On building trustworthy decentralized infrastructure: Experiences from the BlockChain I/O project

Anwitaman DATTA

De Montfort University, Leicester, UK

Nanyang Technological University, Singapore (on leave)

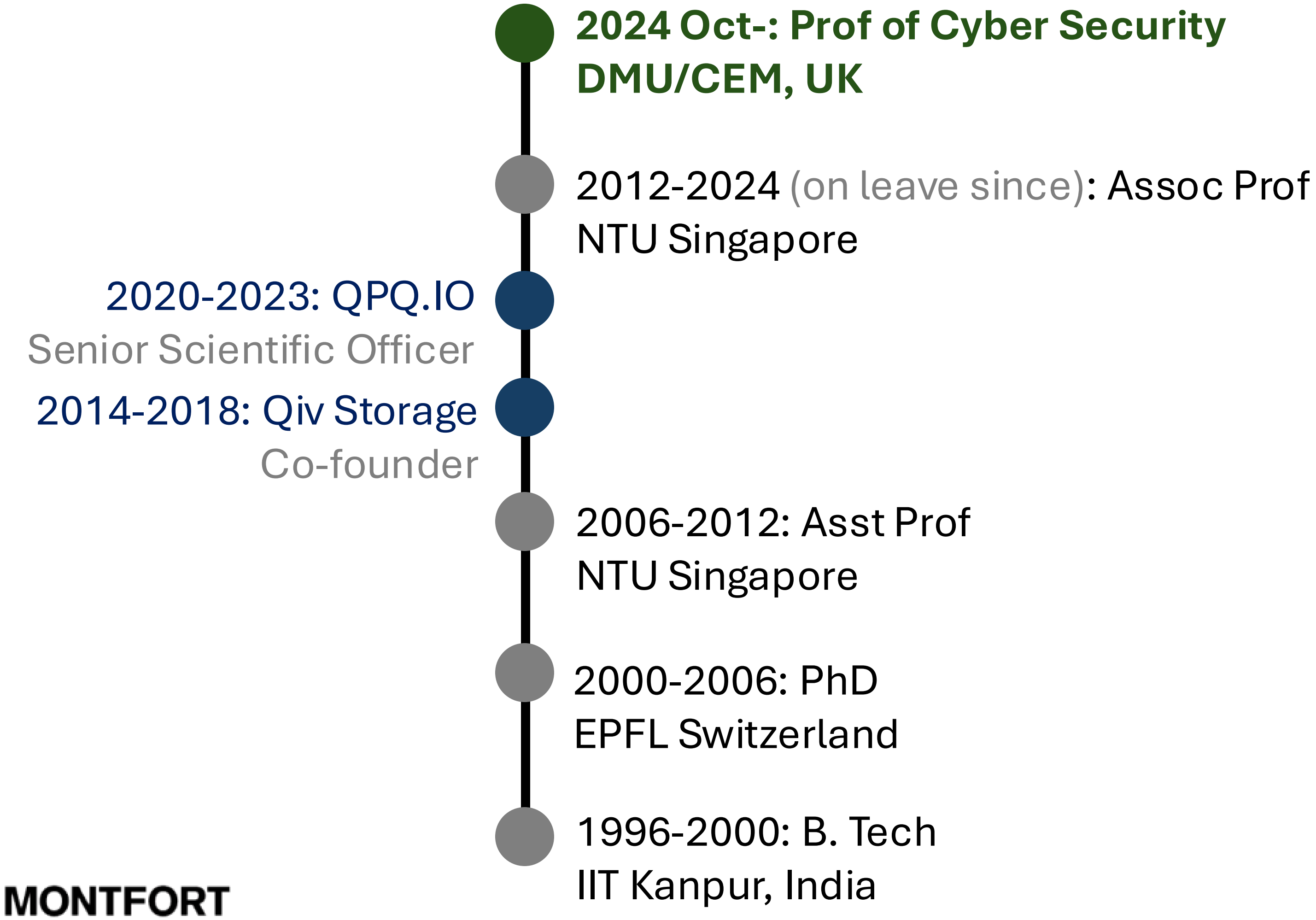
Work done with (and thanks to) members of my team and collaborators:

J. Zhang, D. Reijsbergen, S. Majumder, TTA Dinh

ABOUT ME

Anwitaman DATTA

Professor of Cyber Security, De Montfort University
Anwitaman.Datta@DMU.AC.UK



2024 Oct-: Prof of Cyber Security
DMU/CEM, UK

2012-2024 (on leave since): Assoc Prof
NTU Singapore

2020-2023: QPQ.IO
Senior Scientific Officer

2014-2018: Qiv Storage
Co-founder

2006-2012: Asst Prof
NTU Singapore

2000-2006: PhD
EPFL Switzerland

1996-2000: B. Tech
IIT Kanpur, India

RESEARCH (a bird's eye view)

- Cyber security
  - Data Privacy & Governance
  - Privacy Enhancing Technologies
  - Risk Management & Transfer
- Data science
  - Graph algorithms & applications
  - NLP applications
- Distributed systems
  - Decentralization
  - Self-organization
  - Reliability & Resilience
  - Scalability
  - Distributed Ledgers
- Socio-technological systems

Talking Points

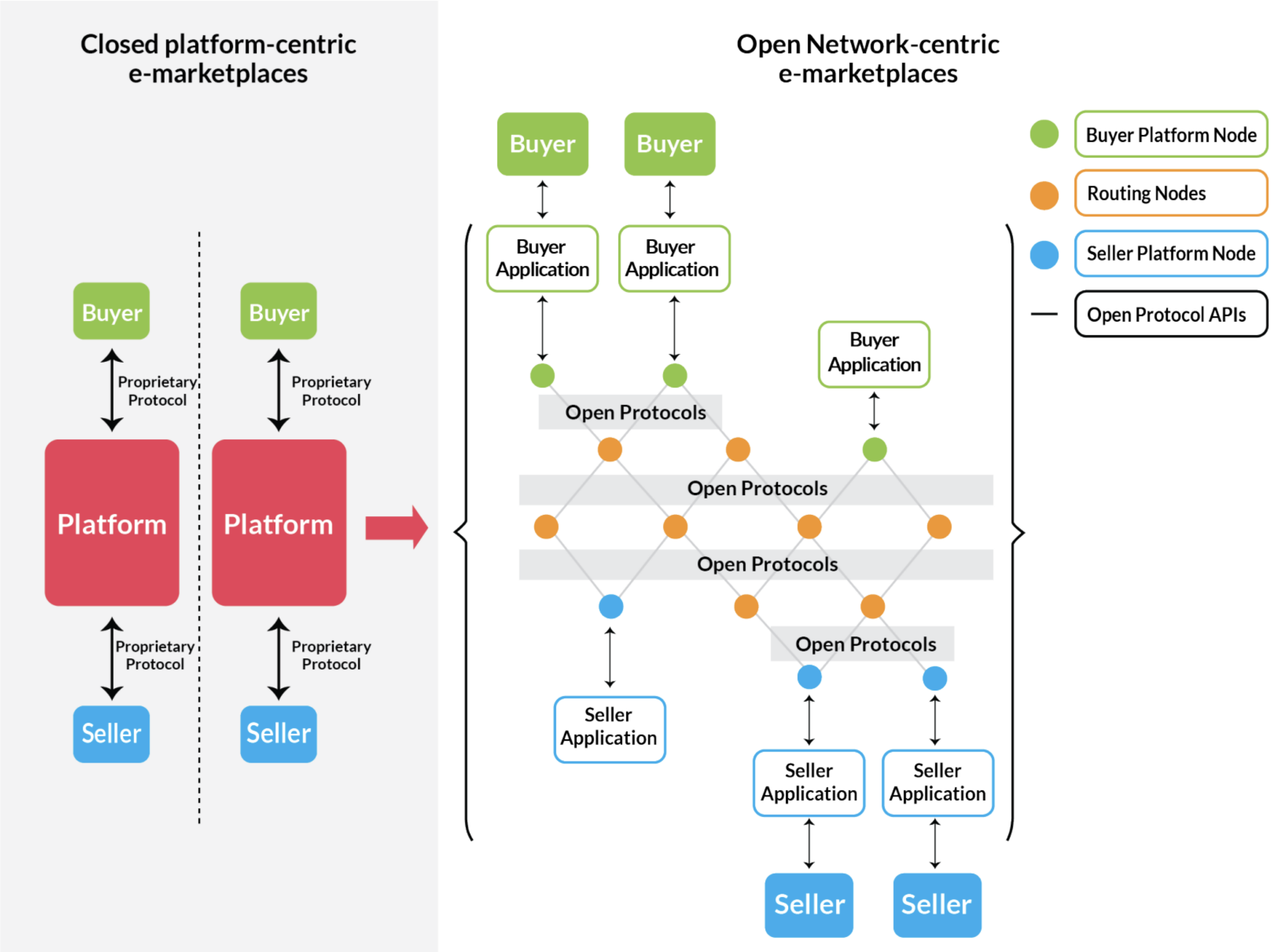
TAKE AWAY

- Interoperable blockchains for a decentralized, trustworthy infrastructure
  - Cryptographic primitives
    - Atomic swaps with Hashed Time Lock Contracts
    - Self-Sovereign Identities
      - Associated privacy benefits
    - Fine-grained (~role based) access control
  - Commerce/DeFi
    - Applications over multiple interoperable blockchains
    - Multi-chain cryptocurrency collateralized stable-coins
    - Global reputation aggregation

Disclaimers & Acknowledgements

- Thrust of the talk is on the what, not the how
- The presented body of work was funded by Ministry of Education (Singapore) through Tier-2 grant, and they were carried out at NTU Singapore
- Some of the work leverage directly or extend third party innovations and artefacts

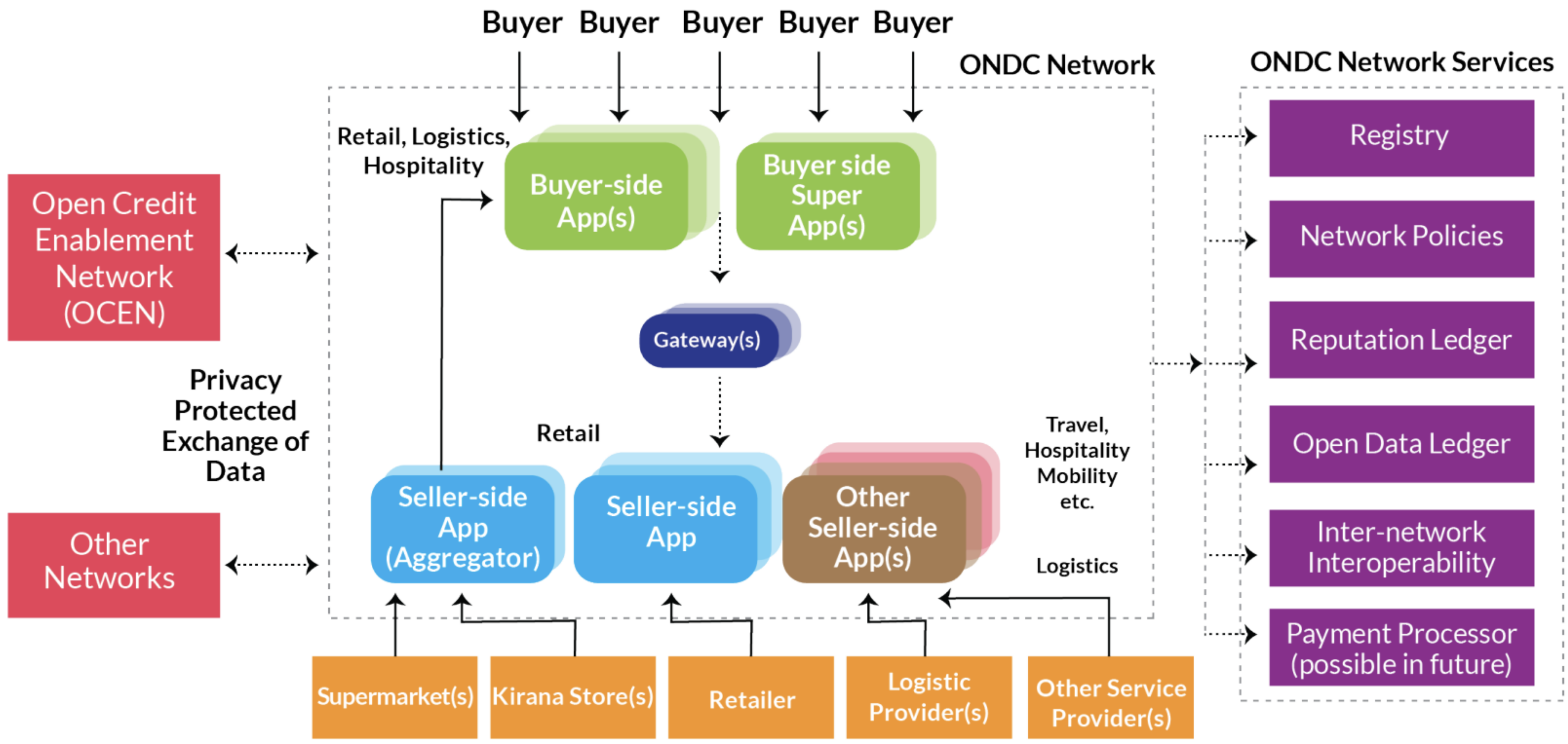
Background/inspirations: ONDC vision paper



Source: https://ondc.org/

Open Network for Digital Commerce

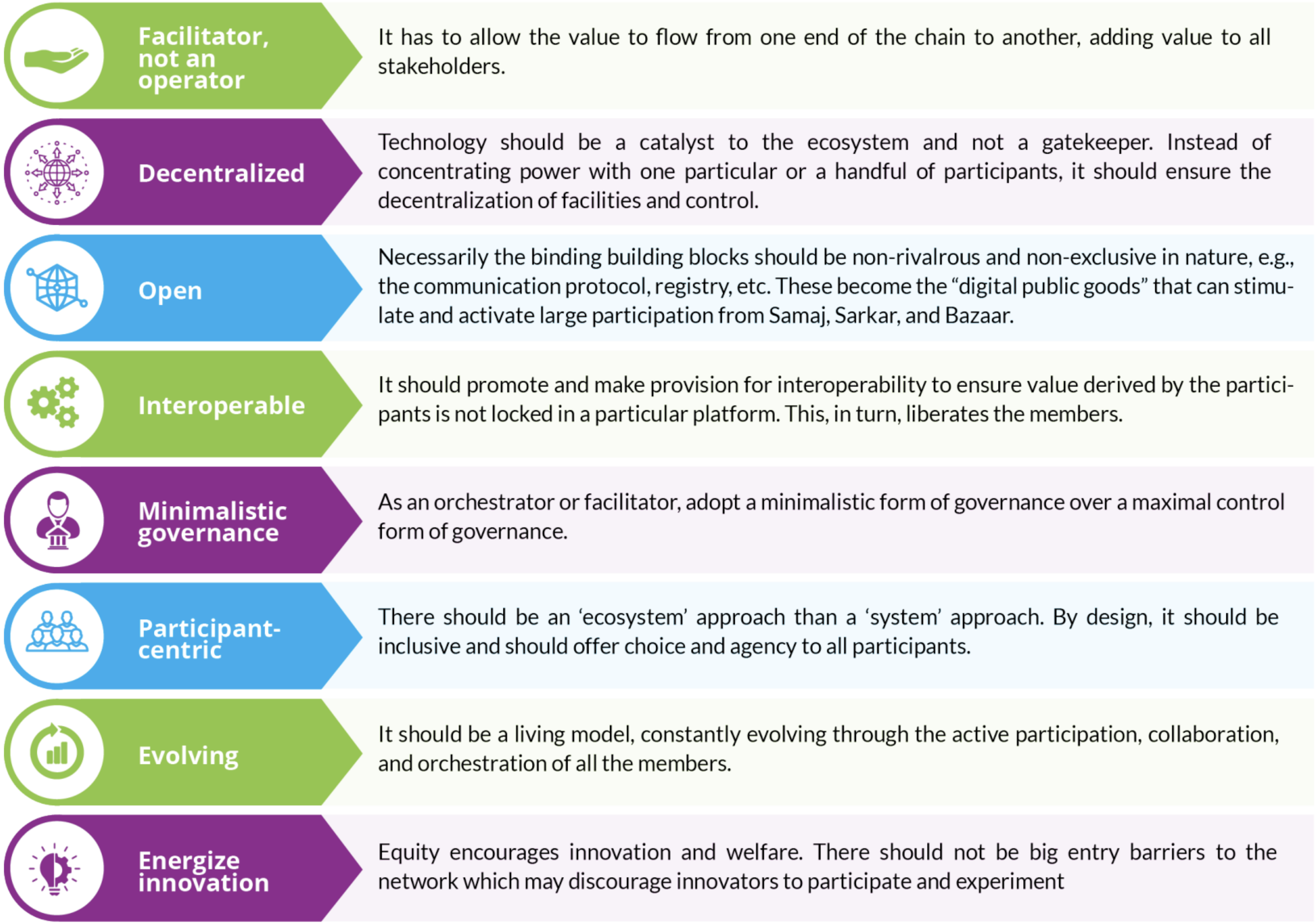
Background/inspirations: ONDC vision paper



Source: https://ondc.org/

Background/inspirations: ONDC vision paper

INDIA'S ONDC



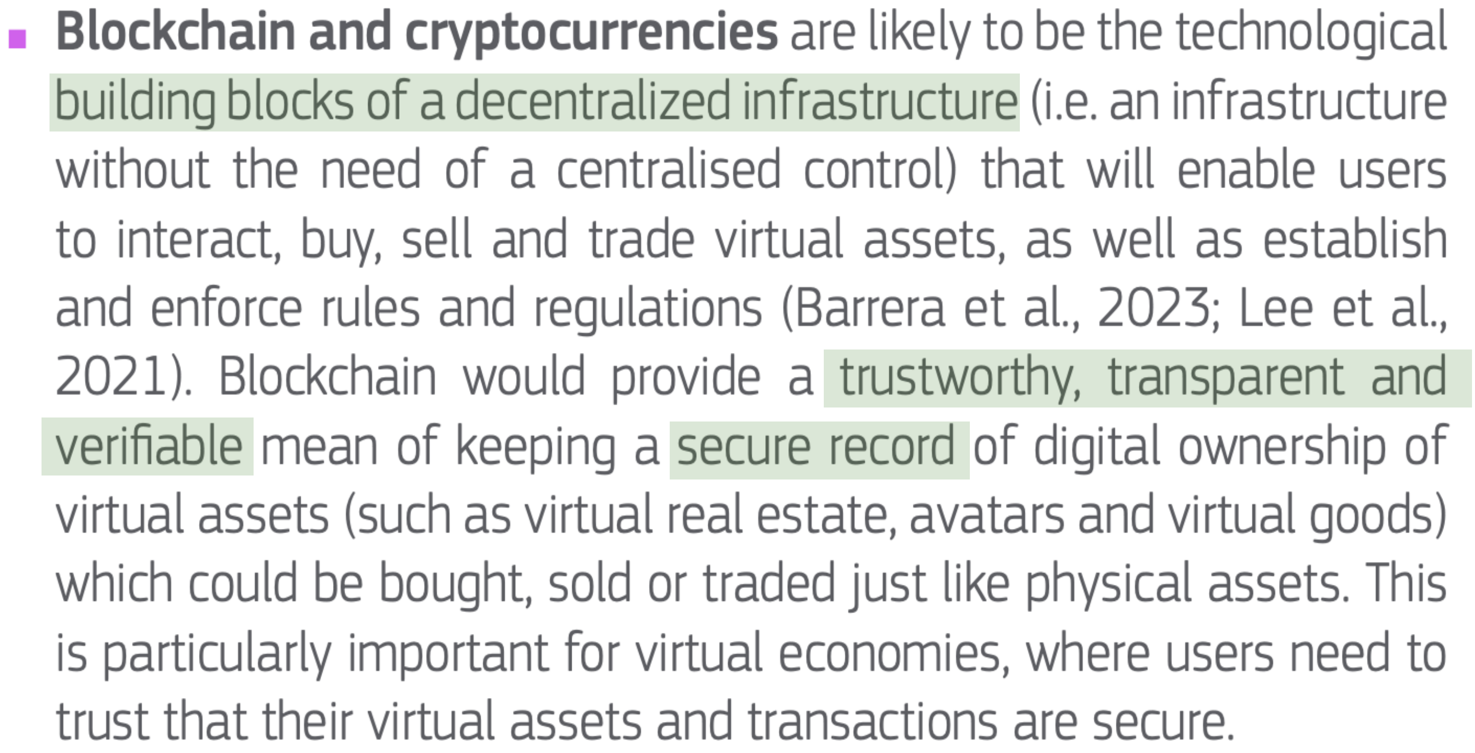
Facilitator, not an operator	It has to allow the value to flow from one end of the chain to another, adding value to all stakeholders.
Decentralized	Technology should be a catalyst to the ecosystem and not a gatekeeper. Instead of concentrating power with one particular or a handful of participants, it should ensure the decentralization of facilities and control.
Open	Necessarily the binding building blocks should be non-rivalrous and non-exclusive in nature, e.g., the communication protocol, registry, etc. These become the "digital public goods" that can stimulate and activate large participation from Samaj, Sarkar, and Bazaar.
Interoperable	It should promote and make provision for interoperability to ensure value derived by the participants is not locked in a particular platform. This, in turn, liberates the members.
Minimalistic governance	As an orchestrator or facilitator, adopt a minimalistic form of governance over a maximal control form of governance.
Participant-centric	There should be an 'ecosystem' approach than a 'system' approach. By design, it should be inclusive and should offer choice and agency to all participants.
Evolving	It should be a living model, constantly evolving through the active participation, collaboration, and orchestration of all the members.
Energize innovation	Equity encourages innovation and welfare. There should not be big entry barriers to the network which may discourage innovators to participate and experiment

Source: https://ondc.org/

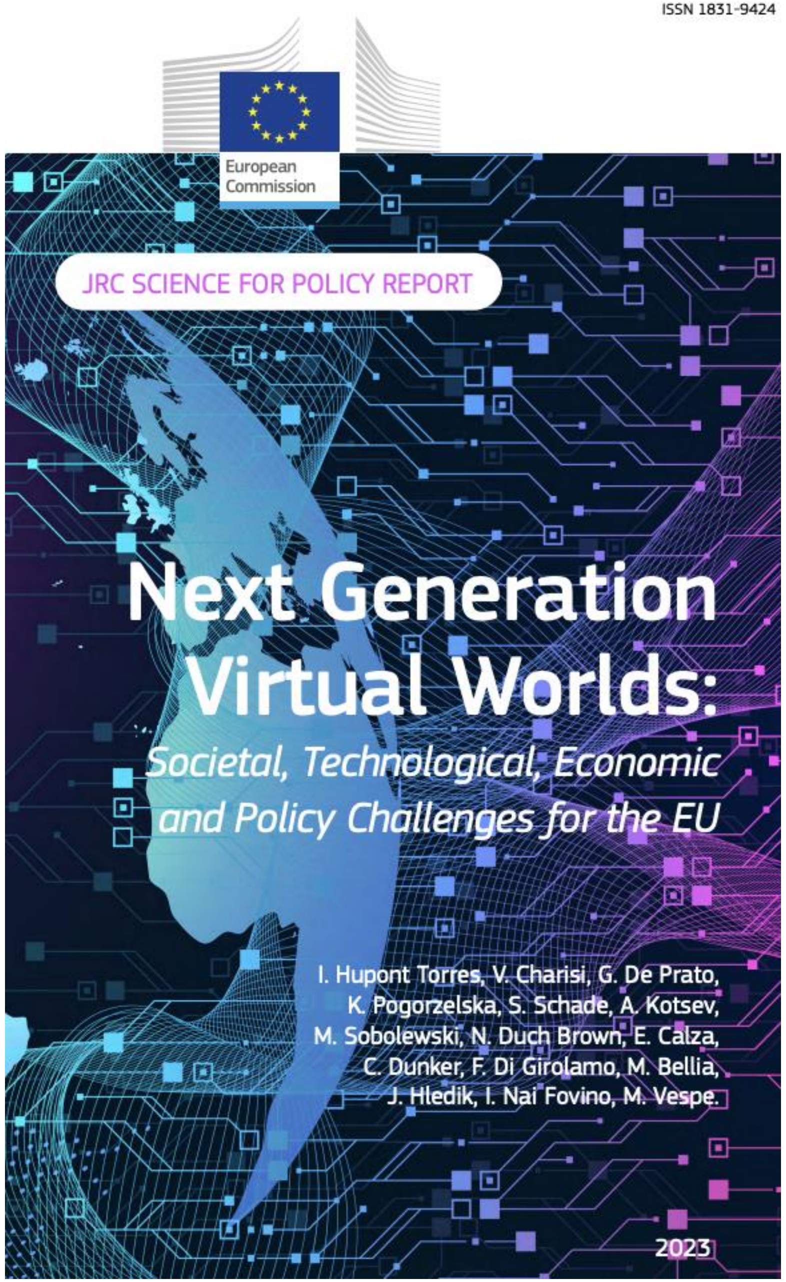
ONDC
Open Network for Digital Commerce

Background/inspirations: Web 4.0

EU STRATEGY PAPER



- **Blockchain and cryptocurrencies** are likely to be the technological building blocks of a decentralized infrastructure (i.e. an infrastructure without the need of a centralised control) that will enable users to interact, buy, sell and trade virtual assets, as well as establish and enforce rules and regulations (Barrera et al., 2023; Lee et al., 2021). Blockchain would provide a trustworthy, transparent and verifiable mean of keeping a secure record of digital ownership of virtual assets (such as virtual real estate, avatars and virtual goods) which could be bought, sold or traded just like physical assets. This is particularly important for virtual economies, where users need to trust that their virtual assets and transactions are secure.



ISSN 1831-9424

European Commission

JRC SCIENCE FOR POLICY REPORT

Next Generation Virtual Worlds:

Societal, Technological, Economic and Policy Challenges for the EU

I. Hupont Torres, V. Charisi, G. De Prato, K. Pogorzelska, S. Schade, A. Kotsev, M. Sobolewski, N. Duch Brown, E. Calza, C. Dunker, F. Di Girolamo, M. Bellia, J. Hledik, I. Nai Fovino, M. Vespe.

2023

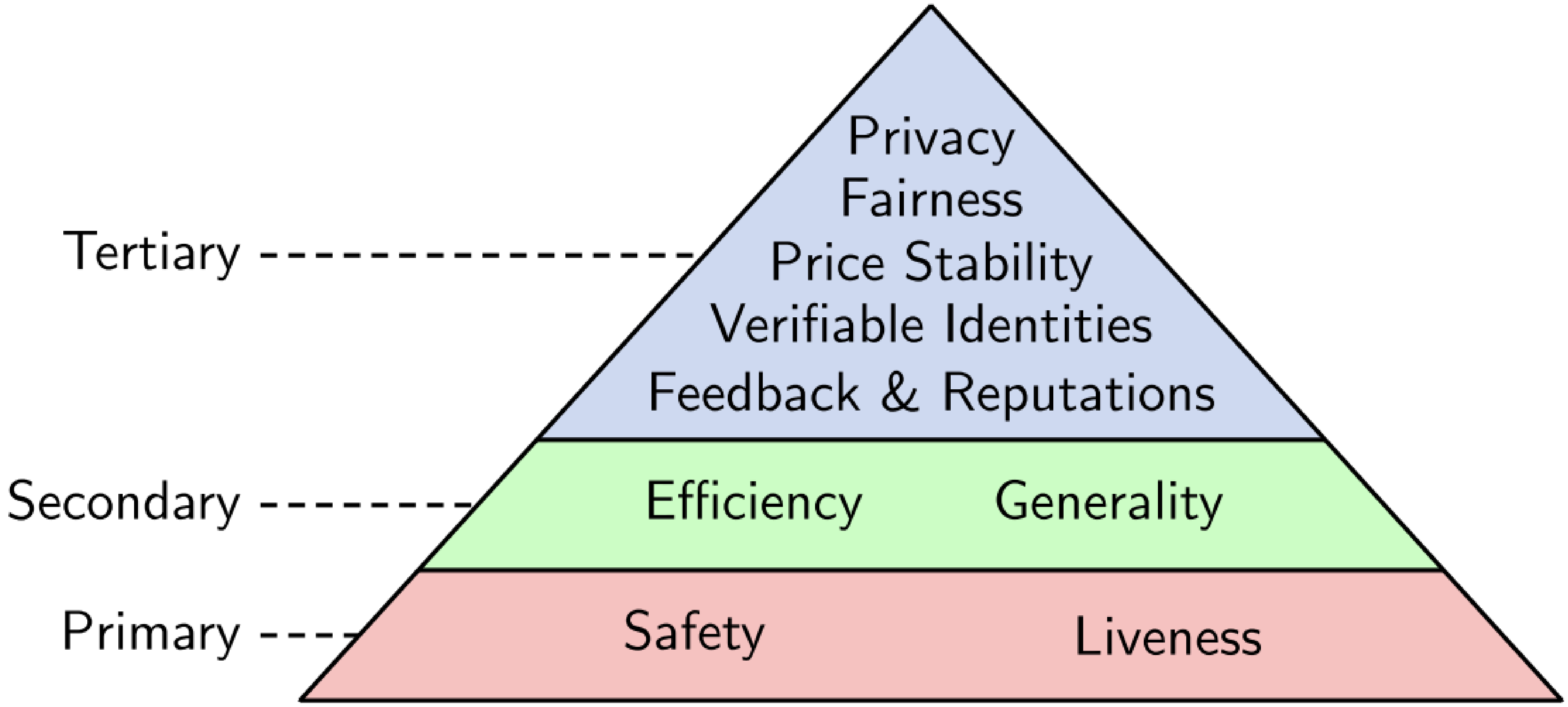
Ref: https://publications.jrc.ec.europa.eu/repository/handle/JRC133757

Background: Blockchains

- Blockchains
  - Tamper-evident decentralized data structure
    - Immutability
    - Verifiability of records
  - Secure token transfers
  - Contracts as self-executing codes
- Silos
  - Native design of blockchain assumes operating in isolation
  - Independent decentralized digital marketplaces

Hierarchy of Needs

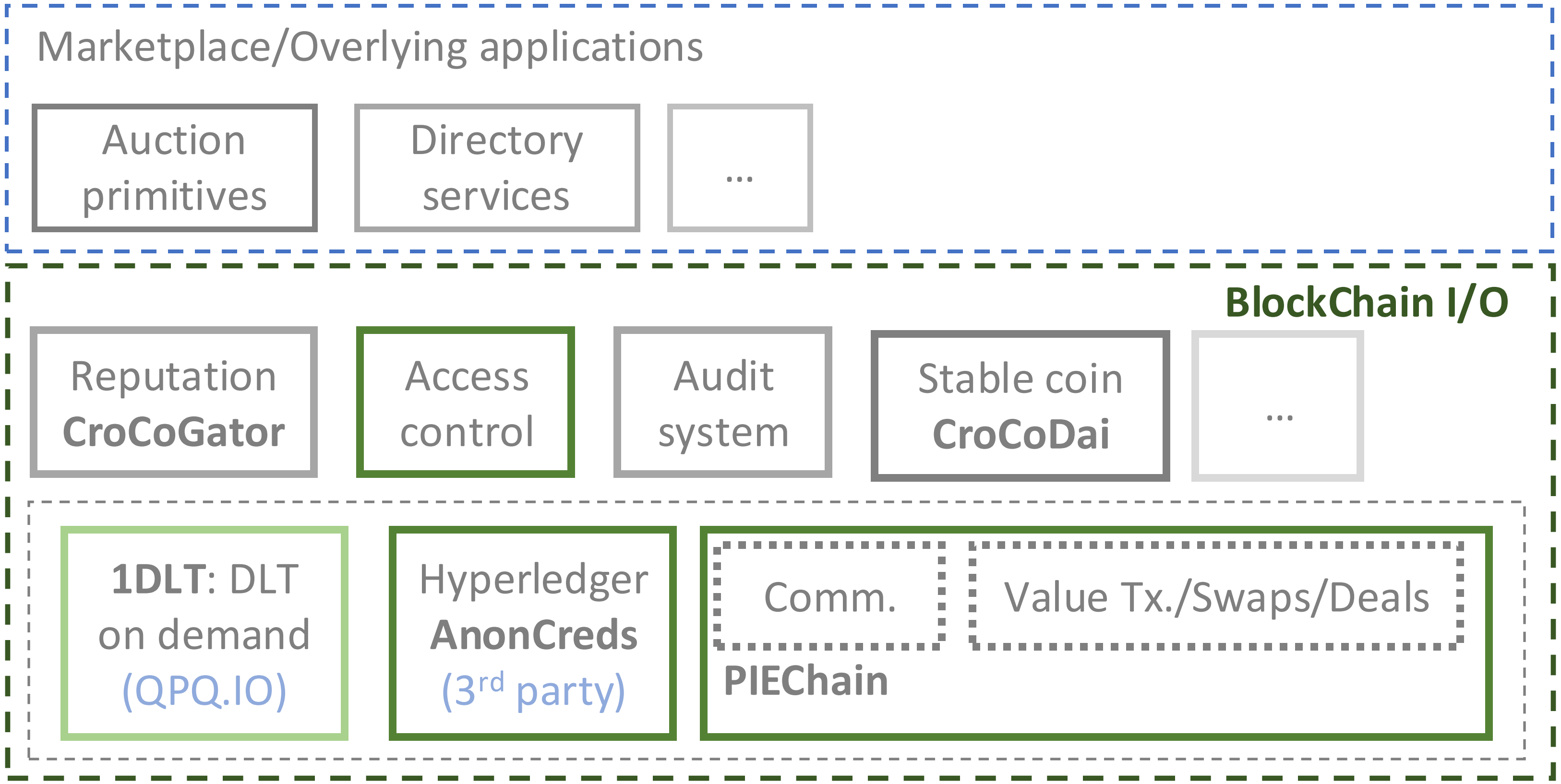
- Desiderata for a trustworthy decentralized (commerce) infrastructure



The work on BlockChain I/O was supported by the Ministry of Education (MOE) Singapore's Tier 2 Grant

MODULAR ARCHITECTURE

Blockchain I/O



Marketplace/Overlying applications

Auction primitives

Directory services

…

BlockChain I/O

Reputation **CroCoGator**

Access control

Audit system

Stable coin **CroCoDai**

…

1DLT: DLT on demand (QPQ.IO)

Hyperledger **AnonCreds** (3rd party)

Comm.

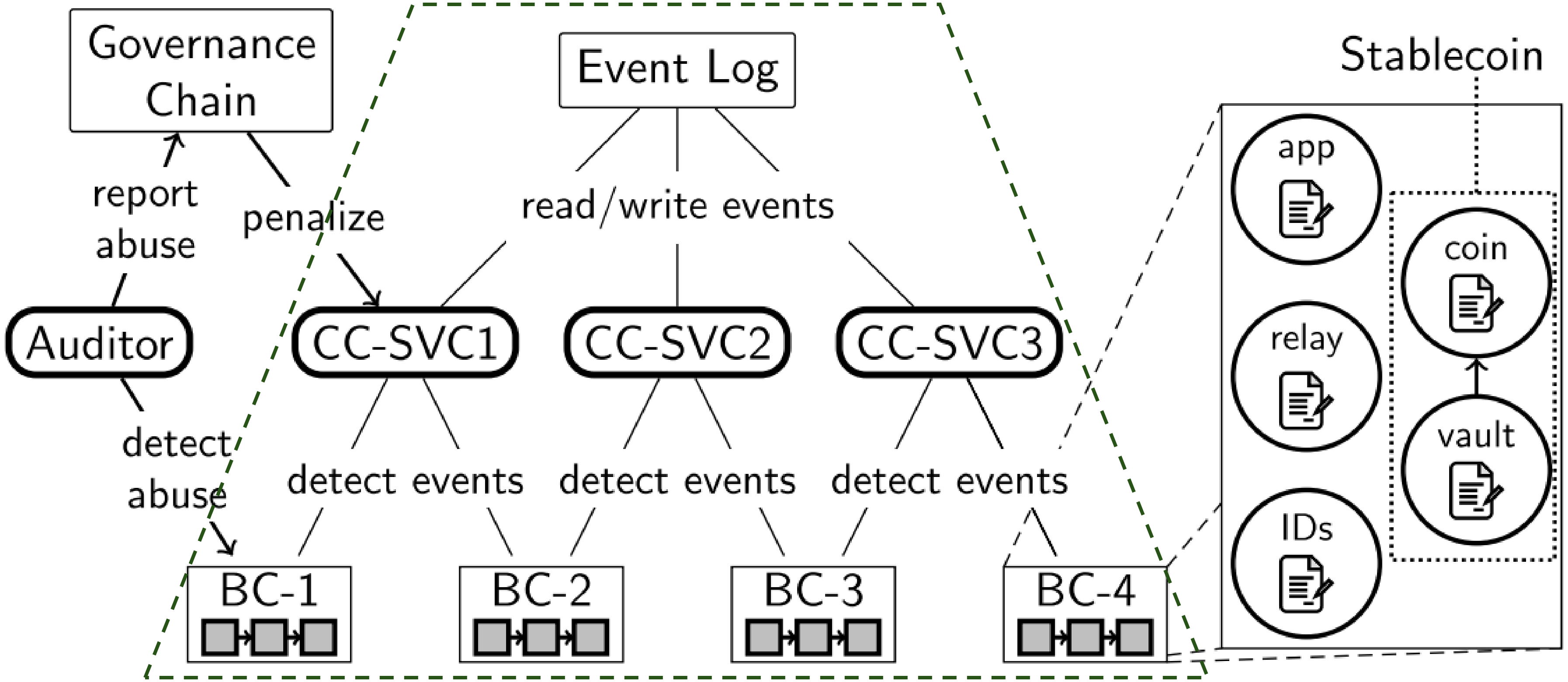
Value Tx./Swaps/Deals

PIEChain

BlockChain I/O core tech stack + publications:

- Putting PIEChain, AnonCreds & CroCoDai together: IEEE Access 2024
- PIEChain: Demonstrated at ICDCS 2023
- CroCoDai: ACM DLT 2024, some further extension/optimization: MARBLE 2024
- AnonCreds: 3rd party technology (Hyperledger)
- 1DLT: Tokenomics 2022 (built at QPQ.IO)
- Data governance/confidential data sharing: TrustCom 2024, PeerJ 2024
- Multi-chain reputation aggregation: Under review

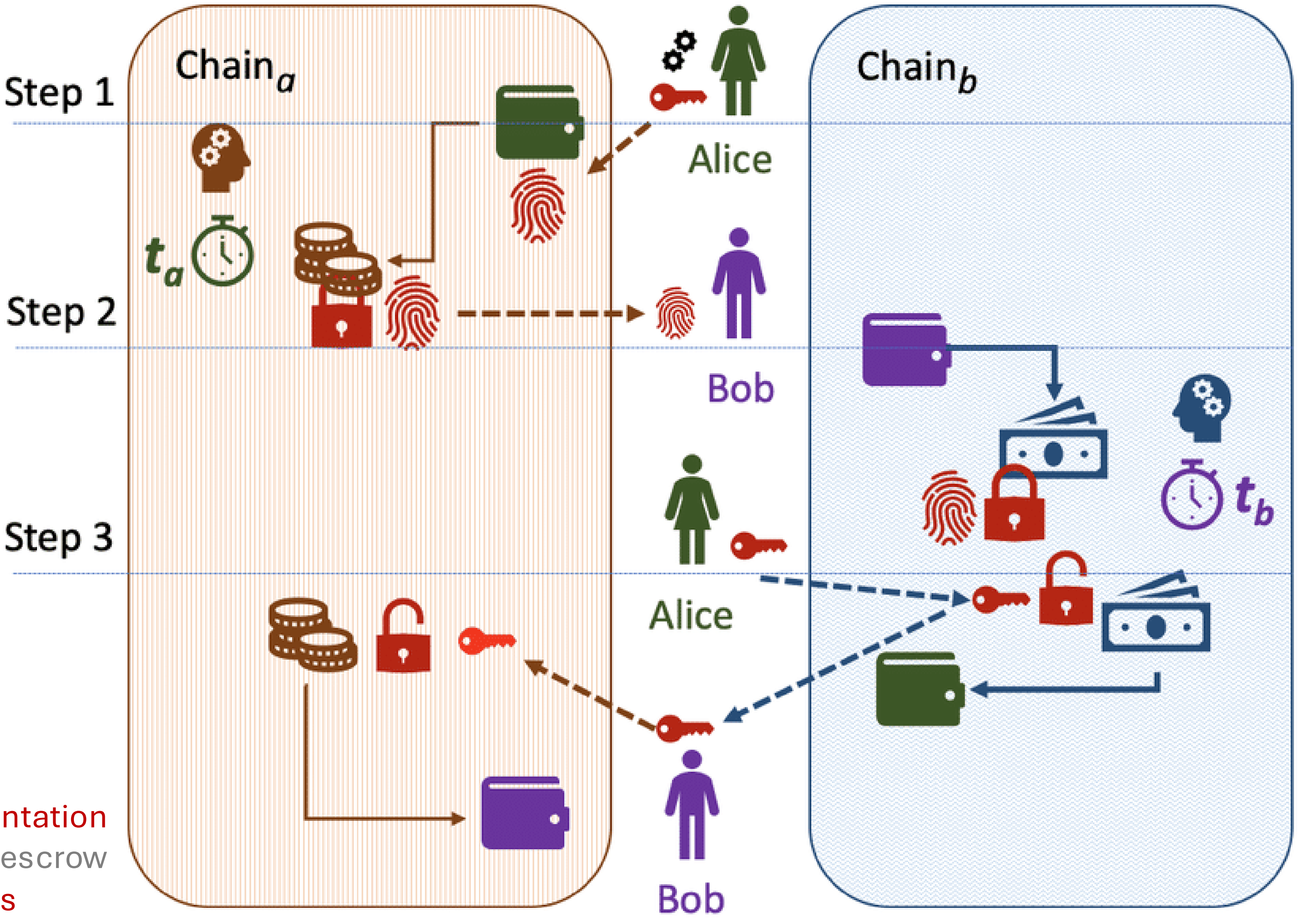
Blockchain I/O internals



Decoupled Communication & Transaction

- Interactions through Cross-Chain Services CC-SVCs (Kafka based)
  - Reputation system to prevent CC-SVCs abuse
- Transaction semantics: Escrows (Cross-chain deals)
- Value volatility mitigation: Stablecoin (CroCoDAI)

Hashed Time Lock Contract

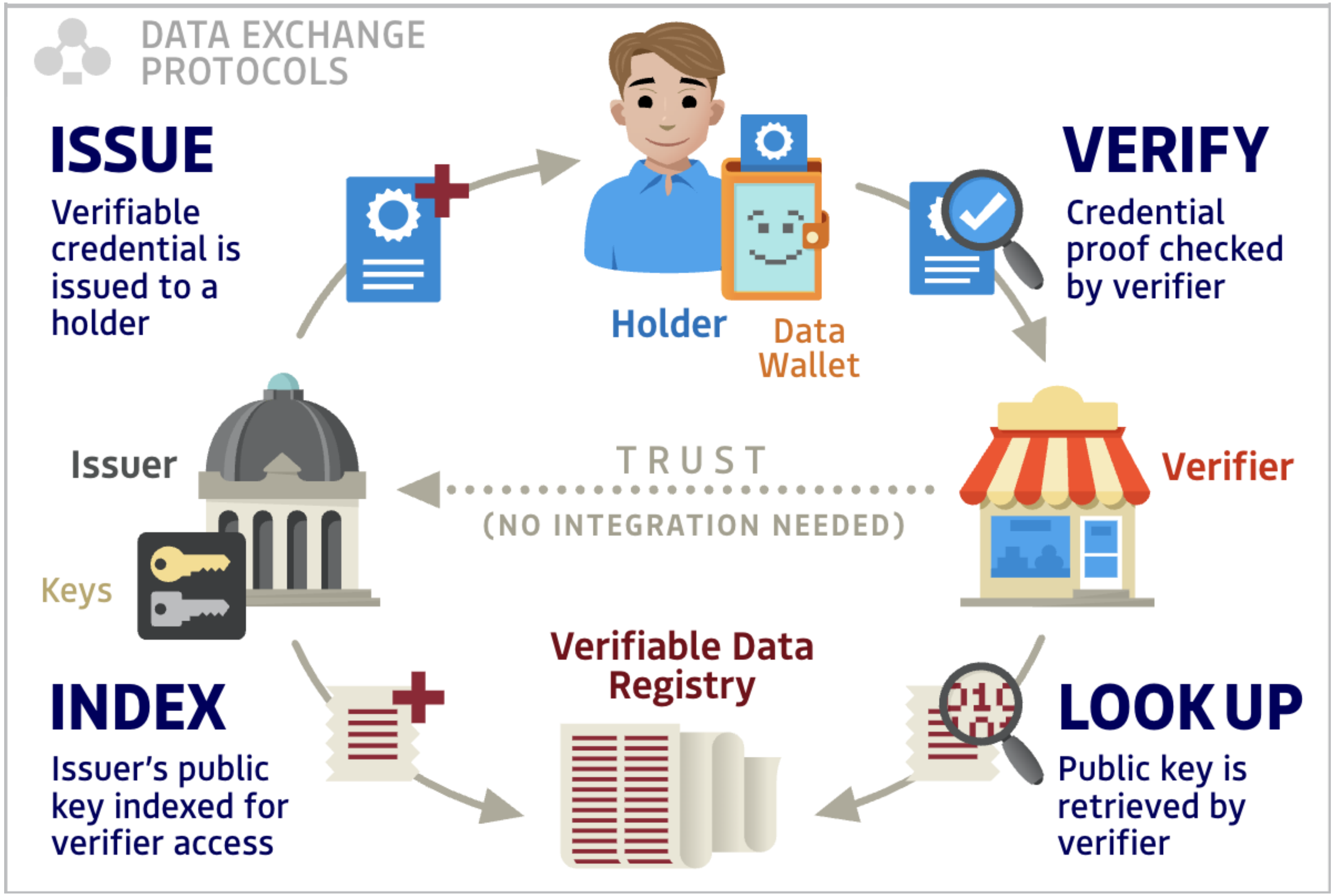


Note: BlockChain I/O implementation supports a more sophisticated escrow variant known as Cross-chain deals

Image source: A Game-Theoretic Analysis of Cross-Chain Atomic Swaps with HTLCs, Xu et al.

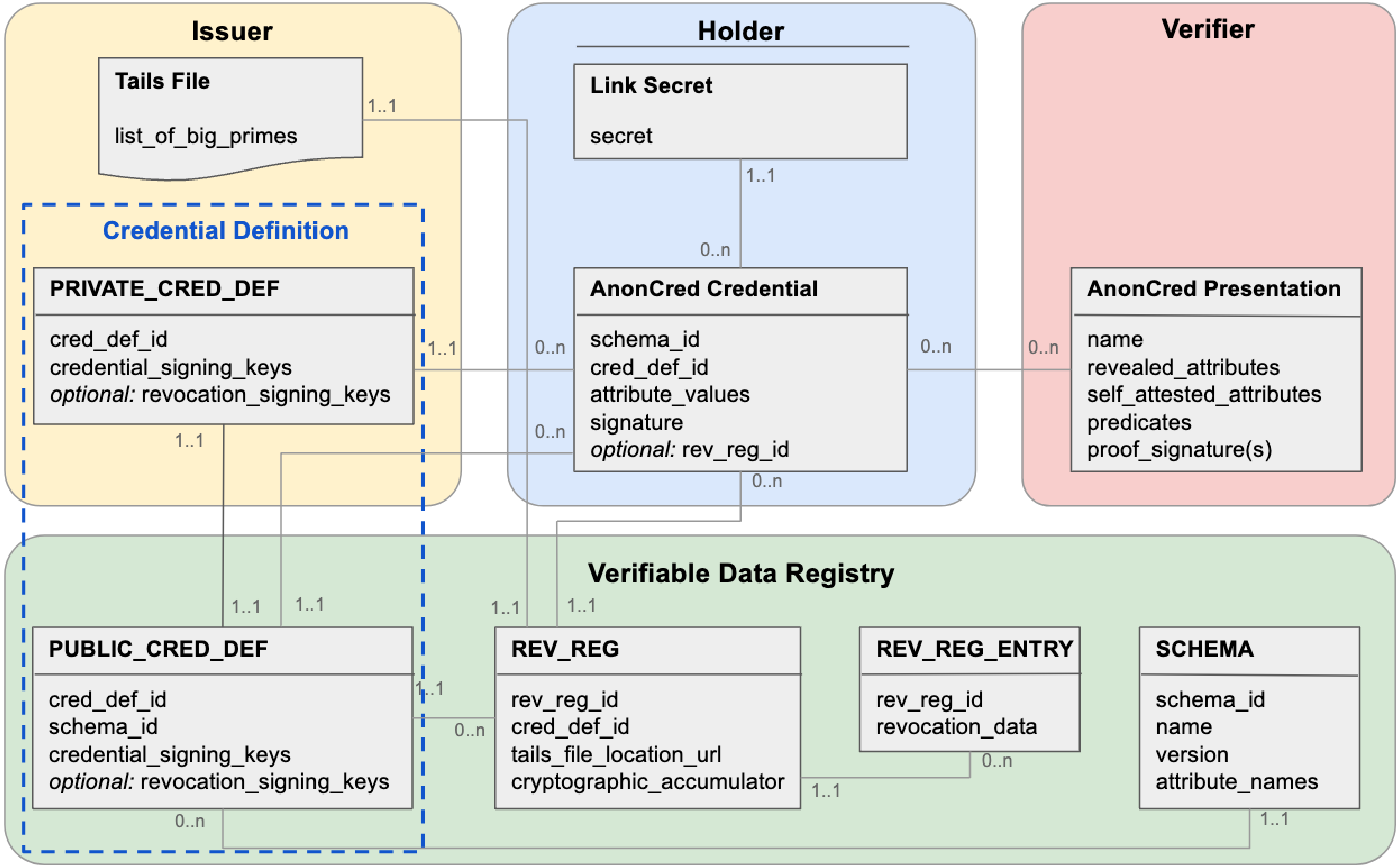
Self-Sovereign Identity

TRUST TRIANGLE


DATA EXCHANGE PROTOCOLS
ISSUE
Verifiable credential is issued to a holder
Holder
Data Wallet
VERIFY
Credential proof checked by verifier
Issuer
Keys
TRUST
(NO INTEGRATION NEEDED)
Verifier
INDEX
Issuer's public key indexed for verifier access
Verifiable Data Registry
LOOK UP
Public key is retrieved by verifier
010

Ref: https://trustoverip.org/wp-content/toip-model/

AnonCreds



Issuer

Tails File
list_of_big_primes

Credential Definition

PRIVATE_CRED_DEF
cred_def_id
credential_signing_keys
optional: revocation_signing_keys

Holder

Link Secret
secret

AnonCred Credential
schema_id
cred_def_id
attribute_values
signature
optional: rev_reg_id

Verifier

AnonCred Presentation
name
revealed_attributes
self_attested_attributes
predicates
proof_signature(s)

Verifiable Data Registry

PUBLIC_CRED_DEF
cred_def_id
schema_id
credential_signing_keys
optional: revocation_signing_keys

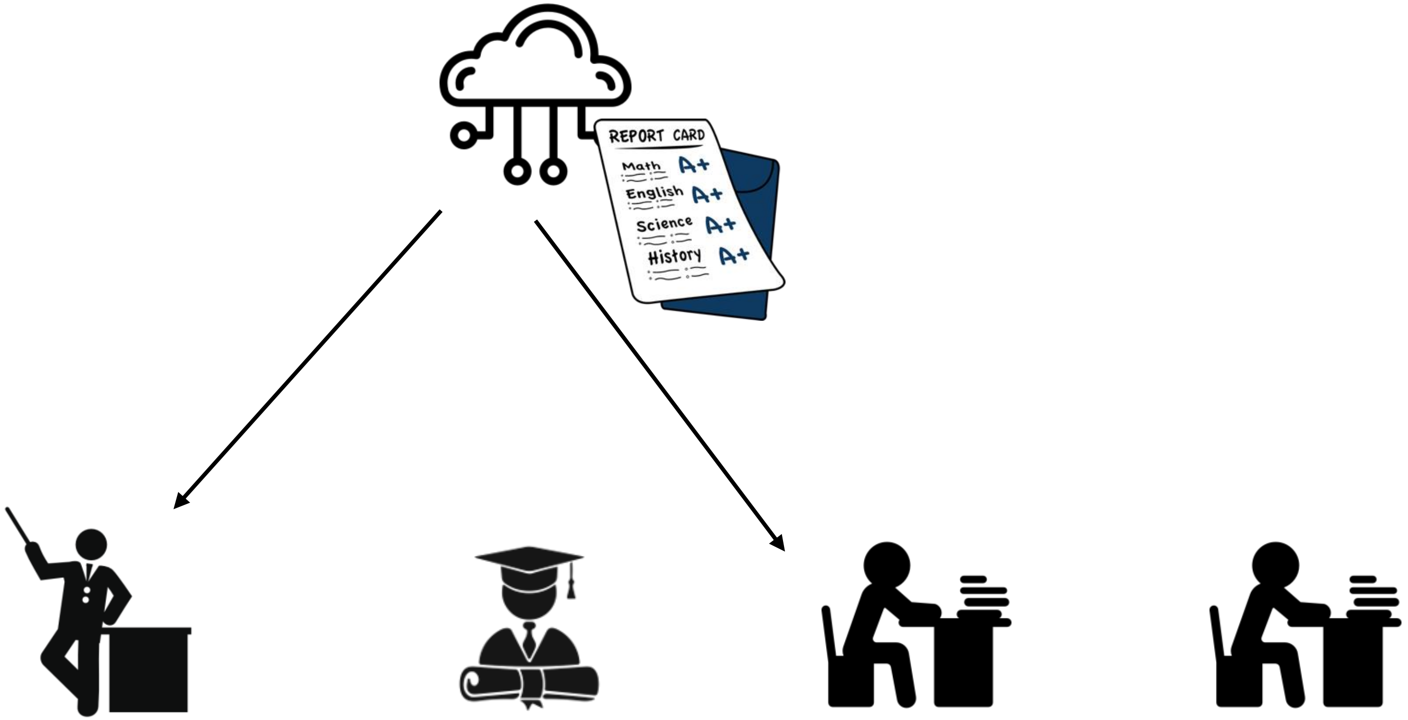
REV_REG
rev_reg_id
cred_def_id
tails_file_location_url
cryptographic_accumulator

REV_REG_ENTRY
rev_reg_id
revocation_data

SCHEMA
schema_id
name
version
attribute_names

Ref: https://hyperledger.github.io/anoncreds-spec/

Access Control



Prof,
Alice

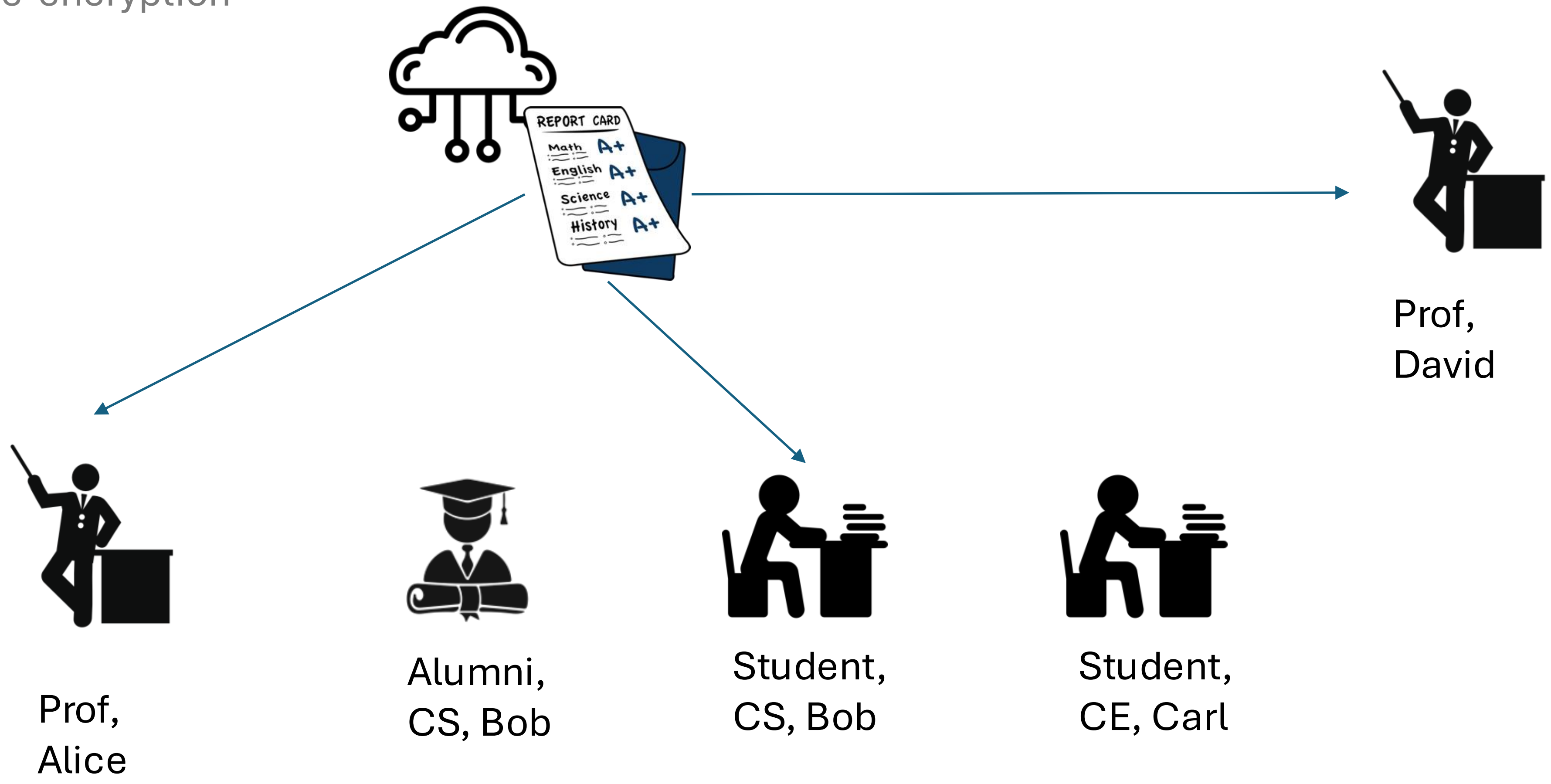
Alumni,
CS, Bob

Student,
CS, Bob

Student,
CE, Carl

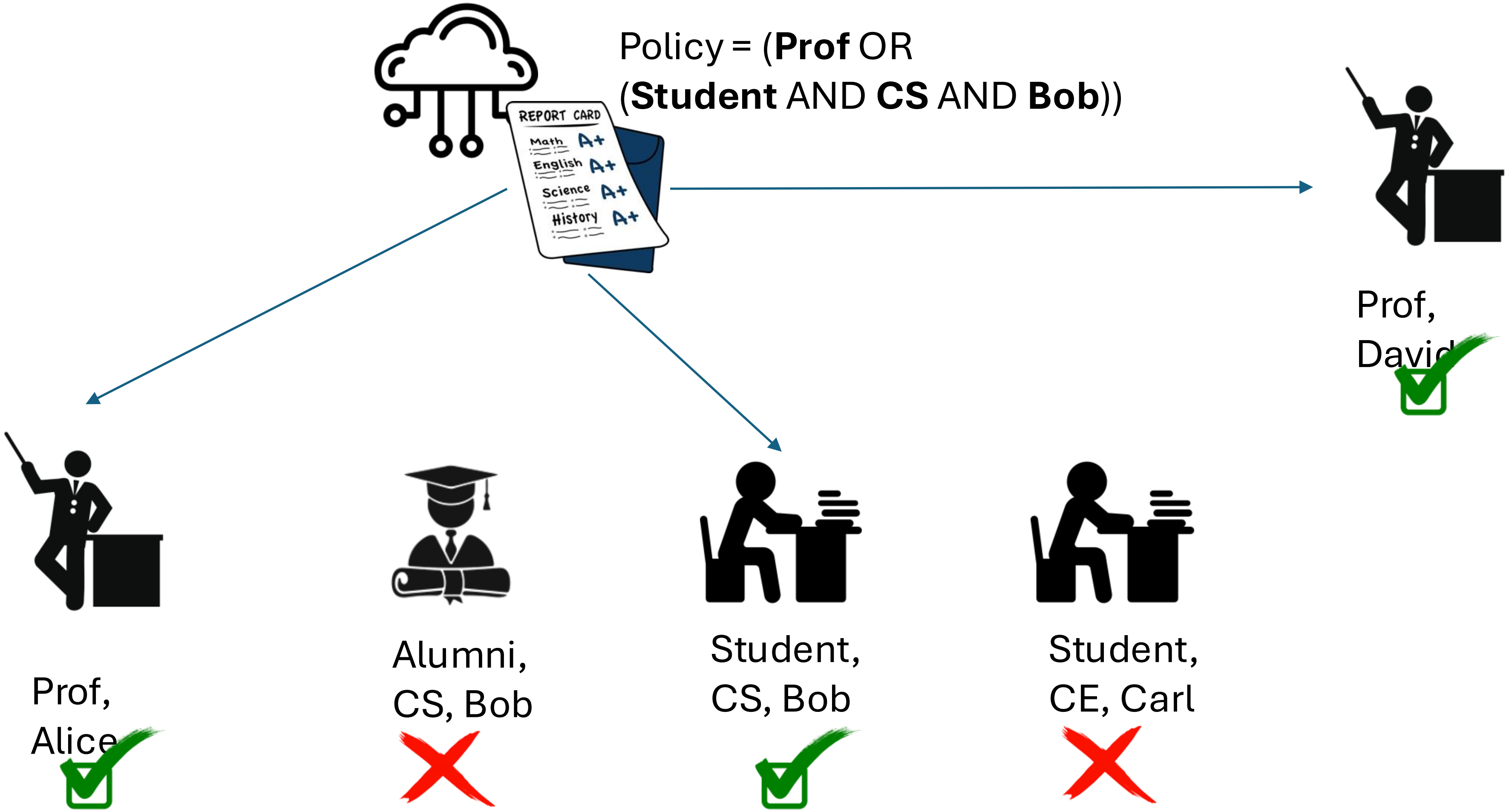
Fine-grained Control?

- Don’t scale well (on their own)
  - Symmetric key encryption
  - Public key cryptography
    - Proxy re-encryption



Fine-grained Control

- Attribute Base Encryption (ABE)



Policy = (**Prof** OR (**Student** AND **CS** AND **Bob**))

Fine-grained Control

- Cypher-text Attribute Base Encryption (CP-ABE)

  - Conceptually like traditional access control methods such as Role-Based Access Control.

  - A user is described by a set of descriptive attributes, and a corresponding private key is issued to the user by an authority.

  - During encryption, an encryptor associates an access policy over attributes with the ciphertext.

Bethencourt, John, Amit Sahai, and Brent Waters. "Ciphertext-Policy Attribute-Based Encryption." In *IEEE Symposium on Security and Privacy (**S&P 2007**)*, 321–34. Berkeley, CA: IEEE, 2007. https://doi.org/10.1109/SP.2007.11.

Fine-grained Control

- Multi-Authority Cypher-text Attribute Base Encryption (MA-CP-ABE)

  - It might not be realistic to have one single authority to manage all attributes.
    - ❖ E.g., an encryptor may want to share data with users who are computer science alumni of University X and currently working as an engineer for Company Y.
    - ❖ The access policy is P=UnivX.CS AND UnivX.ALU AND CompY.Engineer

  - Some practicality needs:
    - ❖ Different attribute domains are managed by different authorities.
    - ❖ Expressiveness, efficiency and security are not weaker than that of the single-authority CP-ABE
    - ❖ No authority can independently decrypt any ciphertext

Lewko, Allison, and Brent Waters. “Decentralizing Attribute-Based Encryption.” In *Advances in Cryptology – **EUROCRYPT 2011***, edited by Kenneth G. Paterson, 6632:568–88. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011. https://doi.org/10.1007/978-3-642-20465-4_31.

Fine-grained Control

- Multi-Authority Cypher-text Attribute Base Encryption (MA-CP-ABE) with Policy Hiding
    - individual authorities do not know the full set of attributes possessed by the recipient

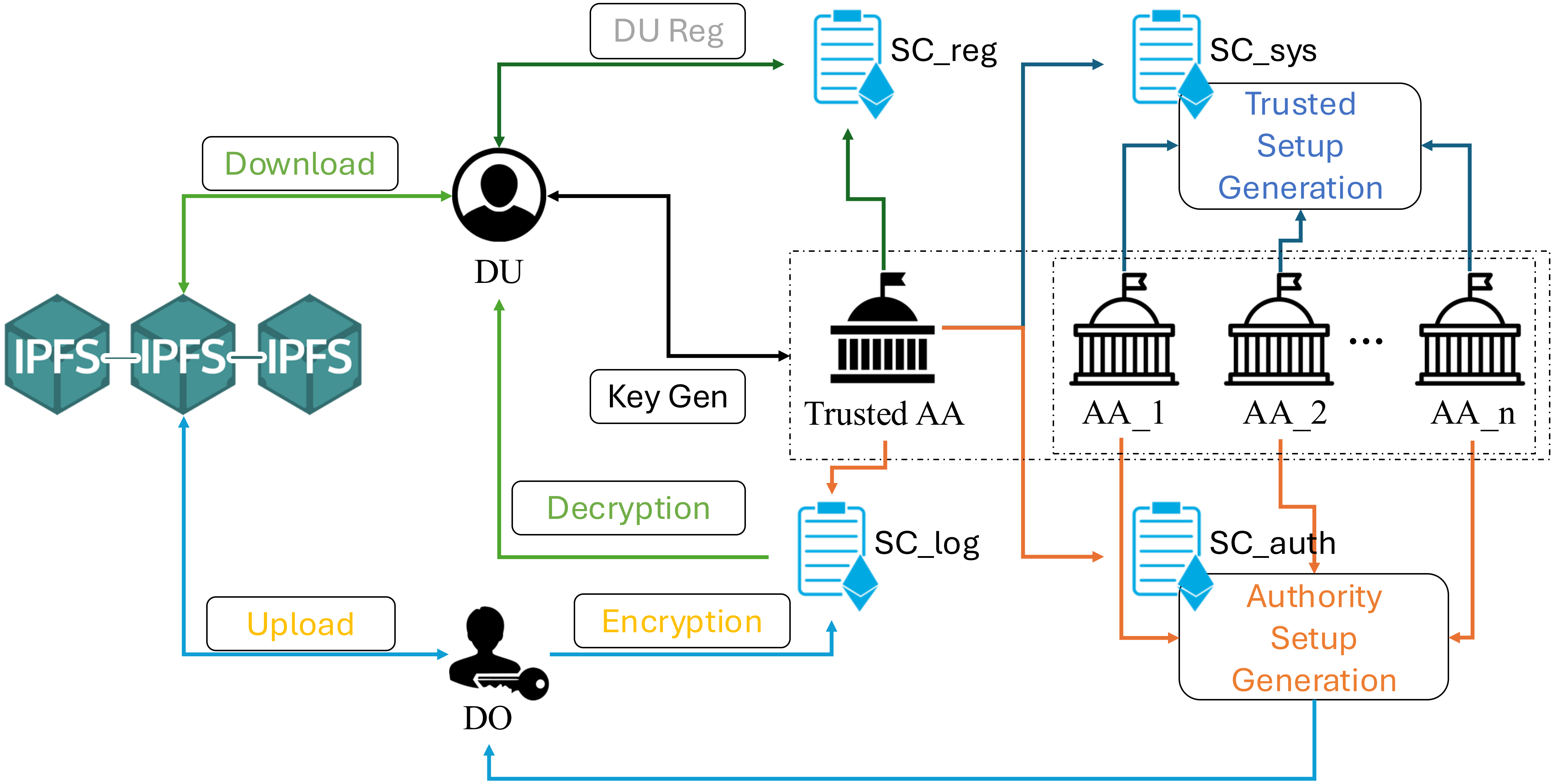
Michalevsky, Yan, and Marc Joye. "Decentralized Policy-Hiding ABE with Receiver Privacy." In *Computer Security, 2018*, edited by Javier Lopez, Jianying Zhou, and Miguel Soriano, 11099:548–67. Lecture Notes in Computer Science. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-98989-1_27.

- Mitigation (using Multi-party Compute + Zero Knowledge Proofs) of a vulnerability: rogue-key attack

Jingchi Zhang, Anwitaman Datta:
Enhancing Privacy-Preserving Multi-Authority Attribute-Based Encryption: Addressing Rogue-Key Attacks Under Adaptive Corruption of Authorities. TrustCom 2024: 524-531

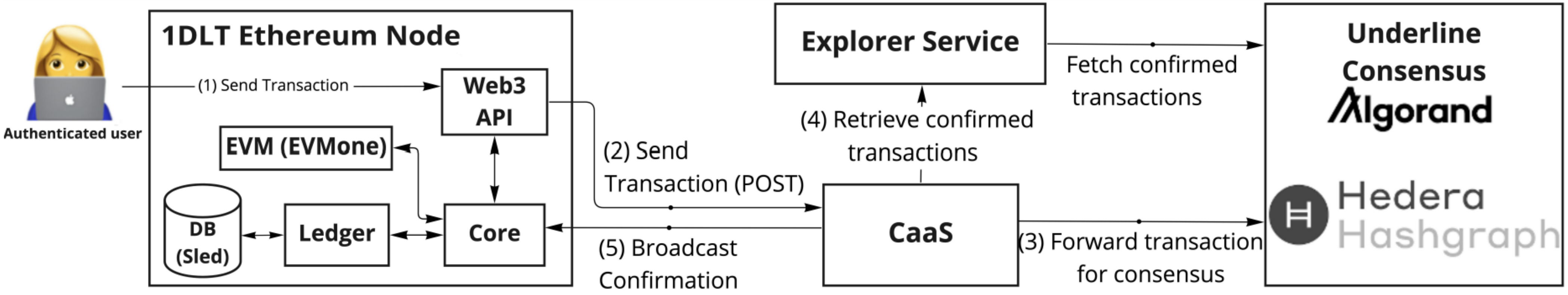
Jingchi Zhang, Anwitaman Datta:
Blockchain-enabled data governance for privacy-preserved sharing of confidential data. PeerJ Comput. Sci. 10: e2581 (2024)

Fine-grained Control



1DLT internals

Decouple transactions from consensus
- Facilitate on-demand EVM based DLTs

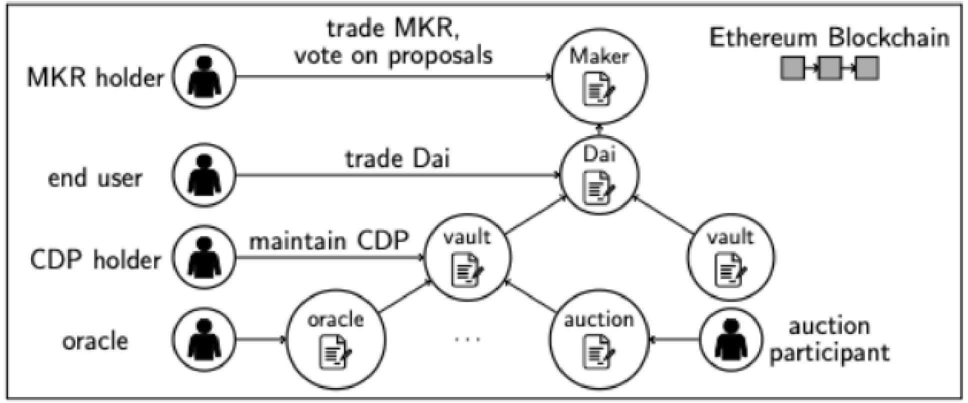


CroCoDAI

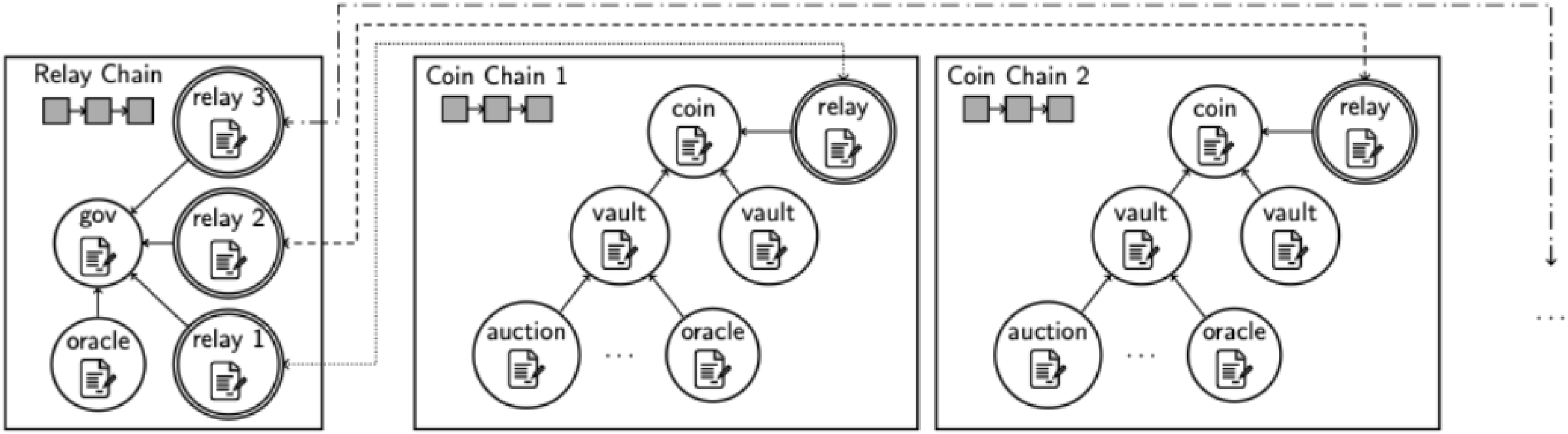
STABLE COIN

Extends ideas from DAI to accommodate non-Ethereum cryptocurrencies

DAI

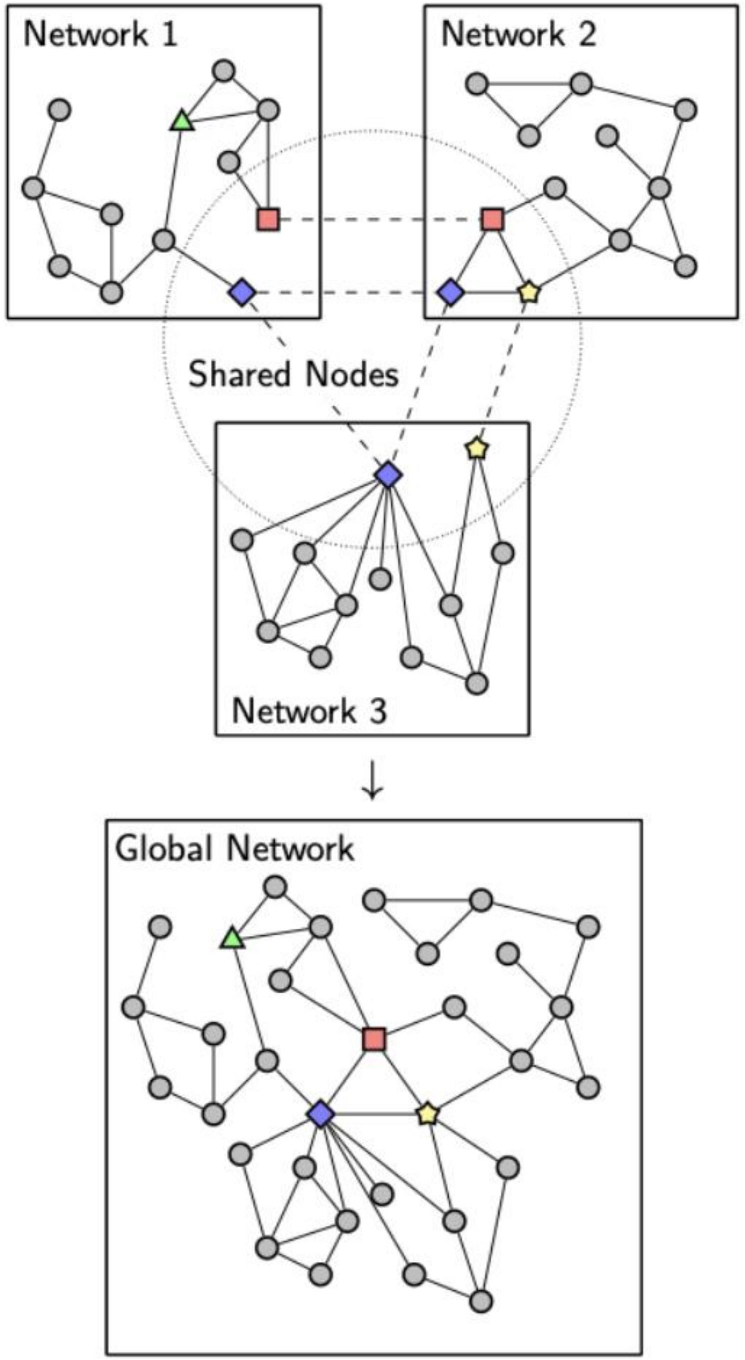


CroCoDAI



CroCoGator

Reputation Aggregation
- with (some sort of) completeness guarantees



Concluding Remarks

KEY TAKEAWAYS

- Cryptographic primitives
  - Atomic swaps with Hashed Time Lock Contracts
  - Self-Sovereign Identities (SSI)
    - Associated privacy benefits
  - Fine-grained (like, role based) access control (using ABE)
    - Caveat: Our current work with ABE is stand-alone, and it is yet to be integrated with the rest of BlockChain I/O
- Digital ecosystem/markets/DeFi
  - Applications over multiple interoperable blockchains
    - POC/TRL4: Various forms of auctions, ticket scalping prevention
  - Multi-chain cryptocurrency collateralized stable-coins
  - Global reputation aggregation
- Code
  - https://github.com/ntublockchain/I-O

Q&A

THANKS

Hvala