**Assignment 2**

* **Public ledgers**
* **What is Ledger in Crypto?**

A ledger (not to be confused with Ledger) is a record-keeping system: it tracks value as is moves around, so the viewer can always see exactly what value resides where at a given moment. Traditional finance systems like banks use ledgers to track all transactions completed within a period.

Blockchains are a form of digital ledgers that validate and store all transactions within their network. For example, the Bitcoin blockchain records all transactions involving bitcoins using blocks secured by cryptography.

Blockchain technology is an effective ledger system because it operates an immutable and autonomous record-keeping network, which means that you can’t change any data once it is stored on the blockchain.

* **What is a Public Ledger in Crypto?**

A public ledger is an open-access network; anyone can join at any time. The public ledger is fully decentralized, and no single entity controls the blockchain network. The Bitcoin and Ethereum blockchains are both considered public ledgers.

Public ledgers are also the most secure blockchains; they maintain a pseudo-anonymous system for their users’ identities. While all transactions are recorded publicly, user identities remain private.

This means that while you can view any wallet address with its balance and transaction records, you cannot gain access to the identity of the wallet owner.

* **The General Purpose of a Crypto Ledger**

A crypto ledger keeps an immutable record of all transactions on a cryptocurrency network. This system helps keep users’ identities anonymous, while still maintaining an accurate history of transactions within the network.

* **Block in a blockchain**
* **What Is a Block (Blockchain Block)?**

Blocks are data structures within the blockchain database, where transaction data in a cryptocurrency blockchain are permanently recorded. A block records some or all of the most recent transactions not yet validated by the network. Once the data are validated, the block is closed. Then, a new block is created for new transactions to be entered into and validated.

A block is thus a permanent store of records that, once written, cannot be altered or removed.

* **How a Block (Blockchain Block) Works?**

A blockchain network witnesses a great deal of transaction activity. When used in cryptocurrency, maintaining a record of these transactions helps the system track how much was or wasn't used and which parties were involved. The transactions made during a given period are recorded into a file called a block, which is the basis of the blockchain network.

A block stores information. There are many pieces of information included within a block, but it doesn't occupy a large amount of storage space. Blocks generally include these elements, but it might vary between different types:

* **Magic number**: A number containing specific values that identify that block as part of a particular cryptocurrency's network.
* **Blocksize**: Sets the size limit on the block so that only a specific amount of information can be written in it.
* **Block header**: Contains information about the block.
* **Transaction counter**: A number that represents how many transactions are stored in the block.
* **Transactions**: A list of all of the transactions within a block.

The transaction element is the largest because it contains the most information. It is followed in storage size by the block header, which includes these sub-elements:

* **Version**: The cryptocurrency version being used.
* **Previous block hash**: Contains a hash (encrypted number) of the previous block's header.
* **Hash Merkle root**: Hash of transactions in the Merkle tree of the current block.
* **Time**: A timestamp to place the block in the blockchain.
* **Bits**: The difficulty rating of the target hash, signifying the difficulty in solving the nonce.
* **Nonce**: The encrypted number that a miner must solve to verify the block and close it.

One 32-bit number in the header is called a nonce—the mining program uses random numbers to "guess" the nonce in the hash. When a nonce is verified, the hash is solved when the nonce, or a number less than it, is guessed. Then, the network closes that block, generates a new one with a header, and the process repeats.

Different mechanisms are used to reach a consensus; the most popular for cryptocurrency is proof-of-work (PoW), with proof-of-stake (PoS) becoming more so because of the reduced energy consumption compared to PoW.

* **Transaction**
* **Consensus**
* **Public vs private blockchain**
* **Permissioned model of blockchain**
* **Security aspect of blockchain**