Foundations of Blockchain Technology

ECOM215

Dr. Daniele Bianchi[1]

[1]School of Economics and Finance
Queen Mary, University of London

Summary

In this lecture, we introduce the basic principles of Blockchain technology and discuss its fundamental properties. We place particular emphasis on differentiating alternative types of blockchains (Public, Private, and Consortium). Finally, we introduce one of the core ingredients of blockchain technology: Cryptography.

Contents

Definition and core concepts

What is Blockchain?

Blockchain is an emerging technology that combines:

(i) Cryptography.

(ii) Data management.

(iii) Distributed computing (network).

(iv) Economic incentives.

To support the checking, executing, and recording transactions between parties based on a distributed digital ledger.

Simply put, a Blockchain ledger is a list ("chain") of (groups of) transactions ("blocks") that are securely recorded via cryptographic tools.

What is Blockchain?

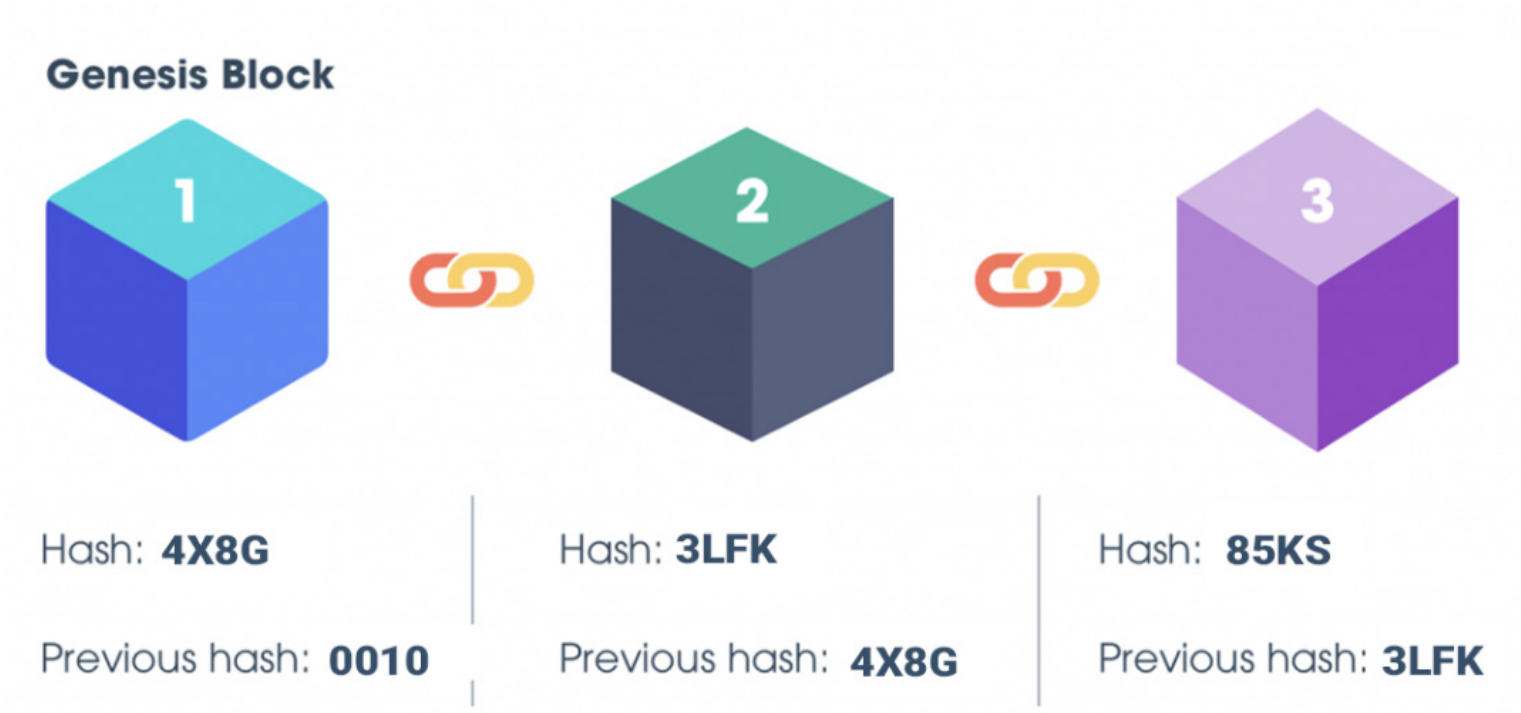


Figure: A simplified representation of a blockchain where cryptographic tools link blocks of transactions. More on cryptography later in the slides.

What is Blockchain?

Blockchain is a cleverly designed bookkeeping system:

- ↪ Parties proposing a transaction add it to a block to be recorded.
- ↪ Participants in the network ("nodes") check the integrity of the transaction and record it in new blocks on the ledger.
- ↪ The content of the updated ledger is distributed among all participants in the network.

N.B., The processing nodes can maintain the update and the integrity of the ledger without the central control of any trusted third party.

- ↪ Consensus among nodes is guaranteed by an incentive mechanism.

What is Blockchain?

The successful operation of a blockchain system relies on several key elements, including:

- ↪ A mechanism to ensure the integrity of transactions.
- ↪ Cryptographic tools to identify parties and check their authority.
- ↪ A solid governance protocol to manage network interactions.
- ↪ Economic incentives to motivate processing nodes and behave trustworthy and transparently.

Just like a traditional database, a blockchain can be used to represent transactions in any kind of application domain. However, blockchains are different from conventional databases in essential ways.

Why should we care?

Transactions between parties, such as payments, voting, and coordination, are critical aspects of the relationship among private entities and between private entities and the government.

Traditionally, trusted third parties ("intermediaries") support these transactions, such as banks, legal firms, and government agencies.

Blockchain provides a different perspective on the relationship between different entities.

↪ Instead of trusting intermediaries, we trust the collective network operating the blockchain and the transparency of the technology.

Defining Blockchain

We must first define the main concepts and terminology at the core of Blockchain technology.

Distributed Ledger: A distributed ledger is an "append-only" store of transactions distributed across many network nodes.

The key term is "append-only" $\Longrightarrow$ new transactions can be added, but old transactions cannot be deleted or modified.

This guarantees one of Blockchain's fundamental properties: the ledger's retrospective **immutability**.

$\hookrightarrow$ A new transaction might reverse a previous transaction, but both remain part of the ledger.

$\hookrightarrow$ This ultimately provides transparency.

Defining Blockchain

Block: A list of transactions recorded into a ledger over a given period. The block size, period, and triggering event differ across blockchains.

Think about a block as a page of a conventional ledger. Instead of updating one transaction at a time, transactions are updated in batches.

↪ The network needs to find a consensus on which batch should be appended first.

↪ Transactions are still checked individually within each block.

Defining Blockchain

A typical solution to secure the link from one new block to its predecessor is to use cryptographic hashes.

> **Hash function:** A mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash).

It is designed to be a one-way function, effectively impossible to invert. This ensures data integrity, authentication, and digital signatures.

Cryptographic hashes ensure that a previous block cannot be changed.

↪ If the previous block was changed, its new hash would not match the originally recorded hash so that the block link would break.

Defining Blockchain

A distributed ledger is at the core of a much broader system, which includes:

(i) A distributed **network** of computers (nodes) that guarantee the integrity of the ledger.

(ii) A **data structure** that is replicated across the network. Nodes with a full replica of the ledger are called **full nodes**.

(iii) A **protocol** that disciplines the network governance. This includes rights, responsibilities, transaction verification and validation, consensus mechanisms, etc.

Before discussing blockchain's fundamental properties, we must introduce some basic notions of cryptography.

A bird's-eye view on cryptography

A bird's-eye view on cryptography

Cryptography protects information from unauthorized access $\Longrightarrow$ only the individuals for whom the transaction data is intended can access, read, and process the transaction data.

Blockchain security is built upon two key concepts:

- ↪ **Cryptography**: encrypts messages in the peer-to-peer network.
- ↪ **Hashing**: assists in securing block information and linking blocks in the blockchain

Data are secured by transforming it into a format that is unintelligible to unauthorized individuals.

- ↪ Such transformation is achieved through mathematical algorithms and a combination of public and private keys.

A bird's-eye view on cryptography

Main features of a cryptographic structure:

- ↪ Only the intended recipient can access the information.
- ↪ Information cannot be modified while being stored or transmitted between a sender and a recipient without the recipient being notified.
- ↪ The creator/sender of information cannot revoke his intention to send data.
- ↪ The identities of the sender and recipient, as well as the origin and destination of the information, are verified by the network.

Cryptography in Blockchain

Cryptography forms the backbone of blockchain technology, ensuring the immutability, security, and trustworthiness of the data stored within the blockchain.

Key cryptographic components within the blockchain ecosystem are hash functions, digital signatures, and encryption.

A Hash function takes an input of any size and produces a fixed-length string of characters, known as the hash.

↪ One-way functions, meaning it is computationally infeasible to derive the original input from the generated hash.

Hash function

Hash functions are cryptographic tools that take an input (often called a message or data) and produce a fixed-length string of characters, typically a hexadecimal number. Common hash functions include SHA-256 (used in Bitcoin).

Hash function

```python
import hashlib

# Function to generate SHA-256 hash
def generate_sha256_hash(input_string):
    # Encode the input string to bytes
    input_bytes = input_string.encode()

    # Create a new SHA-256 hash object
    sha256_hash = hashlib.sha256()

    # Update the hash object with the bytes-like object
    sha256_hash.update(input_bytes)

    # Get the hexadecimal representation of the digest
    hex_digest = sha256_hash.hexdigest()

    return hex_digest

# Example usage
input_string = "Hello, World!"
hash_result = generate_sha256_hash(input_string)

print(f"Input String: {input_string}")
print(f"SHA-256 Hash: {hash_result}")

# Expected Output:
# Input String: Hello, World!
# SHA-256 Hash: a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b8f34d043cce1b8b9
```

Figure: A simple example of a Hash function in Python using the `hashlib` library.

Hash function

Main properties of a hash function:

(a) *Deterministic:* The same input produces the same hash value.

(b) *Fixed length:* The output (hash) is always of a fixed length, regardless of the input's length.

(c) *Pre-image resistance:* It should be computationally infeasible to reverse the hash to find the original input (pre-image).

(d) *Collision resistance:* It should be extremely unlikely for two different inputs to produce the same hash value (collision).

(e) *Avalanche effect:* A tiny change in the input should result in a significantly different hash value.

Encryption

Encryption: Encryption plays a crucial role in securing sensitive data within the blockchain.

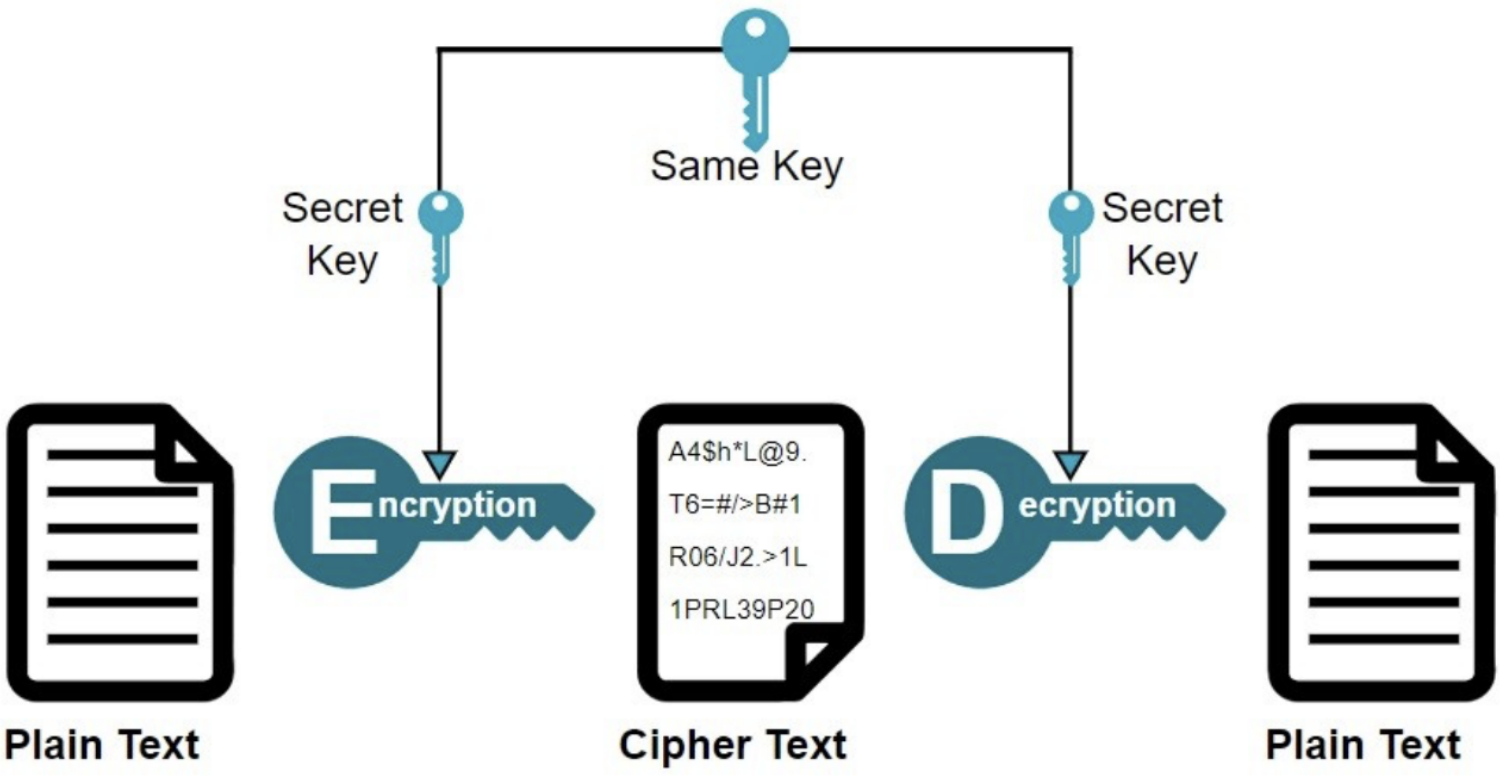
We can differentiate between symmetric and asymmetric encryption:

- ↪ Symmetric encryption uses a single shared key for encryption and decryption.
- ↪ Asymmetric encryption uses a pair of mathematically related keys, namely the public and private.

Asymmetric encryption is commonly used for key distribution, ensuring confidentiality within the blockchain network.

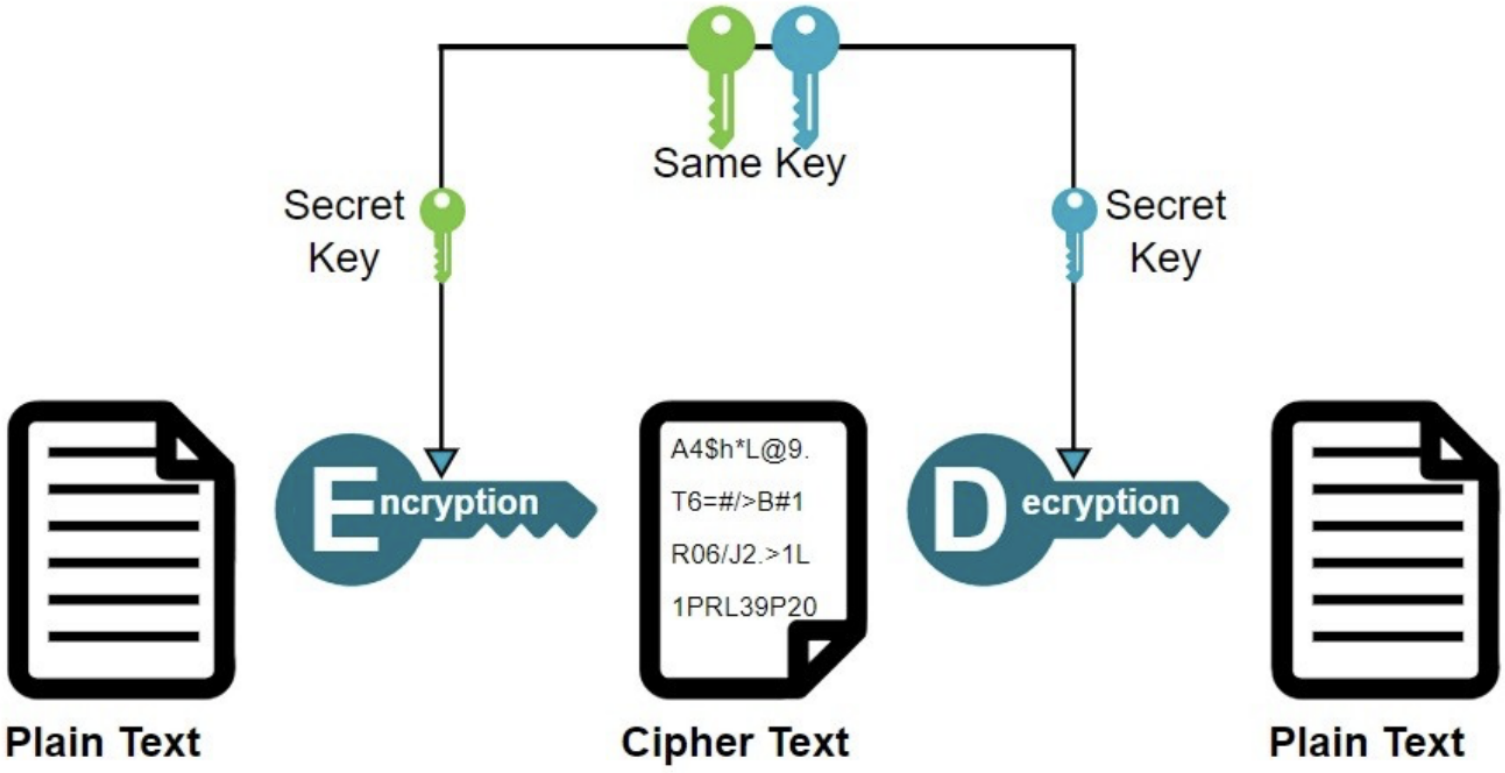
Symmetric Encryption

It is an encryption system where the sender and receiver of a message use a single common key to encrypt and decrypt messages.



Asymmetric Encryption

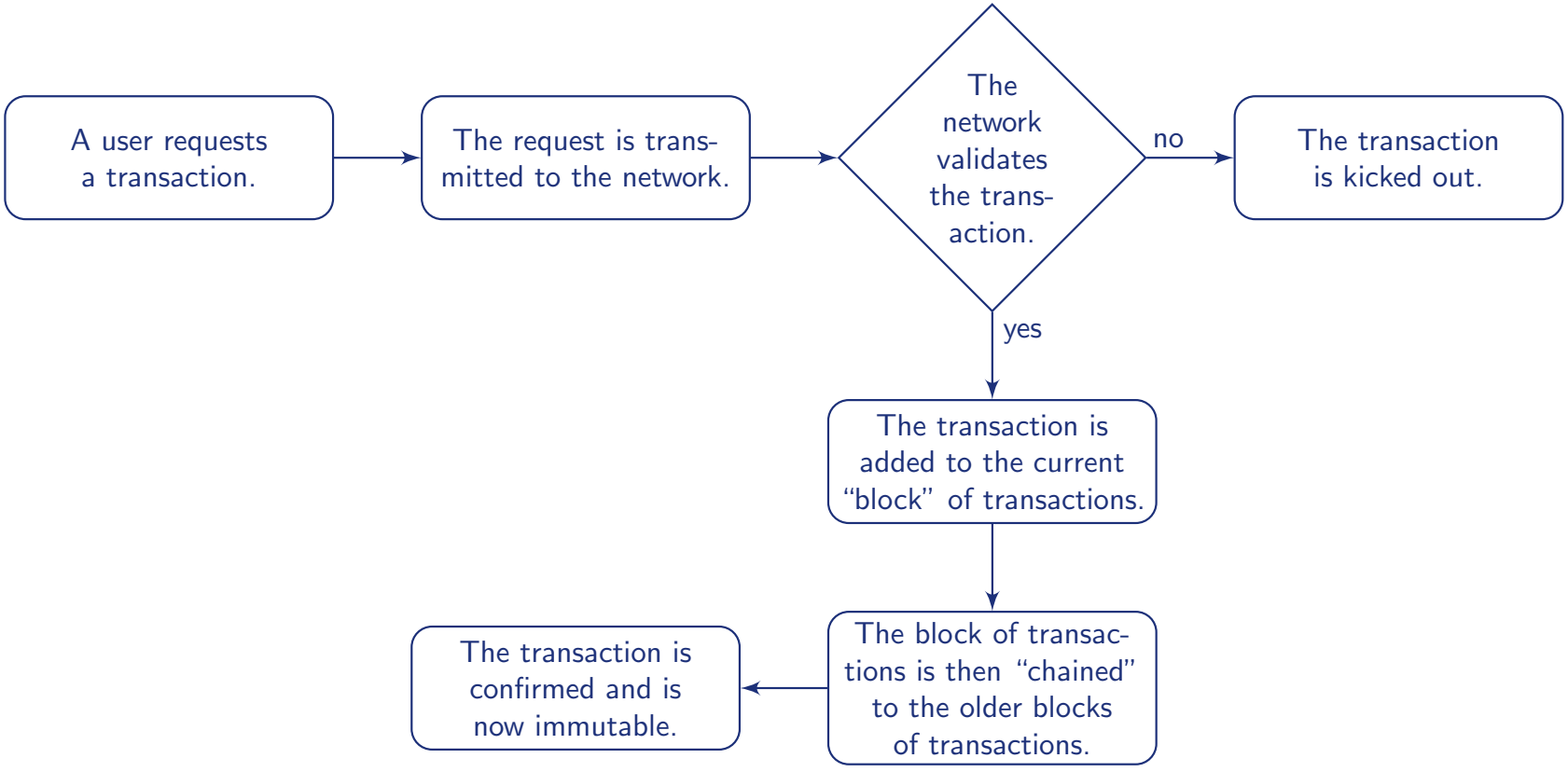
Public keys and private keys are different. Even if everyone knows the public key, the intended receiver can only decode it because he knows his private key.



Fundamental properties of Blockchain

Fundamental properties of Blockchain

A recap of how transactions work in a Blockchain...



Fundamental properties of Blockchain

The fundamental properties of a functioning Blockchain are:

(1) **Immutability:** Once a transaction is recorded and confirmed on the blockchain, it becomes very difficult to alter. Immutability is guaranteed by the hash function linking blocks together, where each block contains a previous block hash.

(2) **Irreversibility:** Blockchain transactions cannot be reversed after they have been confirmed. This feature is critical for preventing fraud and double-spending.

(3) **Integrity:** Transactions must be agreed upon before they are recorded. Once processed, a transaction is encrypted and linked to the previous one, contributing to a tamper-resistant ledger.

Fundamental properties of Blockchain

(4) **Transparency:** Transactions are visible to all participants and are immutable once confirmed. This transparency can build trust among users and helps ensure data integrity.

(5) **Decentralization:** Unlike traditional databases, blockchain distributes data to a dispersed network of computers. A central authority is unnecessary, potentially increasing resistance to malicious attacks.

Different blockchains satisfy these properties to different extents, balancing scalability, security, and decentralization needs according to their intended use case.

↪ N.B. Balancing different aspects, e.g., scalability vs security, is far from easy. More on this later in the course.

Existing Blockchain platforms

Existing Blockchain platforms

The properties described so far are relatively broad and can encapsulate different Blockchains based on their openness, governance systems, and consensus protocols.

To a first approximation, we can distinguish between:

- ↪ Public Blockchains (e.g., Bitcoin and Ethereum).
- ↪ Private Blockchains (e.g., Hyperledger, R3's Corda, Ripple).
- ↪ Consortium Blockchains (e.g., Energy Web Chain).

Each type has pros and cons, depending on the intended use case.

Public Blockchain

A **public blockchain** has an entirely open network where nodes can join and leave without requiring permission from anyone, i.e., permissionless.

Records are transparent, and participants can verify and audit transactions independently.

↪ Full network nodes can verify each new piece of data in the ledger, including blocks and transactions.

A consensus protocol is used to ensure the integrity of the ledger.

↪ Common examples are Proof-of-Work (PoW) and Proof-of-Stake (PoS). More on this later in the course.

Public Blockchain

Advantages:

- ↪ **Decentralization**: No single entity controls the entire network, which can reduce the risk of censorship or control by a single party.
- ↪ **Security**: Highly secure due to their large number of nodes, making it difficult to attack or manipulate.
- ↪ **Trustless**: Users do not need to trust each other as the consensus protocol ensures the community safeguards the ledger integrity collectively.

Disadvantages:

- ↪ **Scalability**: Public blockchains often face scalability issues due to the nature of the consensus protocols.
- ↪ **Performance**: Transactions confirmation can be energy intensive.

Private Blockchain

A **private blockchain** is a closed network where a single organization or entity restricts access to outside participants.

A Blockchain often used within an organization where only certain people are allowed to participate.

The consensus mechanism can be centralized as it does not require trust among parties.

↪ Often supports fewer processing nodes than public blockchain.

Private Blockchain

Advantages:

- ↪ **Control**: A single entity controls blockchain governance and can restrict who can participate and view the blockchain.
- ↪ **Scalability**: Higher transaction throughput and faster processing since there are fewer nodes to manage and achieve consensus.

Disadvantages:

- ↪ **Centralization**: Higher risk of data manipulation and points of failure since one entity has exclusive control.
- ↪ **Security**: Less distributed consensus can make the network more susceptible to security breaches.
- ↪ **Limited Immutability**: The governing entity might be able to alter transactions, compromising the principle of immutability.

Consortium Blockchain

A **consortium blockchain** is usually semi-private and operates under the leadership of a group of participants.

Unlike a fully private blockchain, multiple organizations manage the blockchain.

- ↪ Pre-authorized nodes control the consensus process in a consortium blockchain.
- ↪ The right to update and audit the blockchain can be spread between the consortium organisations.

Consortium Blockchain

Advantages:

- ↪ **Efficiency and scale**: They can process more transactions quickly due to fewer nodes.
- ↪ **Transparency**: they can still offer a certain level of transparency among the permitted organizations.

Disadvantages:

- ↪ **Collusion risk**: The governing bodies may collude for their benefit at the expense of the blockchain users.
- ↪ **Complex governance**: The need for a clear governance structure might complicate the operation and maintenance of the blockchain.
- ↪ **Limited public trust**: Since consortium blockchains are not fully open, they may lack the level of trust that a public blockchain offers.

Blockchain use cases

Blockchain-based applications

Blockchain has been first adopted in the context of cryptocurrencies but is now used for many other purposes.

However, blockchain is a foundational horizontal platform technology that can be used in any industrial sector, including agriculture, utilities, manufacturing, retail, transport, education, healthcare, etc.

The technology's potential can help increase efficiency and improve transparency in traditional financial services.

Industrial use cases

Blockchain can provide a trusted registry of transactions or intellectual property and ensure the ability to transfer access and rights information for goods and services securely and transparently.

A key industrial application is **supply chain management**.

↪ When tracking physical assets through changes in ownership and handling, key events and agreements can be recorded and communicated through a blockchain.

↪ Key events could also be linked to automatic payments using smart contracts (more on smart contracts later in the course).

This makes blockchain a convenient technology for tracking the ownership of goods and services.

↪ Access control mechanisms may allow public data sources to be integrated with private analysis services.

Industrial use cases

IBM Food Trust (IFT) network: joiners, builders, and expanders.

31%
Network Joiners

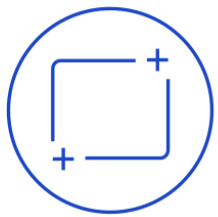
Join blockchain networks to seek efficiency

Example: Walmart joins IFT and brings along food supply chain

18%
Network Builders

Build blockchain networks that offer value beyond efficiency

Example: IBM builds IFT



51%
Network Expanders

Co-create platforms on blockchain networks to grow market size

Example: Farmer Connect offers innovative service on IFT

Source: IBM Institute for Business Value analysis.

Industrial use cases

An increasingly popular application of blockchain technologies is **corporate governance**.

For instance, the voting authorities of board members or company shareholders can be recorded and proxied on a blockchain.

↪ Smart contracts on blockchains can use that record to adjudicate votes conducted on the blockchain for specific motions.

N.B. As blockchain registries are not necessarily hidden, cryptographic mechanisms may be required to prevent potentially undesirable strategic voting behaviours.

Industrial use cases

Santander shareholders voting in 2019. Voting took place by traditional methods, but they used blockchain to produce a shadow register.

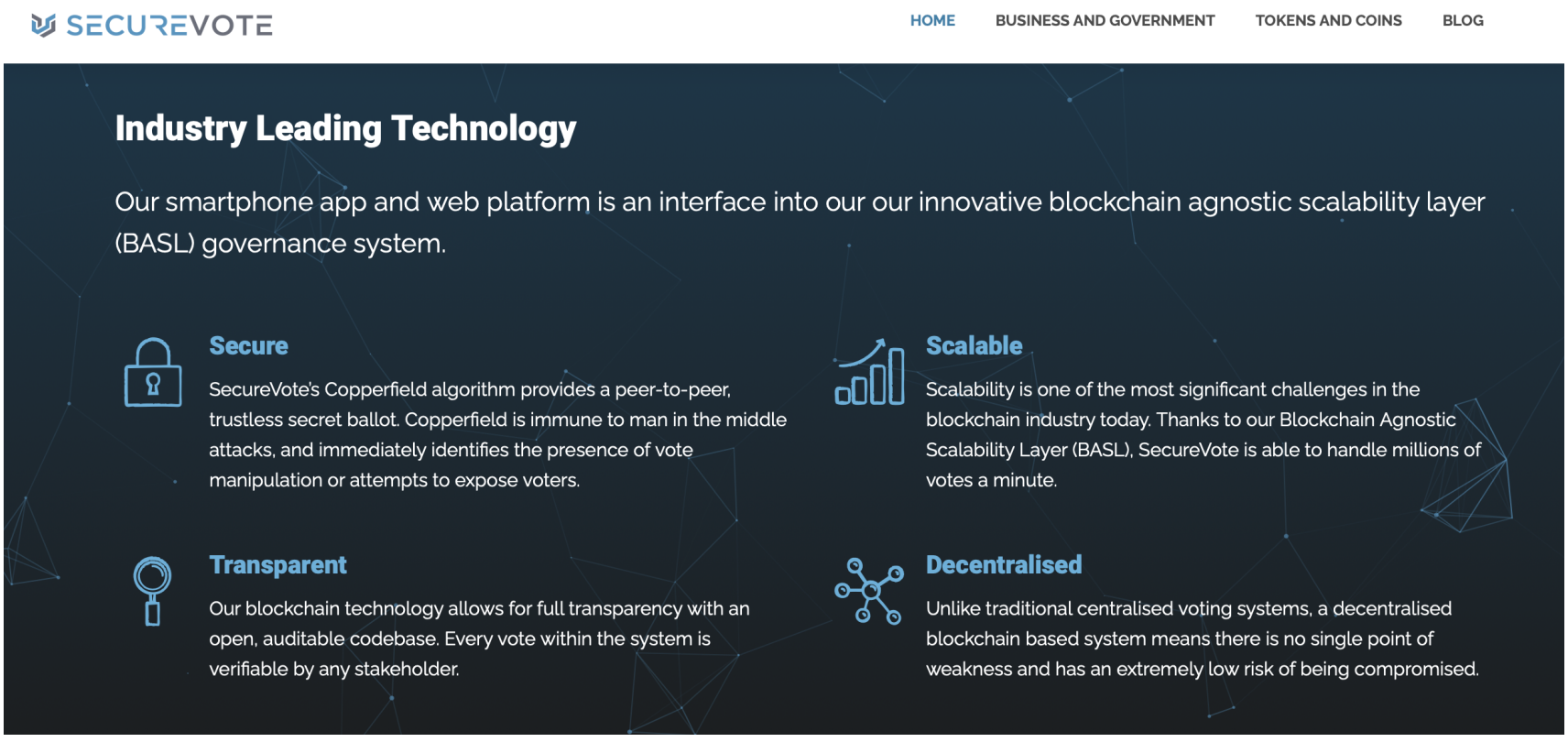
FTfm European companies + Add to myFT

Santander shows potential of blockchain in company votes

Spanish bank points to way to improving annual meetings

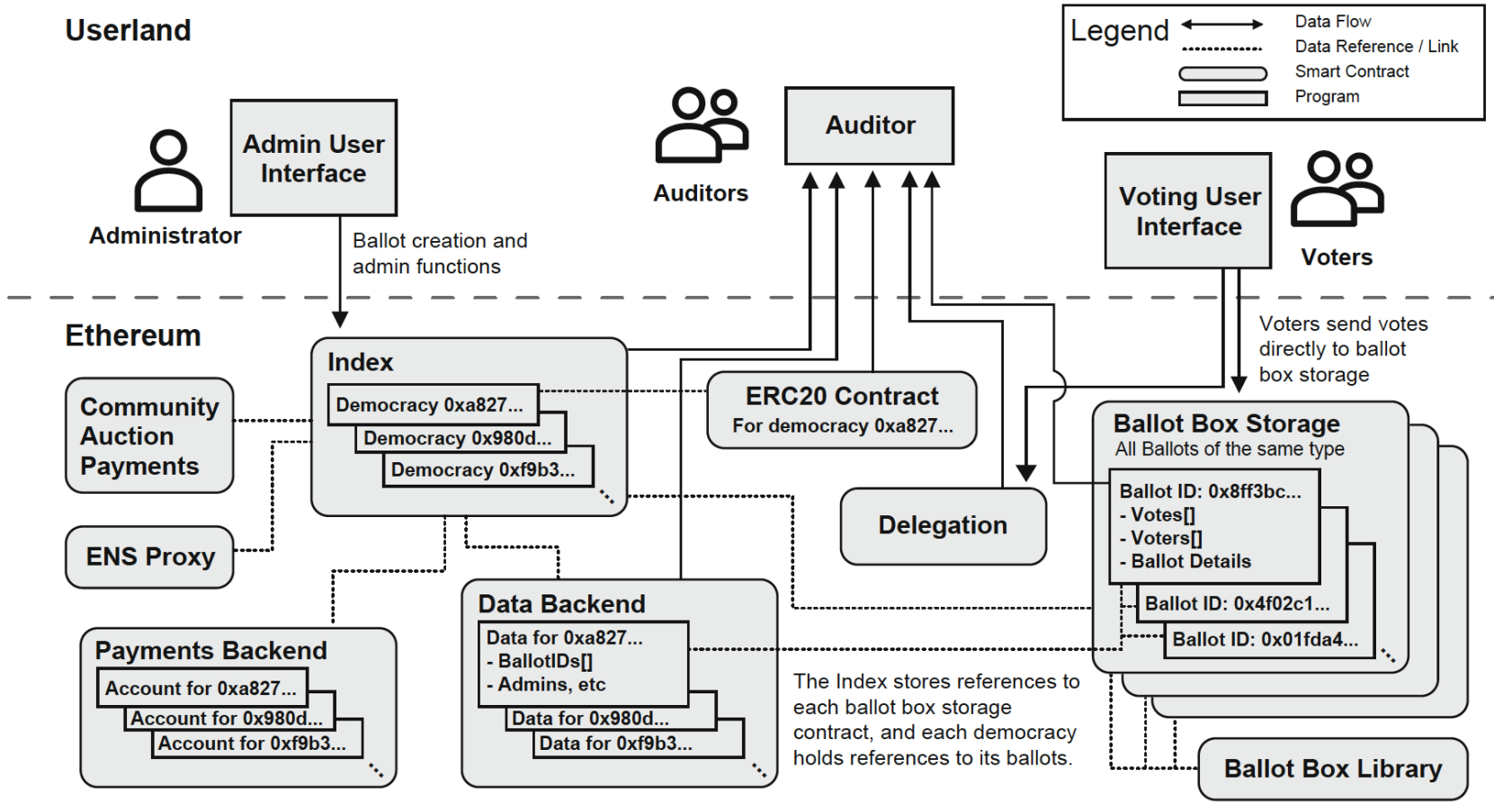
Industrial use cases

A voting system based on blockchain technology: SecureVote



Industrial use cases

The architecture of SecureVote at deployment.



Source: Xu et al. 2019 "Architecture for Blockchain Applications".

Government services

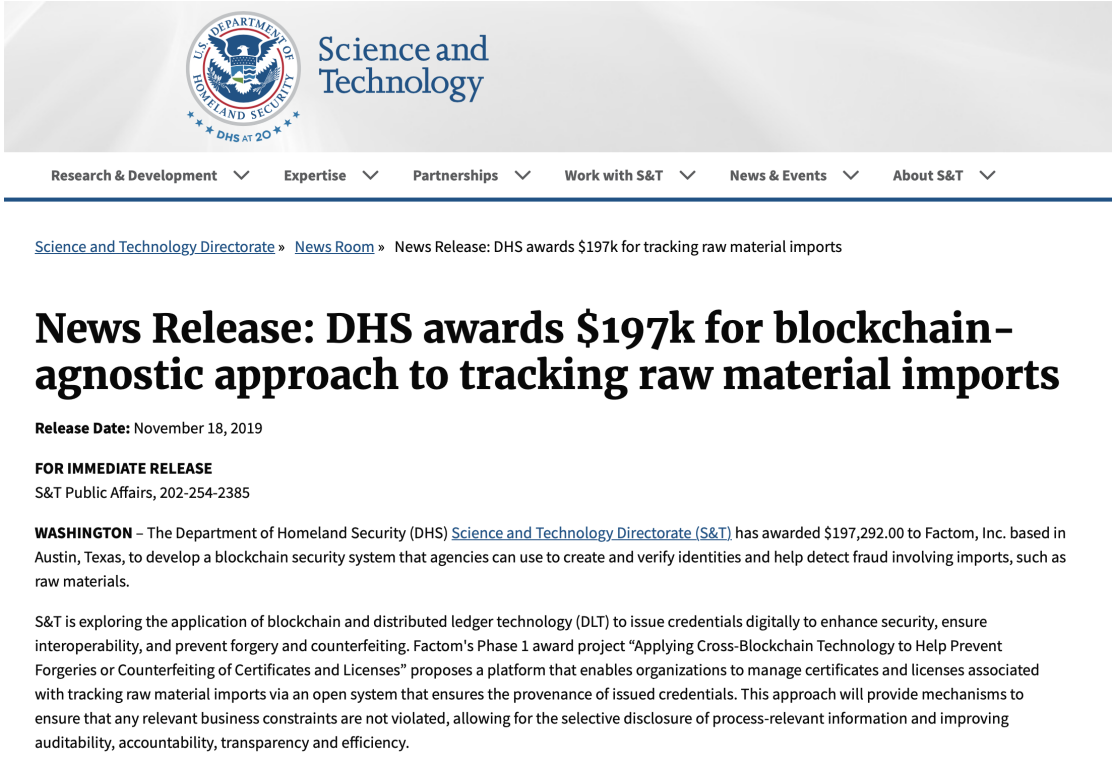
Blockchains could target improved **government service** delivery, and private blockchains could facilitate information sharing and process coordination across agencies within the government.

Application areas being explored in governments globally include:

- ↪ **Grants and social security:** Smart contracts could automate the process coordination to apply for, decide on, and distribute grants and social security payments.
- ↪ **Taxation:** from an automated tax collection using smart contracts to improved compliance.
- ↪ **Registries and identity:** Including border security and travel documentation. Assessing the identities and attributes of persons, companies, or devices, licensing, qualifications, and certifications.
- ↪ **Voting:** Including local and political elections.

Government services

The U.S. Department of Homeland Security has been exploring how to secure Internet-of-Things (IoT) devices used by Customs and Border Protection (CBP) by leveraging blockchain technology.



Science and Technology

Research & Development | Expertise | Partnerships | Work with S&T | News & Events | About S&T

Science and Technology Directorate » News Room » News Release: DHS awards $197k for tracking raw material imports

News Release: DHS awards $197k for blockchain-agnostic approach to tracking raw material imports

Release Date: November 18, 2019

FOR IMMEDIATE RELEASE
S&T Public Affairs, 202-254-2385

WASHINGTON – The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) has awarded $197,292.00 to Factom, Inc. based in Austin, Texas, to develop a blockchain security system that agencies can use to create and verify identities and help detect fraud involving imports, such as raw materials.

S&T is exploring the application of blockchain and distributed ledger technology (DLT) to issue credentials digitally to enhance security, ensure interoperability, and prevent forgery and counterfeiting. Factom's Phase 1 award project "Applying Cross-Blockchain Technology to Help Prevent Forgeries or Counterfeiting of Certificates and Licenses" proposes a platform that enables organizations to manage certificates and licenses associated with tracking raw material imports via an open system that ensures the provenance of issued credentials. This approach will provide mechanisms to ensure that any relevant business constraints are not violated, allowing for the selective disclosure of process-relevant information and improving auditability, accountability, transparency and efficiency.

Source: Department of Homeland Security (DHS), United States.

Government services

There is an increasing issue of trust in political institutions, which can be mitigated by increasing transparency.

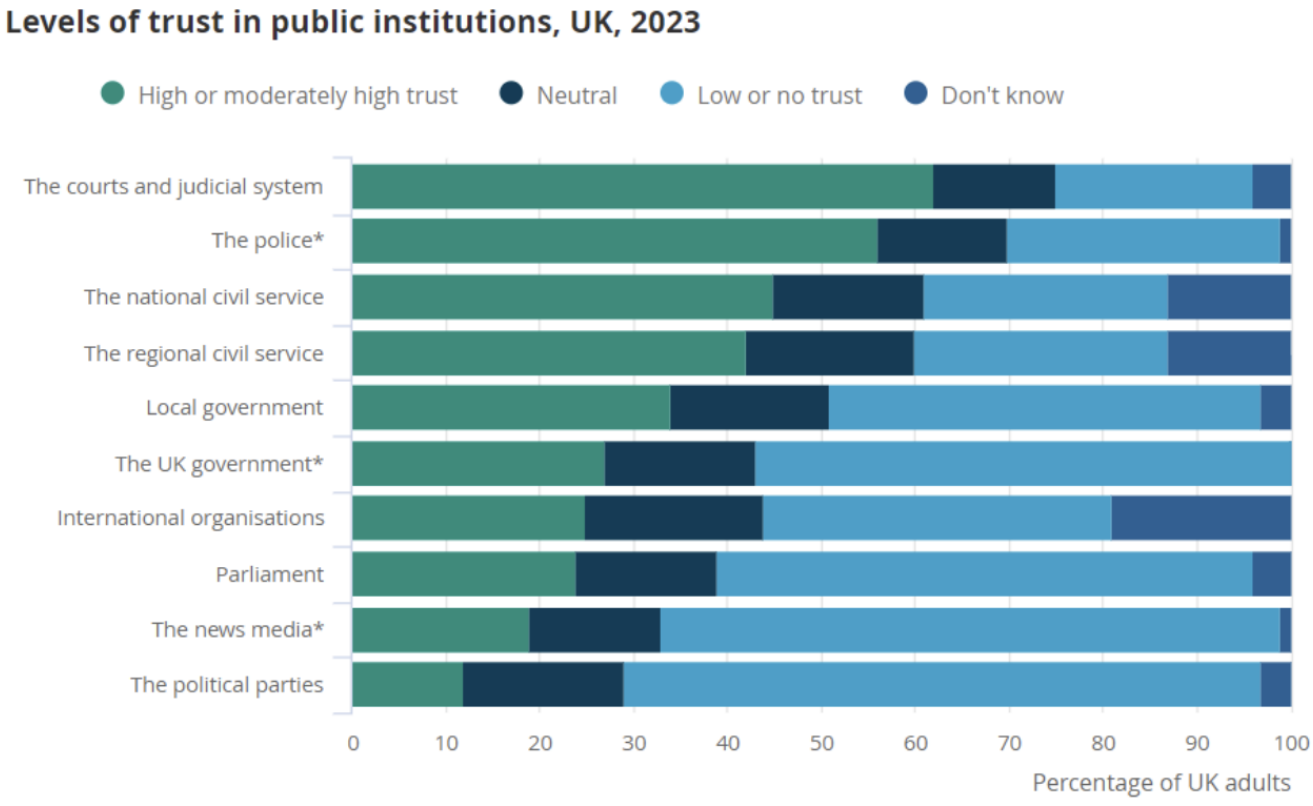


Figure: Levels of trust in public institutions in the U.K. in 2023.
Source: Office for National Statistics (ONS).

What did we learn?

Blockchain technology builds upon cryptographic solutions to support the checking, executing, and recording of transactions between parties based on a distributed (usually public) digital ledger.

At the core of blockchain, there are (1) cryptographic tools (e.g., hashing functions and encryption) and (2) consensus protocols.

Key properties of blockchain are immutability and irreversibility of transactions, integrity of the ledger, transparency and decentralisation.

Balancing those aspects while facilitating mass adoption is not easy.

Use cases go beyond financial applications, ranging from industrial use cases to government services.