Blockchain Technology Applications

Amit Vishwakarma
Under the Supervision of:
Prof Y. N. Singh, Prof Haiwang Zhong

IIT Kanpur, Tsinghua University

amitv@iitk.ac.in

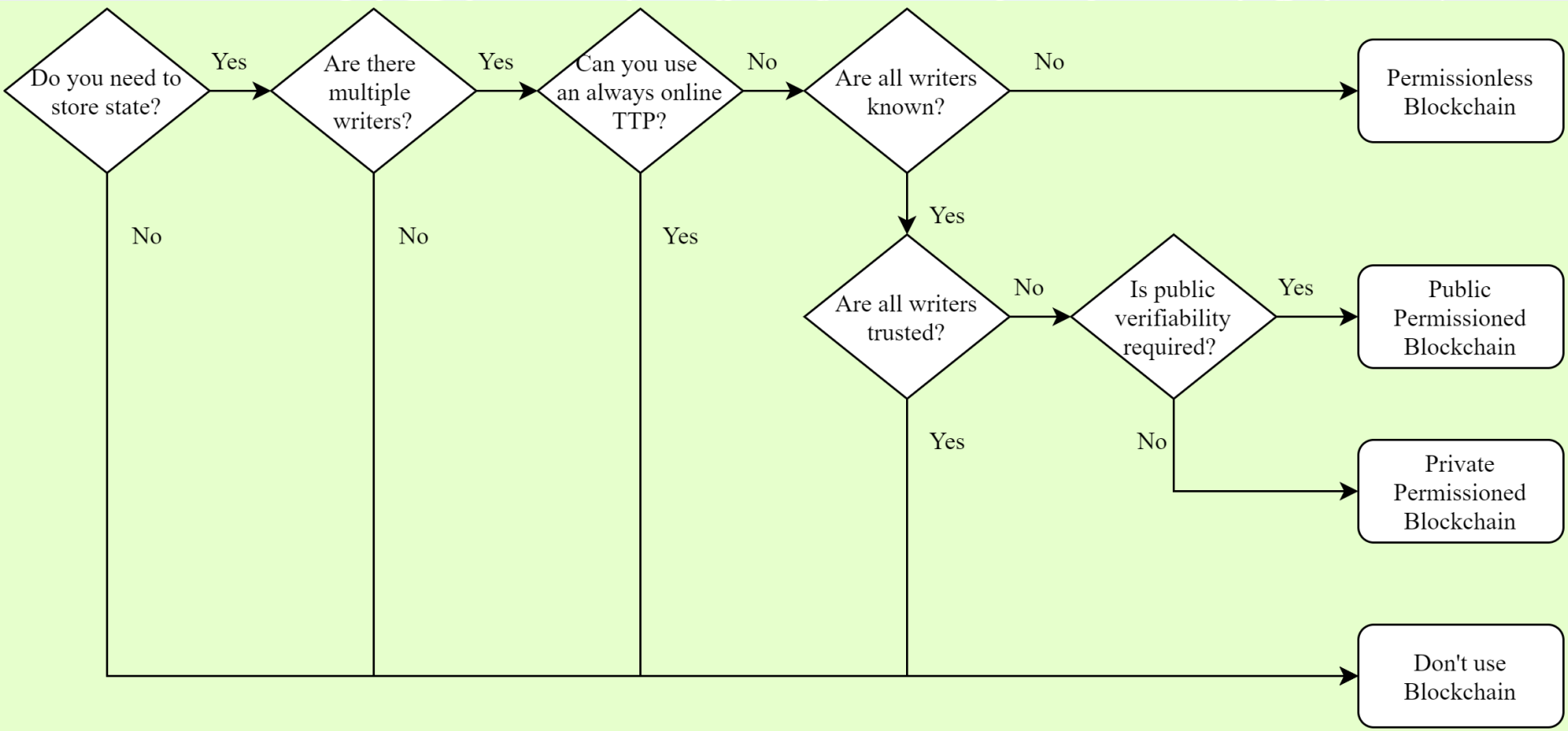
June 24, 2020

Table of Content

Blockchain Technology Application

- Do you really need blockchain?
- Will only blockchain can solve?
- What type of blockchain fit for your research?
- Who are the players?
- What is the overhead?
- Is the overhead tolerable?
- How will you encourage mining if no rewards?

Blockchain Technology Application



Blockchain Technology Application

Blockchain ≠ Bitcoin

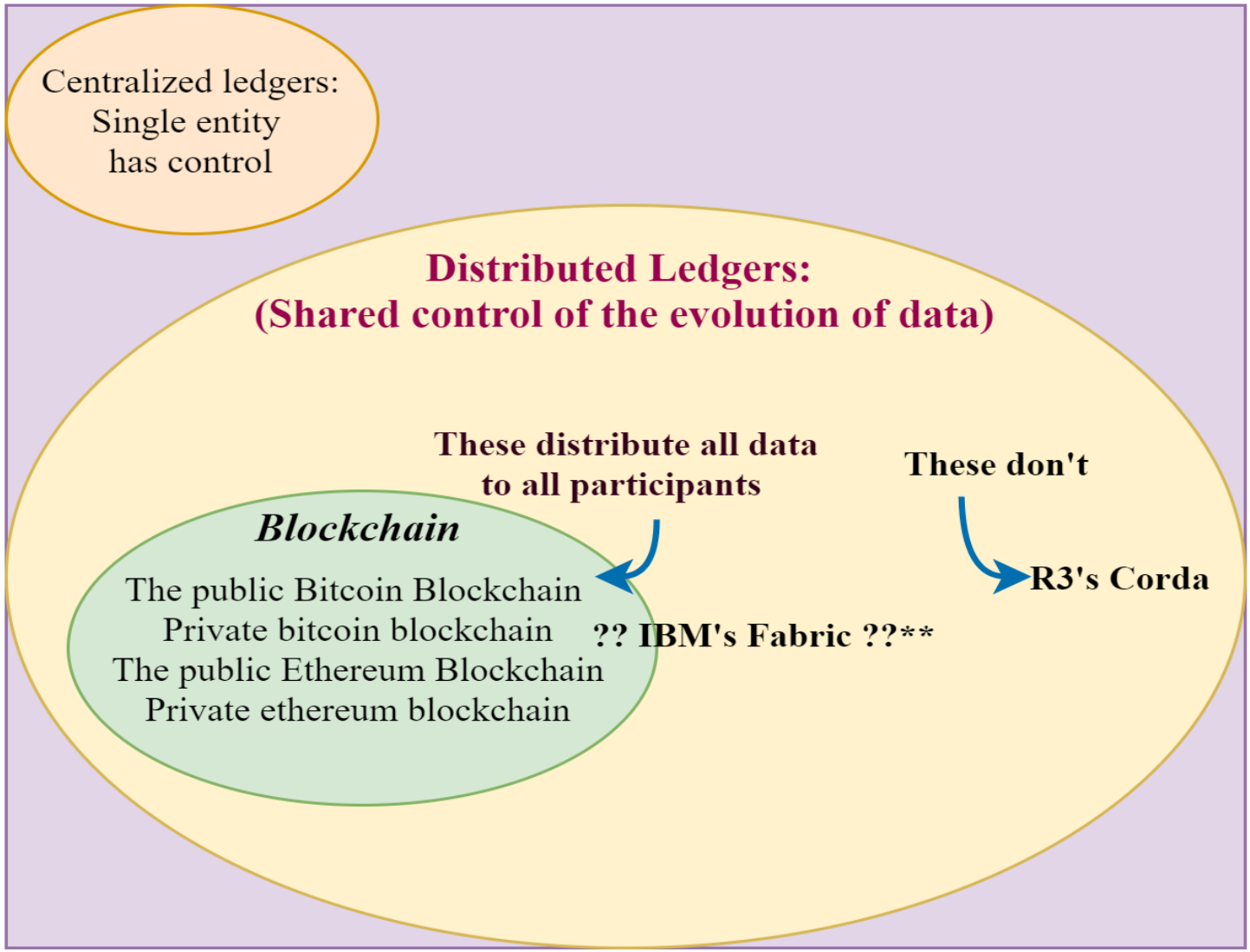
Bitcoin

Blockchain

- The leading digital currency
- Numerous customers and financial service payment applications, particularly in developing economics
- A favorite for speculators given its volatility and liquidity, with high frequency trading and hedge fund participation

- Distributed ledger with cryptographic integrity
- Potential replacement for middle-ware networks and clearing houses in financial transactions where 3rd party verification is required
- Application extended to other networks where veracity is critical to performance

DLT ≠ Blockchain



Smart vs Traditional Contracts

Traditional Physical Contracts

- Created by legal professionals
- contains legal language
- vast amounts of printed documents
- heavily rely on third parties for enforcement
- If things go bad, rely on the public judicial system

Smart Contracts

- created by computer programmers
- entirely digital and written using programming code
- defines the rules and consequences
- stating the obligations, benefits and penalties
- code can be automatically executed by a distributed ledger system

Industrial Blockchain Benefits

- Reduce costs and complexity
- Trusted record-keeping
- Improve discover-ability
- Shared trusted processes

Patterns for Customer Adoption

1. Internal ledger

- Ledger for internal reporting, audit and compliance's
- Consistent view of key business assets
- Provenance, immutability and finality more important than consensus
- Access to auditor and regulator

2. Consortium Shared Ledger

- Created by a small set of participants
- Share reference data between themselves and consumers
- Consistent real-time view of key information

Patterns for Customer Adoption

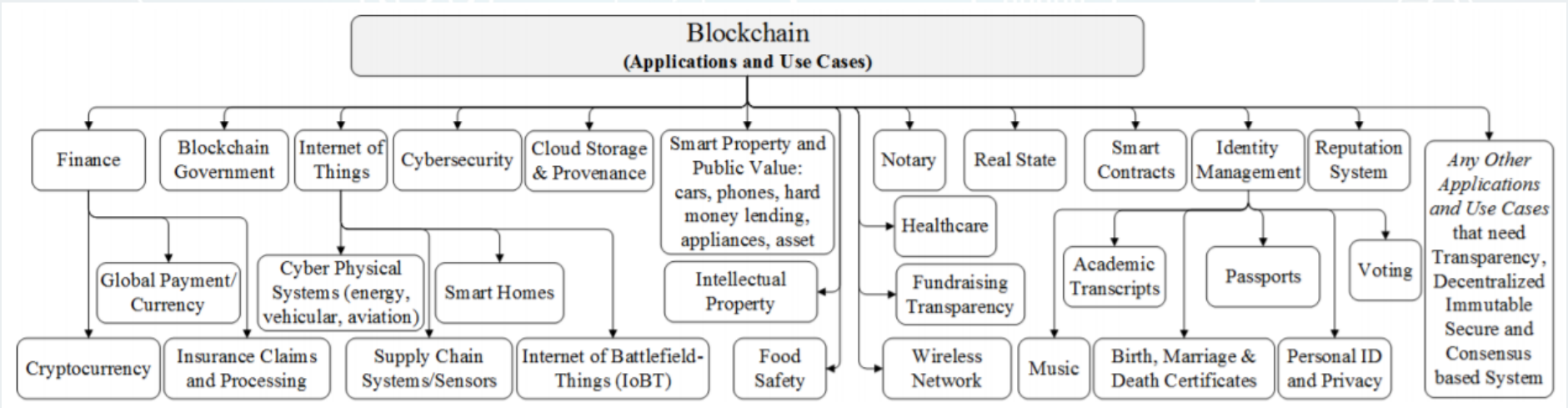
3. Information Hub

- A ledger set up in a single organization Sharing of information between participants (e.g. voting, dividend notification)
- Assets have information, not financial value
- Require provenance, immutability and finality

4. High Value Market

- Ledger for the transfer of high financial value assets
- between many participants in a market
- Requires all enterprise features of blockchain

Blockchain Technology Application



Use Case - Letter of credit

What?

- Bank handling LOC wants to offer then to a wider range of clients including startups
- Currently constrained by costs and the time to execute

How?

- Blockchain provides common ledger for LOC
- Allows bank and counter-parties to have the same validated record of transaction and fulfillment

Benefits

- Increased trust
- Increase speed of execution (Less than 1 day)
- vastly reduced cost

Use Case - Corporate Debt

What?

Bank holding a corporate debt would like to

- pay vendors quickly for transactions validated by the client
- allow the corporate client to see the payment is made
- provide government with oversight of the process

How?

- Blockchain provides a common ledger for recording the corporate debt / bond
- available to bank, corporate client, vendors and government

Benefits

- Speeds up vendor payment bigger net discounts
- Eliminates risk and accelerates decision making
- Owning bank can spread the across each market

Use Case - Business to Business Contracts

What?

- Buyer wants efficient way of converting a purchase order into validated, self executing contract updated to reflect the status of the supply
- Agreement must be visible to the buyer, the seller, banks, logistics partners and other stakeholders

How?

- Blockchain provides a shared record of the contract status which is updated as the contract progresses
- Available to all parties to the agreement, their banks and partners

Benefits

- increased efficiency and transparency across the supply chain
- risk management improved through the near real time update of all contracts

Use Case - Open, Trusted Supply Chain

What?

- Consumers demanding transparency on where and how their products are made
- people requires more information about corporate supply chains, with penalties for non-compliance

How?

- Blockchain enable safe digital transfer of property across the end to end supply chain

Benefits

- verifiable, preventing any party from altering
- efficiencies through greater transparency
- consumers can make informed purchases
- governments get reliable information

Use Case - Aircraft Maintenance

What?

- Provenance of each component part in complex system hard to track
- Manufacturer, production date, batch and even the manufacturing machine program

How?

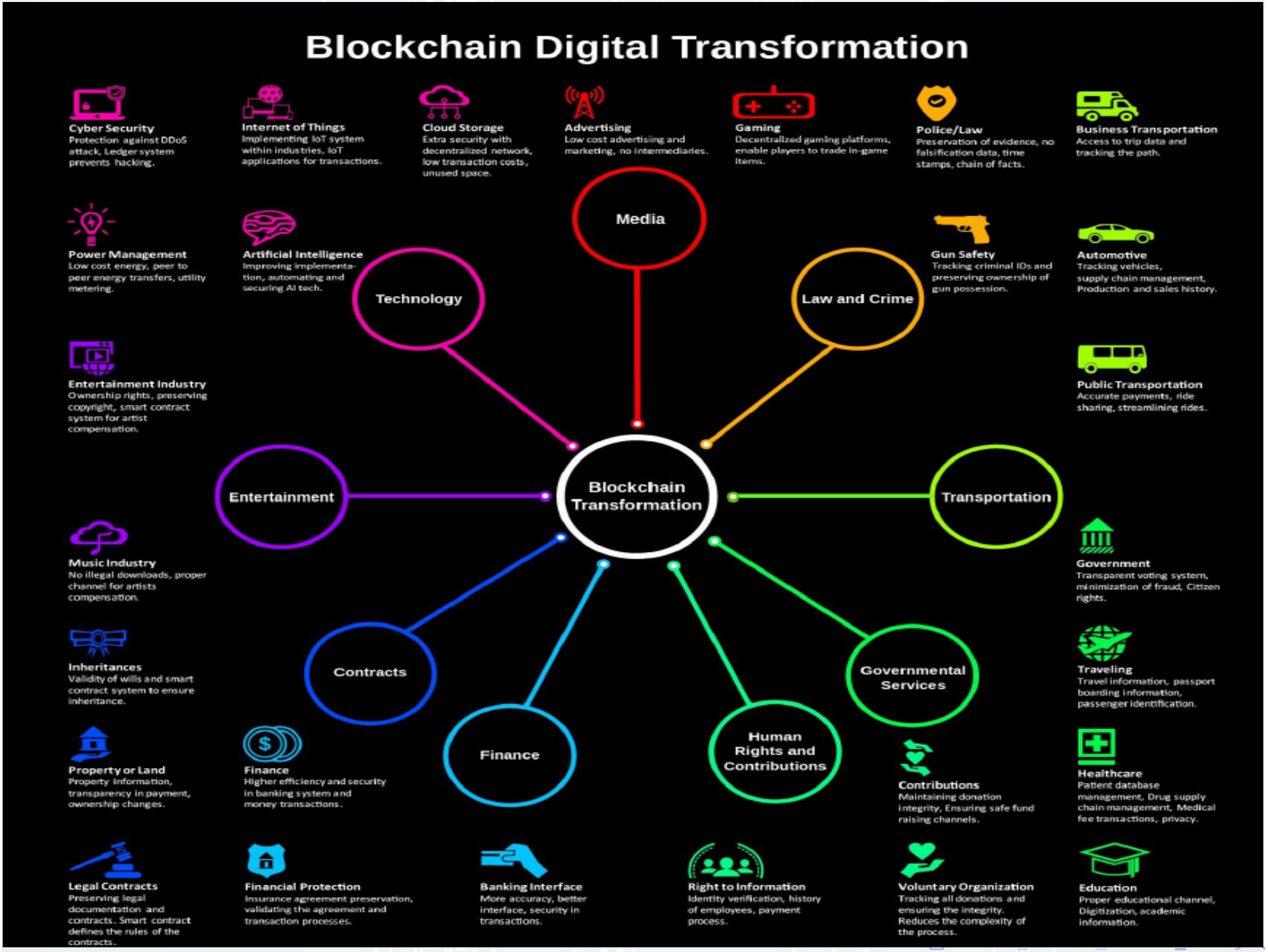
- Blockchain holds complete provenance details of each component part
- Accessible by each manufacturer in the production process, the aircraft owners, maintainers and government regulators

Benefits

- trust increased no authority owns provenance
- improvement in system utilization
- recalls specific rather than cross fleet

9 Verticals of Blockchain Transformation

- Technology
- Media
- Law and Crime
- Transportation
- Governmental Services
- Human Rights
- Finance
- Contracts
- Entertainment

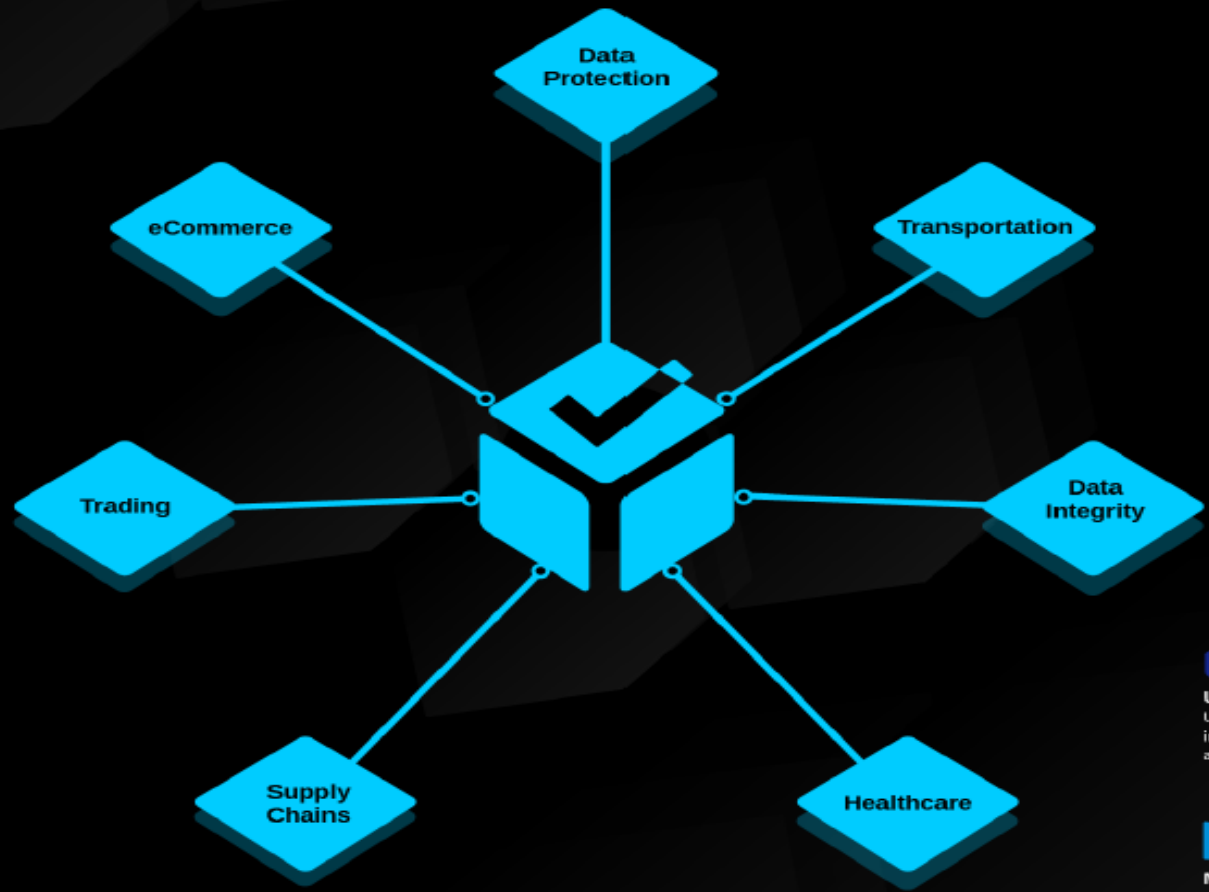

Blockchain Digital Transformation
Cyber Security
Protection against DDoS attack, Ledger system prevents hacking.
Internet of Things
Implementing IoT system within industries, IoT applications for transactions.
Cloud Storage
Extra security with decentralized network, low transaction costs, unused space.
Advertising
Low cost advertising and marketing, no intermediaries.
Gaming
Decentralized gaming platforms, enable players to trade in-game items.
Police/Law
Preservation of evidence, no falsification data, time stamps, chain of facts.
Business Transportation
Access to trip data and tracking the path.
Power Management
Low cost energy, peer to peer energy transfers, utility metering.
Artificial Intelligence
Improving implementation, automating and securing AI tech.
Media
Technology
Law and Crime
Gun Safety
Tracking criminal IDs and preserving ownership of gun possession.
Automotive
Tracking vehicles, supply chain management, Production and sales history.
Entertainment Industry
Ownership rights, preserving copyright, smart contract system for artist compensation.
Public Transportation
Accurate payments, ride sharing, streamlining rides.
Entertainment
Blockchain Transformation
Transportation
Music Industry
No illegal downloads, proper channel for artists compensation.
Government
Transparent voting system, minimization of fraud, Citizen rights.
Inheritances
Validity of wills and smart contract system to ensure inheritance.
Contracts
Governmental Services
Traveling
Travel information, passport boarding information, passenger identification.
Property or Land
Property information, transparency in payment, ownership changes.
Finance
Higher efficiency and security in banking system and money transactions.
Finance
Human Rights and Contributions
Contributions
Maintaining donation integrity, Ensuring safe fund raising channels.
Healthcare
Patient database management, Drug supply chain management, Medical fee transactions, privacy.
Legal Contracts
Preserving legal documentation and contracts. Smart contract defines the rules of the contracts.
Financial Protection
Insurance agreement preservation, validating the agreement and transaction processes.
Banking Interface
More accuracy, better interface, security in transactions.
Right to Information
Identity verification, history of employees, payment process.
Voluntary Organization
Tracking all donations and ensuring the integrity. Reduces the complexity of the process.
Education
Proper educational channel, Digitization, academic information.

2020 Leading Sectors

- Supply Chains
- FinTech
- Retail
- Trading
- Mining
- Healthcare
- Insurance

and more .....

Enterprises Which Are Implementing Blockchain Technology



Apple
Patented blockchain technology for time stamping data.

Facebook
Exploring the use of blockchain to enhance data security and users privacy.

Google
Exploring the use of blockchain technology to enhance cloud service security and for data protection.

Baidu
Using blockchain to enhance intellectual rights management.

Ford
Leveraging blockchain technology to enhance the mobility of technologies.

Tencent
A Solution for verifying invoice authenticity and for ensuring tax compliance.

Toyota
Planning to use blockchain technology to enhance autonomous driving technology.

Alibaba
Using blockchain technology to track luxury goods in its e-commerce platforms.

British Airways
Implementing blockchain to manage flight data as well as verifying travelers identity.

Prudential
Unveils a blockchain powered trading platform for small and medium-sized enterprises.

AIA Group
Launched the first of its kind bancassurance for sharing policy data.

BHP Billiton
Leveraging blockchain technology for supply chains management.

UnitedHealthcare
Using blockchain technology to improve doctors directories to enable accurate insurance claim fillings.

FedEx
Working on blockchain solution for settling customer disputes.

Metlife
Using blockchain technology for storing patients medical records for insurance purposes.

Nestle
Using blockchain technology in supply management to track baby food products.

Maersk
Blockchain system for tracking movement of shipments between ports.

UPS
Blockchain powered logistics monitoring and management solution.

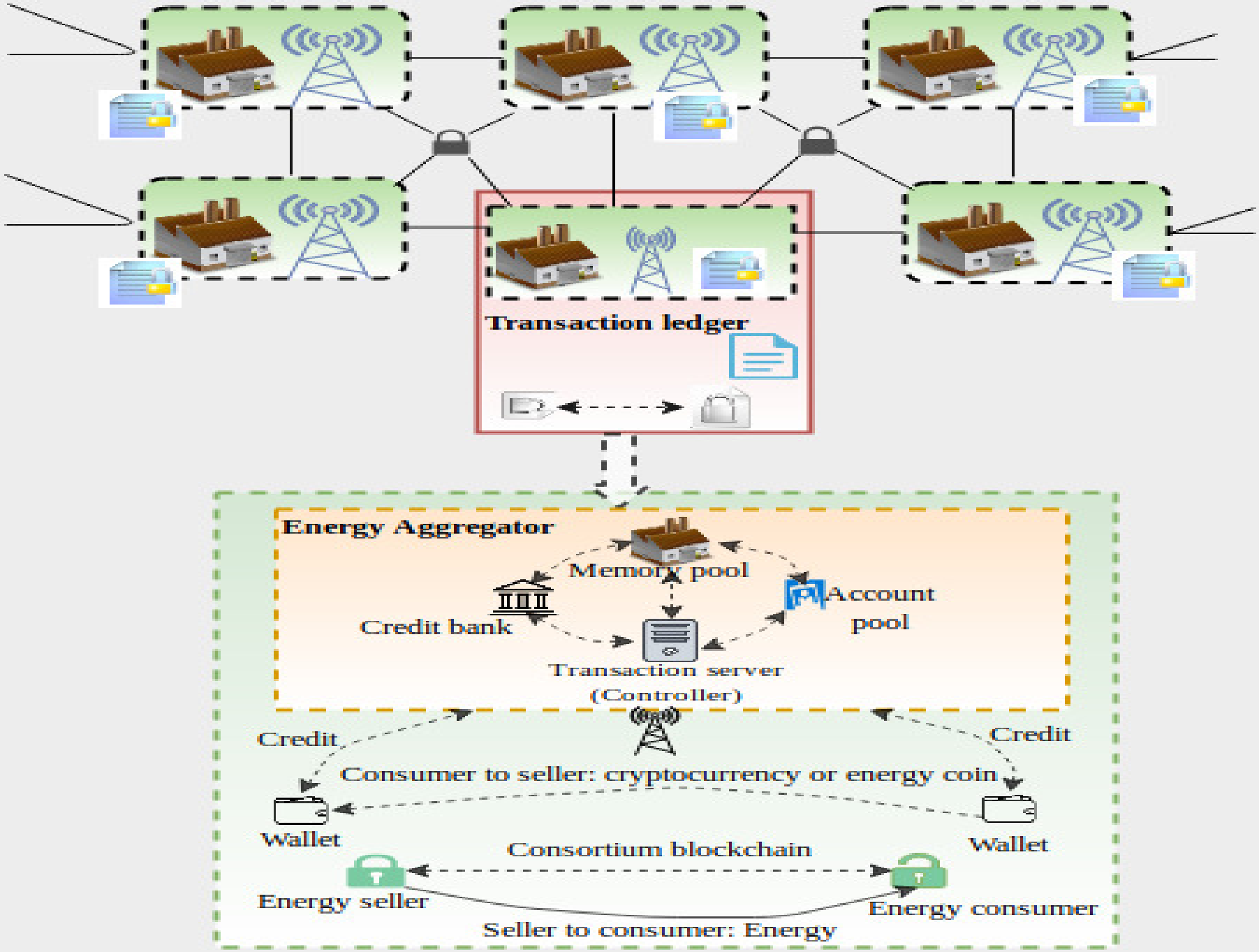
Samsung
Intends to use blockchain technology to enhance supply chain management when it comes to electronics shipments.

Walmart
Using blockchain technology to track product movement from farmers to stores.


LEGAL ENFORCEMENTS
Governments can use Public Blockchain data to monitor transactions to facilitate legal transactions and stop money laundering.
LEGISLATION RECORDS
With decentralized ledger, Governments can keep records of all the legislation reports in a better way.
TAXATION
With decentralized ledger, Governments can foster better transparency in solving tax issues.
BILLS AND PAYMENTS
Governments can impose blockchain technology to improve the traditional billing and payment systems.
BLOCKCHAIN FOR GOVERNMENT
SECURITY & SAFETY
With blockchain technology, Governments can provide better social security against online frauds.
WELFARE DISTRIBUTION
Blockchain technology can be a great way to cut off the system losses which will pave the way for better welfare distribution.
CYBER-PROTECTION
Governments can use Blockchain technology to protect vital Govt. infrastructure against cyber-attacks and hacks.
DIGITIZED IDS
With decentralized ledger, Governments can implement digital IDs for the citizens.
HEALTHCARE SERVICES
Government can improve healthcare services by utilizing distributed ledgers.

P2P Energy Trading

- Step 1. Customer to Network: The customer will announce into network that he wants to purchase energy
- Step 2. Blockchain Network: Miner nodes will check the credibility of customer, request, and requirement
- Step 3. Blockchain Network: Find the seller based on the credit of customer and seller
- Step 4. Blockchain Network: Creating the shared wallet and public-private keys for smart contract
- Step 5. Network to buyer and seller: share the generated key pairs to customer and buyer


Transaction ledger
Energy Aggregator
Memory pool
Credit bank
Account pool
Transaction server
(Controller)
Credit
Credit
Consumer to seller: cryptocurrency or energy coin
Wallet
Wallet
Consortium blockchain
Energy seller
Energy consumer
Seller to consumer: Energy

P2P Energy Trading

- Step 6. Customer to Buyer: Cryptographically exchange of smart contract between buyer and seller
- Step7. Seller to Network: Blockchain Network will verify the credibility of seller and the amount of energy
- Step 8. Seller to Buyer: Cryptographically agreement on smart contract
- Step 9. Seller to Buyer: Energy transfer
- Step 10: Blockchain Network: Update the ledger

P2P Energy Trading

- The Prosumer P_i will announce that he wants to sell the surplus energy to a customer C_i. The address of prosumer is P_a, and customer C_a. The credit information represented by $C_r(i,k)_{k=1}^{K}$.
- DSO will be installed in every legitimate user's smart meter if any transaction gets initiated it will go to every DSO for the verification like blockchain network. We have to give some money to the infrastructure service provider that amount e decided by the government. This amount will be paid by the seller node (like in Blockchain we pay to miners) suppose 2% of the total transaction.

P2P Energy Trading

- $$Pi \rightarrow DSO : Announce = \{Pi||C_r(i,k)_{k=1}^{K}||Address \\ ||Price||EnergyAmount||Timestamp\} \quad (1)$$
- $$Address = \{Randomly\ generated\ hash\ value\} \quad (2)$$
- After the announcement, DSO will verify the amount of energy price and credit information.
- The credit value can be checked by the token which every energy nodes have according to their transaction. This credit information is for checking the authenticity of the prosumer, and in case of customer, it will act as a credit bank and for authentication.
- Now the DSO will find the nearest neighbour customer in the P2P network, and it will allot public-private key P_{bi} and P_{ri}. Customer will get a smart contract digitally signed by the prosumer $DS_{pri}(T_i)$

P2P Energy Trading

- $$P_i \rightarrow DSO : \{(P_{bi}, P_{ri})||T_i|| DS_{p_{ri}}(T_i)||Smart\ contract||Timestamp\} \quad (3)$$

- $$Ti = \{Previous\ Transactions||Timestamp\} \quad (4)$$

- $$Previous\ Transaction_i = \{Hash(energy\ unit\ transaction||Amount\ Transaction||credit\ from\ DSO\ ||illegalTransaction)\} \quad (5)$$

P2P Energy Trading

- The transaction is carried out in terms of energy coin E_c and credit.
- The customer is taking the loan C_l from credit bank and rest he is paying using energy coin.
- DSO will check the information of customer for payment to prosumer.
-

$$C_i \rightarrow DSO = \{T_i||DS_{p_{ri}}(T_i)||C_l||Amount \\ ||Timestamp\} \quad (6)$$

-

$$DSO \rightarrow P_i = \{(Amount - 2\%)||signed\ payment||Bill \\ ||Timestamp\} \quad (7)$$