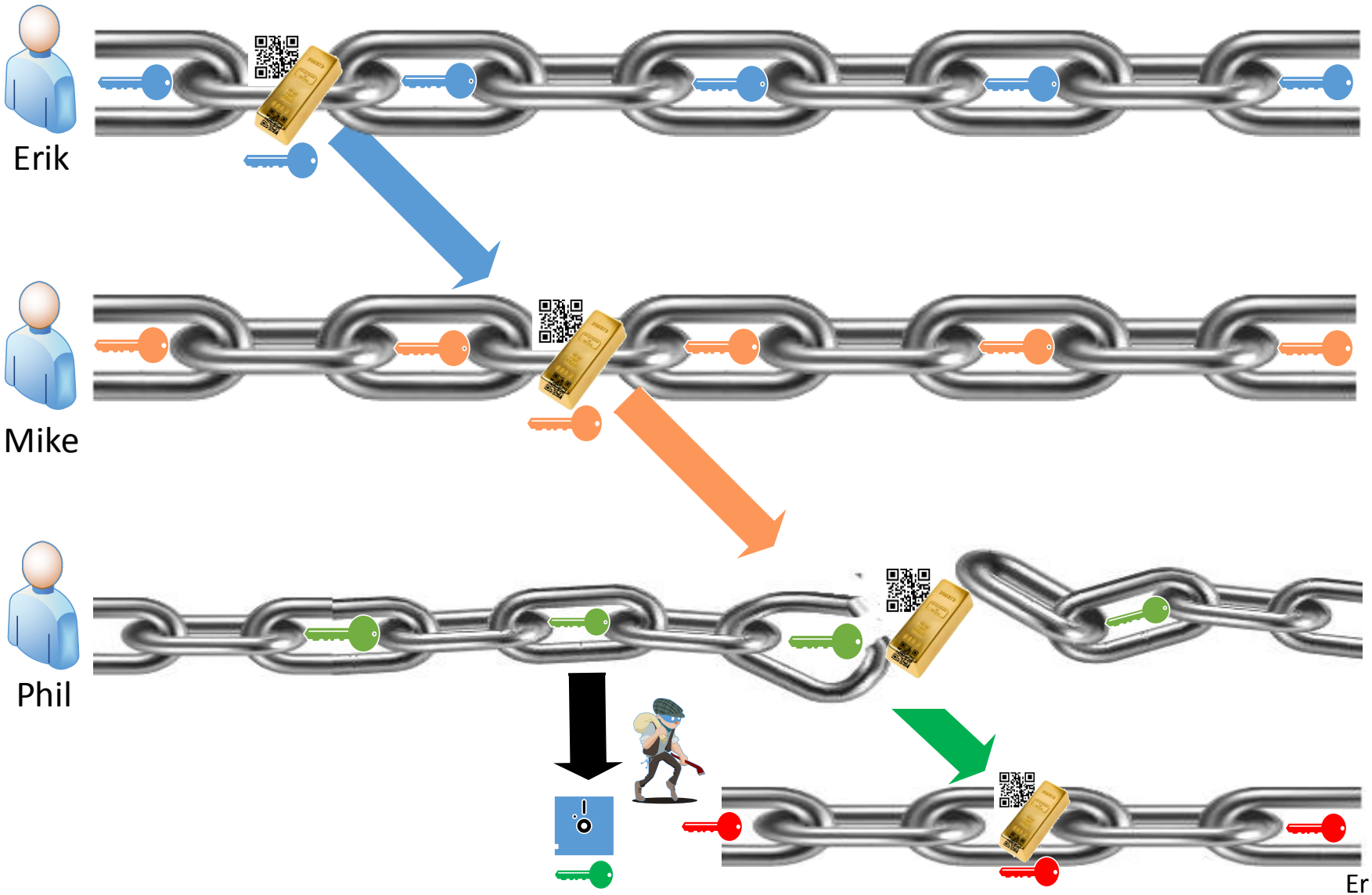
Pragmatics

- Business rules overlay information security engine
- Language for conversations not data semantics
- description language not engineering execution language
- static semantic structures underlying dynamic pragmatic behaviour
- multiparty communications
- business protocols
- Models conversations & scenarios
- How environment interacts with ontology
- prescribed scenario of interactions
- Processes of information exchange
- International, domestic, and regional specification to local runtime verification
- Mathematical enforcement of design-by-contract framework for business behaviors

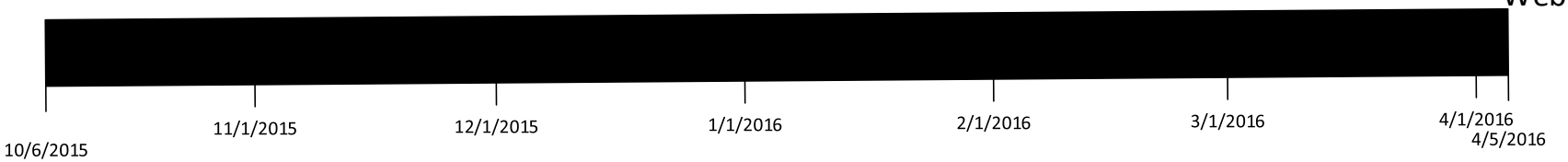
Erik Anderson
Bloomberg, X9 & W3C
Web Payments

Identity theft is easier with current Blockchain. Its just 1 private key and the protected assets are yours.

Public: 1BoJiyRnCN5E2FEG3gbC85d6h3c7Xmcqs1
Private: 5KgEvEvubwVJGjVBr8UZPe73kksTLk2dqVXh3JavzGaaJSQBUk4

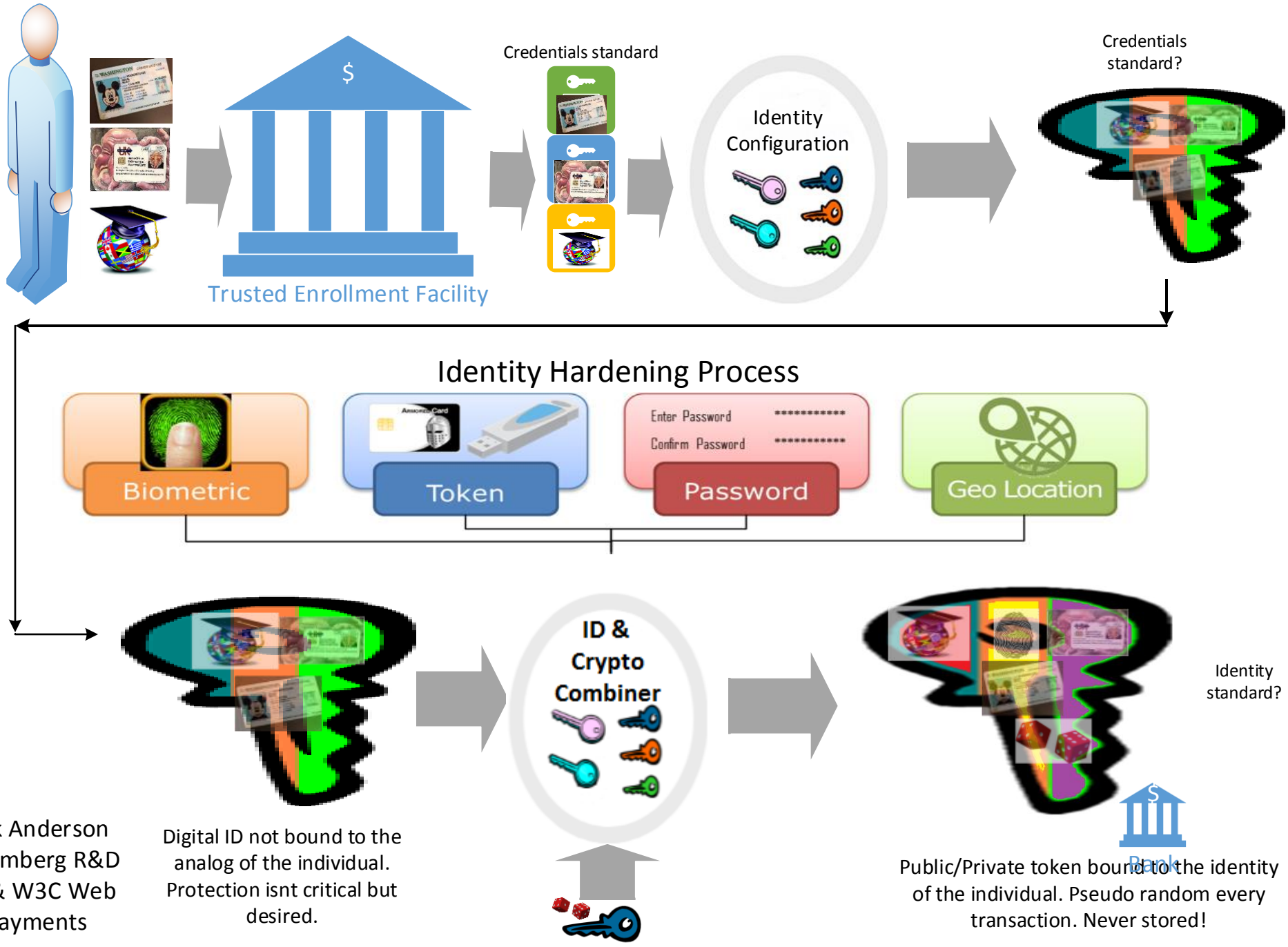


Erik Anderson
Bloomberg, X9 & W3C
Web Payments



Privacy Respecting Identity Management

Random Identity every transaction with permissioned mathematical forensics



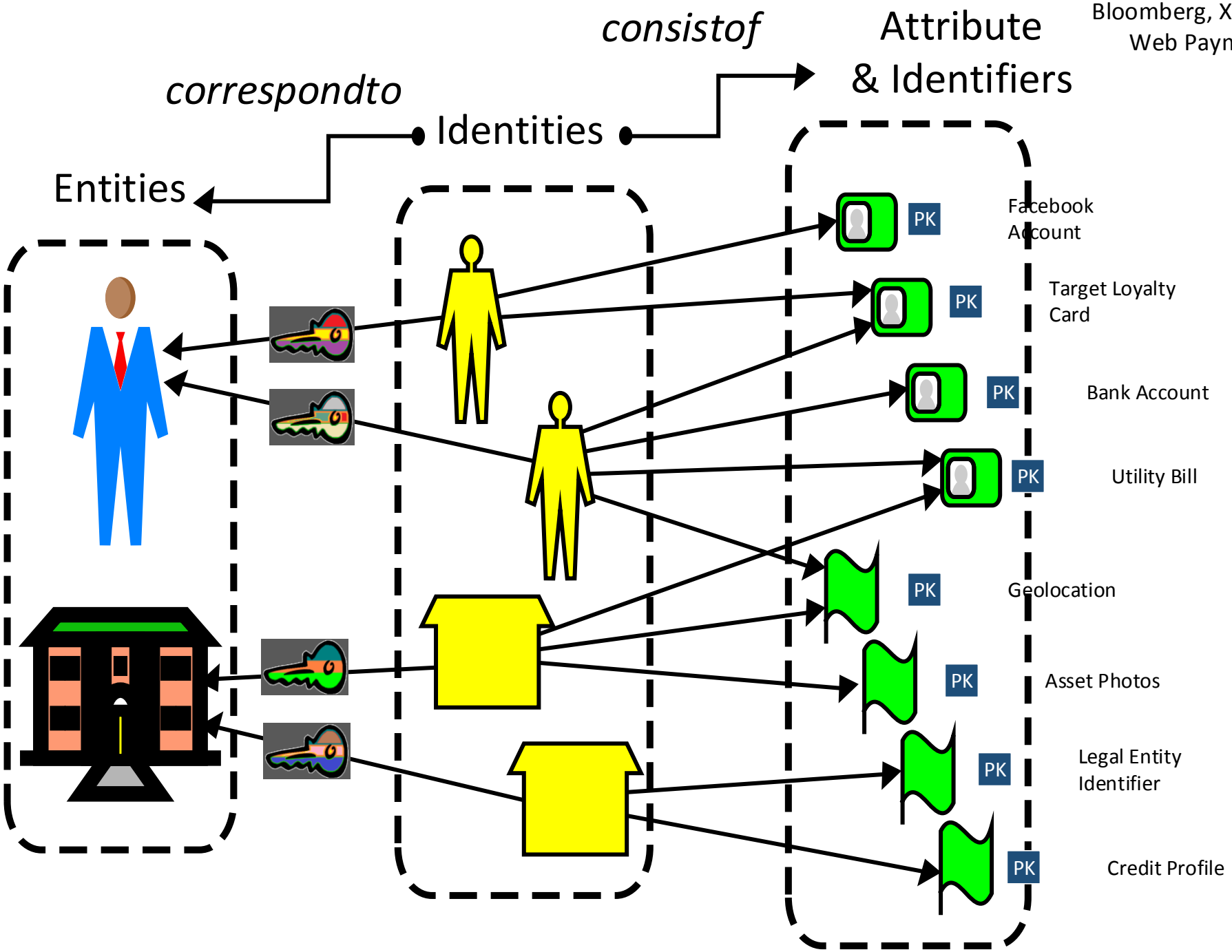
Erik Anderson
Bloomberg R&D
X9 & W3C Web Payments

Digital ID not bound to the analog of the individual. Protection isnt critical but desired.

Public/Private token bound to the identity of the individual. Pseudo random every transaction. Never stored!

Many Different Identities

Erik Anderson
Bloomberg, X9 & W3C
Web Payments



Identity Provider (IdP) Key Construction & Materials

Erik Anderson
Bloomberg, X9 & W3C
Web Payments

Identity Provider feeds the Asymmetric keying materials (Domain Values)

- Regulatory & Compliance Roles
- Legal/Law Enforcement Roles
- Employee Roles
- Biometric Template Hash
  - Facial Thermography
  - Finger Template
  - Voice Template
  - etc
- Hardware Token Serial Numbers

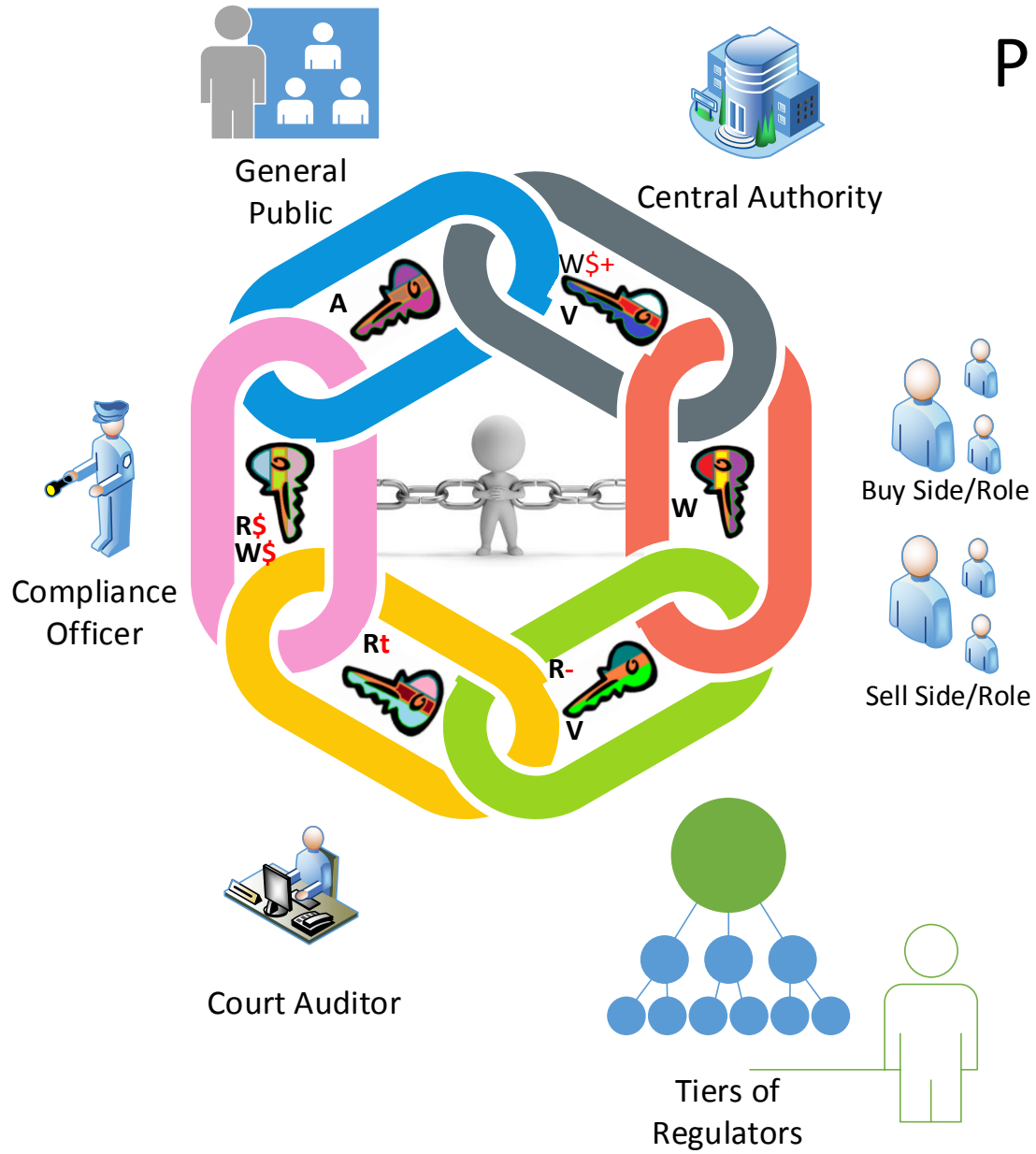
- Block Ciphers: AES,ARIA,CAMELLIA,SEED,TDES,BLOWFISH,XTEA
- Modes: ECB,CBC,CFB8,CFBfull,OFB,CTR,CMAC,CCM,GCM,XTS
- Digests: MD5,SHA1,SHA224/256/384/512,SHA3-224/256/384/512/RIPE-MD160
- Asymmetric: RSA 1024/2048/3072, Diffie-Hellman 1024/2048/3072
- DSA 1024/2048/3072,EC-CDH P256/P384/P521,ECDSA P256/P384/P521
- Random Number: FIPS 186-3 A.1.1.2,FIPS 186-3 A.1.2.1,FIPS 186-3 B.3.3,FIPS 186-3 B.3.4,FIPS 186-3 B.3.5,FIPS 186-3 B.3.6, X9.31
- Key Agree/Transport: RSASVE,RSA-OAEP,RSA-KEM_KAS,RSA-KAS1,RSA-KAS2,KTS-OAEP,KTS-KEM-KWS,KAS
- Signature Types: RSA-X9.31,RSA-PKCS,RSA-PSS,DSA,ECDSA

Cryptographic Enforced Data Permission Matix (ie RISK vs Security)

Unique Symmetric Working key for

- every message/chat
- message elements
- database field
- financial transaction
- different data fields
- Need to Know basis

Role Based Permissioned Public Blockchain&Ledger



A = Anonymous. Can see the transactions but no details.

W = Write access to the Blockchain

R- = Requests permission to read a transaction details.

Rt = Time based access to read all transaction details (Firm based). Times out after xx time.

R = Full read access (Allows regulatory snooping). Role based for a firm's transactions.

R$ = Can read all of its firms transaction & details.

W$ = Can countersign all of its firms transactions.

W$+ = Can countersign any transactions (or classification of transactions)

R$- = Can read all transactions (or a category of transactions)

V = Can validate an asset all the way back to its roots but cannot see the details of a transaction.

Erik Anderson
Bloomberg, X9 & W3C
Web Payments