Blockchain

Department of Computer Science and Engineering

Indian Institute of Technology, Jodhpur

Presented By:
Dr. Debasis Das
Computer Science and Engineering Department
Indian Institute of Technology, Jodhpur

Cryptography

Figure 30.1 *Cryptography components*

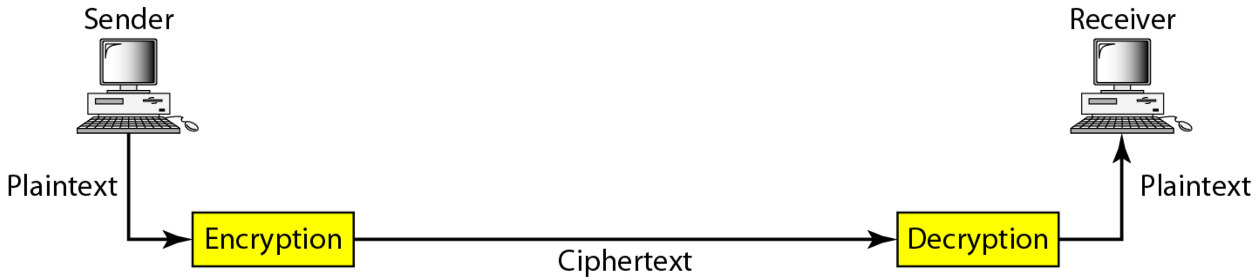
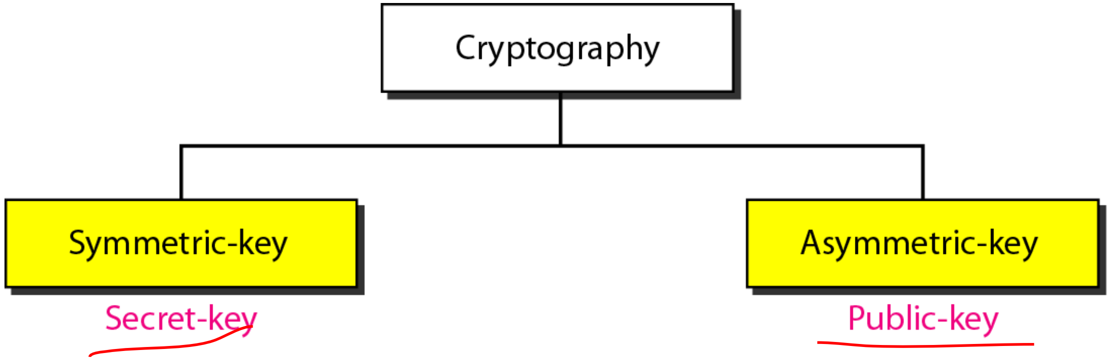


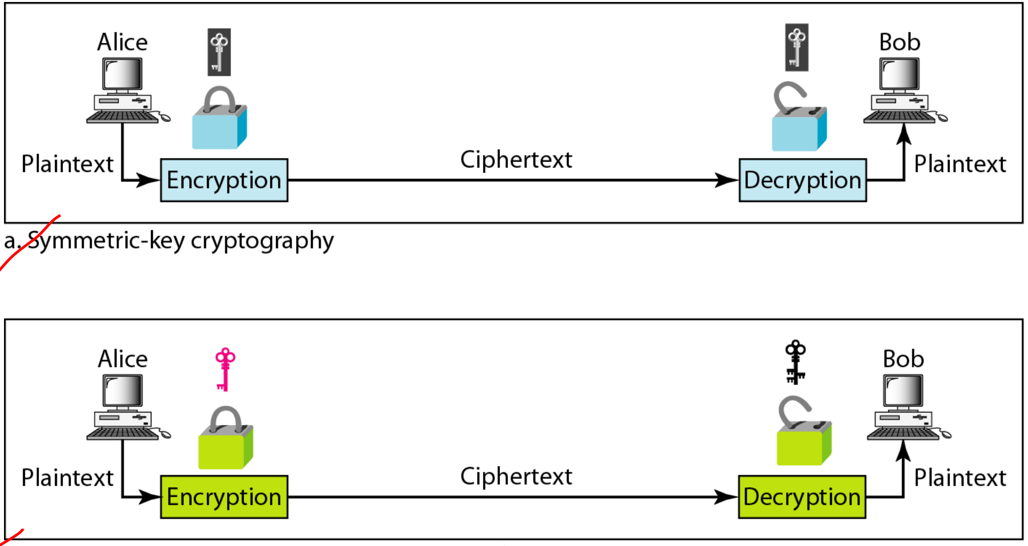
Figure 30.2 *Categories of cryptography*



Note

In symmetric-key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared.

Figure 30.6 *Comparison between two categories of cryptography*



a. Symmetric-key cryptography

b. Asymmetric-key cryptography

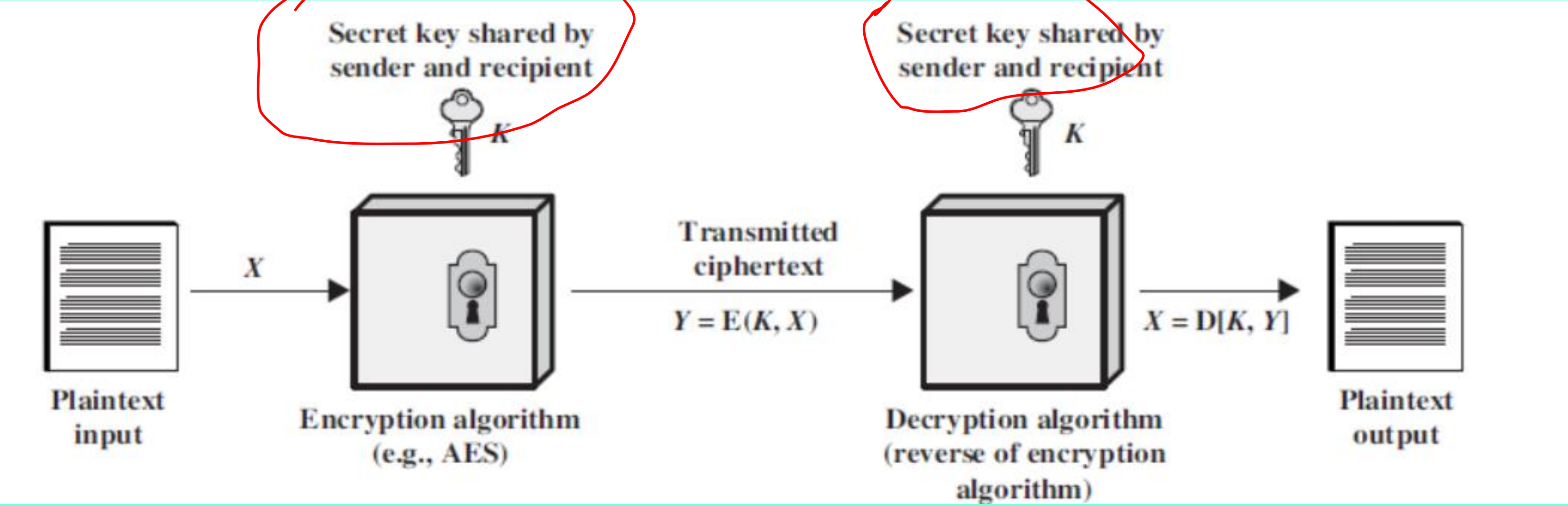
Some basic terminologies used:

- **plaintext -** the original message
- **cipher text -** the coded message
- **Cipher -** algorithm for transforming plaintext to cipher text
- **Key -** info used in cipher known only to sender/receiver
- **encipher (encrypt) -** converting plaintext to cipher text
- **decipher (decrypt) -** recovering plaintext from cipher text
- **Cryptography -** study of encryption principles/methods

Some basic terminologies used:

- **Cryptanalysis (code breaking) -** the study of principles/ methods of deciphering cipher text *without* knowing key
- **Cryptology -** the field of both cryptography and cryptanalysis

Symmetric Key Encryption



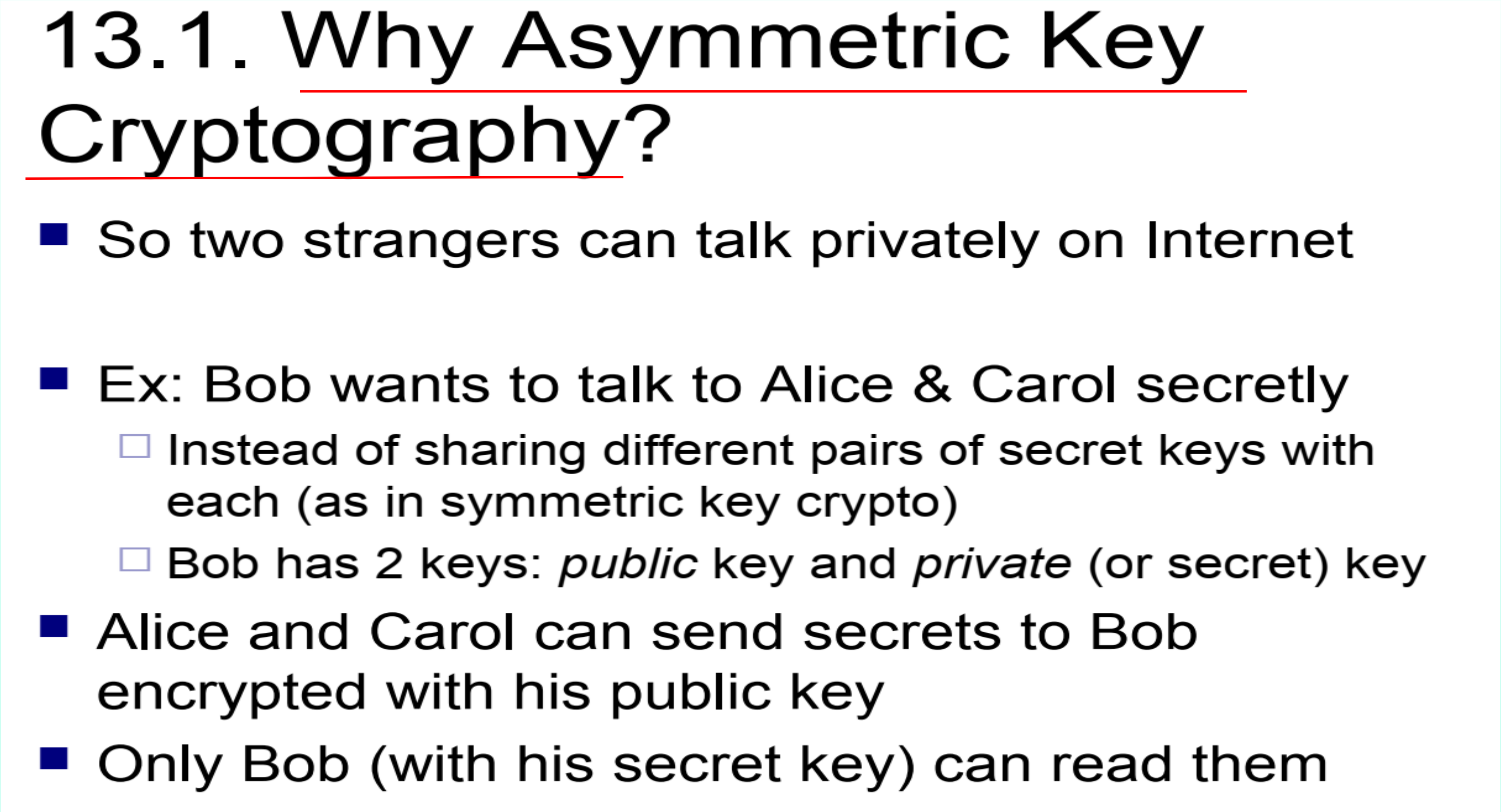
Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Asymmetric Key Cryptography

Agenda

- Problem with Symmetric Key Crypto: Alice & Bob have to agree on key!
- In 1970, Diffie & Hellman propose asymmetric or public key cryptography

- RSA & Elliptic Curve Cryptography (ECC)
- Certificate Authorities (CAs)
- Identity-Based Encryption (IBE)
- Authentication via Encryption

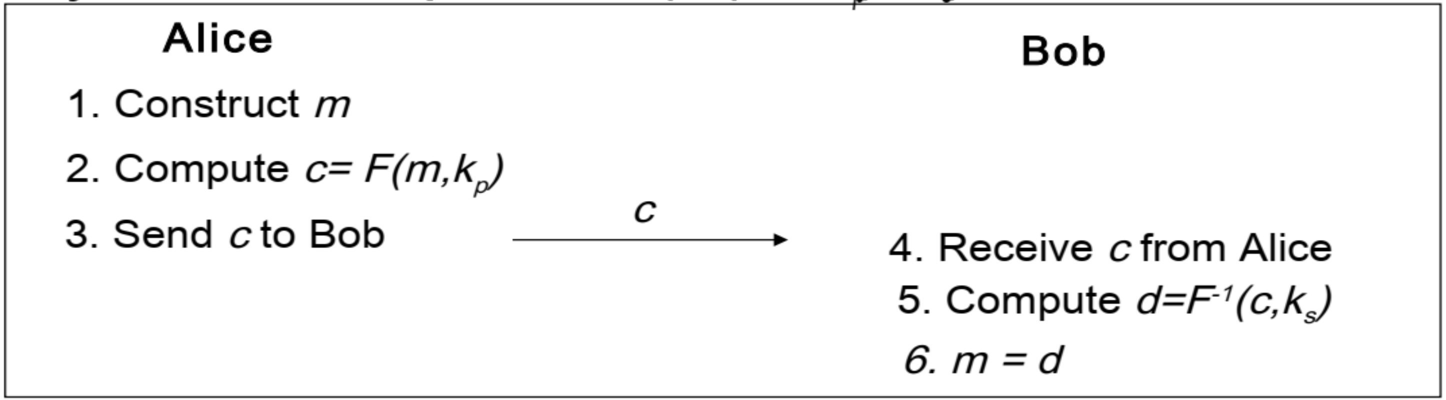


13.1. Why Asymmetric Key Cryptography?

- So two strangers can talk privately on Internet
- Ex: Bob wants to talk to Alice & Carol secretly
  - □ Instead of sharing different pairs of secret keys with each (as in symmetric key crypto)
  - □ Bob has 2 keys: *public* key and *private* (or secret) key
- Alice and Carol can send secrets to Bob encrypted with his public key
- Only Bob (with his secret key) can read them

Asymmetric Encryption

- Alice encrypts a message with ***different*** key than Bob uses to decrypt
- Bob has a public key, k_p, and a secret key, k_s. Bob's public key is known to Alice.
- Asymmetric Cipher: $F^{-1}(F(m,k_p),k_s) = m$



Alice

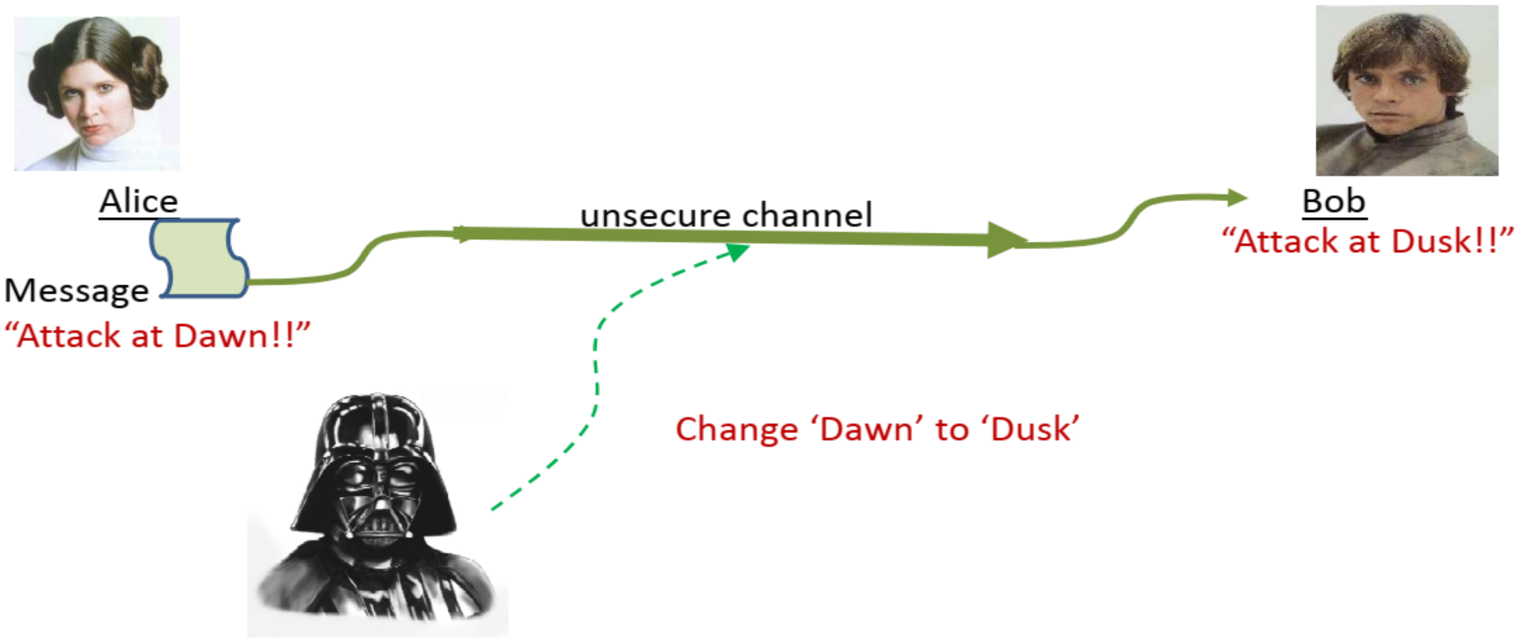
1. Construct *m*
2. Compute $c = F(m,k_p)$
3. Send *c* to Bob

Bob

4. Receive *c* from Alice
5. Compute $d = F^{-1}(c,k_s)$
6. $m = d$

Cryptographic Hash Functions

Issues with Integrity



Alice

Message

“Attack at Dawn!!”

unsecure channel

Bob

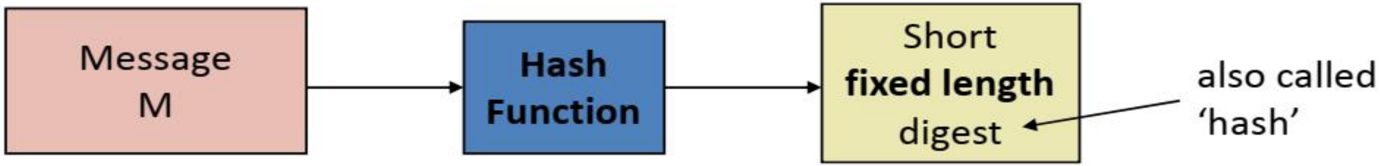
“Attack at Dusk!!”

Change ‘Dawn’ to ‘Dusk’

How can Bob ensure that Alice’s message has not been modified?

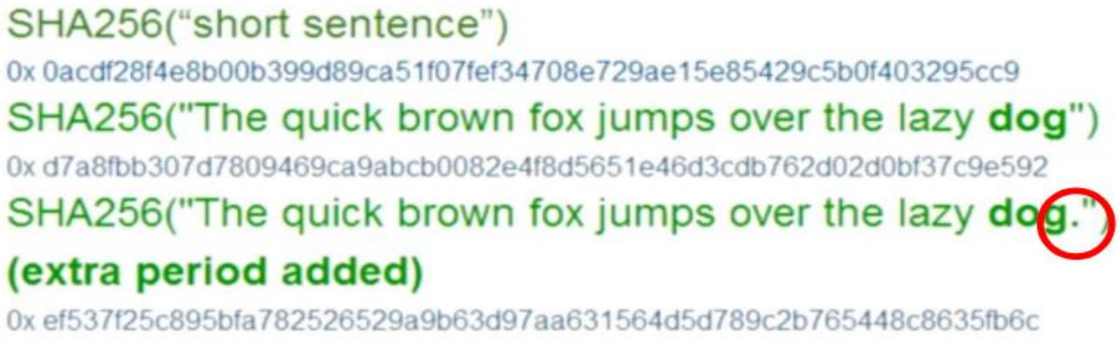
Note…. We are not concerned with confidentiality here

Avalanche Effect



Hash functions provide unique digests with high probability.

Even a small change in **M** will result in a new digest



SHA256("short sentence")

0x 0acdf28f4e8b00b399d89ca51f07fef34708e729ae15e85429c5b0f403295cc9

SHA256("The quick brown fox jumps over the lazy **dog**")

0x d7a8fbb307d7809469ca9abcb0082e4f8d5651e46d3cdb762d02d0bf37c9e592

SHA256("The quick brown fox jumps over the lazy **dog.**")

(extra period added)

0x ef537f25c895bfa782526529a9b63d97aa631564d5d789c2b765448c8635fb6c

Hash functions in Security

- Digital signatures
- Random number generation
- Key updates and derivations
- One way functions
- MAC
- Detect malware in code
- User authentication (storing passwords)

Blockchain

- **Blockchain** is mostly known as the technology underlying the **cryptocurrency Bitcoin.**
- The core idea of a blockchain is **decentralization.**
- This means that blockchain does not store any of **its database in a central location.**
- Instead, the blockchain is copied and spread across a **network of participants (i.e. computers).**
- Whenever a **new block is added to the blockchain**, every computer on the network **updates its blockchain to reflect the change**.

Blockchain (1)

- This decentralized architecture **ensures robust and secure operations** on blockchain with the advantages of tamper resistance and **no single-point failure vulnerabilities.**
- In particular, blockchain can be accessible for everyone and is not controlled by any network entity.
- This is enabled by a mechanism called **consensus** which is a set of rules to ensure the agreement among all participants on the status of the **blockchain ledger.**
- The general concept on how blockchain operates is shown in Figure.

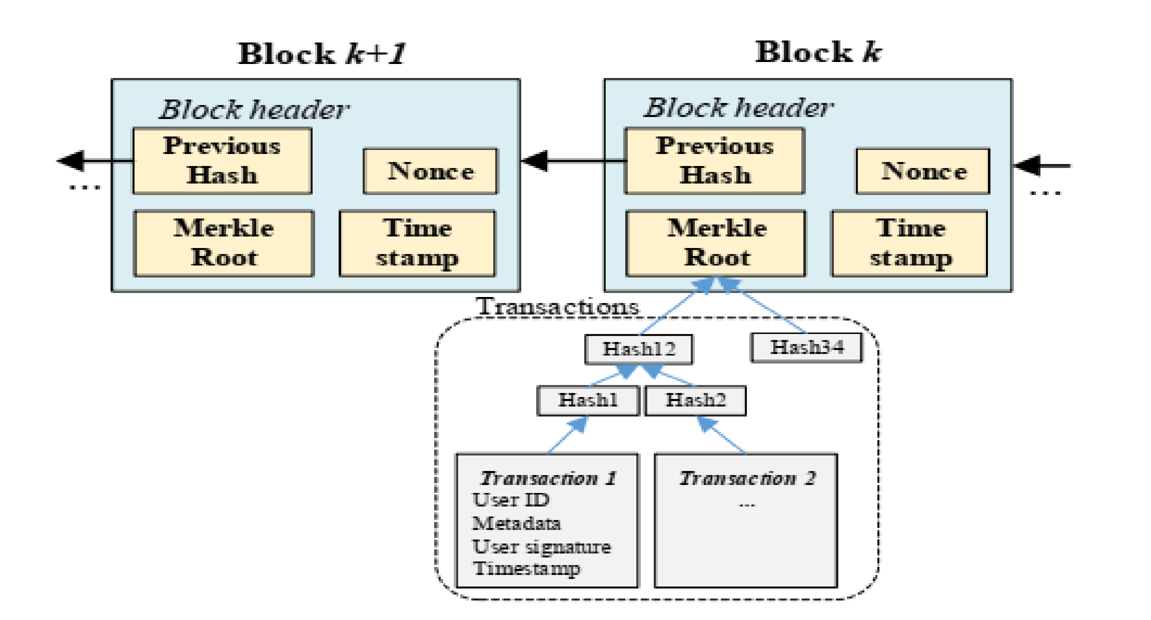
Blockchain(2)

- In general, blockchains can be classified as either a **public (permission-less) or a private (permissioned) blockchain.**

- A public blockchain is accessible for everyone and anyone can join and make transactions as well as participate in the **consensus process**.
- The best-known public blockchain applications include **Bitcoin and Ethereum**.
- Private blockchains on the other hand are an invitation-only network managed by a central entity.
- A participant has to be permissioned using a **validation mechanism**.

Data block

Blockchain is essentially a **chain of blocks**, a linear structure beginning with a so-called **genesis block** and continuing with every new block linked to the chain.



Distributed ledger (database):

- **Distributed ledger** is a type of database which is shared and replicated among the entities of a peer-to-peer network.
- **The shared database is available** for all network participants within the blockchain ecosystem.
- Distributed ledger records transactions similar to the process of data exchange among the members of the network.

Consensus algorithms:

- When nodes start to share or exchange data on a blockchain platform, there is **no centralized parties** to regulate **transaction rules and preserve data against security threats.**
- In this regard, it is vitally necessary to validate the **block trustfulness**, keep track the data flow and guarantee safe information exchange to avoid fraud issue

Smart contracts

- A smart contract is a **programmable application** that runs on a blockchain network.
- Since the first smart contract platform known as Ethereum was released in 2015, smart contracts have increasingly become one of the most innovative topics in the blockchain area.

Main characteristics of blockchain:

- As a general purpose database technology, in theory blockchain can be applied to **any data-related context**.
- However, the efficiency of **distributed ledgers** come with costs.
- **Blockchain** technology may be not the **best solution for every scenario.**
- The important step in assessing the potential benefits of blockchain in 5G is to ask whether its characteristics such as **decentralization, immutability, transparency, security and privacy** are useful for 5G networks and services.

Decentralization

- No central authority or trusted third party is needed to perform transactions.
- Users have full control on their own data.

Immutability

- It is very difficult to modify or change the data recorded in the blockchain

Transparency

- All information of transactions on blockchain (i.e. public ledgers) can be viewable to all network participants.

Security and privacy

- Blockchain **employs asymmetric cryptography** for security with **high authentication, integrity, and nonrepudiation**.
- Smart contracts available on blockchain can support **data auditability, access control and data provenance for privacy**

Public and Private Blockchain

Characteristics	Public Blockchain	Private Blockchain
Accessibility	Anyone	Single Organization
Authority	Decentralized	Partially Decentralized
Transaction Speed	Slow	Fast
Consensus	permissionless	permissioned
Efficiency	Low	High
Immutability	Full	Partial
Example of Blockchain	Bitcoin, Ethereum	Hyperledger
Example of Consensus	PoW, PoS	PBFT, ABFT

Blockchain simplifies complex transactions

Financial assets

- Faster settlement times
- Increased credit availability
- Transparency & verifiability
- No reconciliation cost

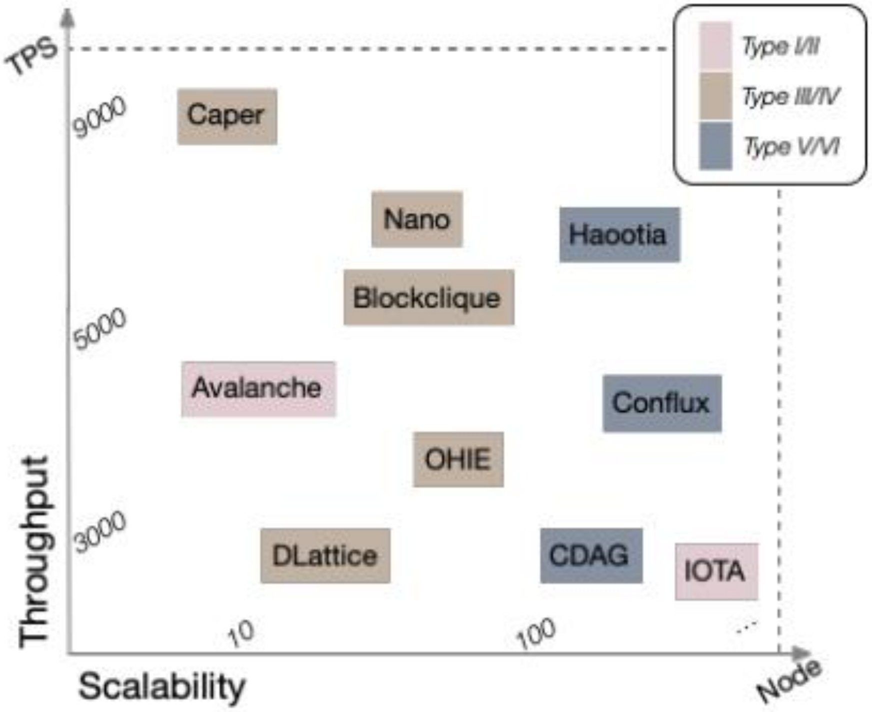
Property records

- Digital but unforgeable
- Fewer disputes
- Transparency & verifiability
- Lower transfer fees

Logistics

- Real-time visibility
- Improved efficiency
- Transparency & verifiability
- Reduced cost

Throughput and Scalability



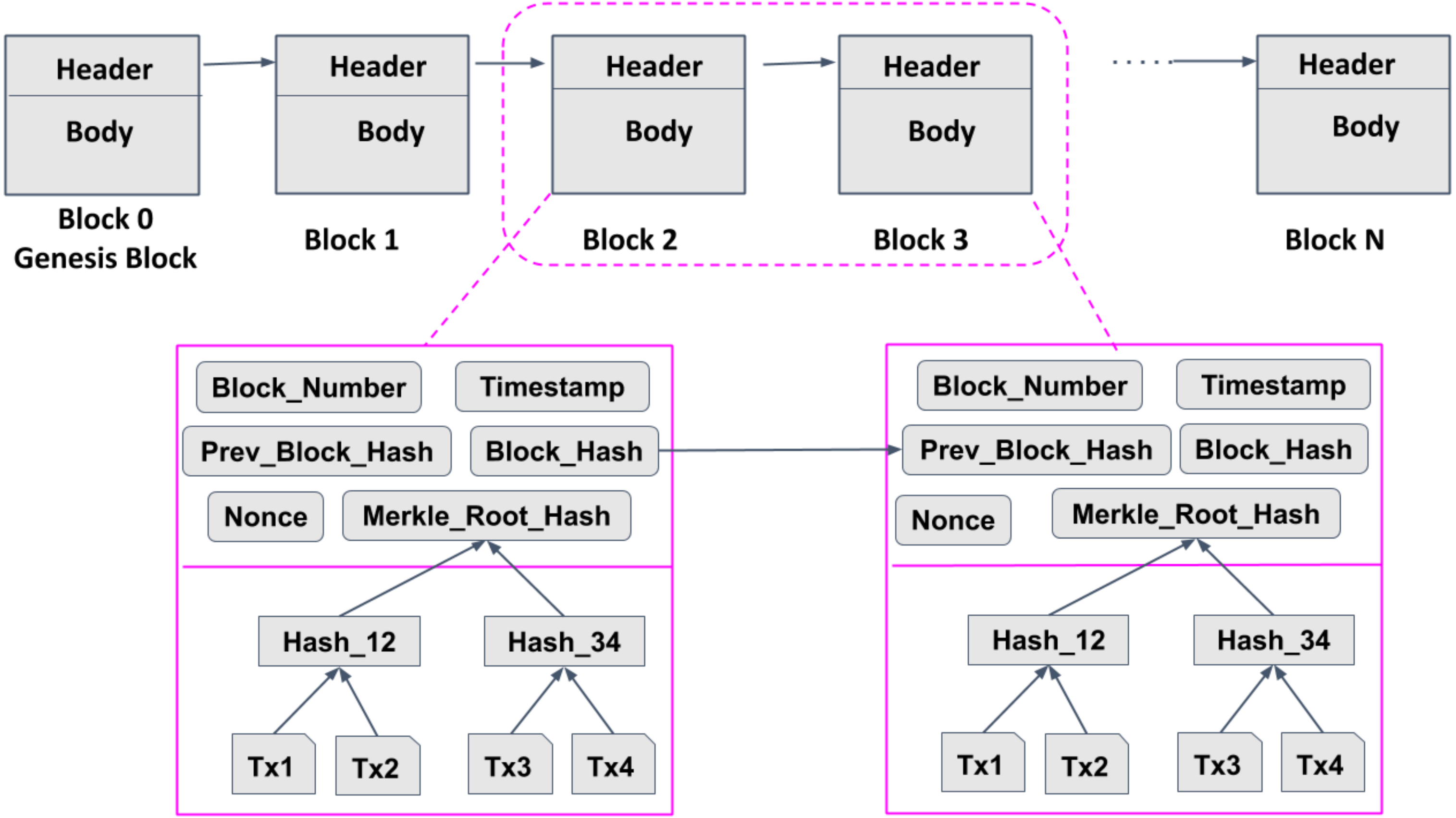
Blockchain

1. The core idea of a blockchain is **decentralization.** This means that blockchain does not store any of its database in a central location.
2. Whenever a new block is added to the blockchain, every computer on the network updates its blockchain to reflect the change.
3. This decentralized architecture **ensures robust and secure operations** on blockchain with the advantages of tamper resistance and no single-point failure vulnerabilities.
4. This is enabled by a mechanism called **consensus** which is a set of rules to ensure the agreement among all participants on the status of the blockchain ledger.
5. In general, blockchains can be classified as either a **public (permission-less) or a private (permissioned) blockchain.**
6. A **public blockchain** is accessible for everyone and anyone can join and make transactions as well as participate in the consensus process.
7. **Private blockchains** on the other hand are an invitation-only network managed by a central entity. A participant has to be permissioned using a validation mechanism.

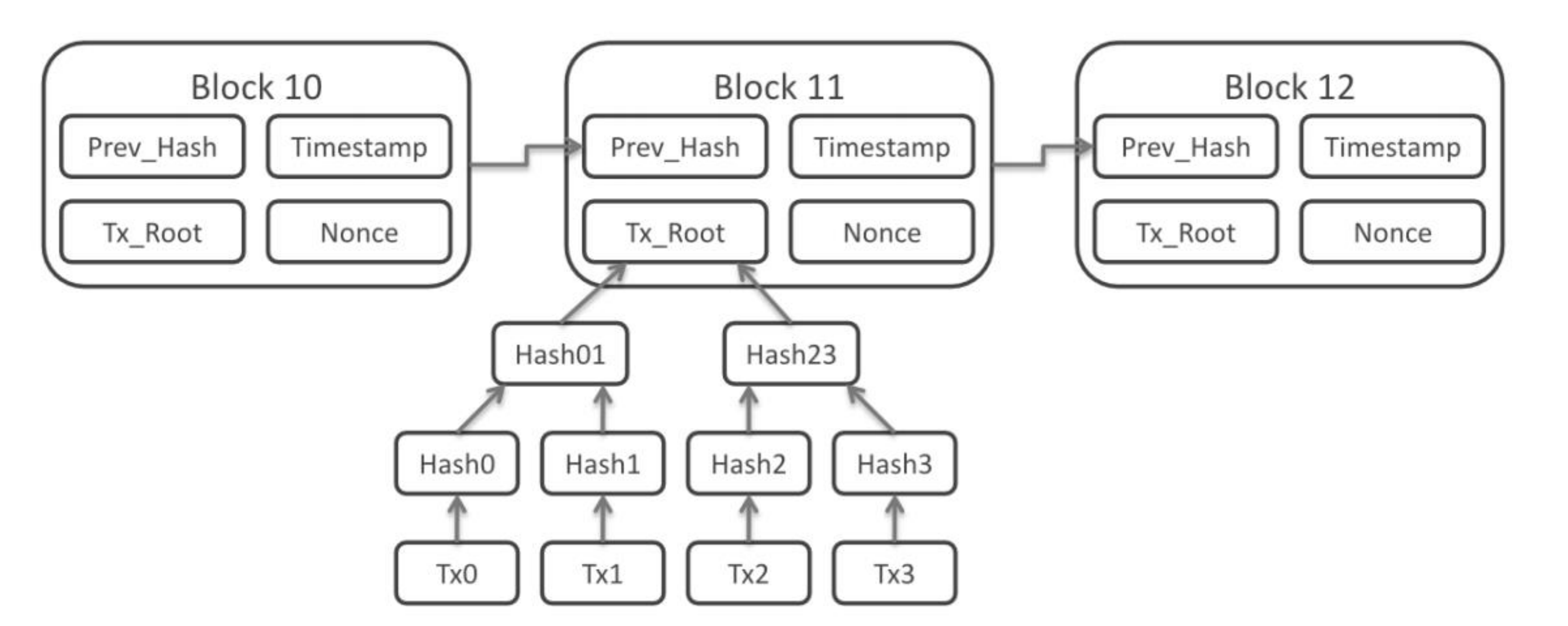
What Is a Merkle Tree?

- A **Merkle tree** is a data structure that is used in computer science applications.
- In bitcoin and other cryptocurrencies, **Merkle trees serve to encode blockchain data more efficiently and securely.**
- They are also referred to as "binary hash trees."

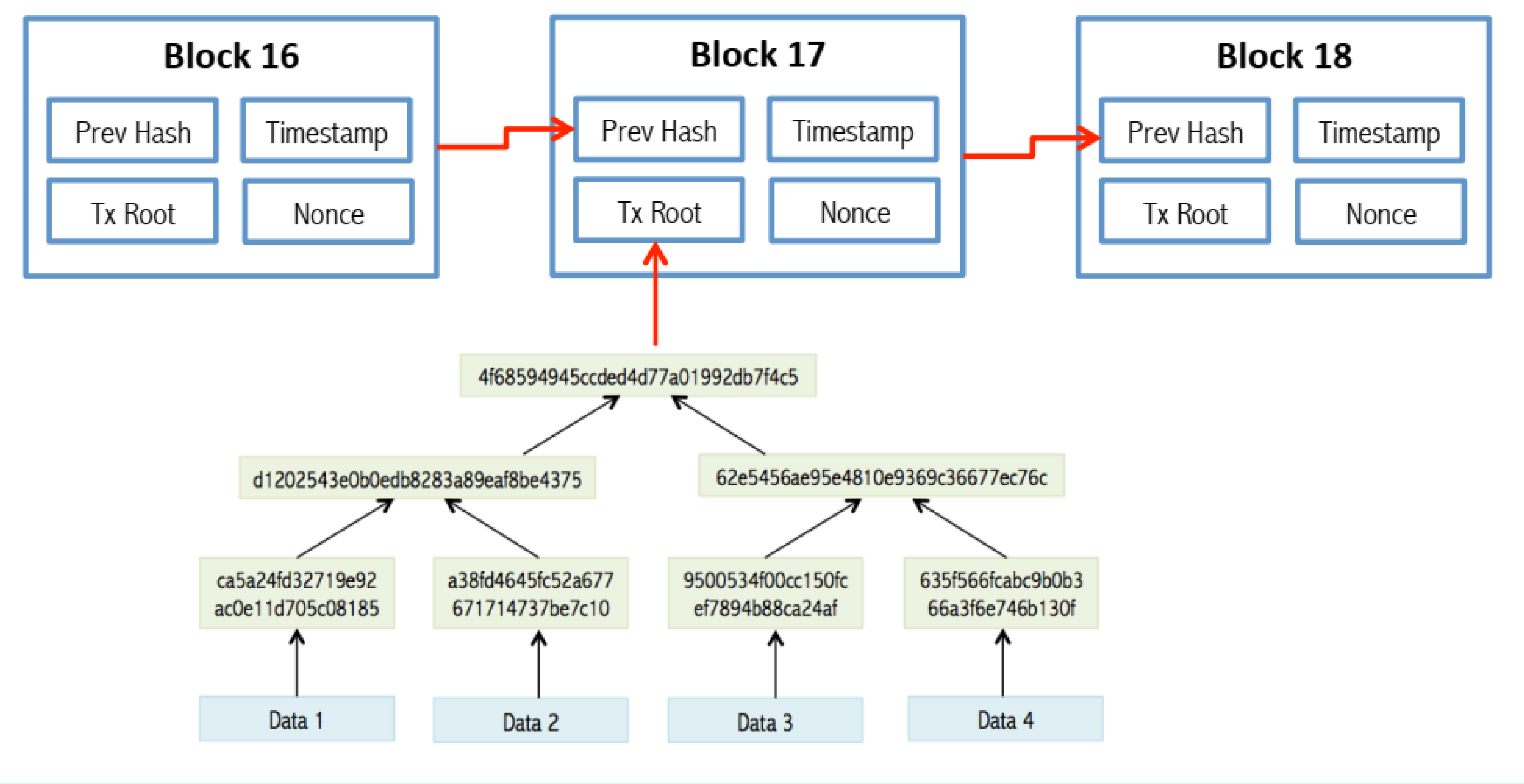
Blockchain


Header
Body
Block 0
Genesis Block
Header
Body
Block 1
Header
Body
Block 2
Header
Body
Block 3
Header
Body
Block N
Block_Number
Timestamp
Prev_Block_Hash
Block_Hash
Nonce
Merkle_Root_Hash
Hash_12
Hash_34
Tx1
Tx2
Tx3
Tx4
Block_Number
Timestamp
Prev_Block_Hash
Block_Hash
Nonce
Merkle_Root_Hash
Hash_12
Hash_34
Tx1
Tx2
Tx3
Tx4

Transactions for are hashed in a Merkle Tree (Blockchain-based protocol)



The data structure of the Bitcoin Blockchains

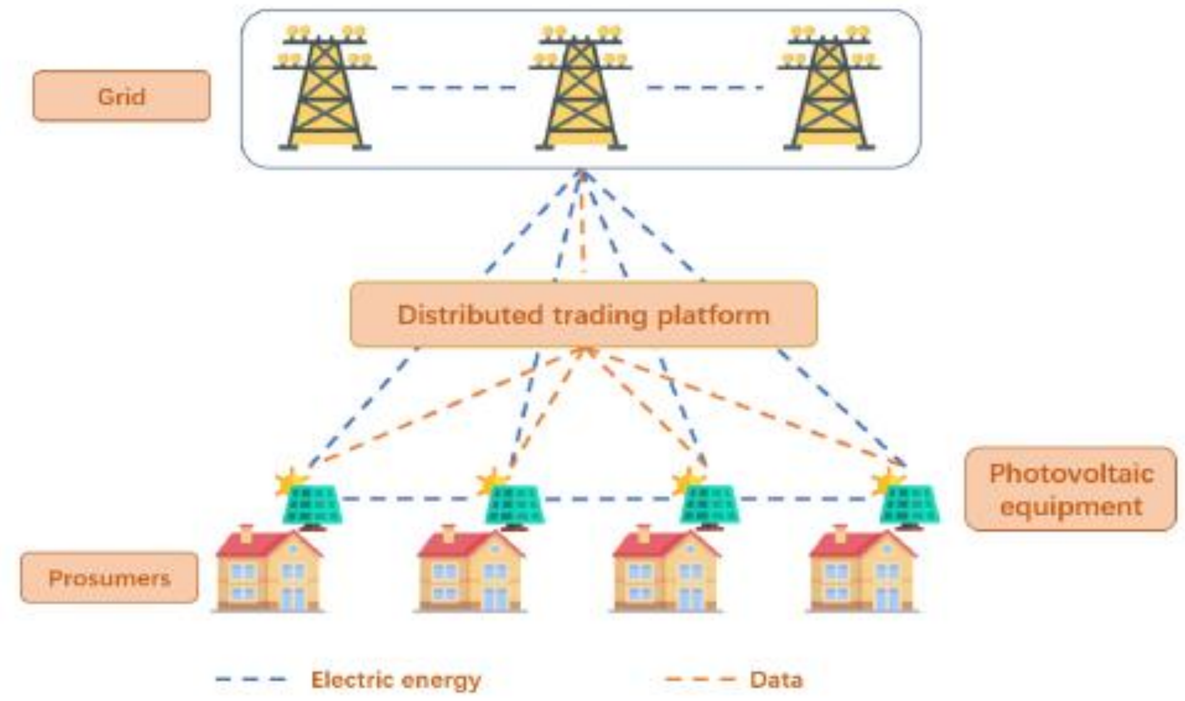


Block 16
Prev Hash
Timestamp
Tx Root
Nonce
Block 17
Prev Hash
Timestamp
Tx Root
Nonce
Block 18
Prev Hash
Timestamp
Tx Root
Nonce
4f68594945ccded4d77a01992db7f4c5
d1202543e0b0edb8283a89eaf8be4375
62e5456ae95e4810e9369c36677ec76c
ca5a24fd32719e92 ac0e11d705c08185
a38fd4645fc52a677 671714737be7c10
9500534f00cc150fc ef7894b88ca24af
635f566fcabc9b0b3 66a3f6e746b130f
Data 1
Data 2
Data 3
Data 4

Introduction

- **Fossil fuels (nonrenewable energy)** are limited, and it has been estimated that they will run out in the **early 22nd century** at the current rate of consumption.
- So, there has been an increased focus to explore the **utility of renewable energy** (e.g., solar energy and wind energy) in replacing fossil fuel.
- The **Householder owners** can install **solar photovoltaic power** generation systems in their own houses for self-use.

Distributed trading platform



Problem Statement

- **Householder owners** can install **solar photovoltaic power generation system** in their own houses for self-use,

- The **surplus electricity** can be uploaded to the **grid for financial rebates** (i.e., **consumers** becoming **prosumers**).

- One challenge associated with such a trend is the **management of the large**, **dynamic number of prosumers.**

Objective

- To design an efficient, safe, fair, and sustainable smart grid system.

Limitations of Existing Systems

- **Conventional grid** generally uses a centralized management system, which does not scale well or is **not suitable for managing the large number of prosumers.**
- The **cost of management and maintenance** will also be prohibitively high in a conventional centralized management mode,
- In addition to the need to deal with challenges due to different (or lack of common) standards, and lack of mutual trust among participants.

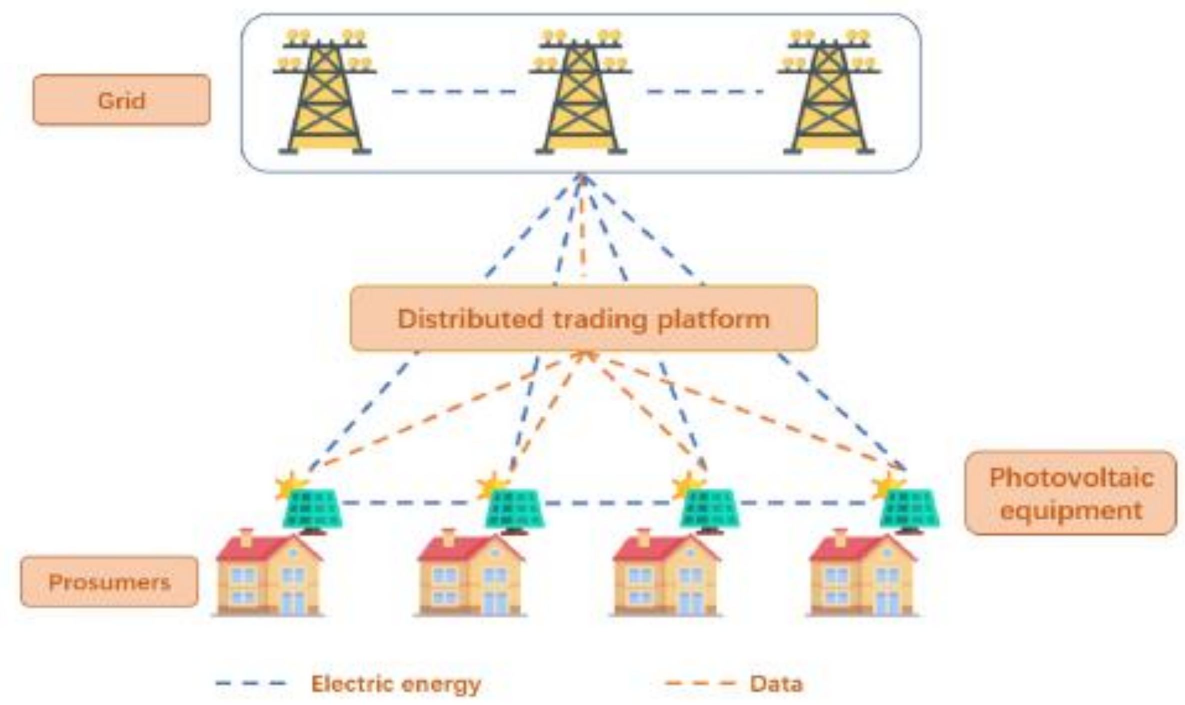
Challenges

- The World is rapidly shifting from conventional energy sources to **renewable energy sources** (e.g., smart grid).
- The widespread adoption of the **smart grid** requires it to be attack proof and leak-proof, and demand decentralizes the system for energy distribution to provide transparency in the smart grid system.
- However, this new modern energy system faces different challenges, such as the **large-scale Internet of Things (IoT) devices adaptation, single-point failure due to a centralized system, slow transaction processing, and the emerging cybersecurity threats.**

Contribution

- **This necessitates the design of an efficient, safe, fair, and sustainable smart grid system**.
- How blockchain technology has been and can be deployed in Distributed trading platforms for **sustainable society applications, ranging from energy management to peer-to-peer trading to electric vehicle-related applications to carbon emissions trading others**.

Distributed Trading platform



Possible Solutions:

- To solve all these issues of smart grid, we proposed a **novel blockchain-based security scheme.**
- This scheme is intended to secure the transactions and make the **energy distribution decentralized, reliable and transparent and immutable.**
- **1. Hybrid blockchain (public and private) with modified Consensus Algorithm, Structure, Leader Selection and Smart Contract etc.**

2.Decentralize trust algorithm for mutual trust among participants

3. Reinforcement Learning for reward and penalty calculation

THANK YOU