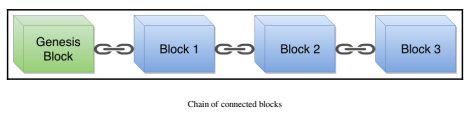
**Blockchain:**

Blockchain is a transaction record database that is distributed, validated and maintained around the world by a network of computers. Instead of a single central authority such as a bank, a large community oversees the record, and no individual person has control over them.

* Each computer that participates in this P2P network is called a node. Each node maintains the records of transactions in multiple consecutive blocks.
* Blockchain technology is also called Decentralized Ledger Technology (DLT), as each node in the network keeps the same copy of the ledger.



**Types of Blockchain:**

* Public Blockchain
* Private Blockchain

**Public Blockchain:**

* Anyone can read without explicit authorization
* More complex rules for better security
* Computationally expensive to mine & add a Block
* Computational power is distributed globally
* Example: Bitcoin Blockchain, Ethereum Blockchain etc.

**Private Blockchain:**

* Only authorized nodes can read the transaction data
* Only authorized nodes can write the transaction into Blockchain
* Easy or computationally less expensive to add a Block
* Many things can be replaced by legal contract giving more control to the one party
* Examples: Recordkeeper Blockchain, ICICI Bank’s Blockchain etc.

**Properties of Blockchain**

* Blockchain has properties of both decentralized and distributed networks.
* Using those types of networks along with cryptography adds more properties.
* We are covering here in this course properties related to the Ethereum blockchain rather than other blockchain implementation properties.
* The other blockchain implementations might have different properties.

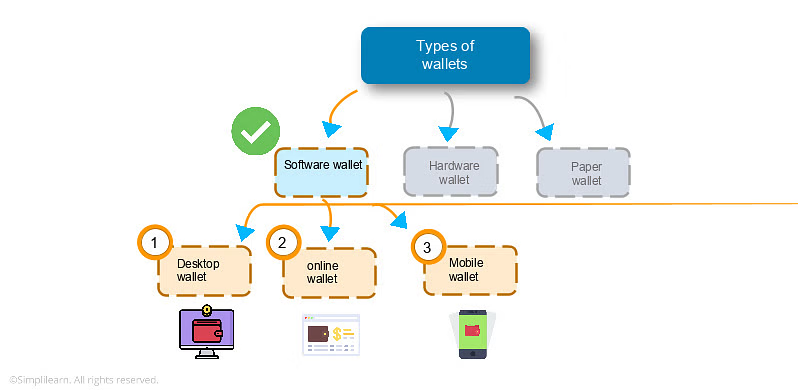
**Wallet:**

A cryptocurrency wallet is a software application that holds private and public keys and communicates with various. blockchains so that users can send and receive digital currencies and track their balance. if you want to use Bitcoin or some other cryptocurrency.

When an individual sends you bitcoins or some other digital currency, they essentially sign off coin ownership at your wallet’s address. The private key kept in your wallet must match the public address with which the money is allocated to, in rider to be avail certain coins and access the funds. The balance in your digital wallet will rise if the public and private keys match, and the balance of the sender will decrease accordingly. Private and public keys both form the basis for a blockchain network. In cryptographic terms, any authentication framework needs a public location key and a private access key.

* A wallet is software that keeps one or more cryptographic private and public keys.
* Using these keys, you can interact with different blockchains and are allowed to send and receive digital currencies.
* You can also interact with smart contracts using any of the accounts present in your wallet.

**Types of Wallets:**



**Proof of Work:**

* Proof of work is a decentralized consensus mechanism that requires members of a network to expend effort solving an arbitrary mathematical puzzle to prevent anybody from gaming the system.
* Proof of work is used widely in cryptocurrency mining, for validating transactions and mining new tokens.
* Due to proof of work, Bitcoin and other cryptocurrency transactions can be processed peer-to-peer in a secure manner without the need for a trusted third party.
* Proof of work at scale requires huge amounts of energy, which only increases as more miners join the network.

**Proof of Stake:**

* With proof-of-stake (POS), cryptocurrency owners validate block transactions based on the number of coins a validator stakes.
* Proof-of-stake (POS) was created as an alternative to Proof-of-work (POW), the original consensus mechanism used to validate a blockchain and add new blocks.
* Proof-of-stake (POS) is seen as less risky in terms of the potential for an attack on the network, as it structures compensation in a way that makes an attack less advantageous

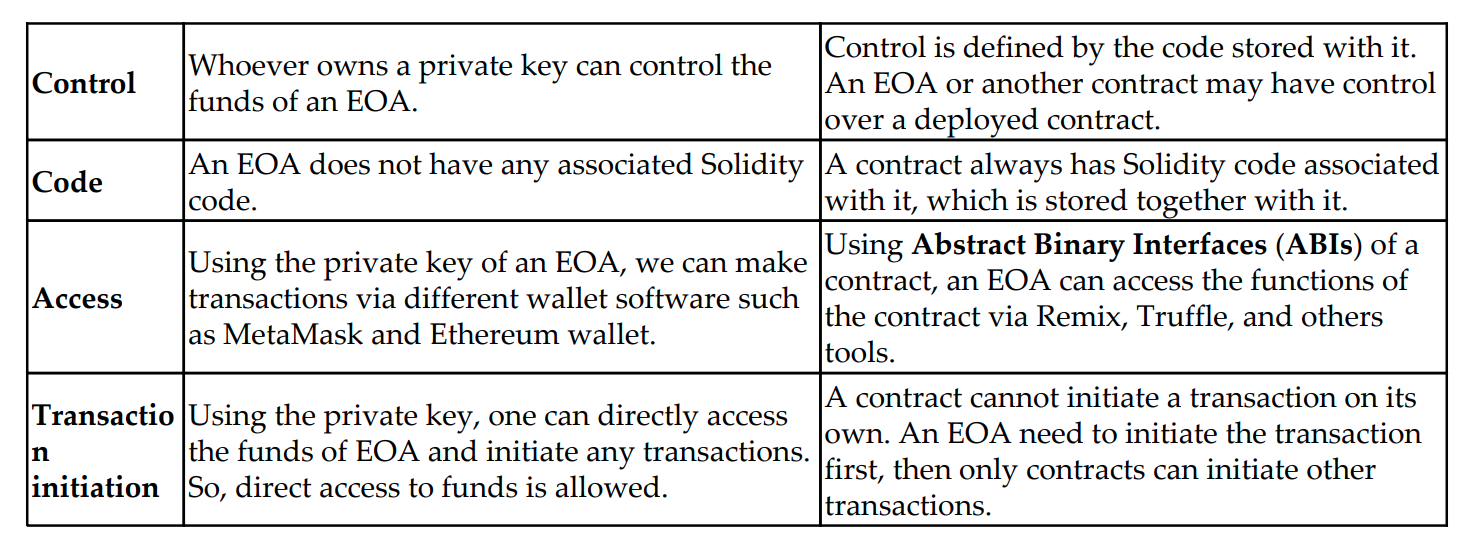
**Externally Owned Account**

The user can interact with the Ethereum network via one of the EOA accounts present in his wallet. A user holds a wallet that can have one or more EOA accounts. Each EOA account has a private key, which the user must use so they can sign the transaction data and send it to the Ethereum network to be executed. The user can also check their account balance from the Ethereum network using their public key

**Contract Account**

This type of account is also known as a contract. Contracts only have a public address, and their code logic controls the flow of the funds and other states of the contract. Contracts do not have any private keys associated. You need an EOA account to create a new contract or to interact with an existing contract. Contract accounts have a Solidity code that defines their behavior.

**The Difference between EOA & Contract Account:**



**Cryptography**

The study of how to send information back and forth securely in the presence of adversaries. A function for encoding or encrypting data to protect the contents from adversaries.

Example:

* Rose Greenhow
* Socialite in Washington D.C.
* Renowned confederate spy during US Civil War.

**PUBLIC/PRIVATE KEY CRYPTO**

* 2 uniquely related cryptographic keys
* Data encrypted with the public key can only decrypted with the private one (and vice versa)
* The mathematical computation behind it is complex Main aim is confidentiality (in messaging)
* Also used for digital signatures (the bit we’re interested in)



What is Mining?

* Most people think of crypto mining simply as a way of creating new coins. Crypto mining, however, also involves validating cryptocurrency transactions on a [blockchain](https://freemanlaw.com/blockchain-technology-explained-what-is-blockchain-and-how-does-it-work/) network and adding them to a [distributed ledger](https://freemanlaw.com/distributed-ledgers-the-technology-behind-blockchain-brings-business-opportunities-and-legal-complexities/).
* Most importantly, [crypto mining](https://freemanlaw.com/taxation-of-crypto-mining/) prevents the [double-spending](https://freemanlaw.com/double-spending-problem-and-byzantine-generals-problem-in-relation-to-cryptocurrency/) of digital currency on a [distributed network](https://freemanlaw.com/distributed-ledgers-the-technology-behind-blockchain-brings-business-opportunities-and-legal-complexities/).
* Like physical currencies, when one member spends cryptocurrency, the digital ledger must be updated by debiting one account and crediting the other. However, the challenge of a digital currency is that digital platforms are easily manipulated. Bitcoin’s [distributed ledger](https://freemanlaw.com/distributed-ledgers-the-technology-behind-blockchain-brings-business-opportunities-and-legal-complexities/), therefore, only allows verified miners to update transactions on the digital ledger. This gives miners the extra responsibility of securing the network from double-spending.
* Meanwhile, new coins are generated to reward miners for their work in securing the network. Since [distributed ledgers](https://freemanlaw.com/distributed-ledgers-the-technology-behind-blockchain-brings-business-opportunities-and-legal-complexities/) lack a centralized authority, the mining process is crucial for validating transactions. Miners are, therefore, incentivized to secure the network by participating in the transaction validation process that increases their chances of winning newly minted coins.
* In order to ensure that only verified crypto miners can mine and validate transactions, a [proof-of-work](https://freemanlaw.com/decentralized-governance-mechanisms/) (PoW) [consensus protocol](https://freemanlaw.com/permission-and-permissionless-blockchains/) has been put into place. PoW also secures the network from any external attacks.

Working Principle of Mining

Mining is the process of recording the pending transaction by adding a new Block into the Blockchain through a mathematical puzzle. Miners get rewarded by receiving the new coins of that Blockchain. The mining process is divided into two types:

* **Pool mining:**
  + There are just not enough resources for one single miner to mine the block.
  + A group of miners merge their resources to mine the Blockchain more quickly.
* **Solo mining:**
* Each miner must set up the equipment and register themselves for the mining.
* All other miners are notified by the first miner that

**WHAT IS SMART CONTRACT**

* Smart contracts are small programs where developers can define the rules of the trust that they intended to code. One of the mind-boggling properties of smart contracts is immutability—once they are deployed on the blockchain, their code cannot be changed. This immutable property makes it very hard to program smart contracts and predict errors/bugs beforehand
* A Smart contract is a term used to describe computer program code that is capable of facilitating, executing, and enforcing the negotiation or performance of an agreement using Blockchain technology.
* The entire process is automated can act as a complement, or substitute, for legal contracts, where the terms of the smart contract are recorded in a computer language as a set of instructions.
* In general, Smart contracts help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman.

**What Are the Advantages of Smart Contracts?**

* Reliability and immutability provided by the decentralized data storage system in the blockchain technology;
* Transparency of actions in smart contracts on blockchain in the system, along with the confidentiality of the parties to the contract;
* Automation of smart contracts work;
* Cost reduction due to exclusion from the chain of intermediaries;
* High speed of execution thanks to the use of mathematical algorithms in blockchain applications instead of bureaucratic mechanisms.

**Disadvantages of Smart Contracts**

* Weak legal regulation of smart contracts work;
* The necessity to address the issue of transaction processing speed and scalability in blockchain technology;
* Inability to adjust smart contracts work;
* High dependence on programmers and exposure to bugs.