

AN INTRODUCTION TO **BLOCKCHAIN**





What is a blockchain?

- » is a **novel** solution that provides **trustless trust**
- » is a shared, trusted, public, distributed ledger of transactions
- » allows **public inspection** of the system
- » a **de-centralized** system
- » is a **distributed P2P** database
- » maintains a continuously growing list of transactional records
- » is cryptographically secured from tampering and revision

A Few Basics

To understand blockchains, one must first understand:

- » Public key crypto systems
- » Digital signatures
- » Cryptographic hashes

Public Key Crypto Systems

» ENCRYPT & DECRYPT

» Keys are the inverse of each other (Public & Private)

» Mathematically proven



Digital Signatures

» SIGN & VERIFY

- » Keys are inverse of each other
- » Public and Private Keys
- » Provides non-repudiation



Crypto Hashing Functions

- » One-Way compression algorithm / system
- » Any input provides a fixed size output
- » Changing one bit changes the whole hash
- » Mainly used for integrity





The Basics Combined

If Alice wants to send a message M to Bob, Alice can:

» Hash the message (nobody can tamper with the message anymore)

»Sign the generated hash (Alice cannot deny later on sending it)

»Encrypt the message (only Bob can see it)





BACK TO THE BLOCKCHAIN

A Block in the Chain

» can store any data

- » LIMITED storage size
- » First block is known as the Genesis Block (G)

A Block in the Chain



The Ledger in the Chain



The Ledger in the Chain



The Ledger in the Chain



Peer-2-Peer Networks (P2P)

» No center exists. Decentralized by nature

» All nodes are connected to each other

» Only way to get network down is to shut down all servers.

Switched Network



Distributed Ledger

 » Ledgers are shared across many network servers (known as miners)

» Network uses a Peer-2-Peer structure



Blockchain Consensus

- » Updating the blockchain requires network consensus
- » All miners are notified
- » Each miner verifies the legitimacy of the transaction
- » Majority of network must accept the change to become legitimate



Each network participant keeps a copy of the entire blockchain - the file where all past transactions are recorded. Consensus of network validators verifies new transactions. In the Bitcoin network transactions are validated by network miners who are incentivised to verify transactions through PoW (Proof of Work).

Blockchain **Technologies**

» Cryptography for data protection and tampering

» P2P for De-centralization

» Game Theory for incentives to miners



Again, What is a blockchain?

- » is a **novel** solution that provides **trustless trust**
- » is a shared, trusted, public, distributed ledger of transactions
- » allows **public inspection** of the system
- » a **de-centralized** system
- » is a **distributed P2P** database
- » maintains a continuously growing list of transactional records
- » is cryptographically secured from tampering and revision



USING THE BLOCKCHAIN

Where Are Blockchains Used?

» Tokens (Bitcoin, Ethereum, etc)

» Smart Contracts (Ethereum)

Traditional Organizations





One legal entity Employment contracts

Many layers of management for coordination & enforcement of processes. Many information & decision bottleneck as well as sources of corruption.

Decentralized Autonomous Organizations (DAOs)



Distributed Network of Autonomous Stakeholders

No centralized legal entity! No employment contracts!

Machine consensus around token governance rulsets and smart contracts instead of legal employment contracts.

Types of Blockchains

»Public: Bitcoin, Ethereum, Litecoin, Monero, Dash, Dodgecoin, etc.

»Federated: R3 (Banks), B3I (Insurance), EWF (Energy)

»Private: Monax, Multichain



Bitcoin



Ethereum



Smart Contracts





Smart contracts eliminate the need for trusted third parties

Traditional Car Sale



Verify the deal

A trusted third party is

required for verification. In order to officially transfer the ownership of the car, the terms of the contract have to be met. The process differs from country to country but always involves one or more trusted third parties: motor vehicle registration authority, in combination with a notary and/or insurance company. It's a complicated and lengthy process. Middlemen fees apply





Bob wants to sell his car. He identifies himself with Bob leaves his car and car key in a garage locked with a smart contract controlled smart lock. The car has its own blockchain address (public key) 13849Z stored on the blockchain



pick up her car by unlocking the smart lock with her private key



(public key) 757382 and

define the terms of the sale signing it with his

If 20 000€ were sent to my account number 757382 then automatically transfer car ID 13849Z as well as grant smart lock access to the account from which the money has been transferred </contract> each node on the blockchain network checking if Bob is the owner of the car and if Alice has enough money to pay Bob

If the network agrees, that all conditions are true, Alice automatically gets the access code to the smart garage lock. The blockchain registers Alice as the new owner of the car. Bob has 20 000€ more in his account, and Alice 20 000€ less

The smart contract accessible from a web arowser. Traditional conline services can use smart contracts is the backgood

B



Bob leaves his car and car key in a garage locked with a smart contract controlled smart lock. The car has its own blockchain address (public key) 13849Z stored on the blockchain



The smart contract is accessible from a web browser. Traditional online services can use smart contracts in the backend

Alice wants to buy a car. She finds Bob's car listed on the Internet. She signs the contract with her private key transferring 20 000€ from her blockchain address (public key) 389157 to Bob's blockchain address 757382

contract controlled smart lock. The car has its own blockchain



her private key

(public key) 757382 and



<Smart contract>

If 20 000€ were sent to my account number 757382 car ID 13849Z as well as grant smart lock access to the account from which the money has been transferred

network checking if Bob is the owner of the car and if Alice has 🥻 enough money to pay Bob

If the network agrees, that all code to the smart garage lock. The



The smart contract is verified by each node on the blockchain network checking if Bob is the owner of the car and if Alice has enough money to pay Bob



If the network agrees, that all conditions are true, Alice automatically gets the access code to the smart garage lock. The blockchain registers Alice as the new owner of the car. Bob has 20 000€ more in his account, and Alice 20 000€ less





Can We Trust Smart Contracts?



Smart Contracts Types





VSAWMA@NDU.EDU.LB VICTOR.SAWMA@INTOUCHMENA.COM

I CAN BE REACHED AT



ANY QUESTIONS ABOUT
BLOCKCHAIN?