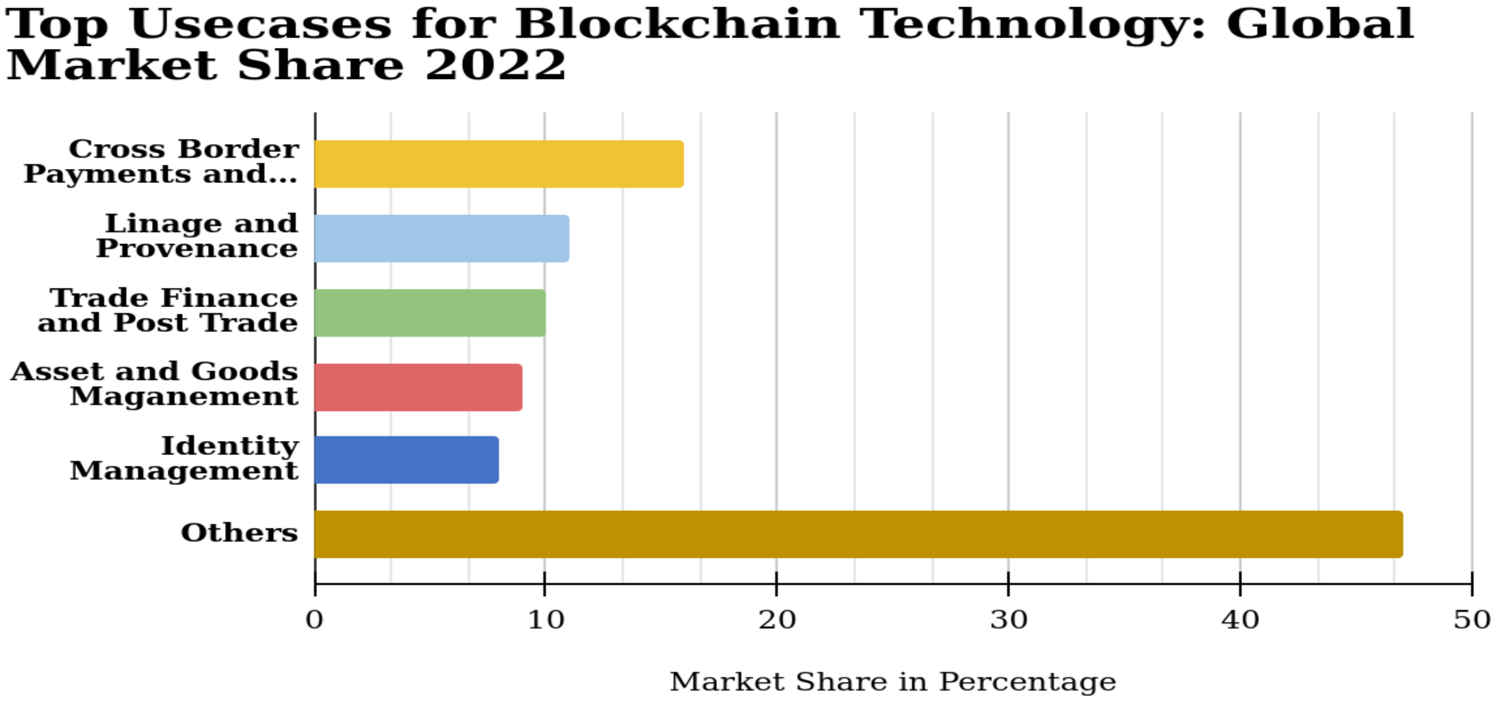
IoT security issues using Blockchain

Top Blockchain Technology use cases

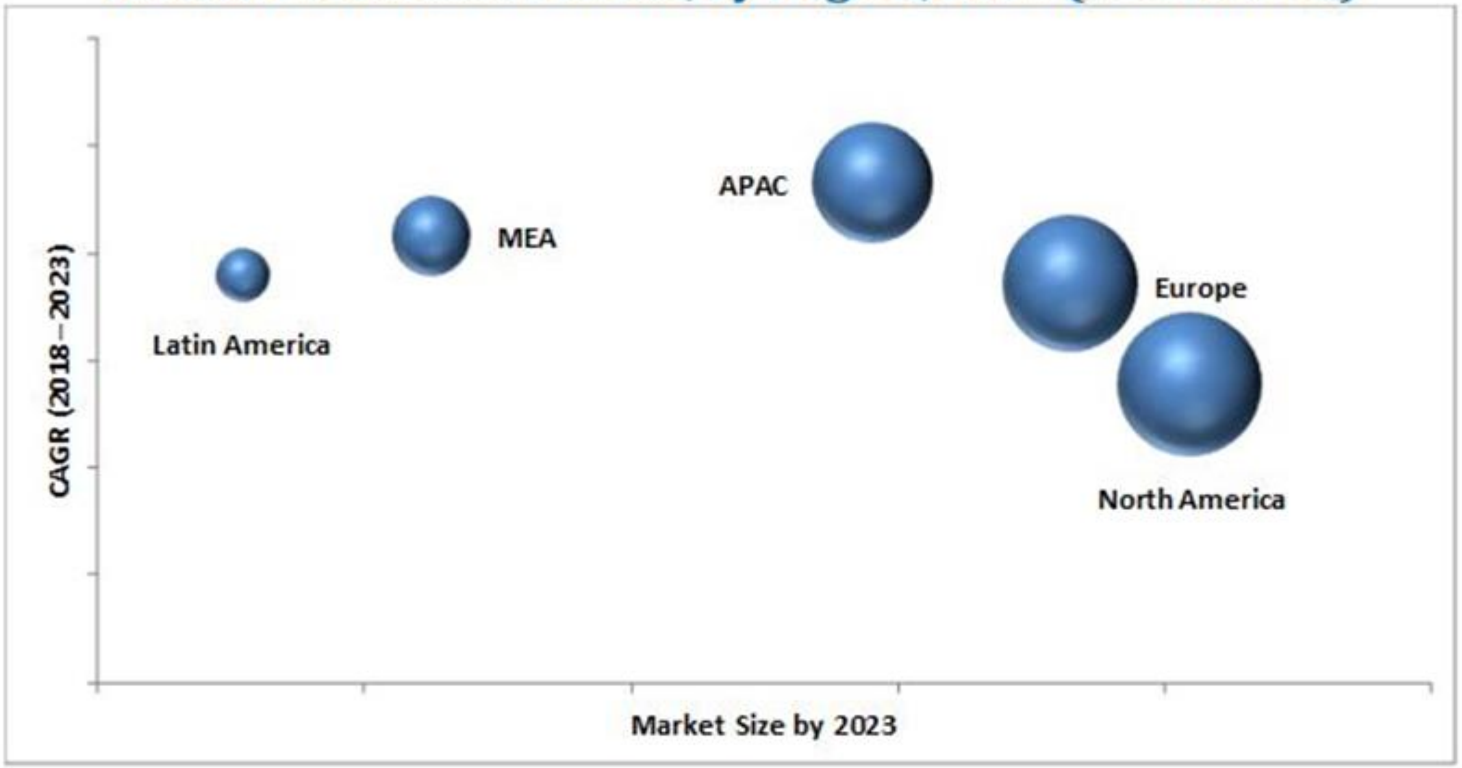
- The developing convergence of financial services and technology is referred to as FinTech and Top Blockchain Technology use cases are shown in Figure 1



Blockchain Based new financial services and products

- The development of blockchain technology has made it possible to create new financial services and products that are very secure for **FinTech Blockchain Market** shown in Figure 2(Compound Annual Growth Rate (CAGR))

Fintech Blockchain Market, by Region, 2023 (USD Million)

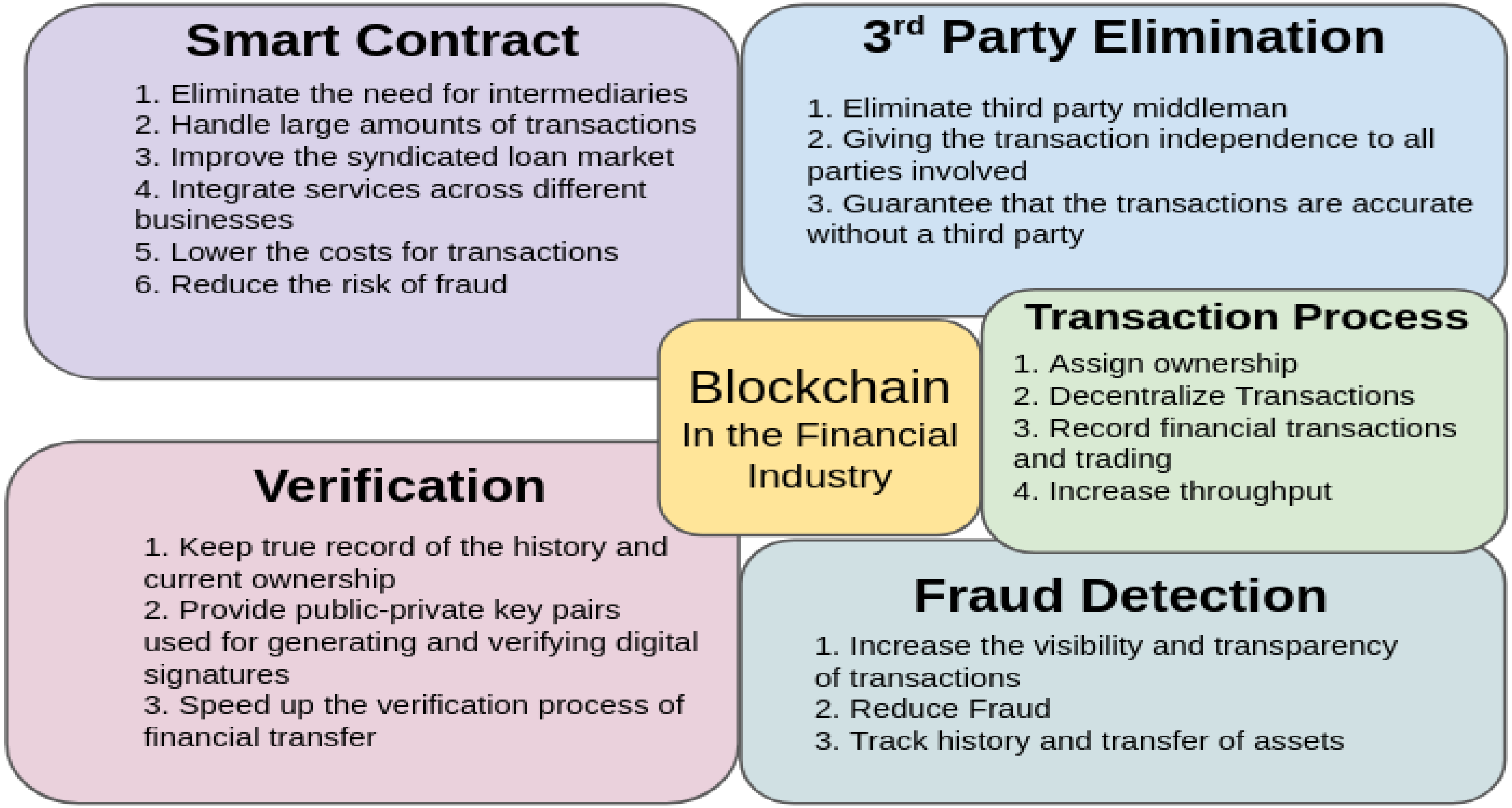


Best FinTech App

- In Figure 3 shown some of the best FinTech App in the world wide and Figure 4 shows that the Blockchain Startups Disrupting the Financial Services Industry

BEST FINTECH APPS
intuit mint
MoneyLion
Revolut
robinhood
coinbase
chime
N26
nubank
DOWNLOAD

Blockchain Startups (the Financial Services Industry)



Smart Contract

1. Eliminate the need for intermediaries
2. Handle large amounts of transactions
3. Improve the syndicated loan market
4. Integrate services across different businesses
5. Lower the costs for transactions
6. Reduce the risk of fraud

3rd Party Elimination

1. Eliminate third party middleman
2. Giving the transaction independence to all parties involved
3. Guarantee that the transactions are accurate without a third party

Blockchain In the Financial Industry

Transaction Process

1. Assign ownership
2. Decentralize Transactions
3. Record financial transactions and trading
4. Increase throughput

Verification

1. Keep true record of the history and current ownership
2. Provide public-private key pairs used for generating and verifying digital signatures
3. Speed up the verification process of financial transfer

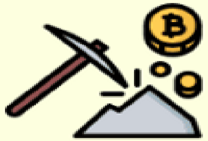
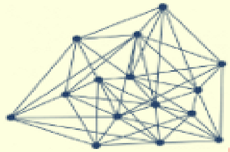
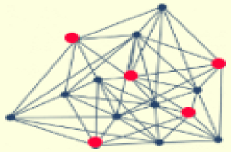
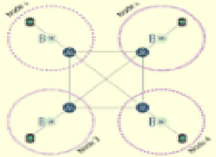
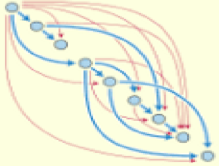
Fraud Detection

1. Increase the visibility and transparency of transactions
2. Reduce Fraud
3. Track history and transfer of assets

Example

- **Stellar** is a decentralized hybrid blockchain network available to anybody who wants to join. Lumens are the unit of measure for stellar currency
- **Ripple** is a cryptocurrency that is designed to address the present problems associated with cross-border transactions, and it performs the same functions as the SWIFT system (which is a central equivalent).
- **IOTA:** IOTA is an open-source distributed ledger and cryptocurrency designed for the Internet of things. It uses a directed acyclic graph to store transactions on its ledger, motivated by a potentially higher scalability over blockchain based distributed ledgers.

Comparison of Consensus Algorithms

	Proof-of-Work (POW)	Proof-of-Stake (POS)	Delegated Proof-of-Stake (DPOS)	Byzantine Fault Tolerance	Directed Acyclic Graphs (DAG)
Energy Consumption	High	Low	Very Low	Very Low	Very Low
Transaction Per Second	7 [redacted]	30 - 173	2.5 - 2,500	100 - 2,500	180 - 7,000
Transaction Fees	High	Low	Low	Very Low	None
Structure	Decentralized	Decentralized	Centralized	Decentralized	Decentralized
Example	Bitcoin	Dash	Bitshares	Stellar	IOTA

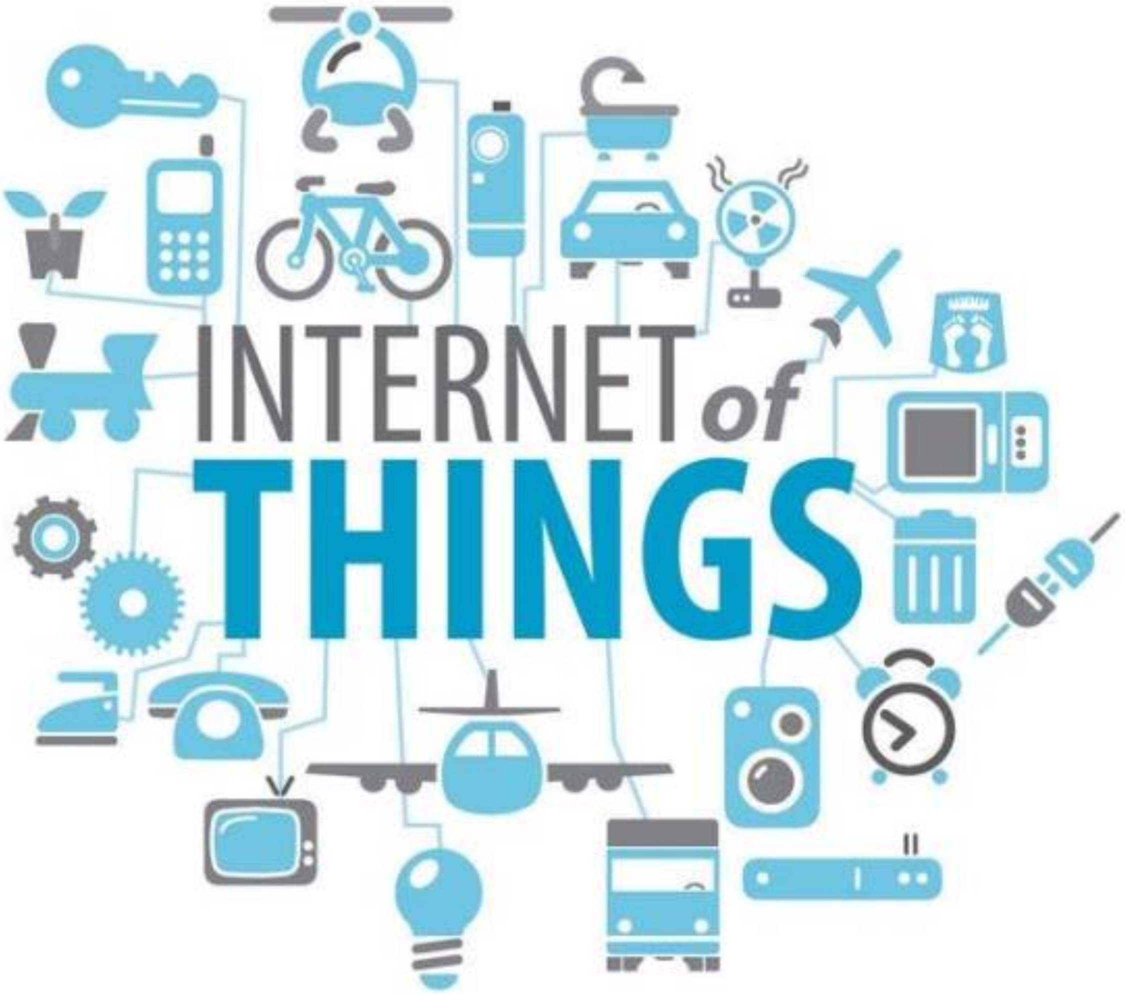
Where Might Blockchain Use Cryptography?

Initiation and Broadcasting of Transaction	• Digital Signatures • Private/Public Keys
Validation of Transaction	• Proof of Work and certain alternatives
Chaining Blocks	• Hash Function

IoT security issues using Blockchain and smart contracts

Dr. Debasis Das
Department of Computer Science and Engineering
IIT Jodhpur

Internet of Things (IoT)



- The Term IoT was first coined by Kevin Ashton in 1999

- Network of devices able to:
  - Configure themselves automatically,
  - Generate, process, and exchange data as we as
  - Request a service or start an action without human intervention at many levels.

Important Areas of Research for IoT

- Smart devices, sensors in real-time, Energy Saving
- WiFi, Bluetooth, ZigBee, etc …
- Big-data, Machine learning, Predictive analytics, …
- *Security/Privacy, Trust, Authenticity/Identity, Anonymity, …*

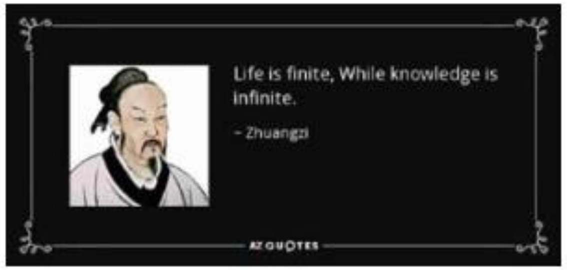
Security Requirements for IoT Devices

- Authentication & Data integrity
- Confidentiality (Encryption) is a NOT always required!
- Secure against node(s) key leakage

Security Issues for IoT Devices

Can be lost and stolen (security difficult)

Not reachable (mostly disconnected)



Life is finite, While knowledge is infinite.

- Zhuangzi

AZ QUOTES

Finite life (Credentials tied to lifetime)

Resource Constrained (no processing power for crypto)

Security Issues for IoT Devices

Studies Reveal 70% Of IOT Devices Are Vulnerable To Attack.

Majority of IoT devices had the following security issues:

- Privacy concerns
- Lacked encryption (processed/exchanged data and Firmware upgrades)
- Insecure updates
- Lack of mutual authentication (device, gateway)

Security Issues for IoT Devices

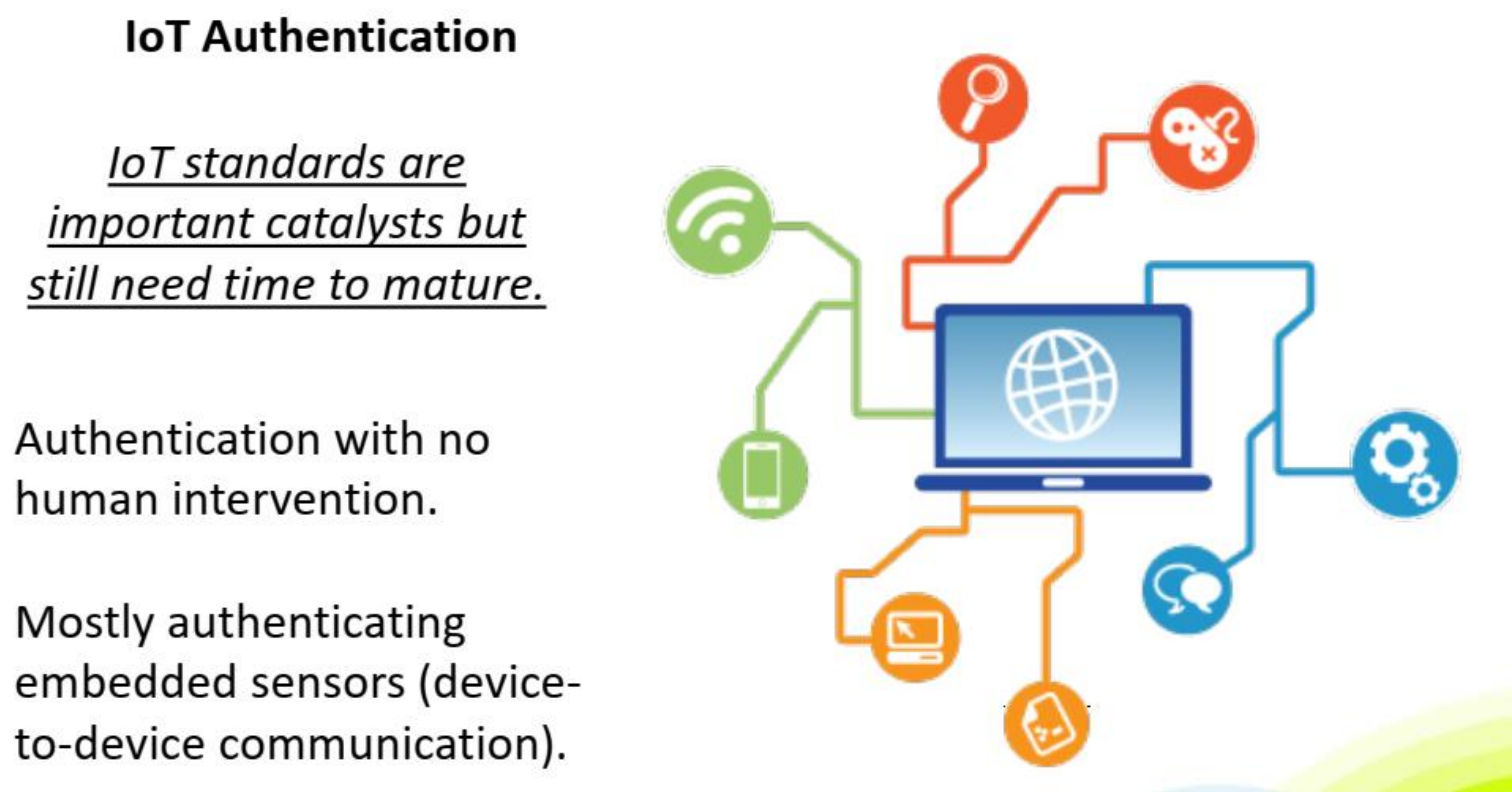
IoT Network Security

More challenging than traditional network security.

A wider range of communication protocols, standards, and device capabilities.

Pose significant issues and increased complexity!

Security Issues for IoT Devices



IoT Authentication

IoT standards are important catalysts but still need time to mature.

Authentication with no human intervention.

Mostly authenticating embedded sensors (device-to-device communication).

Security Issues for IoT Devices

IoT Encryption

Encryption is an absolute must

Encrypting data at rest and in transit.

Limited capability to have standard encryption processes and protocols.

Encryption key lifecycle management processes.

Data integrity and confidentiality.

Security Issues for IoT Devices

IoT PKI

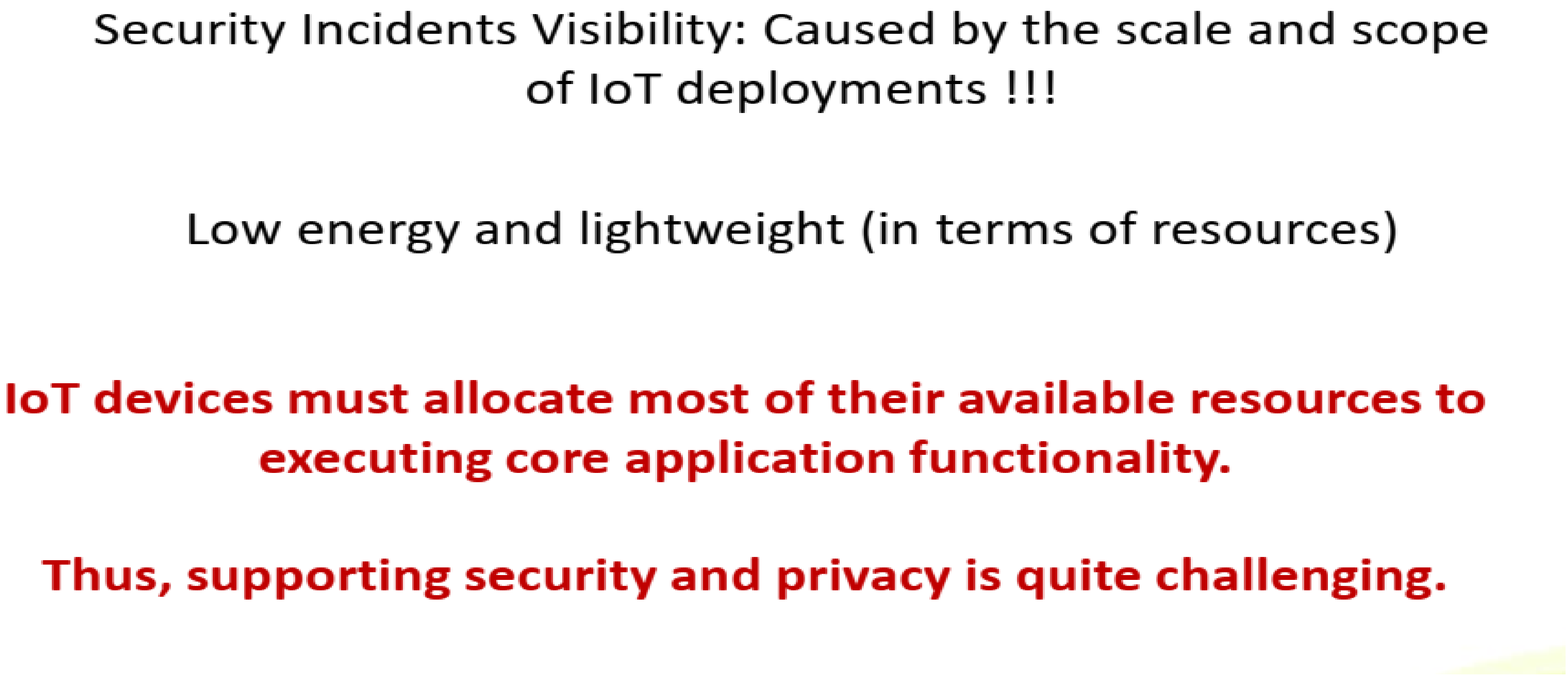
Digital certificate, and key (generation, distribution, management, and revocation).

Limited ability to utilize PKI.

Digital certificates securely loaded onto IoT devices at the time of manufacture or installed post-manufacture.

Data integrity and confidentiality.

Security Issues for IoT Devices



Security Incidents Visibility: Caused by the scale and scope of IoT deployments !!!

Low energy and lightweight (in terms of resources)

IoT devices must allocate most of their available resources to executing core application functionality.

Thus, supporting security and privacy is quite challenging.

Security Issues for IoT Devices

More IoT-specific security threats will definitely drive innovative Security Solutions mainly in new Cryptographic Primitives and Blockchain-based Approaches

Blockchain Technology

What is the problem that Blockchain attempts to solve?

Blockchain Technology

A Blockchain is an append-only distributed ledger that stores a time-ordered set of facts, aka transactions. Transactions are grouped into “blocks” and form a cryptographic hash-chain, hence the name Blockchain.

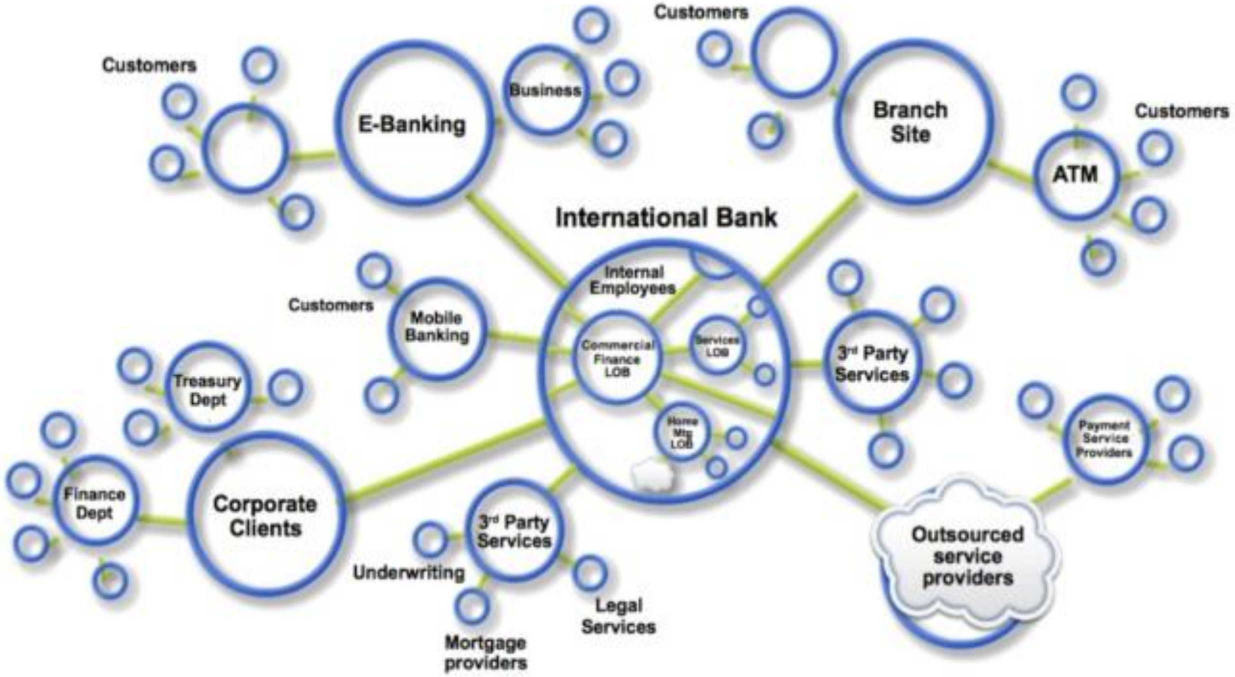
Role of Cryptography in Blockchain !!!!

- Integrity of ledger (Cryptographic hash function)
- Authenticity of transactions (Ellitpic Curve Digital Signature Alg.)
- Privacy of transactions (Pseudonymity through crypto tools)
- Identity of participants (Cryptographic signatures)
- Auditability and Transparency (Cryptographic hash chain)

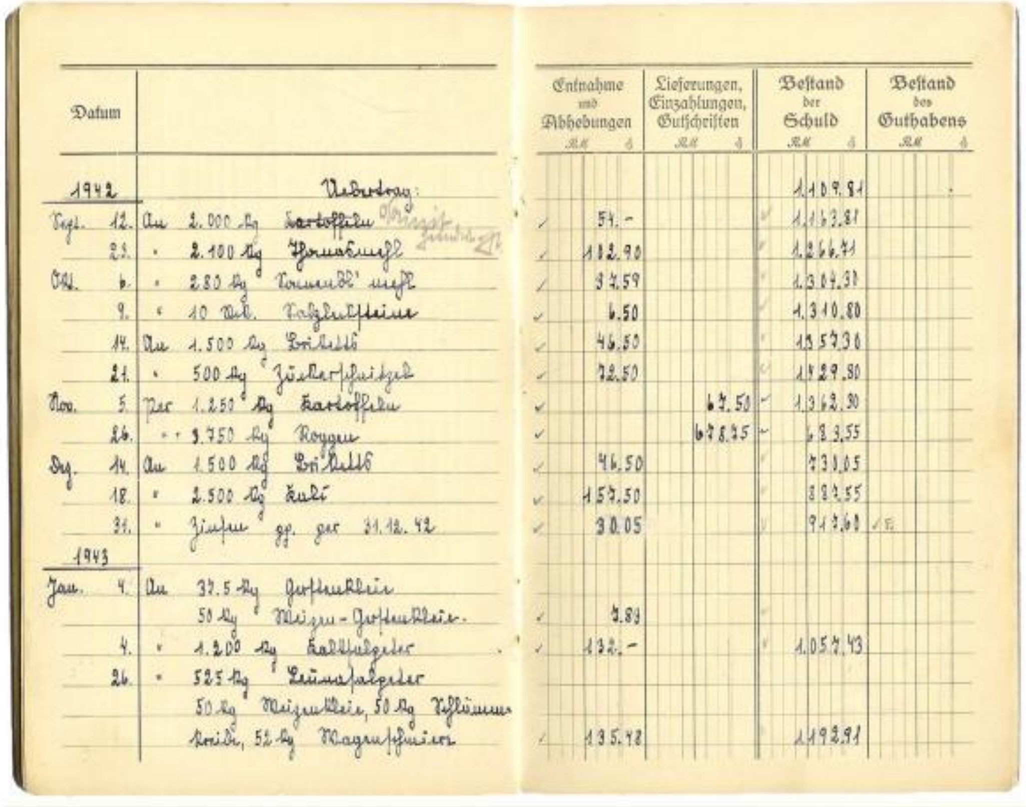
Exploit advanced cryptographic techniques, trust in Blockchain is shifted to Technology (not in participants or nodes)

Connected markets

- Networks connect participants
  - Customers, suppliers, banks, consumers
- Markets organize trades
  - Public and private markets
- Wealth generated by flow of assets and services among participants
  - Physical (house, car …) and virtual assets (bond, patent …)
  - Services
- Transactions exchange assets



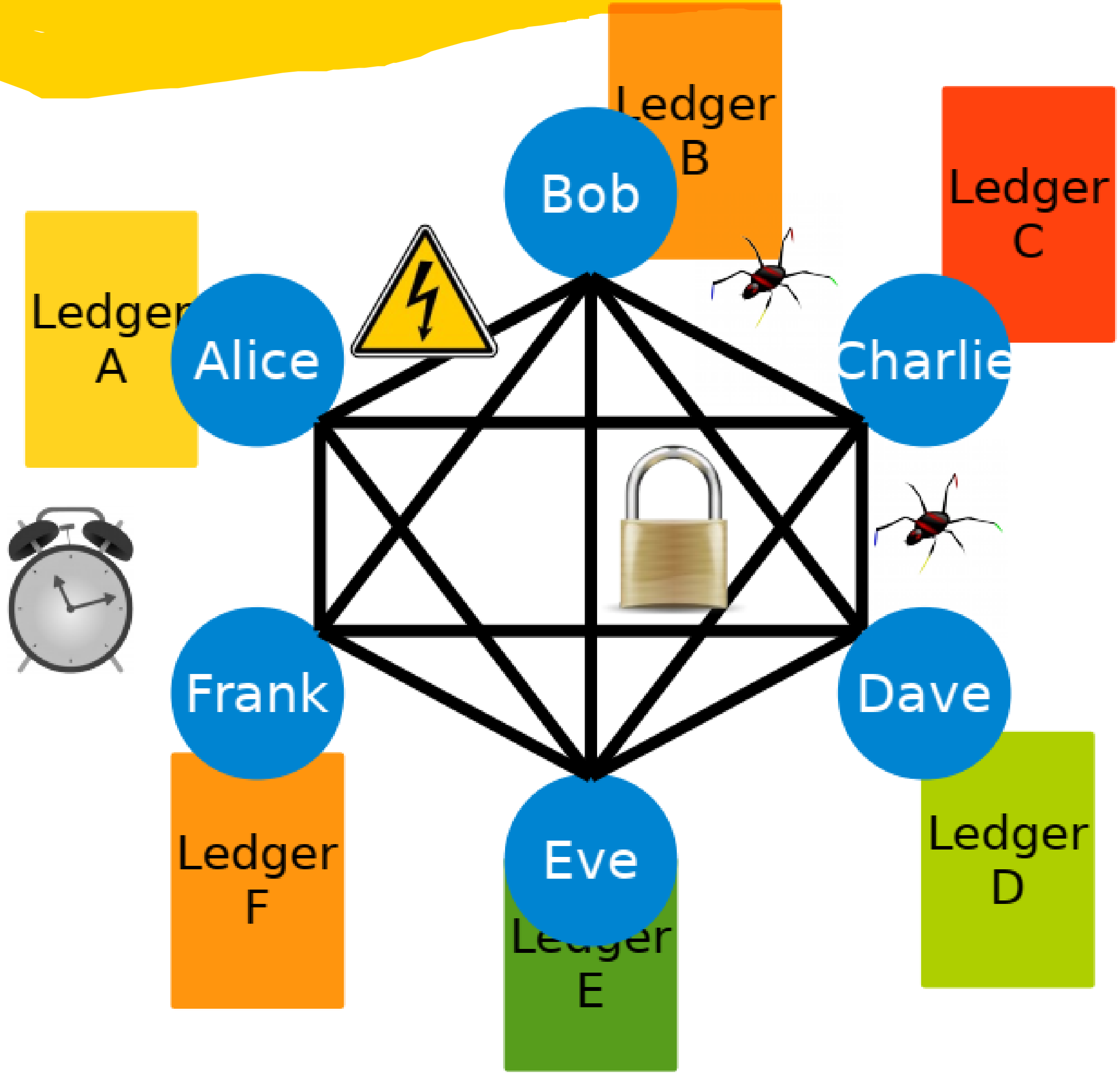
Ledger



Datum			Entnahme und Abhebungen RM ₰	Lieferungen, Einzahlungen, Gutſchriften RM ₰	Beſtand der Schuld RM ₰	Beſtand des Guthabens RM ₰
1942		Uebertrag:			1.109.81	
Sept.	12.	An 2.000 kg Kartoffeln	54.–		1.163.81	
	23.	" 2.100 kg Thomasmehl	102.90		1.266.71	
Okt.	6.	" 280 kg [illegible] mehl	37.59		1.304.30	
	9.	" 10 Stk. Salzlecksteine	6.50		1.310.80	
	14.	An 1.500 kg Briketts	46.50		1.357.30	
	21.	" 500 kg Zuckerschnitzel	72.50		1.429.80	
Nov.	5.	Per 1.250 kg Kartoffeln		67.50	1.362.30	
	26.	" " 3.750 kg Roggen		678.75	683.55	
Dez.	14.	An 1.500 kg Briketts	46.50		730.05	
	18.	" 2.500 kg Kali	157.50		887.55	
	31.	" Zinsen gg. per 31.12.42	30.05		917.60	✓F.
1943						
Jan.	4.	An 37.5 kg Gerstenkleie 50 kg Weizen-Gerstenkleie.	7.83			
	4.	" 1.200 kg Kalksalpeter	132.–		1.057.43	
	26.	" 525 kg Leunasalpeter 50 kg Weizenkleie, 50 kg Schlämmkreide, 52 kg Magerschrot	135.48		1.192.91	

- Ledger records all business activity as transactions
  - Databases
- Every market and network defines a ledger
- Ledger records asset transfers between participants
- Problem — (Too) many ledgers
  - Every market has its ledger
  - Every organization has its own ledger

Multiple ledgers



- Every party keeps its own ledger and state
- Problems, incidents, faults
- Diverging ledgers

Four elements characterize Blockchain

Replicated ledger

- History of all transactions
- Append-only with immutable past
- Distributed and replicated

Cryptography

- Integrity of ledger
- Authenticity of transactions
- Privacy of transactions
- Identity of participants

Consensus

- Decentralized protocol
- Shared control tolerating disruption
- Transactions validated

Business logic

- Logic embedded in the ledger
- Executed together with transactions
- From simple "coins" to self-enforcing "smart contracts"

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

Blockchain scenario features

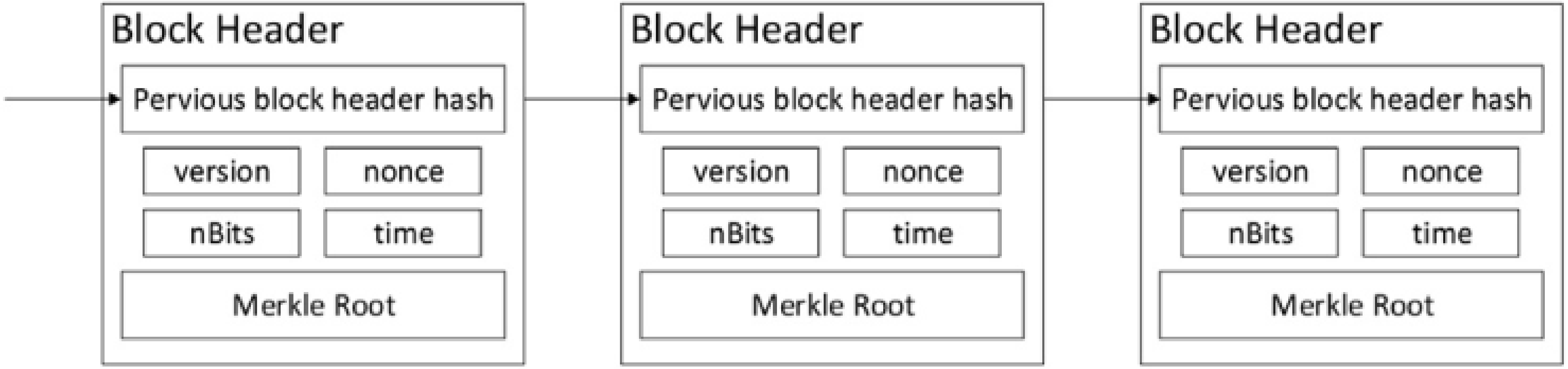
- A given task or problem, but no (central) trusted party available
- Protocol among multiple nodes, solving a distributed task
  - The writing nodes decide and reach consensus collectively
- Key aspects of the distributed task
  - Stores data
  - Multiple nodes write
  - Not all writing nodes are trusted
  - Operations are (somewhat) verifiable
- If all writing nodes are known → permissioned or consortium blockchain
- Otherwise, when writing nodes are not known → permissionless or public blockchain

Blockchain Primer

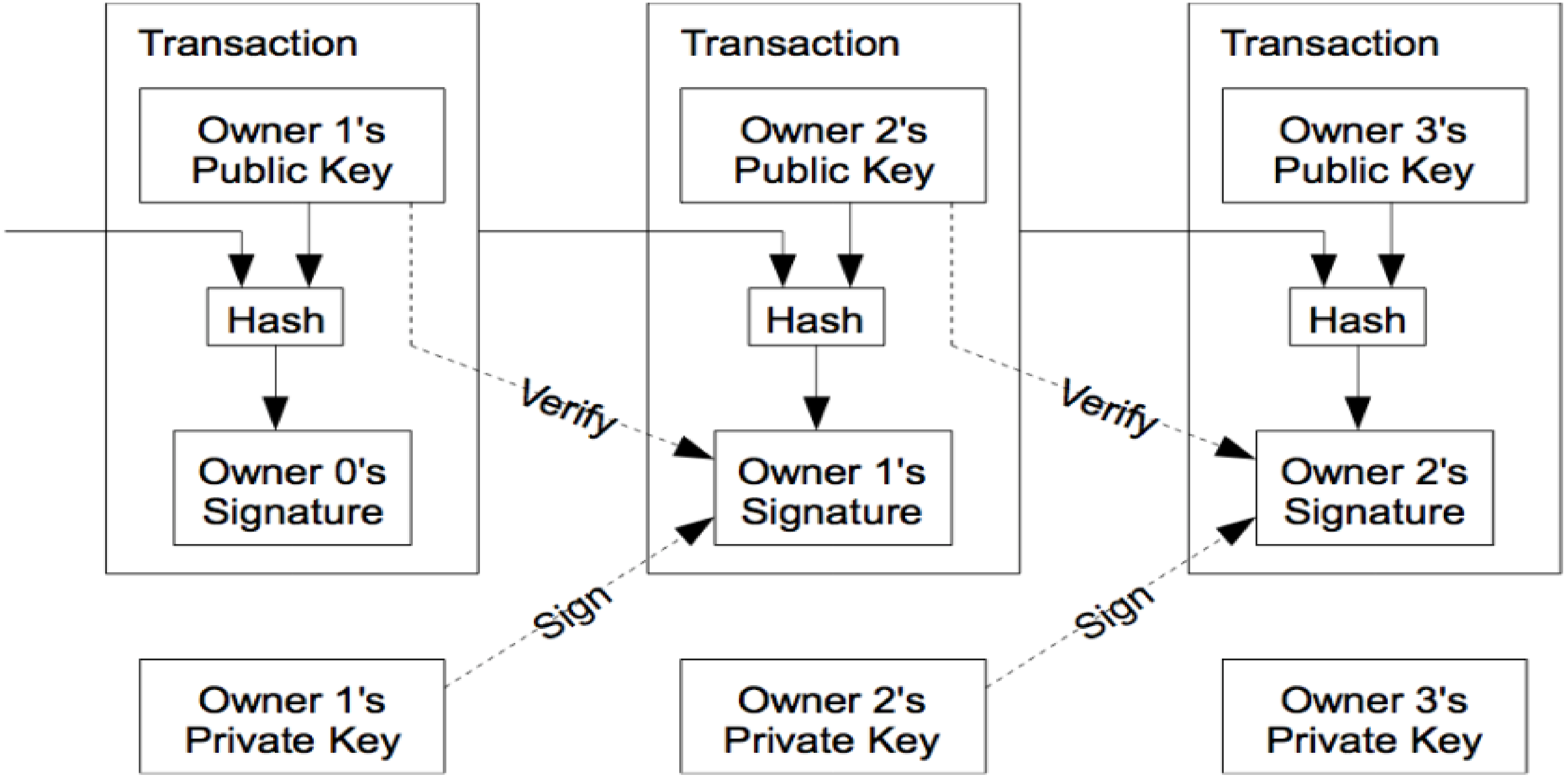
Public Distributed Verifiable Cryptographic Leger

- Public
  - All participants gain access to "read"
- Distributed
  - Peer-to-Peer Data Communication, Fully Decentralized
- Cryptographic
  - Digitally signed transactions, proof-of-work limits rate of input
- Ledger
  - Verifiable Transactional Database

Data Structure of Blocks

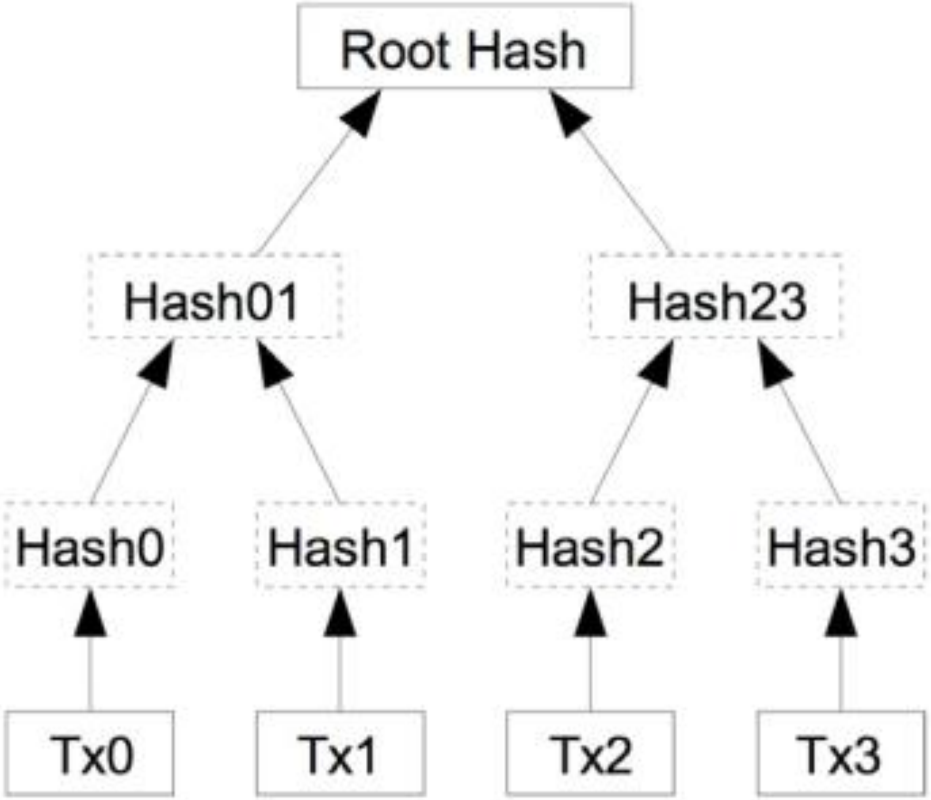


The data structure of the Bitcoin Blockchains

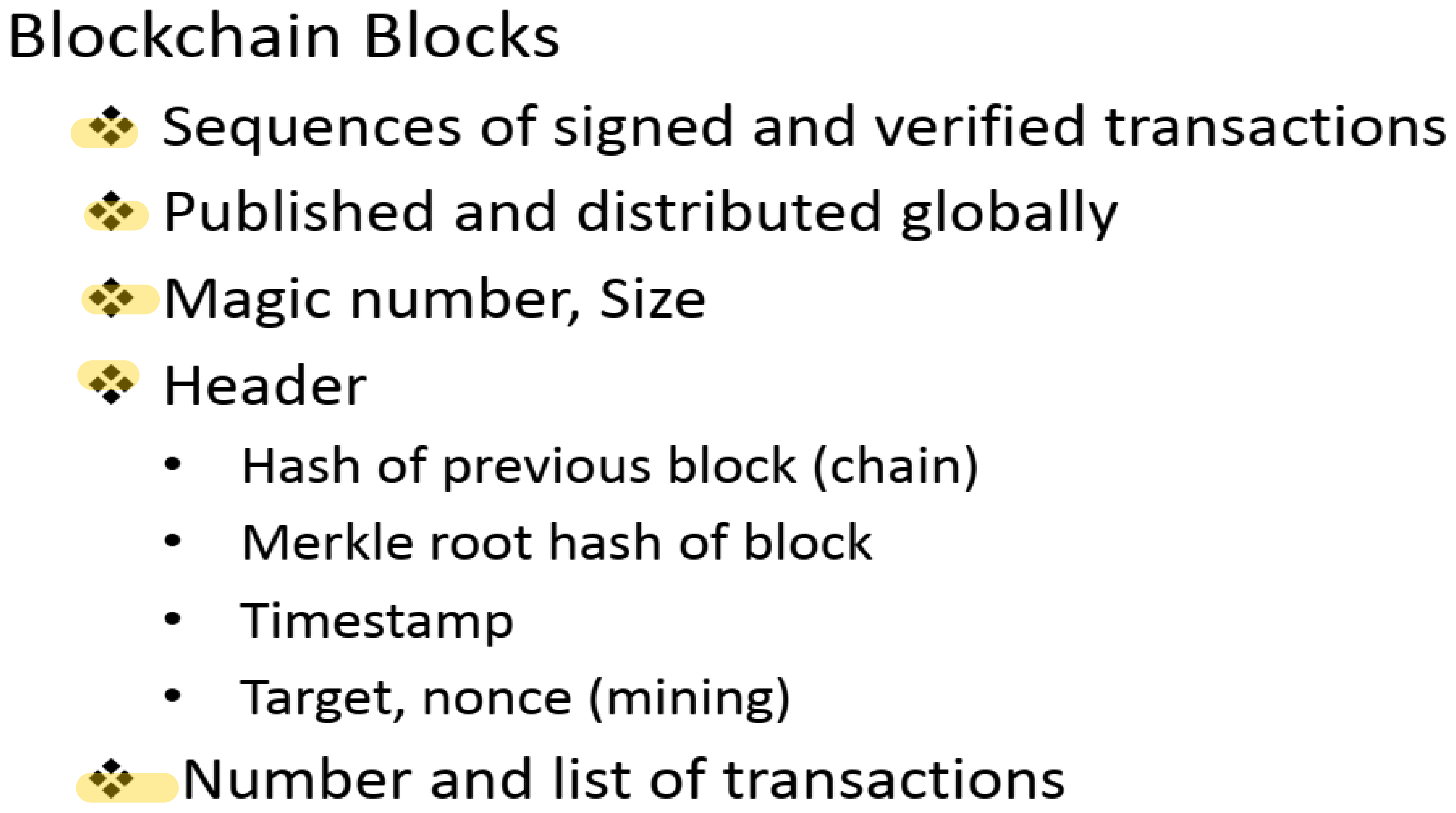


Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto

Transactions are hashed in a Merkle Tree



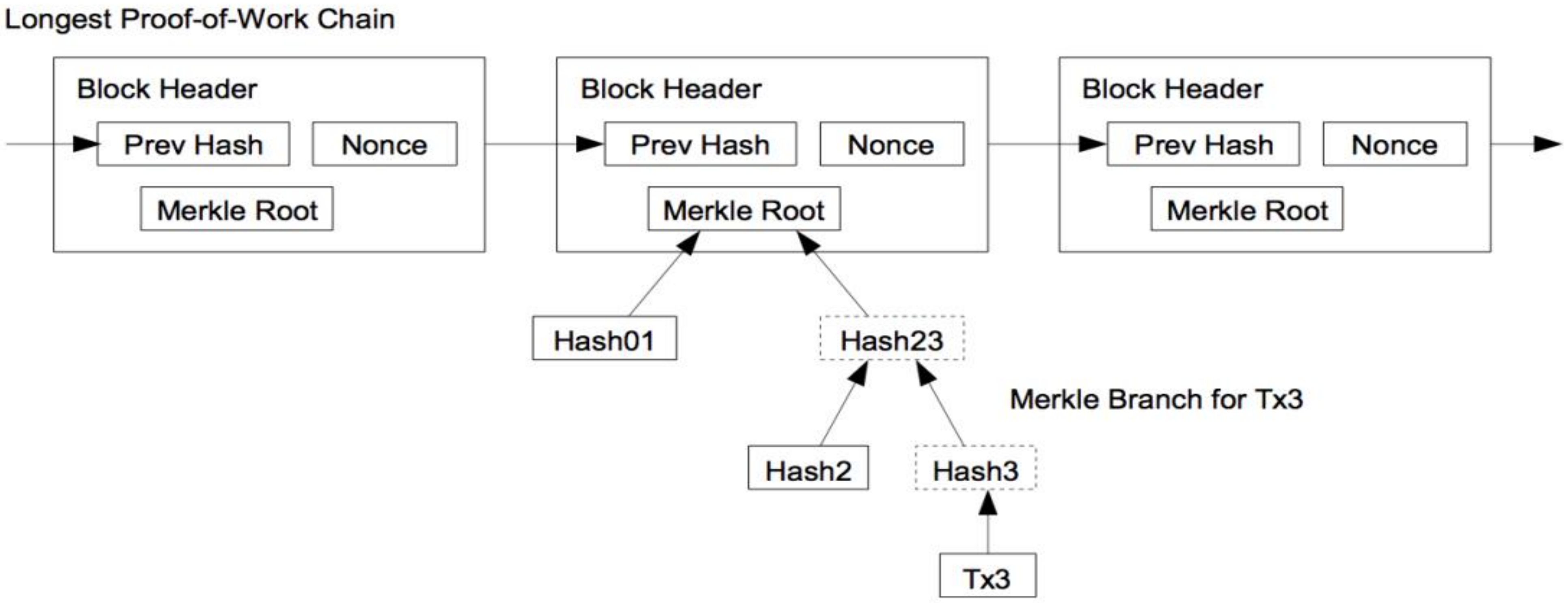
Blockchain Blocks



Blockchain Blocks

- Sequences of signed and verified transactions
- Published and distributed globally
- Magic number, Size
- Header
  - Hash of previous block (chain)
  - Merkle root hash of block
  - Timestamp
  - Target, nonce (mining)
- Number and list of transactions

Longest Proof of Work Chain



Is Blockchain Directly Applicable in IoT?

Desirable Properties

- Distributed protocol with verifiable transaction history
- Dynamic membership multi-party signatures

Undesirable Properties

- Requires proof of “work”
- Requires PKI
- Size of the Ledger an issue for “small” devices
- Anonymous (unverifiable) Join/Leave operations

What can we do?

Eliminate undesirable properties

- ~~Requires proof of "work"~~

  Requires proof of earlier participation using history

- ~~Requires PKI~~

  Hash-based signatures (or other Merkle-tree schemes)

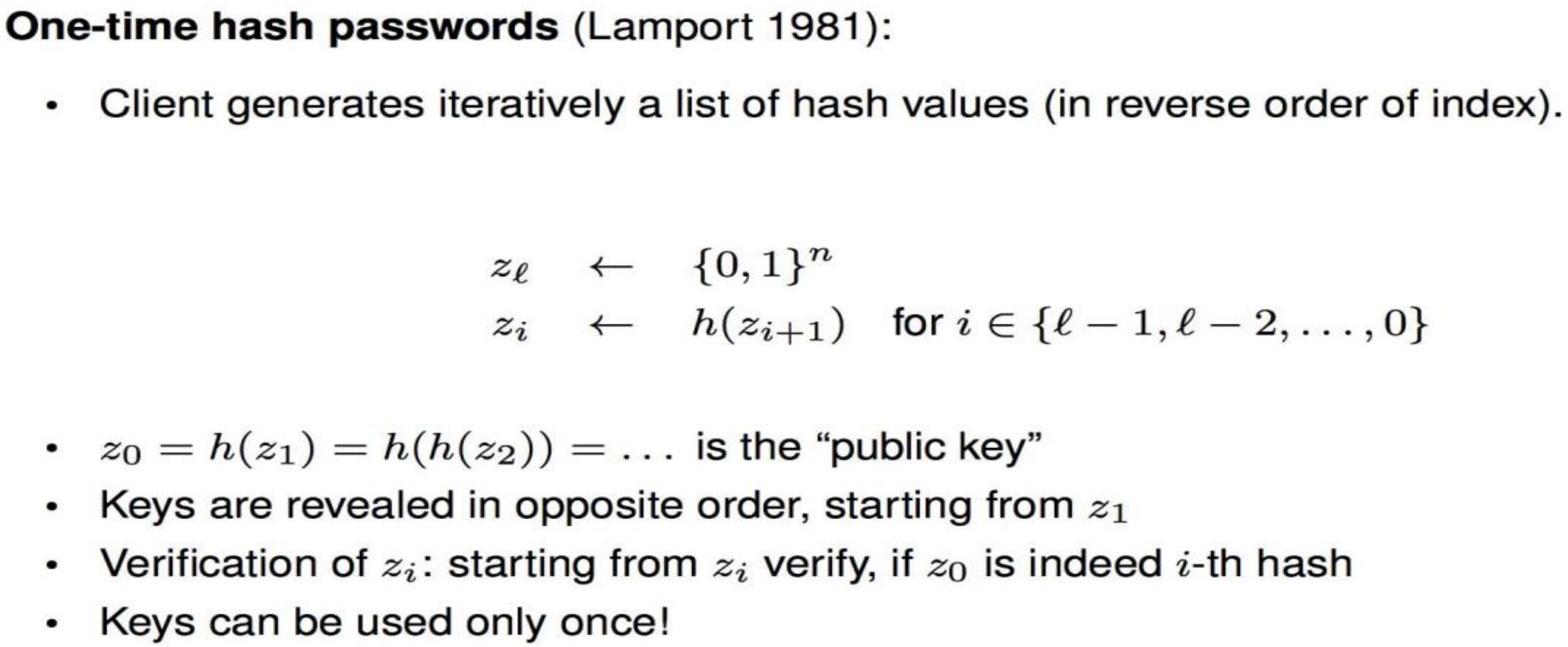
- ~~Size of the Ledger an issue for "small" devices~~

  Prune and Compress Ledger. Maintain only device-relevant transaction ledger when device is too resource constrained

- ~~Anonymous (unverifiable) Join/Leave operations~~

  Group signatures using pre-shared group Key(s)

Hash-Chain



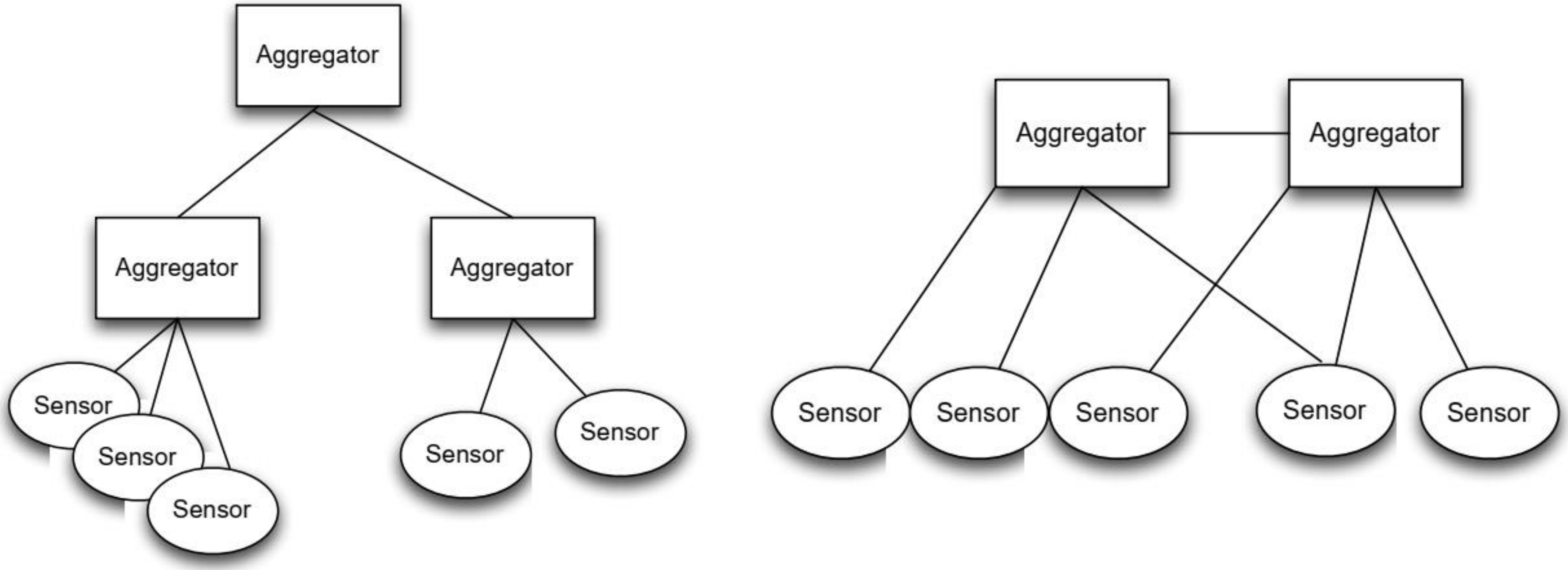
One-time hash passwords (Lamport 1981):

- Client generates iteratively a list of hash values (in reverse order of index).

$$\begin{aligned} z_\ell &\leftarrow \{0,1\}^n \\ z_i &\leftarrow h(z_{i+1}) \quad \text{for } i \in \{\ell-1, \ell-2, \ldots, 0\} \end{aligned}$$

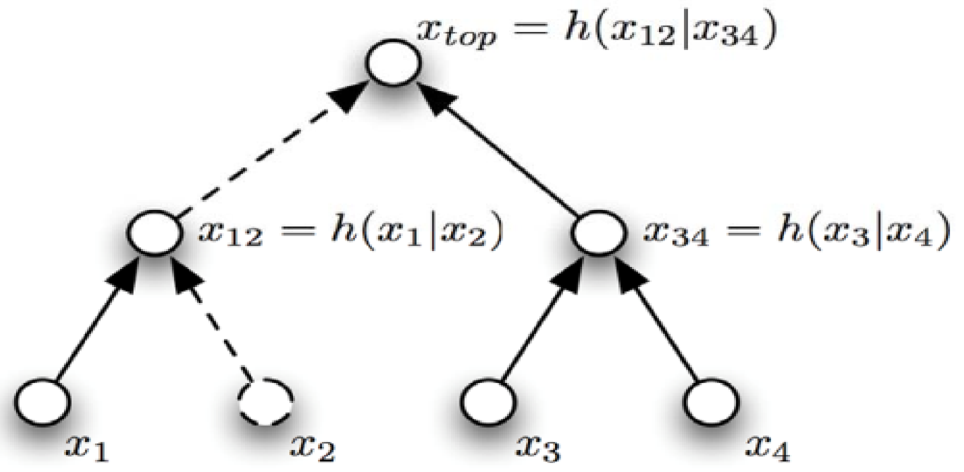
- $z_0 = h(z_1) = h(h(z_2)) = \ldots$ is the “public key”
- Keys are revealed in opposite order, starting from z_1
- Verification of z_i: starting from z_i verify, if z_0 is indeed i-th hash
- Keys can be used only once!

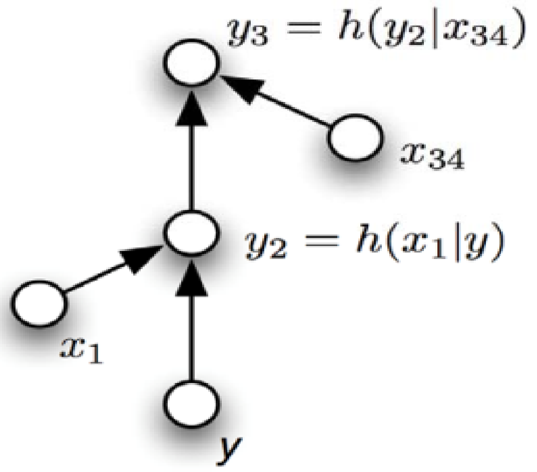
Typical IoT Aggregation Networks



Blockchain-based Protocol for IoT?

We suggest a Blockchain-based protocol that uses the following blocks:



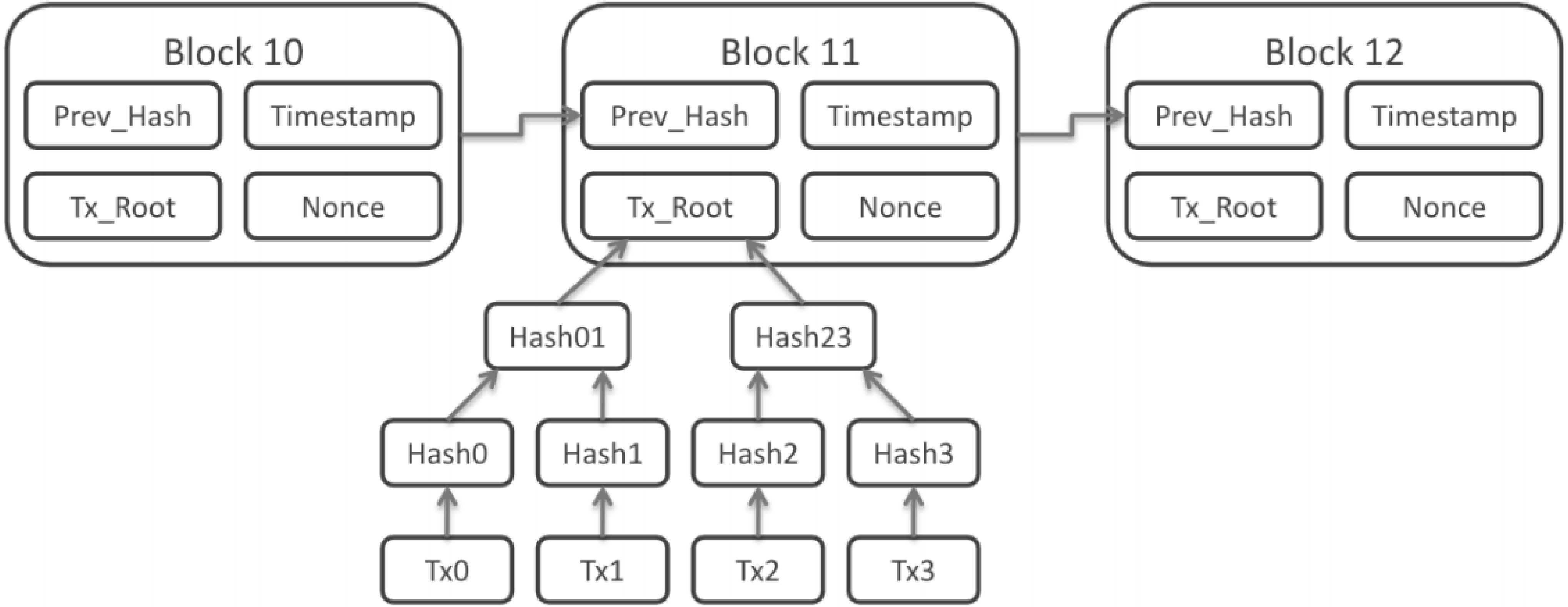


$$x_i = H(Data \,||\, K_G \,||\, H(z_i)^n), H(z_i)^{n-1}$$

$$H = Hash, K_G = group\ Key, z_i = sensor\ i\ "public\ \ key"$$

Blockchain-based Protocol for IoT?

We suggest a Blockchain-based protocol that uses the following blocks:



Thank you!