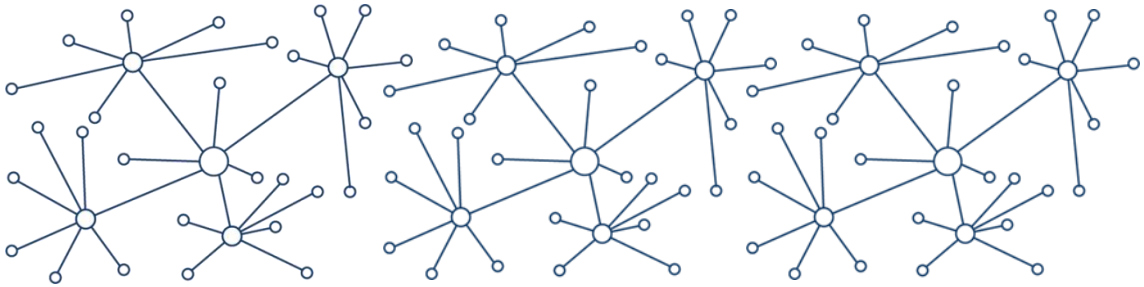


Blockchain Technology

Core Elective 3 – CS423

B. Tech. IV CSE 7th Sem

Lecture#7 and 8 (30 Aug 2022)

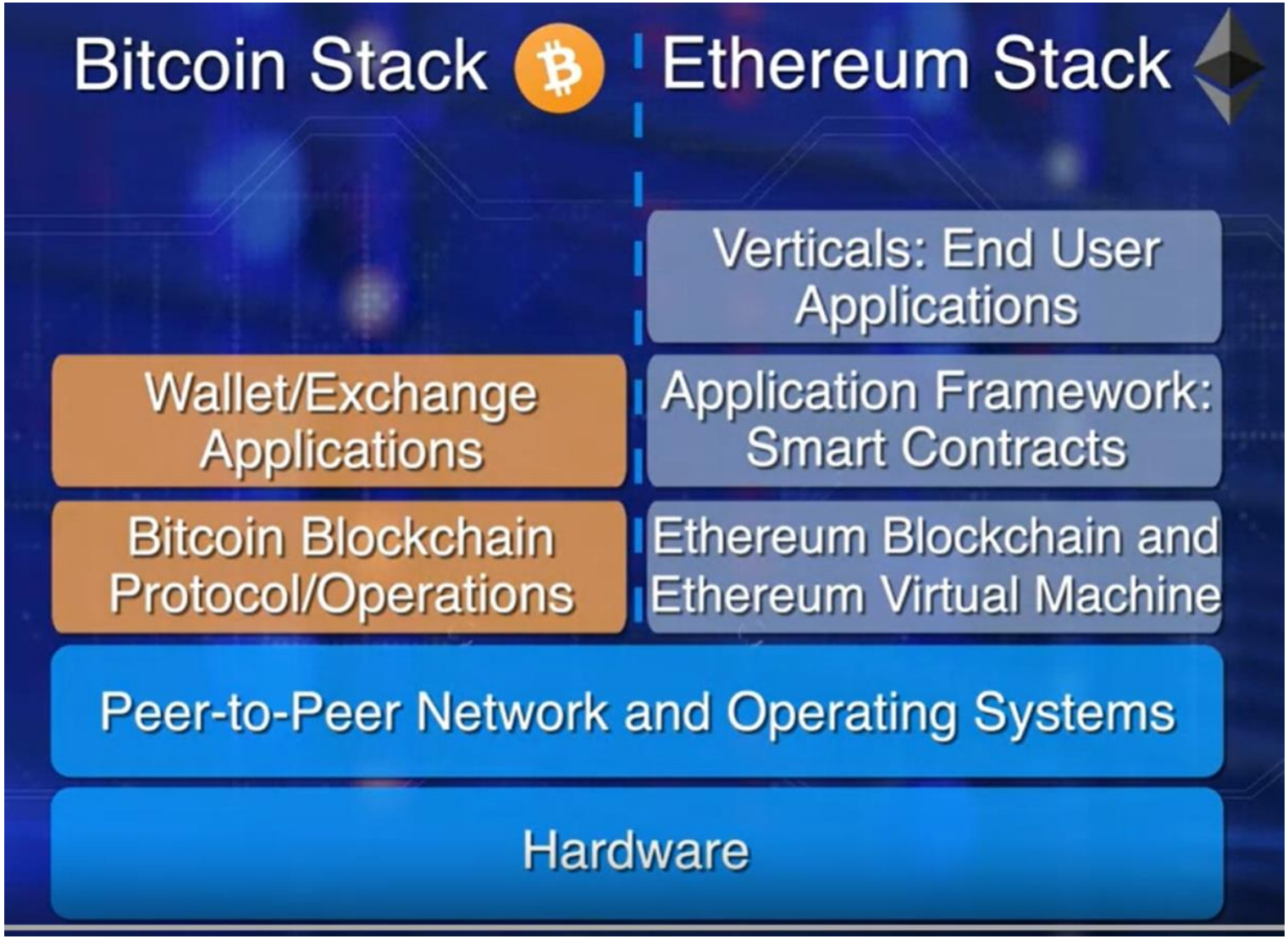
Ethereum

Dr. Dhiren Patel

Ethereum

- Bitcoin blockchain is the mother of all blockchains. (2009)
- It was intended for peer to peer transfer of value and it does that well. ((Digital currency transfer request simple addition and subtraction)
- Around 2013, a framework for code execution was introduced by Ethereum Founders.
- The centerpiece and thrust of this Ethereum blockchain is a smart contract.

Comparison –
Bitcoin v/s Ethereum Blockchain



Smart contracts

- Ethereum supports smart contracts and of virtual machine on which smart contracts execute.
- Smart contracts in turn enable decentralized application that accomplish more than a transfer of value.
- E.g. Efficient automation of decentralized application such as supply chain.

Objectives

- Smart contracts
- Ethereum blockchain protocol – elements and operations
- Concept of gas - the fuel or the payment model for code execution and the incentive model for the Ethereum blockchain.

Smart contract

- A smart contract is a piece of code deployed in the blockchain node.
- Execution of a smart contract is initiated by a message embedded in the transaction.
- Ethereum enables transaction that may carry out more sophisticated operations.
- For example, a transaction could require a conditional transfer,
- it may require some evaluation,
- it may need more than one signature for transfer of assets,
- or it may involve waiting for a specific time or date.

Smart contract

- Structurally, a smart contract resembles a class definition in an object oriented design.
- It has data, functions or methods with modifiers public or private,
- along with getter and set of functions.
- Specific programming languages have been designed for coding smart contracts.
- Solidity is one such language.

Smart contract example

- An auction bidding smart contract could execute this logic -
- If the age of a bidder is greater than 18 and the bid is greater than the minimum bid,
- then, accept the bid,
- or else reject the bid.

Ethereum Virtual Machine

- Every node in Ethereum network should be able to execute the code irrespective of that underlying type of hardware or operating system.
- Enter Ethereum Virtual Machine, EVM.
- An EVM provides a run anywhere abstraction layer for the contract code.
- A smart contract written a high level programming language is translated into EVM byte code, and then, deployed on the Ethereum Virtual Machine, EVM.

Smart contracts

- smart contracts add a layer of logic and computation to the trust infrastructure supported by the blockchain.
- Smart contracts allow for execution of code.
- The code for this smart contract is written in a high level language like Solidity and compiled into byte code.
- The code for the smart contracts is executed on a special structure known as Ethereum Virtual Machine.

What are Smart Contracts?

- A smart contract is a self-executing digital agreement that enables two or more parties to exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the need for a third party.

Smart contract

- With smart contracts, you drop a bitcoin or ether into the vending machine (i.e. ledger), and your escrow, deed, contract, goods, driver's licence, or whatever the contract is for, simply drops into your account.
- The smart contract does all the work to determine whether the conditions of the order were satisfied.
- Smart contracts both define the rules and penalties around an agreement in the same way that a traditional contract does, and also automatically enforces those obligations.

Smart contract

- Smart contracts are verified, executed, and enforced by a computer program that runs on a blockchain network. When both parties involved in the smart contract agree to its terms, the program will automatically execute.
- This eliminates the need for a third party, as the contract is verified and enforced by the blockchain network.
- Because smart contracts are executed by code rather than people, they remove the possibility of human error and can automate many tasks that would traditionally require human interaction.

Smart contract

- In a smart contract approach, an asset or currency is transferred into a program and the program runs this code and at some point it automatically validates a condition and it automatically determines whether the asset should go to one person or back to the other person, or whether it should be immediately refunded to the person who sent it or some combination thereof.
- the decentralized ledger also stores and replicates the document which gives it a certain security and immutability

DeFi

- Decentralized finance is an exit from traditional banking services and norms.
- Smart contracts in DeFi are facilitating the exchange of goods, services, data, funds and so on. Users of centralized financial institutions, such as banks and credit unions, rely on intermediaries to execute a transaction. Whereas, DApps are using smart contracts to ensure that each action is genuine, transparent, and free of human error.

NFTs

- the Market cap of NFTs is closing in at a whopping $40.9 billion in 2021 as they turned out to be the most successful use-case of smart contracts.
- A smart contract is a tool that allows implementing a sale agreement between the NFT owner and the buyer. The smart contract contains information on the NFT, such as the work's creator, other parties who are entitled to royalties each time the NFT is sold, and the work's ownership history.

NFTs

- The majority of NFTs are not recorded on the blockchain since keeping so much data on the blockchain is both costly and energy intensive.
- As a result, smart contracts frequently include a link to the work they represent, which can be viewed by only the owner.

Supply Chain

- “UPS can execute contracts that say, ‘If I receive cash on delivery at this location in a developing, emerging market, then this other [product], many, many links up the supply chain, will trigger a supplier creating a new item since the existing item was just delivered in that developing market.’”
- supply chains are hampered by paper-based systems, where forms have to pass through numerous channels for approval, which increases exposure to loss and fraud. The blockchain nullifies this by providing a secure, accessible digital version to all parties on the chain and automates tasks and payment.

Autonomous cars

- One example is the self-autonomous or self-parking vehicles, where smart contracts could put into play a sort of ‘oracle’ that could detect who was at fault in a crash; the sensor or the driver, as well as countless other variables.
- Using smart contracts, an automobile insurance company could charge rates differently based on where, and under which, conditions customers are operating their vehicles.

Real estate

- A decentralized solution can help cut your costs. All you do is pay via cryptocurrency and encode your contract on a smart contract.
- Everyone sees, and you accomplish automatic fulfilment.
- Brokers, real estate agents, hard money lenders, and anyone associated with the property game can profit.
- Smart contracts are revolutionary in terms of transforming the current real estate practices.

Real estate

- All the parties including the bank, the agent, and the mortgage lender can sign an agreement via smart contracts.
- Because transactions are kept on a blockchain, this shared ledger enables the parties involved to look over the process at any moment and from anywhere.

Autonomy (Benefits of Smart Contract)

- You're the one making the agreement; there's no need to rely on a broker, lawyer, or other intermediaries to confirm.
- Incidentally, this also knocks out the danger of manipulation by a third party, since execution is managed automatically by the network, rather than by one or more, possibly biased, individuals who may err.

Benefits of Smart Contract

- Trust
- Your documents are encrypted on a shared ledger. There's no way that someone can say they lost it.
- Backup
- Imagine if your bank lost your savings account. On the blockchain, each and every one of your friends have your back. Your documents are duplicated many times over.

Problems?

- Much like what happened with The DAO hack in 2016, a mere loophole in a smart contract resulted in the biggest heist of the crypto market.
- Had that loophole been addressed earlier, it could have been prevented.
- But here's the catch, because you can track every movement on a blockchain, the minute the stolen ether/ETH enters circulation, those behind the heist will be exposed. So all that stolen crypto is as good as nothing.

Human Errors and Bugs in programming

- A simple human-error in writing a smart contract compromised its safety. To prevent that, you will need the right developers who could write a fool-proof smart contract.
- Automated contracts are not only faster and cheaper but also avoid the errors that come from manually filling out heaps of forms

Smart Contracts are not Perfect

- What if bugs get in the code? Or how should governments regulate such contracts? Or, how would governments tax these smart contract transactions?
- Smart contracts are not reversible, meaning that if there is a problem with the contract, it can be difficult or impossible to fix.

Problems??

- Smart contracts theoretically can be subject to downtime and outages, although Ethereum has proven incredibly reliable, newer smart contract networks like Solana have experienced a few outages as the technology is still very much in development
- Smart contracts can be costly to develop and require a high level of technical expertise.
- Smart contracts are not always customizable, meaning that they may not be suitable for all businesses or transactions.