Theme D: Systems Infrastructure for Open Markets

- Goal: to enhance food traceability and to deter counterfeiting
  - Coupling DNA profiling and densely instrumented food supply chains with a distributed ledger (or blockchain) framework

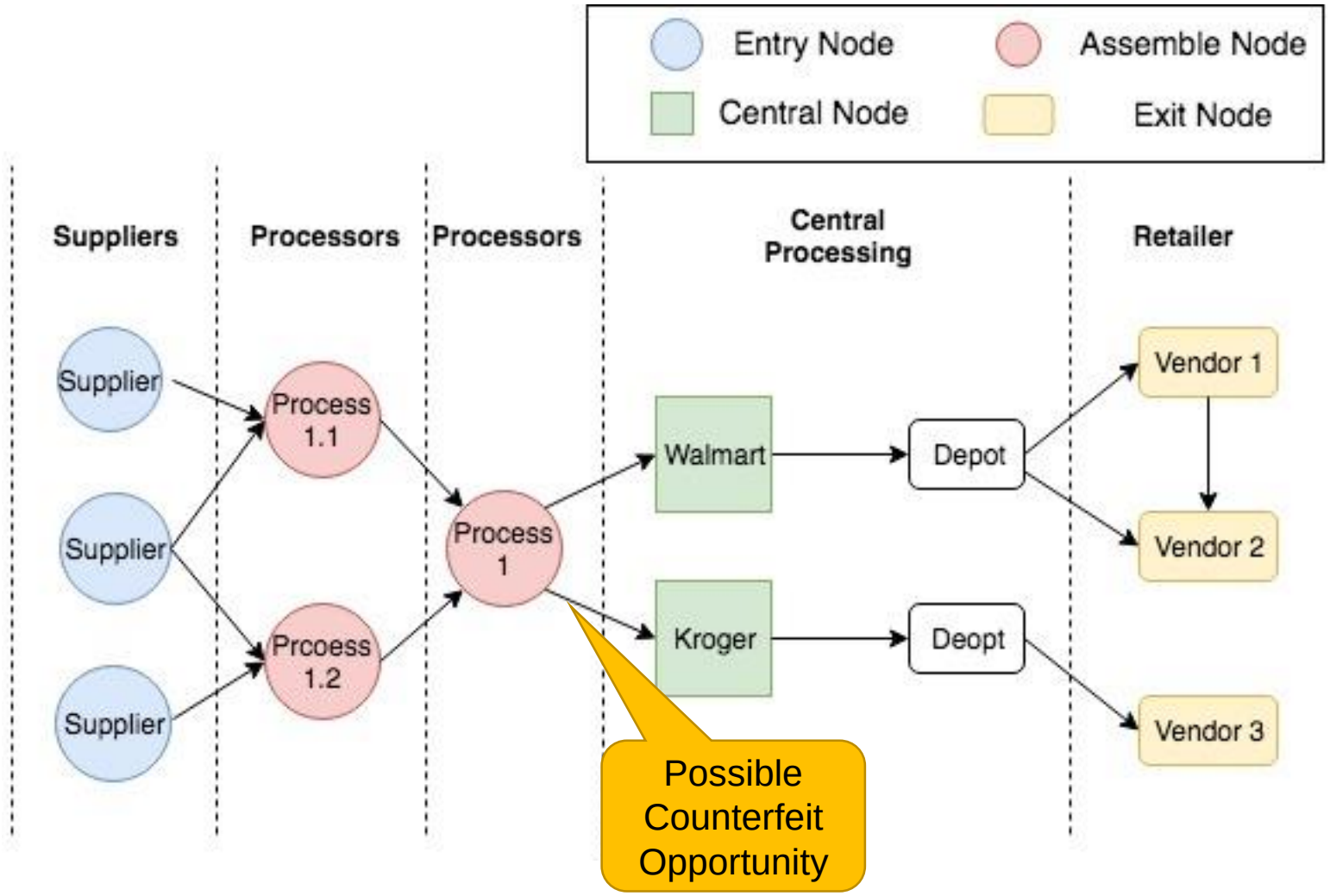
- Challenge: the current commercial inclinations towards building blockchains inside and at the periphery of organizational boundaries have inherent limitations

- We aim to design and develop an open multi-vendor permissioned blockchain platform offering a powerful trade-off between privacy, traceability, and performance

Technical Challenges

- The key technical challenges in accomplishing overall goal are:
  - Blockchains can mitigate, but do not entirely solve the problem of uniquely associating identities to assets
  - Multi-vendor blockchain information should not be ubiquitously accessible across the platforms and should be protected from competitors
  - Employing generic privacy solutions can be prohibitively expensive

Technical Challenges



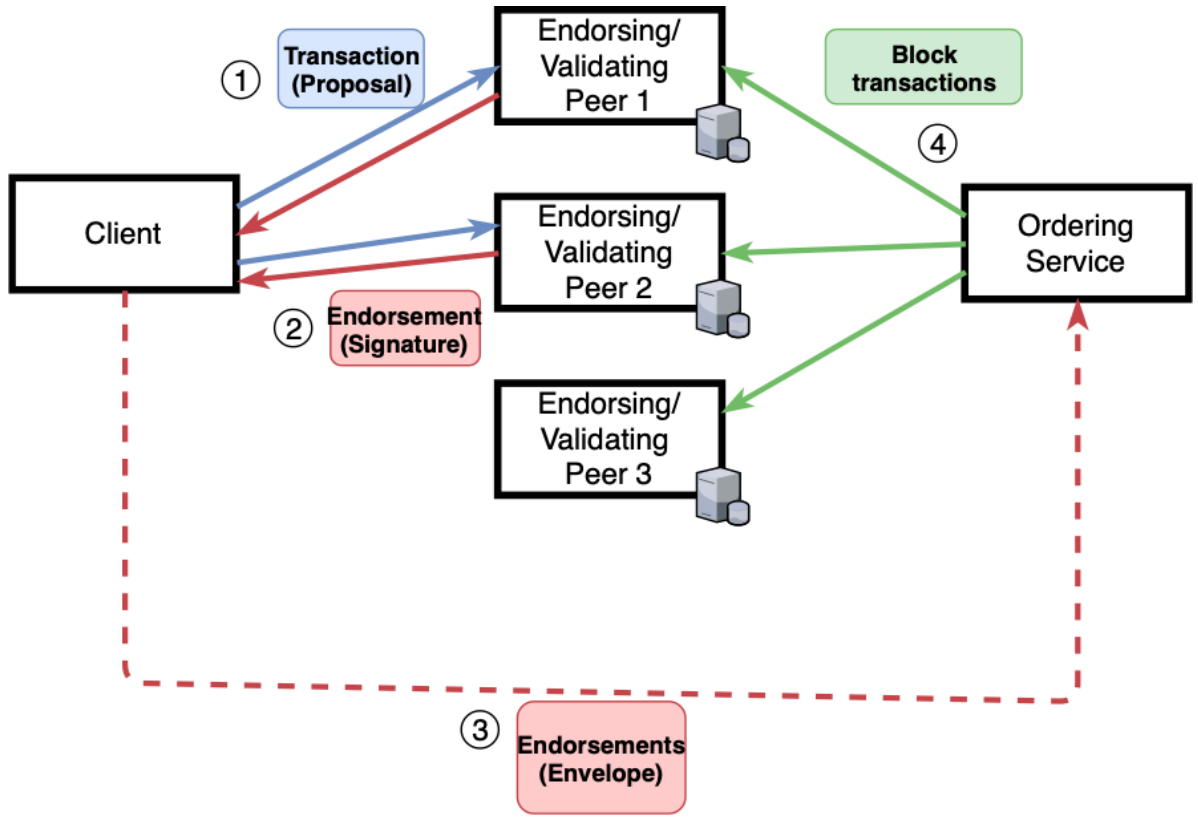
Technical Approach (1 of 3)

- Our approach to these problems is:
  - multi-vendor permissioned blockchain platform

Permissionless Blockchain	Permissioned Blockchain
Anyone can join, read, write, and govern (validate, commit, and regulate)	Only authorized participant can join, read, and write
Functions as an overlay network over the Internet	Only a selected few govern (validate)
Proof of work, stake, etc. to deal with Sybil attacks	Employ strong identity and requires n-party consensus protocols (BFT, Libra)
Slow, Low Scalability	Fast, High Scalability

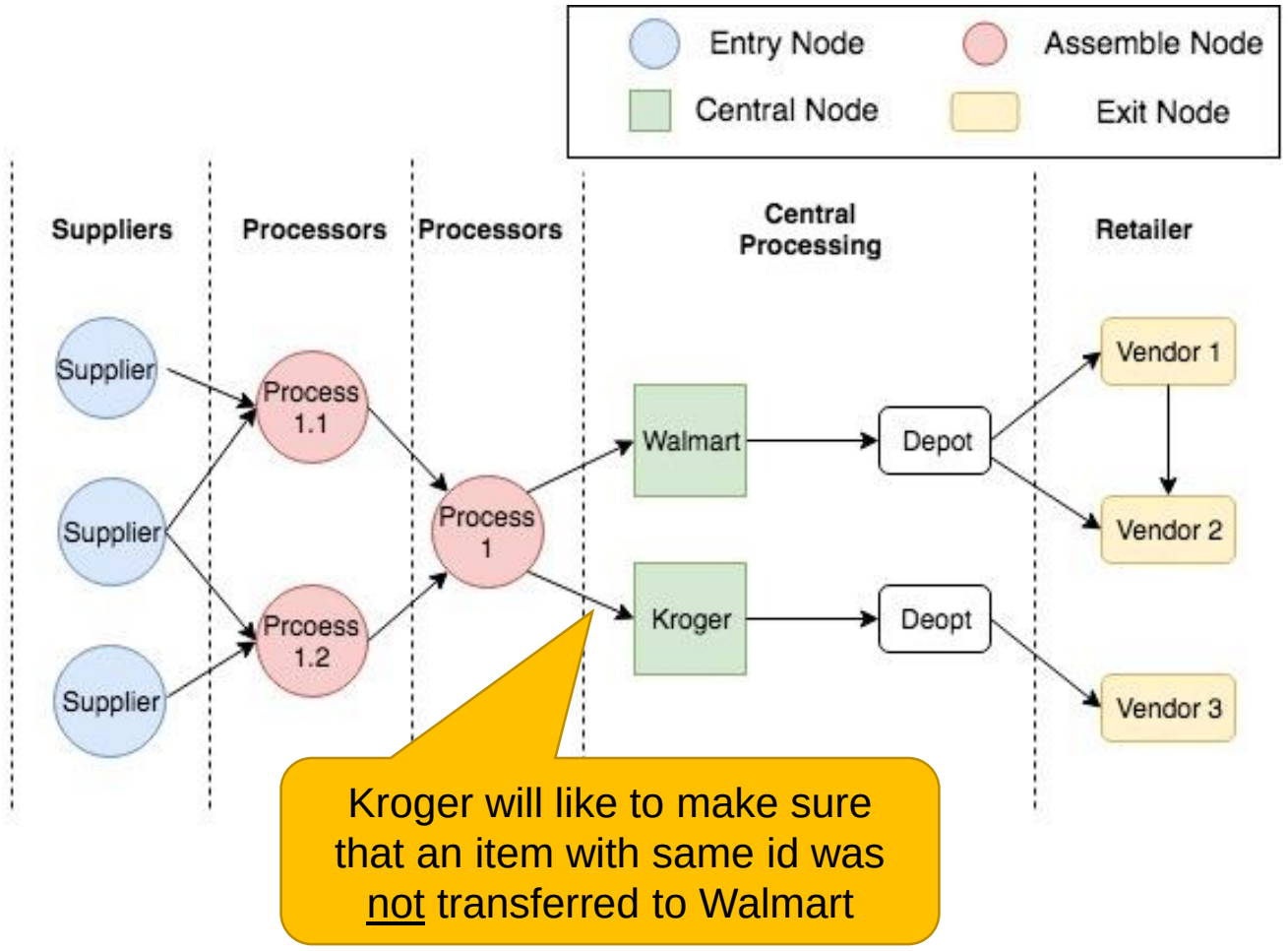
Technical Approach (1 of 3)

- The Execute-Order-Validate approach + Endorsement policies of Hyperledger Fabric is ideally suited for the problem
  - Scalability
  - Control over the write ops



Technical Approach (2 of 3)

- Understanding privacy, access control requirements

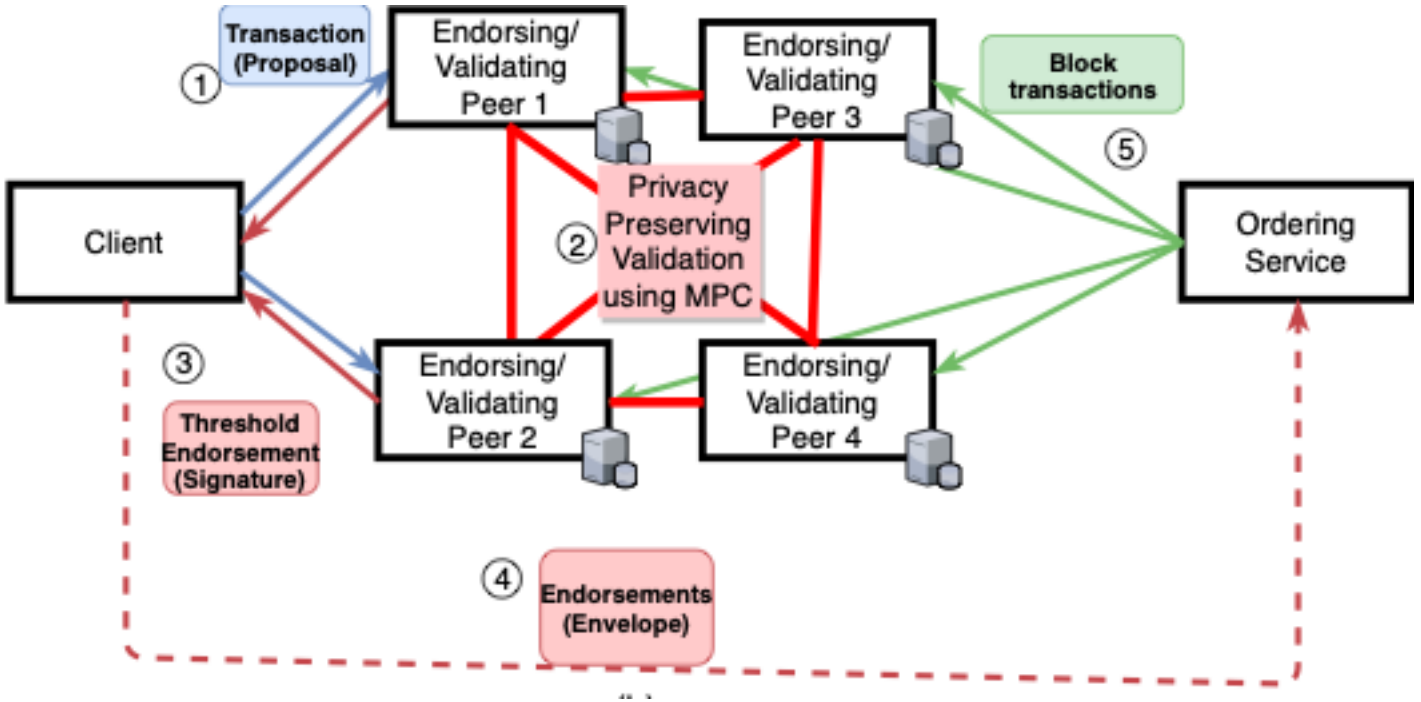


Technical Approach (3 of 3)

- Realizing achieve those using cryptographic and distributed computing techniques
  - Secure Multi-party Computation (MPC)
    - Non-collusion assumption
    - Covert adversary
  - Non-interactive Zero-knowledge proofs (of knowledge) (NIZK)
    - One-wayness, trapdoor permutation
  - Meta-data hiding communication

Technical Approach (3 of 3)

- Endorsing nodes performs MPC to validate transactions and create private blockchain writes



Related Research and Novelty of Proposed Approach

- Federated blockchains / Blockchain for Supply-chains
  - Privacy problems are ignored assuming that blockchainsare not ‘public’
    - Privacy issues against competitors/insiders are ignored
  - With all nodes inhouse, the chain manipulations can be possible
- Current NIZK-based solutions are cryptocurrencies are not suitable for supply-chains
- Robustness guarantees are not available for the current MPC systems
- Current meta-data hiding communication solutions such as Tor are not acceptable to the industrial settings

Novelty of Proposed Approach

- Innovation in the MPC space
  - Asynchronous MPC systems with linear communication complexity
  - Optimizing MPC pre-processing towards making computation constant round
  - Developing combinations of NIZK and MPC operations towards optimizing performance
- Innovations in the meta-data hiding space
  - Meta-data hiding solutions for the permissioned setting

Theme Outcomes

- Privacy-preserving Multi-supply-chain Blockchain with applicability beyond food supply-chain
- Robust, Efficient MPC Protocols and Systems with applicability to secure computation in general
- Meta-data hiding communication protocols tailored for the consortium scenarios

Interaction With Other Themes

- Theme A: Utilizing DNA profiling
  - When available, our system will utilize DNA watermarks as stronger IDs
- Theme B: Supply-chain Optimizations
  - End-to-end traceability, Forward/backward Historical Queries can be highly beneficial towards optimizing supply-chains
- Theme C: Realizing the virtual payment/incentive system
  - Our blockchain solution will be ideally suited for realizing and experimenting with the incentive mechanism