6/11/2022

UNIT-I: BLOCK CHAIN BASICS

Basics of crypto economics - Blockchain - Cryptocurrencies over blockchain in Nut Shell : Benefits and challenges - Block chain types - Block chain peer to peer n/w : consensus mechanism - IJM proof of work, Proof of stack, mining layer, Propagation layer, semantic layer, application layer

CRYPTO ECONOMICS

→ Production, Distribution and consumption of goods and services in a decentralized digital economy

→ Crypto economics → design & characteristics of Protocols

Cryptoeconomics ← Cryptography
Economics

Peer to peer file system

→ torrent system - file sharing

failure - No incentives

Satoshi Nakemoto → Block chain

2008 → Paper → bitcoin → Crypto economics

Economics Incentives → "follow the rules"

↓

Consensus mechanism

CRYPTO ECONOMICS PROPERTIES:

① Block chain → Block → Hash, transition

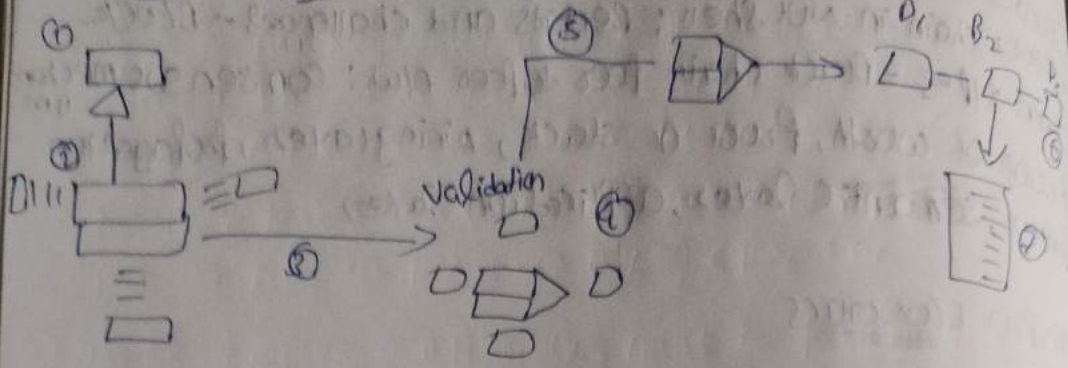
② Immutable

③ Valid transaction

④ Anywhere, Anytime, Anyone access & checks

⑤ Transcation fee

WORKING MODEL OF CRYPTO ECONOMICS: [★]



models:

① Transcation Request ② Transcation boocadcast ③ Transcation validation

④ Verification Process

↙

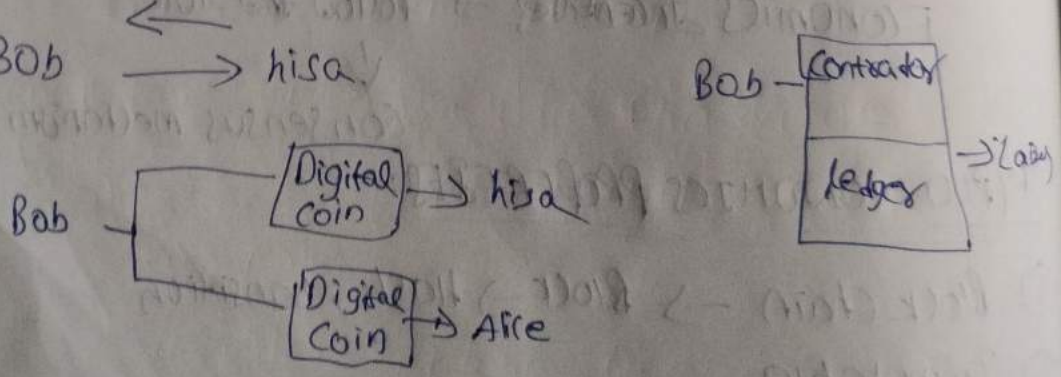
Authentication

Authorization

⑤ BLOCK FORMATION ⑥ Adding to the block

⑦ Transcation Complete

Emergence of Block Chain Double spending:



- digital transactions can solve double spending
- Validation, ~~further~~

Cryptocurrency, overlooked

History:

Barter System
- apple → orange
- coincide problem
- No common measure tive
- transport problem
- realized → cryptocurrency

Traditional currency ~~vs~~ Vs cryptocurrency:

- Technical issue
- DOS attack
- Transcation limit

Bit app.

- notification appears
- If Y=1 Proceed takes place
- Payment transferred

Public block chain: It is the permissionless distributed ledgers on which anybody can join and conduct transcation

=> It is a non-respective form of the ledgers in which peer has a copy this also means that anyone with the node internet can access the public block chain.

=> The user have access to historical and contemporary records and ability to perform mining operation.

=> These complex computations must be perform to verify transcation and add them to ledgers.

ADVANTAGES:

(i) Trustable [Proof of work] : knows do not need to know
(ii) Secure [Many users]
(iii) Open and transparent

USES:
VOTING
Fund Raising

DES Advantages:

(i) Scalability Issues
(ii) High energy consumption

PRIVATE BLOCK CHAIN: A NW operates in a private context such as a restricted nw (or) controlled by single identity

=> When it have a Similar peer to peer ~~P to~~ connection and while decentralization to the public block chain nw the block chain is far smaller

=> Permission block chains and business block chain are two more terms for them

→ they often run on small N/w with in organization

ADVANTAGES:	DISADVANTAGES	USES
1) speed	=> instability	1) supply chain management
2) scalability	=> lower security	2) Asset ownership
	=> centralization	3) Internal voting

HYBRID BLOCK CHAIN: Organization to expect the best of both users hybrid block chain which combines the features of private and public

=> It enables enterprises to construct the private permission based system along side the public permission less system allowing them to choose two who has access to block chain data and what data is made public

=> In hybrid b.c transactions and records are typically not made public but they can be validated by granting access via smart contract {Digital signatures}

ADVANTAGES:	DISADVANTAGE
=> secure {51% of attack}	=> lack of transparency
=> cost effective	=> less incentive

USES:

Real estate

Retail

highly regulated markets

CONSORTIUM BLOCK CHAIN: Same way like hybrid block chain has both private and public features.

=> It is also known as Federated block chain

=> However it differs bec it involves various organizational [illegible] working together on a decentralized N/w

=) Pre determined nodes control the consensus [mutual agreement] method in a consortium block chain

=) It has a validated nodes responsible for initiating, receiving, validating transcation

=) Transcations can be intiated or received by members nodes

ADVANTAGES:

=) secure

=) Scalable

=) EFFICIENT

DISADVANTAGES:

=) Lack OF transparency

USES:

=) Banking and Payments

=) Research

=) Food tracking

CONSENSUS: It means acheiving a state of decision on which N/w participants agreed

Ex: Goa trip

=) In order to avoid centeralization and confict among members the system requires consensus mechanism or algorithm

CONSENSUS MECHANISM:

=) the algorithm is made to keep N/w memebers synchoonized under democracy

=) the purpose of mechanism in decenteralized N/w is to allow a group of independent nodes to distribute right to update as well as the validate the change in a N/w equally.

HOW DOES Consensus work:

=) there is a no of consensus mechanism to operate on decentralized N/w

Each algorithm has a n/w update

=) Generally Conse N/w to agree system gets change by n

DIFFERENT TY

1. Proof of wo
2. Proof of St
3. Proof of
4. Proof of C
5. Proof of

1. POW: Pow either

Here mad Cha

The Rev

to

It us

Al to

Each algorithm has its own way reaching the global agreement on a new update

=) Generally Consensus Protocols form atleast 51% of Participants in N/w to agree on upcoming change. If they agree the n/w system gets updated with a new change else it rejects the change by mutual aggrement.

DIFFERENT TYPES OF CONSENSUS MECHANISM:

1. Proof of work:
2. Proof Of Stake
3. dedicated proof of stake
4. Proof of Importance
5. Proof of capacity
6. Proof of elpased time
7. Proof of activity
8. Proof of authority
9. Proof of burn
10. Bluigendent fault tolerant

1. POW: Popular Consensus algorithm used by bitcoin and ethereal N/w.

Here miners are block adder have to do heavy mathematical computations to find a right Hash by Changing Norms of the block.

The miners who finds the hash below the difficulty level gets to add his block to the n/w. Hence the chain takes the reward

It B PUZZle friendly way to reach consensus by using high computational power.

Afterwards already present N/w Participants, valid transcations in the block added by the miner.

2. POS: Eliminat of high energy consumption of POW

=) PoS uses a staking mechanism in which miners (or) validators, ~~exchange~~ some of their earned points in the N/W to get selected for adding the block.

=) It is not an initial consensus algorithm for the N/W. It can only implemented after a n/w has a good amount of participants (or) nodes

TYPES OF BLOCK:

1. Consensus block 2. Valid block 3) Orphan block

CONCEPTS:

1. Public distributed ledger 2. SHA 256 3) Proof of work

TYPES OF MINING:

1. Individual mining 2. Pool mining 3. Cloud mining

USES:

1. Validating TXNS 2. Confirming TXNS 3. Maintaining safe channels

layers Decomposition:

consensus - format of ledgers

Mining - incentivizes parties

Propagation - To maintain consensus, and add how ledgers and blocks are transmitted

Semantic - How new block relays to previous block

Application - Implement

CONSENSUS LAYER: Protocol that decides the format of a ledger
Publicly visible and consensus function that
anyone can use to determine which of multiple candidate ledgers
is the consensus ledger.

MINING LAYER - Protocol that incentivize parties to maintain
the consensus and add blocks to the ledger.

Propagation Layer: Protocol that describes how the ledger
and blocks are transmitted b/w the
nodes in the N/w.

SEMANTIC LAYER: Specification of how new blocks must relate
to previous block and protocol for verifying conformity
with the specification.

APPLICATION LAYER: application code that implements
some desirable functionality.

Properties

i) Security ii) Liveness iii) Stability

iv) Correctness

=> Blocks - Chain of blocks - Digital signature & hashing - Block data examples: Bitcoin block, Etherium block, Block time & block size, Global Size - blockchain mining & validations - B.C speed: Block Chain throughput & comparision with traditional n/w

BLOCKS:

=> Collection of authenticated Txn, Authenticity safeguarded by inspecting that fun provided in each Txn of signed the Txn cryptographically. This confirms that the fun provided for Txn had an entry to private key which could authorized over funds available

=> After the formation every block is hashed thus generating msg digest that signifies block. The block msg digest is utilited to assist in guarding block from alteration.

=> A block is complete, the data feeds comprising block typically consists of

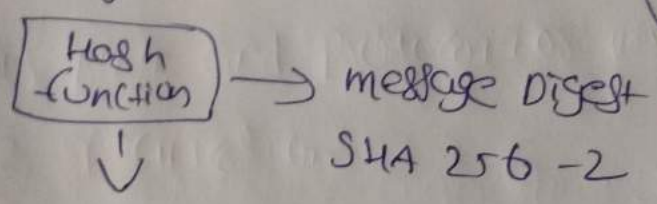
1. Block height (or) block number
2. Block hash value
3. Size
4. Prior block hash value
5. merkle tree root hash
6. time stamp
7. list of Txn
8. unique nonce value

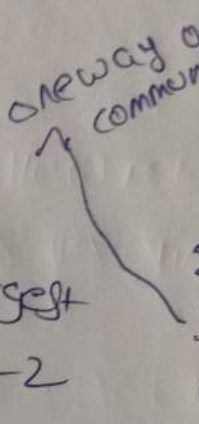
Cryptographically secured Hash function
Digital Signature

Hash function: Used to connect the "blocks" in a block chain in a tamper. proof works TAB any string as an input.

- Input m the message
- Fixed size output (we use 256 bit in block chain)
- Output H(m) - message Digest

* Efficiently compatabile





⊕ Reverse is not possible
⊕ Hashing is not encryption

→ S message
H(S) message divers

Digital Signature: Digitally Signed the data so that no one can deny about their own activities also others can check whether it is authentic

→ small change in data results in significiant change in the output called avalanche effect.

TYPES OF BLOCK CHAIN: (4) types

Public block chain: It is the permissionless distributed ledgers on which anybody can join and conduct transcation

⇒ It is a non-respective form of the ledgers in which peer has a copy this also means that anyone with the node internet can access the public block chain.

⇒ The user have access to historical and contemporary records and ability to perform mining operation.

⇒ These complex computations must be perform to verify transcation and add them to ledger.

ADVANTAGES:

(i) Trustable [Proof of work] : knows do not need to know

(ii) Secure [Many users]

(iii) Open and transparent

USES:

VOTING

Fund Raising

DIS Advantages:

(i) Scalability Issues

(ii) High energy consumption

PRIVATE BLOCK CHAIN: A NW operates in a private context such as a restricted nw (or) controlled by single identity

⇒ When it have a Similar Peer to Peer ~~N to~~ connection and while decentralization to the public block chain nw the block chain is far smaller

⇒ Permission block chains and business block chain are two more terms for them