TORYS

Association of Corporate Counsel ONTARIO

“The Blockchain Deal”

What you need to know about negotiating blockchain deals

Speakers:
Jessica Lumiere, Senior Lawyer, Torys LLP
Adam Armstrong, Partner, Torys LLP
Gord Ackroyd, General Counsel, SecureKey Technologies
Alina Silvestrovici Paun, Senior Counsel, Enterprise Payments, TD Legal Department

Agenda

1 | What is blockchain?

2 | Blockchain implementations

- Currency
- Digital I.D.
- Smart contracts

3 | Privacy considerations

4 | Non-legal considerations

1 | What is blockchain?

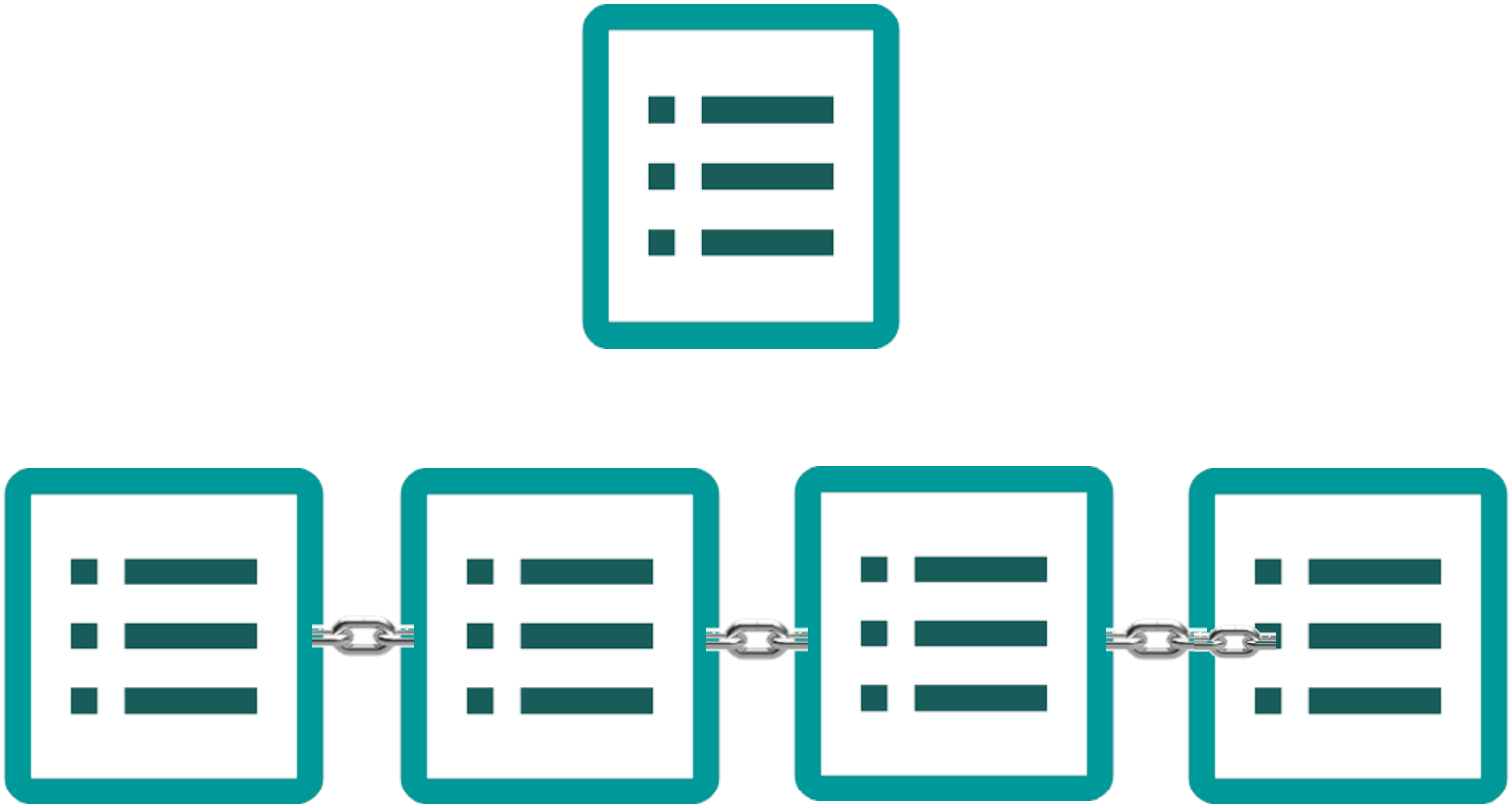
Blockchain Analogy

- Analogous to shareholders' ledger

Shareholder	Number of Shares	To Whom Shares Are Transferred	Date of Transfer
~~Party A~~	~~100 common shares~~	~~Party B~~	~~September 26, 2017~~
Party B	100 common shares		

Transaction → Block → Chain

Transaction → Block → Chain



The Bitcoin blockchain in action

https://tradeblock.com/bitcoin

What is new?

- Technical answer: a decentralized, distributed database operating on an autonomous network of nodes which follow cryptographic consensus rules.
  - Decentralized politically – no central administrator
  - Decentralized architecturally – no central infrastructure
  - Distributed – each node is connected to many other nodes. This means there is no single point of failure or attack because each node has its own copy of the master, and once transactions are recorded, they cannot be altered.
  - Nodes – computers on the network that maintain a copy of the ledger (aka "miners")
  - Consensus rules – method by which nodes agree on the 'true' version of the ledger
  - Cryptography replaces verification functions that are commonly performed by third party intermediaries – this has the potential to dramatically decrease costs and increase speed

2 | Blockchain Implementations

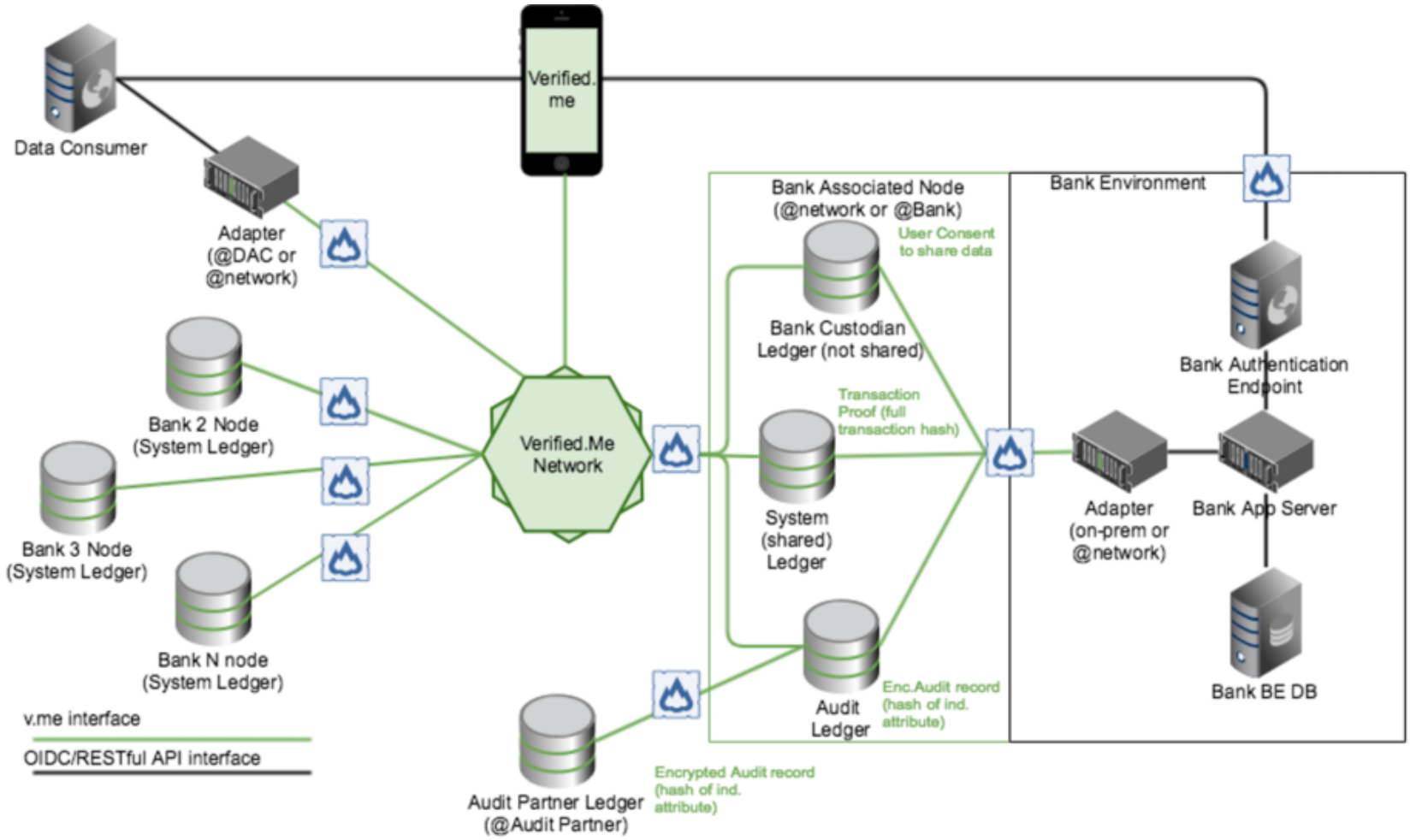
Currency: Bitcoin

=

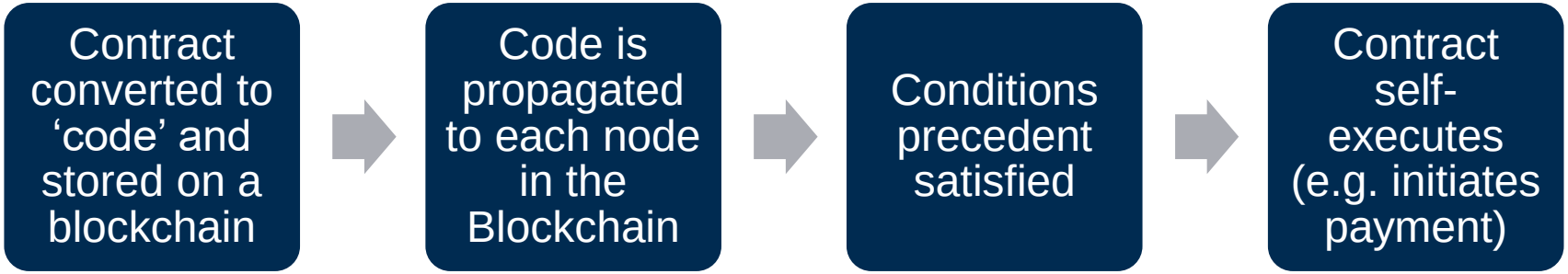
Digital ID: Why Use Distributed Ledger (Blockchain)

- 'Decentralized and distributed' (shared) ledgers = a highly available system.
- Use of private ledgers for Service Hosts = controlled access.
- No single party can change the data without network consensus.
  - Distributed database with messaging layer & tamper proof audit log in blocks
  - Participating organizations cannot access or corrupt another organization's records/data.
- 'Blinding' of user and participant(s) as default = privacy & confidentiality (health care use cases);
- 'Unblind' data providers/recipients when required (KYC for account opening/sharing of credit file)
- Minimize computing requirements on each peer (trusted peers and endorsement model)
- To avoid development of a customized and distributed solution, SecureKey used Hyperledger Fabric open-source project, open to contributions and assessments:
  - A distributed, permission-based ledger, protecting the service's security and availability
  - Licenses or "smart-contracts" within network so competitive organizations can participate fairly
  - Immutable ledger for recording transactions = audit, billing and fraud monitoring features

Architectural Deployment



Smart Contracts

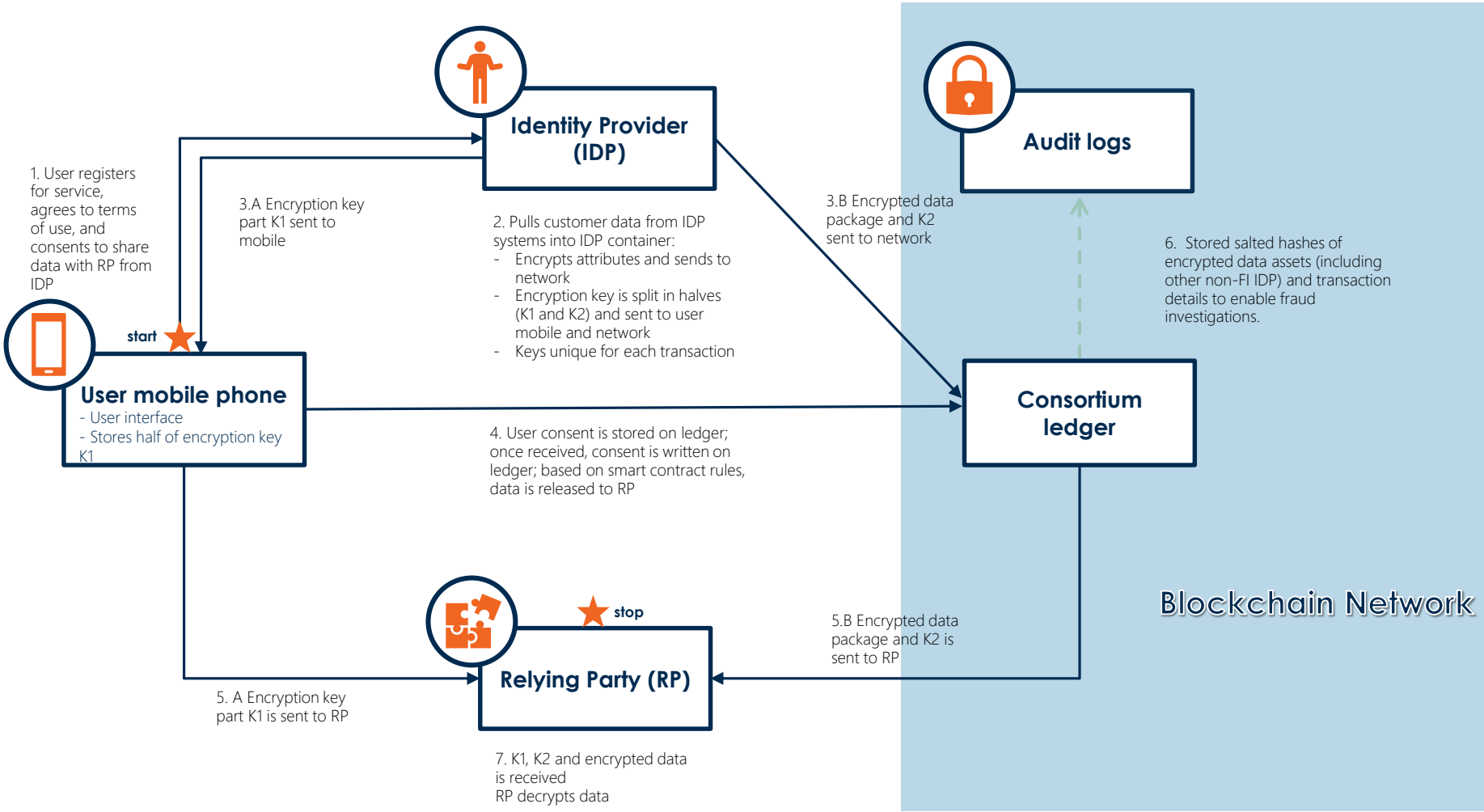


- What a smart contract CAN do:
  - Make decisions based on numbers/ For example: A sells stock options to B with an exercise price of X; the terms of the options are written as code on the blockchain; when the stock price hits X, the contract executes and the payment set forth in the contract is delivered to B.
- What a smart contract CANNOT do:
  - Assess whether vague or subjective conditions precedent are met, unless a tremendous amount of time and money spent describing all the possible ways for when and how those conditions could possibly met, not to mention implementing the consensus rules for verifying that a condition has been met

3 | Privacy Considerations

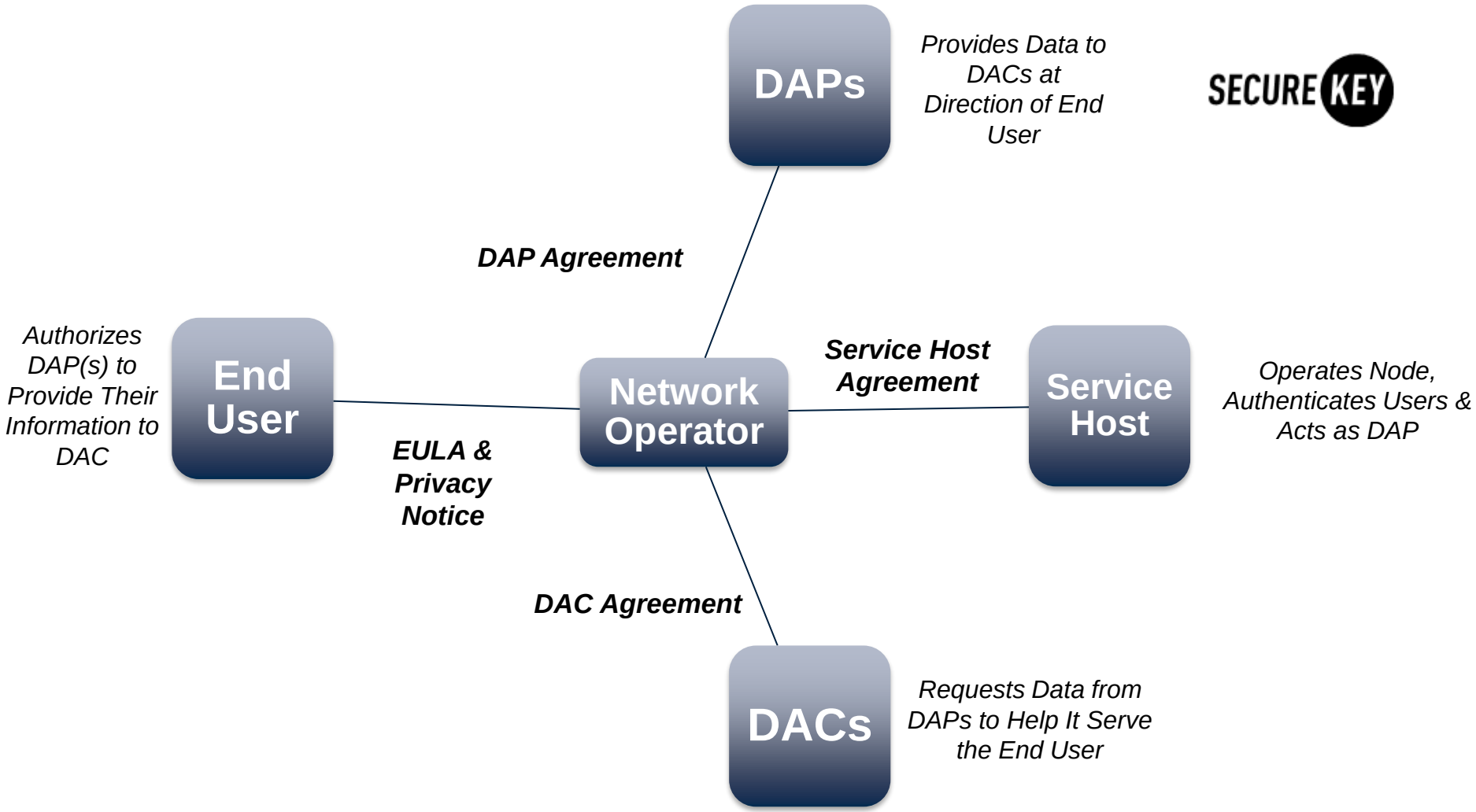
Privacy Considerations

- Canadian privacy compliance:
  - Access to information, return or deletion of information, security measures, disclosure, consent, incident reporting
- Blockchain considerations:
  - Recall: 1) information on the blockchain is visible to every node, and 2) information on the blockchain is immutable – it cannot be deleted or altered (changes can be made in “new blocks” but the unchanged information is still in “old blocks” and changes are invalid unless made by consensus across all nodes).
  - Data retention and deletion: Canada and the E.U. - generic blockchains do not allow parties to minimize data and limit storage, but there are some options:
    - security: hashing and salting
    - public, private or permissioned blockchains; oracles and side chains
  - Blockchain complexity:
    - disclosure; consent
    - incident management


Identity Provider (IDP)
Audit logs
1. User registers for service, agrees to terms of use, and consents to share data with RP from IDP
3.A Encryption key part K1 sent to mobile
2. Pulls customer data from IDP systems into IDP container:
- Encrypts attributes and sends to network
- Encryption key is split in halves (K1 and K2) and sent to user mobile and network
- Keys unique for each transaction
3.B Encrypted data package and K2 sent to network
6. Stored salted hashes of encrypted data assets (including other non-FI IDP) and transaction details to enable fraud investigations.
start
User mobile phone
- User interface
- Stores half of encryption key K1
Consortium ledger
4. User consent is stored on ledger; once received, consent is written on ledger; based on smart contract rules, data is released to RP
Blockchain Network
stop
Relying Party (RP)
5.B Encrypted data package and K2 is sent to RP
5. A Encryption key part K1 is sent to RP
7. K1, K2 and encrypted data is received
RP decrypts data

4 | Non-legal Considerations

Reminder: Ecosystem Structure…



Pre-Launch

- Ecosystem participants' requirements
- Clear decision-making authority
- Multi-party, decision-making model during negotiations
- Technical expertise, data flows
- Contractual terms
- [NTD: Add something about making sure that the blockchain is designed to have the security and other technical requirements to deal with issues such as deleting data?]

Post-Launch

- Ecosystem Participants:
  - Governance
  - Change management
- Participant Entry and Exit
- Disputes/Breach

www.torys.com

ACC Association of Corporate Counsel ONTARIO

TORYS