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:

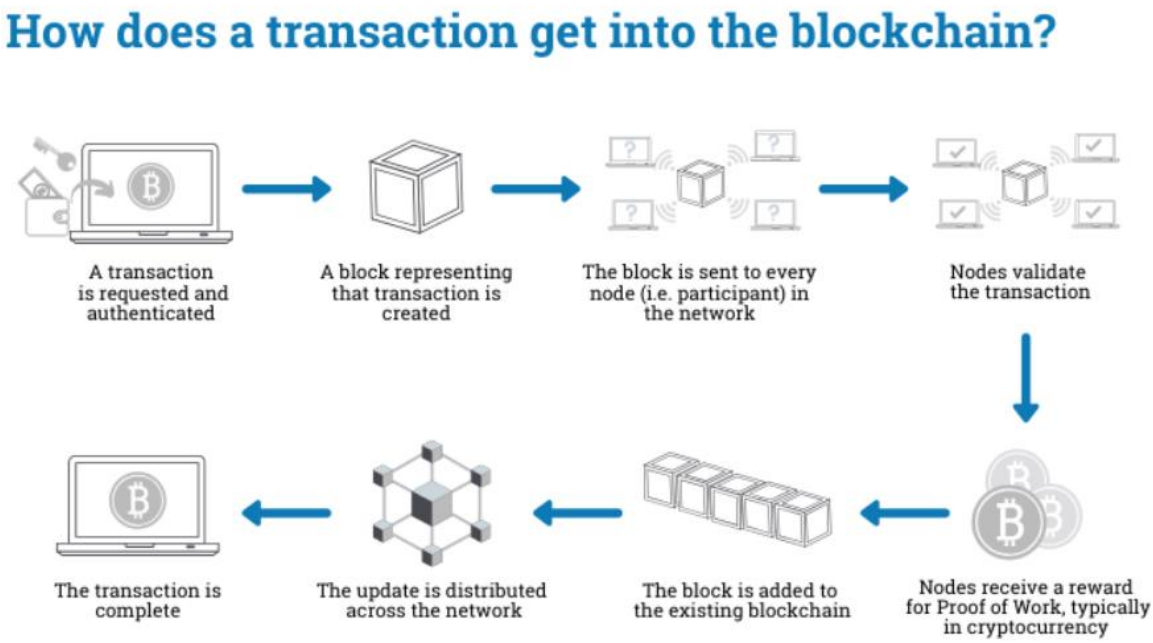
    - **Version**: The cryptocurrency version being used.
    - **Previous block hash**: Contains a hash (encrypted number) of the previous block's header.
    - **Hash Merkle root**: Hash of transactions in the Merkle tree of the current block.
    - **Time**: A timestamp to place the block in the blockchain.

- **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**



A transaction refers to a contract, agreement, transfer, or exchange of assets between two or more parties. The asset is typically cash or property. Likewise, a blockchain transaction is nothing but data transmission across the network of computers in a blockchain system. The network of computers in a blockchain store the transactional data as replicas with the storage typically referred to as a digital ledger.

Blockchain technology leverages peer-to-peer (P2P) networks to form a shared and secured ledger that records transactions as immutable time-stamped digital blocks. It is a decentralized ledger of transactions with no third-party involvement, and only participants in the blockchain network can validate transactions among them. While a blockchain can store different types of information, its most widespread use has been as a digital ledger for transactions.

In the context of cryptocurrency, a blockchain transaction example is an individual payment, such as Person A sending .10 BTC (bitcoin) to Person B. A blockchain transaction would typically involve the following information getting stored in blocks:

- Data about the transaction, such as the date, time, amount of money paid, place, etc.
- Data about the participants of the blockchain transaction or the username.
- Block specific data or hash, a unique code that distinguishes one block from another.

- **Consensus**

We know that Blockchain is a distributed decentralized network that provides immutability, privacy, security, and transparency. There is no central authority present to validate and verify the transactions, yet every transaction in the Blockchain is considered to be completely secured and verified. This is possible only because of the presence of the consensus protocol which is a core part of any Blockchain network. A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the distributed ledger. In this way, consensus algorithms achieve reliability in the Blockchain network and establish trust between unknown peers in a distributed computing environment. Essentially, the consensus protocol makes sure that every new block that is added to the Blockchain is the one and only version of the truth that is agreed upon by all the nodes in the Blockchain. The Blockchain consensus protocol consists of some specific objectives such as coming to an agreement, collaboration, cooperation, equal rights to every node, and mandatory participation of each node in the consensus process. Thus, a consensus algorithm aims at finding a common agreement that is a win for the entire network. Now, we will discuss various consensus algorithms and how they work.

- **Proof of Work (PoW)**

  In cryptocurrency blockchains based on the PoW algorithm, miners or validators -- also known as participant nodes -- must prove that the work they've done and submitted gives them the right to add new transactions to the blockchain. They must solve a complex mathematical problem by finding a cryptographic hash of a particular block.

  This is done by taking data from a block header as an input, and continuously running this data through a cryptographic hash function. Every time this is done, small changes are made to the input data by including an arbitrary number called a nonce. This is the blockchain version of guesswork to find a solution.

  Ultimately, when the miner finds the solution that leads to consensus, they're rewarded in cryptocurrency. However, all these actions require multiple iterations that consume a considerable amount of computational power. That's why PoW is considered an inefficient consensus mechanism.

- **Proof of Stake (PoS)**

  Proof of Stake (PoS) is considered an alternative to PoW. Unlike PoW, PoS requires little specialized hardware or software resources to mine cryptocurrencies since it doesn't involve solving complex computational problems. Rather, crypto validators lock up or stake some of their coins in a

wallet. They then validate blocks if they discover a block that can be added to the blockchain.

Validators get a reward -- or their stake increases -- proportionate to their bets based on the blocks added to the blockchain. Since the algorithm is incentive-based, it consumes less computational energy than PoW.

Despite this advantage, the PoS algorithm has a serious drawback. The mining capacity of a validator depends on the number of tokens they have, so a miner who starts with more coins gets more control over the consensus mechanism. Additionally, a few miners can purchase many coins, further diluting the mechanism and reducing the system's decentralization property.

- **Proof of Burn (PoB)**

  Proof of Burn (PoB) is being tested as a viable and sustainable alternative to PoW and PoS algorithms. PoB is like PoW, but it consumes much less computational energy. This is because its block validation process on the blockchain doesn't require computational resources or hardware. Instead, miners "burn" or invest coins in the blockchain to achieve consensus.

  Coins are sent to an address from where they can't be retrieved, rendering them inaccessible and useless. This demonstrates the miners' commitment to the network and gives them the right to mine new coins and validate new transactions on the network. The more coins a miner burns, the more mining power they have, which increases their chances of becoming the next block validator.

  Burning coins in PoB reduces the supply of coins and increases their value. It also improves the security of the network through an investment of burned coins.

- **Proof of Capacity**

  In the Proof of Capacity consensus, validators are supposed to invest their hard drive space instead of investing in expensive hardware or burning coins. The harder drive space validators have, the better their chances of getting selected for mining the next block and earning the block reward.

- **Public vs private blockchain**
  - **Public Blockchain**

    Public blockchains are open networks that allow anyone to participate in the network i.e., public blockchain is permissionless. In this type of blockchain anyone can join the network and read, write, or participate within the blockchain. A public blockchain is decentralized and does not have a single entity which controls the network. Data on a public blockchain are secure as it is not possible to modify or alter data once they have been validated on the blockchain.

    Some features of public blockchain are:

    High Security
    It is secure Due to Mining (51% rule).

    Open Environment
    The public blockchain is open for all.

    Anonymous Nature
    In public blockchain everyone is anonymous. There is no need to use your real name, or real identity, therefore everything would stay hidden, and no one can track you based on that.

    No Regulations
    Public blockchain doesn't have any regulations that the nodes have to follow. So, there is no limit to how one can use this platform for their betterment

    Full Transparency
    Public blockchain allow you to see the ledger anytime you want. There is no scope for any corruption or any discrepancies and everyone has to maintain the ledger and participate in consensus.

    True Decentralization
    In this type of blockchain, there isn't a centralized entity. Thus, the responsibility of maintaining the network is solely on the nodes. They are updating the ledger, and it promotes fairness with help from a consensus algorithm.

    Full User Empowerment
    Typically, in any network user has to follow a lot of rules and regulations. In many cases, the rules might not even be a fair one. But not in public blockchain networks. Here, all of the users are empowered as there is no central authority to look over their every move.

Immutable
When something is written to the blockchain, it cannot be changed.

Distributed
The database is not centralized like in a client-server approach, and all nodes in the blockchain participate in the transaction validation.

- **Private Blockchain**

A private blockchain is managed by a network administrator and participants need consent to join the network i.e., a private blockchain is a permissioned blockchain. There are one or more entities which control the network and this leads to reliance on third-parties to transact. In this type of blockchain only entity participating in the transaction have knowledge about the transaction performed whereas others will not able to access it i.e., transactions are private.

Some of the features of private blockchain are:

Full Privacy
It focusses on privacy concerns.

Private Blockchain are more centralized.

High Efficiency and Faster Transactions
When you distribute the nodes locally, but also have much less nodes to participate in the ledger, the performance is faster.

Better Scalability
Being able to add nodes and services on demand can provide a great advantage to the enterprise.

- **Permissioned model of blockchain**

  Permissioned blockchains are a mix between the public and private blockchains and support many options for customization.

  - **Advantages**

    Permissioned blockchain advantages include allowing anyone to join the permissioned network after a suitable identity verification process. Some give special and designated permissions to perform only specific activities on a network. This allows participants to perform particular functions such as reading, accessing, or entering information on the blockchain.

    Permissioned blockchains allow for many functions, but one most interesting to businesses is Blockchain-as-a-Service (BaaS)—a blockchain designed to be scalable for the needs of many companies or tasks that the providers rent out to other businesses.

    For example, say a business wants to improve transparency and accuracy in its accounting processes and financial reporting. It could rent blockchain accounting services from a BaaS provider. The blockchain would provide an interface where entries are made by end users and then automates the rest of the accounting processes. In this way, there are fewer errors and no way for other parties to alter financial data after it is entered. As a result, financial reports to management and executives become more accurate, and the blockchain is accessible for viewing and generating real-time financial reports. The business might choose to have its invoicing, payments, book-keeping, and tax reporting automated. Additionally, blockchain can prevent anyone with dishonest intentions from altering financial data or taking advantage of weaknesses in accounting processes.

  - **Disadvantages**

    The disadvantages of permissioned blockchains mirror those of public and private blockchains, depending on how they are configured. One key disadvantage is that because permissioned blockchains require internet connections, they are vulnerable to hacking. By design, some might use immutability techniques such as cryptographic security measures and validation through consensus mechanisms.

    While most blockchains are thought to be un hackable, there are weaknesses. Cryptocurrency theft occurs when a network is hacked into, and private keys are stolen. Permissioned blockchains also suffer this weakness because the networks that connect the users to the service depend on security measures that can be bypassed. User information can be stolen and accounts hacked into, similar to enterprise-level data breaches.

- ## Security aspect of blockchain

Blockchain isn’t perfect. There are ways that cyber criminals can manipulate blockchain’s vulnerabilities and cause severe damage. Here are four ways that hackers can attack blockchain technology.

Phishing attacks

Phishing is a scamming attempt to attain a user's credentials. Fraudsters send wallet key owners emails designed to look as though they're coming from a legitimate source. The emails ask users for their credentials using fake hyperlinks. Having access to a user's credentials and other sensitive information can result in losses for the user and the blockchain network.

Routing attacks

Blockchains rely on real-time, large data transfers. Hackers can intercept data as it's transferring to internet service providers. In a routing attack, blockchain participants typically can't see the threat, so everything looks normal. However, behind the scenes, fraudsters have extracted confidential data or currencies.

Sybil attacks

In a Sybil attack, hackers create and use many false network identities to flood the network and crash the system. Sybil refers to a famous book character diagnosed with a multiple identity disorder.

51% attacks

Mining requires a vast amount of computing power, especially for large-scale public blockchains. But if a miner, or a group of miners, could rally enough resources, they could attain more than 50% of a blockchain network's mining power. Having more than 50% of the power means having control over the ledger and the ability to manipulate it.