Blockchain Basic - Key Takeaways

Below you will find a number of key points from this course. Defined terms are underlined.

Week One: Defining a Blockchain

The blockchain technology supports methods for

- a decentralized peer-to-peer network
- a collective trust model among unknown peers
- a distributed immutable ledger of records of transactions.

Decentralization means the network operates on a user-to-user (or peer-to-peer) basis.

A **Distributed Immutable Ledger** means the data doesn't sit on one all-powerful server and the data stored in it cannot be deleted or edited

Transactions bring about transfer of value in Bitcoin Blockchain. The concept UTXO defines the inputs and outputs of such a transaction.

Once a block is verified and algorithmically agreed by the miners, it is added to the chain of blocks, viz., the blockchain.

An **Unspent Transaction Output (UTXO)** can be spent as an input in a new transaction.

The main operations in a blockchain are transaction validation and block creation with the consensus of the participants. Yet, there are many underlying implicit operations, as well.

A **Smart Contract** provides the very powerful capability of “code execution” for embedding business logic on a Blockchain.

Significant innovations such as smart contracts have opened up broader applications for blockchain technology. Private and permissioned- blockchains allow for controlled access to the blockchain, enabling many diverse business models.

In a **Private Blockchain**, access to the Blockchain is limited to selected participants.

Permissioned or Consortium Blockchain has the benefits of a public blockchain with allowing only users with “permission” to collaborate and transact.

Week Two: Ethereum Blockchain

Smart contracts add a layer of logic and computation to the trust infrastructure supported by the blockchain.

Smart contracts allow for execution of code, enhancing the basic value transfer capability of the Bitcoin Blockchain.

Solidity is the high level programming language code for writing smart contracts that run on EVM.

Ethereum Virtual Machine (EVM) is a special structure where code is deployed on after being translated into byte-code.

Accounts are basic units of Ethereum protocol: external owned accounts and smart contract accounts.

An Ethereum transaction includes not only fields for transfer of Ethers but also for messages for invoking smart contract.

Externally Owned Accounts, or EOA, are controlled by private keys.

Contract Accounts, or CA, are controlled by code and can be activated only by an EOA.

An Ethereum block contains the usual prev block hash, nonce, transaction details, but also details about gas (fee) limits, the state of the smart contracts and runner-up headers.

Transaction Validation involves checking the timestamp and nonce combination to be valid, and the availability of sufficient fees for execution.

Miner Nodes in the network receive, verify, gather and execute transactions.

Any transaction in Ethereum, including transfer of Ethers, requires fees or gas points to be specified in the transaction.

Gas Points are used to specify the fees instead of Ether for ease of comparison using standard values.

Miners are paid fees for security, validation, execution of smart contract as well as for creation of blocks.

Week Three: Algorithms and Techniques

Elliptic Curve Cryptography (ECC) family of algorithms is used in Bitcoin as well as Ethereum Blockchain for generating the key pair.

Rivest-Shamir-Adelman (RSA) is a commonly used implementation of public-private key in many applications, except Blockchains because of its need for a more efficient and stronger algorithm.

Hashing transforms and maps an arbitrary length of input data value to a unique fixed length value.

The following are two basic requirements of a hash function.

- make certain that one cannot derive the original items hashed from the hash value.
- make sure that the hash value uniquely represents the original items hashed.

A combination of hashing and encryption are used for securing the various elements of the blockchain. Private-public key pair and hashing are important foundation concepts in decentralized networks that operate beyond the trust boundary.

Asymmetric cryptography uses public-private key pairs to encrypt and decrypt data.

Week Four: Essentials of Trust

A **Merkle tree** is constructed by hashing paired data (the leaves), then pairing and hashing the results until a single hash remains

Proof of work is a protocol that has the main goal of deterring cyber-attacks such as a distributed denial-of-service attack (DDoS) which has the purpose of exhausting the resources of a computer system by sending multiple fake requests.

Well-defined processes for handling exceptions improve trust in the blockchain.

Forks are mechanisms that add to the robustness of the Blockchain framework.

Well-managed forks help build credibility in the blockchain by providing approaches to manage unexpected faults and planned improvements.

Soft fork and hard fork in the Blockchain world is like the release of software patches and new versions of operating systems respectively.

A **Soft Fork** is a fork where updated versions of the protocol are backwards compatible with previous versions.

A **Hard Fork** is a change of the protocol that is not backwards compatible with older versions of the client. Participants would absolutely need to upgrade their software in order to recognize new blocks.

Ommer Blocks contribute to the security of the main chain, but are not considered the canonical "truth" for that particular chain height.