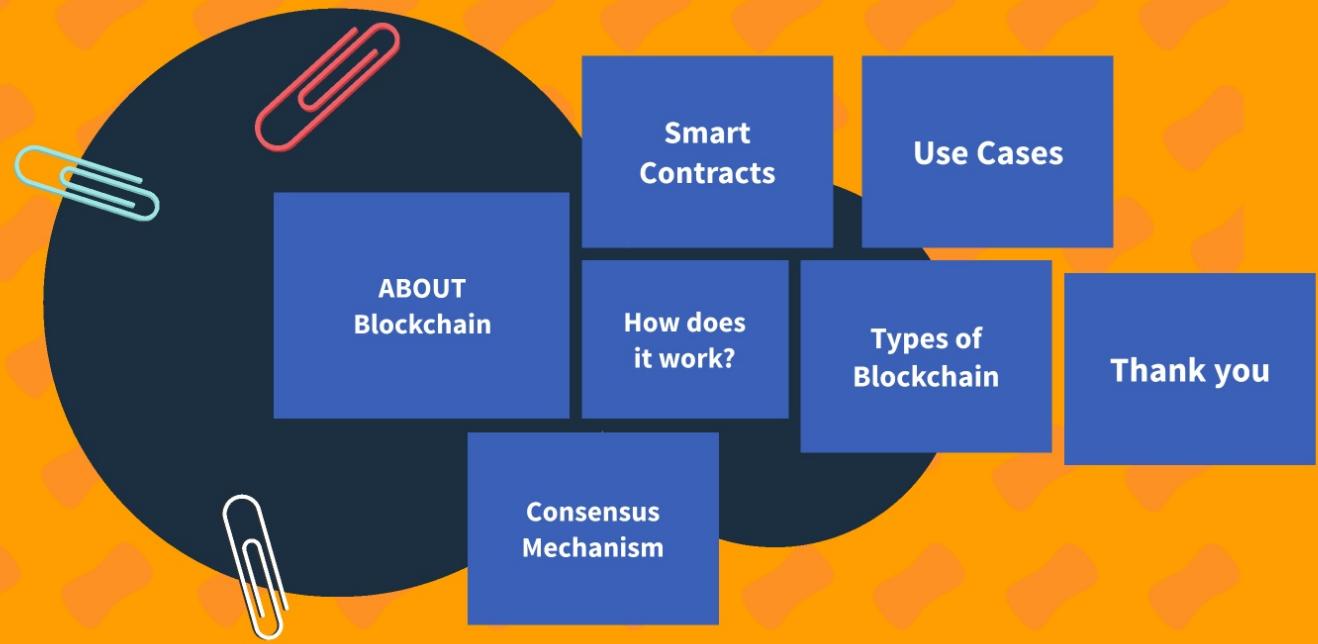




Blockchain Technology



Introduction

What you'll learn through this course:

-  What is Blockchain?
-  How does it work?
-  Consensus Mechanism
-  Types of Blockchain
-  Blockchain Use Cases



Insaf NORI

Decred Group
Community Manager

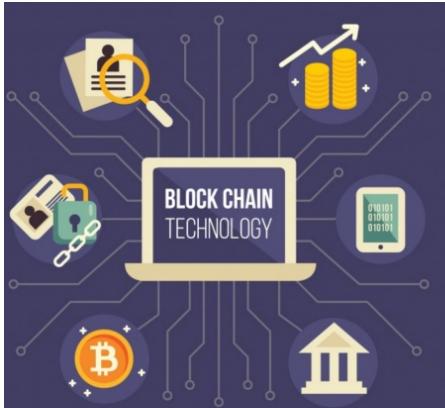
Definition

History

Introduction

Blockchain supports digital transformation





Part 1: Definition

Blockchain is a **shared**, **immutable** ledger that facilitates the process of **recording** transactions and **tracking** assets in a business network. An asset can be **tangible** (a house, a car, cash, land) or **intangible** (intellectual property, patents, copyrights, branding).

What is Blockchain

What is Blockchain



Distributed Ledger

All network participants have access to the distributed ledger and its immutable record of transactions.

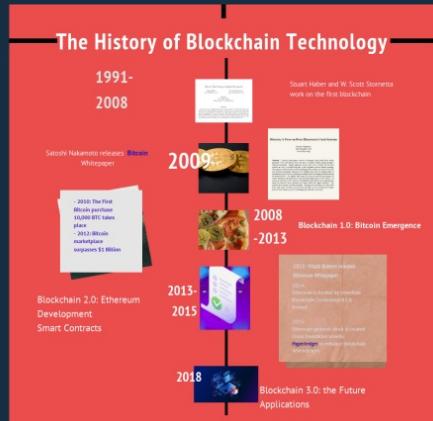
Immutable

No participant can change or tamper with a transaction after it's been recorded to the shared ledger.

Trust-less

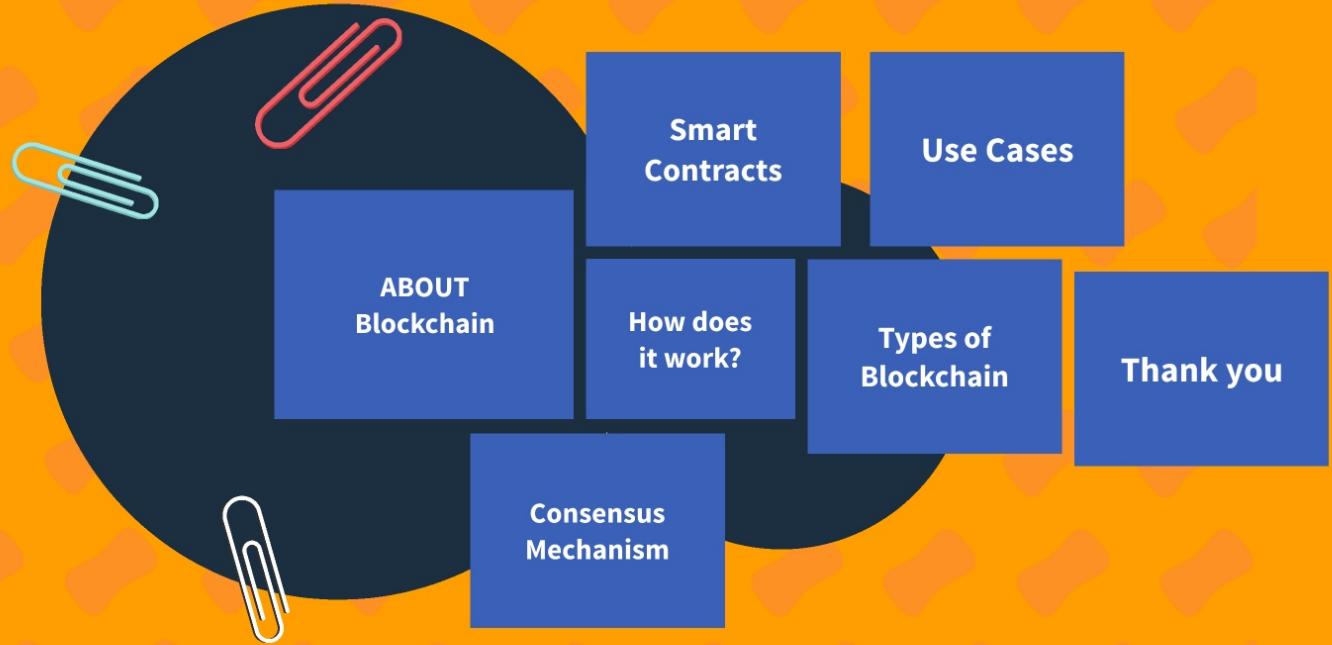
You don't need to know the other person or trust him.

History of blockchain





Blockchain Technology



How does it work?

- How does a Blockchain work: A detailed overview
- What is a Hash Function?
- Public/Private key



Overview

**Hash
Function**

**Public/
Private
Key**

Blockchain

How does a Blockchain Work?



How does a Blockchain work:

A Database

Records are bundled together into blocks and added to the chain one after another. The basic parts:



The record :
can be any information



The Block:
A bundle of records



The Chain:
All the blocks linked together

Step One

Step Two

Step Three

Step Four

How does a Blockchain work:

Here's how a deal gets included in a Blockchain:

STEP ONE

A trade is recorded. For example, let's say Alice is sending to Bob \$100 in crypto. The record lists the details, including a digital signature from each party.



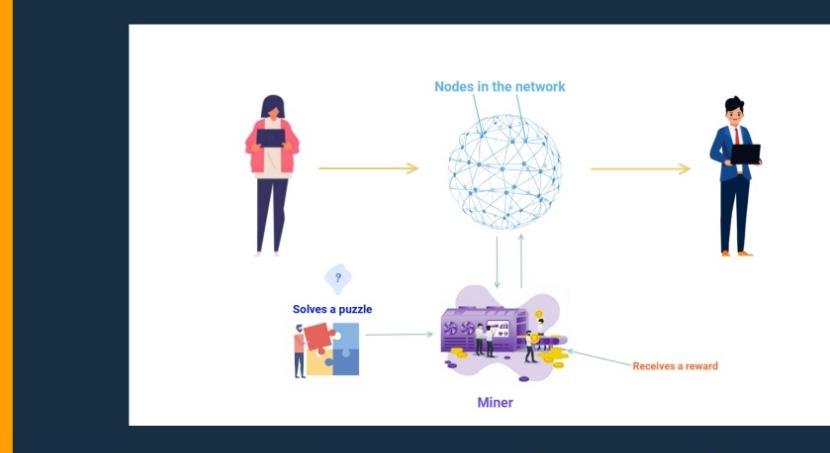
1. She enters Bob's account address as the recipient.
2. She specifies that she wants to send 100\$ in crypto to Bob.
3. She signs the transaction in order to make it official with her private keys.

How does a Blockchain work:

Here's how a deal gets included in a Blockchain:

STEP TWO

The record is checked by the network. The computers in the network, called 'Nodes', check the details of the trade to make sure it is valid.



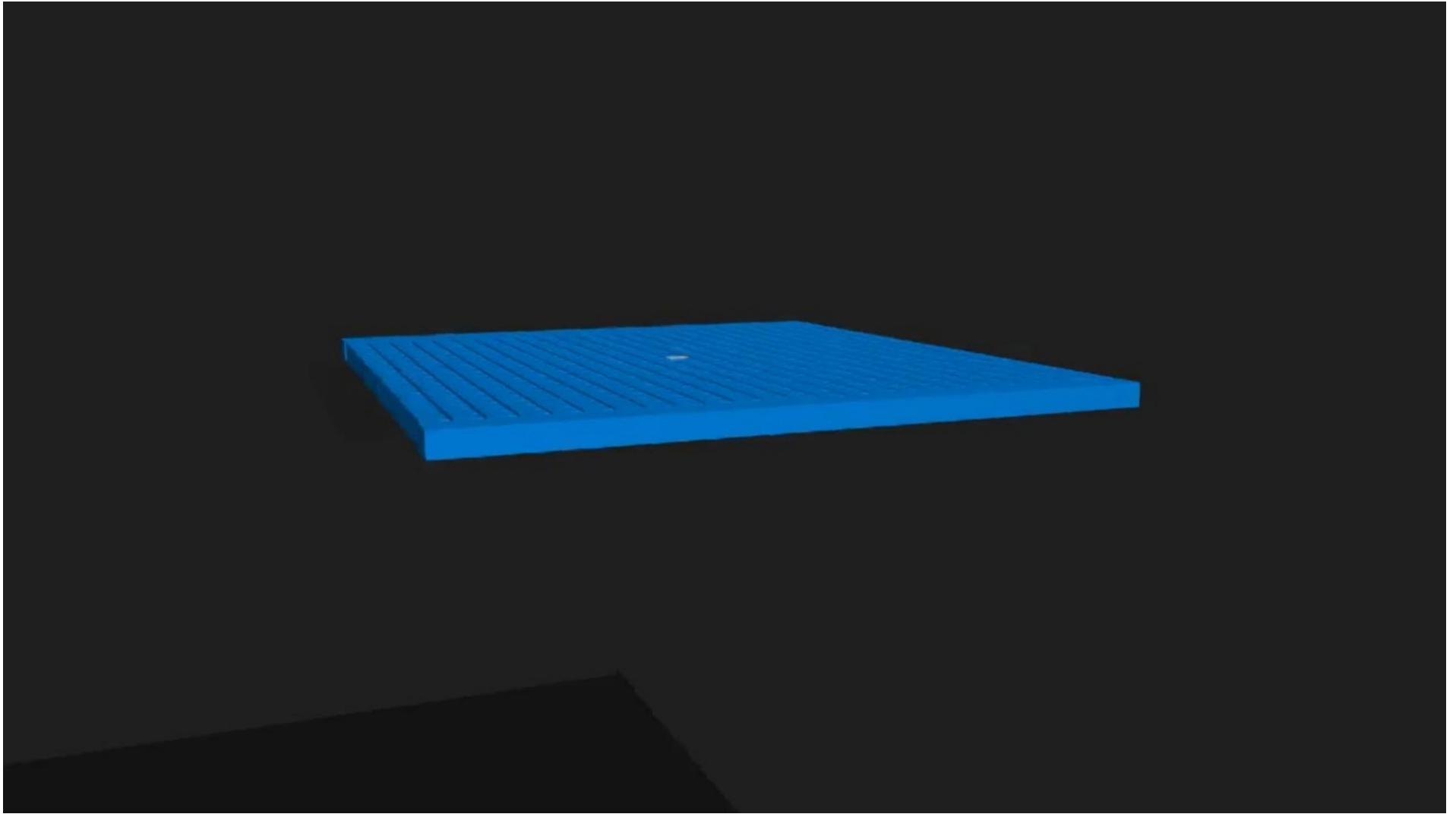
How does a Blockchain work:

Here's how a deal gets included in a Blockchain:

STEP THREE

The records that the network accepted are added to a block. Each block contains a unique code called a hash. It also contains the hash of the previous block in the chain.



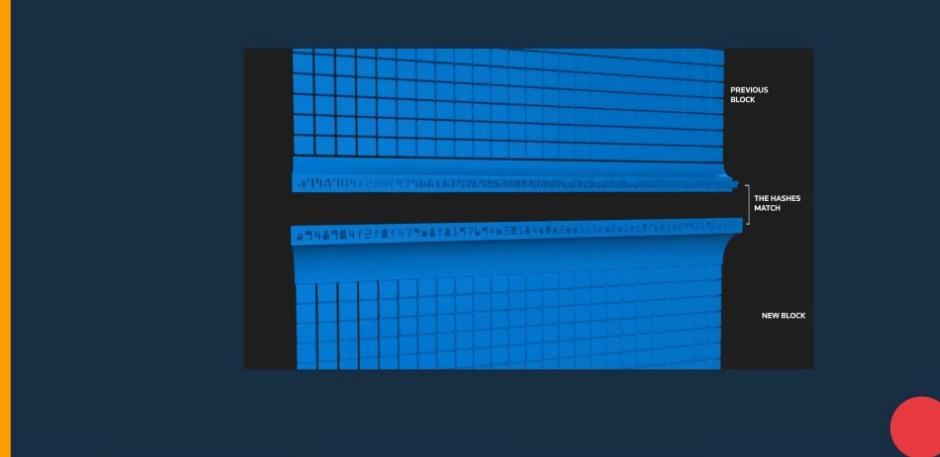


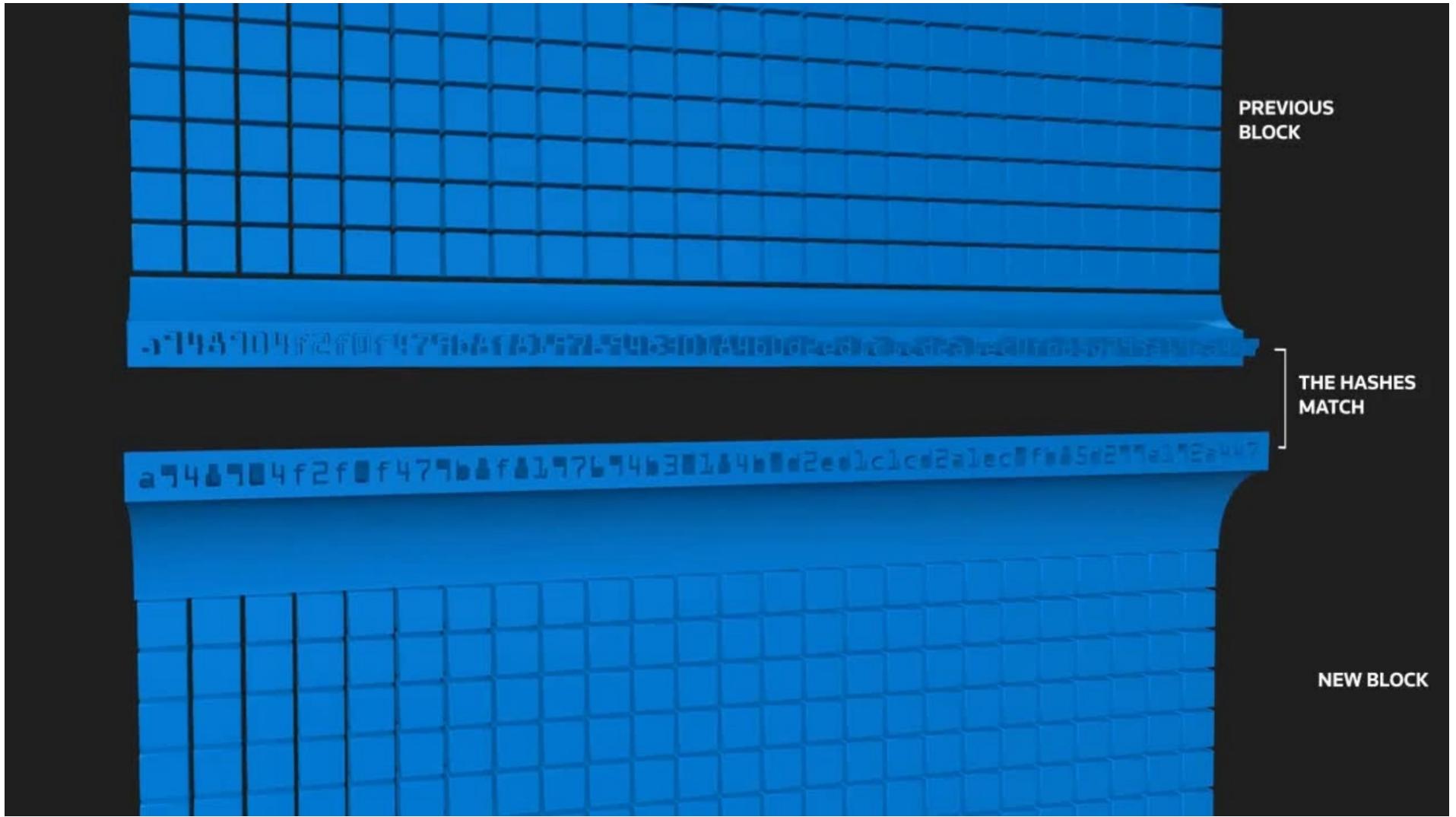
How does a Blockchain work:

Here's how a deal gets included in a Blockchain:

STEP FOUR

The block is added to the blockchain. The hash codes connect the blocks together in a specific order.





Hash Function



A **hash code** is created by a **math function** that takes digital information and generates a **string** of **letters** and **numbers** from it. Let's take a closer look at **two important characteristics** of hash codes:

First, no matter what the **size** of the **original file**, a hash function will always generate a code of the **same length**.

Second, any change to the **original input** will generate a **new hash**.

Example: <https://andersbrownworth.com/blockchain/hash>



Public vs. Private Key



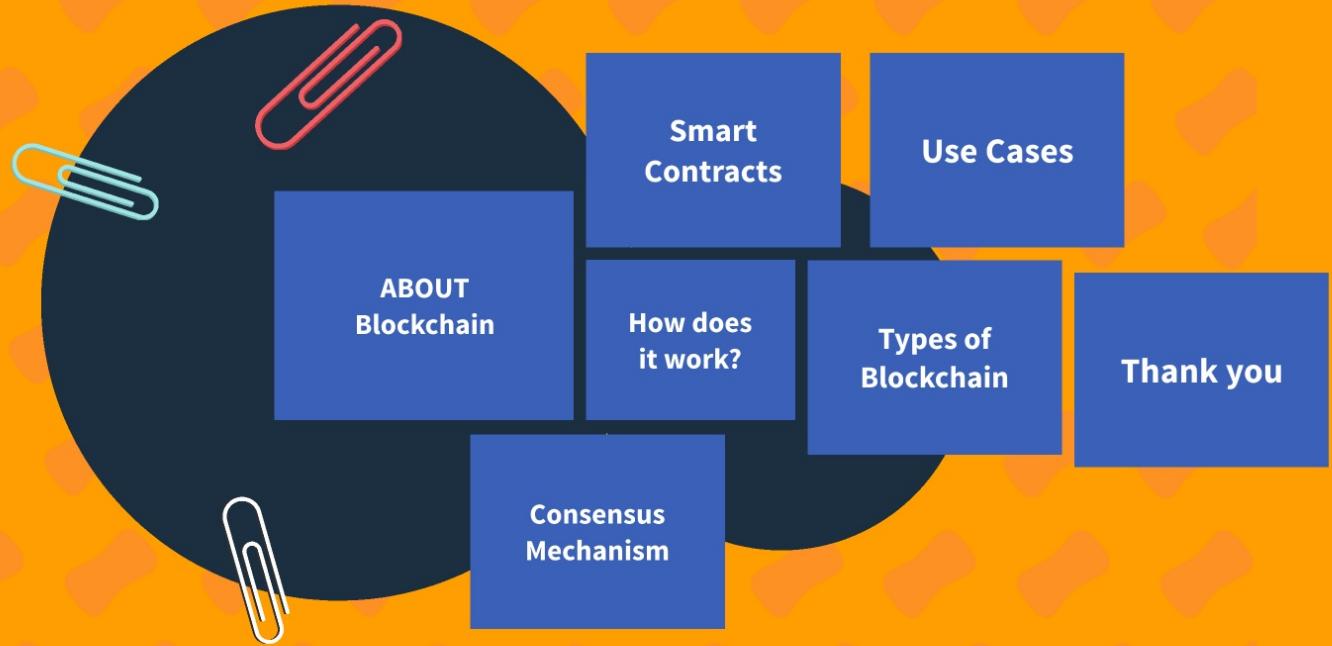
[https://andersbrownworth.com/
blockchain/public-private-keys/keys](https://andersbrownworth.com/blockchain/public-private-keys/keys)

- Public key cryptography uses a pair of a public key and a private key to perform different tasks. Public keys are widely distributed, while private keys are kept secret.
- The goal of public and private keys is to prove that a spent transaction was indeed signed by the owner of the funds, and was not forged.
- When you own cryptocurrencies, what you really own is a “private key.”





Blockchain Technology



Consensus Mechanism



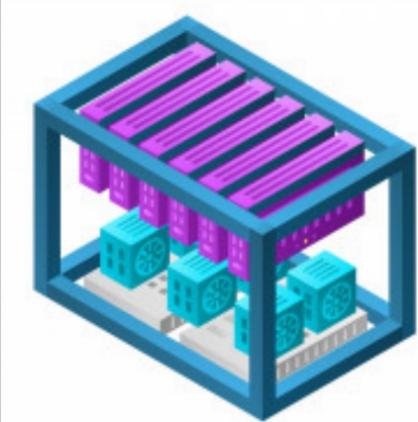
**Proof of Work
Mechanism**



**Proof of Stake
Mechanism**

Hybrid PoW/PoS

How it works



Proof of Work Mechanism

PoW

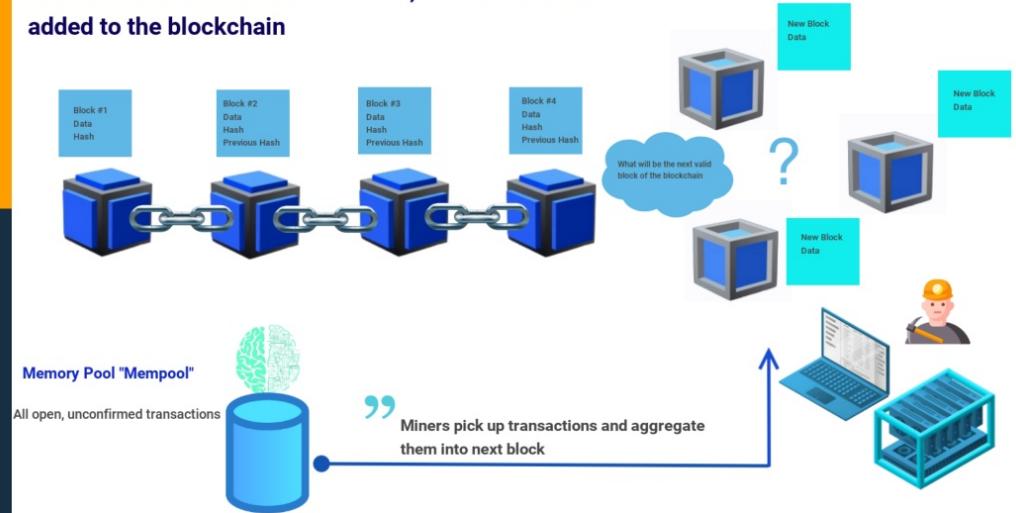
To add a block to the chain, nodes must demonstrate that they have done ‘work’ by solving an increasingly difficult computational puzzle. This process, called mining, uses a lot of computing power. In return for their work, members can receive rewards - tokens for instance, or bitcoins.

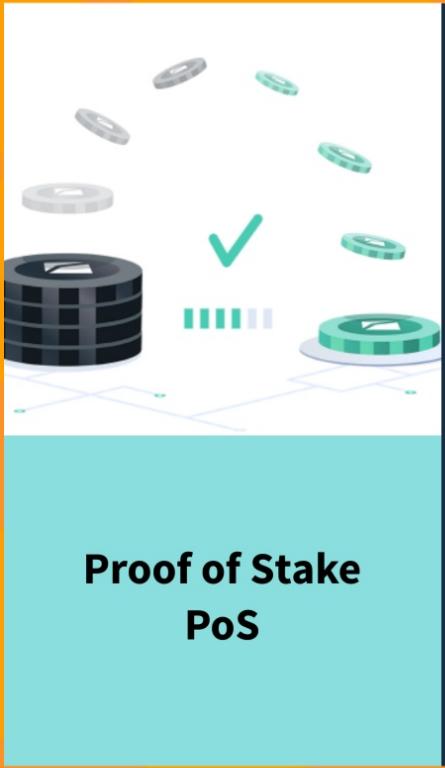


How it works

Proof Work Mechanism

Proof of work is used to select next, valid block to be added to the blockchain



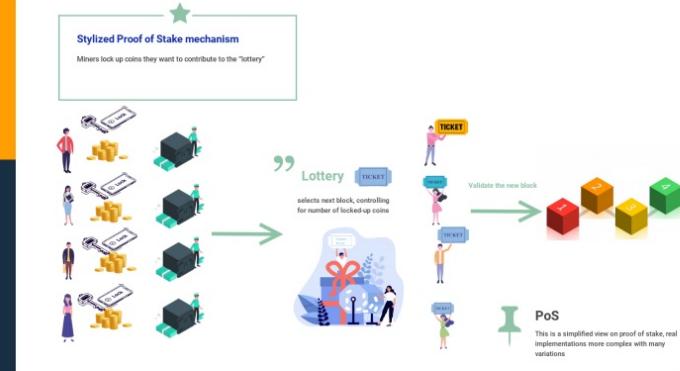


PROOF OF STAKE

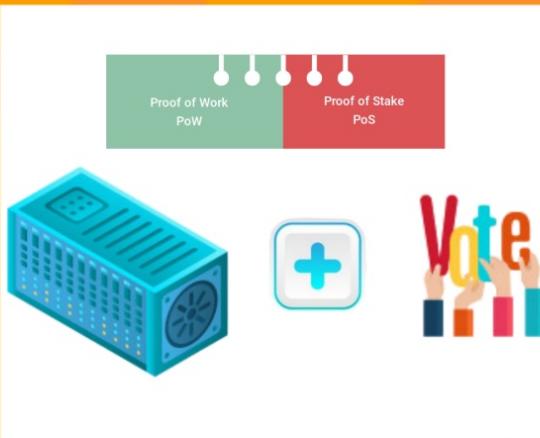
Participants buy tokens which allow them to join the network. The more tokens they have, the more they can mine.

Proof of stake selects next block contributor based on contributed coin stakes of miners

How it works?



How it works

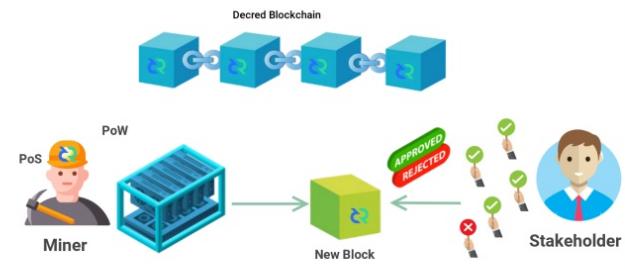


Hybrid PoW/PoS Mechanism

Hybrid Proof of Work/Proof of Stake consensus mechanisms utilize elements of both PoW and PoS models when determining transaction validation rights. In doing so, they aim to mitigate the respective weaknesses of each. While the exact mechanisms of individual hybrid consensus algorithms vary, the following explanation is based on **Decred**, perhaps the most notable project using a hybrid system.

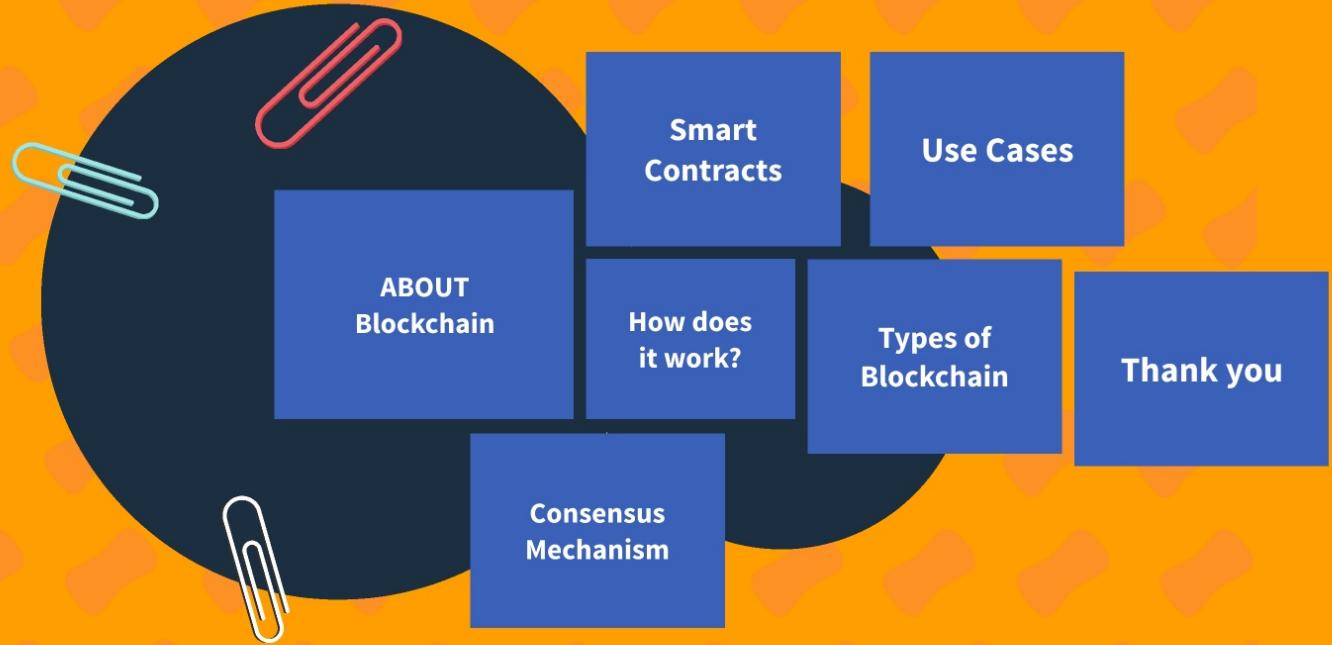
How it works

Hybrid PoW / PoS





Blockchain Technology



Types of Blockchain

Public

Private

Consortium

Hybrid

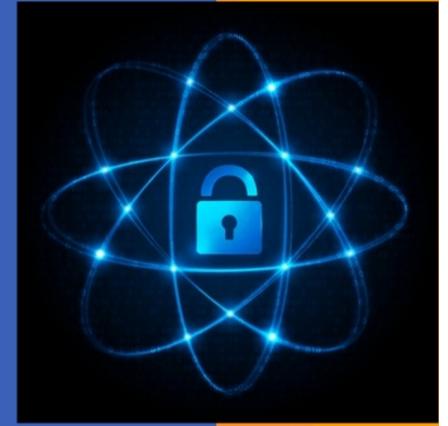
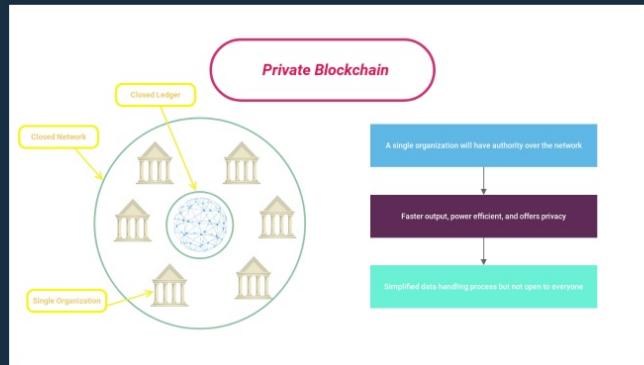




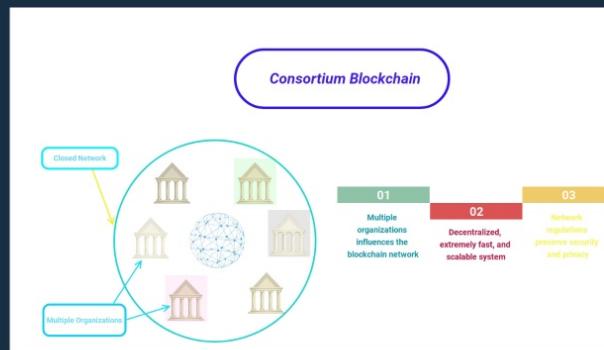
- A **public blockchain** is a blockchain that anyone in the world can **read**, **send** transactions too and expect to see them included if they are valid, and anyone can participate in the consensus process.
- **Public blockchains** are secured by **cryptoeconomics** – the combination of economic incentives and cryptographic verification using mechanisms such as proof of work or proof of stake . These blockchains are generally considered to be “fully decentralized.”



Private Blockchain



Consortium Blockchain



Hybrid Blockchain

What is Hybrid Blockchain?

The hybrid blockchain is best defined as the blockchain that attempts to use the best part of both public and private blockchains.

In an ideal world, a hybrid blockchain would combine the best features of both the public and private blockchains. It would be open to all members, yet still provide privacy and security for its users.

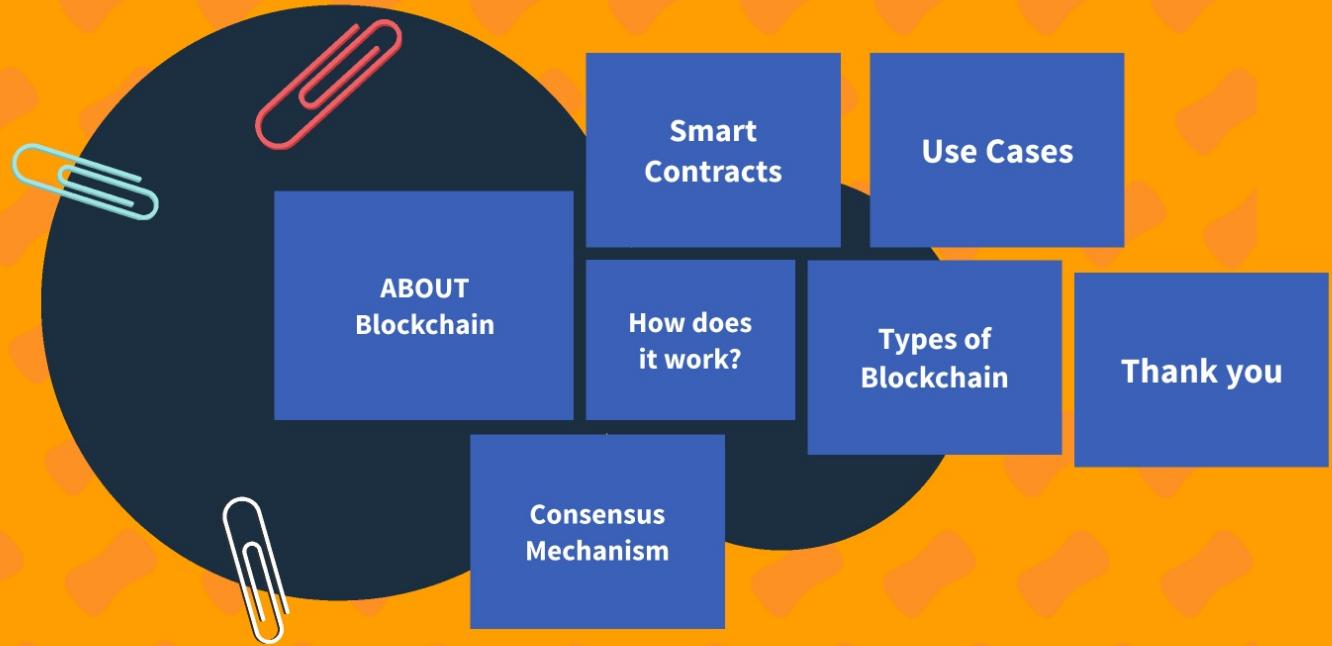
Benefits of Hybrid Blockchain

- Public network with all members
- Private network with other members
- Restriction
- Works in a hybrid ecosystem. This way you can have the best of both worlds on the networks.
- Provides privacy while maintaining the other benefits of the blockchain simultaneously.
- Can change the consensus algorithm. However, the change must be agreed upon by the majority of the hybrid blockchain to be adopted.
- Levers transaction costs as the hybrid blockchain is smaller than the public network, making it faster and more efficient for the transaction.

Created by 101blockchains.com



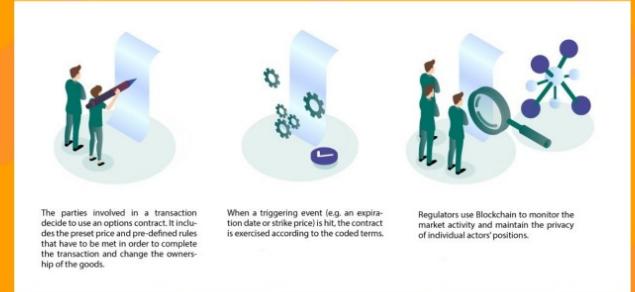
Blockchain Technology



Smart Contracts



• Smart contracts are **computer codes** with predefined sets of rules that run on **blockchains** and set the conditions under for how all parties to the smart contract agree to interact with one another. If and when all the necessary conditions are met, smart contracts then auto-execute.



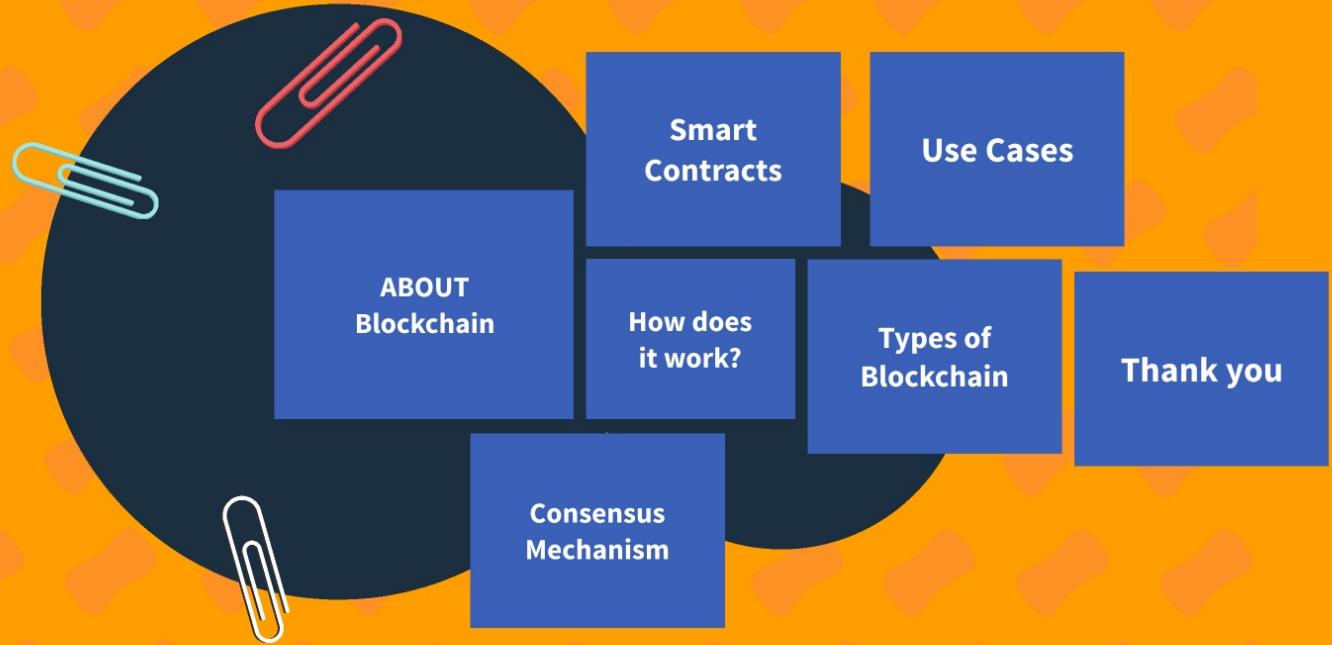
The parties involved in a transaction define the conditions of a contract. It includes the preset price and pre-defined rules that have to be met in order to complete the transaction and change the ownership of the goods.

When a triggering event (e.g. an expiration date or strike price) is hit, the contract is exercised according to the coded terms.

Regulators use Blockchain to monitor the market activity and maintain the privacy of individual actors' positions.



Blockchain Technology



How Does Blockchain Benefit Enterprises Across Industries?

Use Cases



- **Automatic execution.** Streamline business processes through programmable transactions and real-time clearing and settlement.
- **Advanced security.** Mitigate risk with tamper-proof data coordination and granular security controls.
- **Trusted business networks.** Quickly deploy permissioned networks with shared business logic and customizable governance.
- **Digital asset management.** Rapidly create and manage digital assets and instruments.
- **Production grade.** Manage a compliant blockchain platform at scale with zero downtime.



Money Transfer

Energy

Healthcare

Government

Money Transfer



- * Consumers send \$180 trillion in cross-border payments each year.
- * Sending money outside of the United States costs 42 dollars per transaction.
- * Blockchain-powered payment services charge less than one percent in fees on cross-border payments. They take only a few hours to process, and account for billions of dollars in international transfers completed.

Examples

Blockchain in Money transfer

Examples

Companies Trying to Solve This Problem

- * **R3 (Corda)** – Full-service banking solutions on the blockchain.
- * **Santander** – First UK bank to facilitate live international payments with blockchain. Esp. between Europe and South America.
- * **CLS** – Blockchain solutions for Global forex and clearing.
- * **Wyre** – Faster international money transfer on the blockchain.

Blockchain in Energy

What are the Blockchain Use Cases in Energy?



The main benefits of blockchain in the energy sector are:

- Reduced costs
- Environmental sustainability
- Increased transparency for stakeholders while not compromising privacy

Applications

- Wholesale electricity distribution
- Peer-to-peer energy trading
- Electricity data management
- Commodity trading
- Utility providers
- Oil and gas resource exploration
- Oil and gas resource storage and transportation
- Refined resource management and sale





Healthcare

Blockchain technology can help healthcare experts and the overall healthcare industry to improve performance, patient data transparency, tracking, and accountability, as well as reduce costs.

- * Secure management of electronic health records (EHRs)
- * Patient consent management
- * Drug traceability
- * Data security in clinical trials
- * Incentivization through micropayments

Government



Applications

Governments and public sector organizations leverage blockchain technology to move away from soiled and inefficient centralized systems. Current systems are inherently insecure and costly, while blockchain networks offer more secure, agile, and cost-effective structures.

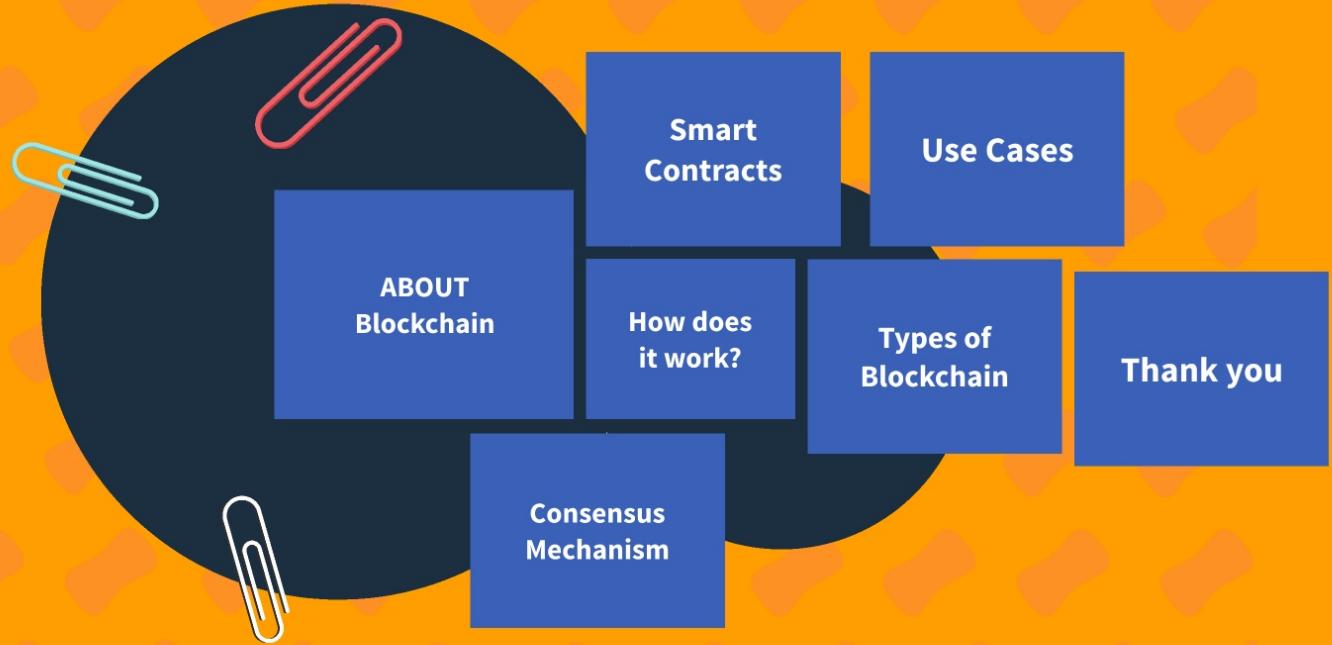
Government

A blockchain-based government has the potential to solve legacy pain points and enable the following advantages:

- * Secure storage of government, citizen, and business data
 - * Reduction of labor-intensive processes
 - * Reduction of excessive costs associated with managing accountability
 - * Reduced potential for corruption and abuse
- Increased trust in government and online civil systems



Blockchain Technology





<https://decred.org/>



@decredproject
@DecredArabia



[https://chat.decred.org/#/
register](https://chat.decred.org/#/register)



@decredproject
@DecredArabia



Decred
DecredArabia



@Decred
@DecredArabia



Blockchain Technology

