Detecting Blockchain Security Threats

2020 IEEE International Conference on Blockchain

Benedikt Putz, Guenther Pernul – Chair of Information Systems - University of Regensburg

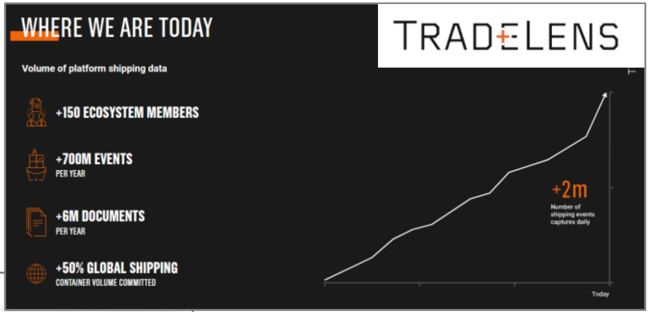
5 November 2020

Agenda

- Motivation
- Attacks and Threat Indicators
- Data Collection and Processing
- Evaluation and Future Work

DLT is used in production environments today

- **TradeLens platform**
  - 150 organizations
  - 50% global shipping volume
- **IBM Food Trust**
  - Walmart, Carrefour, Albertsons,…
  - Mandated for many Walmart suppliers
  - Tracking a range of fresh produce, premium products
- **We.Trade**
  - 16 banks in 15 countries
  - > € 50M transaction value



WHERE WE ARE TODAY

TRADELENS

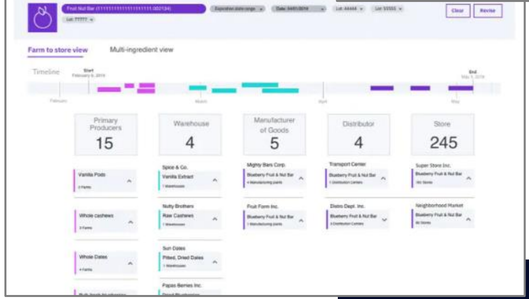
Volume of platform shipping data

+150 ECOSYSTEM MEMBERS

+700M EVENTS PER YEAR

+6M DOCUMENTS PER YEAR

+50% GLOBAL SHIPPING CONTAINER VOLUME COMMITTED



IBM Food Trust™ Trace

Farm to store view | Multi-ingredient view

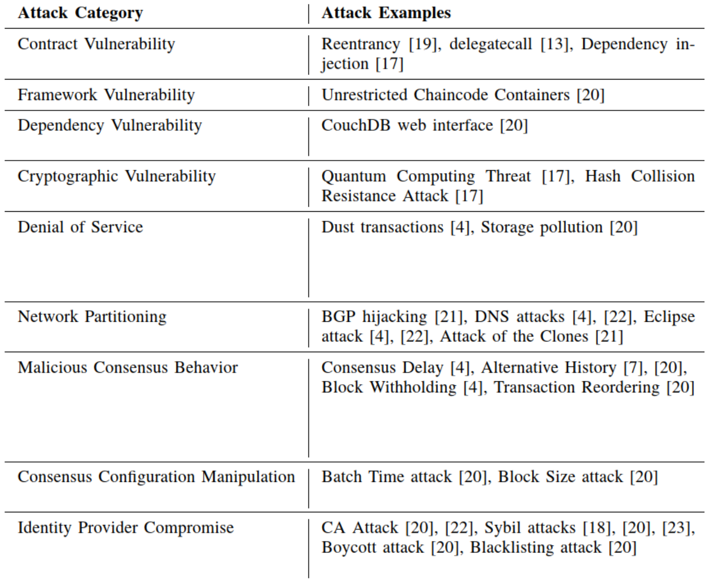
Primary Producers	Warehouse	Manufacturer of Goods	Distributor	Store
15	4	5	4	245

HYPERLEDGER FABRIC

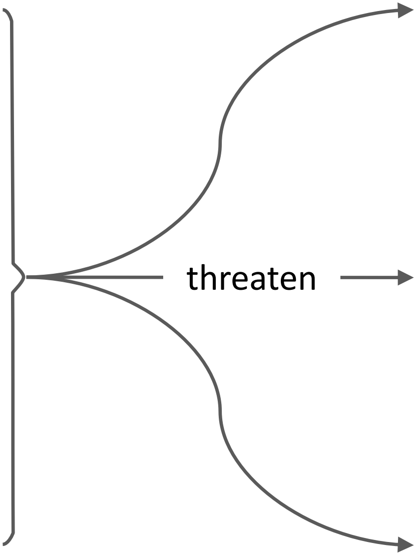
we.trade
more trust. more trade.

Thus, information security of DLT assets is critical

DLT Threats



Attack Category	Attack Examples
Contract Vulnerability	Reentrancy [19], delegatecall [13], Dependency injection [17]
Framework Vulnerability	Unrestricted Chaincode Containers [20]
Dependency Vulnerability	CouchDB web interface [20]
Cryptographic Vulnerability	Quantum Computing Threat [17], Hash Collision Resistance Attack [17]
Denial of Service	Dust transactions [4], Storage pollution [20]
Network Partitioning	BGP hijacking [21], DNS attacks [4], [22], Eclipse attack [4], [22], Attack of the Clones [21]
Malicious Consensus Behavior	Consensus Delay [4], Alternative History [7], [20], Block Withholding [4], Transaction Reordering [20]
Consensus Configuration Manipulation	Batch Time attack [20], Block Size attack [20]
Identity Provider Compromise	CA Attack [20], [22], Sybil attacks [18], [20], [23], Boycott attack [20], Blacklisting attack [20]



Availability

- Tracked assets might be lost
- Users cannot retrieve provenance trail
- No transfers possible

Integrity

- DLT is relied on as a source of truth
- Corrupted data may have expensive consequences due to high value assets

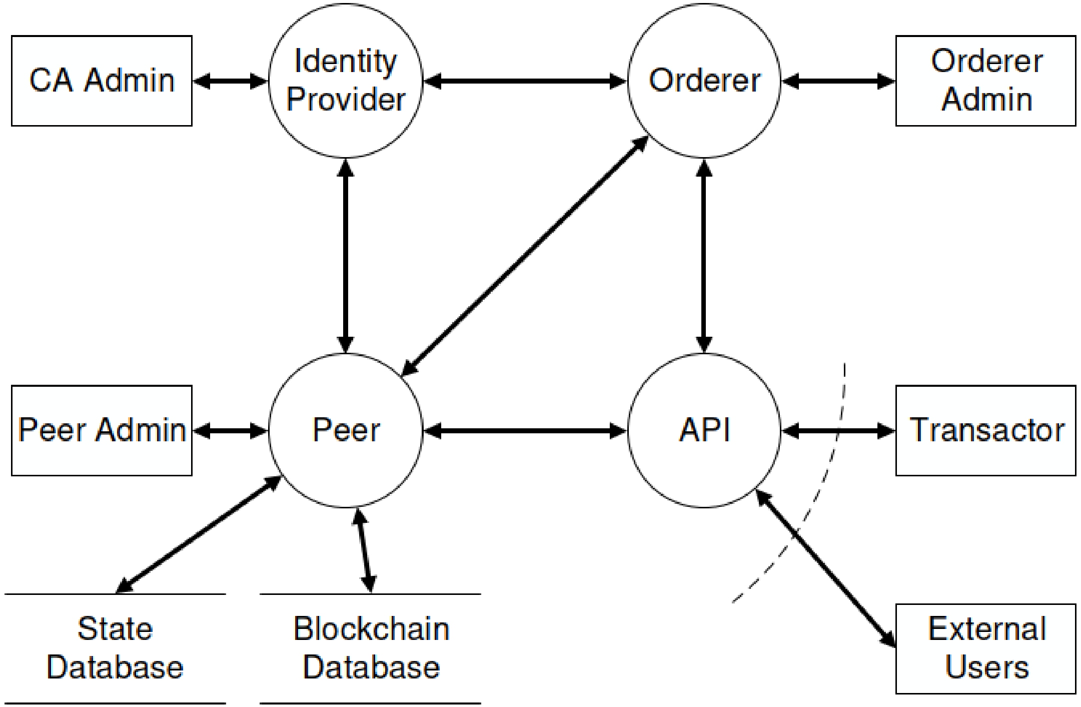
Confidentiality

- Supply chain internals may be leaked
- Transaction participant privacy

Agenda

- Motivation
- Attacks and Threat Indicators
- Data Collection and Processing
- Evaluation and Future Work

Threat Model - Actors



Threat Model – Attack Vectors

Vulnerabilities

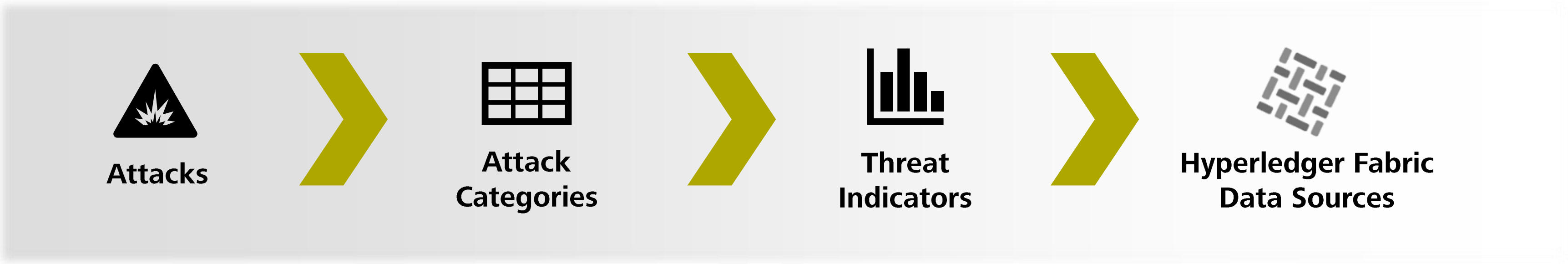
- **Protocol vulnerabilities**
  - Framework implementation bugs (see Hyperledger JIRA, Fabric pen-tests)
  - Framework dependency implementation issues (gRPC, CouchDB)
- **Contract vulnerabilities**
  - DLT-specific bugs (i.e. read-after-write)
  - External dependency vulnerability
- **Misconfiguration**
  - Unsafe defaults
  - Deployment mistakes

Malicious Intent

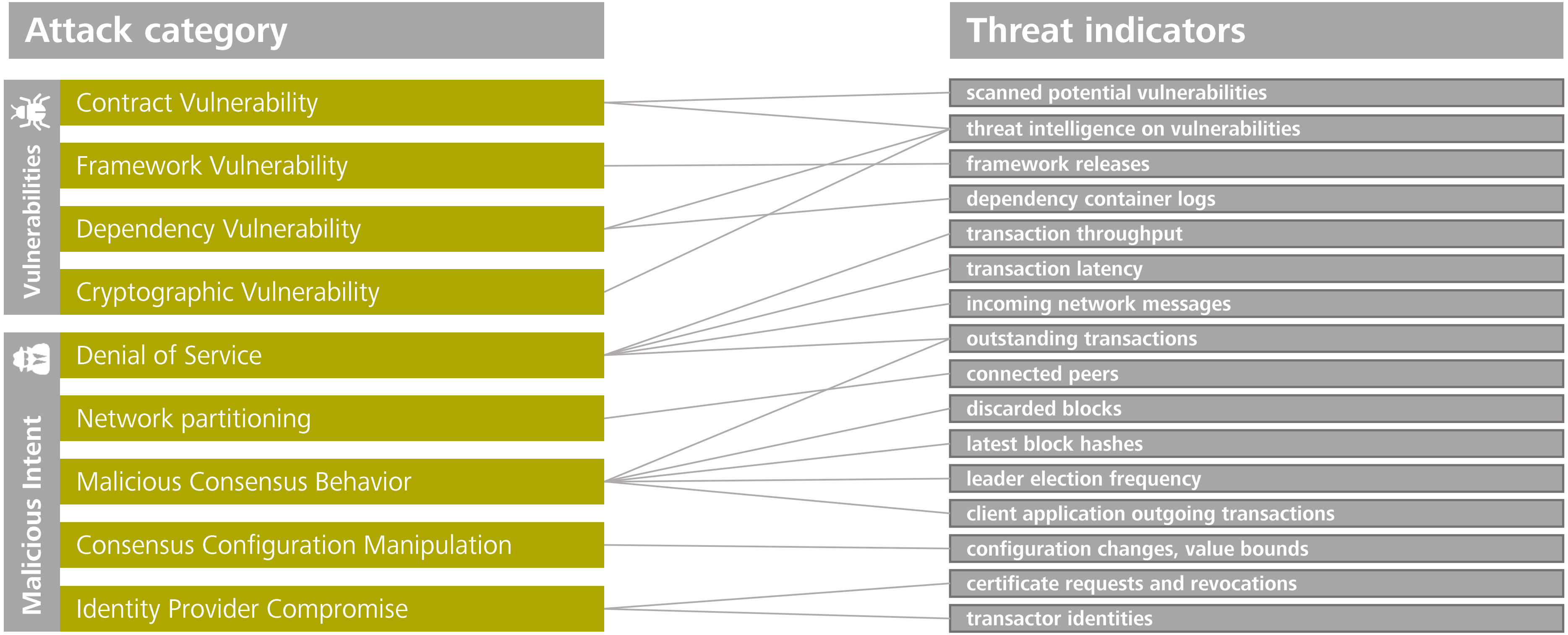
- **Internal threats**
  - Insiders are dangerous, especially with administrative powers
  - Single insider may affect the entire DLT network
- **External threats**
  - main threat to confidentiality
  - traditional network attacks still apply (DDoS)
  - attack surface is increased by every organization that participates

Methodology

- **Literature survey** on threats to permissioned blockchains yields list of **Attacks**
- Determine **Attack Categories** based on **Attacks** and **Threat Model**
- Map Attack Categories to **Threat Indicators**
- Evaluate threat indicators by checking available **Hyperledger Fabric Data Sources**



Threat Indicator Mapping



Attack category

Vulnerabilities

Contract Vulnerability

Framework Vulnerability

Dependency Vulnerability

Cryptographic Vulnerability

Malicious Intent

Denial of Service

Network partitioning

Malicious Consensus Behavior

Consensus Configuration Manipulation

Identity Provider Compromise

Threat indicators

scanned potential vulnerabilities

threat intelligence on vulnerabilities

framework releases

dependency container logs

transaction throughput

transaction latency

incoming network messages

outstanding transactions

connected peers

discarded blocks

latest block hashes

leader election frequency

client application outgoing transactions

configuration changes, value bounds

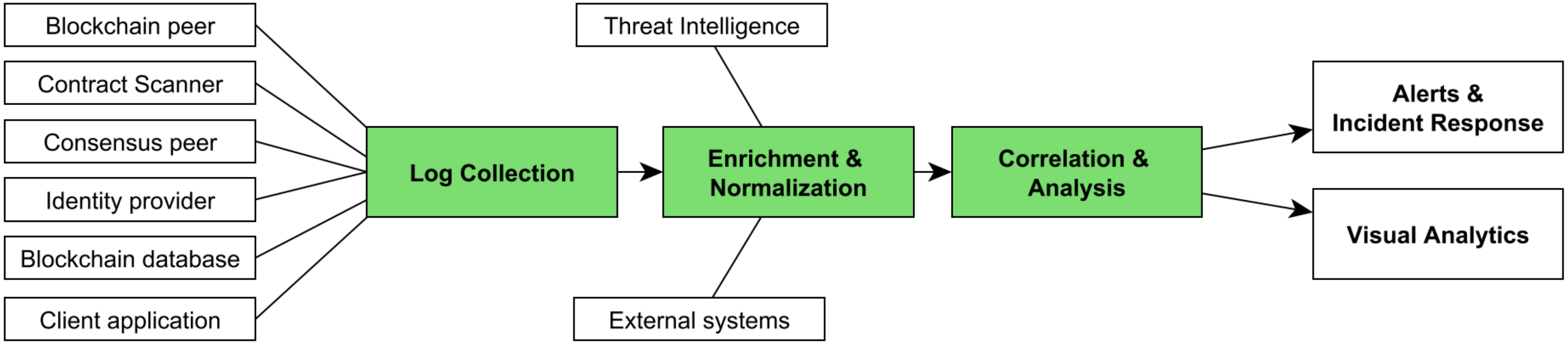
certificate requests and revocations

transactor identities

Agenda

- Motivation
- Attacks and Threat Indicators
- Data Collection and Processing
- Evaluation and Future Work

Data Processing Steps

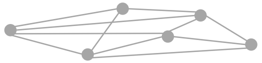


Log Collection

Data Source	Available Data
HYPERLEDGER FABRIC **Client SDK**	– Block and Transaction Subscription – Channel events
docker **Container Logs**	– Fabric-CA logs – Peer logs – Orderer logs
Prometheus statsd	– Chaincode container execution metrics – Peer metrics – Orderer metrics

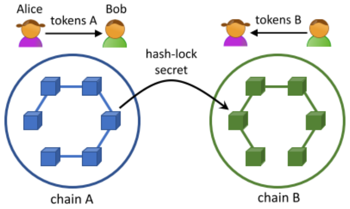
Enrichment & Normalization

- **Other peers/orderers in the network**



- **Threat intelligence**

- **Permissionless blockchain anchoring**
  - validity of the anchoring chain must be monitored
- **Oracles**
  - monitor data from external sources for anomalies
- **Cross-chain interactions**
  - status of asset swaps, reclaiming failed swaps



- **Off-chain storage**
  - monitor availability & integrity

Agenda

- Motivation
- Attacks and Threat Indicators
- Data Collection and Processing
- Evaluation and Future Work

Detection Approach (1/4)

Threat Indicator	Data	Source (for Hyperledger Fabric)	Status
Scanned potential vulnerabilities	Security scanner logs, but lack of good scanners	ChainCode Scanner Go/JS security tools	⊖
Threat intelligence on vulnerabilities	Threat intelligence feeds Structured data (CVE, STIX)	Generic feeds, i.e. cve.mitre.org	⚠
Framework releases	Release notes	GitHub Repository Releases (other sources outdated)	✓
Dependency Container Logs	IP addresses, Request URI	CouchDB	✓
Transaction throughput	Processed transaction count	Orderer Metrics	✓

Detection Approach (2/4)

Threat Indicator	Data	Source (for Hyperledger Fabric)	Status
Transaction latency	Transaction/Block timestamps	SDK Channel Block Event subscription	✓
Incoming network messages	Peer gossip and gRPC metrics	Peer metrics	✓
Outstanding transactions	Unavailable, block fill duration as closest proxy	Orderer metrics	⊖
Connected Peers	Outgoing connections	Peer & Orderer metrics	✓
Discarded Blocks	Blocks from ordering service that fail validation	Peer container logs (requires preprocessing)	⚠

Detection Approach (3/4)

Threat Indicator	Data	Source (for Hyperledger Fabric)	Status
Latest block hashes	Block headers	SDK Channel Block Event subscription	✓
Leader election frequency	Leader elections in consensus	Orderer metrics, logs (new leader) None for failed elections	⚠
Client app outgoing transactions	Track outgoing transactions in client app	SDK	✓
Configuration changes	Proposed and successful CONFIG_UPDATE transactions	Orderer Metrics SDK Channel Block Event subscription	✓
Certificate requests and revocations	CA enroll requests	CA container logs	✓

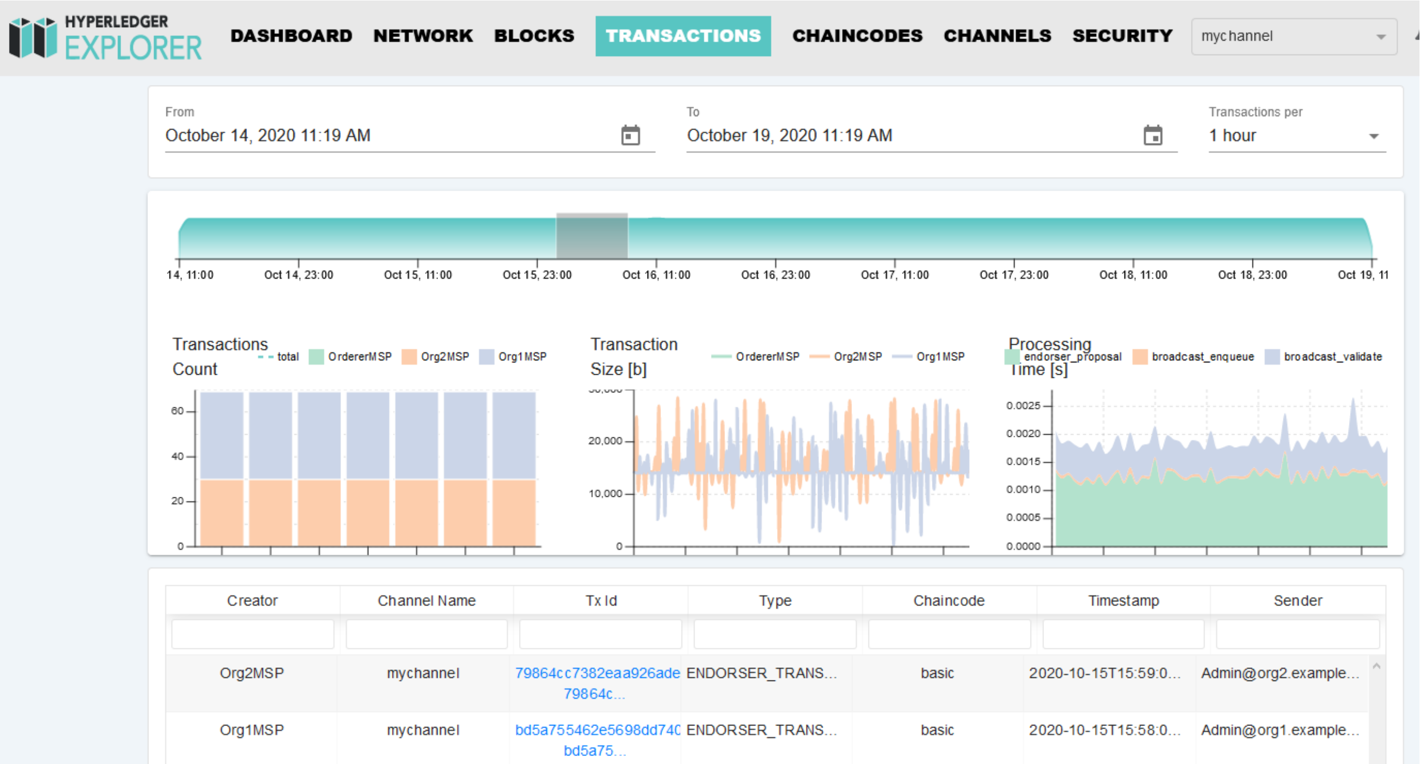
Detection Approach (4/4)

Threat Indicator	Data	Source (for Hyperledger Fabric)	Status
Transactor identities	Transaction headers (signature)	SDK Channel Block Event subscription	✓

Indicator Data Availability Summary:

- ✓ 11
- ⚠ 3
- ⊖ 2

Future Work



From
October 14, 2020 11:19 AM

To
October 19, 2020 11:19 AM

Transactions per
1 hour

Creator	Channel Name	Tx Id	Type	Chaincode	Timestamp	Sender
Org2MSP	mychannel	79864cc7382eaa926ade 79864c...	ENDORSER_TRANS...	basic	2020-10-15T15:59:0...	Admin@org2.example...
Org1MSP	mychannel	bd5a755462e5698dd74C bd5a75...	ENDORSER_TRANS...	basic	2020-10-15T15:58:0...	Admin@org1.example...

Thank you for your attention.

Questions, comments, criticism?