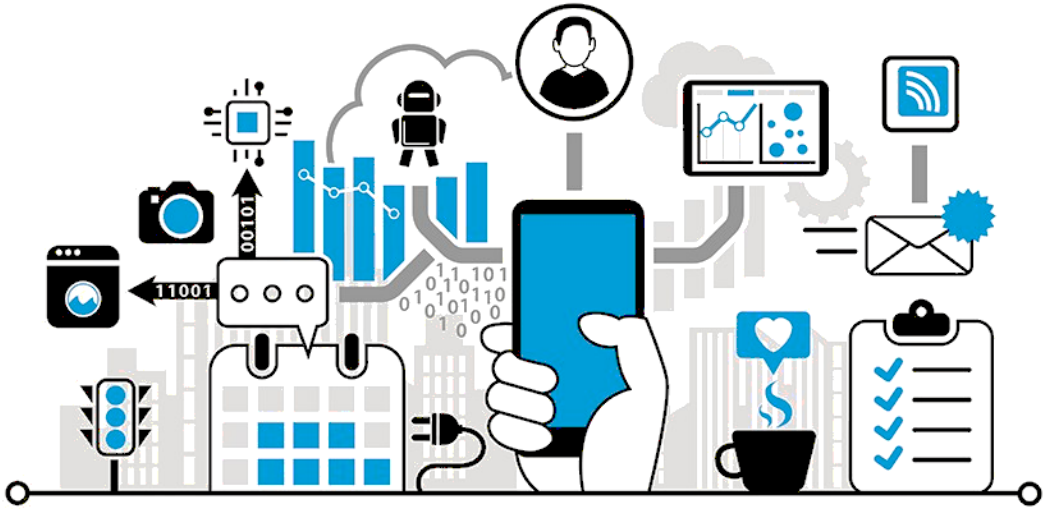
Permissioned Blockchains: Data Security, Privacy and Challenges

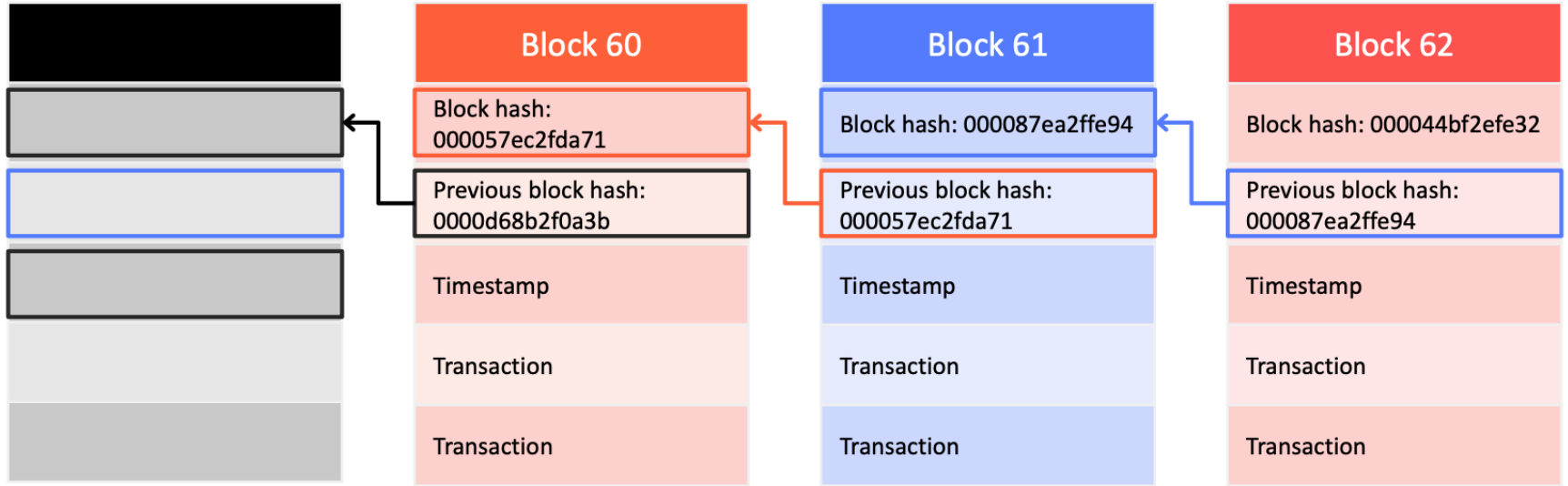


Yusen Wu

Frost Institute for Data Science and Computing

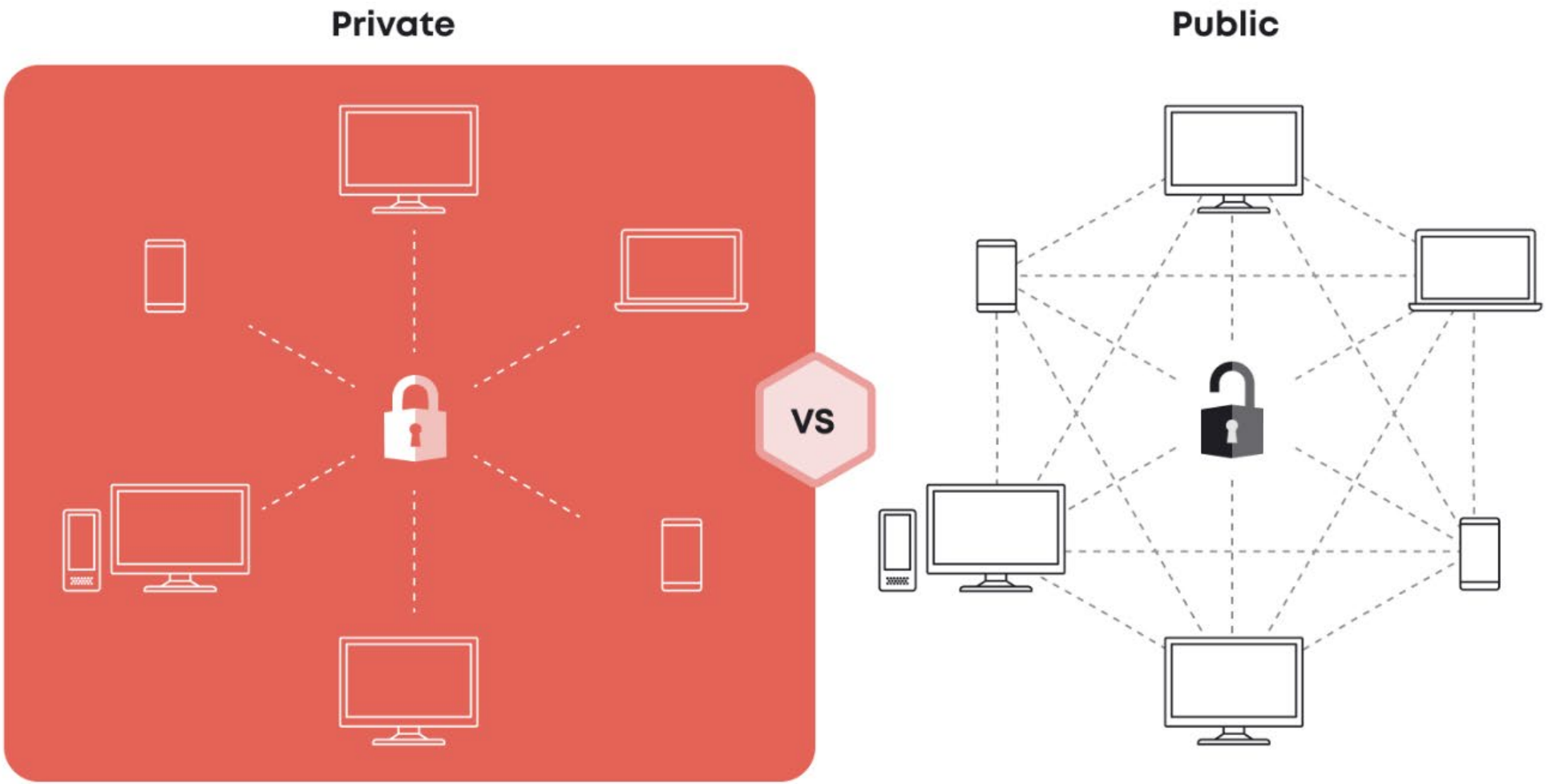
yxw1259@miami.edu

Blockchain components: Distributed ledger database



The journal records an immutable log of all transactions and is maintained by nodes in the blockchain network

Background

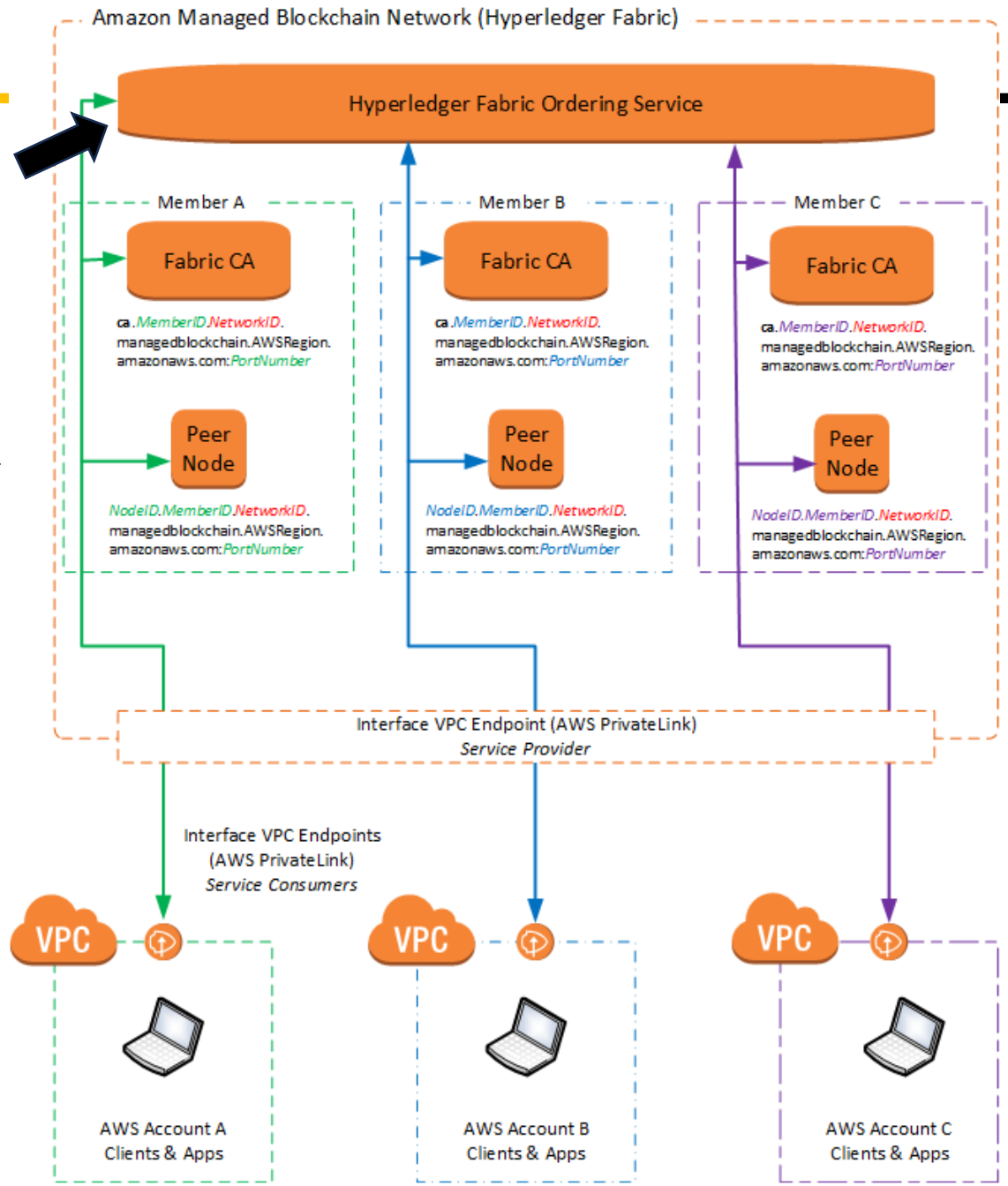


Hyperledger

Ordering services

Three nodes

Three members

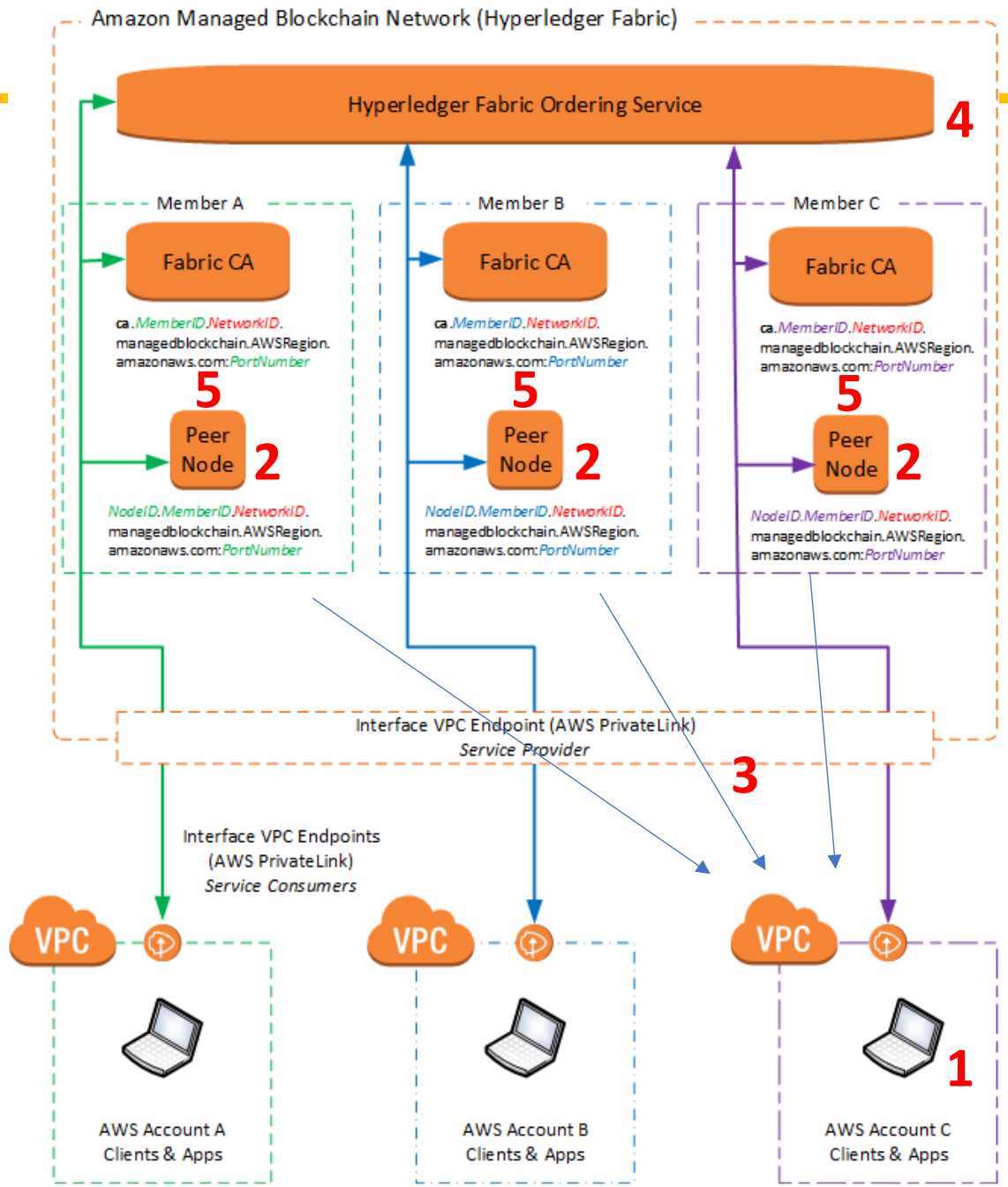


Why it named "Permissioned"?

Permissioned Blockchains are the Future

1. **Enhanced Privacy**
2. **Better Performance and Scalability**
3. **Lower Transaction Costs**
4. **Compliance with Regulations**
   - Meets **data governance requirements** (e.g., GDPR, HIPAA) by controlling who can access or modify data.
   - Enables **auditability and transparency** while ensuring confidentiality.

Workflows



1 User A sends a write request to Blockchain Client.

2 Invoke Smart Contracts function to write the data into a simulation environment for endorsements

3 Collect enough endorsements and reply to client A

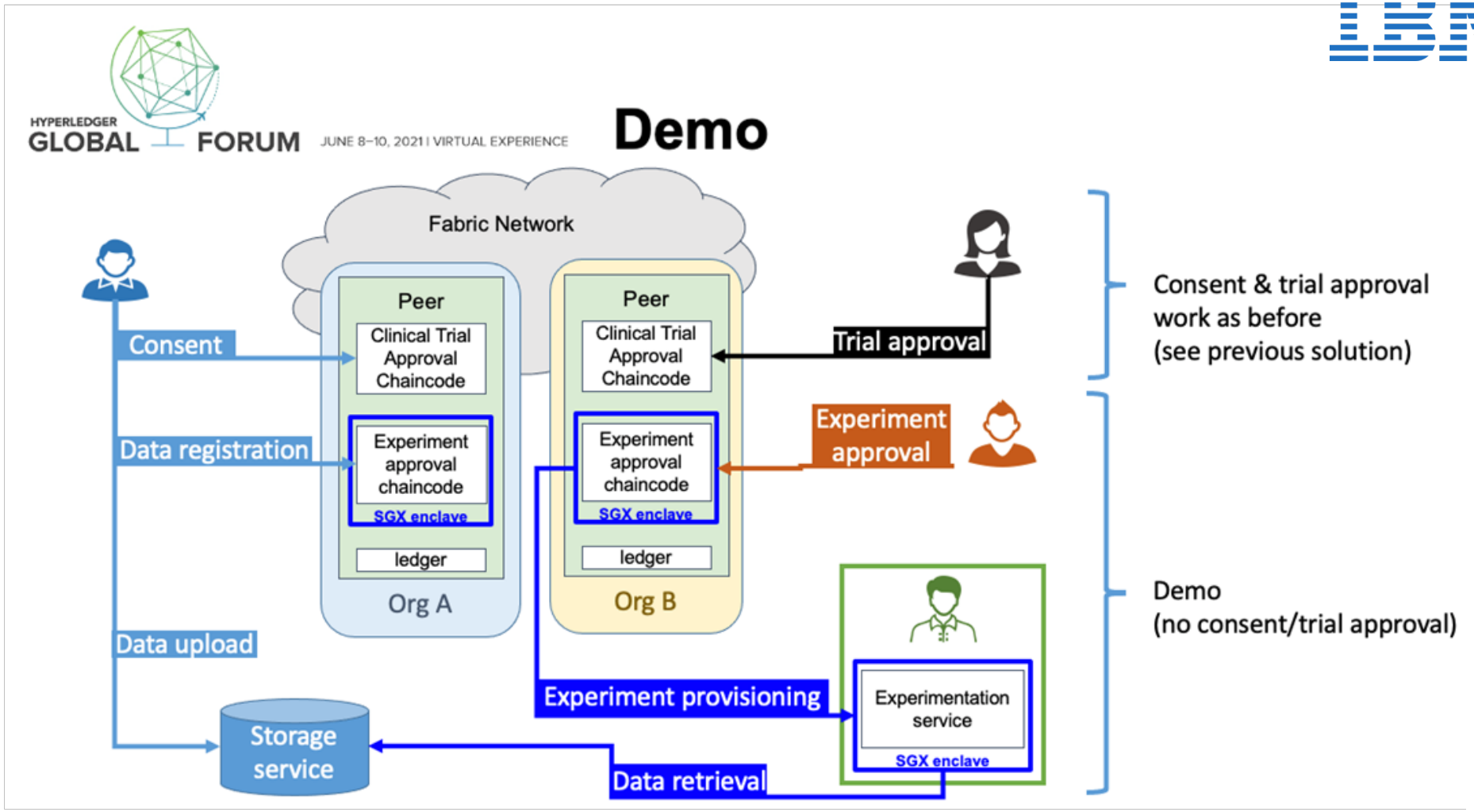
4 Send the message to ordering services for preparing the announcements.

5 BFT leader node will collect enough transactions and send the block to all the peer nodes. Before add to the blockchain, all the nodes will check the block number: if is it in sequence?

Interesting Blockchain Applications

Blockchain with Health care

Funded by IBM



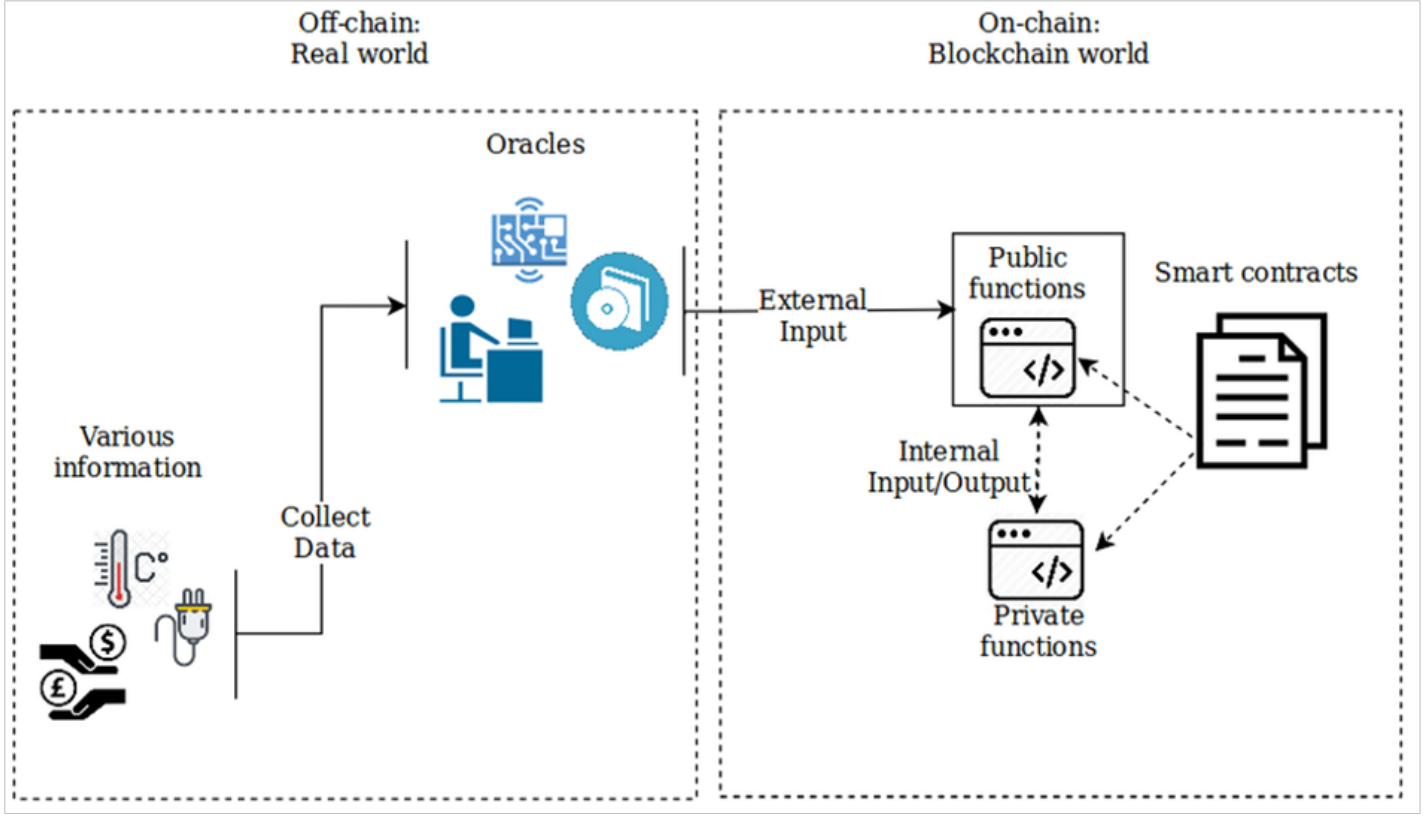
Bringing Trust and Privacy-preserving Smart Contracts to Clinical Trials in Healthcare. Hyperleder Global Forum, June 8-10, 2021

Current: Remote Monitoring and IoT

funded by FDA

Immutable Audit Trails: Every medical transaction, once recorded on the blockchain, is permanent. This immutability ensures that medical histories, treatment records, and other critical information can't be altered maliciously or accidentally, **establishing a clear and unchangeable history for each patient.**

Blockchain with Edge, off-chain on-chain System



Yusen Wu, et al. **PPFChain: Privacy-Preserving Fine-grained On-chain and Off-chain System**. IEEE Transactions on Information Forensics and Security (2024 TIFS)

Some other real applications: Blockchain with Signatures

DocuSign

Solutions ⌄ Products ⌄ Plans & Pricing ⌄ CONTACT SALES BUY NOW TRY FOR FREE

Signatures

Electronic Signature
The #1 way to send and sign

Electronic Notarization
Securely send, sign and notarize agreements online

Contracts

Contract Lifecycle Management
Organized, automated document workflows

Document Generation
Generate documents seamlessly from Salesforce

More

Identity Verification
Incorporate enhanced signer verification into your agreements

Clickwraps
Capture consent with a single click

Web Forms
Streamline data collection and speed up signing

APIs

Integrations

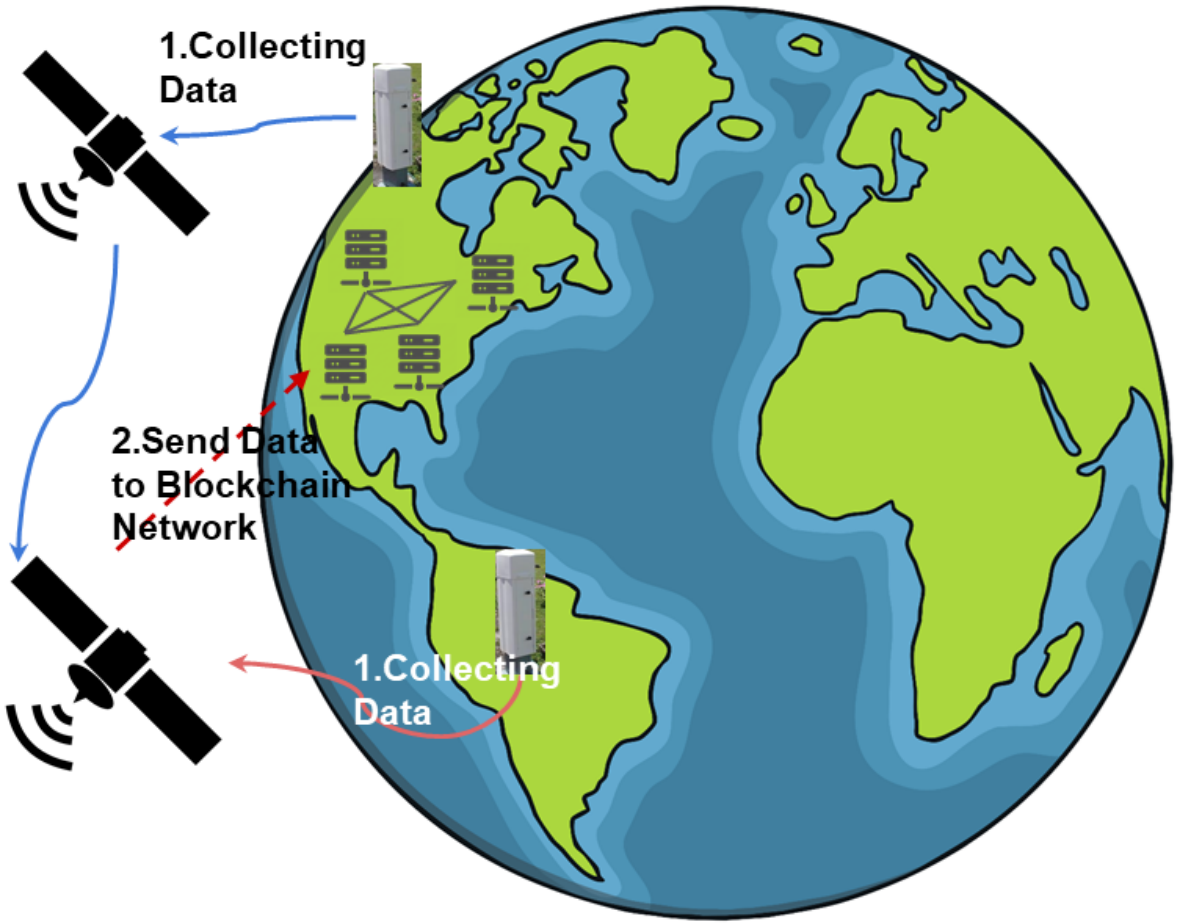
Mobile Apps

All Products →

Verify signer identity beyond the standard practice of clicking an emailed link.

Contact Sales

Blockchain with IoT



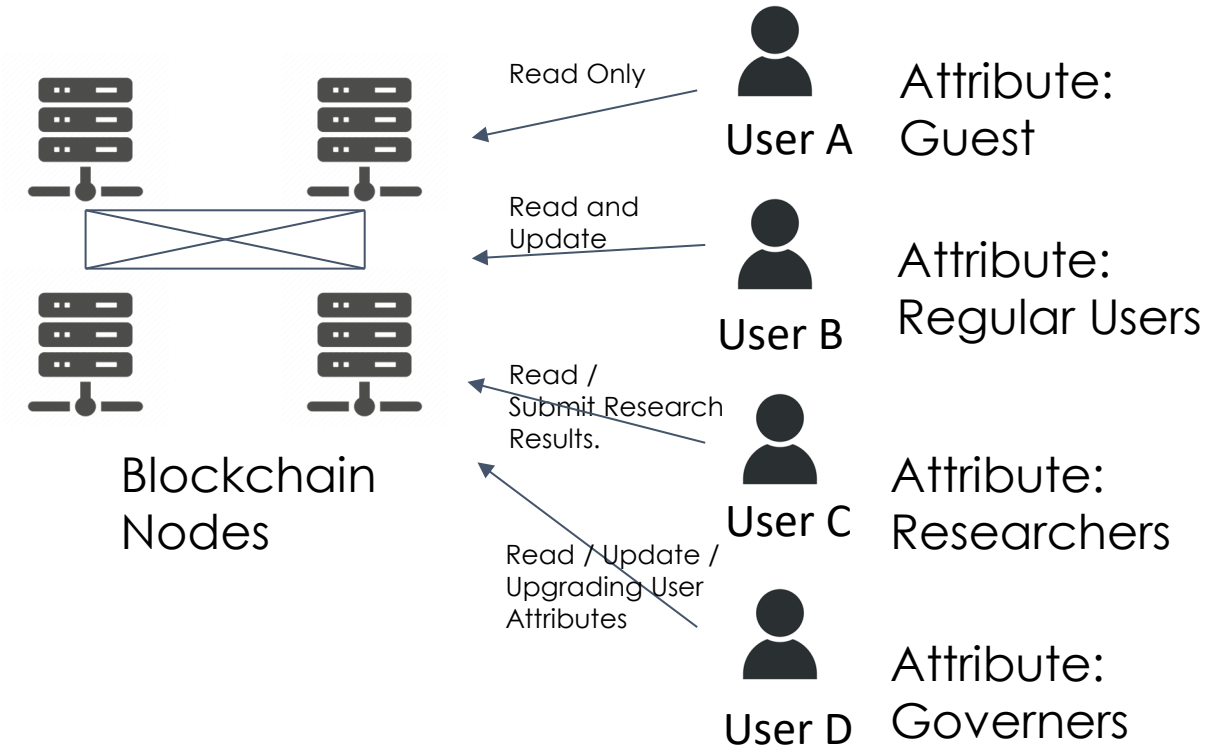
1. Collecting Data from Instruments

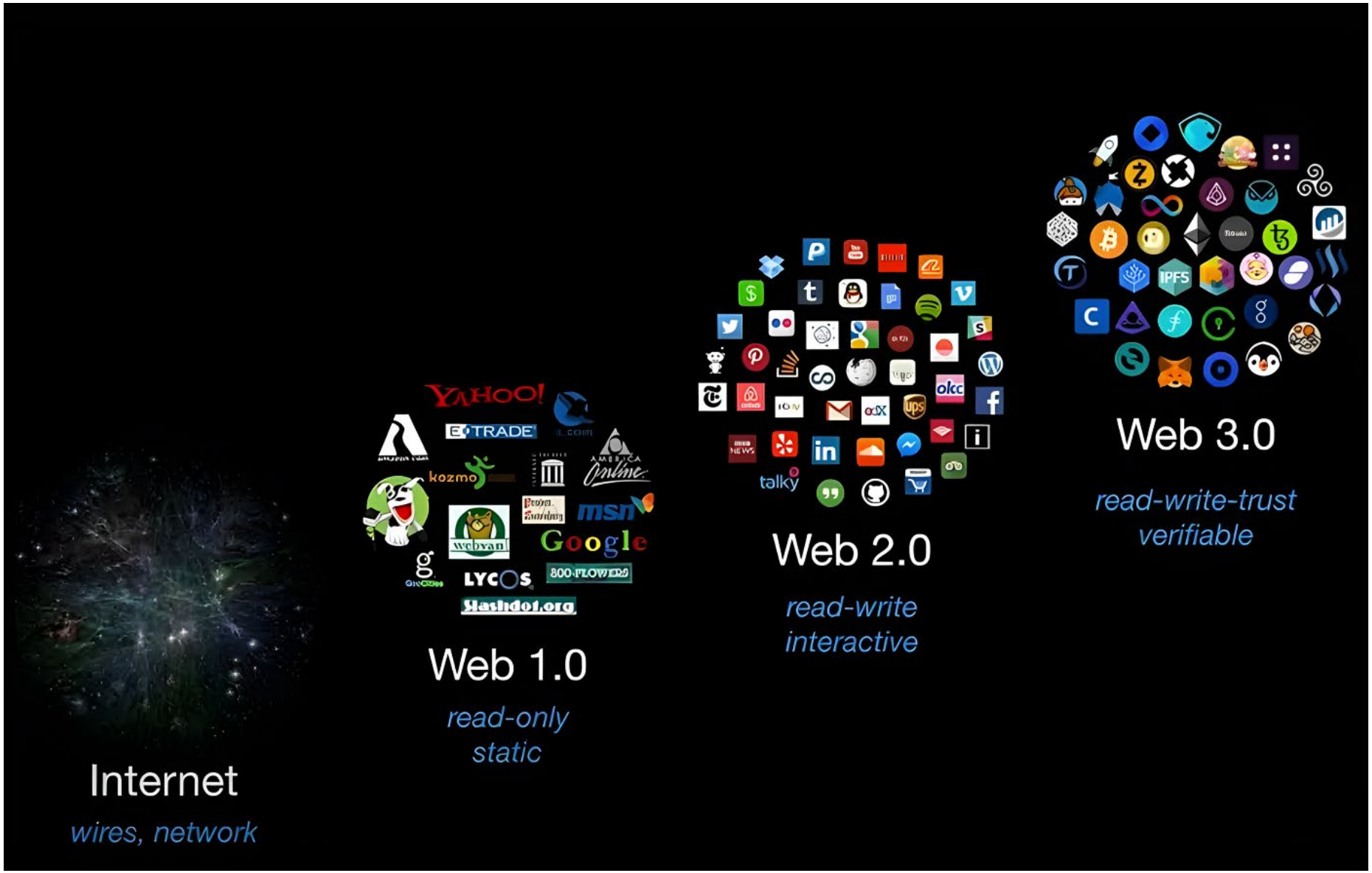
2. Send Metadata to Blockchain, storing large dataset into a secure Database. Querying By Device ID

funded by

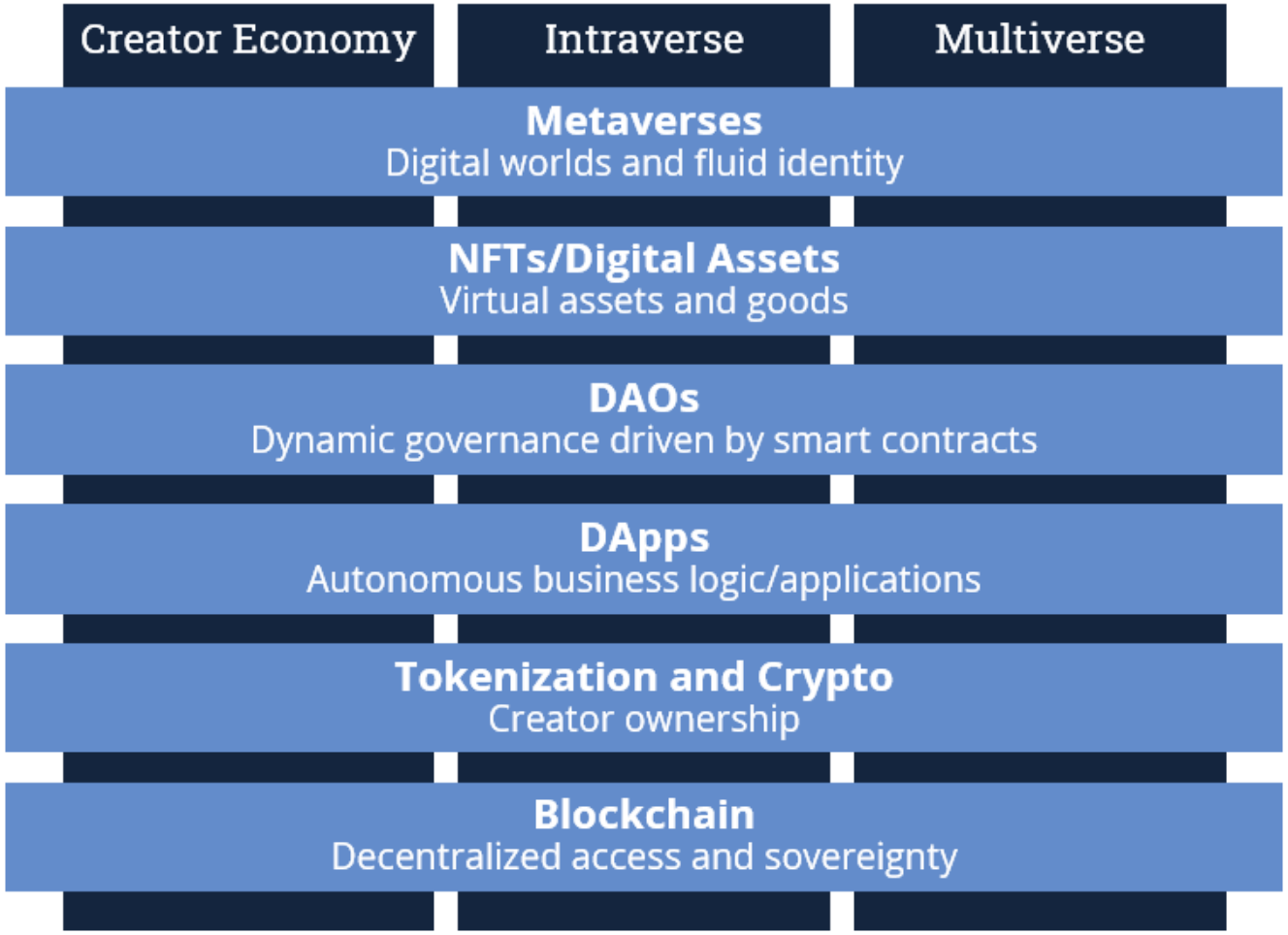
Earth Science Technology Office (ESTO)

Attribute or Role-based Access Control




Internet
wires, network
Web 1.0
read-only
static
Web 2.0
read-write
interactive
Web 3.0
read-write-trust
verifiable

The Web3 Stack



Blockchain with …

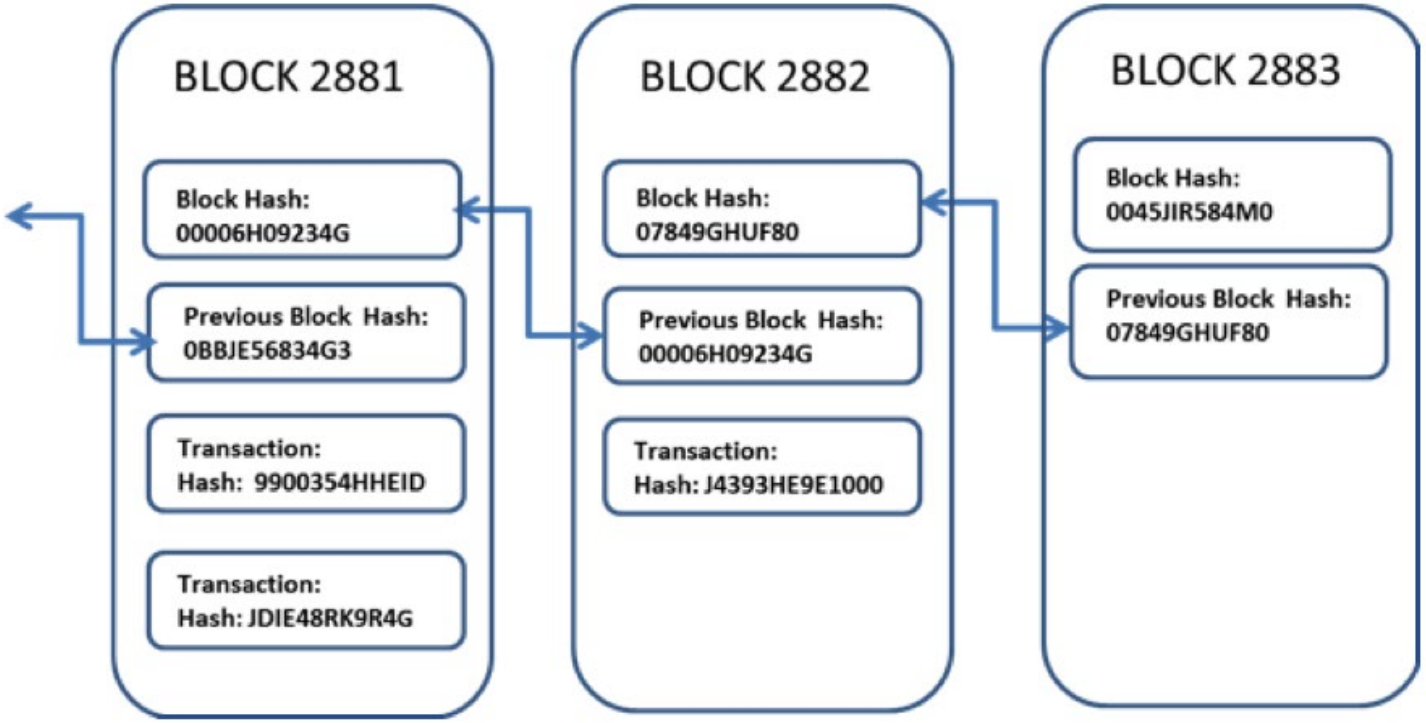
- **Blockchain with Secure Medical Data Sharing / Decentralized Identity Management / Certificate Managements/ Supply chain Traceability /Automated Insurance Claims / Voting Systems / Finance / Grading, etc.**
  - Bring trust to the Data and Transactions
- **Evidence Storage & Digital Notarization**
  - Courts, law firms, and government agencies need tamper-proof records for legal disputes.

Conclusions for Blockchains

- **Decentralization**: Unlike centralized systems, where a single entity has control, blockchain operates on a peer-to-peer network, distributing control among many participants.
- **Immutability**: Once data is added to a blockchain, it's nearly impossible to change. This ensures historical data integrity.
- **Transparency (public)**: Most blockchains are transparent, allowing any user to track and verify transactions.
- **Privacy (permissioned/private):** Permissioned blockchains can bring access control to improve the data privacy.
- **Security**: Transactions must be agreed upon before they're recorded. After validation, they're encrypted and linked to the previous transaction.
- **Trust**: Transactions are transparent and can be verified by any user, ensuring trust without the need for intermediaries.
- **Traceability**: Goods in a supply chain, for instance, can be tracked, ensuring authenticity and reducing fraud.

Challenge A： Data Quality

https://guggero.github.io/blockchain-demo/#!/block



Data Integrity is Enabled，
But Data Quality is hard，especially for IoT Data

- **Pre-processing with AI & Data Sketching**: Use machine learning and **data sketches** for real-time anomaly detection and outlier filtering before data is written to the blockchain.

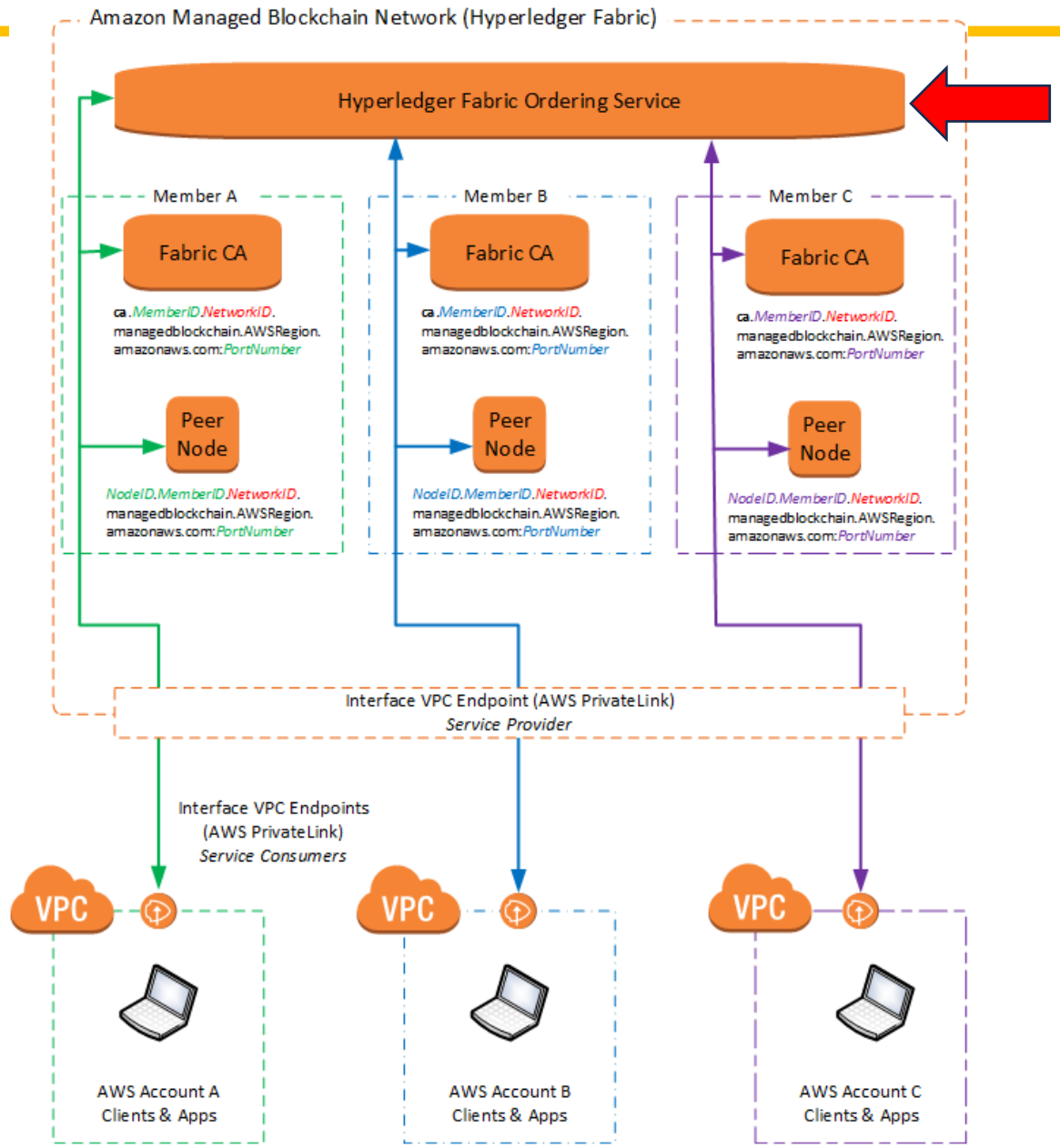
- Using Smart Contract to Analyze the Data Quality (Static).

- AI models for anomaly detection + TEE (Trusted Execution Environment)

Challenge B： Smart Contract Security

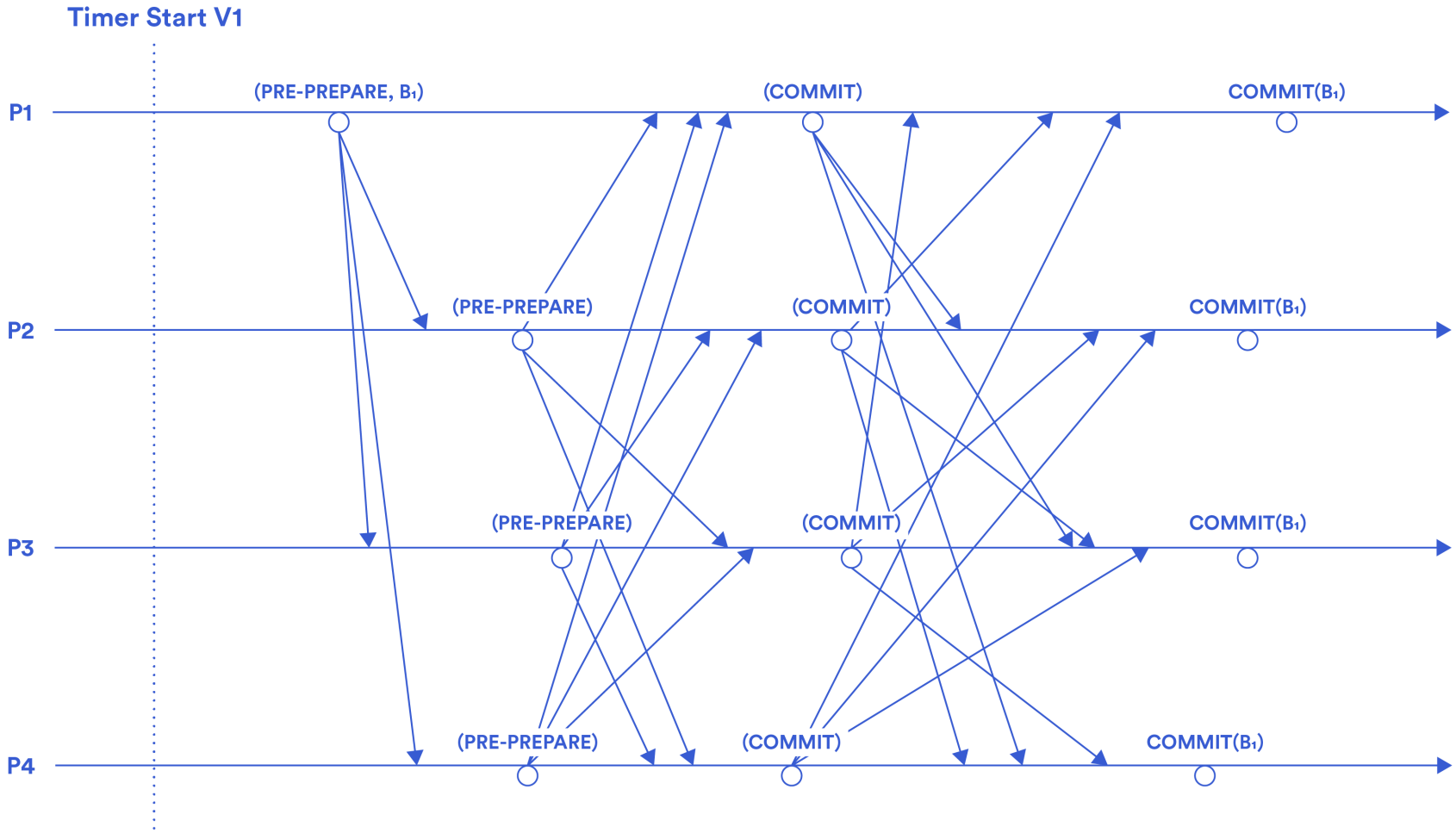
- **Weak Access Control & Unauthorized Access**
  - In permissioned blockchains, role-based access control (RBAC) is crucial. If **access permissions** are misconfigured, an unauthorized user could **invoke or modify** smart contracts, leading to unauthorized data manipulation.
  - In **permissioned blockchains**, smart contracts can often be **upgraded** post-deployment.
- **Low quality Smart contracts**
  - Use AI to write smart contracts
  - Use AI to check the low-quality codes in Smart Contracts
  - Use AI to check access control

Challenge C: BFT Efficiency

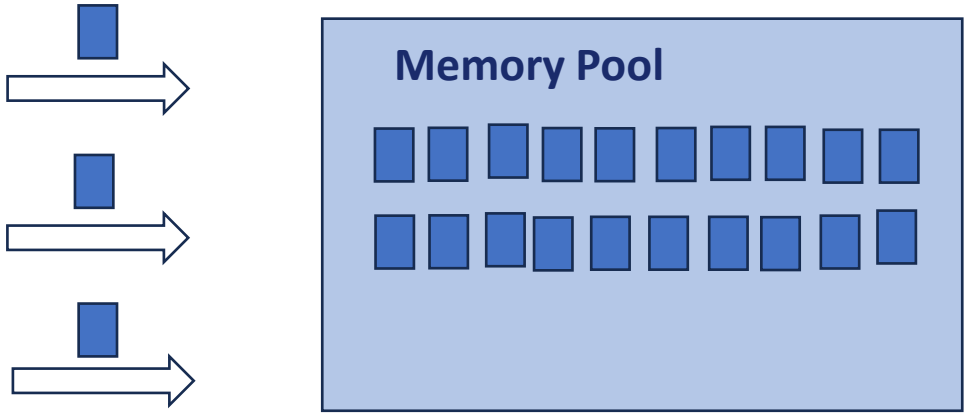


BFT is the main challenge for system efficiency

Exploring Consensus With Parallel Proposals: The Difference Between PBFT and BBCA-Chain

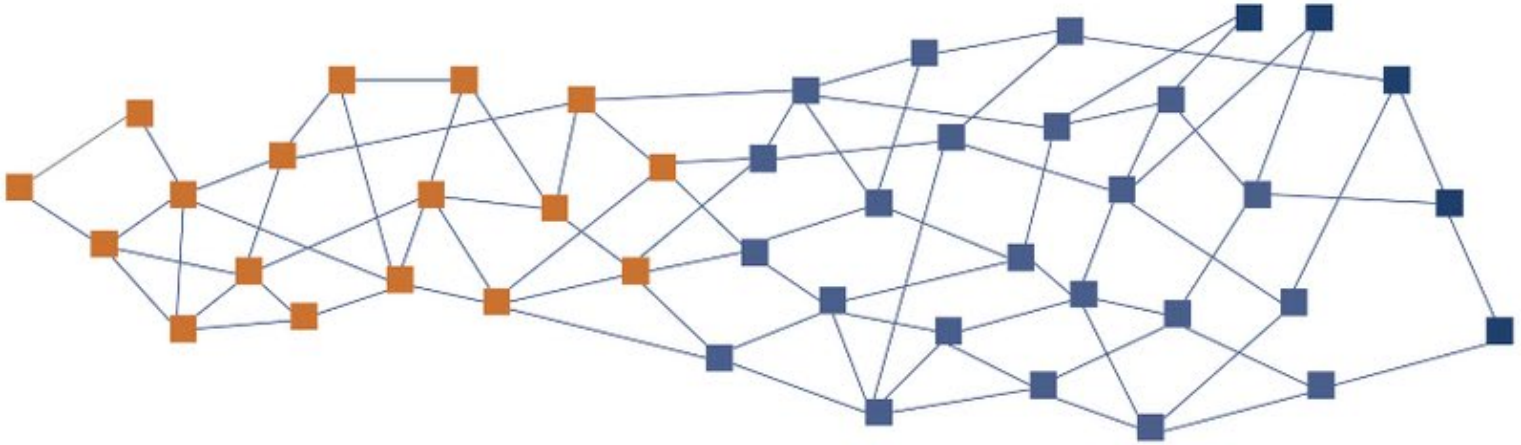


Memory Pool for Blocks



Blockchain

(DAG/Directed Acyclic Graph)



Feature	DAG (e.g., IOTA, Nano)	Blockchain (e.g., Bitcoin, Ethereum)
Transaction Speed	Fast (Parallel Processing)	Slower (Sequential Blocks)
Consensus	Asynchronous (Self-validation)	Synchronous (Mining/PoS)
Mining Required?	No	Yes (for PoW systems)
Scalability	High (No Block Size Limits)	Limited by block size
Transaction Fees	Low / Feeless	High (Especially on Ethereum)
Forks	No forks	Forks can happen (e.g., Bitcoin hard forks)
Security Model	Depends on network adoption	High with established PoW/PoS

DAG query may be time-consuming

Solution： State Database Instead of Full-Chain Lookup

•Instead of searching through **the entire blockchain for transaction history** (like Ethereum or Bitcoin), Hyperledger Fabric **stores the latest state of data** in a **key-value database (state DB)**.

Common Questions be Asked from Previous Presentation

1： Why there are the different types of blockchains?

2： Have you thought to Combine different blockchains?

3: AI combine with Blockchains

Frost Institute for
Data Science and Computing