Security Aspects of Blockchain Technology

Raj Kumar

Security Aspects of Blockchain Technology

- Introduction to Cryptocurrency & Blockchain technology
- Blockchain Challenges
- Improving Business through Blockchain technology

Introduction to Cryptocurrency & Blockchain technology

A cryptocurrency is a digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets - Wikipedia

Cryptocurrencies are classified as a subset of digital currencies and are also classified as a subset of alternative currencies and virtual currencies - Wikipedia

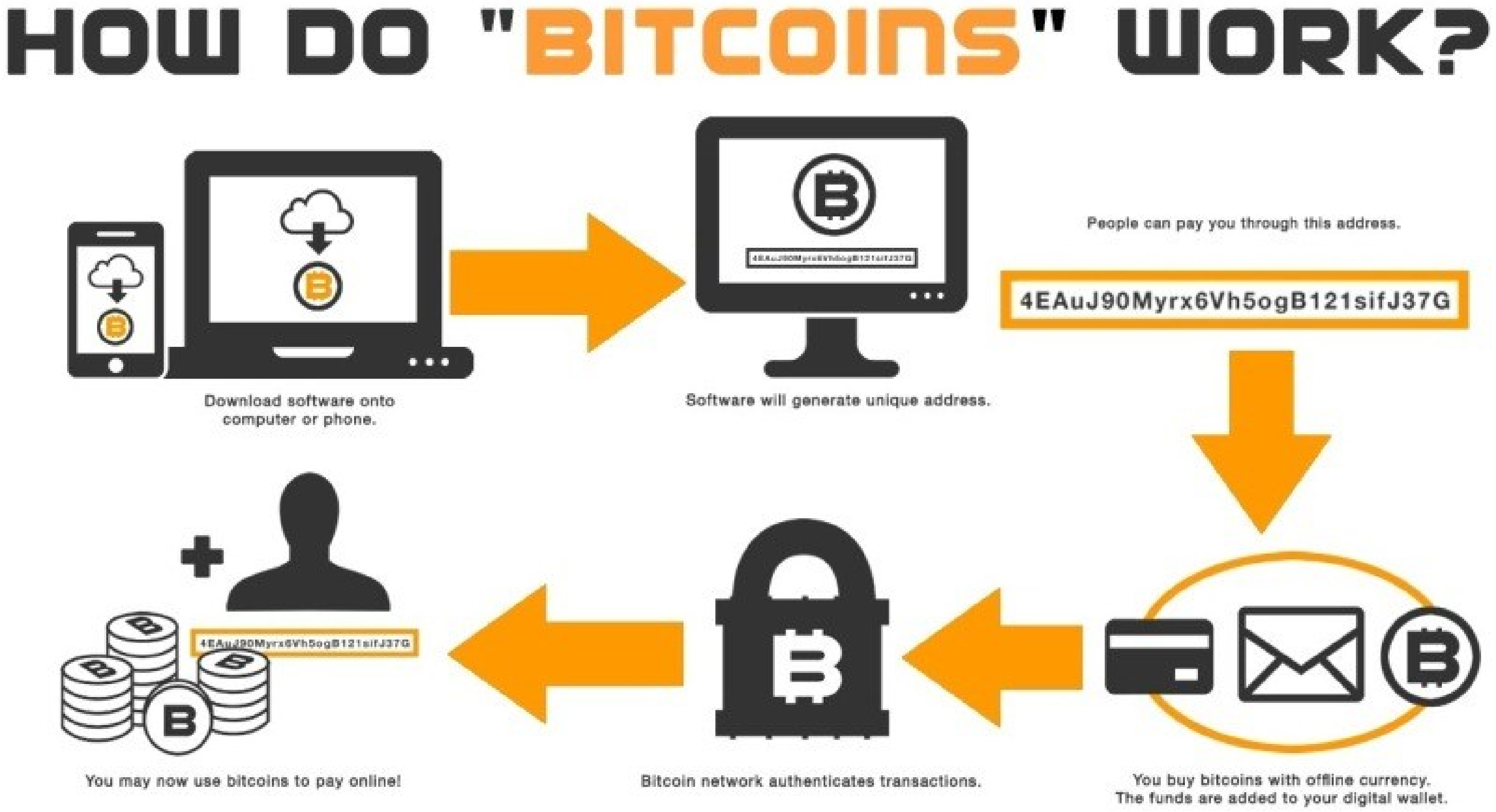
“Virtual currencies, perhaps most notably Bitcoin, have captured the imagination of some, struck fear among others, and confused the heck out of the rest of us.” – Thomas Carper, US-Senator

Introduction to Cryptocurrency & Blockchain technology

- Satoshi Nakamoto invented Bitcoin in 2008 – A cryptocurrency that never meant to be a currency, but rather a Digital Cash
- Implemented the first blockchain
- Deployed the first decentralised digital currency

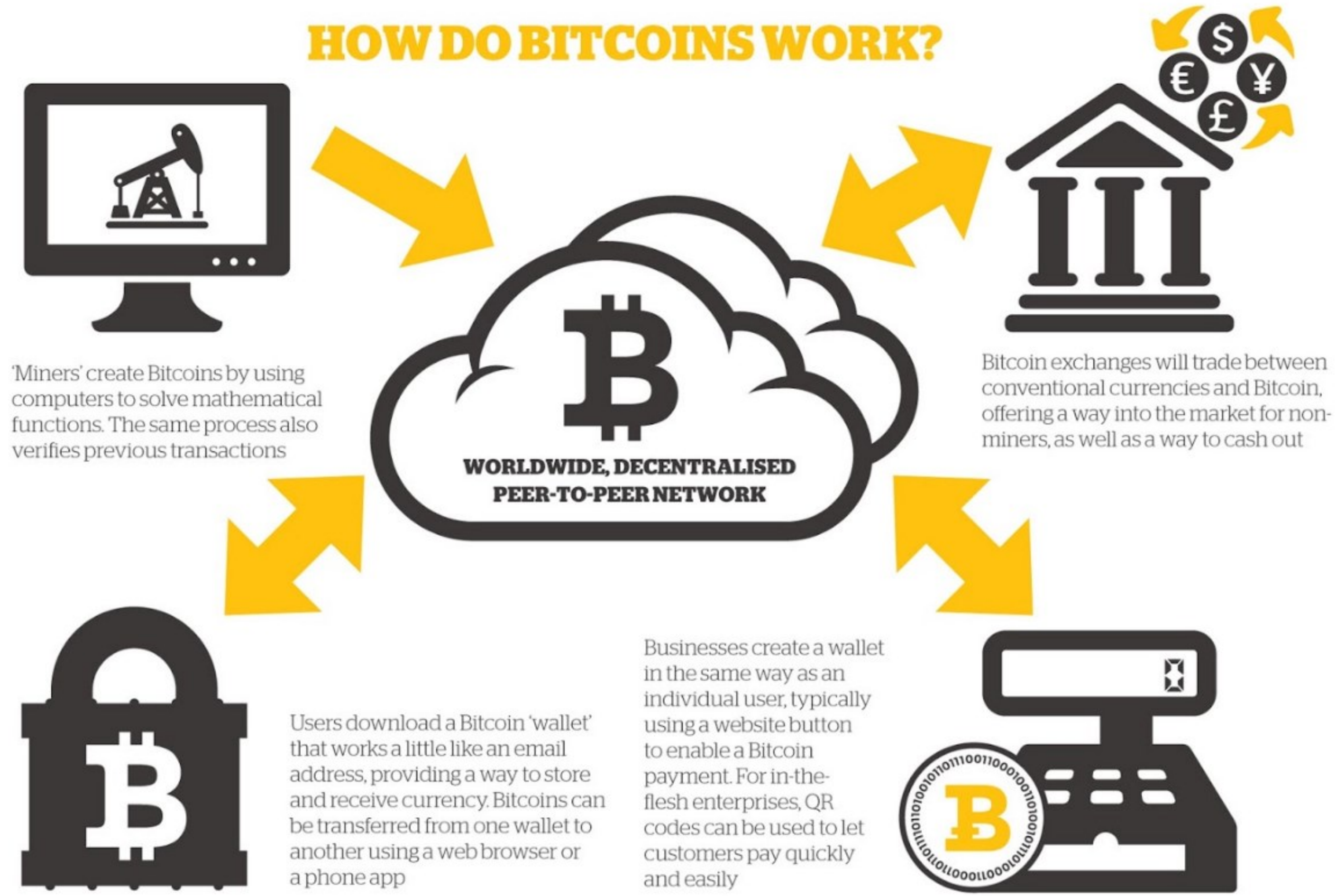
Bitcoin

- A form of digital currency, created and held electronically
- No one controls it
- Not printed in currency noted
- Created by people and businesses using computers around the world that solves mathematical problems


HOW DO "BITCOINS" WORK?
Download software onto computer or phone.
Software will generate unique address.
4EAuJ90Myrx6Vh5ogB121sifJ37G
People can pay you through this address.
4EAuJ90Myrx6Vh5ogB121sifJ37G
You buy bitcoins with offline currency. The funds are added to your digital wallet.
Bitcoin network authenticates transactions.
4EAuJ90Myrx6Vh5ogB121sifJ37G
You may now use bitcoins to pay online!

http://www.ironlotuspt.com/images/content/bitcoin-work-1.jpg

Bitcoin



HOW DO BITCOINS WORK?

'Miners' create Bitcoins by using computers to solve mathematical functions. The same process also verifies previous transactions

WORLDWIDE, DECENTRALISED PEER-TO-PEER NETWORK

Bitcoin exchanges will trade between conventional currencies and Bitcoin, offering a way into the market for non-miners, as well as a way to cash out

Users download a Bitcoin 'wallet' that works a little like an email address, providing a way to store and receive currency. Bitcoins can be transferred from one wallet to another using a web browser or a phone app

Businesses create a wallet in the same way as an individual user, typically using a website button to enable a Bitcoin payment. For in-the-flesh enterprises, QR codes can be used to let customers pay quickly and easily

https://goo.gl/RGuFqo

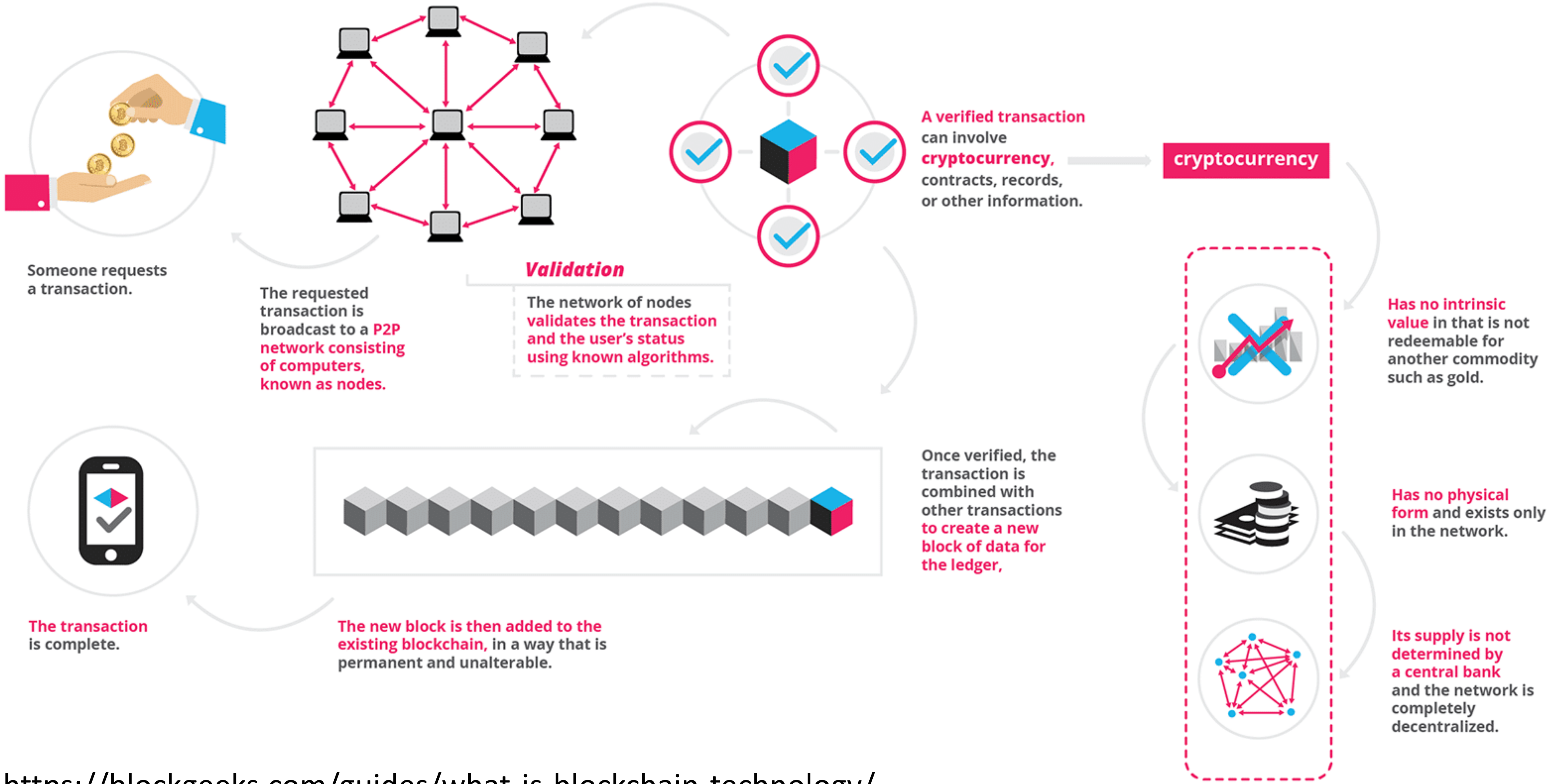
Blockchain

- Block chain is a shared public ledger on which the entire Bitcoin network relies.
- All confirmed transactions are included in the block chain.
- Bitcoin wallets can calculate their spendable balance and new transactions can be verified to be spending bitcoins that are actually owned by the spender.
- The integrity and the chronological order of the block chain are enforced with cryptography.

https://bitcoin.org/en/how-it-works

"The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value."
Don & Alex Tapscott, authors Blockchain Revolution (2016)

Blockchain



Someone requests a transaction.

The requested transaction is broadcast to a P2P network consisting of computers, known as nodes.

Validation

The network of nodes validates the transaction and the user's status using known algorithms.

A verified transaction can involve cryptocurrency, contracts, records, or other information.

cryptocurrency

Has no intrinsic value in that is not redeemable for another commodity such as gold.

Has no physical form and exists only in the network.

Its supply is not determined by a central bank and the network is completely decentralized.

Once verified, the transaction is combined with other transactions to create a new block of data for the ledger,

The new block is then added to the existing blockchain, in a way that is permanent and unalterable.

The transaction is complete.

https://blockgeeks.com/guides/what-is-blockchain-technology/

Blockchain – A distributed database

Picture a spreadsheet that is duplicated thousands of times across a network of computers. Then imagine that this network is designed to regularly update this spreadsheet and you have a basic understanding of the blockchain.

Information held on a blockchain exists as a shared — and continually reconciled — database. This is a way of using the network that has obvious benefits. The blockchain database isn't stored in any single location, meaning the records it keeps are truly public and easily verifiable. No centralized version of this information exists for a hacker to corrupt. Hosted by millions of computers simultaneously, its data is accessible to anyone on the internet.

https://blockgeeks.com/guides/what-is-blockchain-technology/

Blockchain security

- By storing data across its network, the blockchain eliminates the risks that come with data being held centrally.

- Its network lacks centralized points of vulnerability that computer hackers can exploit. Today’s internet has security problems that are familiar to everyone. We all rely on the “username/password” system to protect our identity and assets online. Blockchain security methods use encryption technology.

- The basis for this are the so-called public and private “keys”. A “public key” (a long, randomly-generated string of numbers) is a users’ address on the blockchain. Bitcoins sent across the network gets recorded as belonging to that address. The “private key” is like a password that gives its owner access to their Bitcoin or other digital assets. Store your data on the blockchain and it is incorruptible. This is true, although protecting your digital assets will also require safeguarding of your private key by printing it out, creating what’s referred to as a paper wallet

https://blockgeeks.com/guides/what-is-blockchain-technology/

Blockchain Challenges

Cultural Adoption

- Disruptive technology
- Moving from centralised authority to a distributed
- Impact on business process, organisation structure, governance
- Resistance from users

Integration Concerns & Initial Cost

- Replacement of existing system
- Heavy cost to move from centralised to distributed trusted model

Uncertain Regulatory and Compliance Status

- Biggest concern for Bitcoin
- Need to work with existing regulatory framework
- Breach and Accountability
- Compliance moves from reporting to consensus model

Identity, Security and Privacy

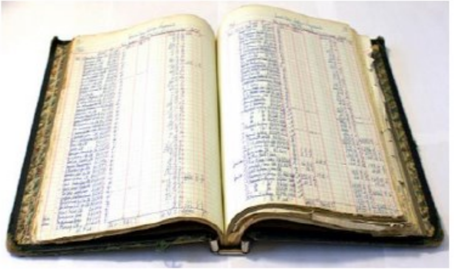
- Anonymity and security varies across application and ecosystem
- Smart contract application may require contracts and transaction linked to known identities
- Cryptocurrency tied to wallet rather than individuals
- Financial industry required PCI-DSS
- Security and privacy must be met with new technology, replacing the old

Standardization

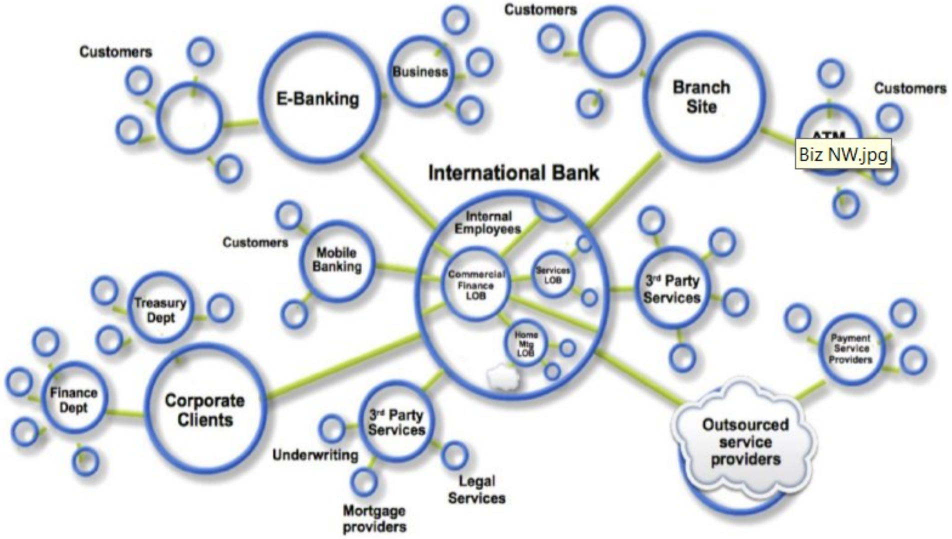
- Lack of definition and standards
- Too many solution
- A common approach required for use case, block data format and structure, security and privacy of datasets, consensus algorithm, governance of smart contracts, regulatory and compliance

Improving Business through Blockchain technology

- Block chain has two main concepts:
  - Business network – users exchange items of value - Asset
  - Ledger – each user possesses and the content is always in syn

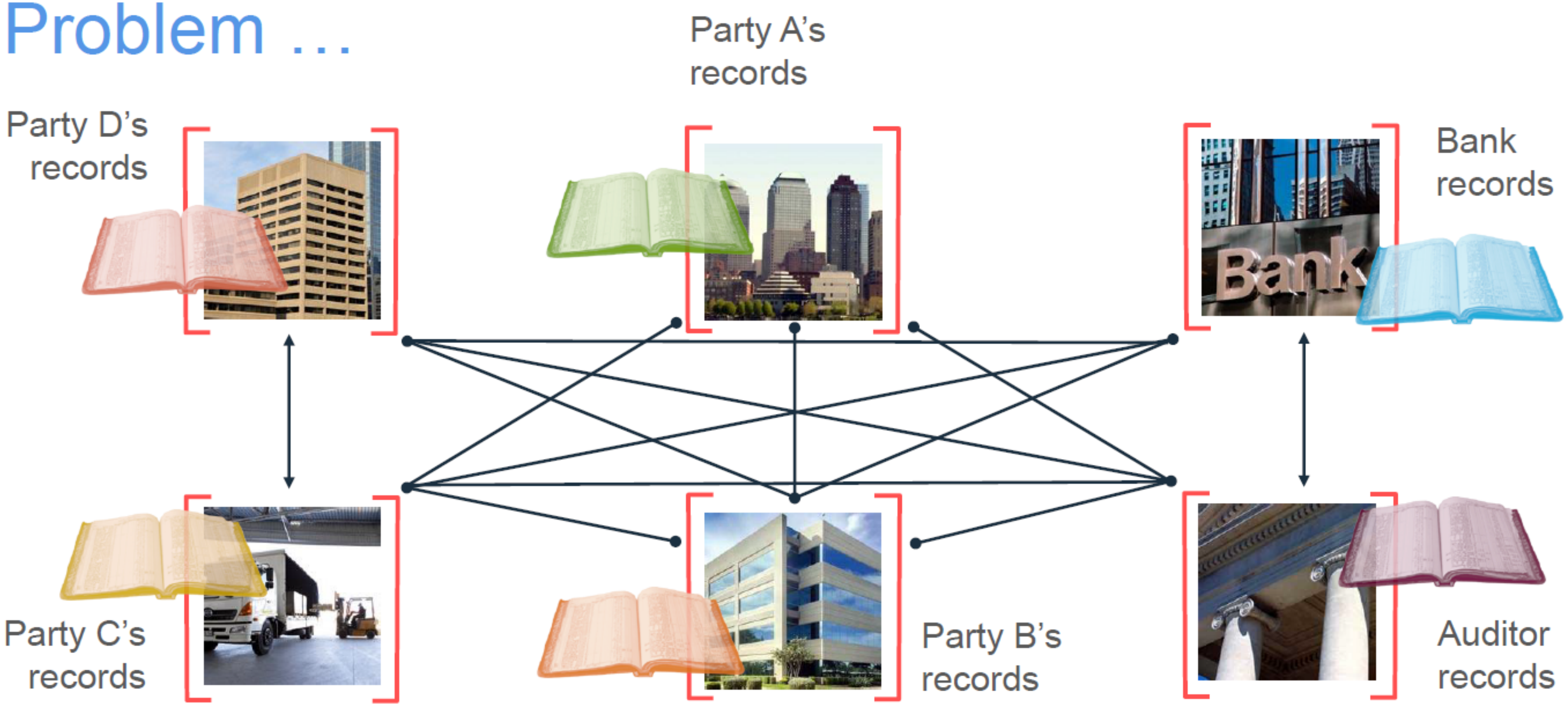


- Benefits:
  - Enhanced connectivity with partners, customers, suppliers, banks
  - Wealth generated from flow of goods and service across network
  - Markets central to the process – Private and Public
  - Ledger will be the system of record for the business - Transactions (asset transfer) and Contracts (conditions for transaction to occur)



Improving Business through Blockchain technology :

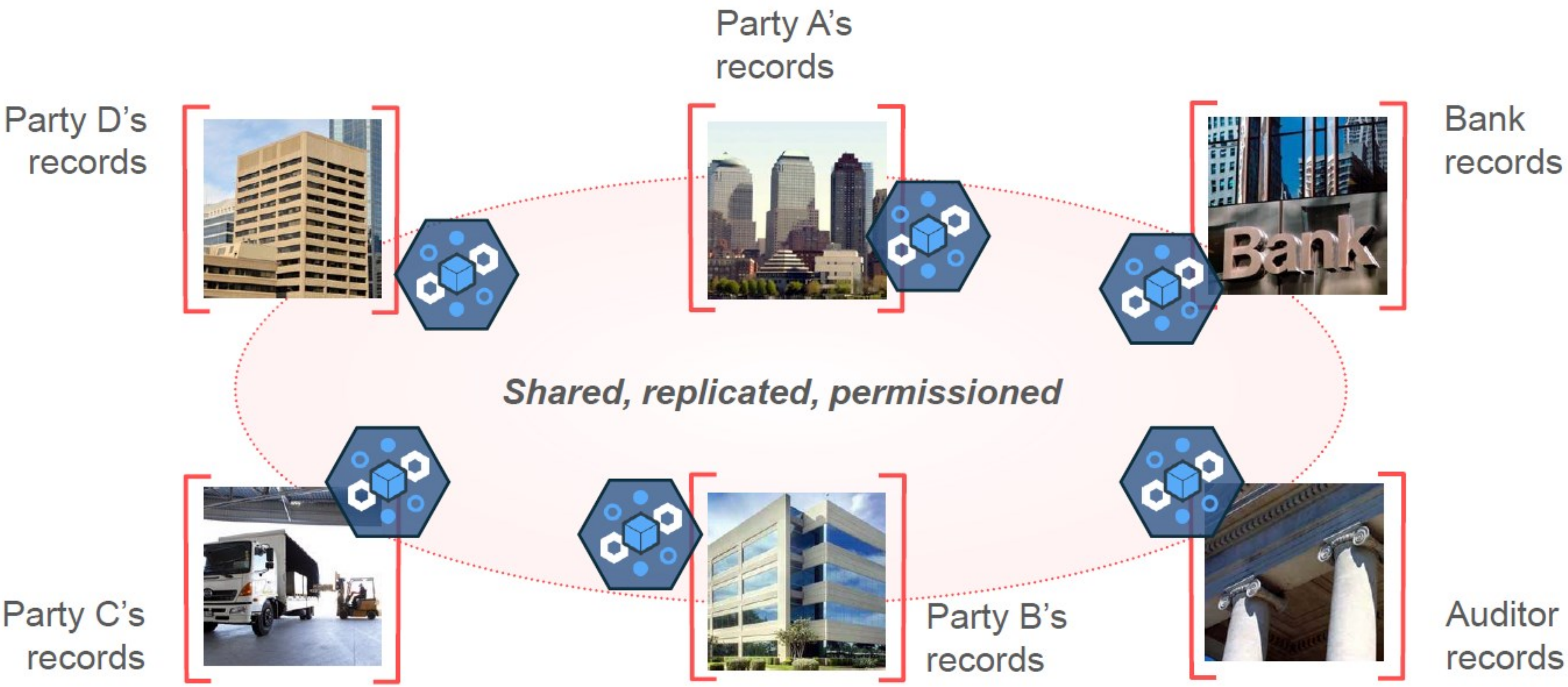
Problem …



… Inefficient, expensive, vulnerable

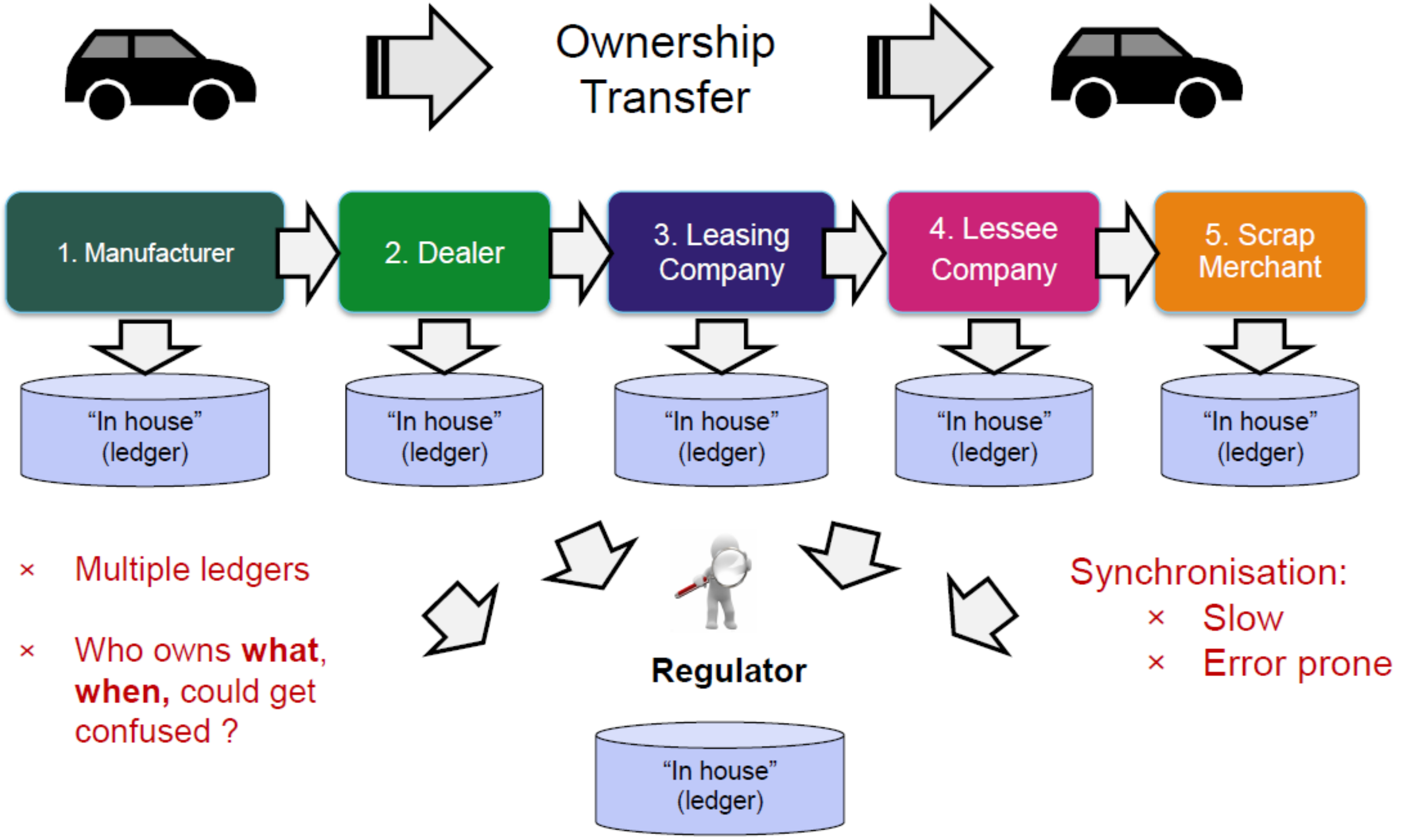
Improving Business through Blockchain technology

Solution …



2016 IBM corp.

Car Leasing Business Network

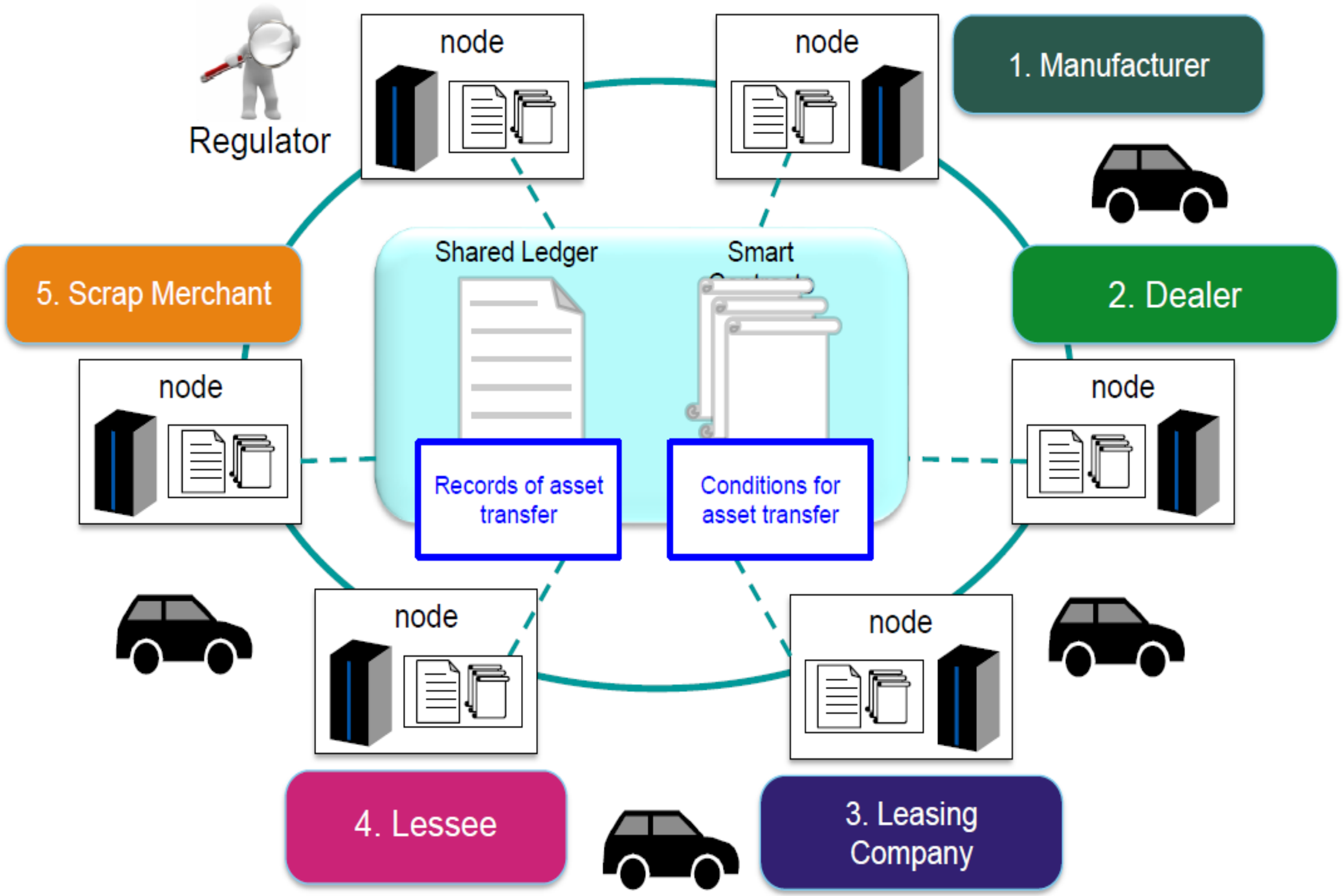


- × Multiple ledgers
- × Who owns **what**, **when,** could get confused ?

Synchronisation:

- × Slow
- × Error prone

Car Leasing Business with Blockchain



ITU : I Thank U