Blockchain for Smart Grid

12.03.2026

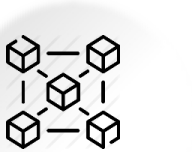


Frank Eliassen

professor emeritus, University of Oslo, Norway

Learning Objectives

Throughout this lecture, it is aimed for the students to be able to:



Blockchain

Understand the Blockchain concept and main features



Blockchain for smart energy systems

Understand the applications of Blockchain for smart energy systems, electric vehicles and charging stations sharing

Industry Invited Talk Today



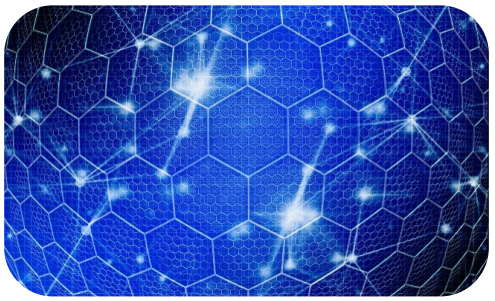
Rune Bøen, Chief Data Officer,
Becour

Blockchain for Smart Energy Systems: an Industry Perspective

BECOUR

Becour enables energy users to choose renewable energy and makes sure that this choice results in the production of even more renewable energy.. Becour strives towards a transparent market for renewable energy. Becour operates with open books and 100% transparent pricing.

Outline



Blockchain

Concept

Tamper-proof

51% attack



Blockchain for Smart Energy

Distributed energy

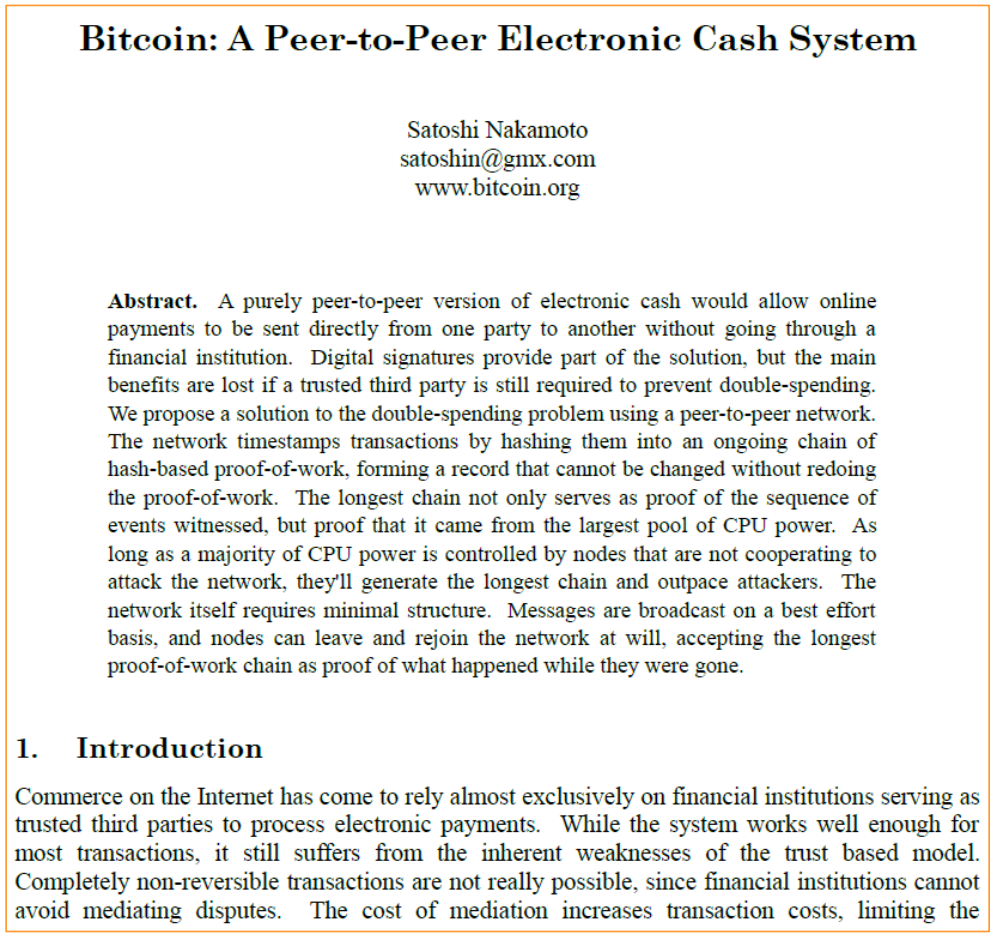
Applications

Examples

01

BLOCKCHAIN CONCEPTS

Blockchain development



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the

- In 2008, Satoshi Nakamoto proposed Bitcoin for the first time in the paper “Bitcoin: a peer-to-peer electronic cash systems”
- At time 02:15:05, 4 January 2009, Satoshi created the first block in the Bitcoin system and left the message:
  - The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

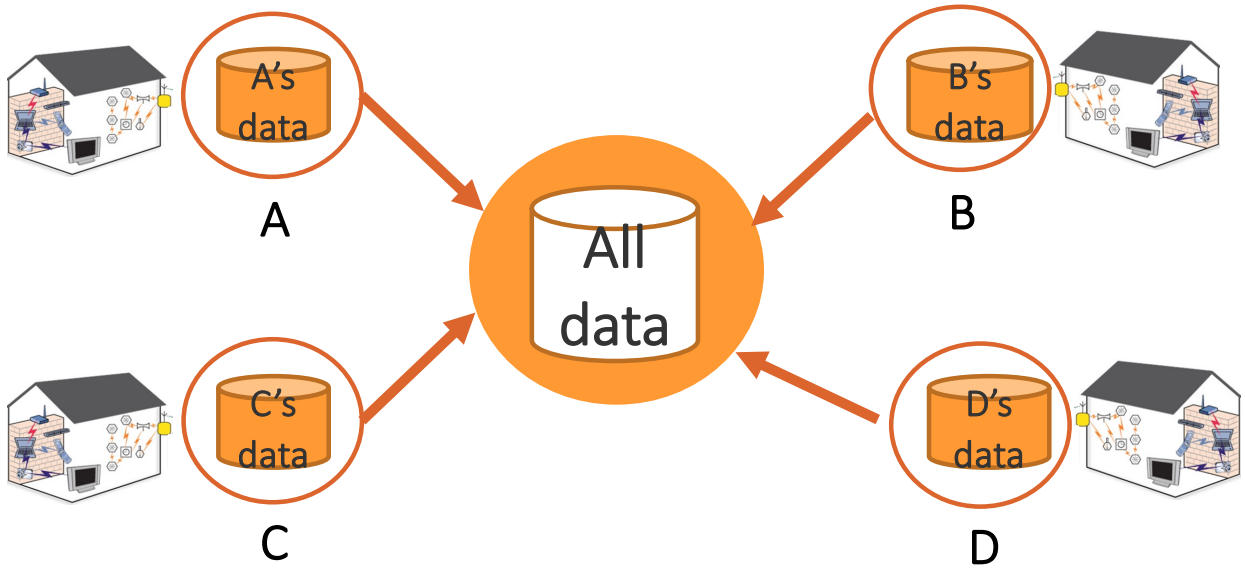
Two concepts: Blockchain and Bitcoin

Bitcoin ≠ **Blockchain**



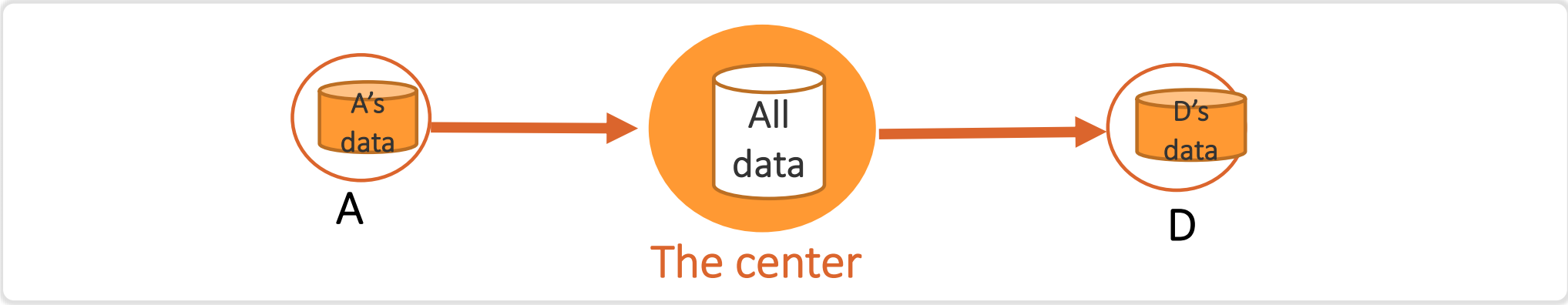
- Bitcoin: unregulated digital currency designed to bypass currency controls and simplify online transactions by getting rid of third-party payment processing intermediaries.
- Blockchain and Bitcoin relationship: Bitcoin was an application of Blockchain. Blockchain has applications far beyond Bitcoin.

Traditional central trusted authority



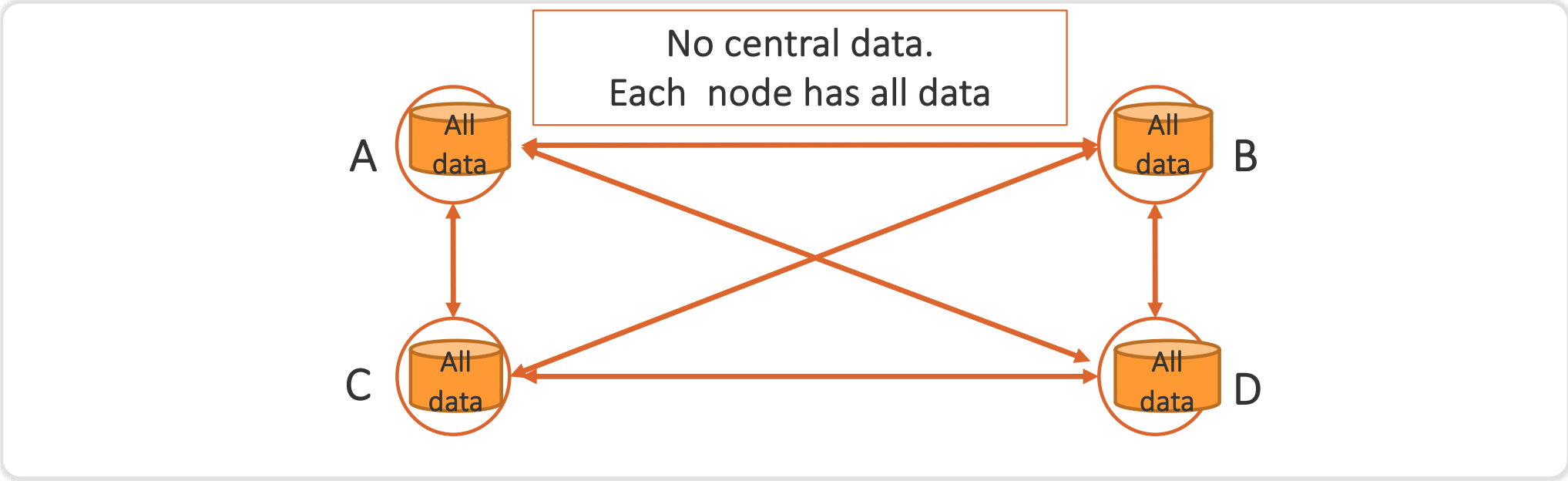
- Individual person: own her data
- Central trusted node: own all users' data, e.g., Visa, Mastercard, PayPal, banks, and Amazon. The center has full control of all data, it can search, add, delete and modify data.

Traditional central trusted authority



- A has data exchange with D (e.g., bank transaction)
  - A sends a request to the center
  - The center answers the request and connects D
  - Data processing
- Q: any disadvantages of such architecture?
- Very high workload in the center since all transactions go through the central node; the central node could become malicious; the single failure point of the central node by cyber attacks.

Blockchain concept

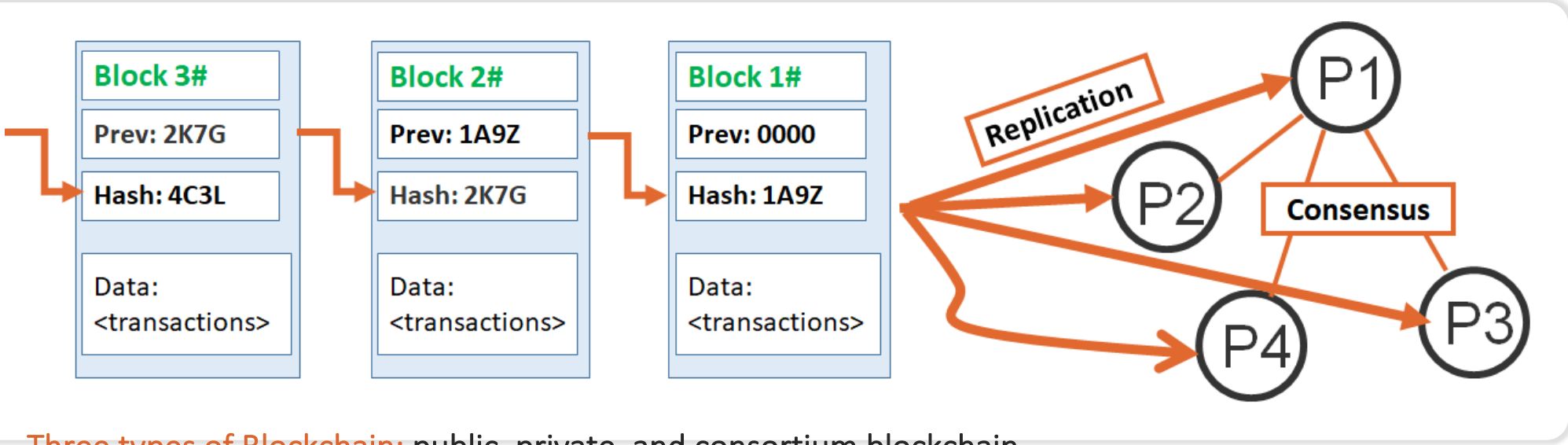


- Blockchain: a globally maintained and shared distributed database. Every node has identical copies of the database and there is no central organization to manage the database. There are no central nodes and all nodes are equal.
- Blockchain records the transactions permanently. Data can only be added (appended) and searched; the data cannot be deleted or modified.

Blockchain principle

Data are replicated at every node

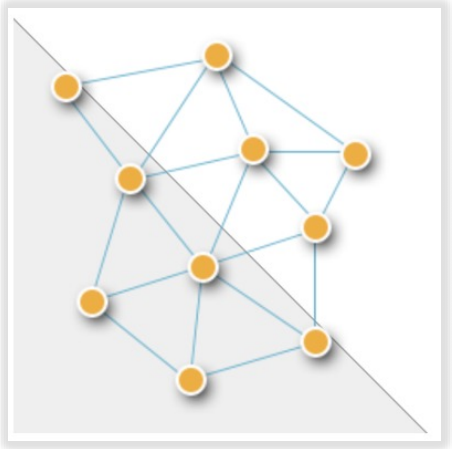
Peer-to-Peer network



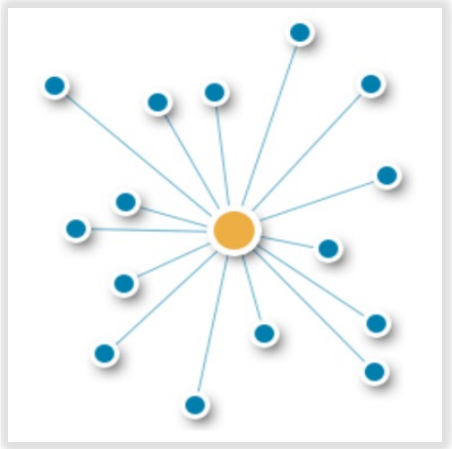
- Three types of Blockchain: public, private, and consortium blockchain
- Features: decentralization, and pseudonymity
- Consensus: All, or a majority of the nodes agree on content of next block.

Blockchain types

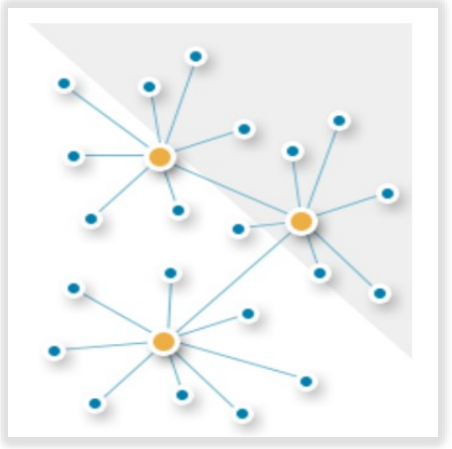
Public



Private

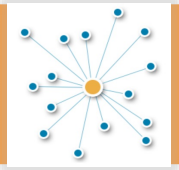
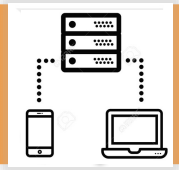


Consortium



	Public	Private	Consortium
Administration	No administrator	Single	Multiple
Permission	Permissionless	Permissioned	Permissioned
Computation cost	High	Low	Medium

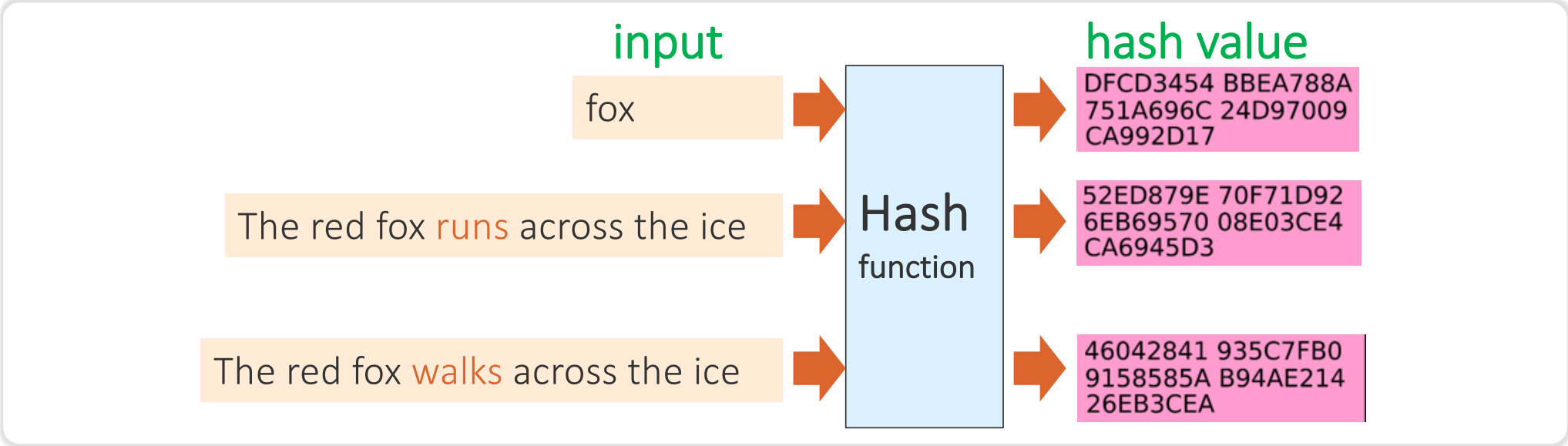
Difference between private blockchain and database

	Private Blockchain 	Database 
Architecture	**Peer-to-peer model**: directly communicate with other users on the network, e.g., doctor-to-doctor information exchange. The administrator is not involved in communications	Client-server model
Authority	**Partially decentralized**: a single authority manages the system and public access to the blockchain is restricted	Centralized
Data processing	**Read and write for the single authority**: once data is saved into the ledger, no one can change it, which is called immutability	Read, write, update, delete
Cryptography	**Yes**: transactions are encrypted, and no one can tamper with them	Usually not: databases have a huge number of entries, and the algorithms that will query the database would have to decrypt every entry to fetch the answer, which is highly time-consuming
Examples	Business-to-business virtual currency exchange network Ripple, Hyperledger	SQL Server, Oracle, Apache

Which type of Blockchain are used in the applications?

Applications	Public, Private or Consortium Blockchain
Bitcoin 	Public
Bank 	Private
Hospital 	Private
Group of hospitals  SØRLANDET SYKEHUS RIKSHOSPITALET	Consortium

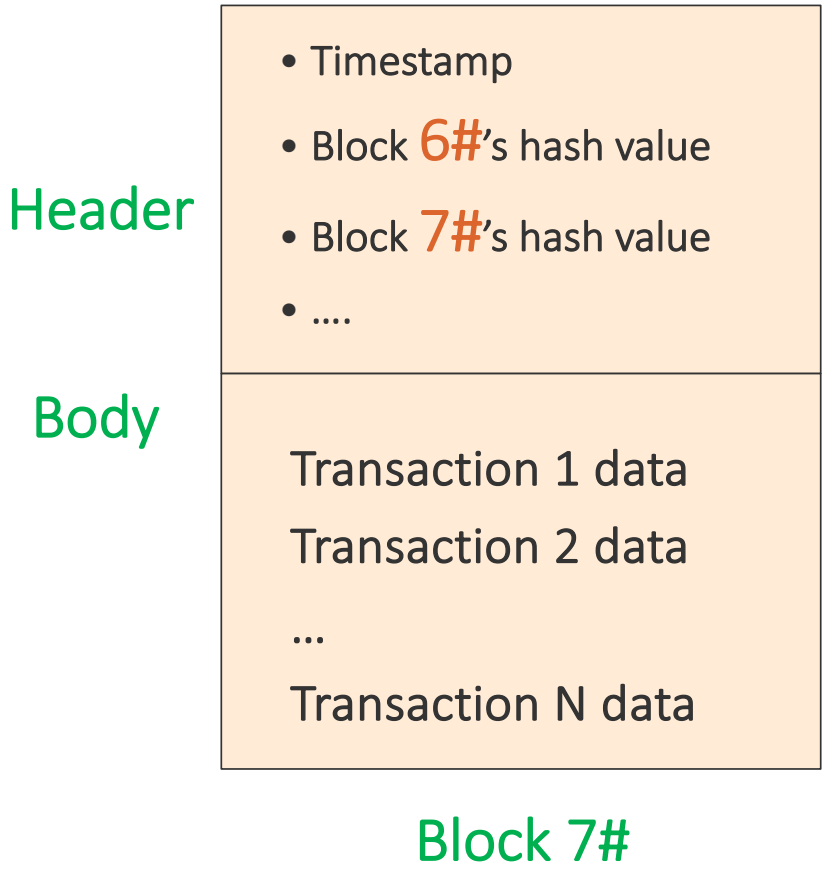
Concept: hash function and hash value



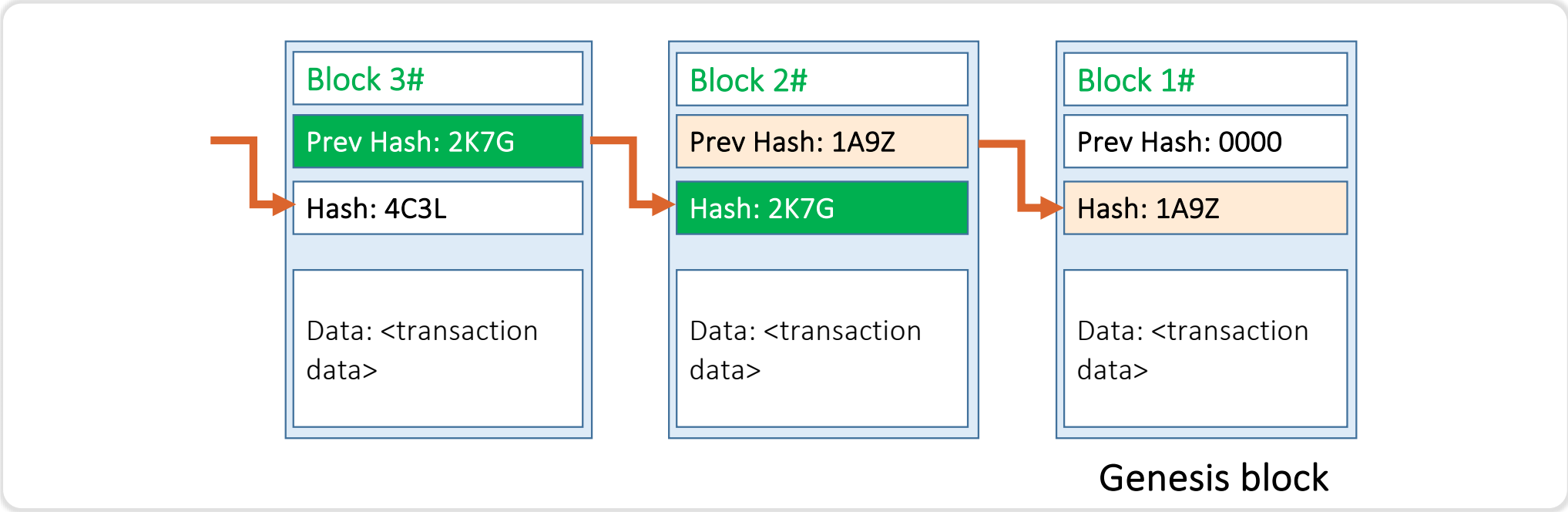
- Hash function: takes any size input text and returns a fixed length string (i.e., hash value).
  - Easy to calculate a hash for any given data
  - Hard to calculate the original text that has a given hash
  - Two slightly different messages produce drastically different hash value
- Bitcoin uses a standard SHA-256 hash algorithm which generates a 256 bit hash value. For example: SHA256(123) = a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3

Blockchain data structure (I)

- Block: a blockchain is composed of blocks. A block contains a group of transactions at a specific time and a hash pointer to the previous block. Each block includes: header and body (i.e., data).
- Each block contains its own hash and also hash of the previous block. For instance, block 7 contains the hash of block 6, and block 6 contains the hash of block 5.
- A simple blockchain in Python: https://github.com/EricAlcaide/pysimplechain

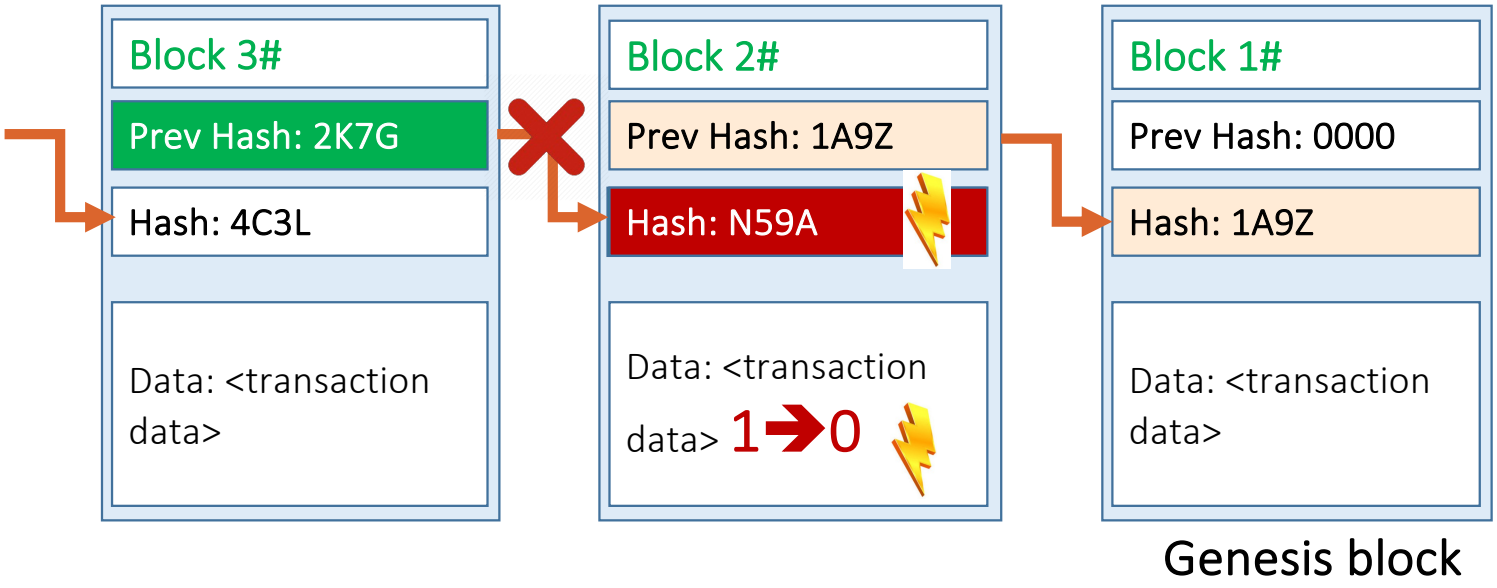


Blockchain data structure (II)



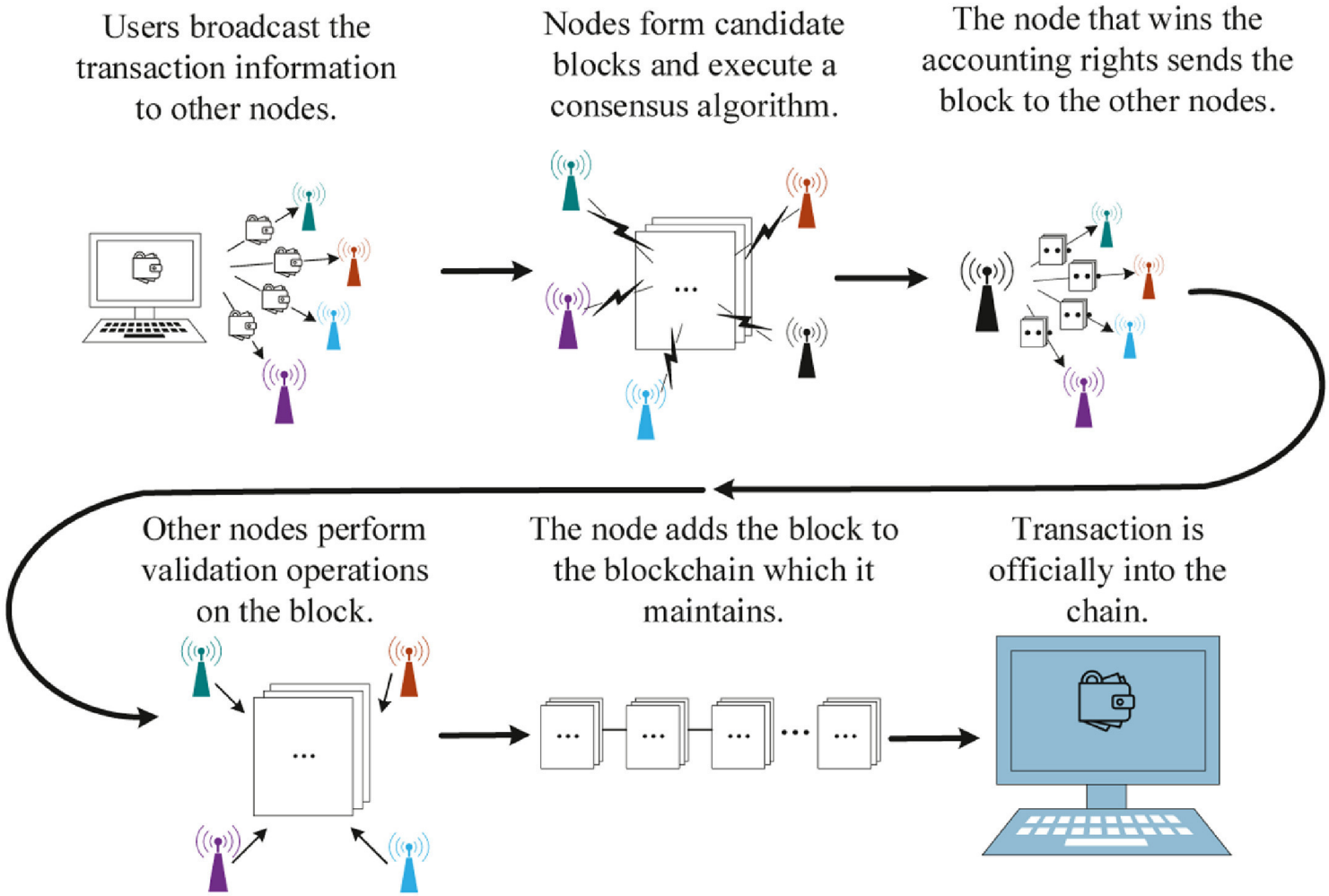
- Blockchain data structure: a linked list with hash pointers used to record all transactions. New blocks are added to the end of the chain.
- Hash pointer: gives you a way to retrieve data along with the hash of the data. A regular pointer only gives you a way to retrieve data.

Tamper-proof mechanism



- Tamper-proof: an adversary is not able to tamper data in any block without getting detected.
- If anyone changes the data in Block 2, even just one bit from 1 to 0, the hash value of this block changes dramatically. Then, Block 3#'s "Prev Hash" is not same as Block 2#'s hash value, this makes the whole chain invalid.

Workflow of a blockchain



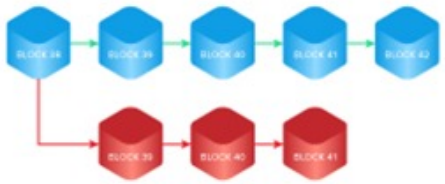
Consensus algorithm:
Several. One well-known is **Proof-of-Work (PoW).**
Based on solving a hash-puzzle: find nonce such that Hash(block,nonce) < 0000000XXXX …
(a hash-value with a certain number of leading zeros)

Winner: the first node (aka miner) that solves the puzzle

source: Y. Chen et al, A survey of blockchain systems: Attacks, defenses and privacy preservation, High-Confidence Computing, 2(2), Elsevier, June 2022, https://doi.org/10.1016/j.hcc.2021.100048

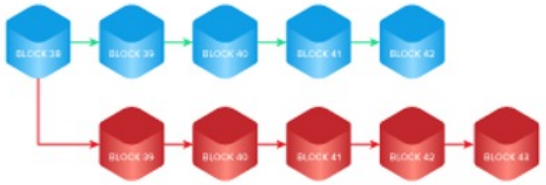
51% attack in Blockchain

- Definition: malicious attackers control a majority (51%) of the total network's computation power (i.e., mining hash rate) and collude to attack bitcoin or other crypto.

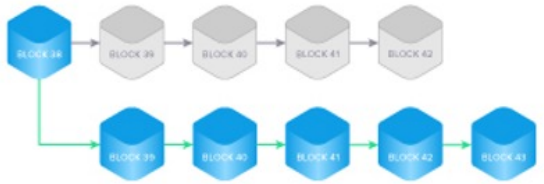


A node adds a block by broadcasting it to the public chain after "winning" a crypto puzzle (i.e, the mining)

Malicious attackers add blocks to the private blockchain without broadcasting, producing a branch



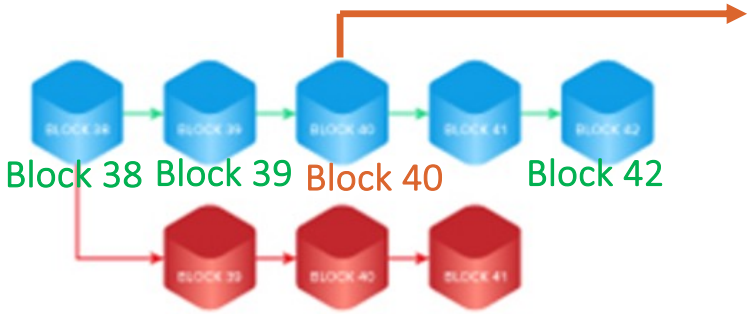
Attackers mine blocks faster with majority computation power.
Rule in Blockchain: the longest chain wins



The old public chain is abandoned because it is shorter, and its data is deemed irrelevant. The attackers roll-back many blocks and start a new blockchain.

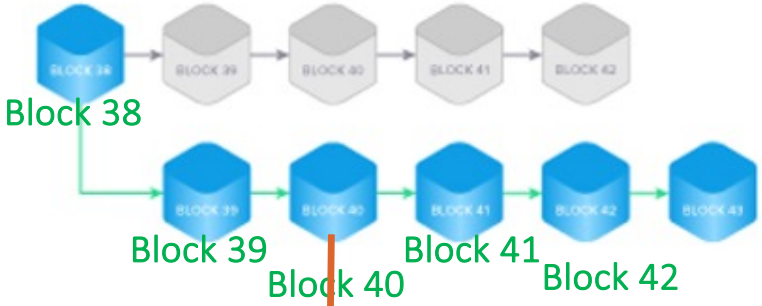
51% attack in Blockchain - consequence

- Consequence: spend coins twice (i.e., double-spending). The attacker can spend the same coins twice and buy two different cars.



Block 40 transaction data: attacker used coins to buy a car and this transaction is stored in Block 40.





With 51% attack, the attacker starts a new Blockchain and the transaction data in the old chain is abandoned. There is no record of using the coins. The attacker can then spend the coins again to buy another car.

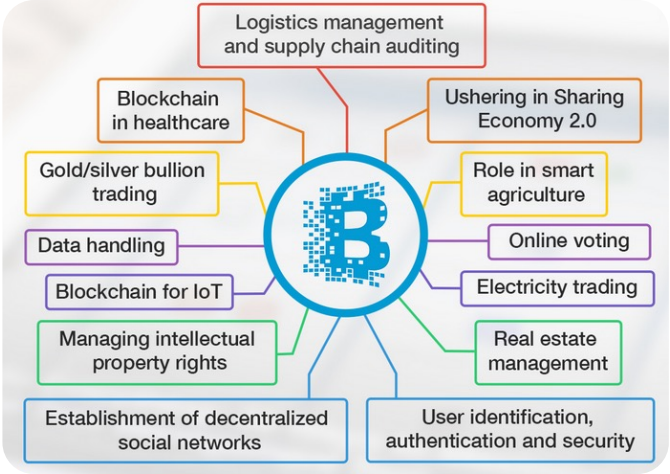


Blockchain applications in general

- Blockchain: decentralized append-only database that keeps a record of all transactions.
- This provides a perfect way for systems to record transactions that should be permanently recorded (immutable).



Sweden officially uses Blockchain to register land and properties





Second-hand car value certification

Properties of Blockchain



Smart Contracts
Auto execution of digital contracts

Distributed
All participants have a copy of the ledger (chain) for complete transparency

Secured
All records are individually encrypted

Immutable
All validated records are irreversable and cannot be changed

Trusted
Data is decentralized and managed by multiple participants

Consensus
All network participants agree to the validity of each record

Time-stamped
A transaction time-stamp is recorded on each block

Properties of Blockchain

Smart contracts are user-defined executable programs that determines the rules of writing and make changes in the ledger, and can be triggered automatically on certain conditions.



Distributed

All participants have a copy of the ledger (chain) for complete transparency

Secured

All records are individually encrypted

Immutable

All validated records are irreversable and cannot be changed

Trusted

Data is decentralized and managed by multiple participants

Consensus

All network participants agree to the validity of each record

Time-stamped

A transaction time-stamp is recorded on each block

Properties of Blockchain



Smart Contracts
Auto execution of digital contracts

Distributed
All participants have a copy of the ledger (chain) for complete transparency

Secured? Not the case for public blockchains which supports pseudonymity only

Immutable
All validated records are irreversable and cannot be changed

Trusted
Data is decentralized and managed by multiple participants

Consensus
All network participants agree to the validity of each record

Time-stamped
A transaction time-stamp is recorded on each block

Discussion

Q: which type of blockchain will be popular in practice: public, private or consortium blockchain?

02

BLOCKCHAIN FOR SMART GRID

The Energy Sector has great interest in Blockchain

BLOCKCHAIN NEWS AUGUST 12, 2016 15:38

Perth Startup Set to Begin Trials of P2P Energy Trading on the Blockchain



Nov 29, 2016 | Jamie Redman | 6669

Siemens Partners With LO3 Building Blockchain Microgrids

USA

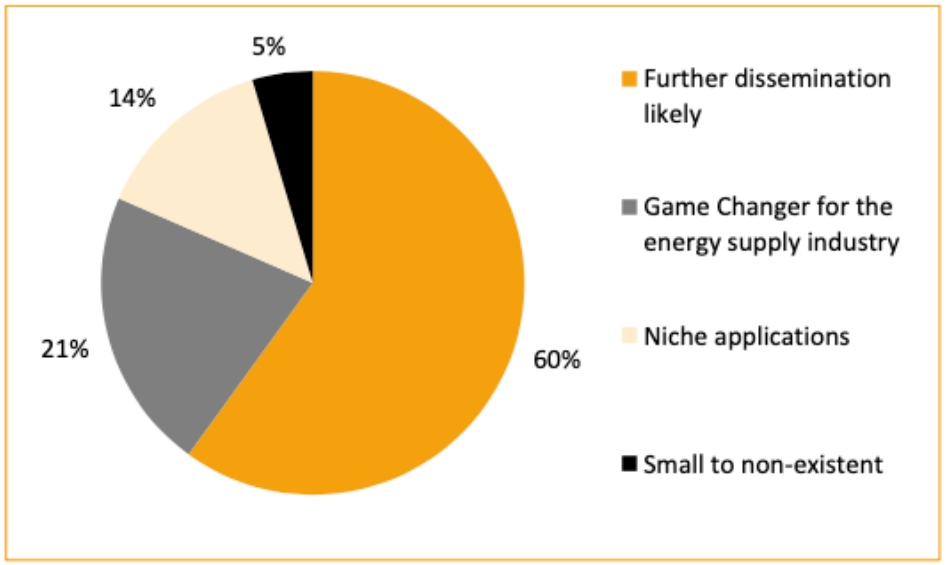
The largest engineering corporation in [illegible] AG has recently announced a energy collaration with fintech startup LO3 Energy to create blockchain microgrids. The blockchain protocol aims to enable energy trades facilitated by a distributed ledger platform.

ACCEPTS BITCOIN NOVEMBER 18, 2016 13:18

A Majority of the German Energy Industry is Interested in Blockchain Tech



Survey among German energy executives*



Potential of dissemination of Blockchain in the energy industry



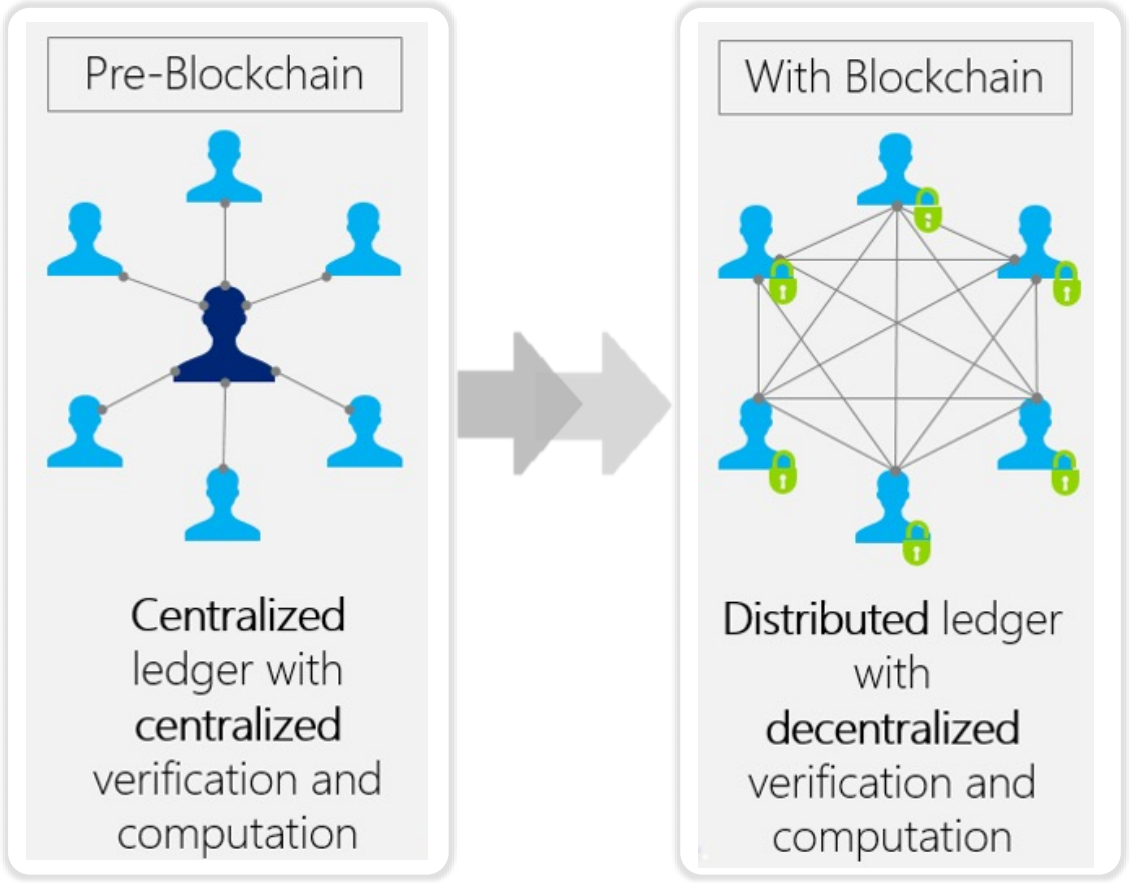
Potential use cases and applications of Blockchain in the energy industry

Color scheme:
- darker color means more potential) and v.v.

Size of circle:
number of individual responses

* Blockchain in the energy transition: A survey among decision-makers in the German energy industry, DENA, 2016

Blockchain in principle: centralized ➔ distributed operation



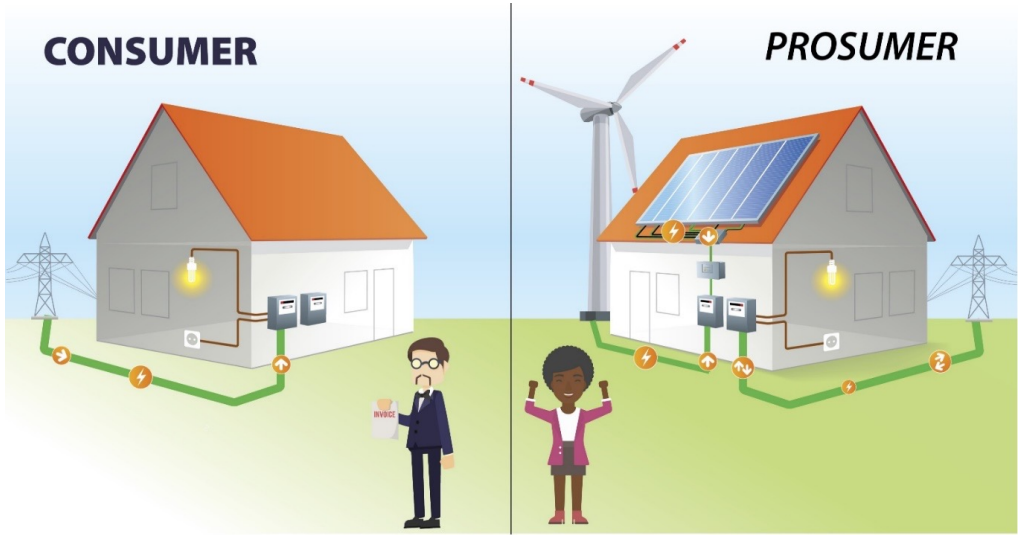
Three conditions to use Blockchain

- **distributed** environment
- nodes **do not trust** each other
- nodes perform **transactions**

Role of Blockchain

- **build trust** among nodes by providing an irreversible and transparent record of mutually validated transactions: then the nodes can safely perform transactions

An emerging concept: *Prosumer = Producer + Consumer*

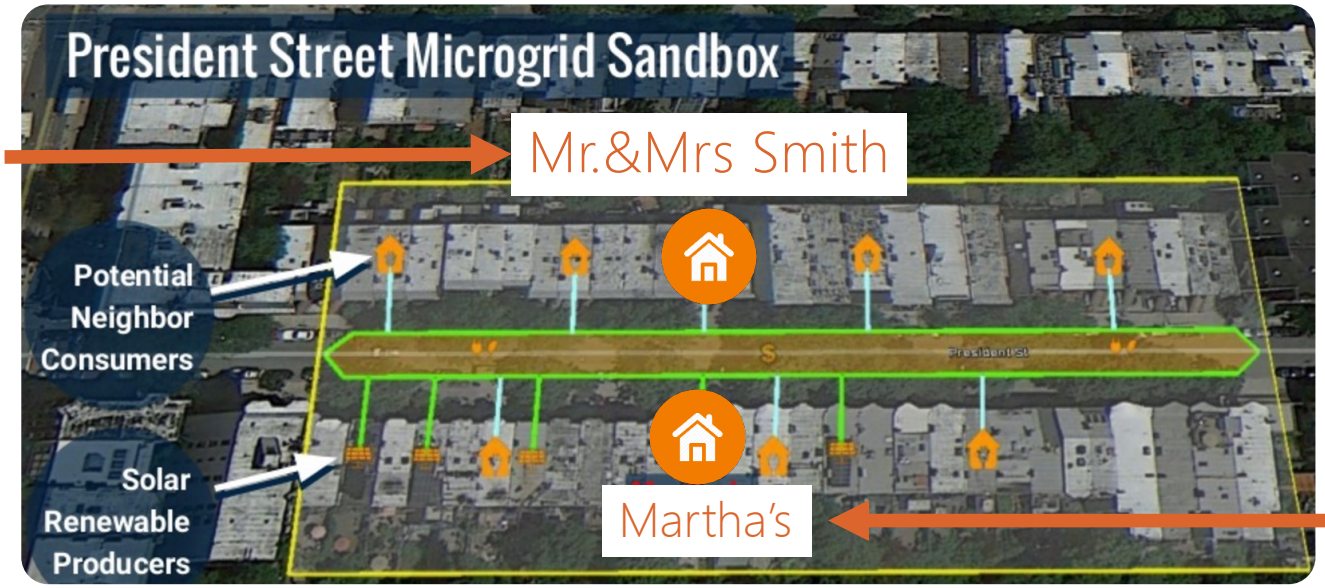


Picture source: US Department of Energy

- Consumer: a house only uses electricity from power grid
- Prosumer: recently, we have renewable energy in our home, consumers are not just customer anymore. A prosumer refers to a house that can both produce and consume energy

Example 1: Selling your power to neighbors (1/2)





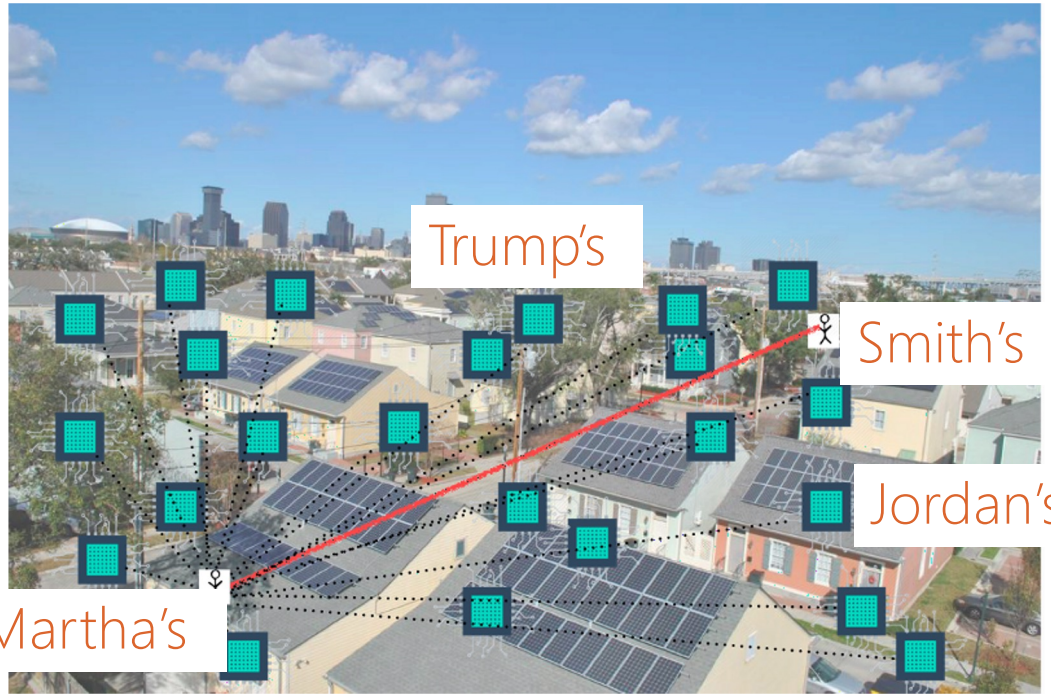


- Brooklyn Microgrid(*): In your house roof, you have solar power. The power can be used by yourself. If you are not able to use all power, you can sell to your neighbors, e.g., Mr.&Mrs Smith and their 6 kids.

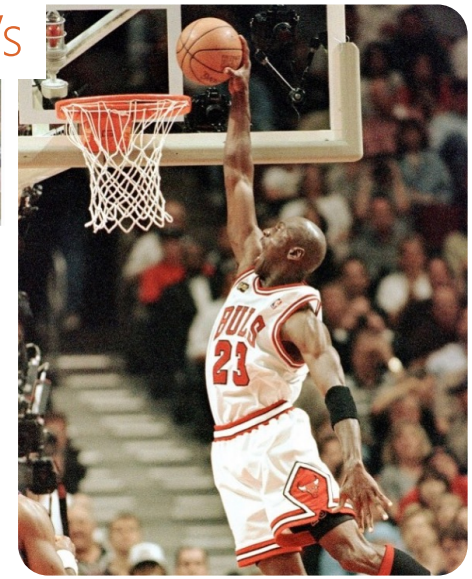
(*) Mengelkamp et al, Designing microgrid energy markets. A case study: The Brooklyn Microgrid, Applied Energy 210 (2018) 870 – 880. http://dx.doi.org/10.1016/j.apenergy.2017.06.054

Example 1: Selling your power to neighbors (2/2)









- Energy Peer-to-Peer (P2P) Sharing Networks: Each house can buy/sell energy from her/his neighborhood. Houses do not trust each other.
- Very similar to P2P networks in Internet that share information/data/movies

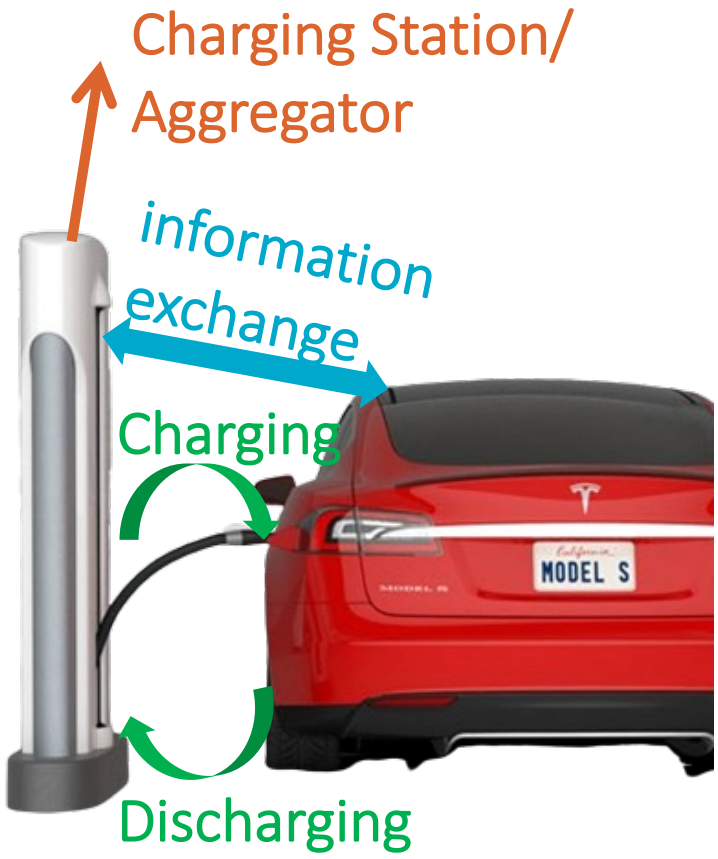
Example 2: Energy P2P Sharing among Electric Vehicles (1/2)

Charging station/aggregator

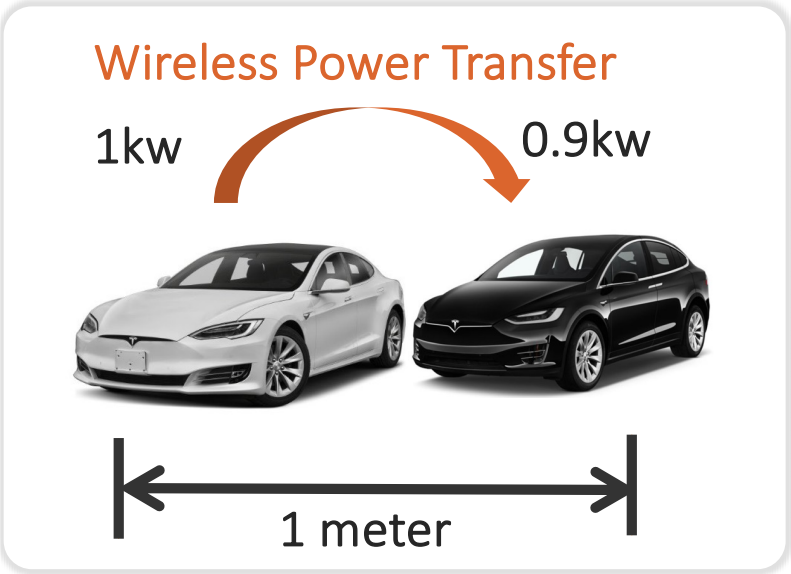
- Energy domain: power charging and power discharging
- Information domain: information exchange between EVs and charging station
- Transport domain: traffic management, traffic flow

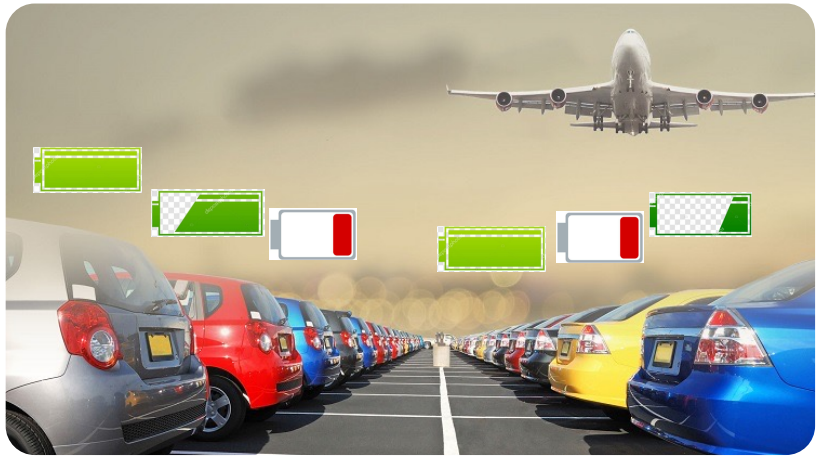
Electric Vehicles (EVs)

- Energy consumer: charging
- Energy storage: battery
- Energy provider: discharging



Example 2: Energy P2P Sharing among Electric Vehicles (2/2)





Airport Parking

- Wireless Power Transfer experiment: At kilowatts power level, the transfer distance can be several hundred millimeters with efficiency above 90% (*)

- Each vehicle can: (1) buy and sell its own electricity with other vehicles in a distributed environment; (2) EVs do not trust each other

(*) S. Li and C. Mi, "Wireless Power Transfer for Electric Vehicle Applications", IEEE Journal of Emerging and Selected Topics in Power Electronics, vol.3, no.1, March 2015.

Example 3: Blockchain for charging stations sharing

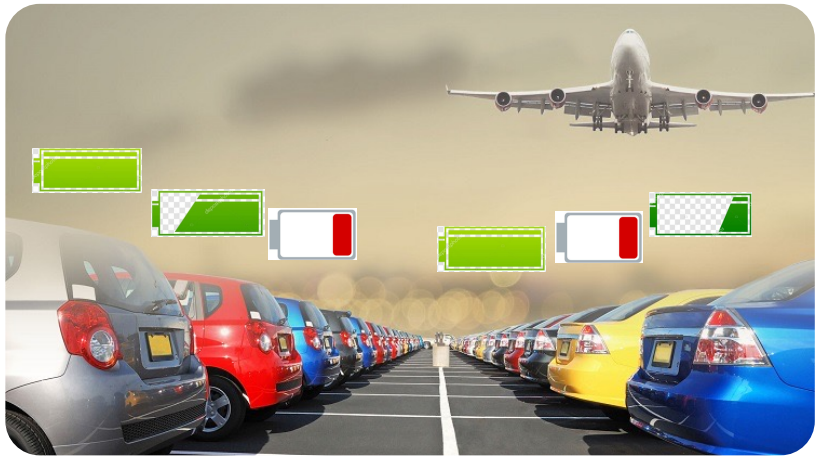
- Sharing charging stations: (1) when your charging station is not in use, someone else can rent the station; (2) you do not trust each other
- Challenge: we need a method to ensure secure charging station sharing → Blockchain's principle!



- Role of Blockchain: (1) allow users to share charging stations across a decentralized platform, without the need for intermediaries; (2) make simple, secure payments using the blockchain; (3) the charging stations operate autonomously, allowing users to access and obtain energy through direct payments.

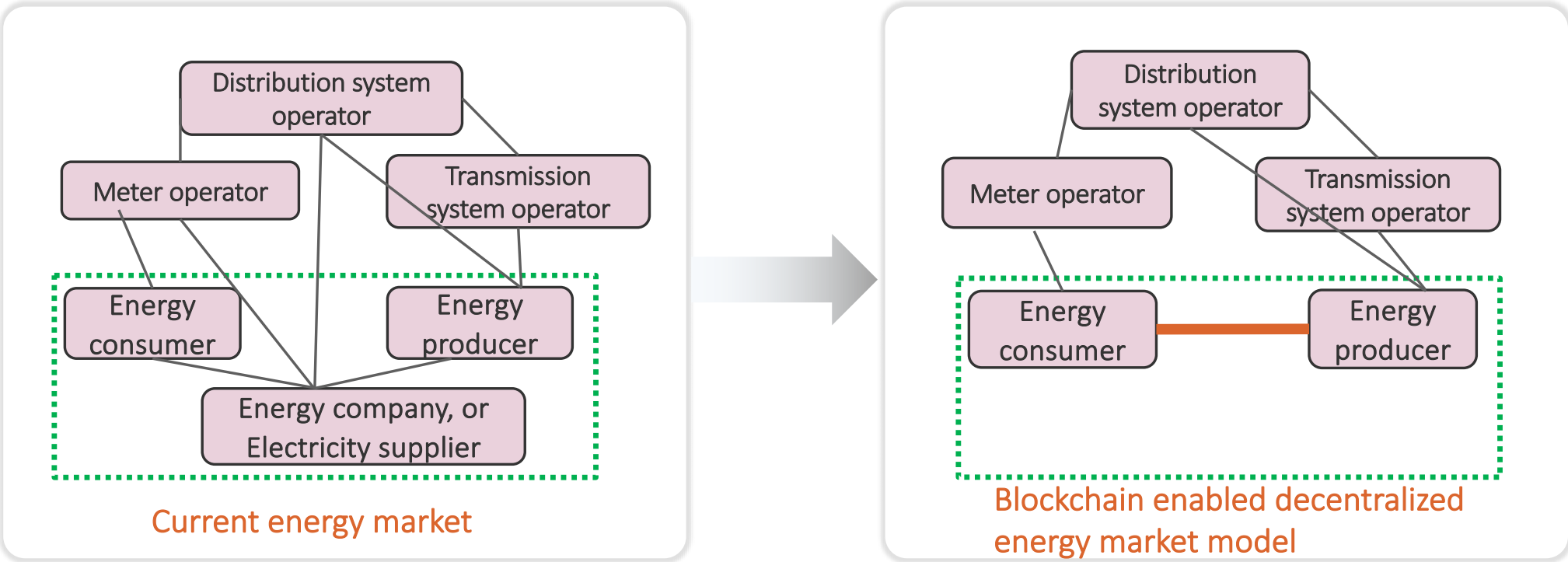
Decentralized energy trading: everyone can contribute/share power





- Common feature: no need for a third-party utility participating in energy exchange among houses or electric vehicles → low cost, flexible, new business models
- Challenge: need a method to ensure secure energy trading in distributed energy trading among untrusted houses or EVs.
- Solution: Blockchain as a distributed ledger, and smart contracts to execute and store local energy transactions

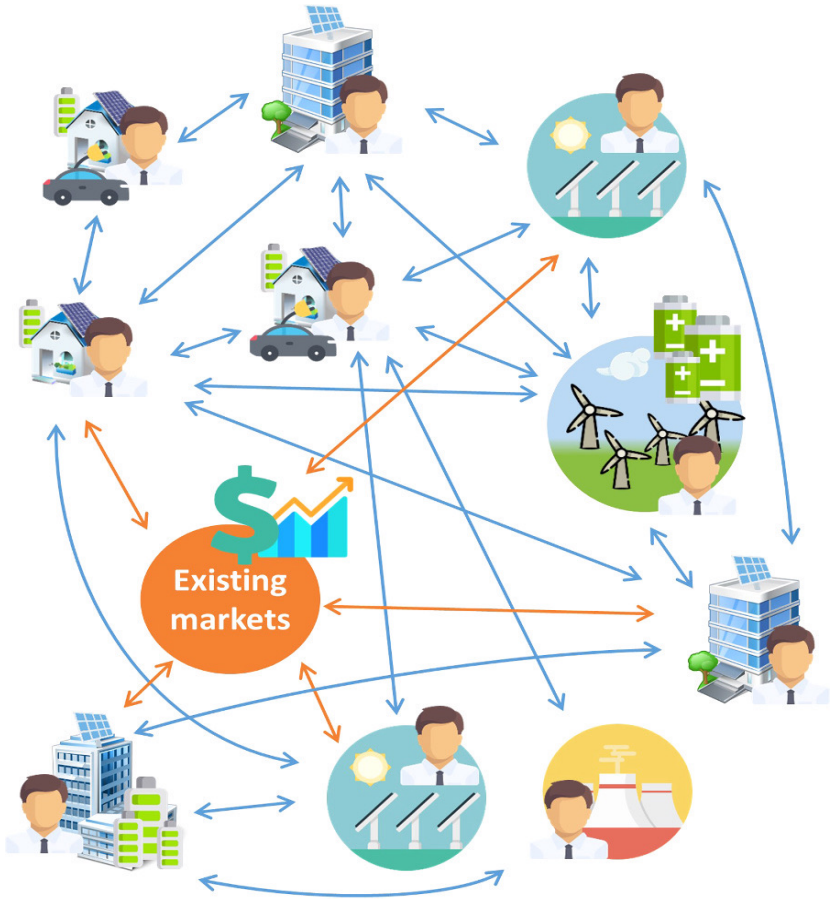
Will blockchain transform the energy market?



- Energy companies or suppliers will not be used in the new energy market.
- Energy consumers and energy producers trade energy directly with each other without a third party.

Q: What challenges are there in realizing a fully decentralized energy market model?

Challenges of a fully decentralized (P2P) energy market design

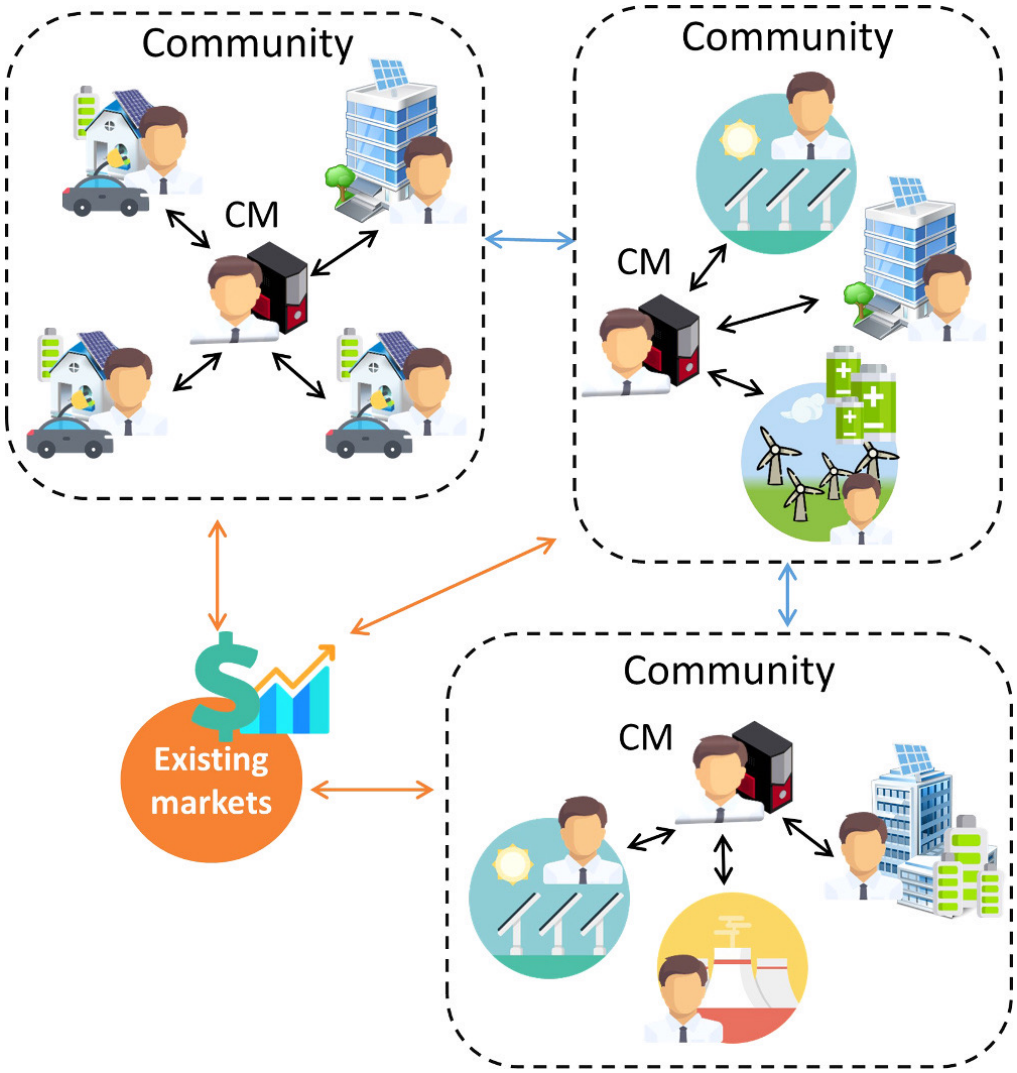


- Challenges include:
  - Safety and power quality
  - Predicting system behaviour
  - Consensus on final energy delivery
  - And more …

Hybrid community-based energy market

The community manager (CM)

- manages trading activities inside the community
- acts as inter-mediator (e.g., aggregator role) between the community and the rest of the system
- (consortium) blockchain empowered to record transactions

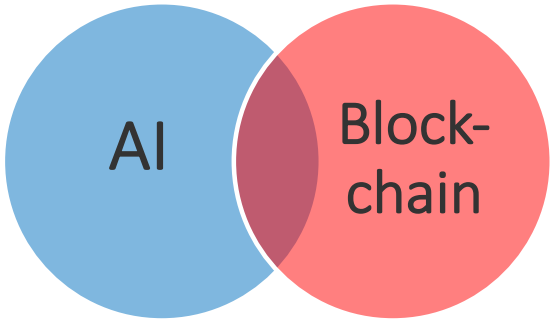


03

MORE CONSIDERATIONS…

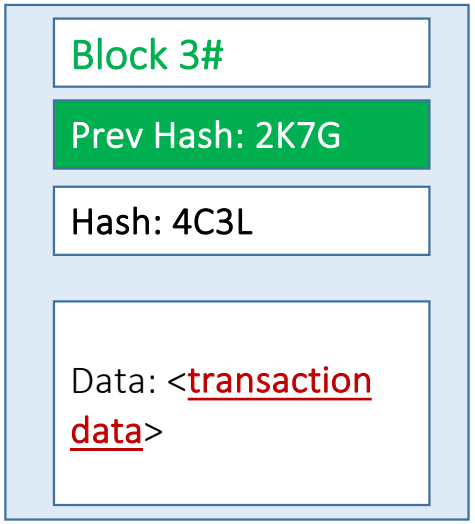
Blockchain and AI

- Q: what is the interaction between AI and Blockchain?



- AI for Blockchain: all transactions are saved in blockchain permanently. Machine learning can be used to analyze the data and find malicious transactions

- Blockchain for AI: In many cases, we send out private data to a server and then the server builds a machine learning model based on the collected data. Blockchain can be used to protect private data; and control the use of data and training models



Similar as Bitcoin, can we create a new cryptocurrency for use within the energy market?

- The SolarChange project was created to financially reward producers of solar energy via a blockchain.
- The project was launched by the company SolarCoin, which has developed its own cryptocurrency – similar to Bitcoin – for the purpose of selling solar energy.
- Main idea: for every MegaWatt of solar energy fed into the grid, the producer is awarded one SolarCoin, which they can either store in their SolarCoin wallet or convert to bitcoins.



SolarChange platform for the exchange of SolarCoin.
See more: http://solarcoin.org/

References

- PWC Global power and utilities, “Blockchain: an opportunity for energy producers and consumers?”

  https://www.pwc.nl/en/publicaties/blockchain-an-opportunity-for-energy-producers-and-consumers.html