SECURING PROCESS CONTROL DATA TRANSMISSION TO THE BLOCKCHAIN NETWORK

Lloyd Kenneth Tugbo & Chimmy Arian Hilis

Who are we?

Khen Tugbo

- Automation, Instrumentation and Control, and Systems Security
- A SAFe Certified Architect
- Software Security Engineer for hybrid technologies like Distributed Control Systems and SCADA.

Chimmy Hilis

- ICS Cybersecurity
- Vulnerability Management and Application Security
- Software Security Engineer

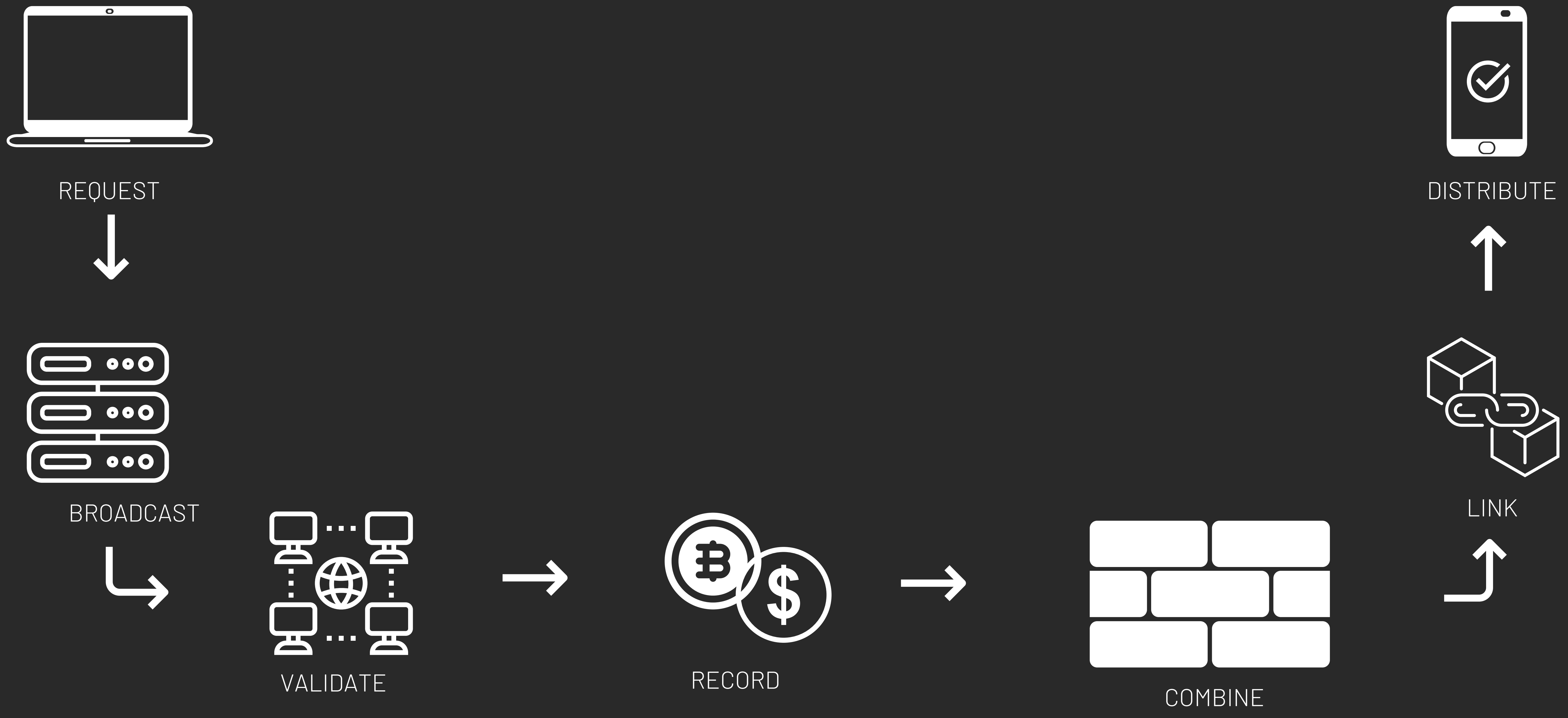
Overview

- Blockchain Demystified
- ICS Acceptance Criteria
- Sending data from L0 to L3
- L3 integration to the Blockchain Network
- Ideal Solution
- Blockchain Security Framework

Blockchain Demystified

Is Blockchain Overhyped?

HOW BLOCKCHAIN TECHNOLOGY WORKS



REQUEST

BROADCAST

VALIDATE

RECORD

COMBINE

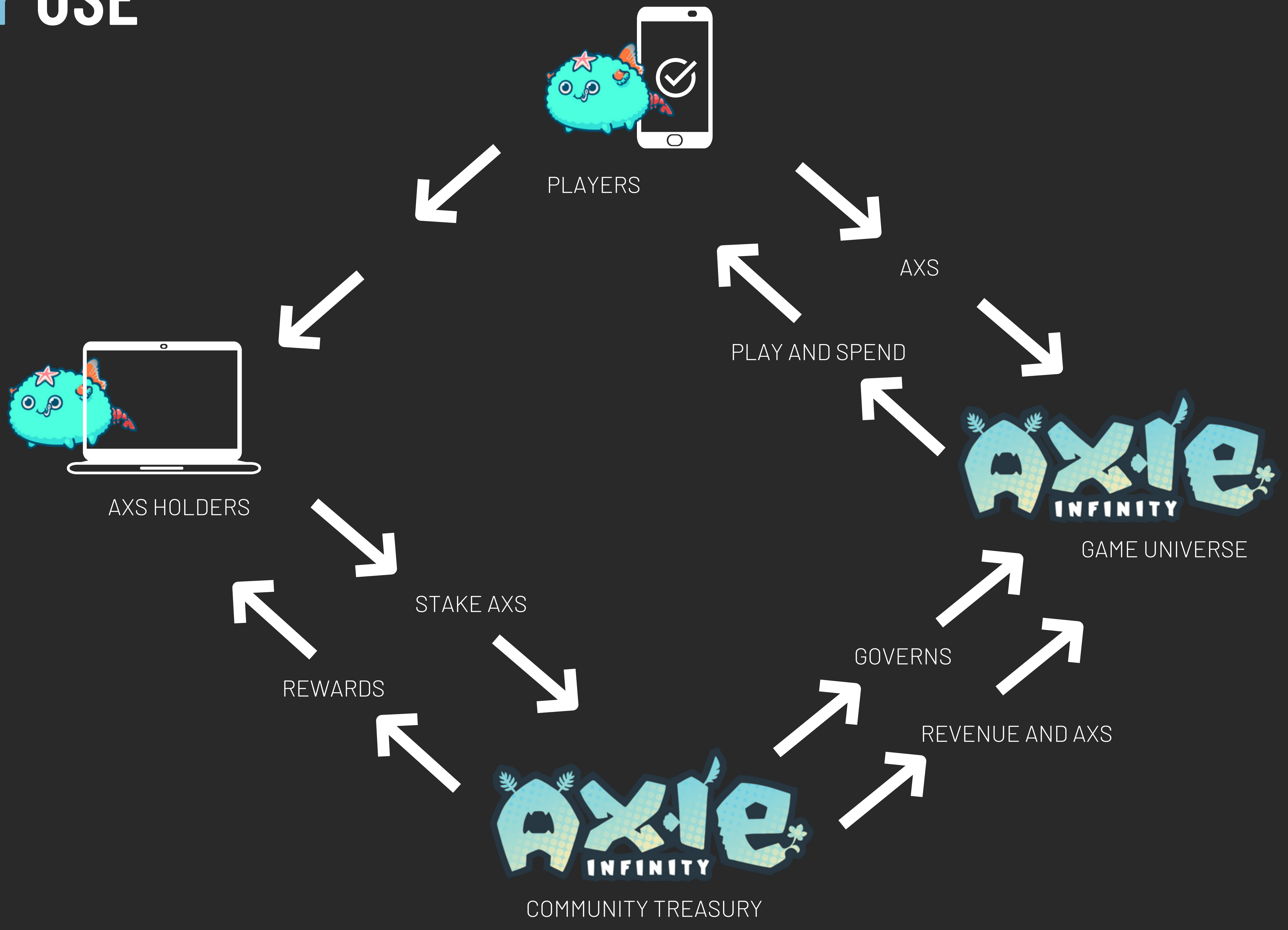
LINK

DISTRIBUTE

Source:https://medium.com/@ipspecialist/how-blockchain-technology-works-e6109c033034

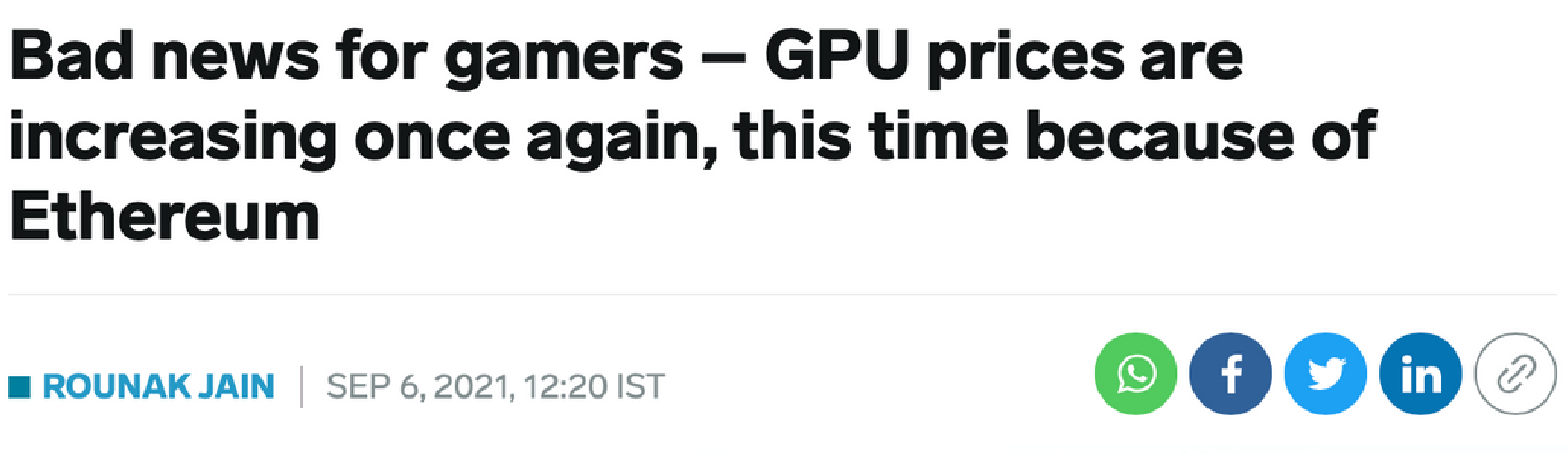
BLOCKCHAIN TECHNOLOGY USE CASES FOR AXIE INFINTY

- GOVERNANCE
- STAKING
- PAYMENT



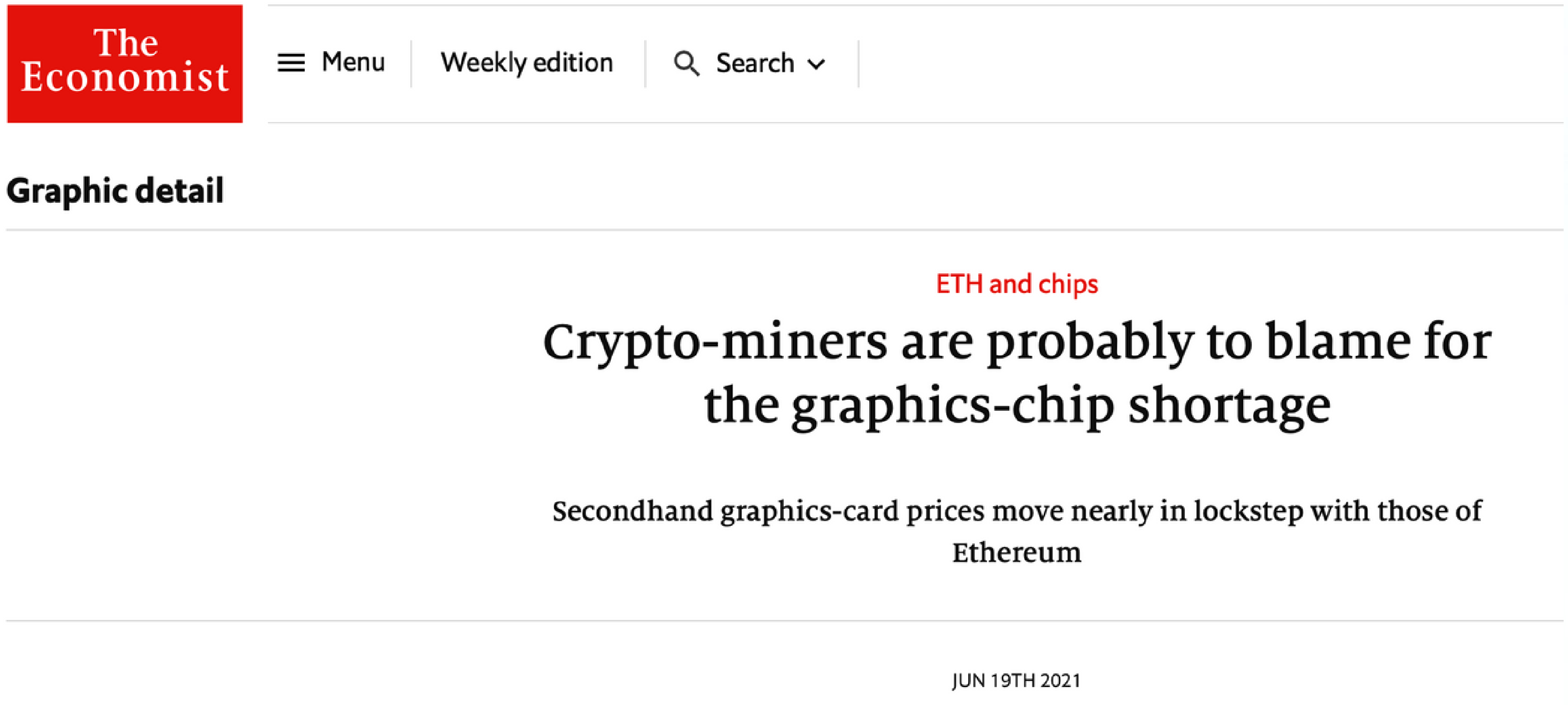
Source:https://whitepaper.axieinfinity.com/axs

GPU PRICE HIKE



Bad news for gamers – GPU prices are increasing once again, this time because of Ethereum

ROUNAK JAIN | SEP 6, 2021, 12:20 IST



The Economist

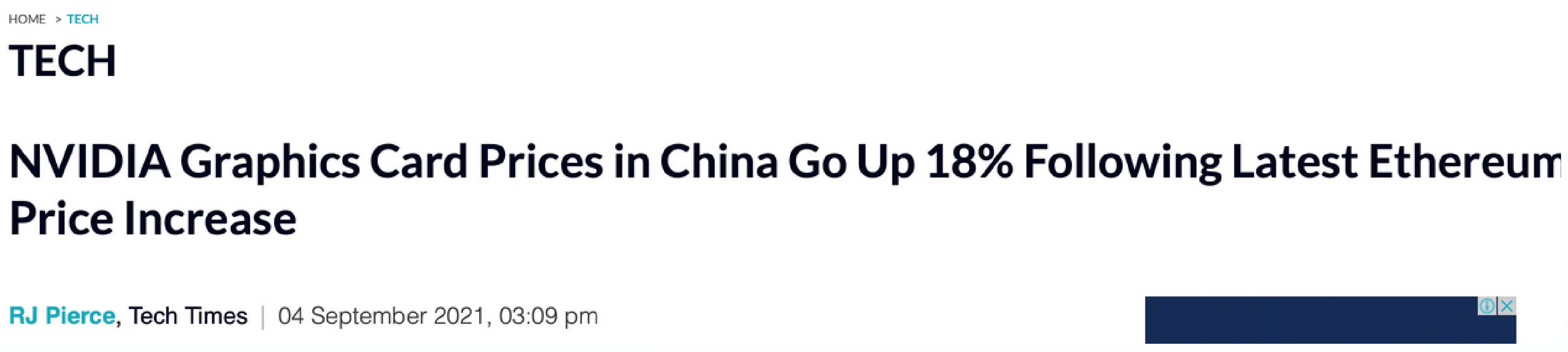
Graphic detail

ETH and chips

Crypto-miners are probably to blame for the graphics-chip shortage

Secondhand graphics-card prices move nearly in lockstep with those of Ethereum

JUN 19TH 2021

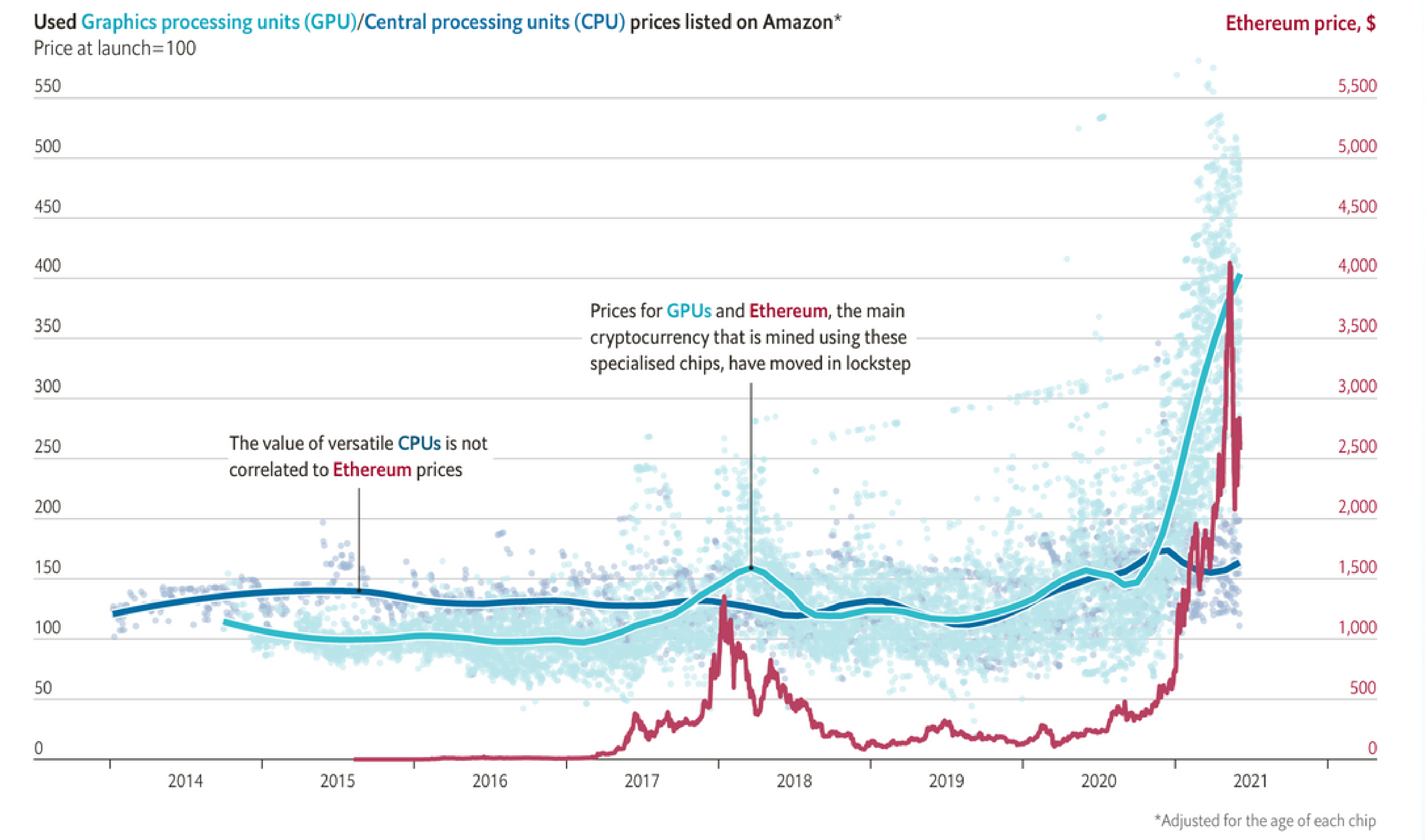


HOME > TECH

TECH

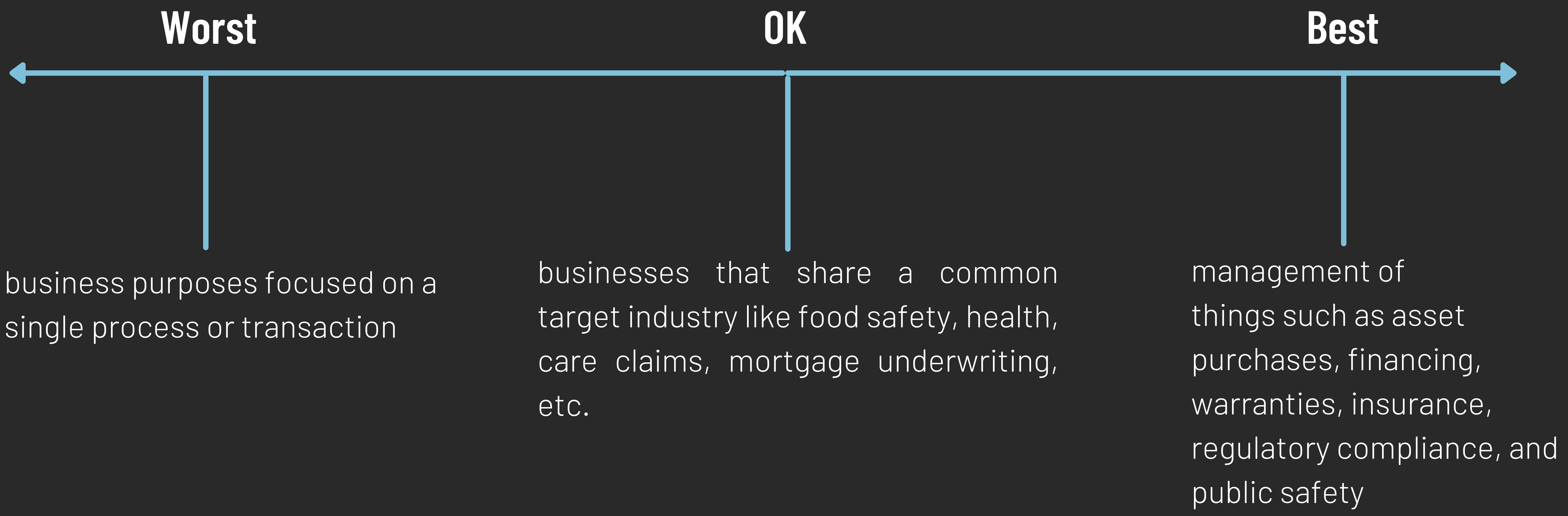
NVIDIA Graphics Card Prices in China Go Up 18% Following Latest Ethereum Price Increase

RJ Pierce, Tech Times | 04 September 2021, 03:09 pm



Source https://www.businessinsider.in/tech/news/bad-news-for-gamers-gpu-prices-are-increasing-once-again-this-time-because-of-ethereum/articleshow/85968902.cmshttps://www.economist.com/graphic-detail/2021/06/19/crypto-miners-are-probably-to-blame-for-the-graphics-chip-shortage
https://www.techtimes.com/articles/265012/20210904/nvidia-gpu-price-increase.htm

BLOCKCHAIN TECHNOLOGY
PURPOSE



Worst

business purposes focused on a single process or transaction

OK

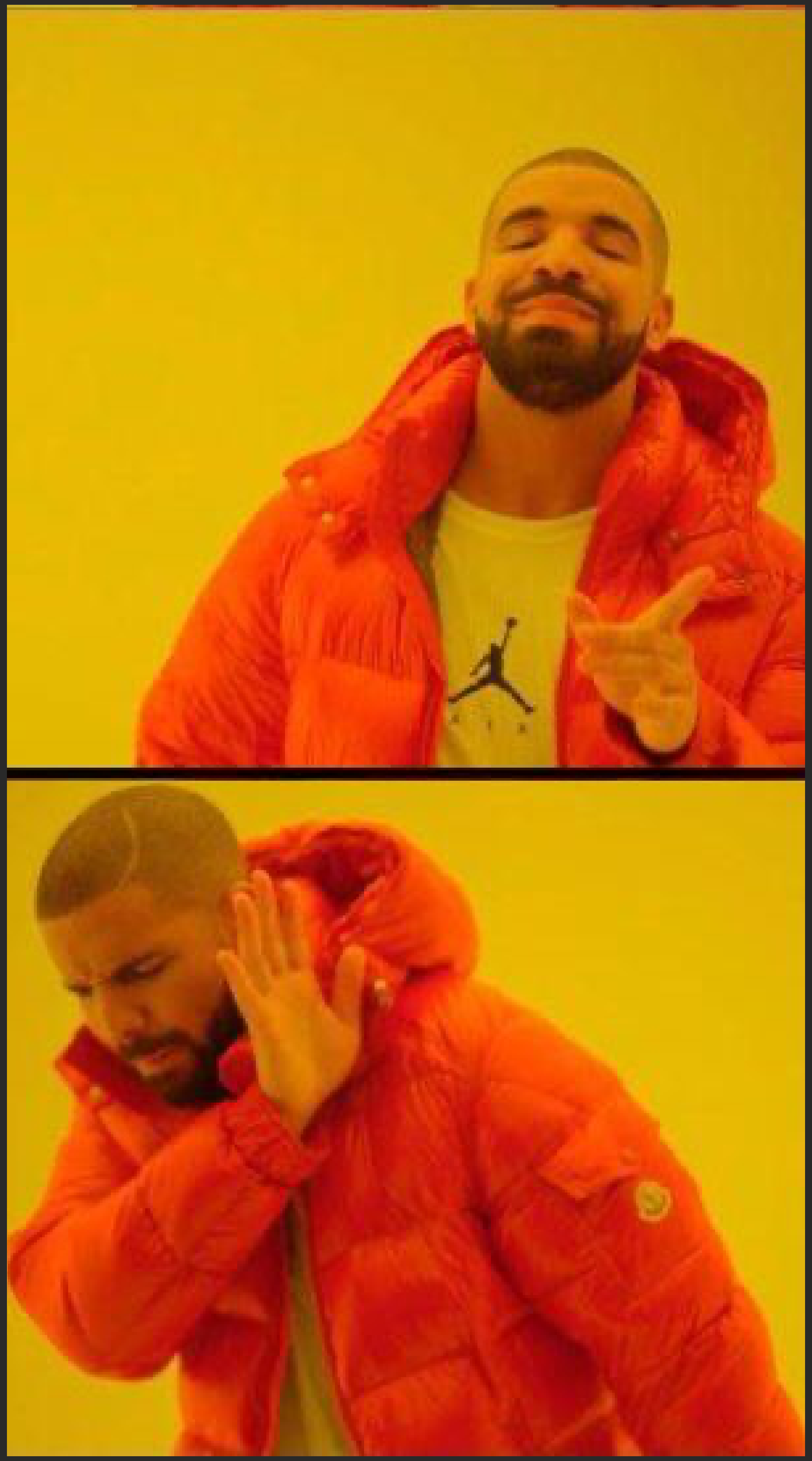
businesses that share a common target industry like food safety, health, care claims, mortgage underwriting, etc.

Best

management of things such as asset purchases, financing, warranties, insurance, regulatory compliance, and public safety

Source: Crunch Time IV - Blockchain for Finance, Deloitte 2018 | Dean Hobbs, Rich de Moll, David Griswold, Deloitte LLP.

BLOCKCHAIN TECHNOLOGY USE CASES



- Luxury Items and Art Selling
- Marriage
- Turkey's Origin

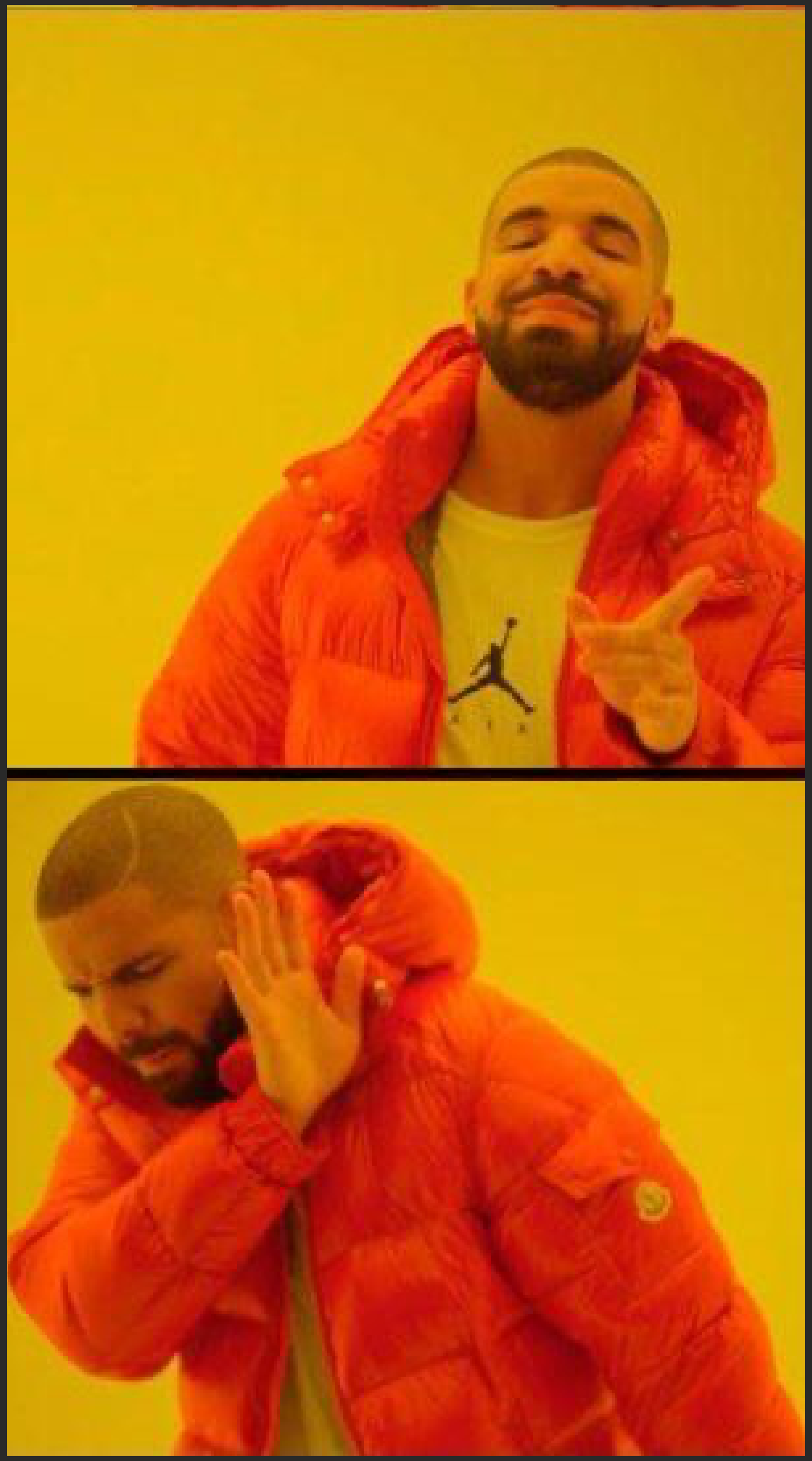
Industrial Control System

(DCS, SCADA)

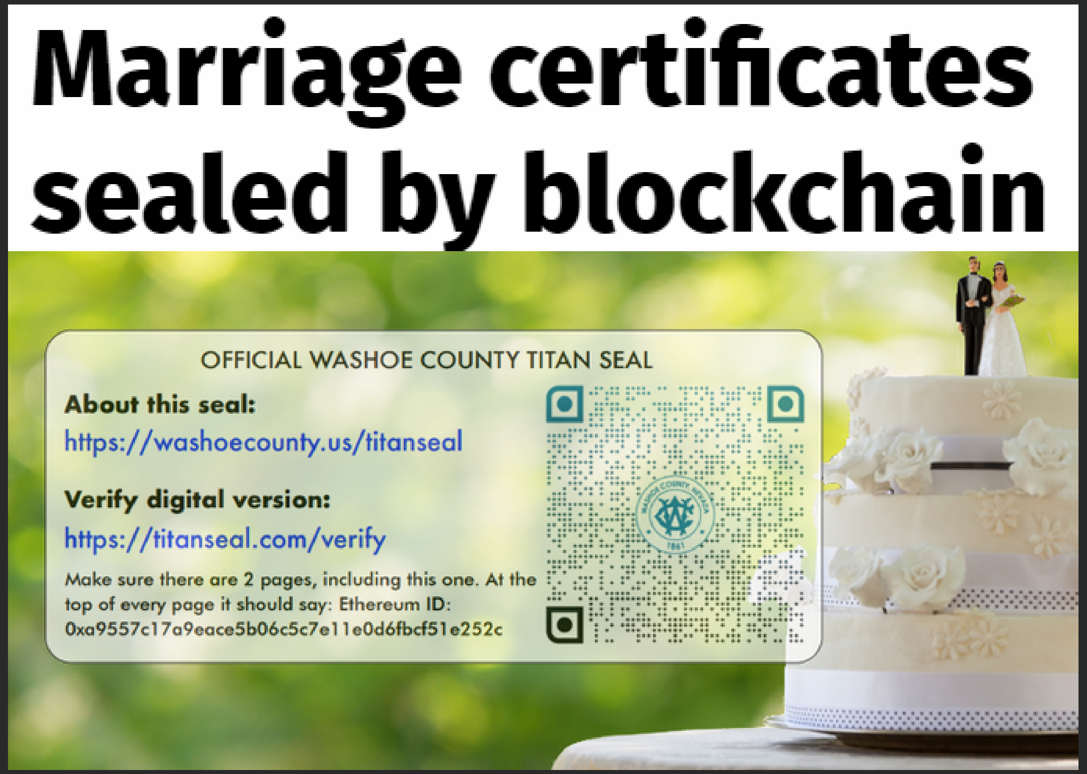
Steph Curry jumps into NFTs with $180,000 purchase of Bored Ape digital artwork

Image Source: https://imgflip.com/memetemplates and https://markets.businessinsider.com/news/currencies/steph-curry-nft-bored-ape-yacht-club-180000-ethereum-nba-2021-8?src=rss

BLOCKCHAIN TECHNOLOGY USE CASES



- Luxury Items and Art Selling
- Marriage
- Turkey's Origin



Marriage certificates sealed by blockchain

OFFICIAL WASHOE COUNTY TITAN SEAL

About this seal:
https://washoecounty.us/titanseal

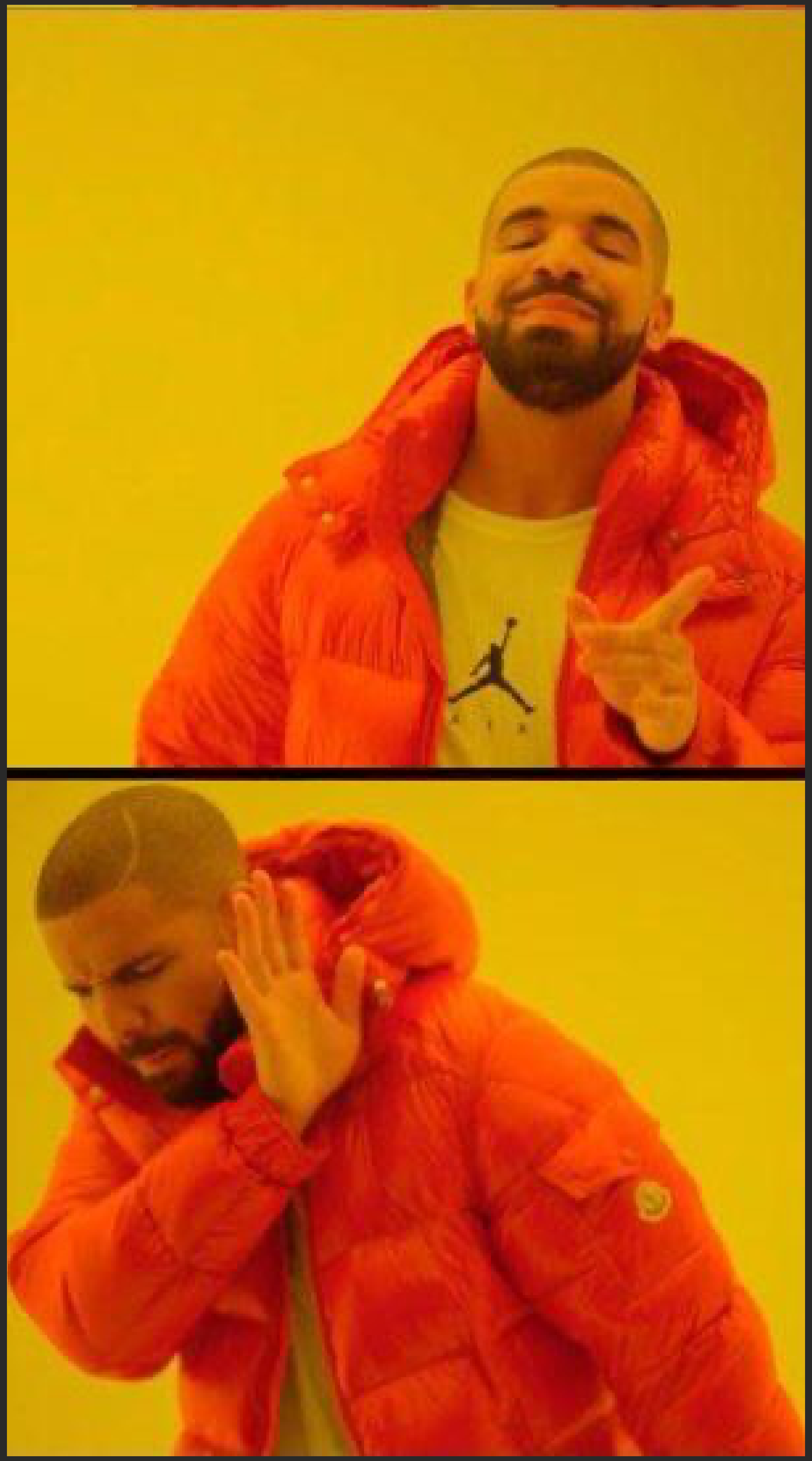
Verify digital version:
https://titanseal.com/verify

Make sure there are 2 pages, including this one. At the top of every page it should say: Ethereum ID: 0xa9557c17a9eace5b06c5c7e11e0d6fbcf51e252c

Industrial Control System
(DCS, SCADA)

Image Source: https://imgflip.com/memetemplates and https://gcn.com/articles/2019/01/17/marriage-certificates-blockchain.aspx

BLOCKCHAIN TECHNOLOGY USE CASES



- Luxury Items and Art Selling
- Marriage
- Turkey's Origin

Industrial Control System
(DCS, SCADA)

Cargill blockchain lets you get to know your Thanksgiving turkey

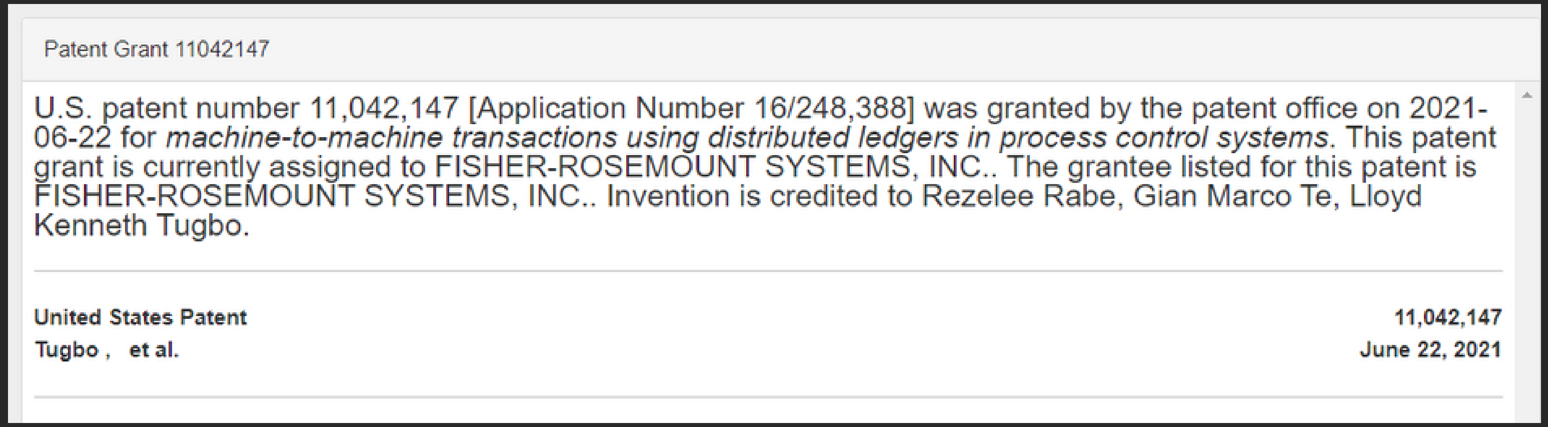
Image Source: https://imgflip.com/memetemplates and https://diginomica.com/cargill-blockchain-lets-get-know-thanksgiving-turkey

Blockchain Is Not The Solution To Every Problem

Will Industrial Control System benefit on Blockchain Technology Integration?

- Statefulness
- Assets
- Transactions
- Intermediaries
- Trust

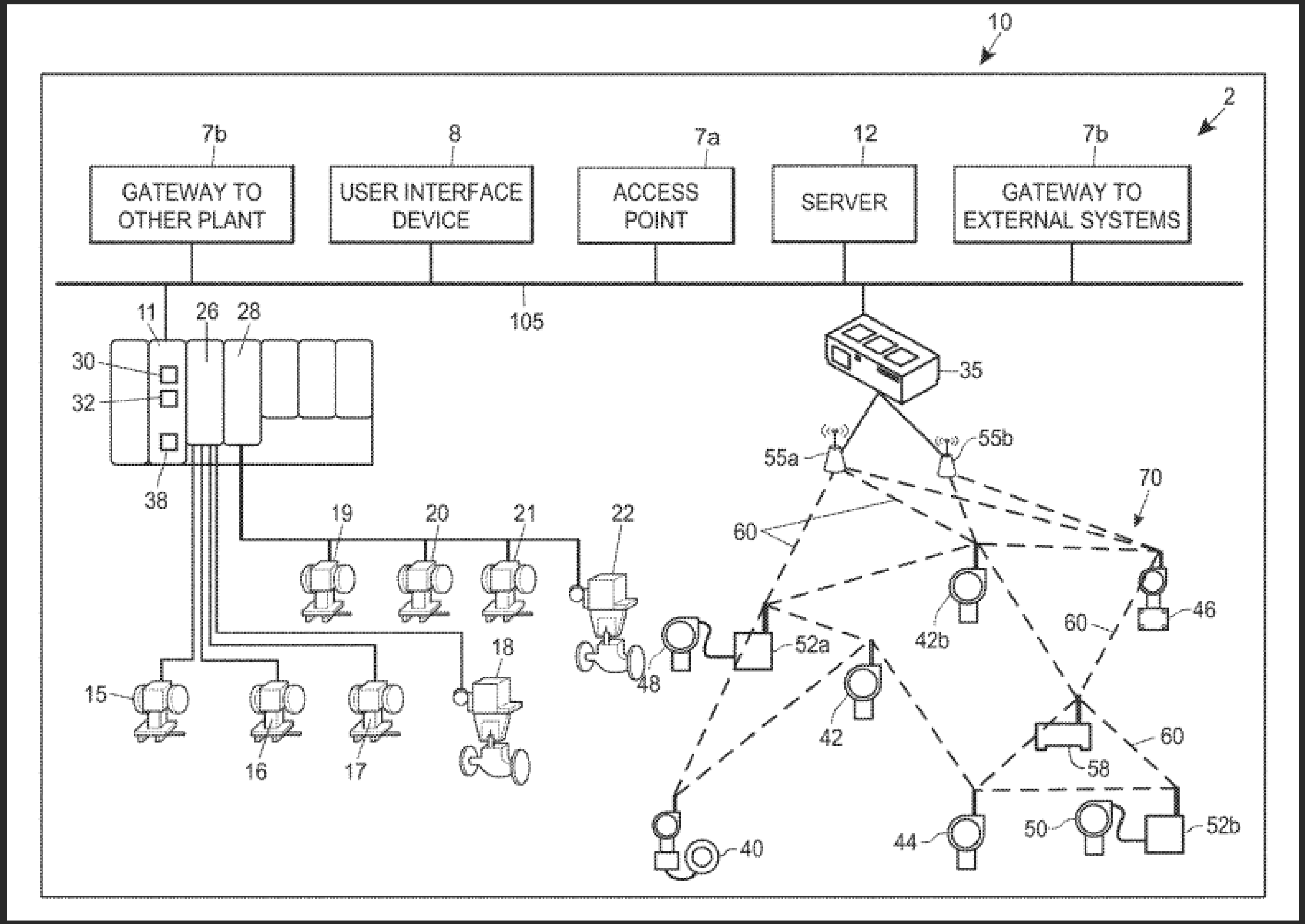
BLOCKCHAIN TECHNOLOGY USE CASE IN ICS



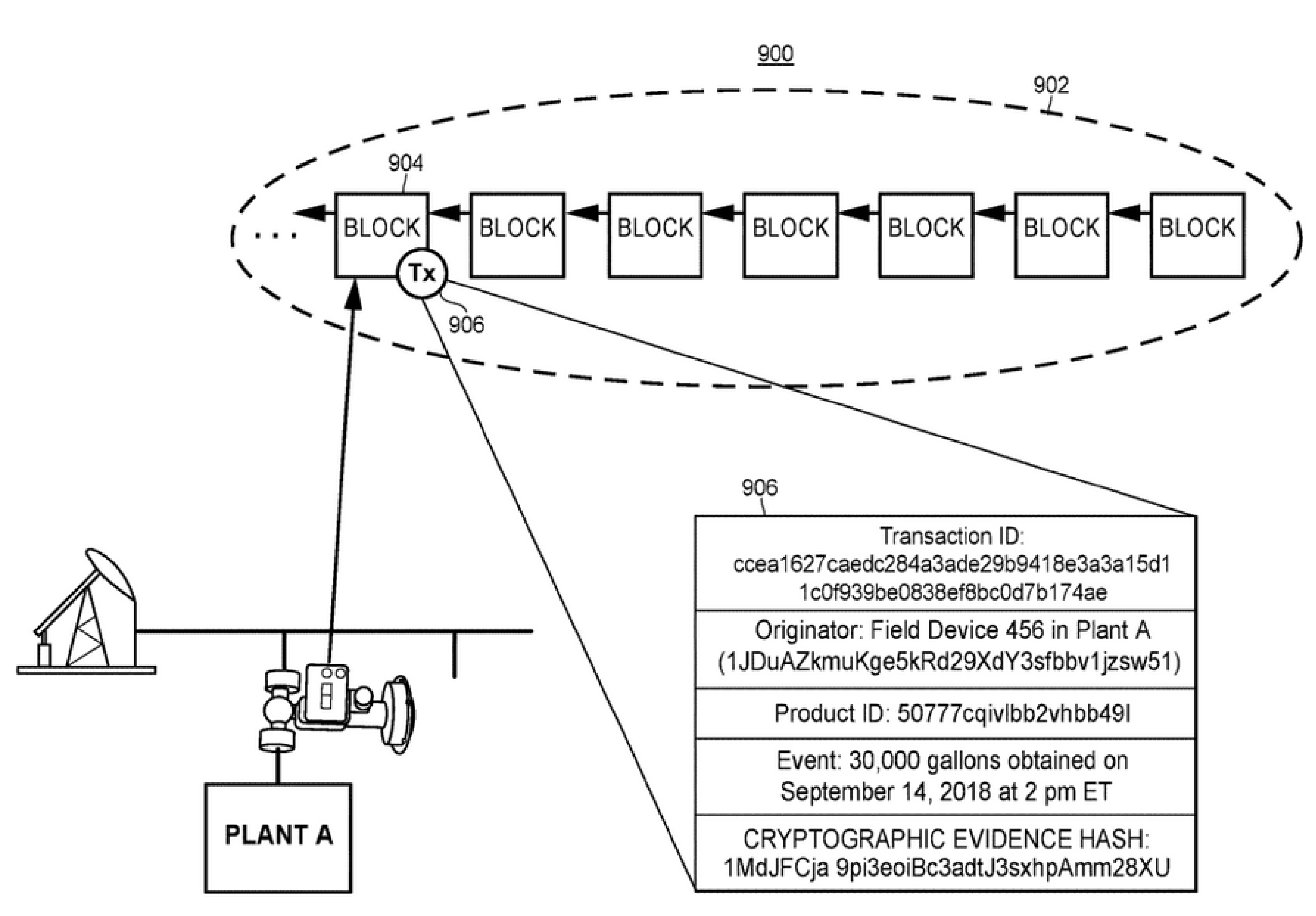
Patent Grant 11042147

U.S. patent number 11,042,147 [Application Number 16/248,388] was granted by the patent office on 2021-06-22 for *machine-to-machine transactions using distributed ledgers in process control systems*. This patent grant is currently assigned to FISHER-ROSEMOUNT SYSTEMS, INC.. The grantee listed for this patent is FISHER-ROSEMOUNT SYSTEMS, INC.. Invention is credited to Rezelee Rabe, Gian Marco Te, Lloyd Kenneth Tugbo.

United States Patent **11,042,147**
Tugbo , et al. **June 22, 2021**



Block diagram of an example process plant or process control system



Transaction ID:
ccea1627caedc284a3ade29b9418e3a3a15d1
1c0f939be0838ef8bc0d7b174ae

Originator: Field Device 456 in Plant A
(1JDuAZkmuKge5kRd29XdY3sfbbv1jzsw51)

Product ID: 50777cqivlbb2vhbb49l

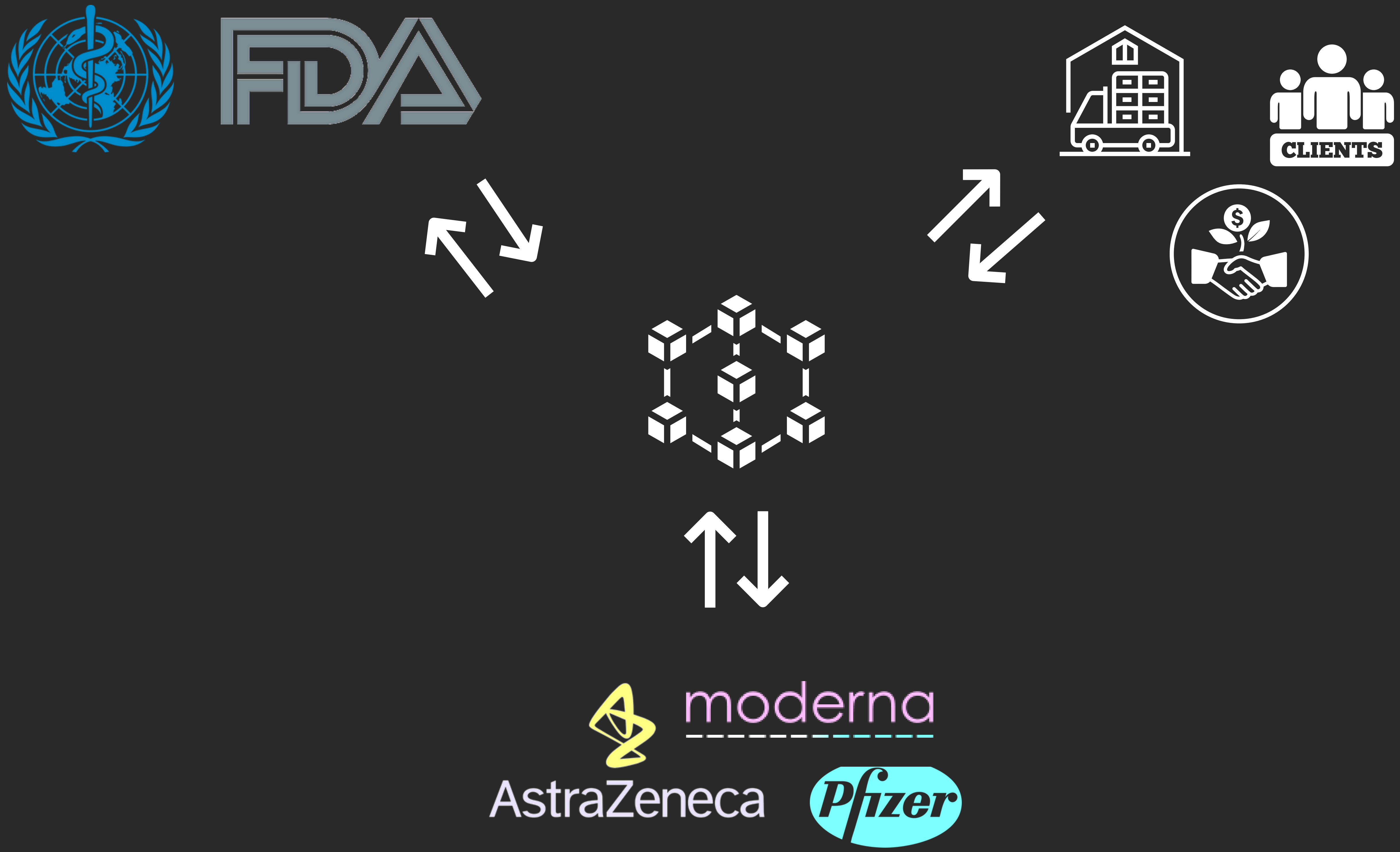
Event: 30,000 gallons obtained on
September 14, 2018 at 2 pm ET

CRYPTOGRAPHIC EVIDENCE HASH:
1MdJFCja 9pi3eoiBc3adtJ3sxhpAmm28XU

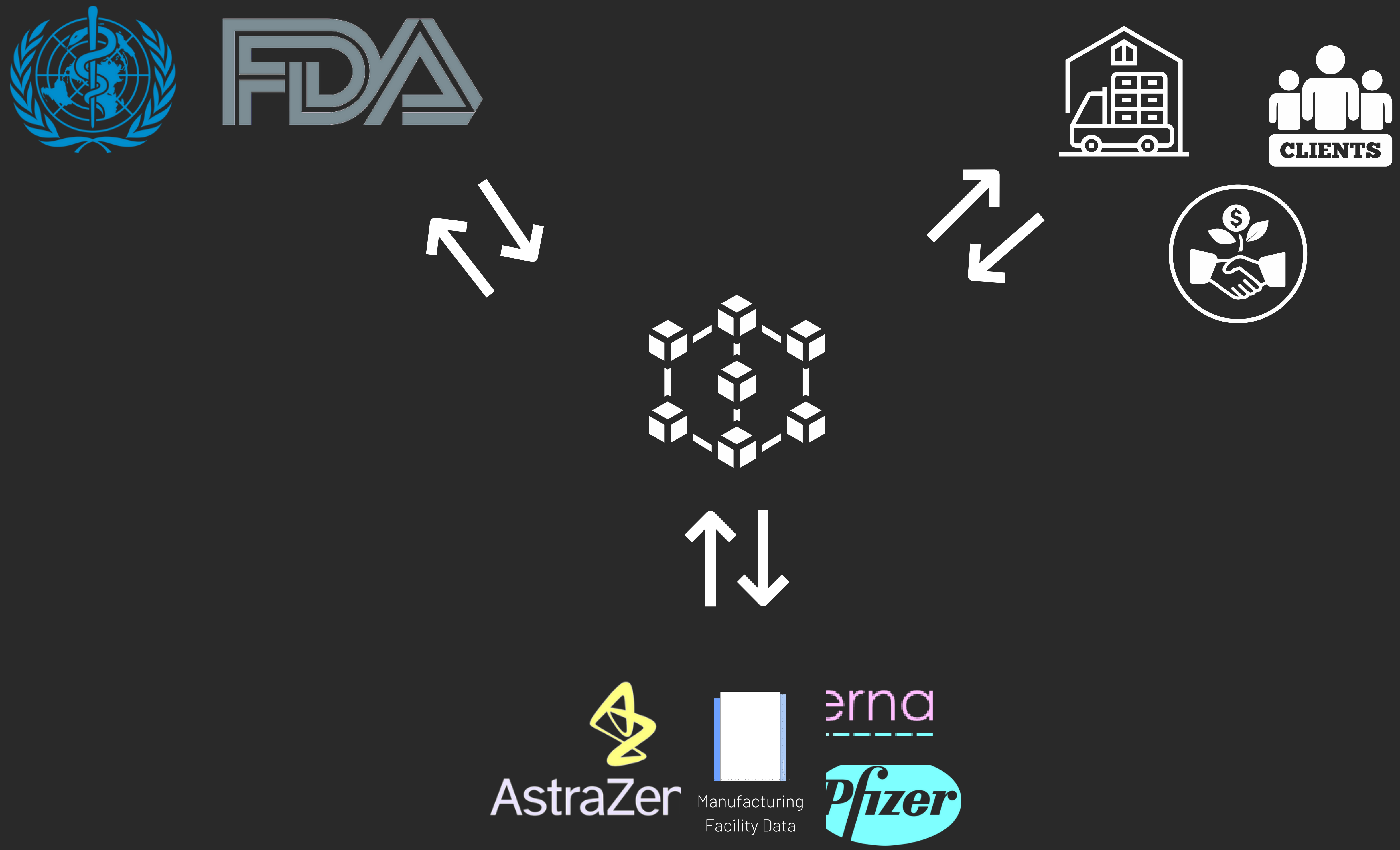
Transaction generated by a field device reporting the amount of oil received from an oil pipeline

Image Source: https://www.uspto.gov/

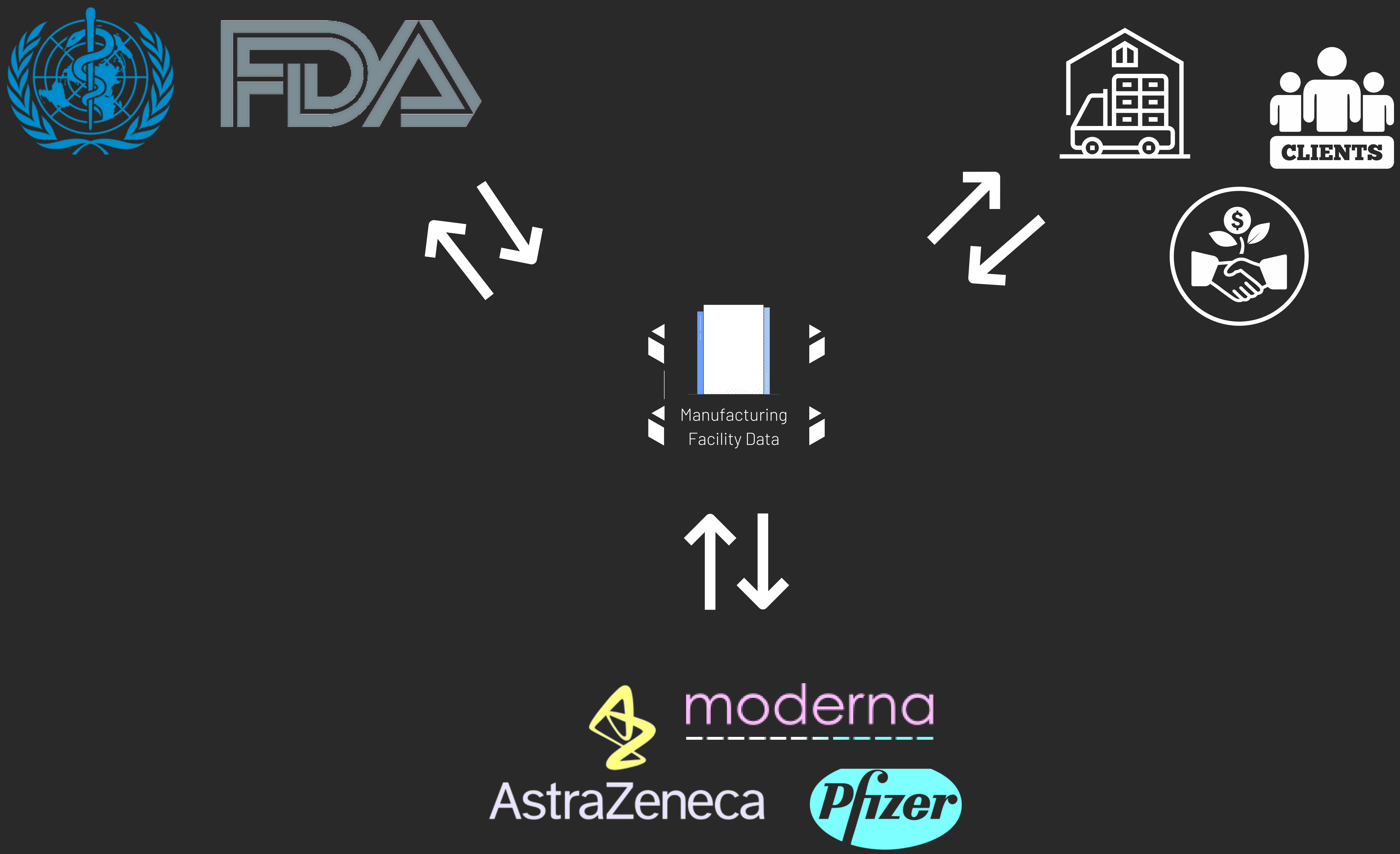
BLOCKCHAIN TECHNOLOGY
IN ICS



BLOCKCHAIN TECHNOLOGY
IN ICS



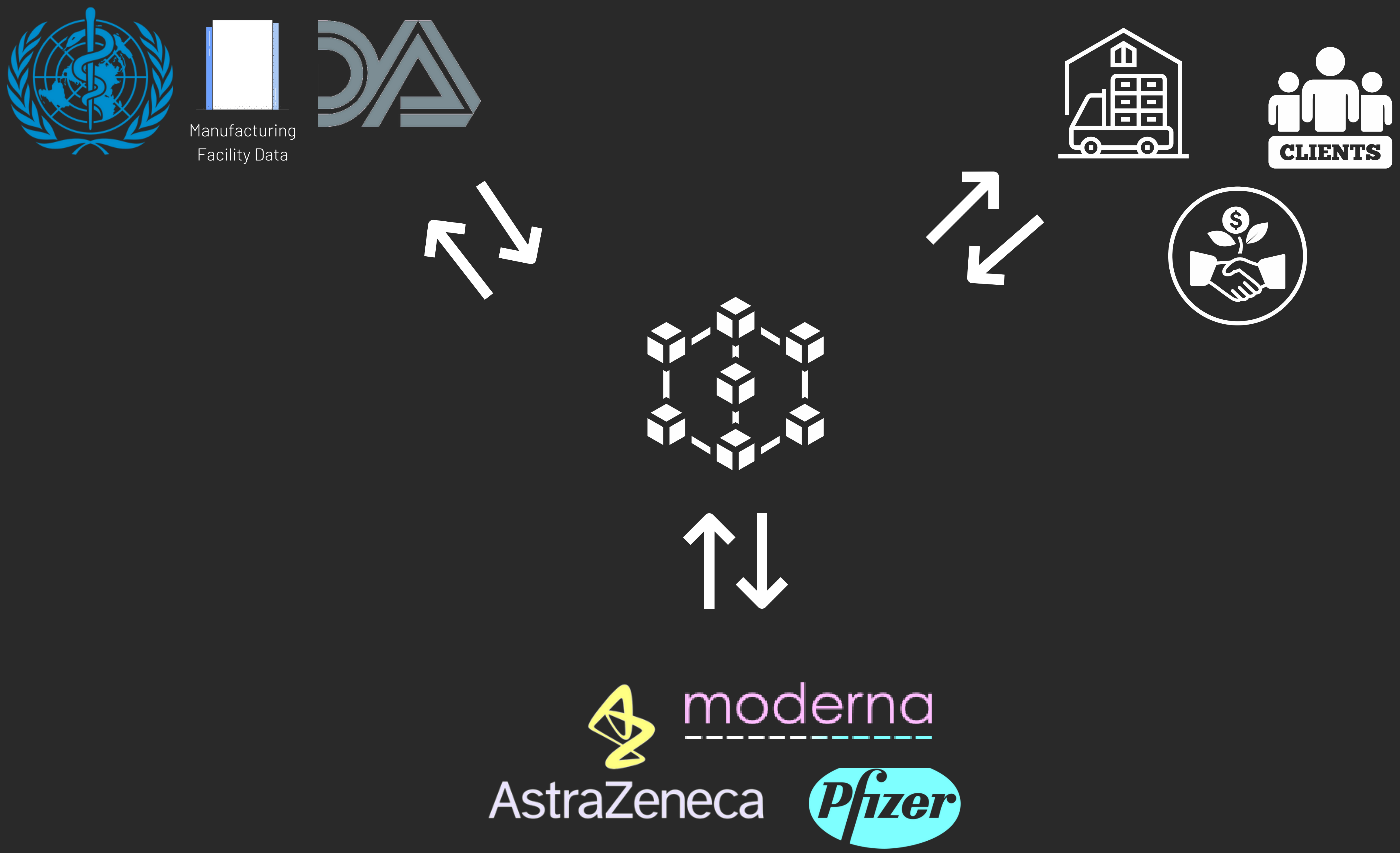
BLOCKCHAIN TECHNOLOGY IN ICS



Manufacturing Facility Data

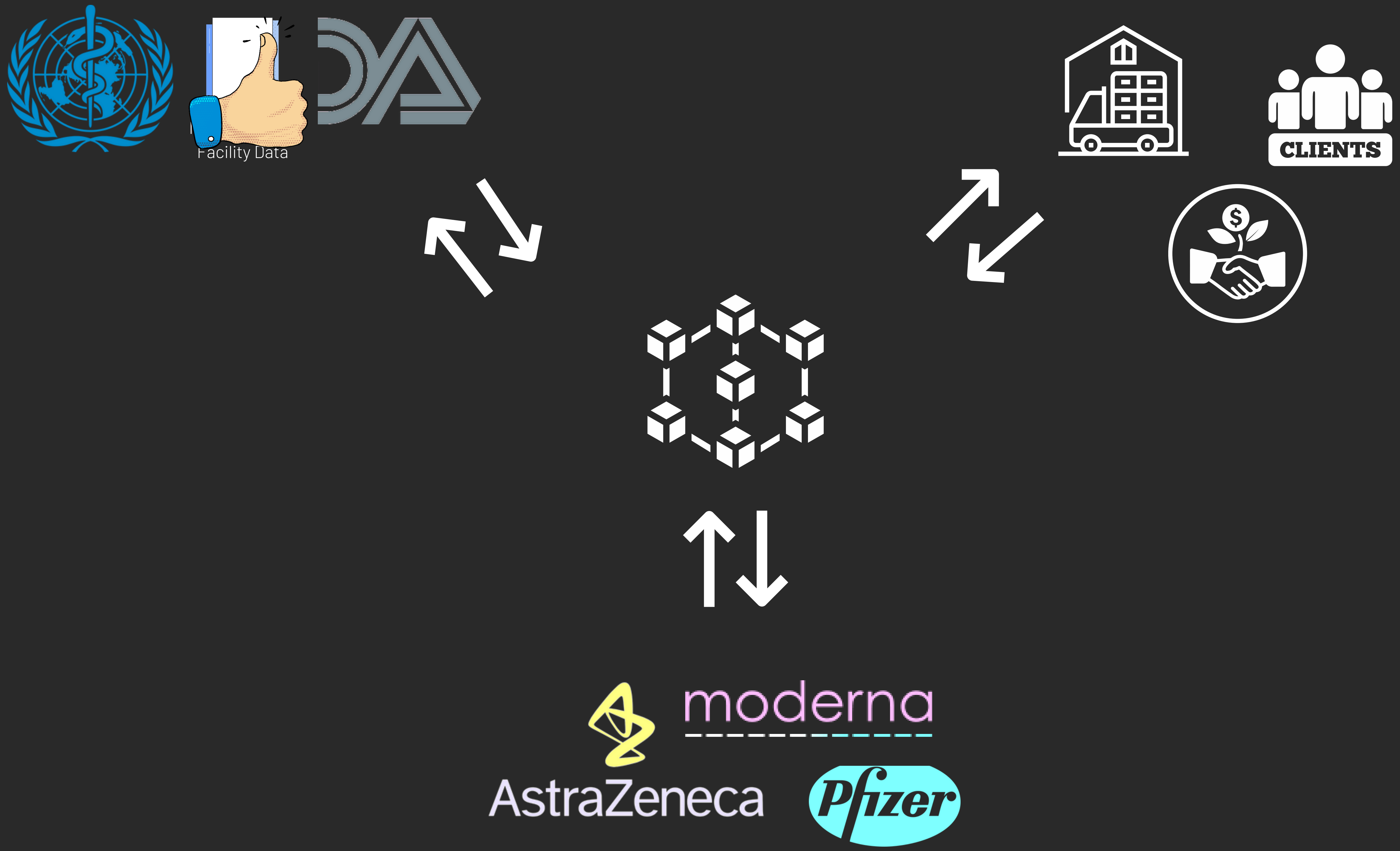
BLOCKCHAIN TECHNOLOGY

IN ICS

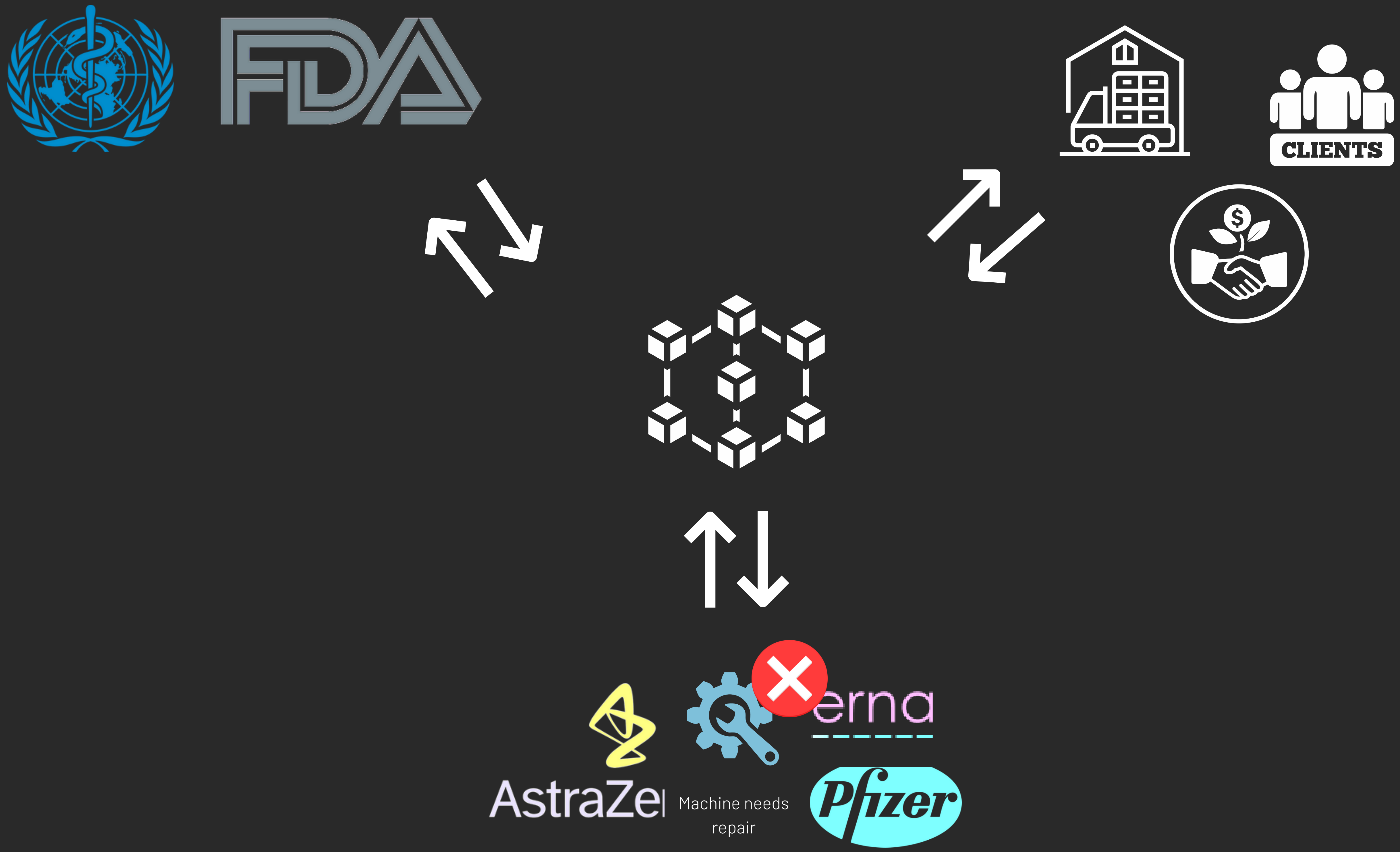


Manufacturing Facility Data

BLOCKCHAIN TECHNOLOGY
IN ICS

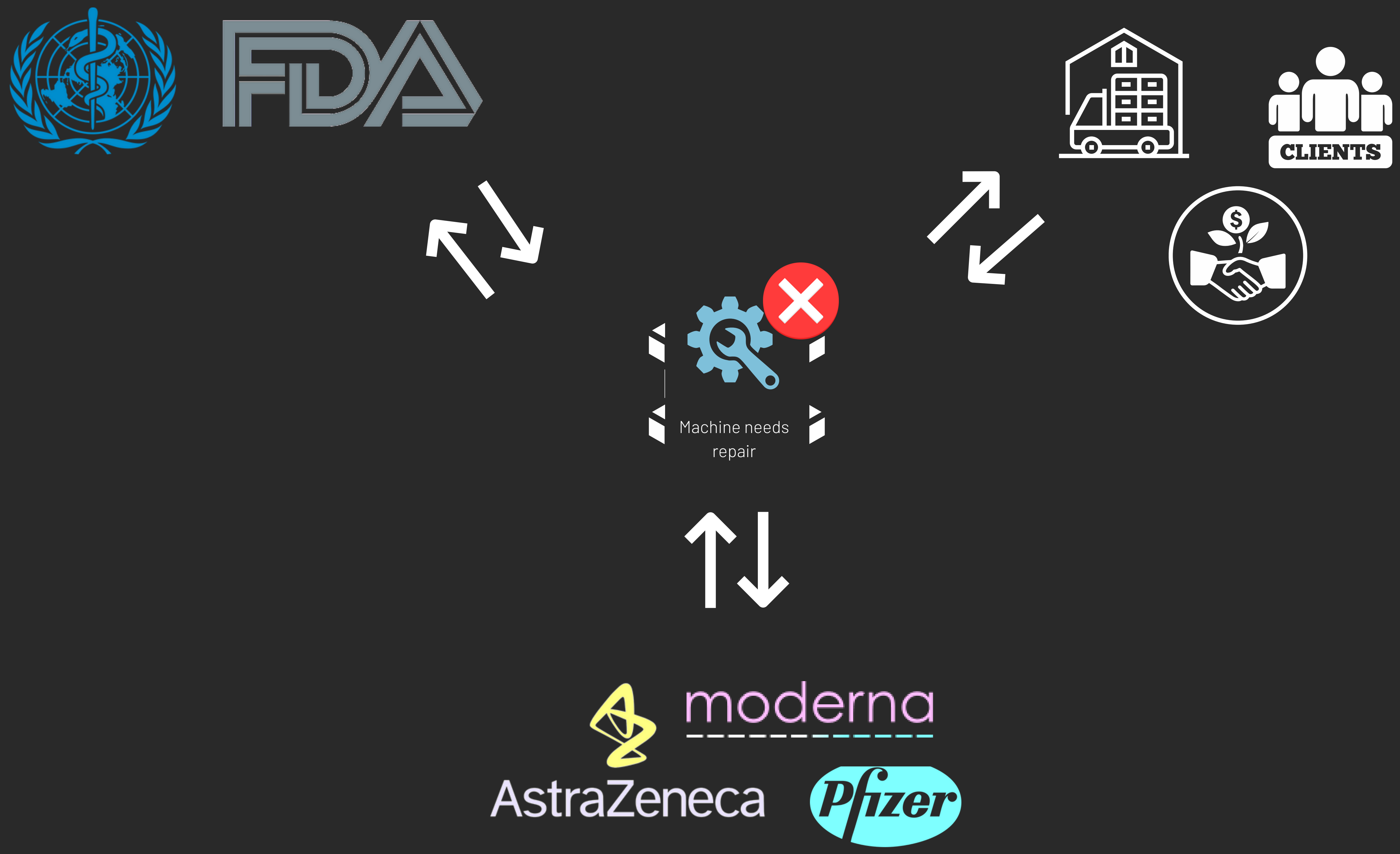


BLOCKCHAIN TECHNOLOGY
IN ICS

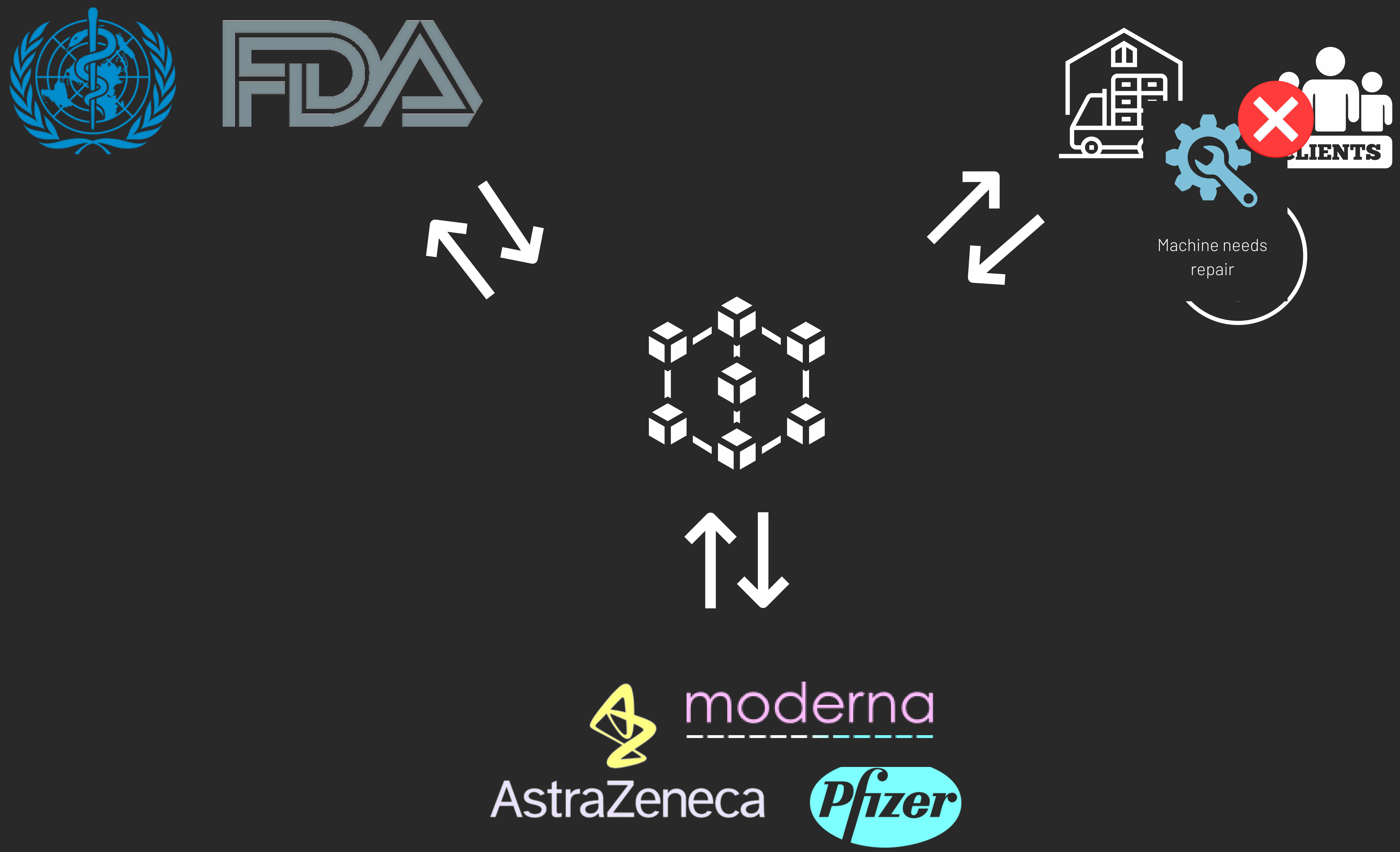


Machine needs repair

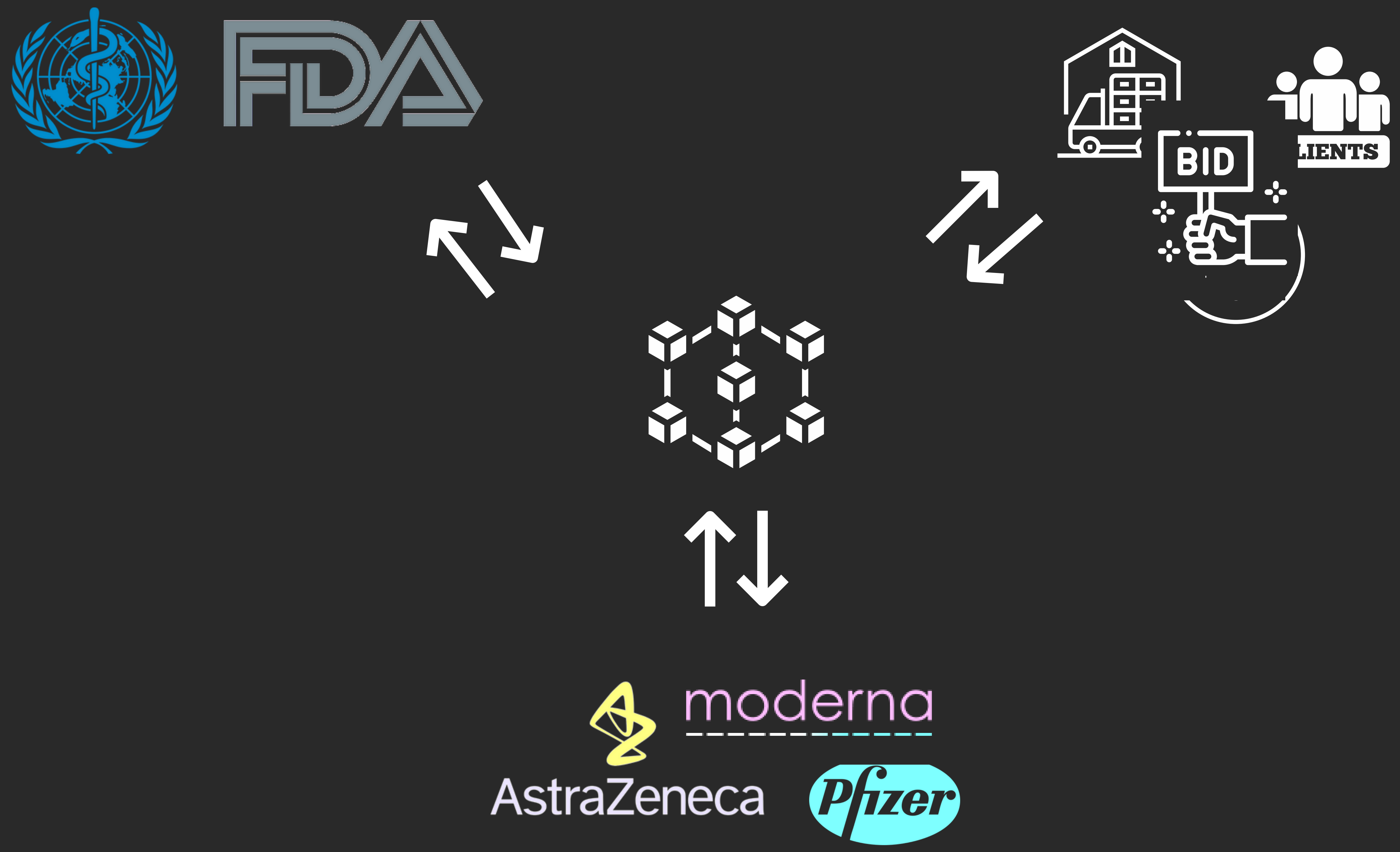
BLOCKCHAIN TECHNOLOGY
IN ICS



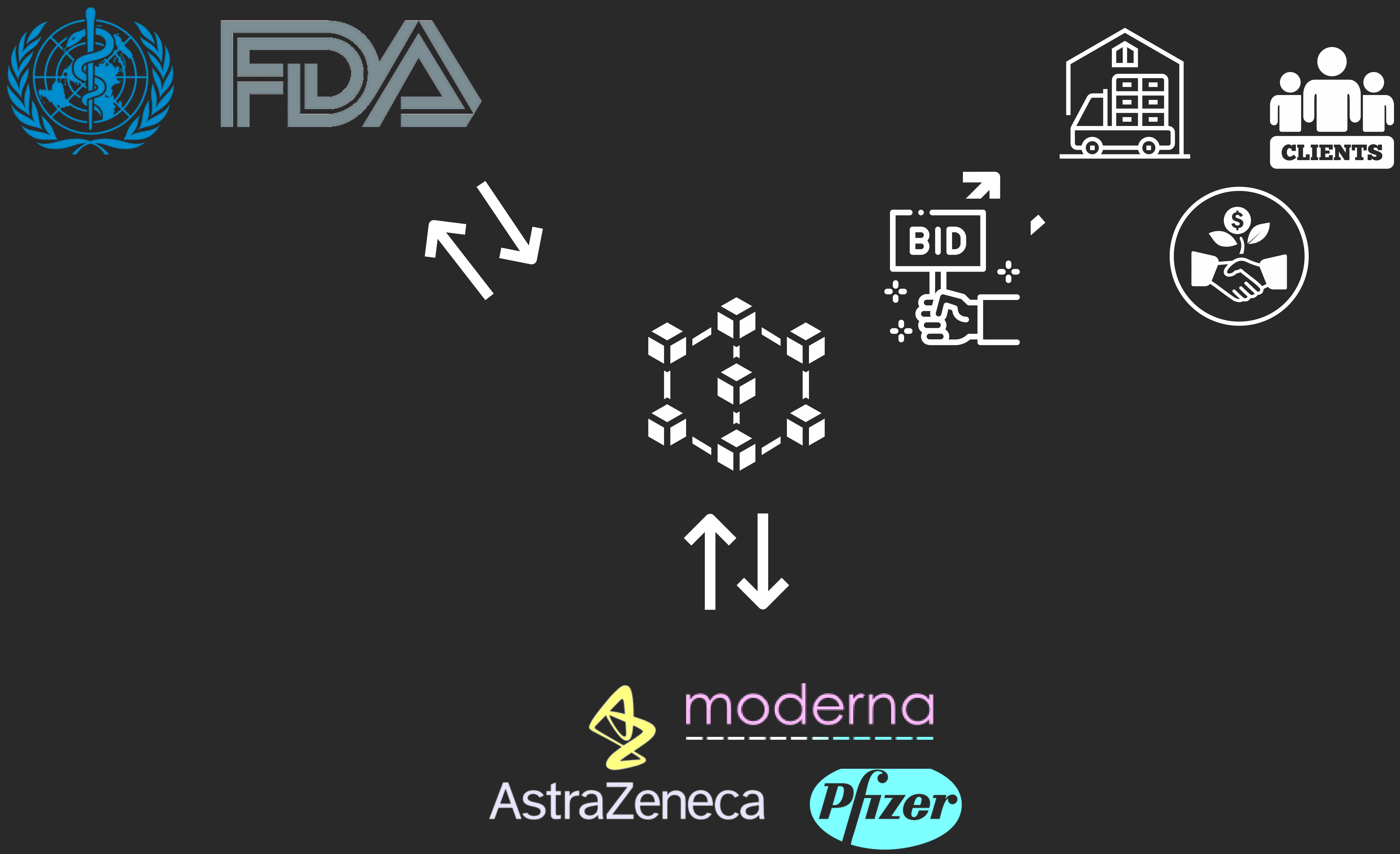
BLOCKCHAIN TECHNOLOGY
IN ICS



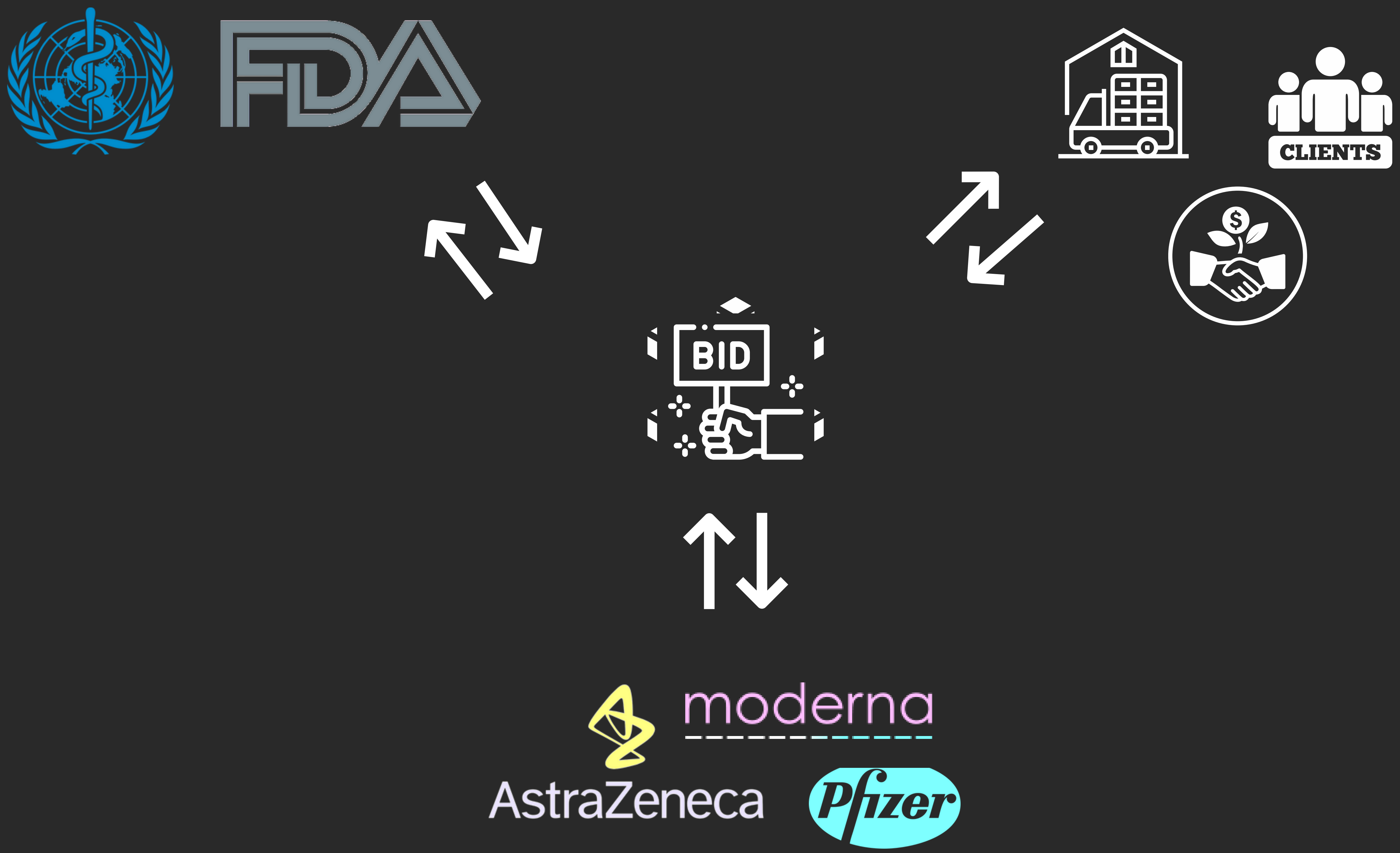
BLOCKCHAIN TECHNOLOGY
IN ICS



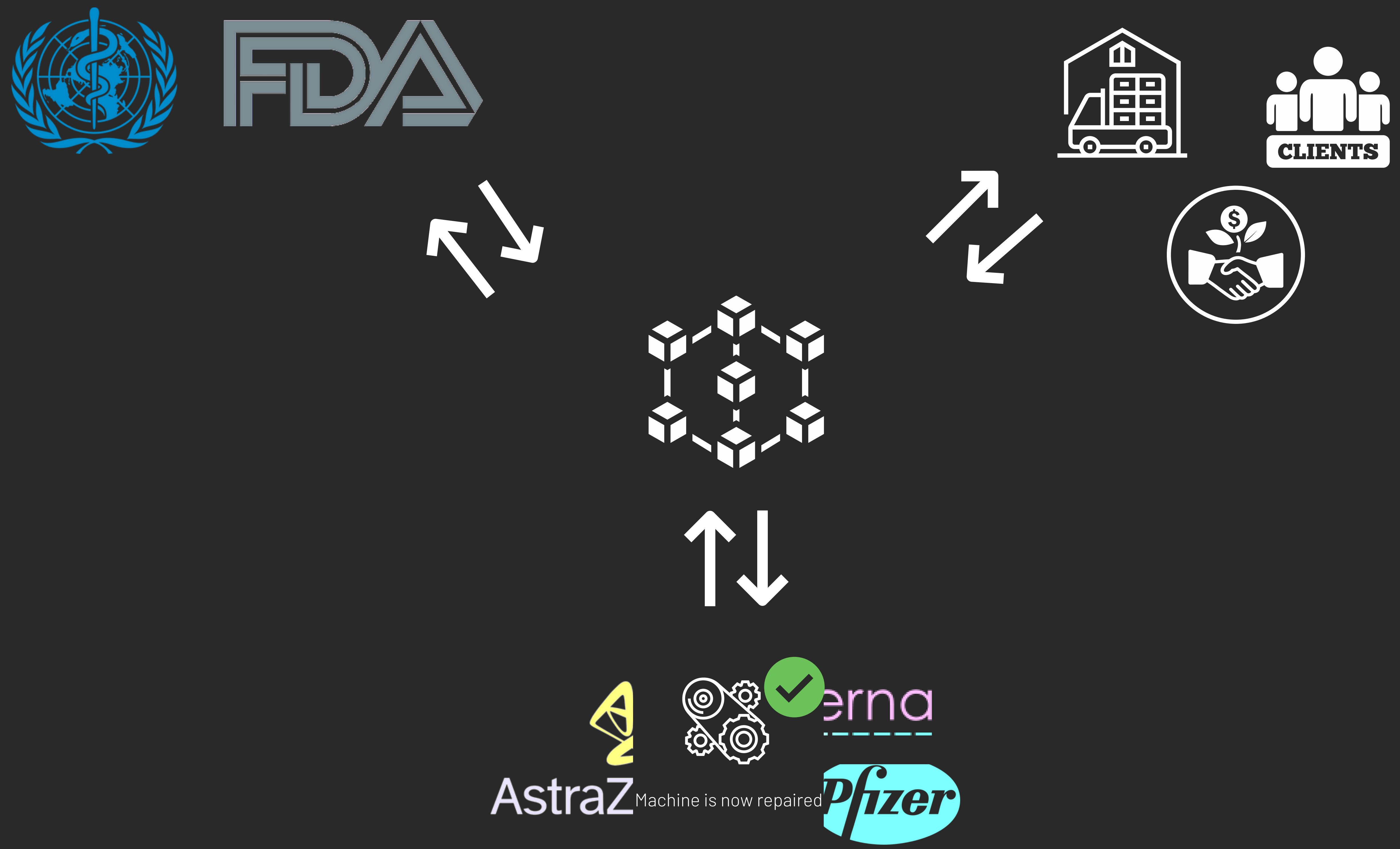
BLOCKCHAIN TECHNOLOGY
IN ICS



BLOCKCHAIN TECHNOLOGY
IN ICS

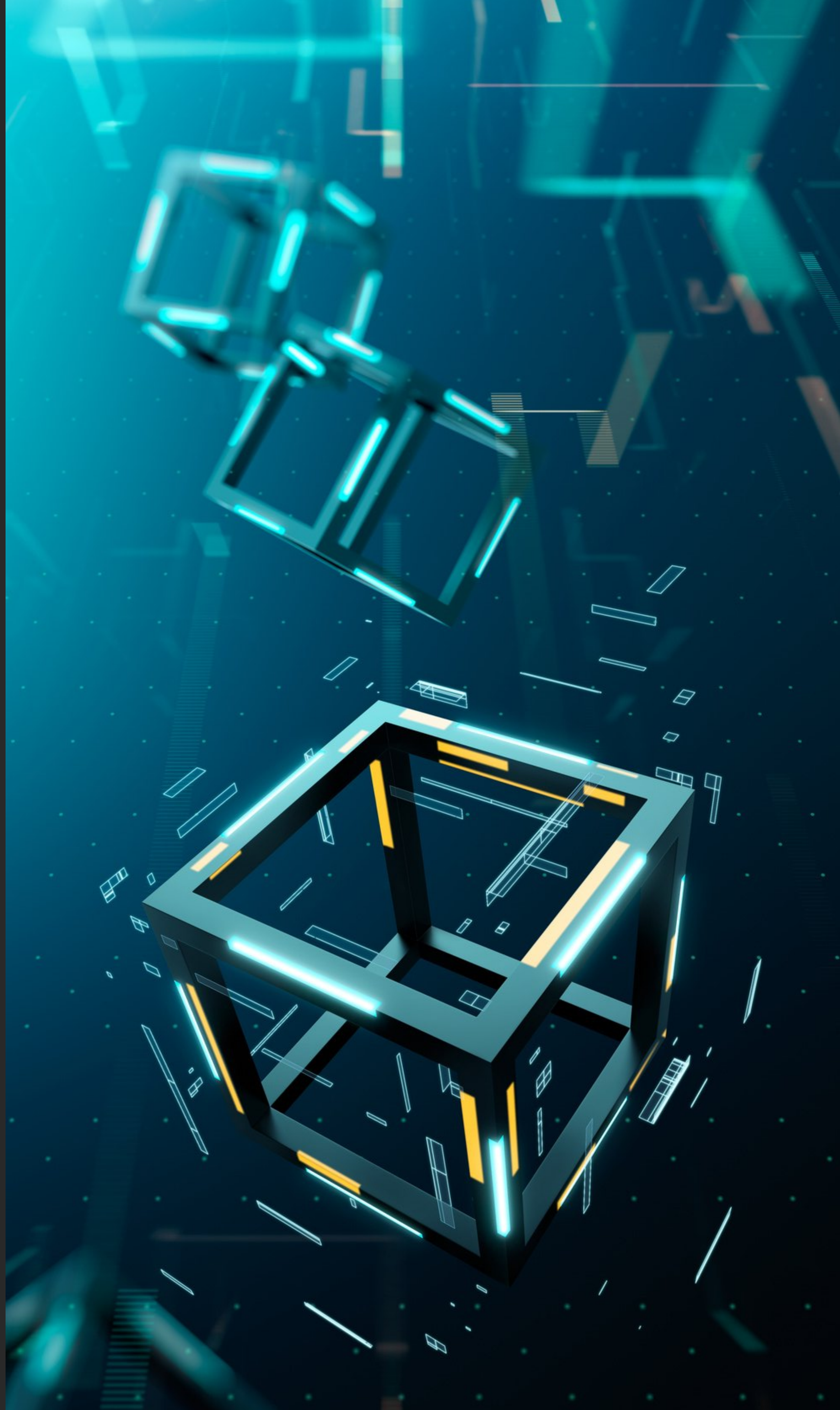


BLOCKCHAIN TECHNOLOGY
IN ICS



Blockchain ICS Acceptance Criteria

Security as the primary roadblock



BLOCKCHAIN TECHNOLOGY

ICS ACCEPTANCE CRITERIA

- Valid ICS use case
- Security
    - Data Privacy
    - Confidentiality
- Technology Complexity
- Others (e.g. Performance , Integration Cost, Data management, etc.)

SECURITY AS A MAIN ROADBLOCK

Data Security is important in ICS

e.g. Recipe, Formulas etc.

Blockchain Security: Cryptography

Cryptography in the blockchain is the core of this technology, making it immutable and reliable.

SECURITY AS A MAIN ROADBLOCK

- **Encryption**
  - Asymmetric-Key Encryption
    - Digital Signature
  - Hashing

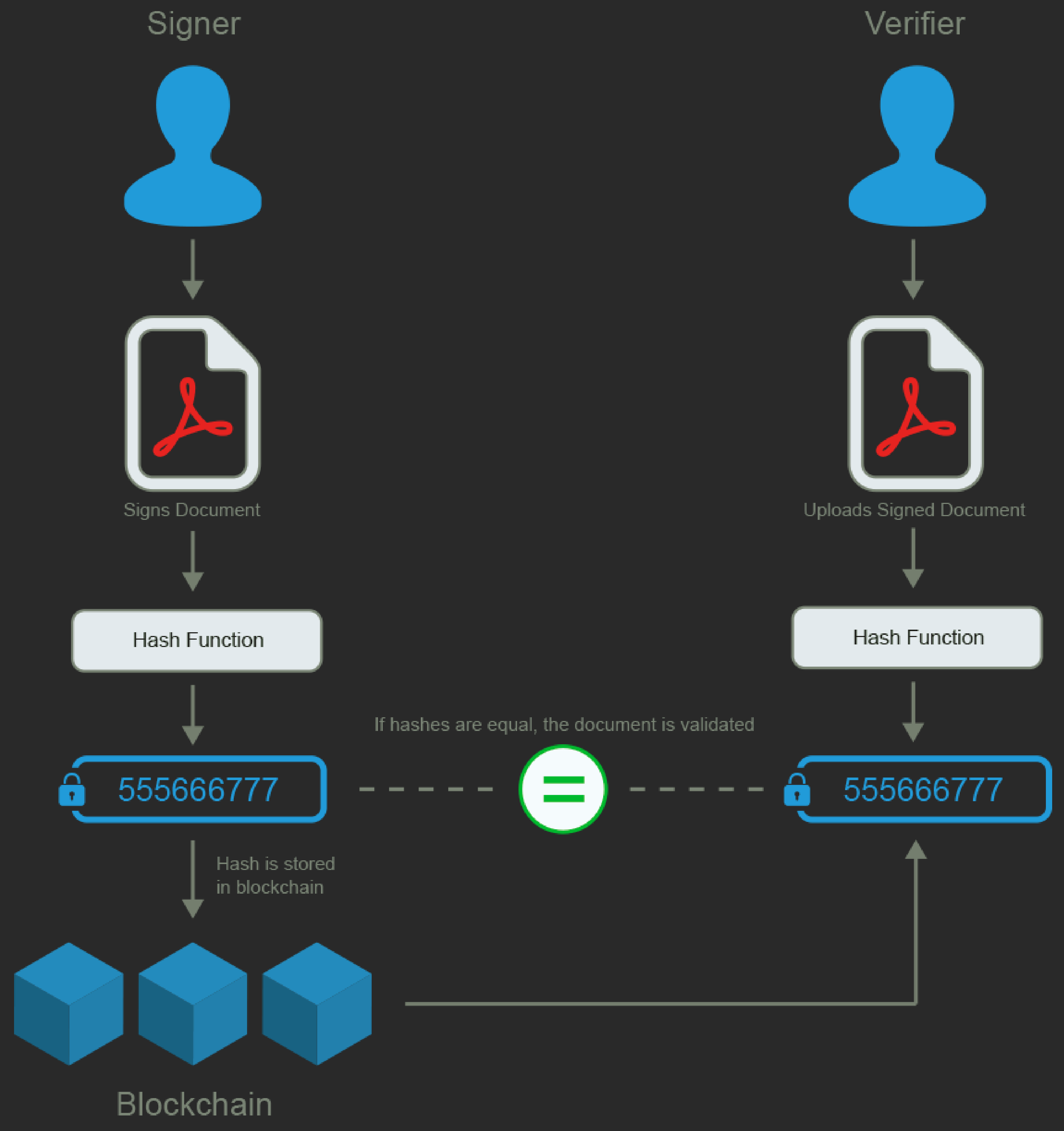


Image Source: https://www.textcontrol.com/blog/2019/08/02/document-signing-and-validation-using-blockchain/

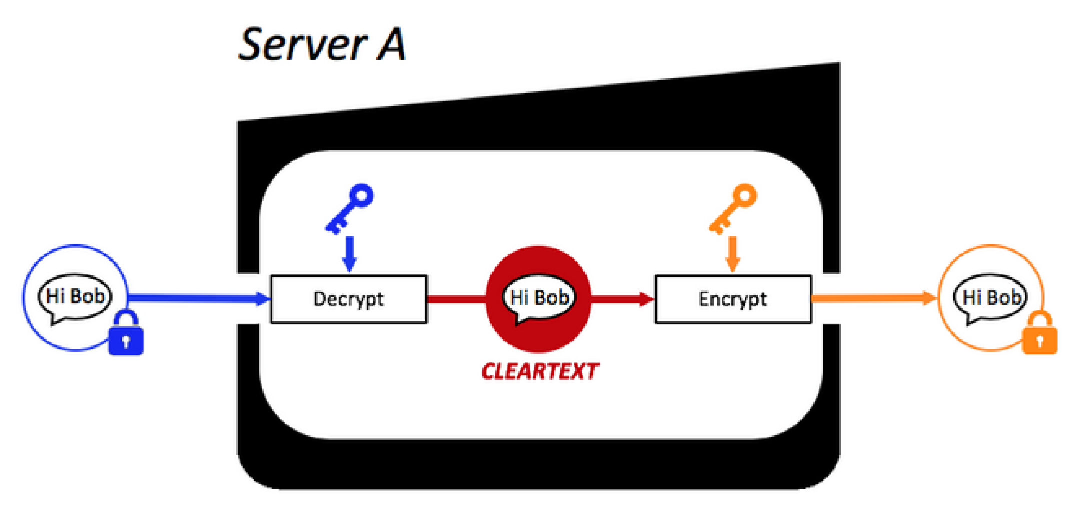
SECURITY AS A MAIN ROADBLOCK

Hop-by-hop encryption

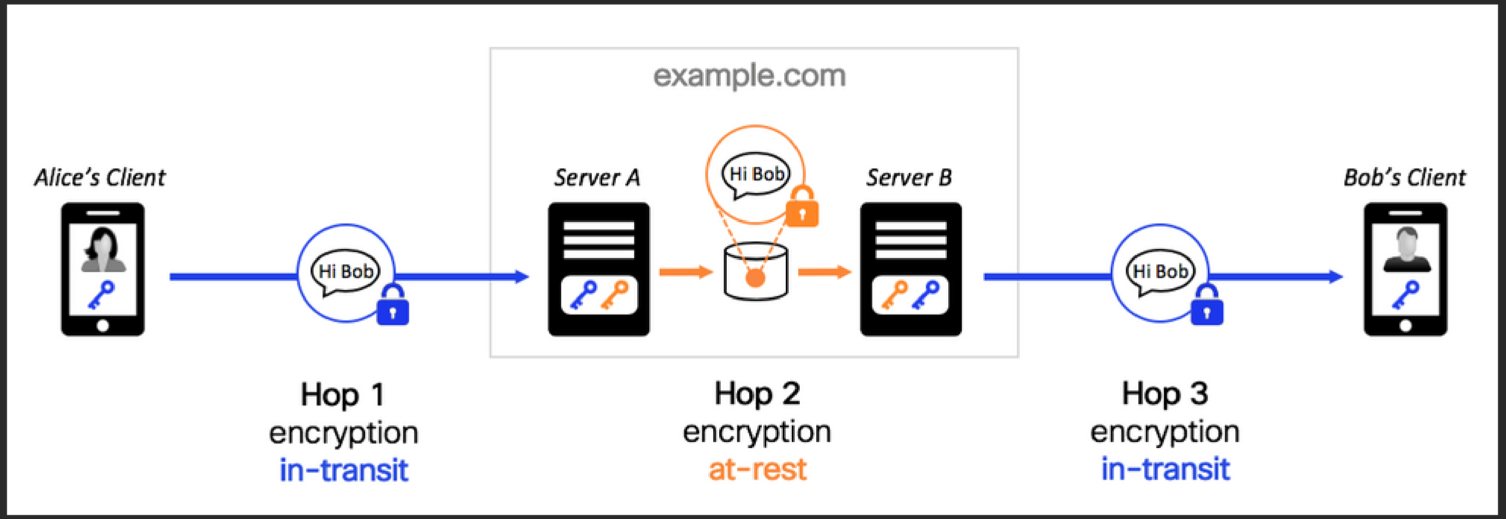
- Most Blockchain Frameworks implementation
  - TLS
  - Application Level Encryption

Challenges

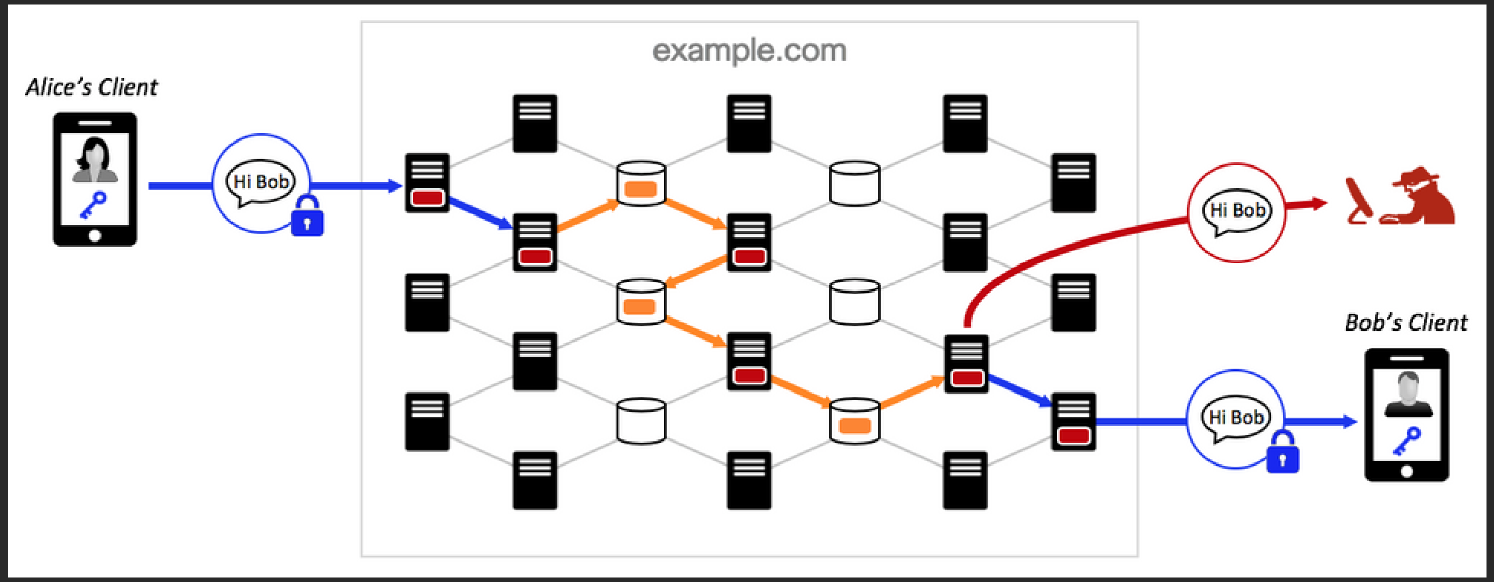
- Easy implementation of Encryption Backdoors
- Allows the intermediate link in the chain



The Privacy Gap of hop-by-hop encryption



Hop-by-hop encryption



hop-to-hop encryption gaps are pervasive

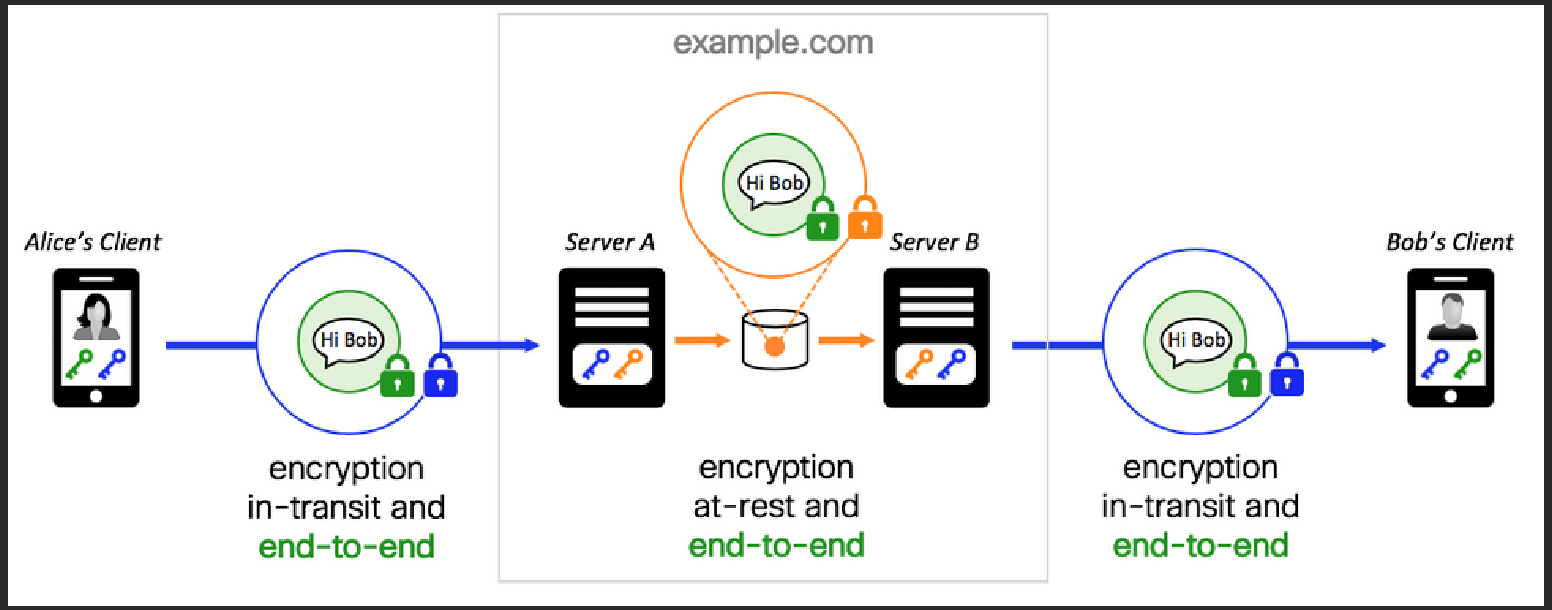
SECURITY AS A MAIN ROADBLOCK

E2EE

- End-to-end encryption is currently the most secure way to transfer confidential ICS data
  - No "man in the middle" could decrypt the intercepted communication not even the service provider could decrypt the contents of the message.
- E2EEs are widely used so far in Instant Messaging

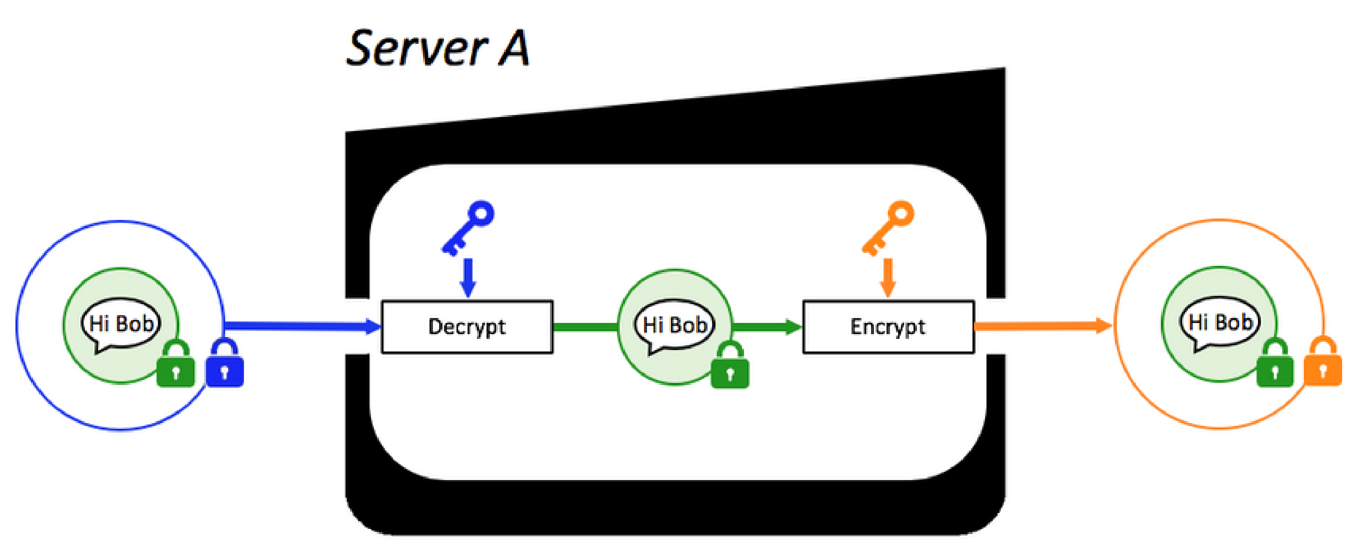
Challenges

- Government and Politics
- Not all services rush toward end-to-end encryption: For users gaining convenience and additional services may be more important than adding even more data security.

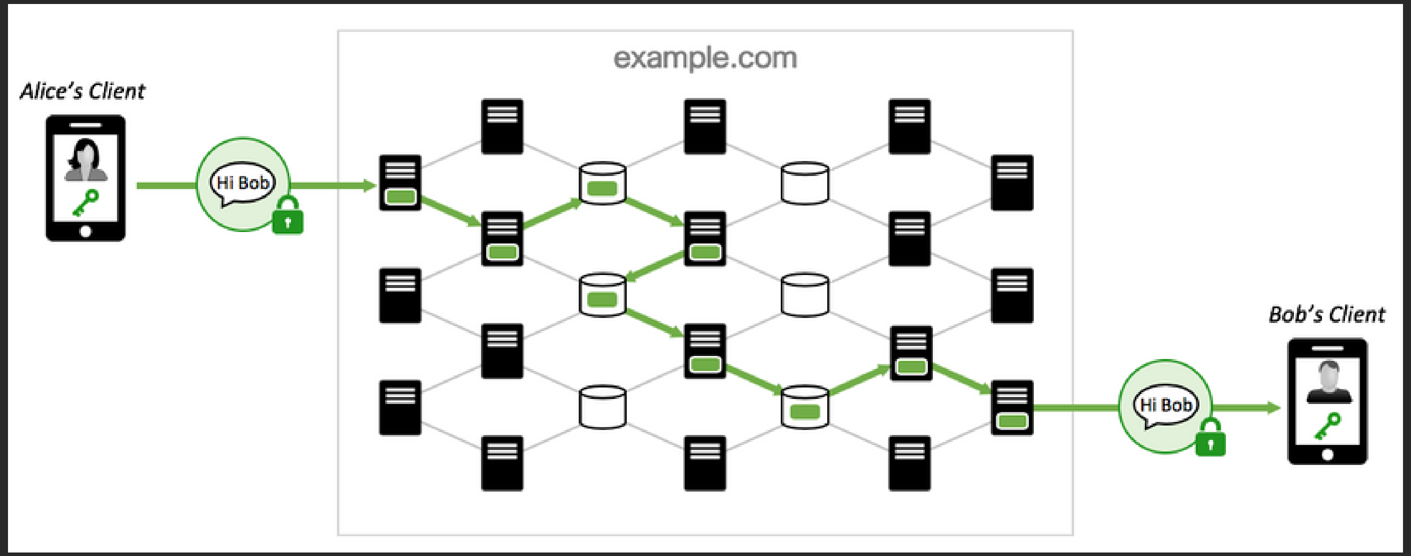


example.com
Alice's Client
Server A
Server B
Bob's Client
Hi Bob
Hi Bob
Hi Bob
encryption in-transit and end-to-end
encryption at-rest and end-to-end
encryption in-transit and end-to-end

End-to-end encryption



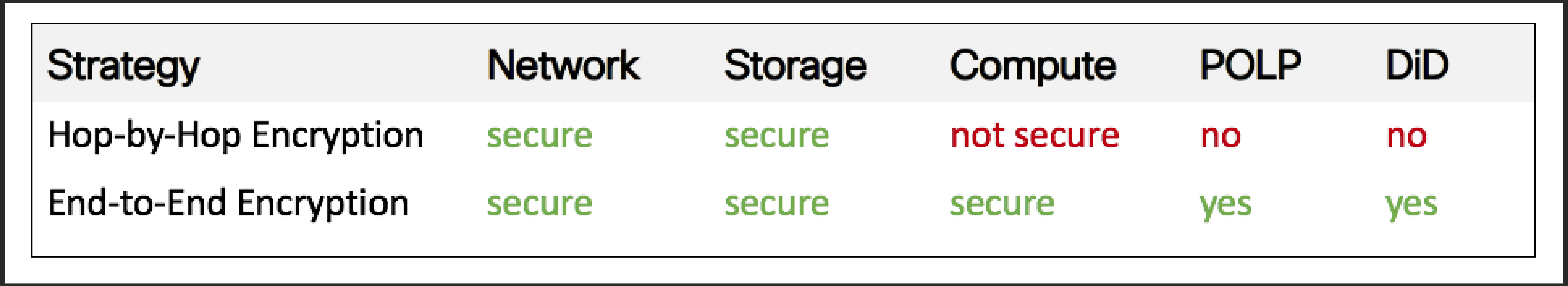
Gap-less privacy



hop-to-hop encryption gaps are mitigated

SECURITY AS A MAIN ROADBLOCK

CLOSING THE GAP



Strategy	Network	Storage	Compute	POLP	DiD
Hop-by-Hop Encryption	secure	secure	not secure	no	no
End-to-End Encryption	secure	secure	secure	yes	yes

End-to-end encryption vs hop-by-hop encryption

E2EE EXAMINED

E2EE Protocol is a key element

- Easy to Integrate
- Supports decentralization
- Secure and Trusted (Peer Reviewed)
- Compatibility for ICS Transactions

E2EE Protocol

Signal

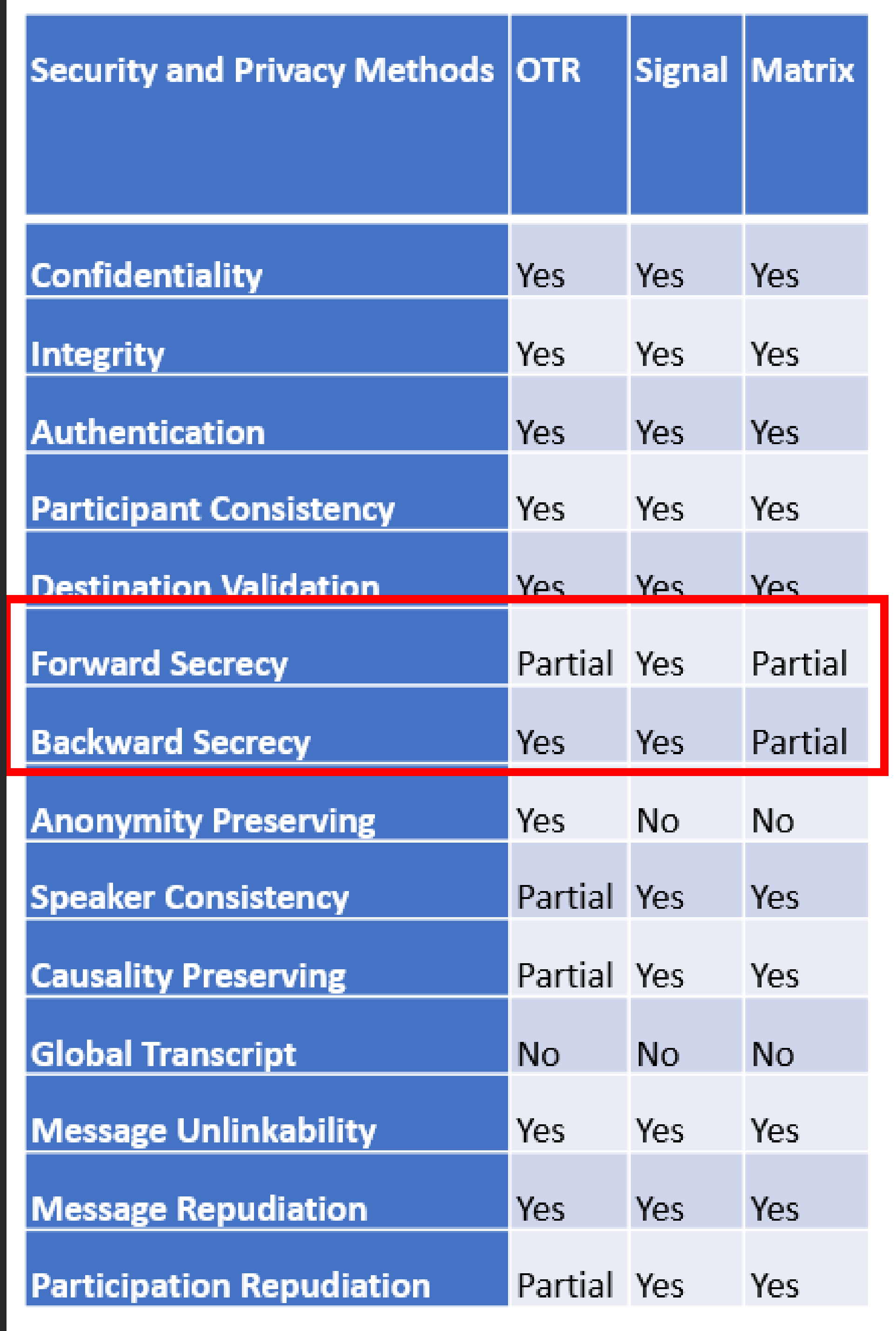
OTR
OFF-THE-RECORD MESSAGING PROTOCOL

matrix

Source: https://signal.org/docs/ , https://matrix.org/ and https://otr.cypherpunks.ca/index.php#docs

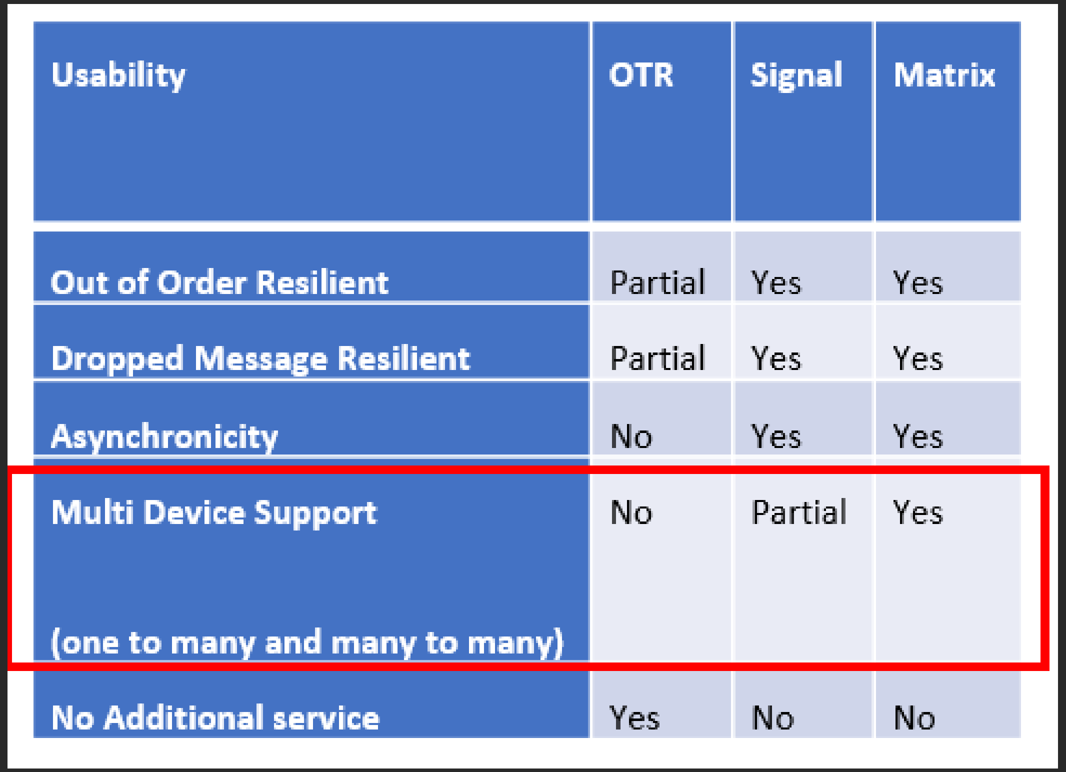
E2EE EXAMINED

Table A: Security Properties



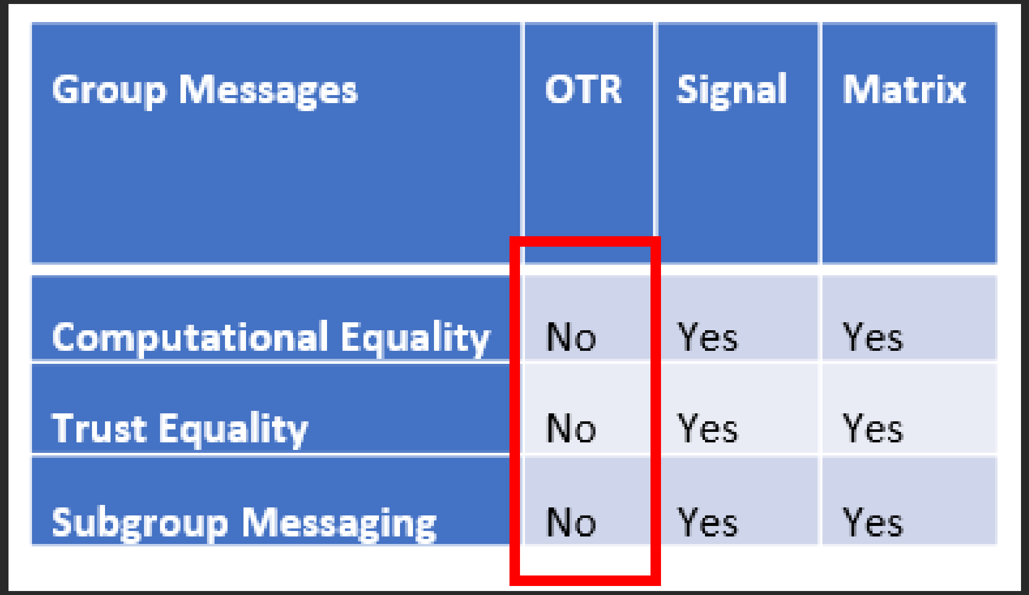
Security and Privacy Methods	OTR	Signal	Matrix
Confidentiality	Yes	Yes	Yes
Integrity	Yes	Yes	Yes
Authentication	Yes	Yes	Yes
Participant Consistency	Yes	Yes	Yes
Destination Validation	Yes	Yes	Yes
Forward Secrecy	Partial	Yes	Partial
Backward Secrecy	Yes	Yes	Partial
Anonymity Preserving	Yes	No	No
Speaker Consistency	Partial	Yes	Yes
Causality Preserving	Partial	Yes	Yes
Global Transcript	No	No	No
Message Unlinkability	Yes	Yes	Yes
Message Repudiation	Yes	Yes	Yes
Participation Repudiation	Partial	Yes	Yes

Table B: Usability Properties



Usability	OTR	Signal	Matrix
Out of Order Resilient	Partial	Yes	Yes
Dropped Message Resilient	Partial	Yes	Yes
Asynchronicity	No	Yes	Yes
Multi Device Support (one to many and many to many)	No	Partial	Yes
No Additional service	Yes	No	No

Table C: Group Messages Properties



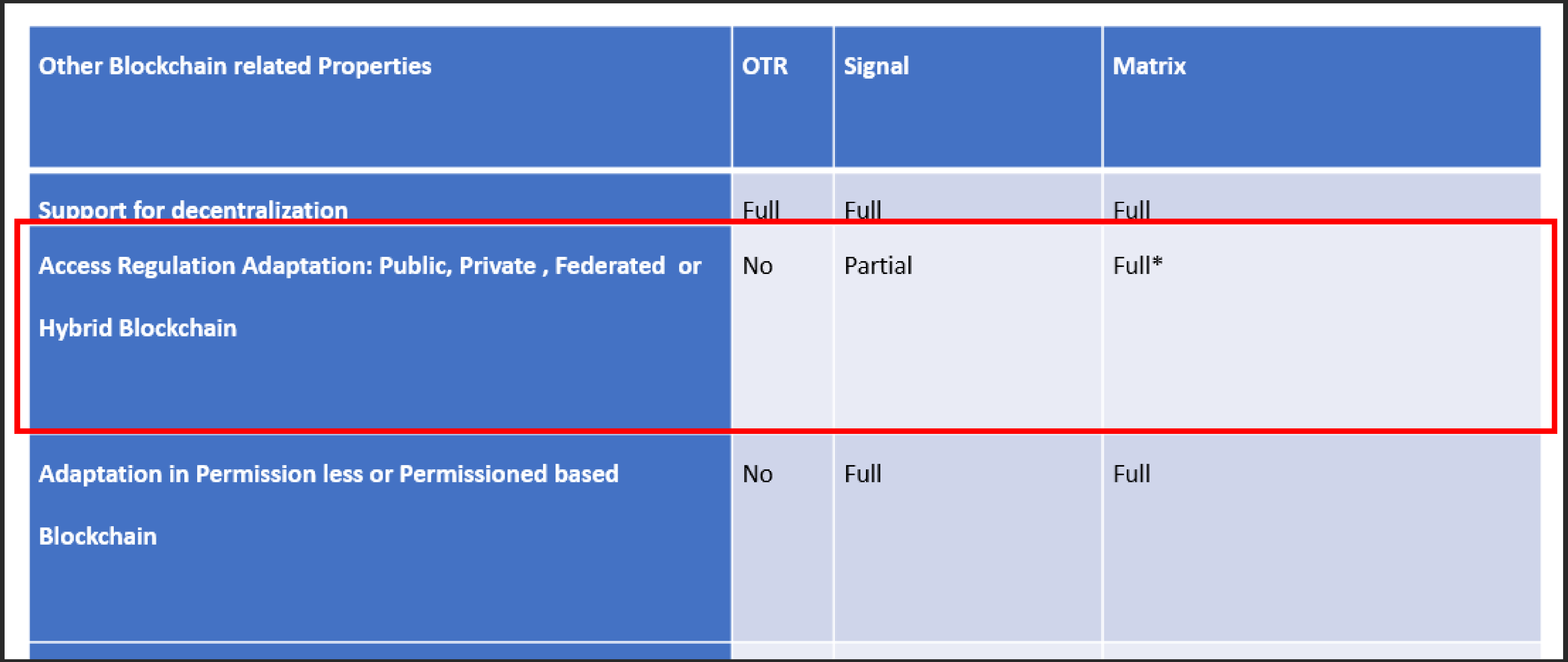
Group Messages	OTR	Signal	Matrix
Computational Equality	No	Yes	Yes
Trust Equality	No	Yes	Yes
Subgroup Messaging	No	Yes	Yes

- Signal and Matrix Protocol mostly support the 3 properties for Secure messaging Implementations

Source: Comparing Implementations of Secure Messaging Protocols Christian Johansen , Aulon Mujaj , Hamed Arshad , Josef Noll Research report 475, November 2017

E2EE EXAMINED

Table D: E2EE protocol Blockchain properties Compatibility



Other Blockchain related Properties	OTR	Signal	Matrix
Support for decentralization	Full	Full	Full
Access Regulation Adaptation: Public, Private , Federated or Hybrid Blockchain	No	Partial	Full*
Adaptation in Permission less or Permissioned based Blockchain	No	Full	Full

- Matrix Instant Messaging Protocol is an E2EE that is fully compatible for a Blockchain ICS implementation

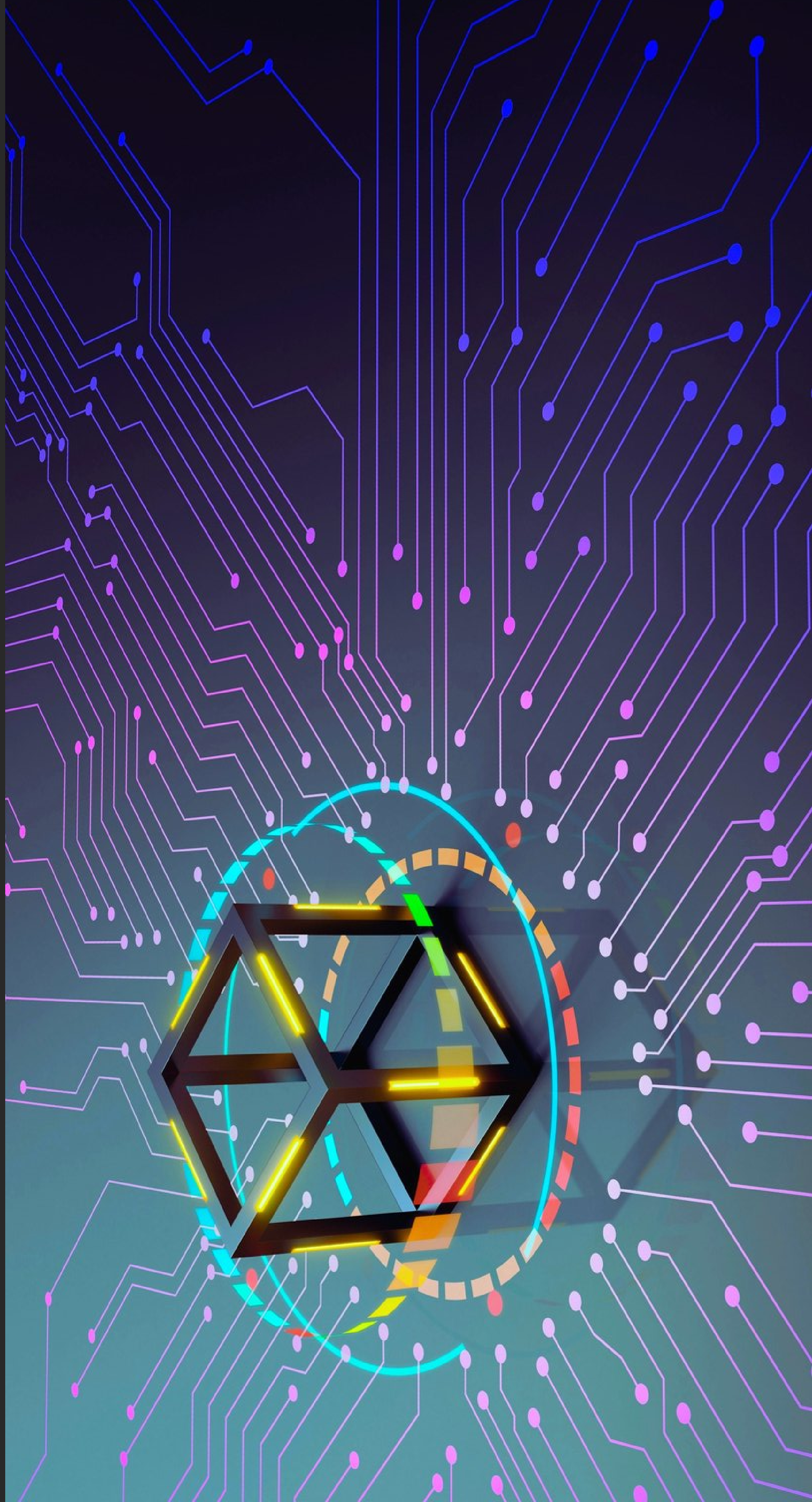
[matrix]

The Matrix protocol contains the properties needed to implement a secure messaging mechanism for Blockchain-based applications.

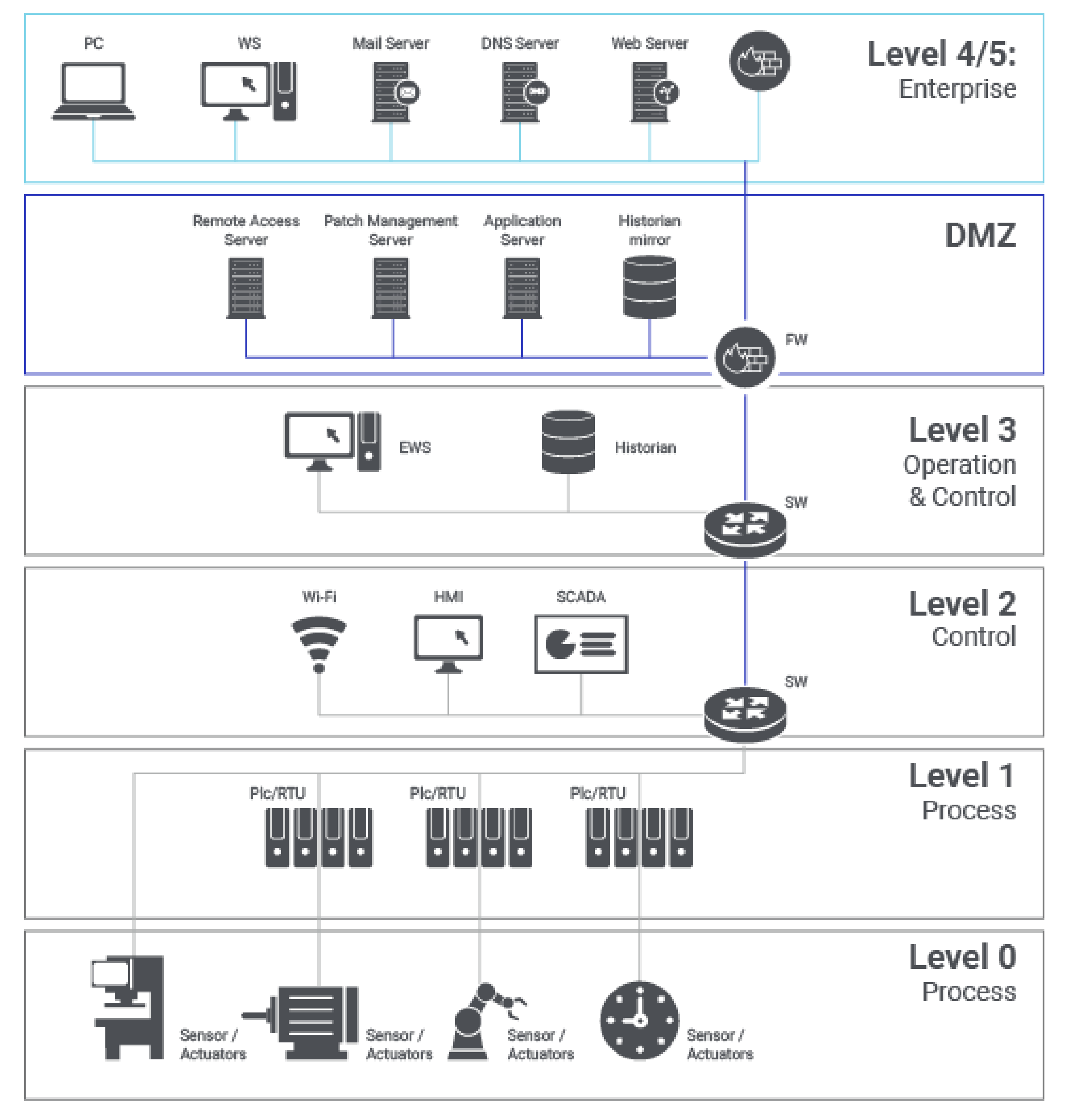
...but how can we integrate this in Blockchain based ICS implementation?

Blockchain ICS Integration

Sending Data from L0 to L3 Network



The Purdue Model Requirement



How can we integrate blockchain given the strict requirements of Purdue model?

Source: https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security

L0 to L3 integration proposed solutions

E4

- a cryptographic implant that IoT manufacturers can integrate into their servers to makes IoT data protection painless
- to have the protection consistent for the whole path (end to end)
- simplifies the use and deployment of end-to-end security for MQTT and other IoT protocols

Challenges

- Early stage of opensource development (2019-2020)
- E2EE protocol Blockchain properties Compatibility e.g. Not decentralized
- Single point of failure
- Risk from untrusted clients
- Security Properties were not audited by a 3rd party

Source:https://teserakt-io.github.io/e4-doc/

L0 to L3 integration proposed solutions

FDI

- developed by FieldComm Group
- supports end-to-end security
- aims to solve the interoperability problem on multiple devices from multiple vendors through a standard software module called FDI Device Package
- supports proprietary device communication protocols

Challenges

- securing data as it moves from one Purdue Model Layer to another requires multiple additional components on top of the current ones being utilized
- not all communication protocols are supported, others are still under development
- requires a single host to act as a pass-through, possibly more expensive

Source: https://www.ask4fdi.com/new-index-1#/1package/

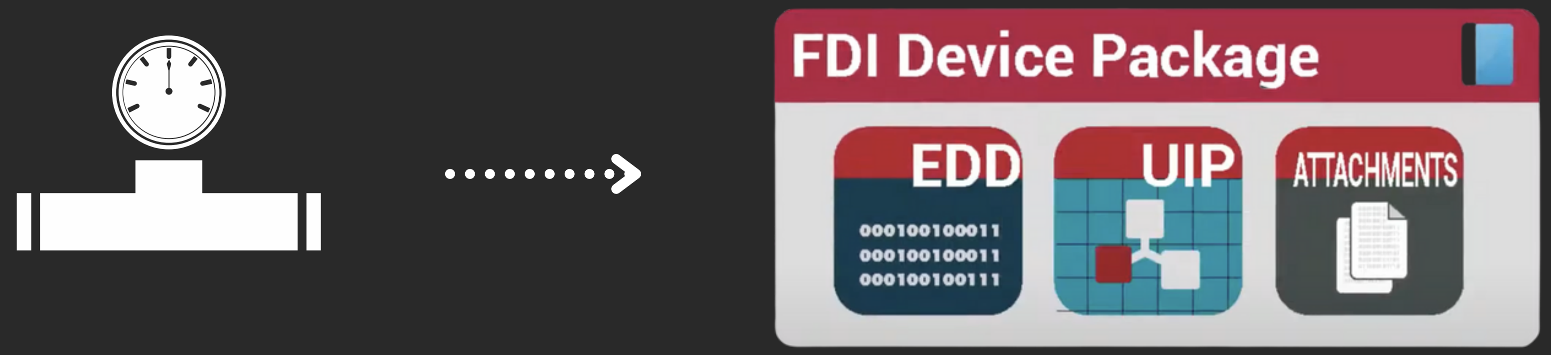
Field Device Integration (FDI)

FDI

- supported protocols: WirelessHART, HART, PROFIBUS, PROFINET, Foundation Fieldbus, Modbus, ISA 100 Wireless
- can support suplementary communication paths e.g. OPC (Open Platform Communications) UA (Unified Architecture)

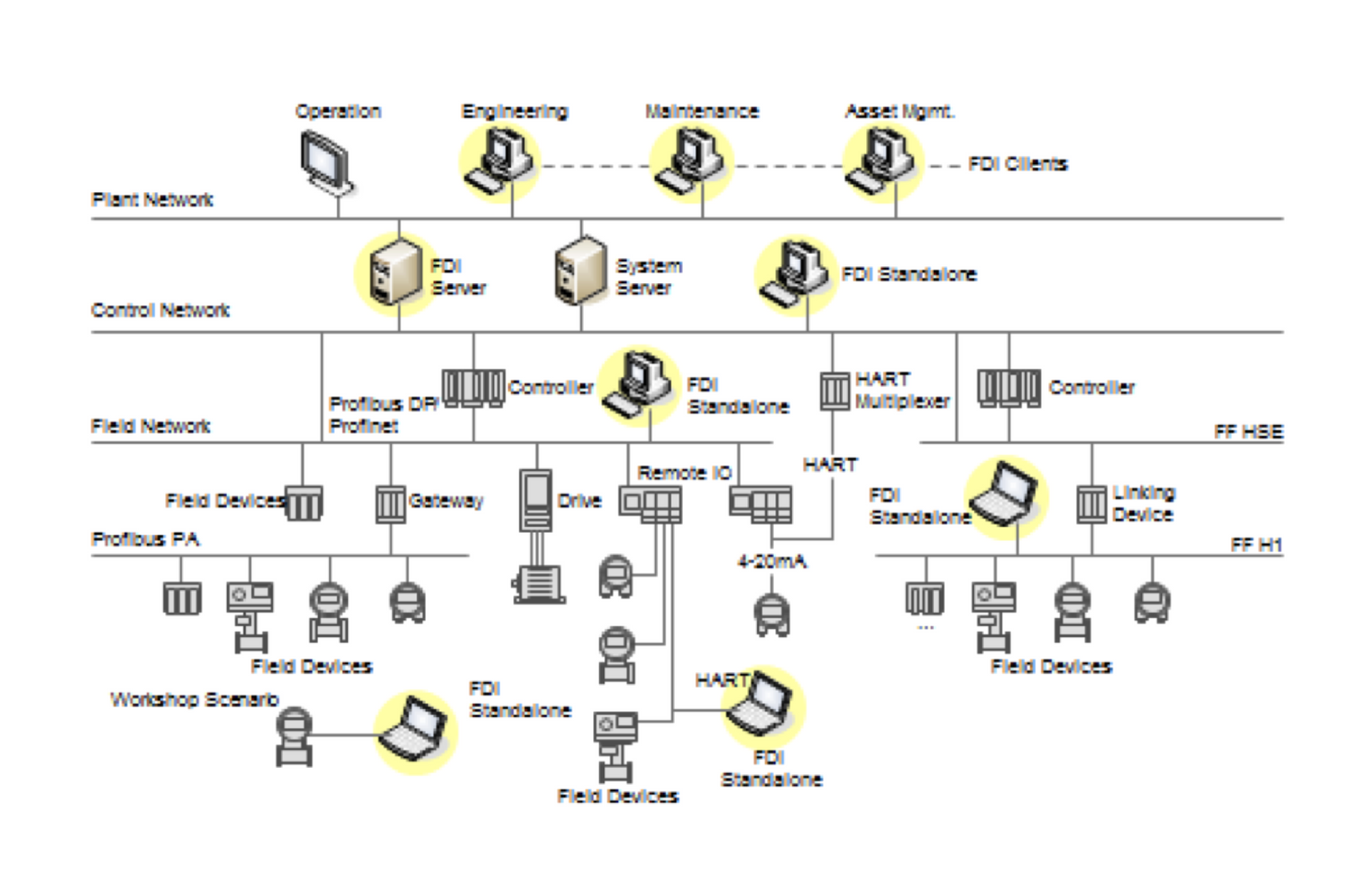
Security Features

- time stamping and digital signatures
- sandbox environments
- built-in security for OPC UA data exchange



Source: https://www.ask4fdi.com/new-index-1#/1package/

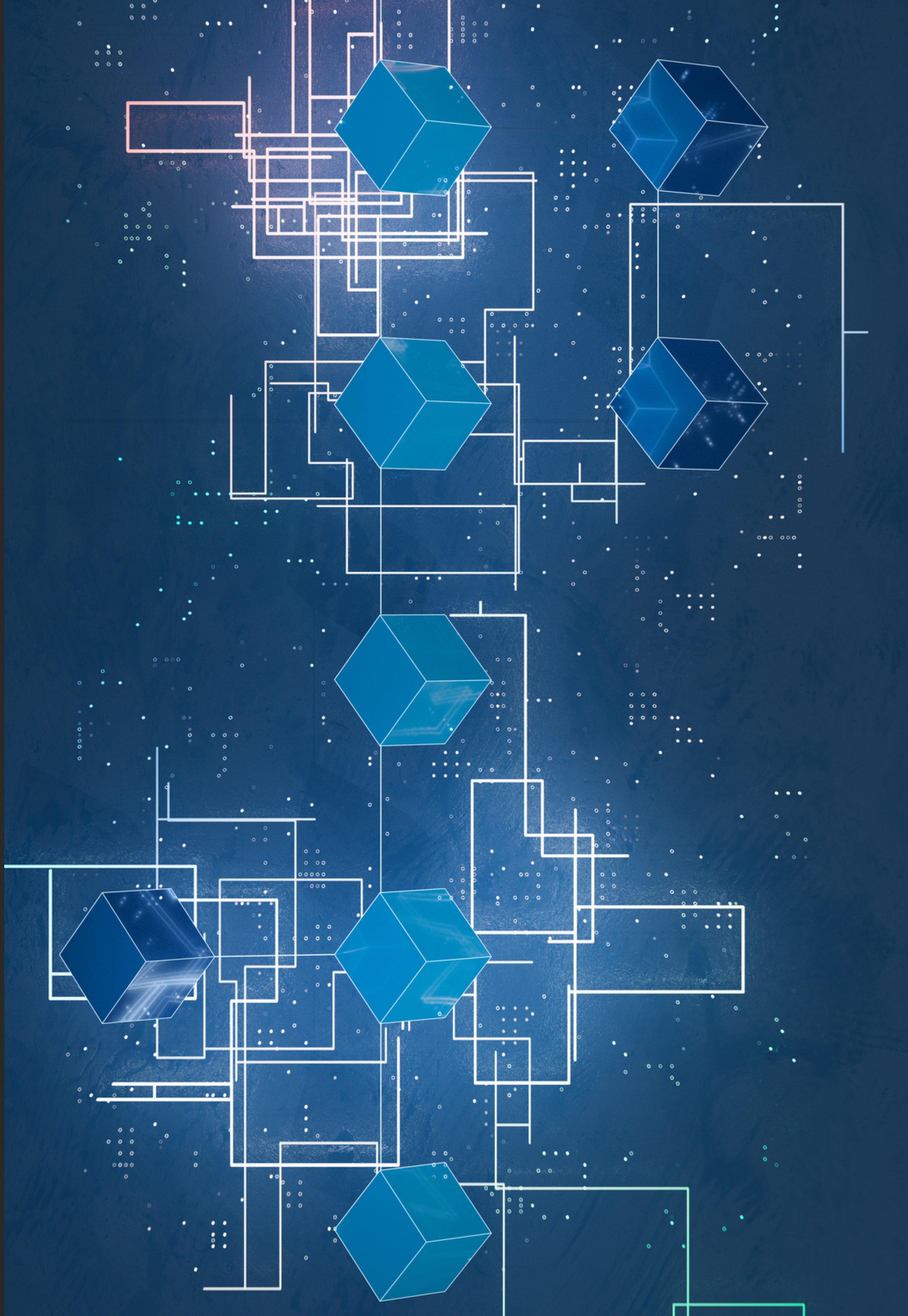
FDI Architecture



Source: https://www.fieldcommgroup.org/sites/default/files/imce_files/technology/documents/fdi-white-paper-2012.pdf

Blockchain ICS Integration

Sending Data from L3 to the Blockchain Network



E2EE PROTOCOL IS A KEY ELEMENT

matrix

Analyze E2EE Protocol Properties

e.g. Security, Efficieny, Usability and Blockchain Compatibility

E2EE protocol: Matrix

Matrix provides state-of-the-art end-to-end-encryption via the Olm and Megolm cryptographic ratchets.

What is Matrix?

- Open standard for interoperable, decentralised, real-time communication over IP.

Matrix is for:

- Group Chat (and 1:1)
- WebRTC Signalling
- Bridging Comms Silos
- Internet of Things Data
- ...and anything else which needs to pubsub persistent data to the world.

Source: https://matrix.org/docs/guides/

matrix

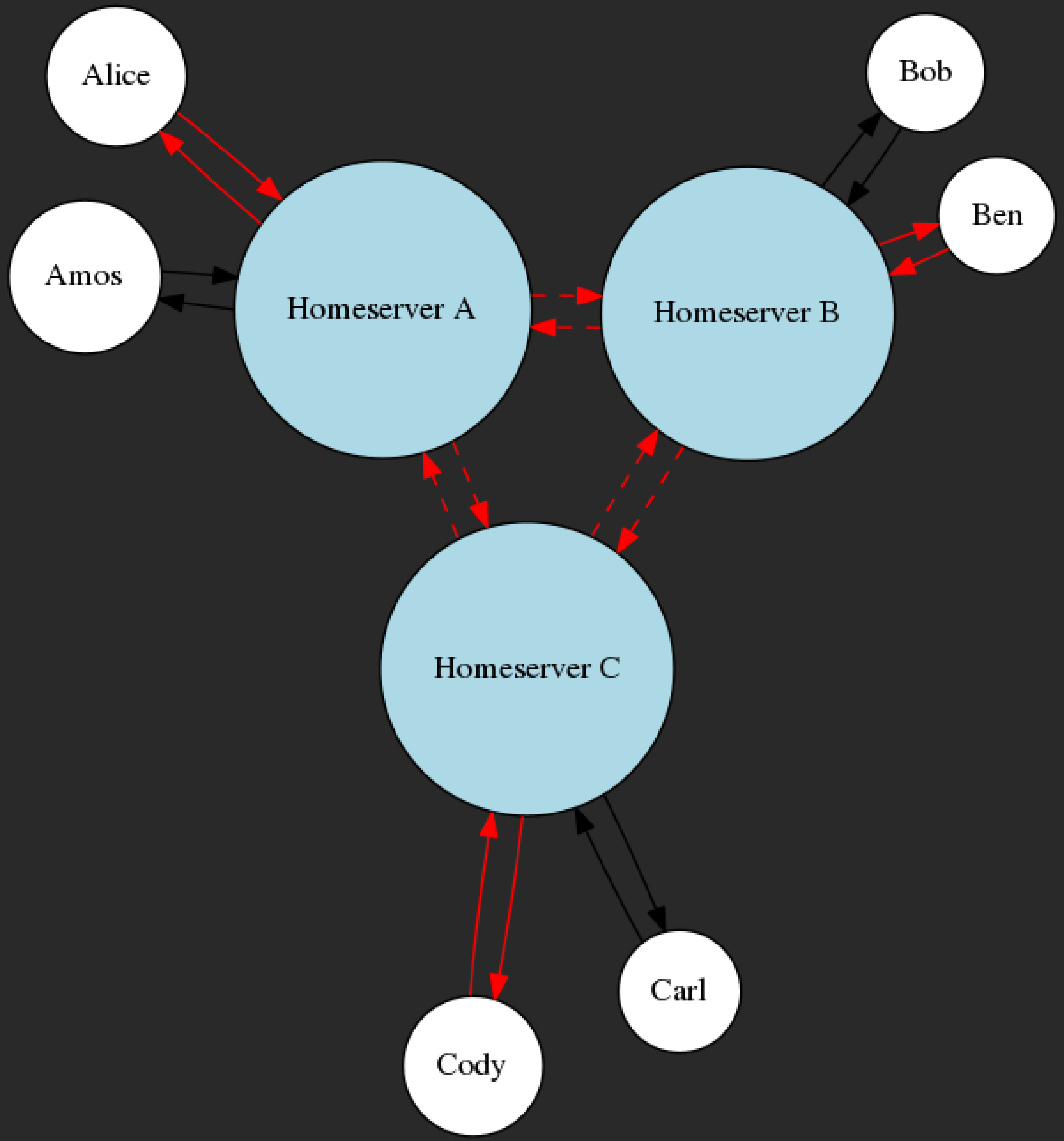
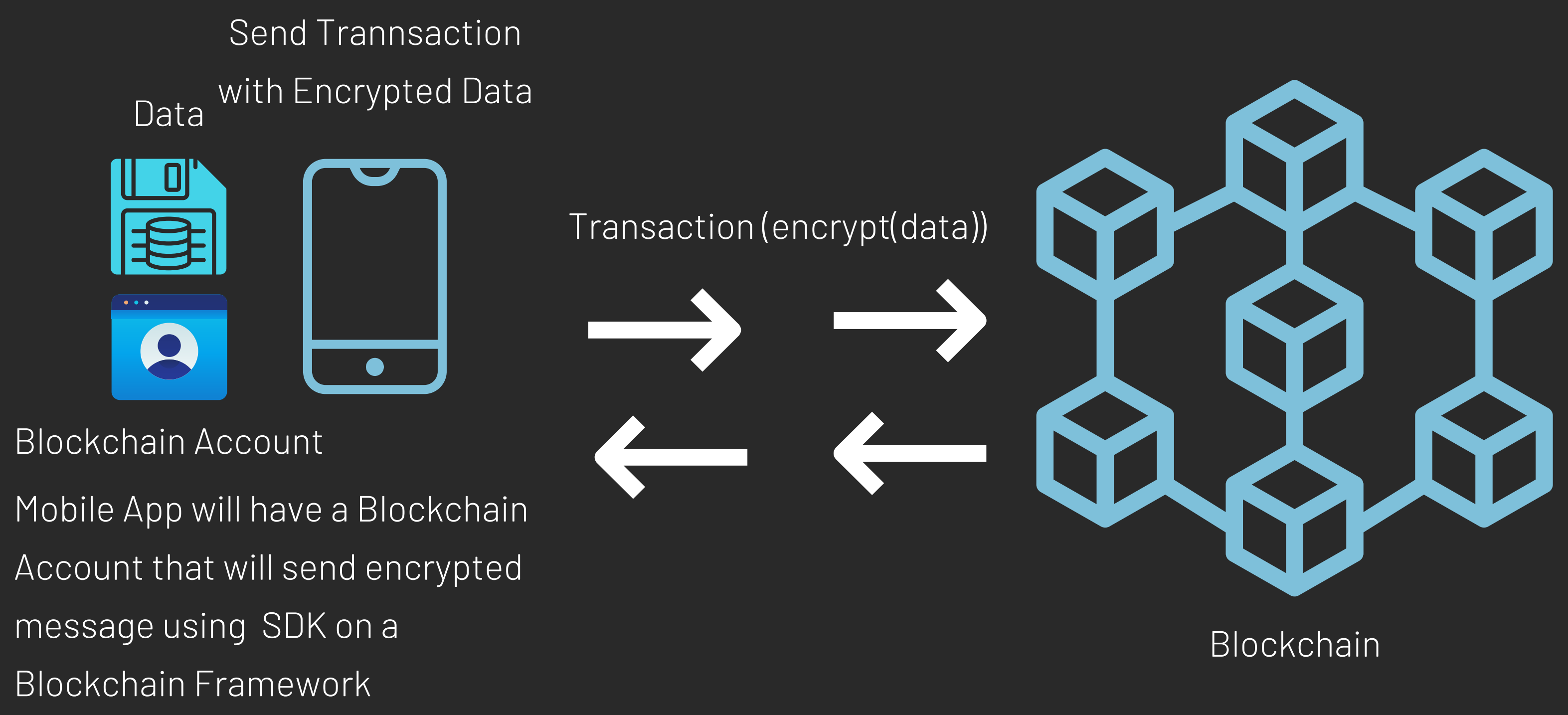


Image Source: https://www.marxwatch.org/matrix/federation.html

Integrate the concept to an ICS use Case



Send Trannsaction with Encrypted Data

Data

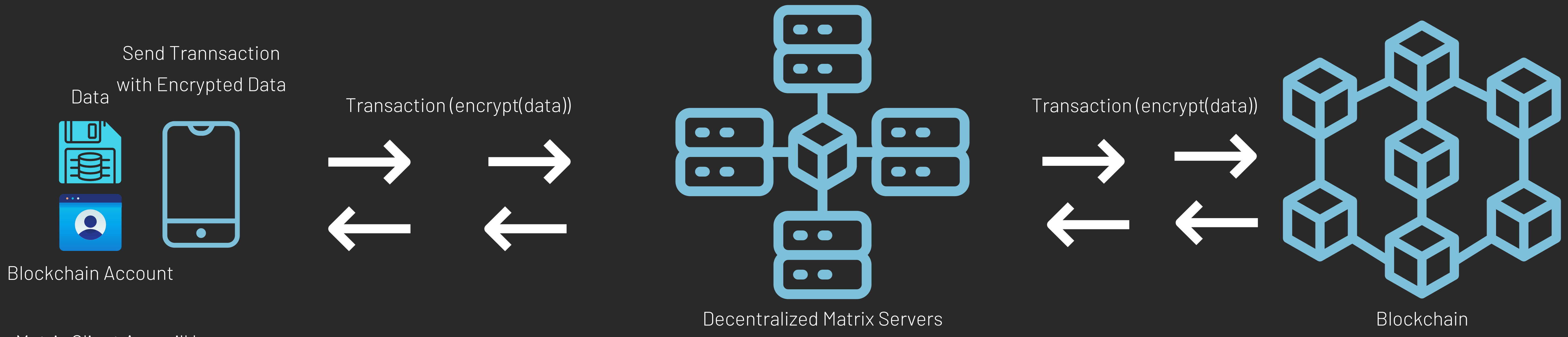
Transaction (encrypt(data))

Blockchain Account

Blockchain

Mobile App will have a Blockchain Account that will send encrypted message using SDK on a Blockchain Framework

Without Matrix E2EE Protocol



Send Trannsaction with Encrypted Data

Data

Transaction (encrypt(data))

Blockchain Account

Decentralized Matrix Servers

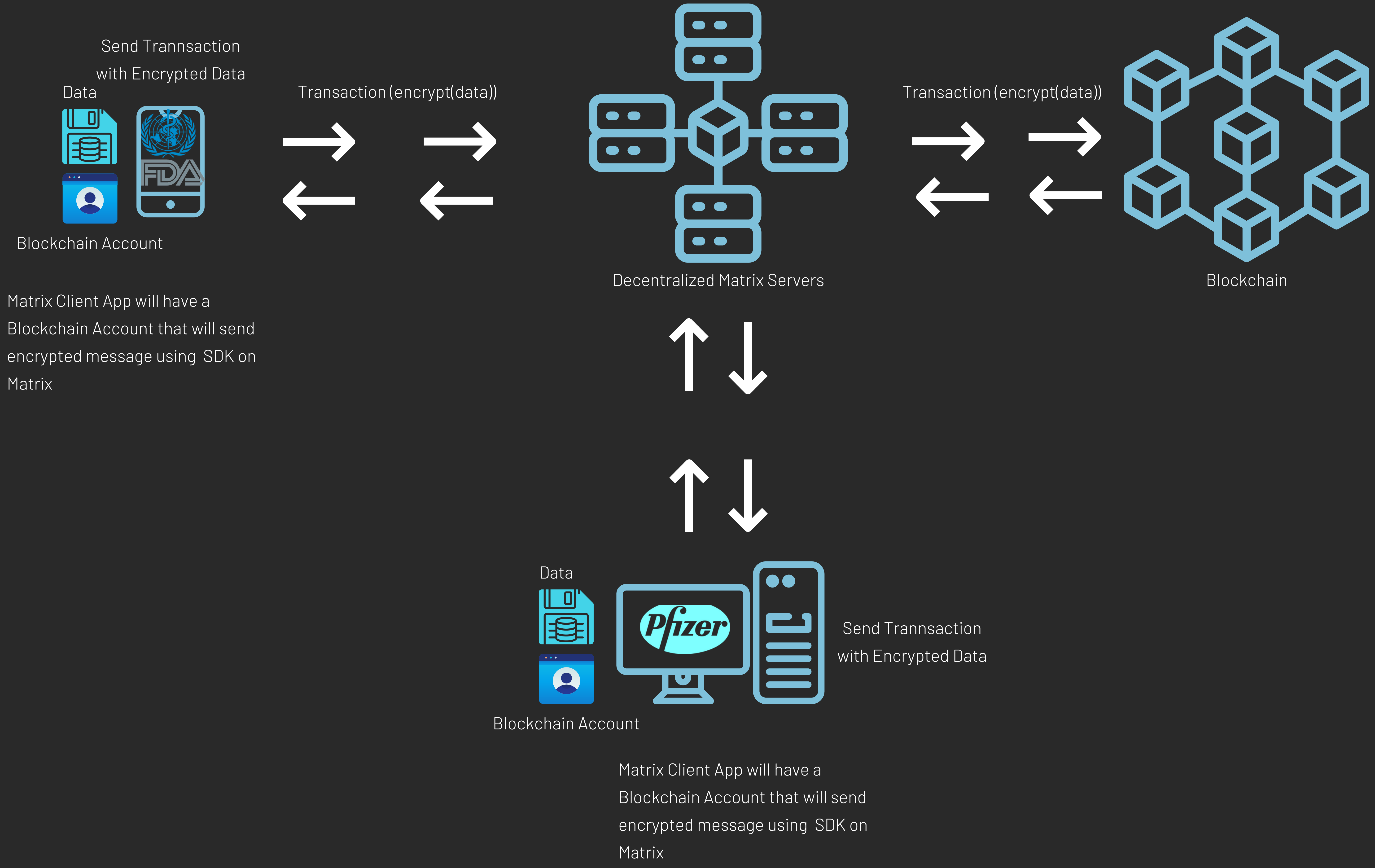
Transaction (encrypt(data))

Blockchain

Matrix Client App will have a Blockchain Account that will send encrypted message using SDK on Matrix

With Matrix E2EE Protocol

Integrate the concept to an ICS use Case



Send Trannsaction with Encrypted Data

Data

Blockchain Account

Matrix Client App will have a Blockchain Account that will send encrypted message using SDK on Matrix

Transaction (encrypt(data))

Decentralized Matrix Servers

Transaction (encrypt(data))

Blockchain

Data

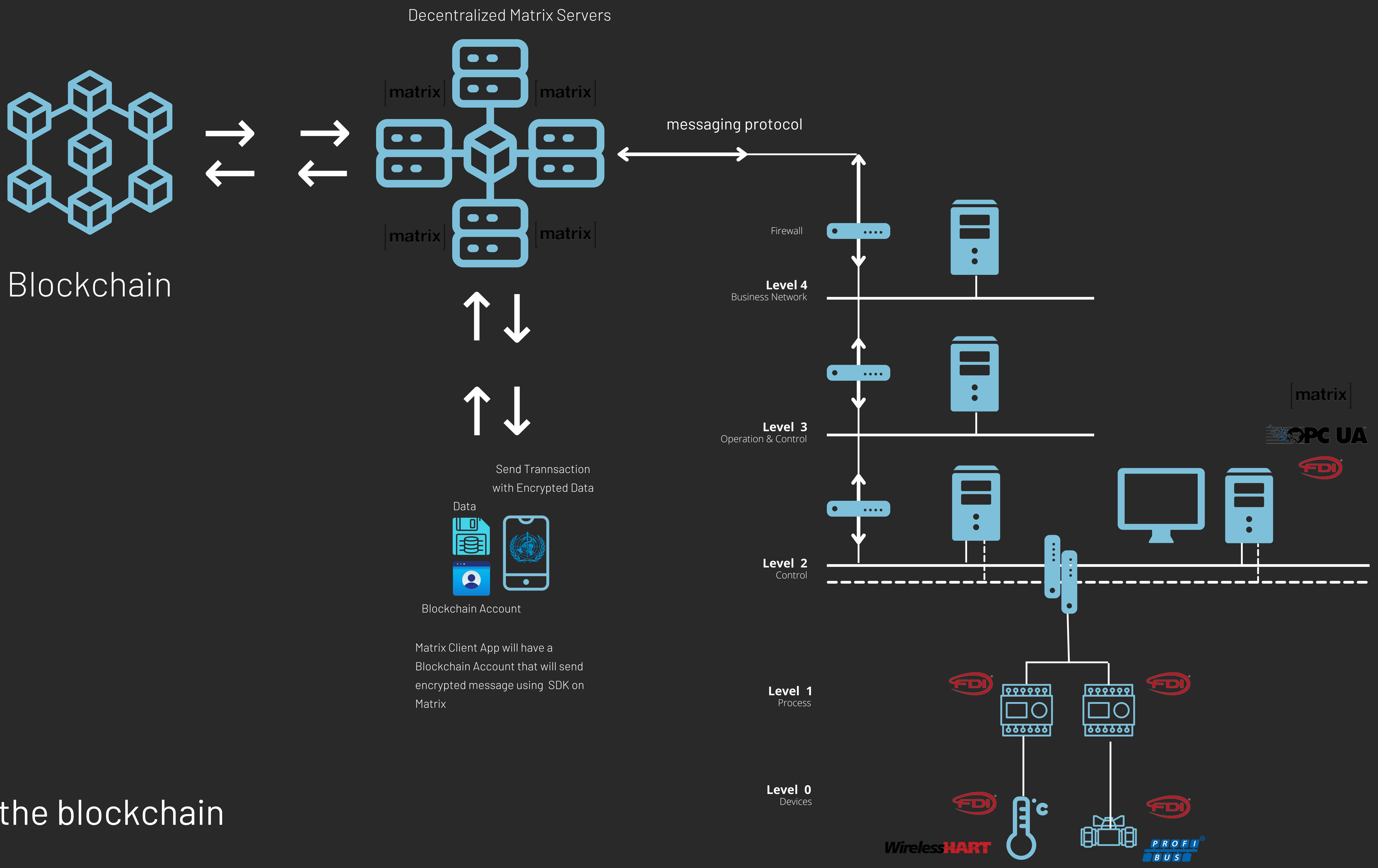
Blockchain Account

Send Trannsaction with Encrypted Data

Matrix Client App will have a Blockchain Account that will send encrypted message using SDK on Matrix

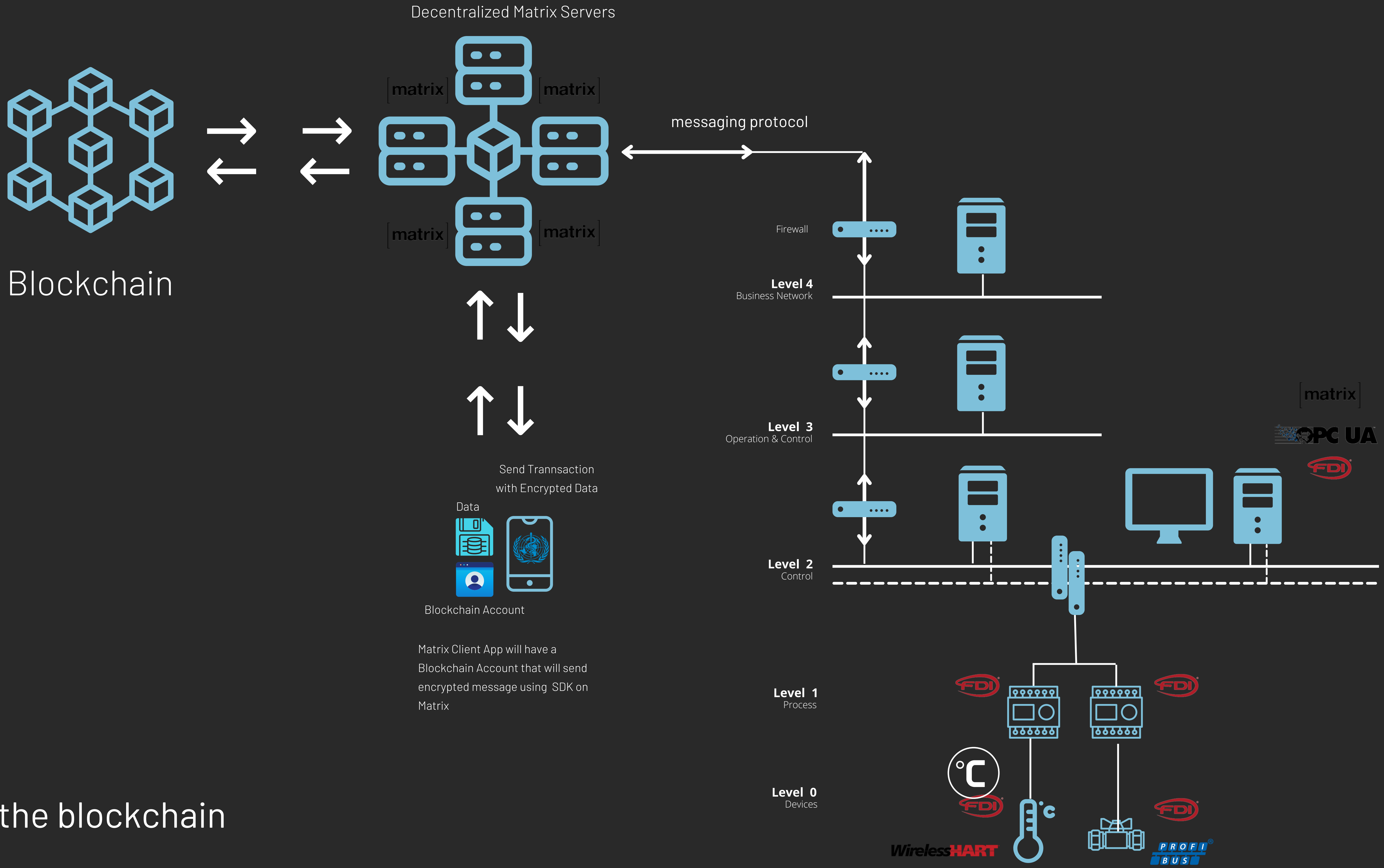
Blockchain ICS Integration

Combining the solution



Matrix Client App will have a Blockchain Account that will send encrypted message using SDK on Matrix

Sending data to the blockchain



Decentralized Matrix Servers

matrix

matrix

matrix

matrix

Blockchain

messaging protocol

Firewall

Level 4
Business Network

Level 3
Operation & Control

Level 2
Control

Level 1
Process

Level 0
Devices

matrix

OPC UA

FDI

Send Trannsaction
with Encrypted Data

Data

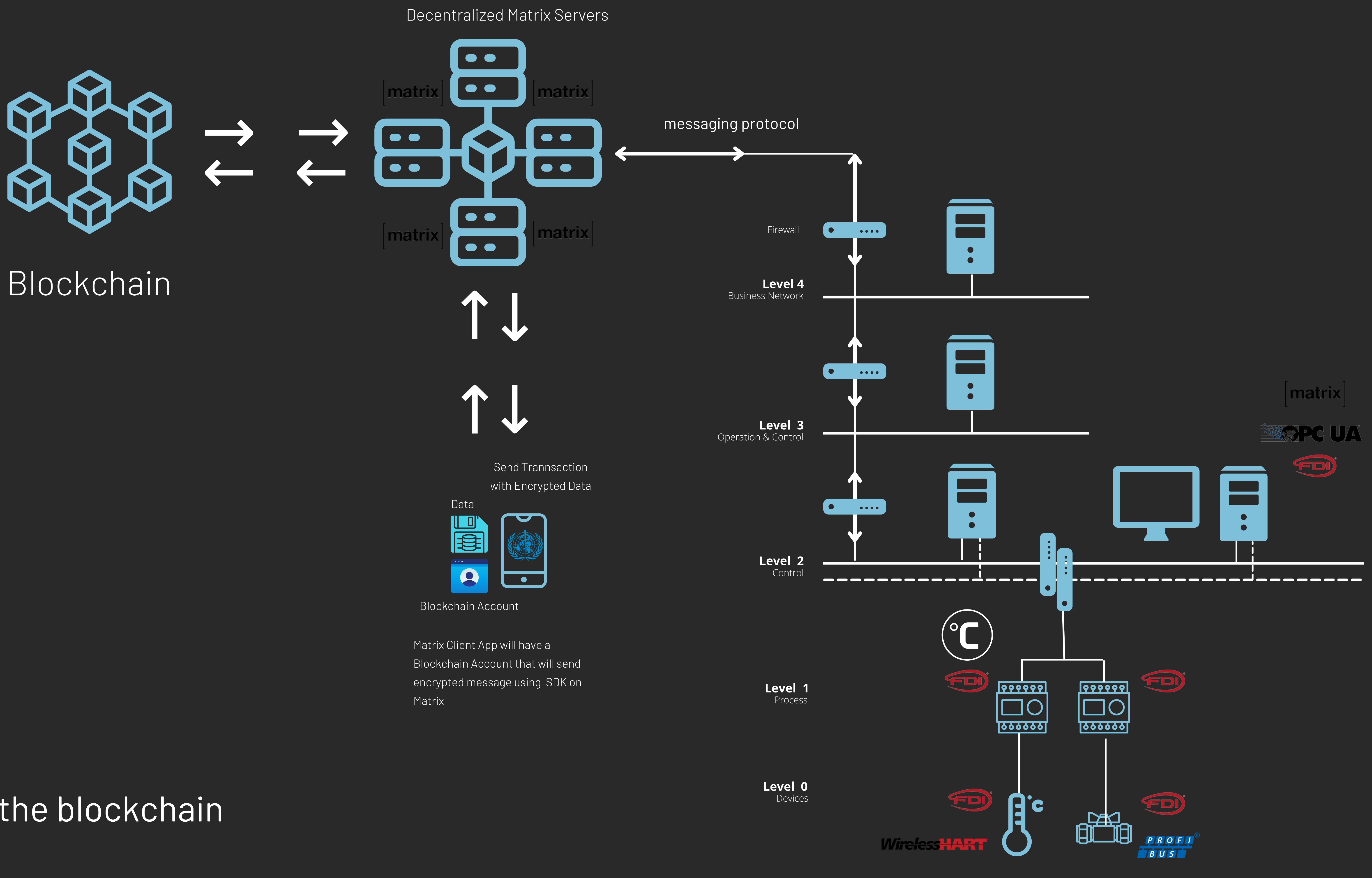
Blockchain Account

Matrix Client App will have a Blockchain Account that will send encrypted message using SDK on Matrix

WirelessHART

PROFIBUS

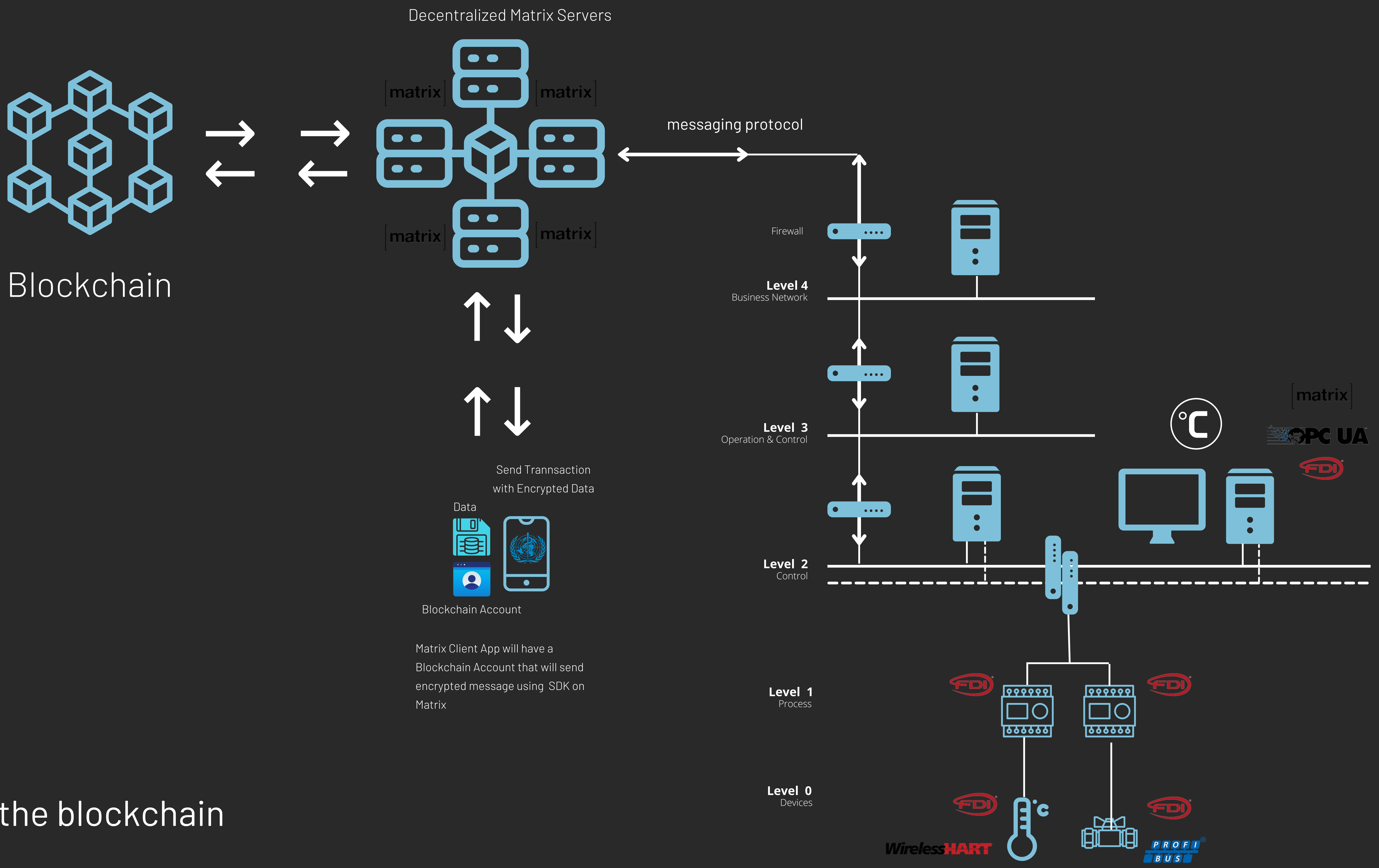
Sending data to the blockchain



Matrix Client App will have a Blockchain Account that will send encrypted message using SDK on Matrix

Sending data to the blockchain

Sending data to the blockchain



Decentralized Matrix Servers

matrix

matrix

matrix

matrix

Blockchain

messaging protocol

Firewall

Level 4
Business Network

Level 3
Operation & Control

Level 2
Control

Level 1
Process

Level 0
Devices

matrix

OPC UA

FDI

WirelessHART

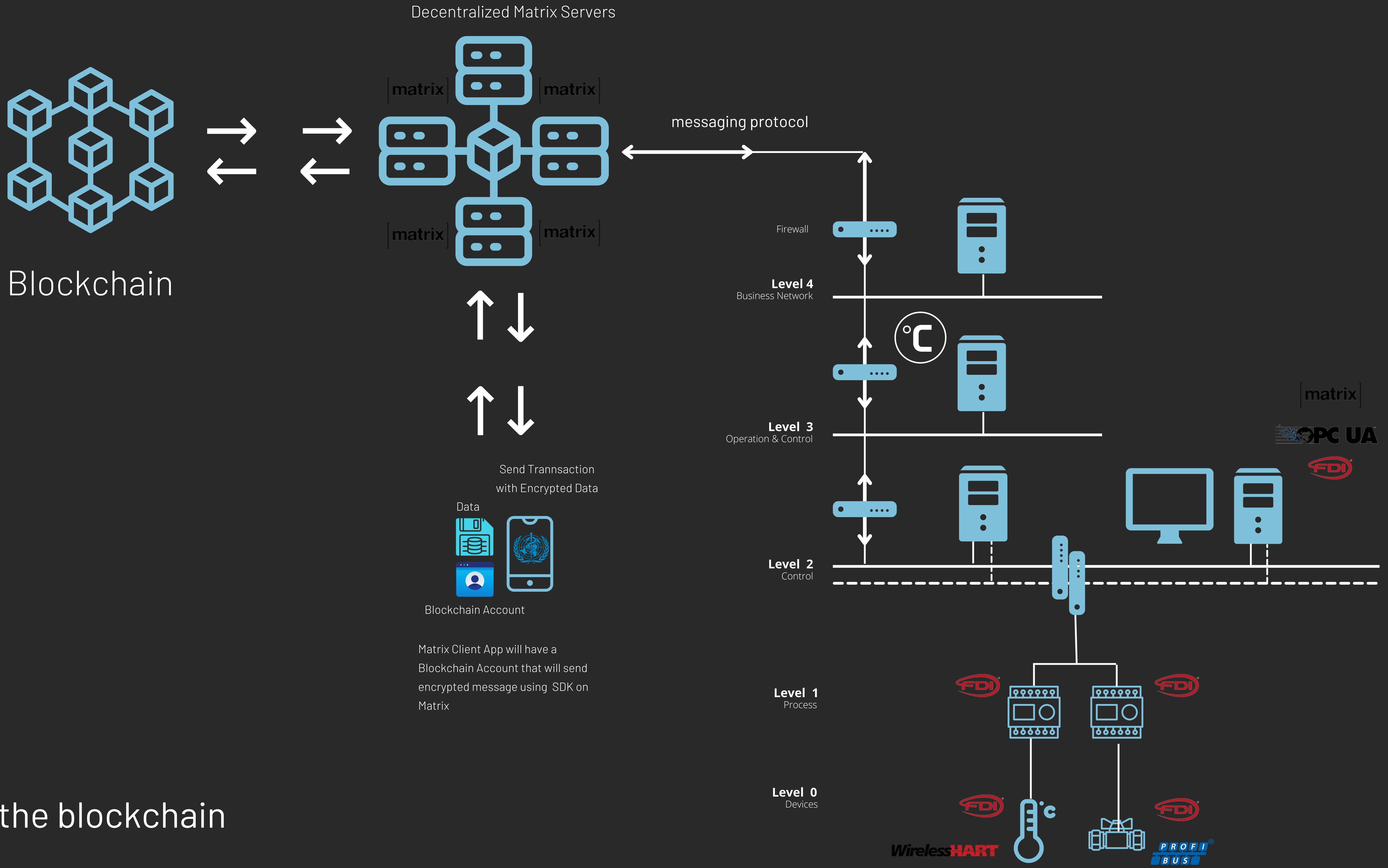
PROFI BUS

Send Trannsaction
with Encrypted Data

Data

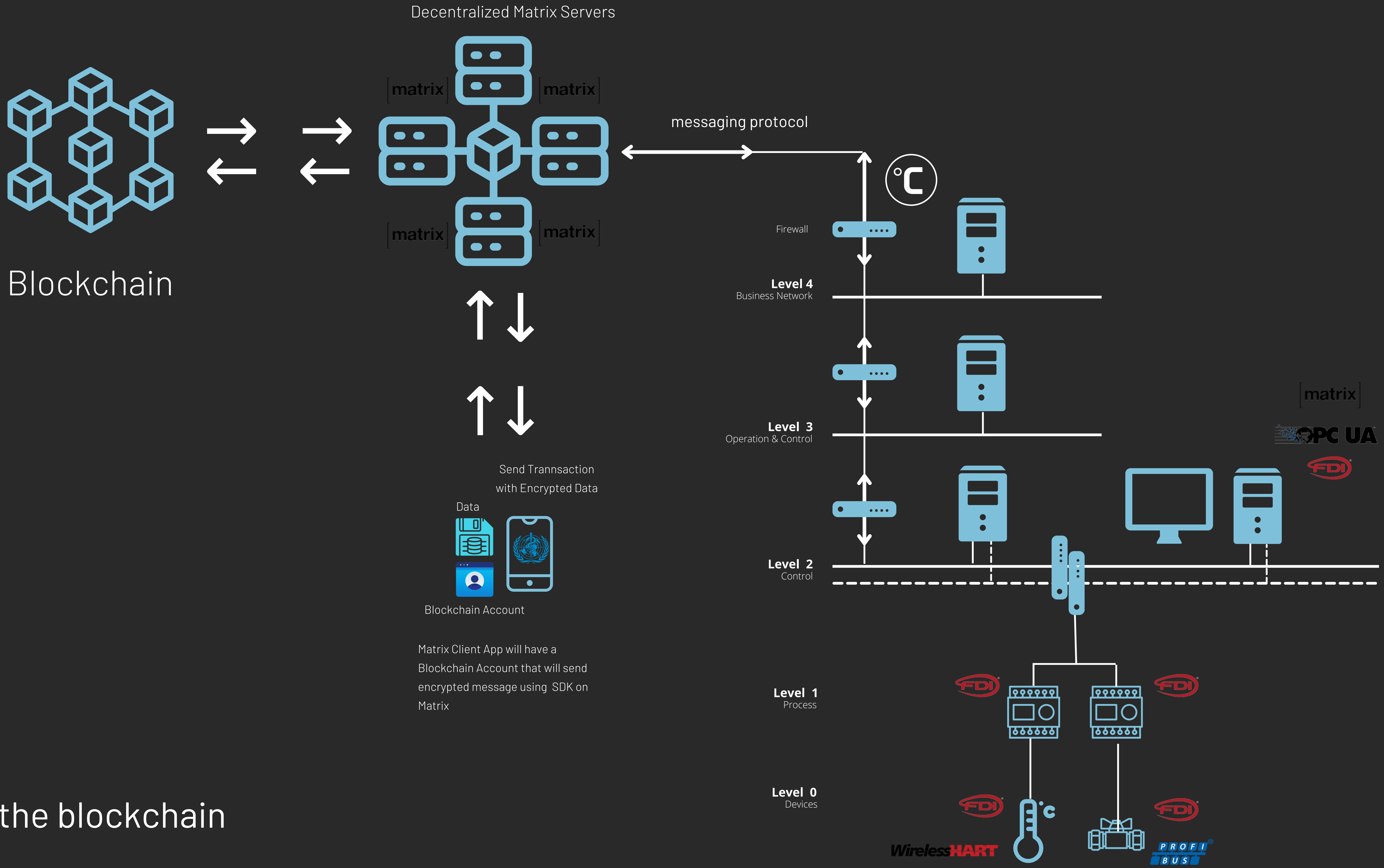
Blockchain Account

Matrix Client App will have a Blockchain Account that will send encrypted message using SDK on Matrix



Matrix Client App will have a Blockchain Account that will send encrypted message using SDK on Matrix

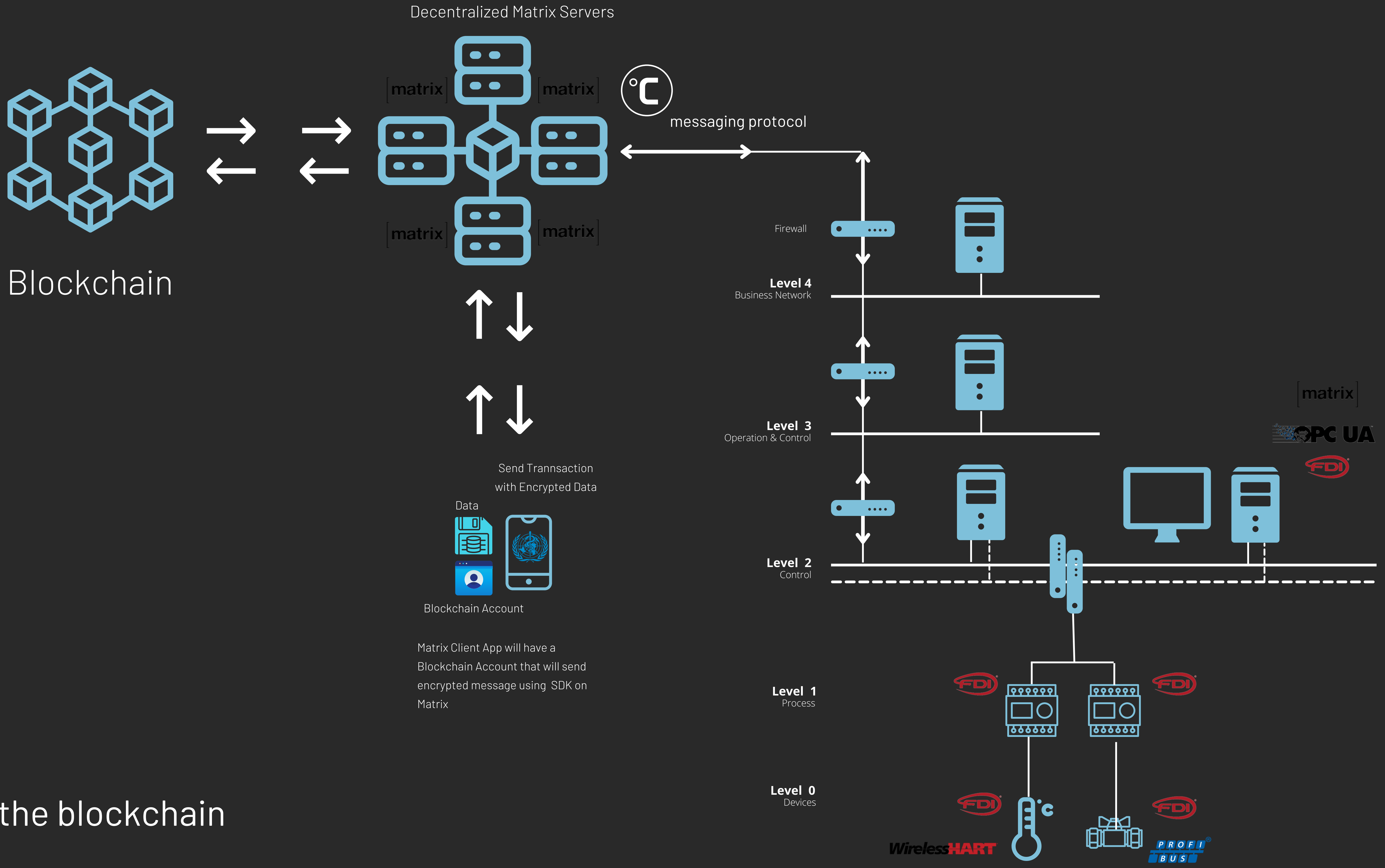
Sending data to the blockchain



Send Trannsaction with Encrypted Data

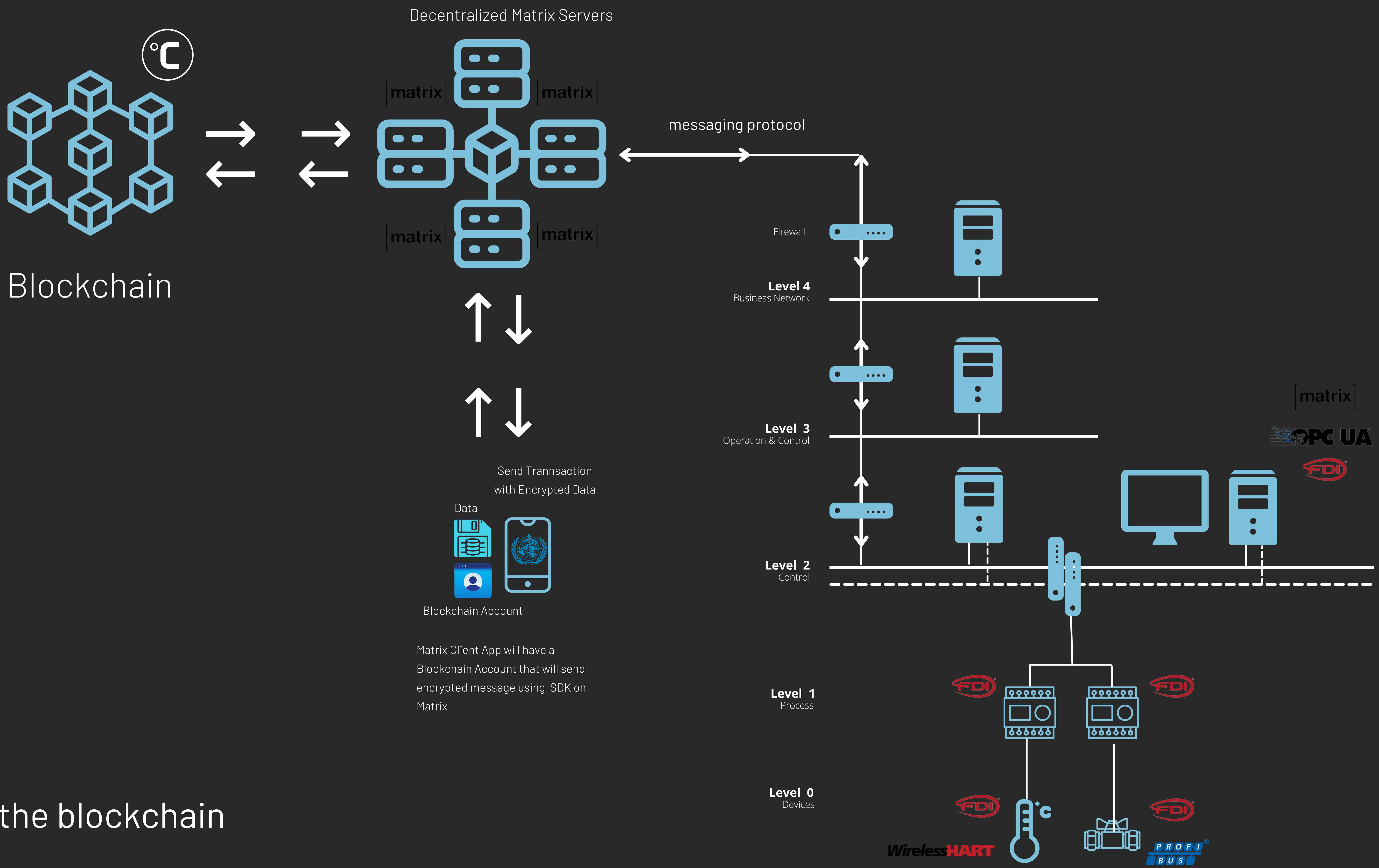
Matrix Client App will have a Blockchain Account that will send encrypted message using SDK on Matrix

Sending data to the blockchain



Matrix Client App will have a Blockchain Account that will send encrypted message using SDK on Matrix

Sending data to the blockchain



Decentralized Matrix Servers

Blockchain

messaging protocol

Firewall

Level 4
Business Network

Level 3
Operation & Control

Level 2
Control

Level 1
Process

Level 0
Devices

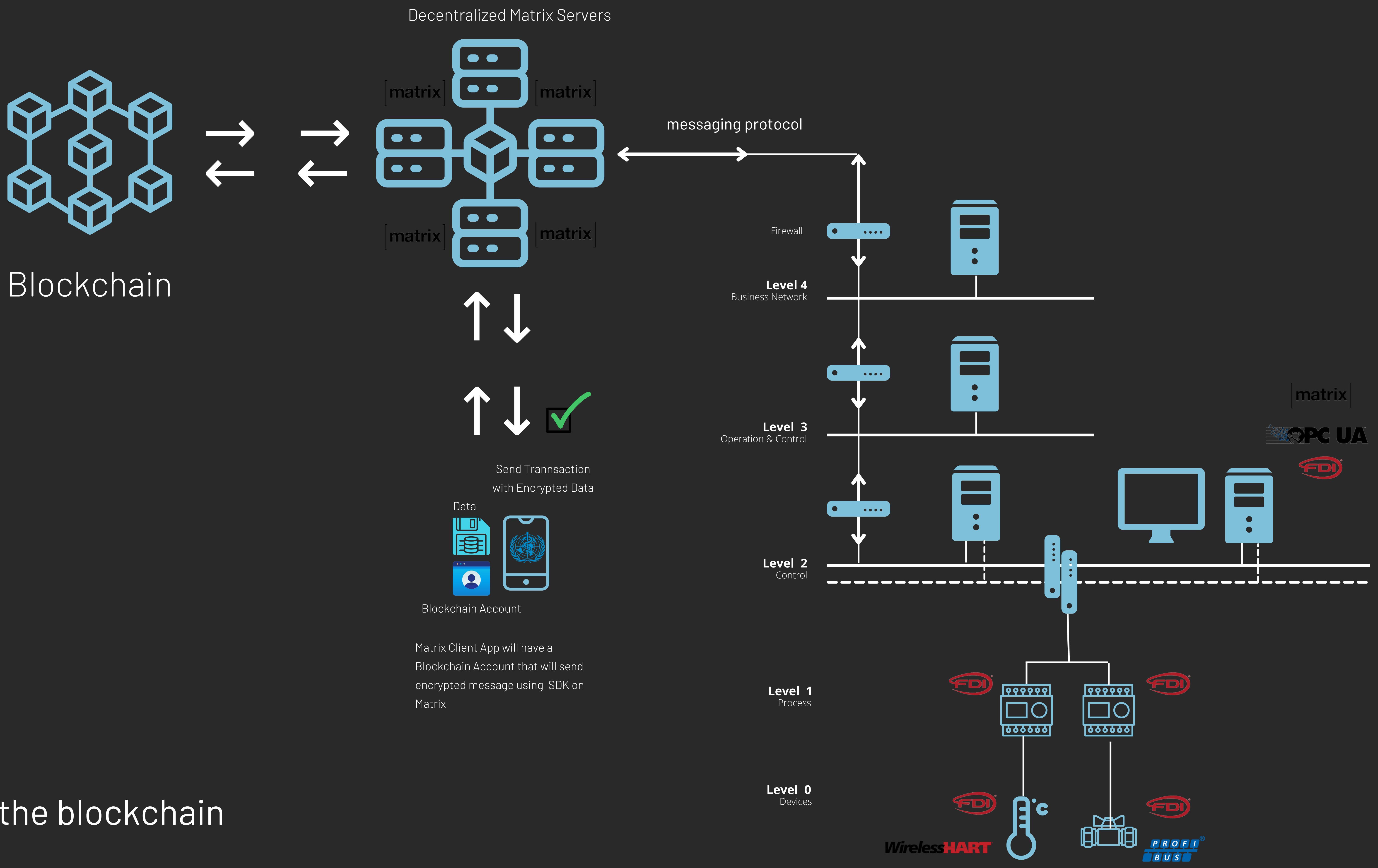
Send Trannsaction
with Encrypted Data

Data

Blockchain Account

Matrix Client App will have a Blockchain Account that will send encrypted message using SDK on Matrix

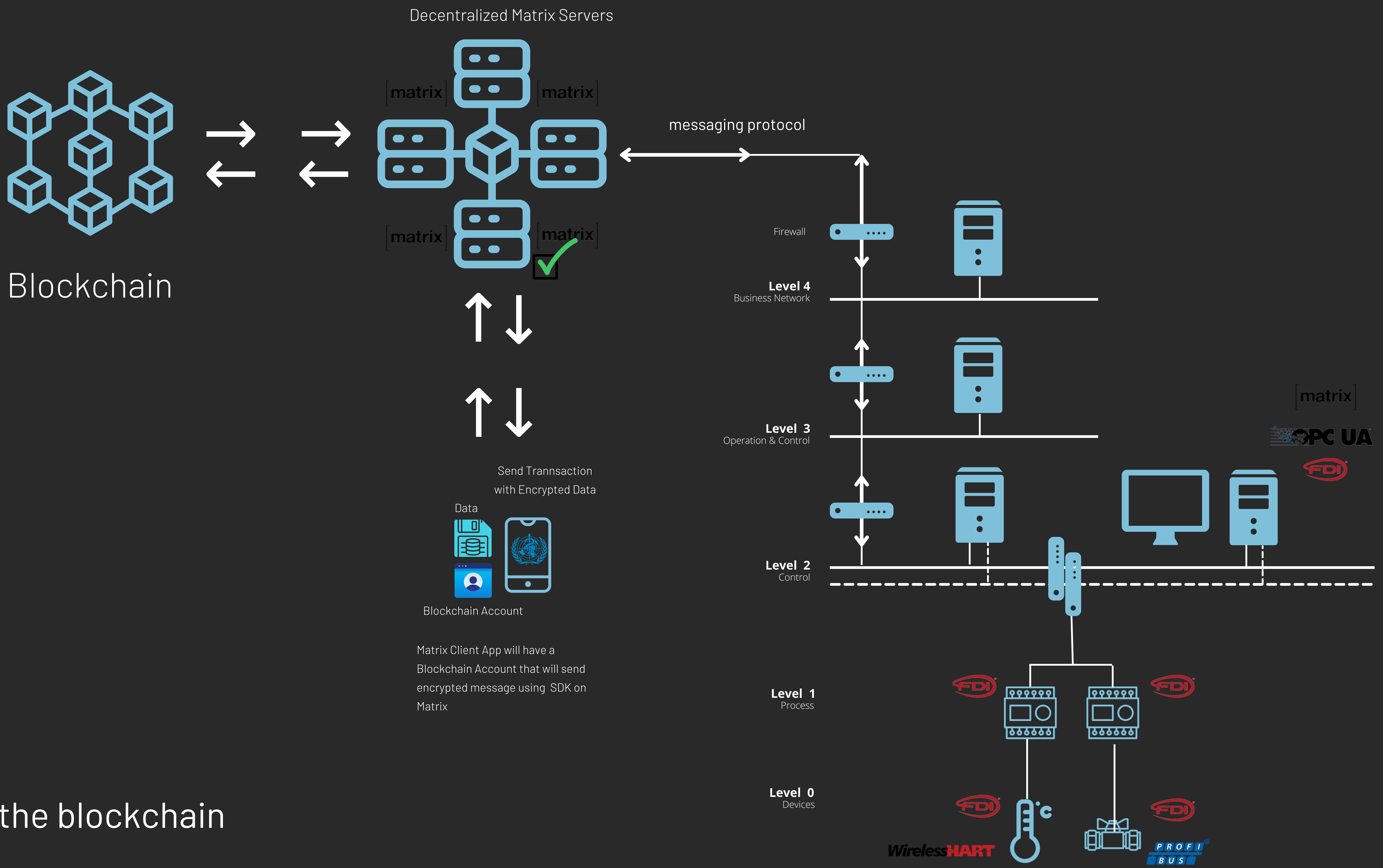
Sending data to the blockchain



Send Trannsaction with Encrypted Data

Matrix Client App will have a Blockchain Account that will send encrypted message using SDK on Matrix

Sending data to the blockchain



Decentralized Matrix Servers

matrix

matrix

matrix

matrix

Blockchain

messaging protocol

Send Trannsaction
with Encrypted Data

Data

Blockchain Account

Matrix Client App will have a Blockchain Account that will send encrypted message using SDK on Matrix

Firewall

Level 4
Business Network

Level 3
Operation & Control

Level 2
Control

Level 1
Process

Level 0
Devices

matrix

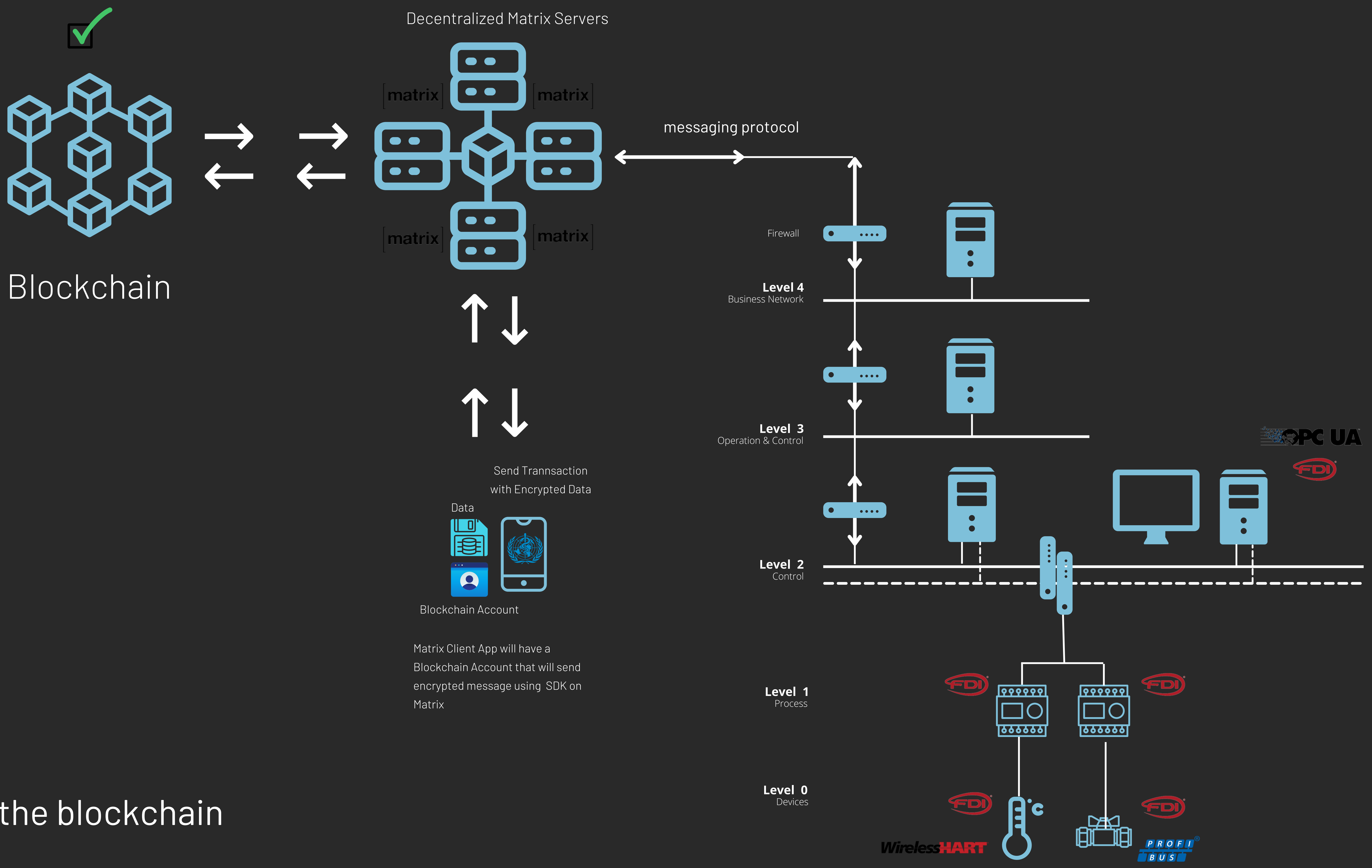
OPC UA

FDI

WirelessHART

PROFI BUS

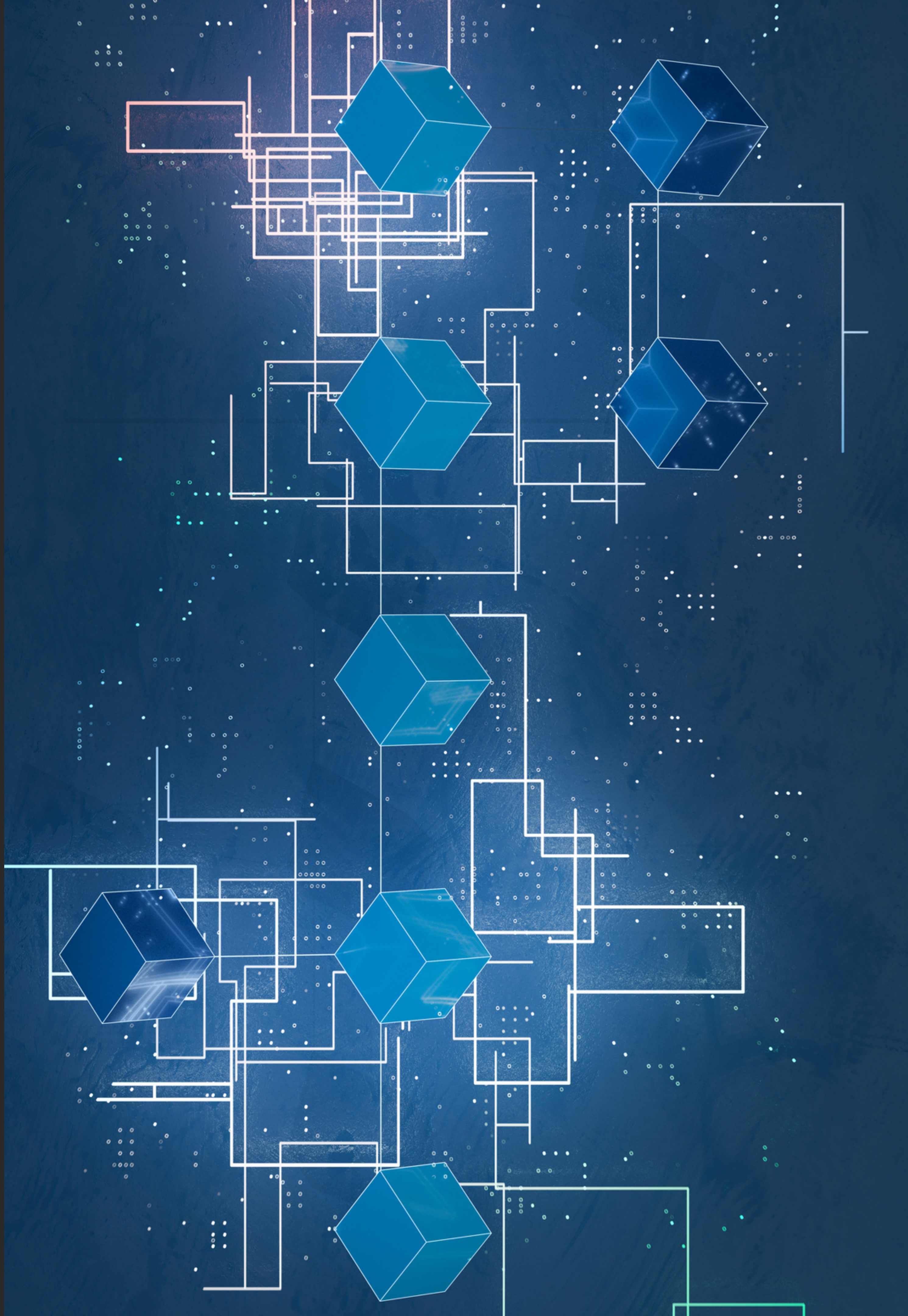
Sending data to the blockchain



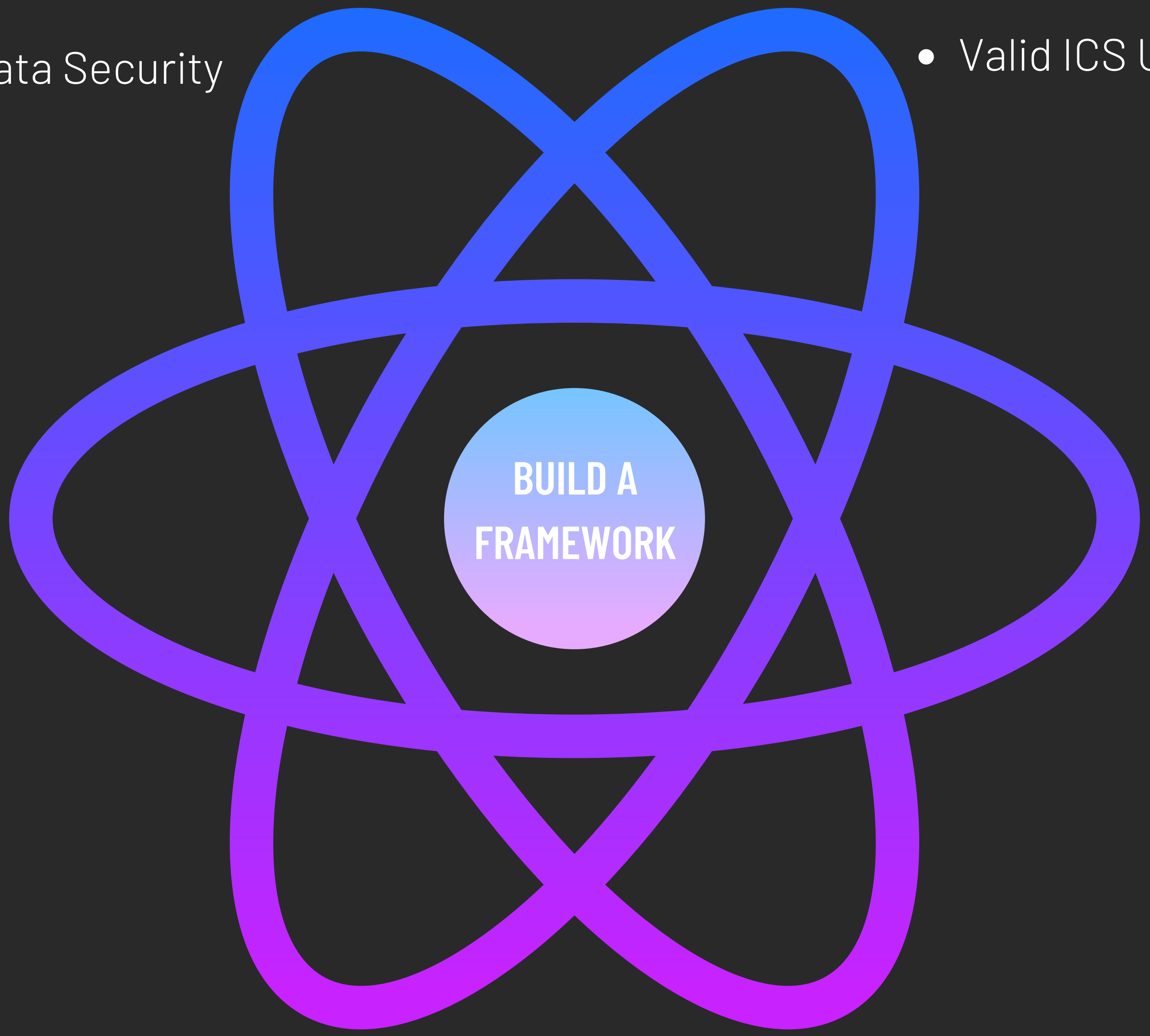
Matrix Client App will have a Blockchain Account that will send encrypted message using SDK on Matrix

Sending data to the blockchain

Blockchain Security Framework



BUILD A BLOCKCHAIN SECURITY FRAMEWORK



IDENTIFY THE RISK

- Data Security

REGULATE THE PURPOSE

- Valid ICS Use Cases

SECURITY REQUIREMENTS

- End to End Solution
  - Securing Data Transmission
    - L0-L3 Network
    - L3 to Blockchain Network

COMPATIBILITY REQUIREMENTS

- Technology Integration Validation
  - E2EE Properties
  - Blockchain Properties
  - IIoT Properties
  - Traditional Industrial Devices Properites

EXISTING SECURITY STANDARDS

- Purdue Model Architecture
  - ISA Secure
  - SDLA

GOVERNMENT COMPLIANCE

- Federal and State Regulations

Lloyd Kenneth Tugbo & Chimmy Arian Hilis