Role of Blockchains in Timing Security

WSTS 2021

Anand Ozarkar (aozarkar@equinix.com Head of Eningeering, Edge Security)
Ankur Sharma (ansharma@equinix.com Senior Engineer, Systems Software)

Agenda

01 Motivation

02 Threat Model

03 Traceability Challenges

04 BlockChains

05 Timing Use-Case

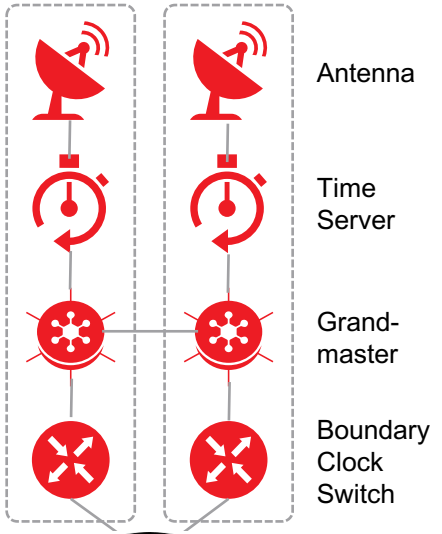
06 Invitation to Participate

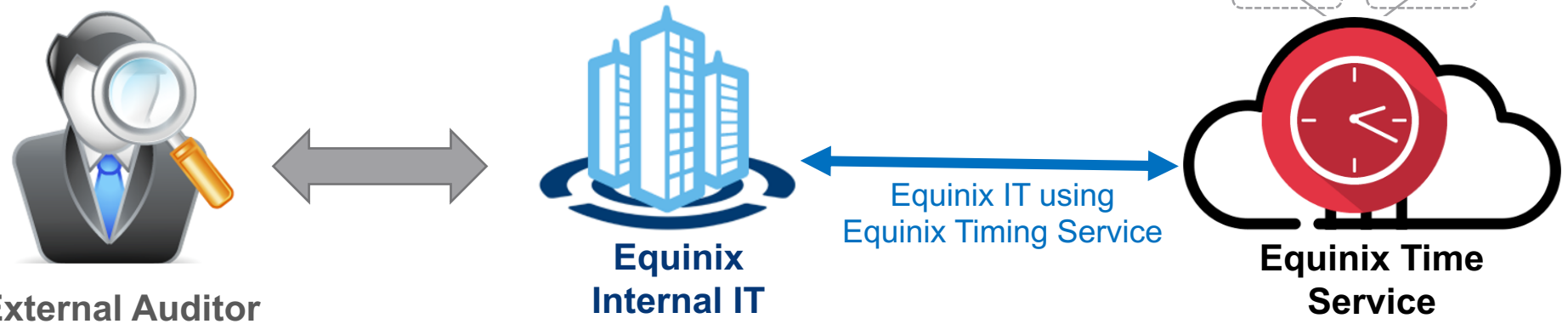
Motivation

MiFID II and FINRA Compliance

Metrological **traceability** requires an **unbroken chain** of calibrations that relate to a reference, with each calibration having a documented measurement uncertainty. In the field of time and frequency metrology, the desired reference is usually Coordinated Universal Time (UTC), or one or more of its official realizations, termed UTC(k), and traceability to UTC is a legal requirement for many entities.

> *"NIST Paper on "Metrological and legal traceability of time signals"*





Logging in Time Synchronization

Identify 01
Security incidents, events, information

Monitor 02
Usage, policy violations

Perform 03
Functional requirements, performance requirements

Incident investigation 04
Provide application specific information

Analyze 05
Behavior, predict capacity

Auditing 06
Trace, deeper insights, compliance

Traceability: Thread Model

Actor	Threat	Classification
System administrator (SaaS provider)	Has direct and at times physical access to the log information, storage. Can steal, modify or destroy logs without any evidence for any or all tenants.	Insider attack
Customer (User)	May have unrestricted access to logs which may contain sensitive information.	
Hacker (Outsider)	Hijack logging, falsify behavior or pretend as a logger.	Man in the middle
Auditor (Outsider too?)	Can access information not relevant to auditing.	

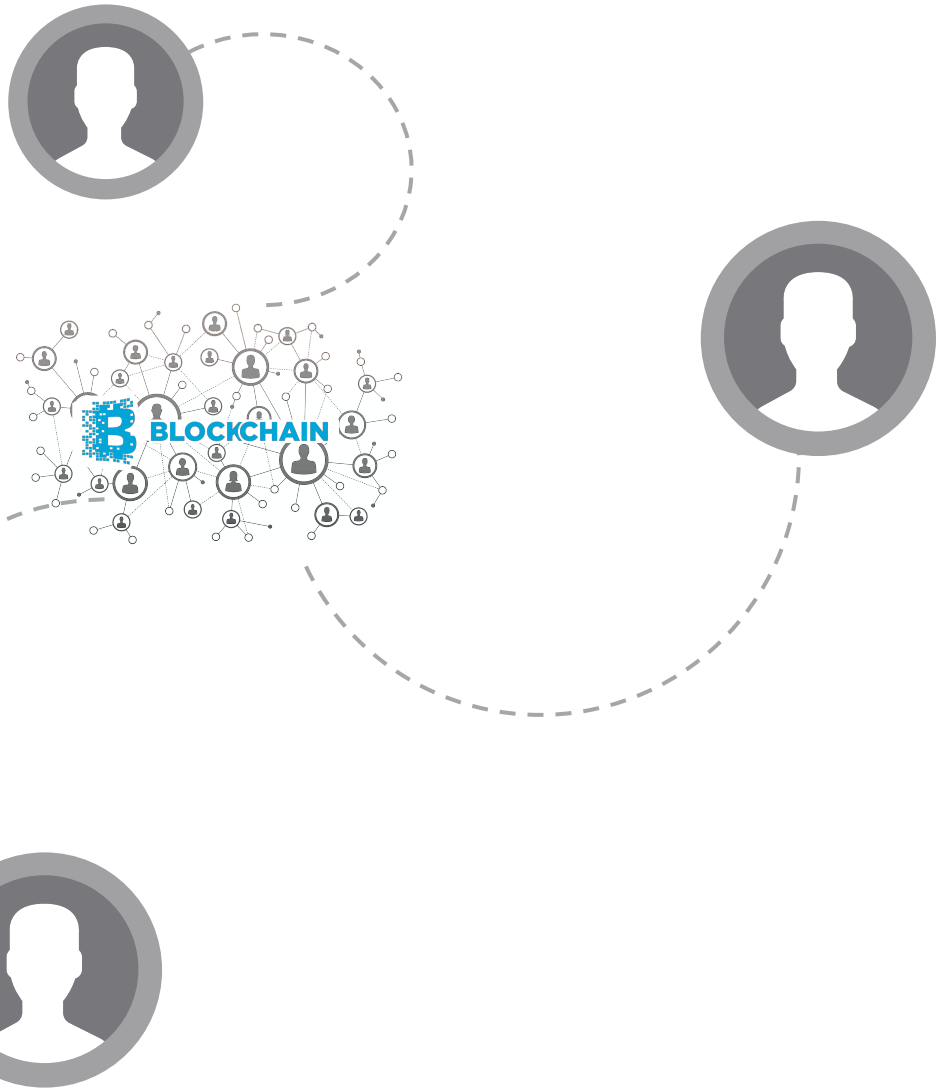
Challenges to Traceability with Today's Logging Systems

Challenges w/ Various Logging Systems	File System Logging	Database Logging	Centralized Logging
Identity Spoofing	Low	Low	High
Decentralization	No	No	No
Access Restriction	Limited	Limited	Low
Spying, Stealing, Sabotage	Easy	Medium	Medium
Auditability	Easy	Depends on Schema design	Very Hard
Performance	Fast with small log file size Slow with huge log file size	Slow with small data Fast with huge data	Slow

Blockchain Structure

Blocks

Blocks hold batches of valid transactions that are hashed and encoded, blocks linked to form a chain



Decentralization

peer-to-peer network, no central point of failure, massive replication

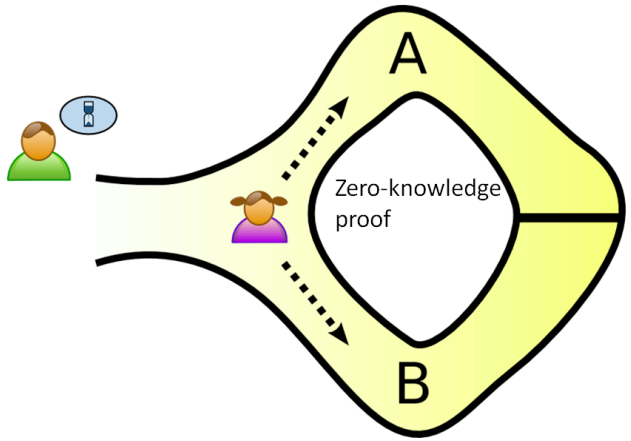
Immutable

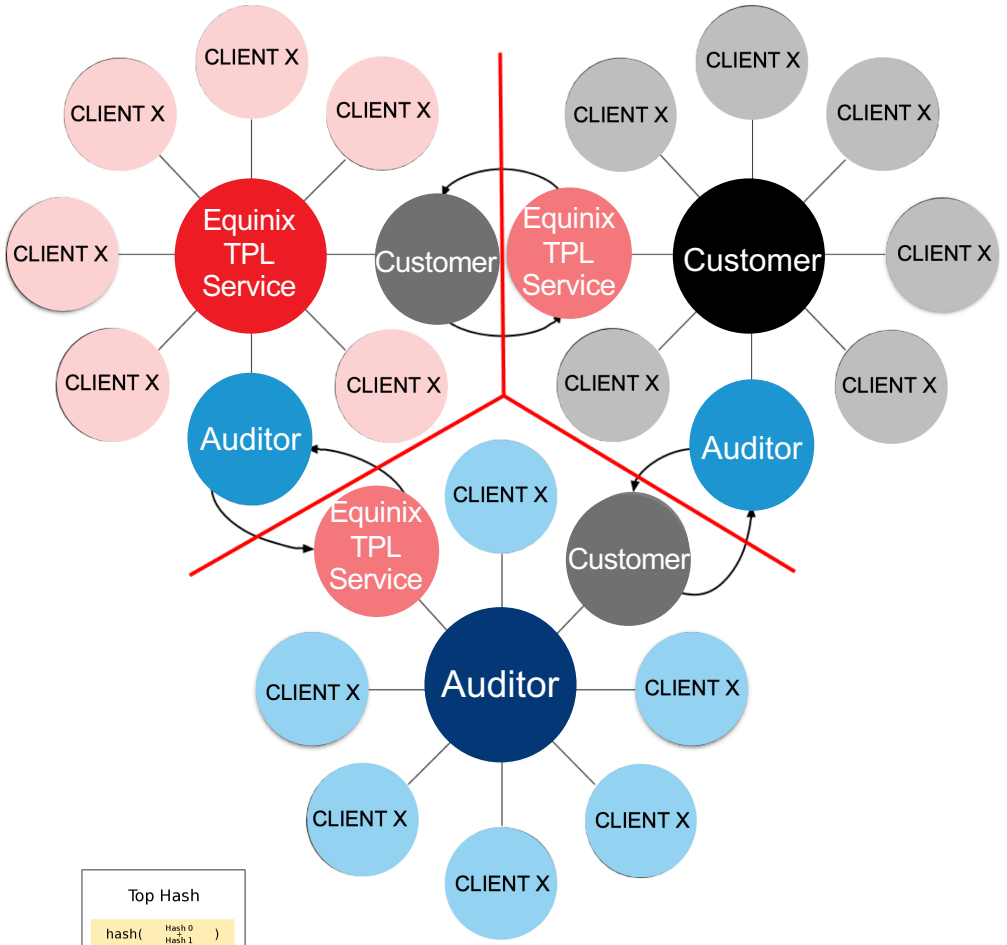
Self auditable, Blockchains can be open

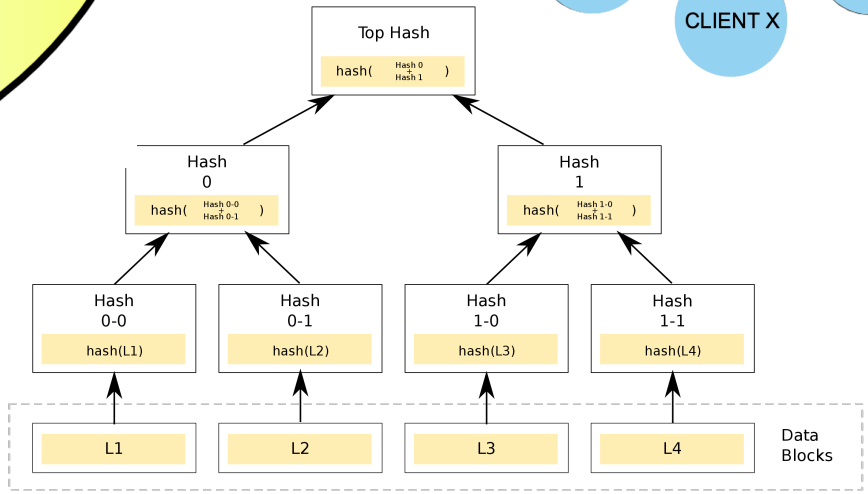
Blockchain to the Rescue

HYPERLEDGER FABRIC + HYPERLEDGER INDY

- **Decentralized identity management**: Globally unique identifiers that are created by their owner, independent of any central authority
  - Used by Indy to create a connection between two endpoints
  - Every identity stores their DIDs on their own secure wallet
- **Verifiable**
- **Immutable**
- Access Management
- SaaS consumable over APIs
- **Zero Knowledge Proofs**
- Public Permissioned Blockchain
- Ledger: Merkle Tree Design
- Scalable
- **Highly Available**

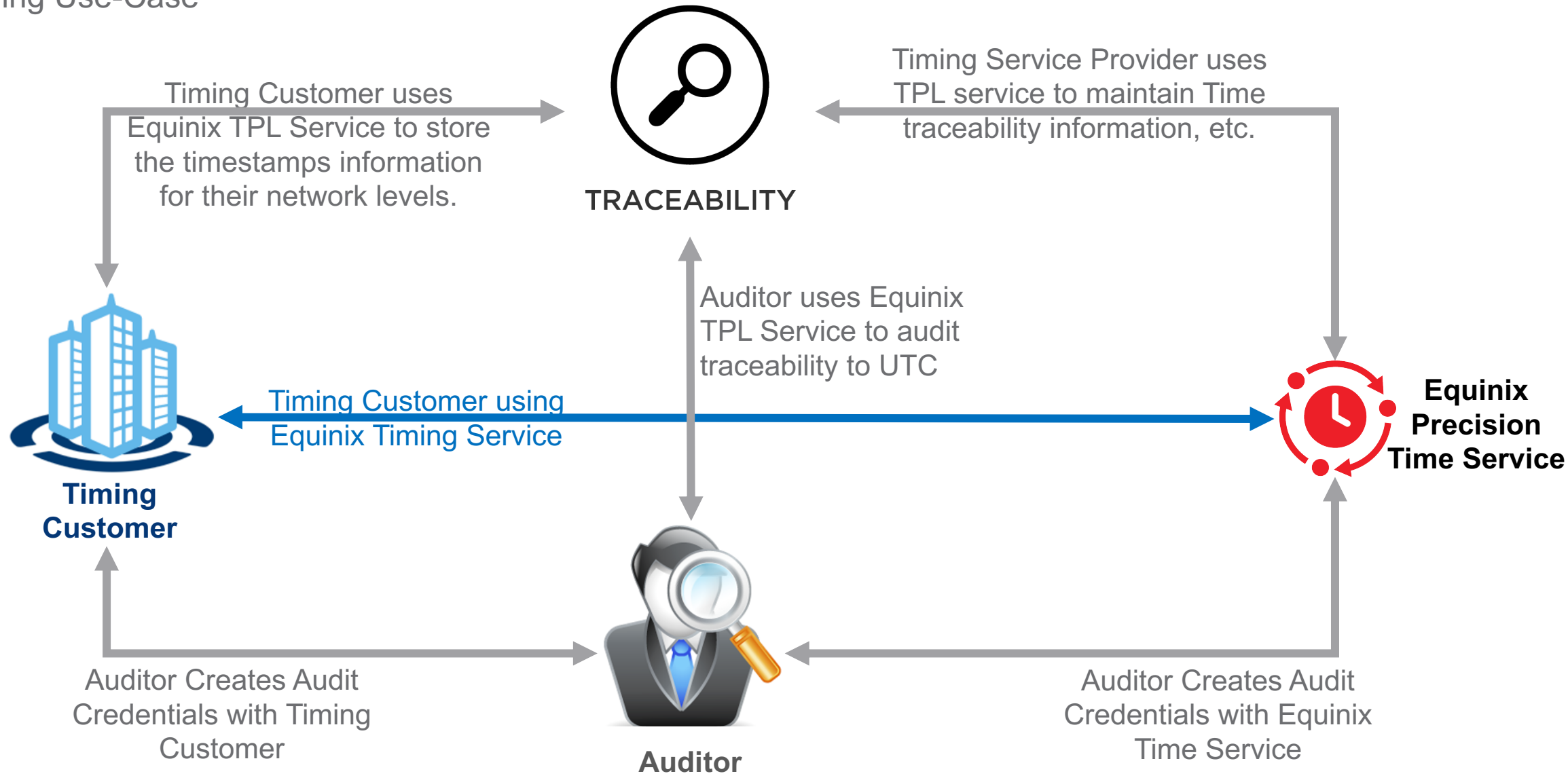






Traceability in Action

Timing Use-Case



Invitation to Participate

Hyperledger Loggy

Open source project, purpose built Hyperledger for logging.

Meetup

Blockchain and Ledger Technology Forum

Partner

Third party verification.

References

https://owasp.org/www-project-cheat-sheets/cheatsheets/Logging_Cheat_Sheet.html

https://web.stanford.edu/~ouster/cgi-bin/papers/lfs.pdf

https://en.wikipedia.org/wiki/List_of_log-structured_file_systems

https://www.hyperledger.org/projects/hyperledger-indy

https://tf.nist.gov/general/pdf/2941.pdf

EQUINIX

WHERE OPPORTUNITY CONNECTS