Nicolas Neven
1/23/2022
ITP 356

Homework 1

**General Blockchain Concepts**

1. A data structure built using cryptography to link or "chain" blocks of data together.
2. Possibly to prevent blocks from being spam and filled with bogus data and transactions.
3. To reconstruct the initial data from the hash values is almost impossible. Having a collision where two separate inputs have identical hash values is also almost impossible. A small change in input data leads to drastically different output data.
4. It changes the hash value of the block header, "breaking" the chain.
5. More than 50% of the computing power of the network. For BTC miners and hash power.
6. Having money that is able to be spent twice.
7. The private key can be used to encrypt and decrypt the data. The public key can only be used to encrypt the data. To decrypt the data encrypted with a public key the private key must be used which is how they are related.
8. A digital signature (generated with public key encryption) is attached to a transaction to verify its contents and the sender's identity.
9. 1) Scalability trilemma 2) Not *everything* is better decentralized sometimes Web2 type architecture is perfectly applicable. 3) Maybe it could all be a huge hype bubble :(

**Ethereum Concepts**

1) Account model updates user balances while UTXO only records transaction receipts.
2) Wei, one ether = 10^18 wei.
3) Keeps track of how many transactions the sender has sent over time.
4) 2, *externally owned* is controlled by anyone with the private keys while *contract* is deployed to the network and controlled by code.
5) Programs on the blockchain that execute when certain conditions are met.
6) Code executes actions while storage is data being held and manipulated by the code.
7) Ethereum uses Merkle trees to securely verify a large amount of transactions in a block.
8) "An ommer is a block whose parent is equal to the current block's parents' parent.
9) V, r, s: values for a transaction's signature on the Ethereum blockchain.
10) State transitions are when values are changed and transferred between different accounts.

**Applied Ethereum**

1) The Ethereum Virtual Machine executes Solidity code and smart contracts.
2) No, instead it is computed from the address of the creator/sender/owners,
3) 1) Decentralized 2) Login with on-chain wallet address rather than KYC identity.

4) Web2 is centralized and uses traditional KYC identity rather than on-chain wallet address. Web3 is decentralized and uses blockchain technology as the backend.
5) Ether is the native token of the Ethereum blockchain and is spent to perform transactions or execute smart contracts via the EVM.
6) ERC-20 as an in-game token, rebasing game theory mechanism, incentive for community building and participation via airdrops. ERC-721 as tokenized real world assets.
7) You can still view the contract or data that was scrubbed via previous blocks of data. Means that it must have already been coded in the first place and thus viewable.

**Class Related**

1) Yes
2) Yes