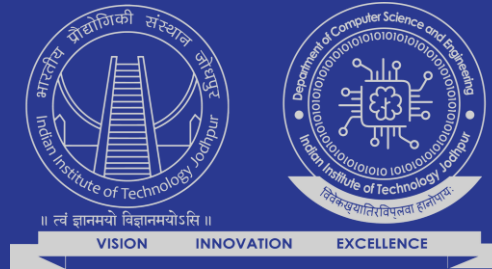


Bitcoin and Bitcoin NG

Department of Computer Science and Engineering

Indian Institute of Technology, Jodhpur



Presented By:

Dr. Debasis Das

Computer Science and Engineering Department

Indian Institute of Technology, Jodhpur



Applications Of Blockchain



Digital IDs



Bitcoin



Real estate



Voting



Payment and
Transfers



Health Care

Internet of Things



Online music

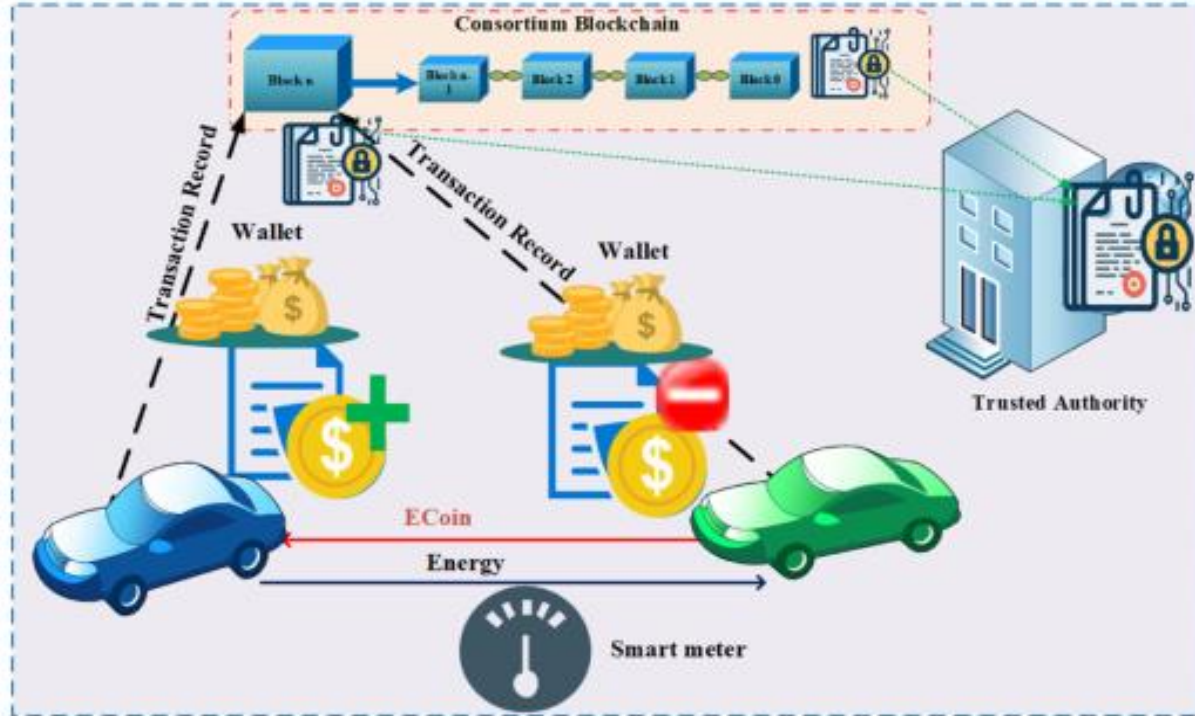


Banking

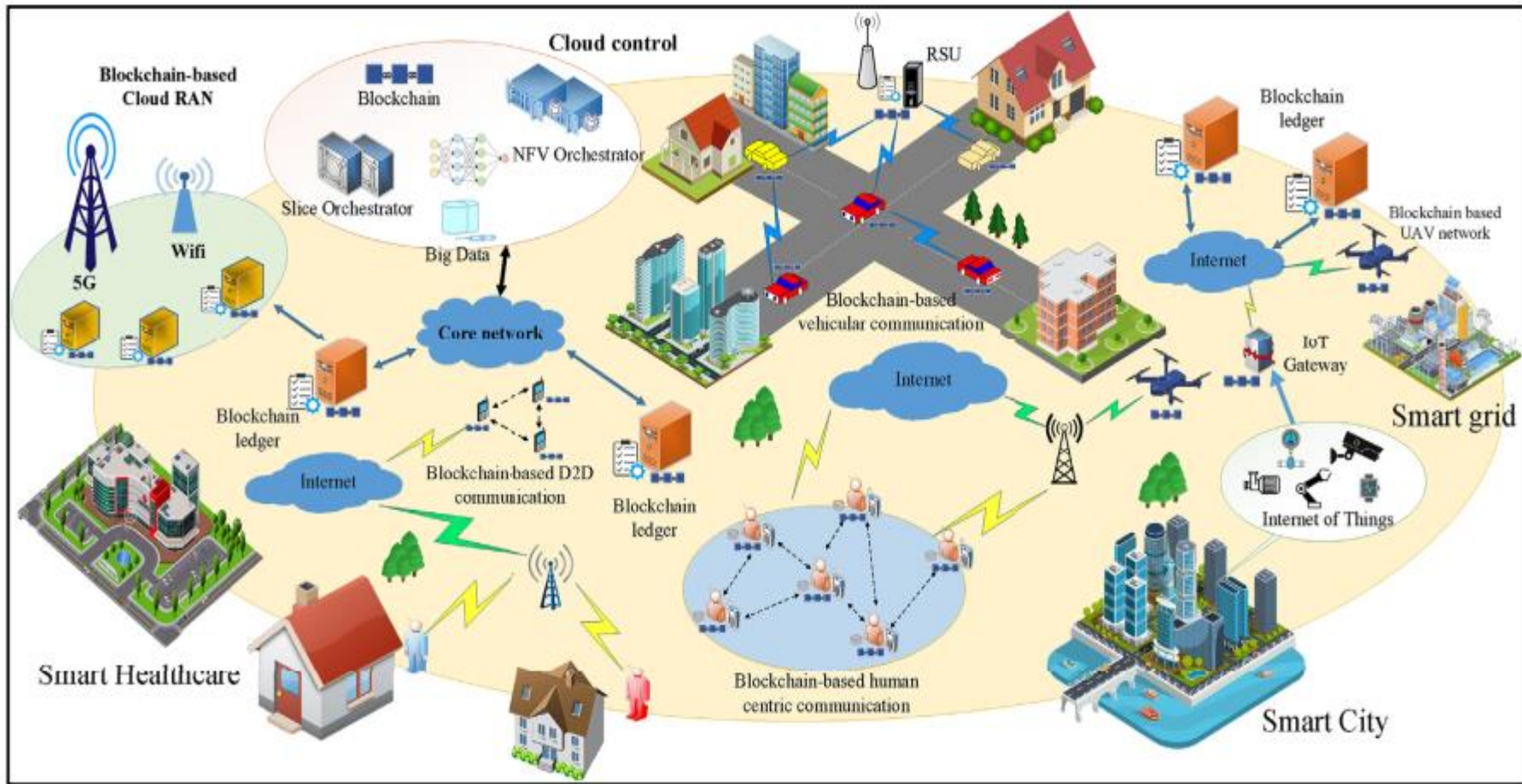


Law Enforcement


Framework of blockchain-enabled V2V energy trading



The convergence of blockchain and 5G

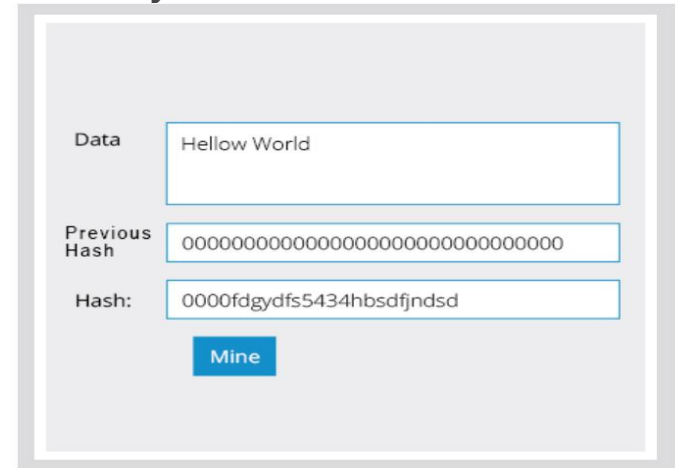


Use it as a quick reference

- **Smart contract**
 - self executing contract with terms and conditions written in lines of codes
 - **Solidity**
 - Programming language for writing smart contracts in Ethereum
 - **Hyperledger**
 - Blockchain platform
 - **Ethereum**
 - blockchain platform
 - **DApp**
 - Decentralized applications
 - **Mining**
 - The validation process in a blockchain (in Bitcoin and Ethereum)
- 

Data Structure of Blockchain

- The data in blockchain is stored as individual blocks, that's why it is called Blockchain. Just like a linked list, the Blockchain is a collection of blocks linked together. So what does the block actually contain? Each block in a blockchain will have the following fields

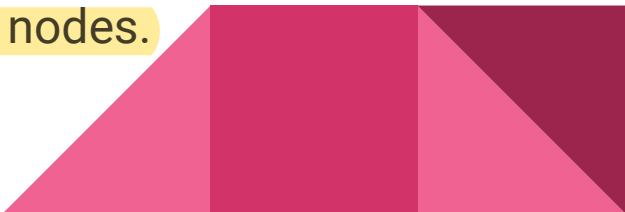


The image shows a form representing a blockchain block. It has three input fields and a button. The first field is labeled 'Data' and contains the text 'Hellow World'. The second field is labeled 'Previous Hash' and contains a string of 20 zeros. The third field is labeled 'Hash:' and contains the string '0000fdgydfs5434hbsdfjndsd'. Below these fields is a blue button labeled 'Mine'.

Data	Hellow World
Previous Hash	00000000000000000000000000000000
Hash:	0000fdgydfs5434hbsdfjndsd

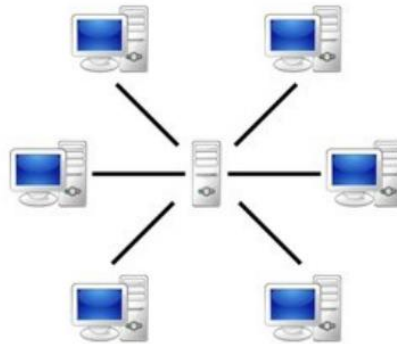
Mine

Data Distribution in Blockchain

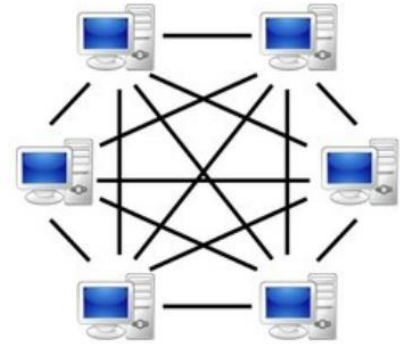
- We saw that blockchain has its own unique Data storage structure, the data distribution in a blockchain has also a different approach. They don't follow the widely adopted client server model.
 - The peer to peer data distribution approach gives the reason behind unfettered nature of Blockchain; there is no central authority to control.
 - Unlike the client-server model, In P2P network the data is stored in all the participant nodes in the network.
 - All the individual nodes will have the copy o the entire 'Blocks' and a single change in a particular block will be updated in all the nodes.
- 

Client-Server model and P2P Model

- But here is the problem, in Client-Server model the data is stored in DB after verification of a central authority; but in P2P network there is no central authority, then how does the authenticity of data assured?
- The answer is the validation process and consensus mechanism of the blockchain network.



Server-based




P2P-network

Block Validation

- The asset and its transactions are stored as **connected blocks** in blockchain. Only the **valid transactions** are added to the blockchain.
- In a blockchain, **all the blocks are added to the blockchain after validation only.**
- Whenever a transaction takes place in the blockchain it will be added to a block; sometimes **one transaction per block and sometimes several transactions per block.**
- It depends on the **block size and the nature of the network.**



Block Validators

- Block validators are the nodes which participates in the process of block validation.
 - The validators are rewarded for their effort, (In fact they are rewarded for the computational power they spent).
 - Different blockchain protocols adopt different methodologies for selecting the validator from available pool of nodes.
 - Some of the methods are described below:
 - PoW (Proof of Work)
 - PoS (Proof of Stake)
 - Proof of Activity
- 

PoW (Proof of Work)

- In PoW, the mining challenge is open to all.
- All the miners compete each other to add the next block.
- A fixed reward is given to the miner who finds the solution first.
- In fact, the node with more computational power usually wins the race.
- Bitcoin uses the PoW algorithm.



PoS (Proof of Stake)

- It is a common alternative of PoW. Here, the validators are chosen based on the fraction of coins they own in the system.
- The nodes with more number of coins have more chance to be selected than the node with lesser number of coins.
- In PoS the reward is in the form of transaction fee.
- Presently, Blackcoin, Ethereum and Peercoin blockchains uses the PoS algorithm.



Proof of Activity

- PoA is a hybrid approach and it is introduced to overcome some of the problems in PoS and PoW.
- In this method, the mining begins with PoW and at some point the process is switched PoS.



Blockchain So far

- According to prominent statistics websites, the blockchain market is expected to grow \$20 billion by 2024.
- In India, the Andhra Pradesh state government has started implementing the complete land registration through blockchain.
- There are much more other areas on the list. Like Voting, Healthcare, Forecasting, Transportation, Energy management, etc



Bitcoin Working

- The first thing we have to do is create an Account in Bitcoin blockchain.
- For that, the simplest way is to create a digital wallet. There is a number of wallet service providers like coinbase and BitCore.
- While creating an account the user has to provide a 'Key' (similar to a password).
- Using this key the wallet will generate a valid bitcoin Private key- Public Key pair.
- The public key will be visible to all and it is the visible account ID of the user.
- On the other hand, the user keeps the private key by himself, it is the access key to his account.
- If a person loses his private key he loses access to his account and his money.



Value of Bitcoin

- So a general question that may arise in anyone's mind is 'who determines the value (or more economically speaking exchange rate) of bitcoin.'
- As we know there is no central bank or any other designated agency to control it; then how the value is determined, or who determines it?
- The answer lays in the basic economics, which is **demand and supply.**



Value of Bitcoin

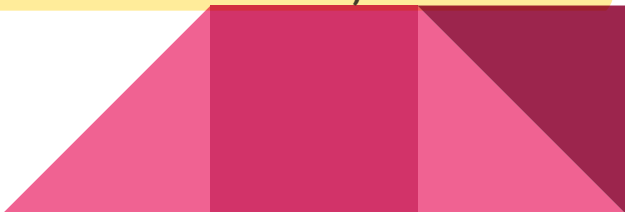
- **T : Total bitcoin transaction/second**
D : Duration that a BTC needed by a transaction
S : Supply of the bitcoin
P : Price of the bitcoin
We have
 S/D = Bitcoins available per Second
 T/P = Bitcoins needed per Second



Value of Bitcoin

- According to demand-supply rule, when the supply of the bitcoin increases the demand decrease consequently the price will also decrease.
- And when the demand increases the supply of bitcoin will also decrease, consequently the price of the bitcoin will also increase.
- At an equilibrium state, where the supply S over D, is equal to the demand T over P.
- We can deduce the price P as
$$S/(D)=T/P$$
- Equilibrium state:-
$$P=TD/S$$
- That is at equilibrium, the price should be equal to T times D divided by S.

Value of Bitcoin

- This is the very basic equation to calculate bitcoin exchange rate.
 - The value of the bitcoin basically depends on the demand and supply.
 - However, there are many other factors including public perceptions, mining difficulty level, energy consumption for mining process etc. that are taken into consideration while calculating the actual exchange rate.
 - So that there will be some slight variations in exchange rate across the different market.
 - It is evident that a single authority can't control the value of bitcoin, rather it is determined strictly based on the user transaction.
- 

Improvized Bitcoin

- However, due to high computational power and high consensus delay, current blockchain protocols, such as Bitcoin, are not suitable for working with lightweight IoT devices.
- However, protocols, such as Bitcoin-NG, are designed to reduce the consensus delay, but they still need high computational power and high energy.
- a new mechanism for blockchain to reduce the consensus delay, reduce energy consumption, and increase the throughput by introducing a new leader election scheme in the blockchain.

Bitcoin

Algorithm 1 Leader Election in Bitcoin

Result: LEADER_BITCOIN(Node,i,transaction)

```
1 nonce  $\leftarrow$  0 ;  
2 hash  $\leftarrow$  null ;  
3 while  $hash \geq difficulty$  do  
4   |  $nonce \leftarrow nonce + 1$ ;  
5   |  $hash \leftarrow calculatehash(transaction, nonce)$ ;  
6 end
```

Bitcoin-NG

Algorithm 2 Leader Election in Bitcoin-NG

Result: LEADER_NG(Node,i,leader,transaction)

```
1 nonce  $\leftarrow$  0 ;
2 hash  $\leftarrow$  null ;
3 if leader  $\neq$  i then
4   while hash  $\geq$  difficulty do
5     | nonce  $\leftarrow$  nonce+1;
6     | hash  $\leftarrow$  calculatehash(transaction,nonce);
7   end
8   return Node[i];
9 end
```

Modified

Algorithm 3 Leader Election Modified

Result: LEADER_MODIFIED(Node,n,i,cur,next,data)

```
1 nonce  $\leftarrow$  0 ;
2 hash  $\leftarrow$  null ;
3 if  $next = i$  then
4   while  $hash \geq difficulty$  do
5     nonce  $\leftarrow$  nonce+1;
6     hash  $\leftarrow$  calculatehash(data,nonce);
7   end
8   cur  $\leftarrow$  i;
9   next  $\leftarrow$  nonce % n;
10  return Node[cur];
11 end
```

SECURITY COMPARISON OF DIFFERENT ATTACKS

Types of Attacks	[27]	[35]	[42]	[43]	[44]	Proposed
Identification	✓	✓	✓	✓	✓	✓
Message integrity	✓	✓	✓	✓	✓	✓
Non-Repudiation	✓	✓	✓	✓	✓	✓
Sybil attack	✓	✓	✓	✓	✓	✓
Spoofing attack	✓	✓	✓	✓	✓	✓
Message replay attack	✓	✓	✓	✓	✓	✓
DoS/DDoS attack	✓	✓	✓	✓	✓	✓
Blockchain Modification	✓	✓	✓	✓	✓	✓
Man-in-Middle attack	✓	✓	✓	✓	✓	✓

✓✓✓ COMPARISON OF BLOCKCHAIN PROTOCOLS

Protocol	Leader Election	# of Nodes	Consensus Time	# of Operations
✓ Bitcoin	Proof of Work	All	10 min	<i>Highest</i>
✓ Bitcoin NG	Key Block	All	3 min	<i>Lesser</i>
✓ Modified	Nonce Hash	1	3 min	<i>Lowest</i>

THANK

YOU