upGrad

#LifeKoKaroLift

Introduction to DeFi

upGrad

Course: PGD Software Development (Blockchain)

Lecture On: Introduction to DeFi

Instructor: Jitender Bhutani

upGrad

Topics covered in the previous class...

1. Ethereum Blockchain
2. Smart Contract
3. ERC20 Token
4. Ethereum Wallet
    a. Metamask

upGrad

Module Map

- **Session 1 : Understand the Architecture of DeFi Application**
- Session 2 : Develop DeFi App Smart Contract
- Session 3 : Develop DeFi App Backend
- Session 4 : Further scope
  - Frontend
  - Upgradable smart contract
  - Administration
  - Scalability

upGrad

Today's Agenda

- What is DeFi?
- Centralized vs Decentralized
- Discuss live use cases
  - Uniswap
  - Aave
  - MakerDAO
  - Compound
  - Binance
- DeFi app architecture

upGrad

CENTRALIZED FINANCE

CENTRALIZED FINANCE

upGrad

- Governed by the **rules** that are defined by a central authority
- **Funds** are managed by **single** entity running the system
- Standard for cryptocurrency **exchanges**
  - Example
    - Binance
    - Wazirx
    - Zebpay
- Cryptocurrency exchange define
  - Which **coins** to be **listed** for trading
  - How much **fees** you need to pay for trading
  - Minimum and maximum **limits** for trading

upGrad

Where is the problem?

PROBLEM

upGrad

- Since there is lack of **transparency**
  - **Fraud** and **hack** can happen, which can lead to **loss** of user **funds**
- Often **manual errors** can lead to big losses
- Example:
  - **Mt. Gox** announced in Feb 2014 that around **850,000 bitcoins** were missing and most likely stolen
  - Evidence concluded that most of the **bitcoins** were stolen from Mt. Gox **hot cryptocurrency**
- Lot of other cryptocurrency **exchanges** got hacked over time leading to loss of user funds

upGrad

SOLUTION
DECENTRALIZED FINANCE

SOLUTION - DEFI

upGrad

- User need **transparency** in the system in order to build the trust
- User wants to manage their **funds** by their own
- **Automation** can eliminate manual errors
- **Accessible** throughout the world with no boundaries
- Figure out what makes **DeFi different** from the **traditional** financial system?
    - At their core, DeFi and their associated business processes are not **managed** by a company, institution, or an individual.
    - Instead, the processes are all **automatic**, and the associated **rules** are hardcoded in the **smart contract**.
    - Here, they are visible to all and **transparently** is represented in the form of **code**.

WHAT IS DeFi?

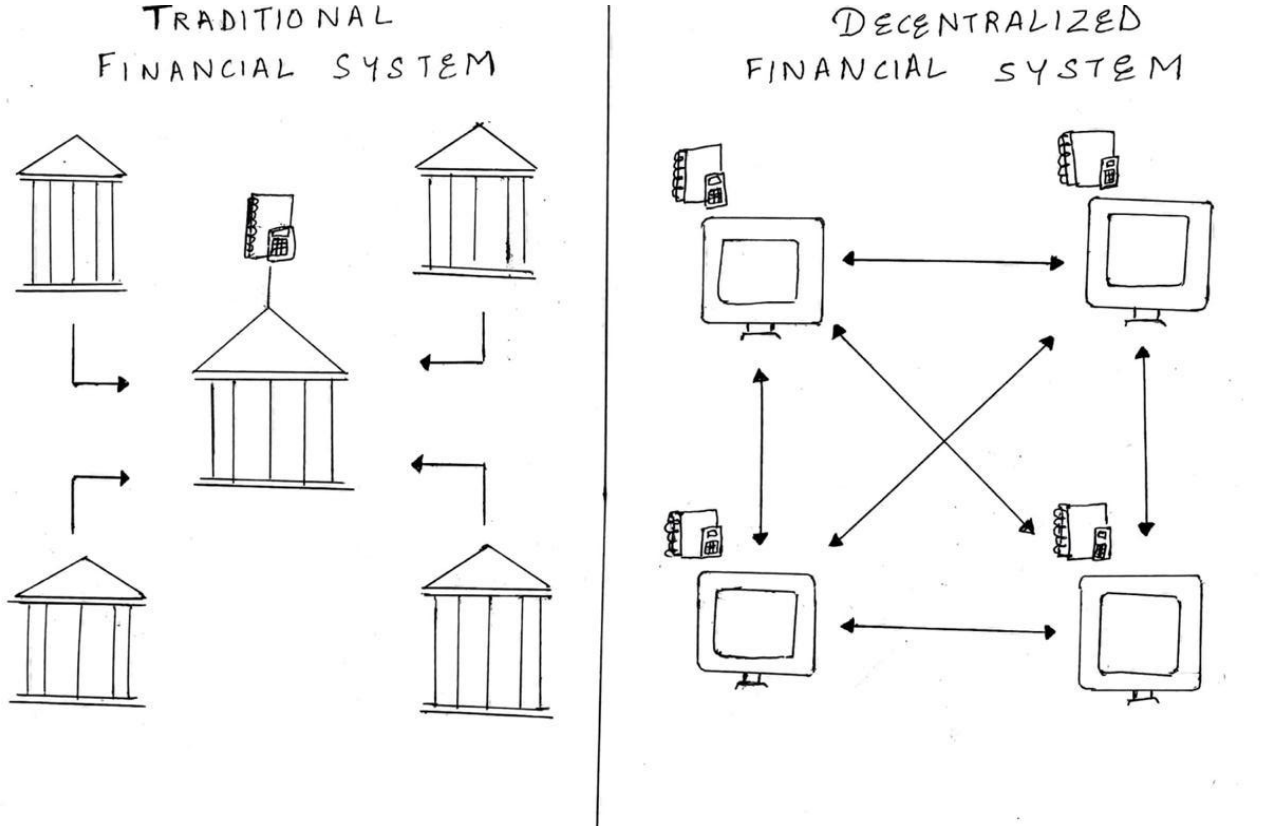
WHAT IS DeFi?

upGrad

- DeFi is short for **Decentralized finance**
- Needless to say
  - DeFi is an ecosystem of financial applications developed using the **Blockchain technology**
  - It operates on transactions without allowing **any third-party interventions**
- Business logic is written in **smart contracts**
- Primarily, the **Ethereum** blockchain is used for this purpose

WHAT IS DeFi?

upGrad



WHY DeFi?

upGrad

- **Accessibility**
  - Anyone in this world with an internet connection can start using DeFi technology. Moreover, the barrier is usually getting **money out** of government-issued 'fiat' money and into crypto.
  - Fortunately, now this is becoming even easier thanks to payment gateways, such as those available in Argent.

- **Ownership**
  - Because the Ethereum blockchain is decentralized , there is no **central authority** who can block your transactions. You can always retain full control over **assets** like crypto, property, etc.

WHY DeFi?

upGrad

- **Autonomy**
  - Because the Ethereum network is fully decentralized, it is resistant to being shut down by the **governments** as every node in the network has a full copy of the blockchain so they can validate transactions.
  - This implies that the network is **tamper-resistant**, making it very hard for anyone to modify the transaction record.

- **Transparency**
  - While some of the traditional banks have been embracing the '**open banking'** movement, and the 'open finance' model is already built-in to DeFi. Every transaction is visible on the blockchain, verified by other users
  - Fraudulent transactions and **bad actors** can be captured
  - End users can trust the system as the smart contracts can be verified publically

WHY DeFi?

upGrad

- One advantage of this is that there is less **'asymmetry'** in information between market makers (pro traders) and everyday users.
- It's also easy to check how much a protocol is being used, and what the **current loan rates** are at a glance.

- **Innovation**
  - Whenever you use DeFi, you are taking part in a global experiment that is changing the world of finance.

WHY WOULD YOU USE DeFi?

upGrad

- **Don’t** have **access** to the **banking** or financial services
- Want to **invest** in assets but don’t have time to go with all the **paperwork** and institutional providers
- Have some **cryptos lying around** and want to earn some interest without risk
- Want to **experiment** a bit with new technology and appear smart in a bar

RISKS IN DeFi?

upGrad

- **Three** most common types of risks of DeFi include
  - Technical Risk
    - API
    - Race conditions
    - Exception handling
    - Memory Safety
    - Testing Errors
  - Procedural Risk
    - Relate to the users and methods they usually follow for using the DeFi products or services that can compromise security
  - Financial Risk
    - Objectives of an individual or organization
      - Risk tolerance

POPULAR APPS

upGrad

- **Compound** is a borrowing and lending platform thet offers rewards for anyone that borrows or supplies assets on the platform (Liquidity mining)
- **Aave** is a lending protocol, and it allows collateralized loans, “rate switching”, flash loans and other unique collateral types.
- **Uniswap** is a Decentralized exchange where users provide liquidity for the swaps and earn fees from swaps
- **MakerDAO** is like a credit facility that issues loans with a certain interest rate
- **dYdX** is a decentralized margin trading platform and it allows users to lend, borrow, and make bets on the future prices of cryptocurrencies

SO WHAT YOU CAN DO WITH DeFi?

upGrad

- Same things you do with your money and other finances, but the main difference is that you don't have to rely on the banks or financial companies and you don't have to deliver any **proof**
- You don't even need an **ID** or aproofs. Everything can be done online with smartphone and computer.
- All these proofs and the trust is made by blockchain technology and you don't need any **middle-men** for verifications.

ADVANTAGES

upGrad

- **Avoiding human error and mismanagement**
  - The financial **crises** were mainly due to the mismanagement of central banks and also the **third party intermediaries**. But due to smart contracts, human error is removed from the process; unless the contracts themselves are written properly.
- **Quick and also permanent access**
  - Before the DeFi technology, if you wanted to get a loan, you would have to go to the bank and a **lot of time would be wasted**. but now with DeFi, you can get your loan with just click of a button. We just require good internet connection to access the market from anywhere in the world at any time.

ADVANTAGES

upGrad

- **Permissionless**
  - In our centralised financial system, you have to get permission from an external intermediary to carry out any financial operation. But in DeFi, we can have **permissionless operations.**
- **Transparency**
  - It can help people identify and avoid potential **financial scams** and also avoid harmful business practices. As the ledger is available to every node in the blockchain network.
- **Immutability**
  - Eliminate **bad actors**
  - Eliminate **fraudulent** transactions

DISADVANTAGES

upGrad

- **Scalability**
  - The biggest issue with DeFi is the **lack of speed** when it comes to trading because users send their coins or tokens through blockchain, which may take many minutes or more
  - Transactions are extremely **expensive** at times of congestion
- **Uncertainty**
  - If something goes wrong, then there is no central authority that would protect you, since no one controls the system. So you can't run to your financial manager and claim your money back or complain
  - It's still an experimental technology. At the end of the day, you trust everything in technology which can be **buggy, unstable** and unpredictable. You have to know that when the smart contract is executed, there is **no way back**

DISADVANTAGES

upGrad

- DAO Attack
  - Decentralized autonomous organization iwas as an investor-directed venture capital firm.
  - After raising a huge amount that is **$150 million** worth of ether (ETH) through a token sale, The organization was **hacked** due to **vulnerabilities** in its **code**.
  - Hackers managed to drain more than 3.6 million ether into a “child DAO” that has the exact same structure as The DAO.
  - Resulted in Hard Fork

DISADVANTAGES

upGrad

- **Smart Contract Problems**
  - Contract vulnerability is a major issue for many Decentralized Finance projects. If there is the **slightest bug** in the code of any smart contract, it may result into loss of huge amount of funds.
- **Low Interoperability**
  - There are several types of blockchains such as Ethereum, Bitcoin, Binance Smart Chain. And each of these with its own ecosystem and community. Interoperability enables DeFi platforms, DApps, tools, and smart contracts on different blockchains to communicate and interact with each other. And until this problem of low interoperability is resolved , many projects are isolated.

ROADMAP FOR IMPROVEMENTS

upGrad

- ETH 2.0
  - Consensus : Proof Of Stake
  - ETH 2.0 will introduce **shard** chains that will boost its **capacity** and **scalability** significantly.
  - Shard chains will act as additional lanes that will enable **simultaneous** rather than the **consecutive** processing of transactions. This will help in increasing speed and scalability.
  - This will help Ethereum to handle more transactions per second (**TPS**) because of parallel processing.

SUMMARY

upGrad

- If you are passionate about blockchain industry, it will be a good choice to pay attention to the growth and adoption of anything related to Decentralized Finance.
- Many projects and platforms are coming up with innovations and useful products that are willing to innovate the centralized finance. The DeFi industry is here to stay and will perhaps revolutionise the world
- Not without reason, DeFi is currently one of the fastest-growing sectors in the crypto field. More than $600 million worth of cryptocurrencies have already been invested in smart contracts in question, and thus in infrastructure.

upGrad

CENTRALIZED VS DECENTRALIZED

CENTRALIZED VS DECENTRALIZED

upGrad

Parameters	Centralized	Decentralized
Fund Management	Custodial	Non Custodial
Permission	Permissioned (KYC)	Permissionless (No KYC)
Trust	Trust Financial Organization	Trust Smart Contract
Transparency	No	Yes
Fiat Conversion	Yes	No
Cross Chain (Interoperability)	Yes	No
Stablecoins	Yes	Yes

CENTRALIZED VS DECENTRALIZED

upGrad

Parameters	Centralized	Decentralized
Trading	Yes	Yes
Lending	Yes	Yes
Payments	Yes	Yes
Borrowing	Yes	Yes

FUND MANAGEMENT

upGrad

- **Custodial**
  - Centralized cryptocurrency exchanges hold users **funds**. From which they would be able to perform their activities of trading, lending, staking etc
- **Non Custodial**
  - DeFi empowers people to independently manage their **funds** without the need of a central system. Users own and control their private keys

Poll 1 (15 seconds)

Which of the following property(s) regarding DeFi is/are true? (More than one option may be correct)

A. Custodial

B. Permissionless

C. Fiat Conversion

D. Smart Contract Based

E. Cross Chain Support

Poll 1 (15 seconds)

Which of the following property(s) regarding DeFi is/are true? (More than one option may be correct)

A. Custodial

B. Permissionless

C. Fiat Conversion

D. Smart Contract Based

E. Cross Chain Support

upGrad

USE CASES

USE CASES

upGrad

- Binance
- Aave
- Uniswap
- MakerDAO
- Compound
- StableCoins
- dYdX

AAVE

upGrad

- Aave is a lending protocol, and it allows collateralized loans, “rate switching”, flash loans and other unique collateral types
- Aave is a DeFi platform for lending and borrowing assets. In our traditional finance world, lending and borrowing often involves a third party such as a bank, but Aave changes this process. Because the protocol is decentralized, no third party is involved, and it’s permissionless — anyone can participate.
- It also has testnet for developers
    - https://testnet.aave.com/

upGrad

AAVE TESTNET DEMO

MakerDAO

upGrad

- **MakerDAO** at its core, uses Ether as a collateral to generate DAI which is a USD-pegged stablecoin
- Unlike the traditional loans, people won't be needing **credit history** now, or any bank account. Any user which has a compatible wallet and and Ethers to spend, can generate DAI using Ether(ETH) as collateral.
- MakerDAO's DAI is fully decentralized and all transactions can be tracked and validated on the blockchain. This avoids many issues like trouble getting bank accounts and non-transparency.

MakerDAO

upGrad

- Any user of MakerDAO can validate and examine the blockchain to check if the ETH that is locked up is enough to **collateralize** DAI in circulation.
  .
- Users can check the current interest rates, current prices, government decisions etc. And by buying some MKR tokens, they are allowed to participate in the governance themselves

UNISWAP

upGrad

- **Uniswap** is a Decentralized exchange where users provide liquidity for swaps and earn fees from swaps
- Users log onto the uniswap website and can trade directly through their wallet like metamask or any other crypto compatible wallet.
- With better UX, good exchange rates, **no registration**, **no withdrawal fees(**besides gas fees) requirement, it can be considered as an efficient decentralized exchange platform

COMPOUND

upGrad

- **Compound** is a borrowing and lending platform offering rewards for anyone that borrows or supplies assets on compound (Liquidity mining)
- Compound does not hold funds **custodially**. Moreover, Smart contracts holds the cryptocurrency and funds.
- Compound has a smart-contract-based money market. All the loans by the users are pooled into these markets. And this approach of liquidity pool, allows Compound to provide good liquidity on each of the coin it supports

BINANCE

upGrad

- https://www.binance.org/
- Binance Smart Chain is an extension to Binance Chain. With the dual chain architecture, both chains are complementary - Binance Smart Chain is built for running smart contracts on blockchain and caters to dApps without congesting the original chain(Binance Chain) which is optimized for ultra-fast trading.
- These features make it very efficient and optimized for running dApps, DeFi applications and transacting at a lower fee.
- Applications
  - DEX (https://www.binance.org/en/trade/TWT-8C2_BNB)
  - Staking (https://www.binance.org/en/staking)

dYdX

upGrad

- **dydx** platform helps to integrate lending with a **Decentralized Exchange** to create a fully decentralized exchange with leverage. The other use cases like Compound lets you earn interest on your crypto and dexes like forkdelta allows trading cryptocurrency trustlessly, dydx does all of it.
- Users are allowed to deposit their funds, which will help them start earning interest automatically, and then can use those funds to trade, with or without the margin.

UNDERSTAND DEFI APP ARCHITECTURE

WHICH BLOCKCHAIN TO USE?

upGrad

- Public or Private Blockchain?
  - **Public Blockchain**
    - Permissionless
      - Anyone can Read/Write
    - Decentralized
    - Transaction fee
  - **Private Blockchain**
    - Permissioned
      - Authorized entities can Read/Write
    - Partially Centralized
    - Transaction can be free
- Public blockchains are more suitable for DeFi as it is more available for end users

WHICH BLOCKCHAIN TO USE?

upGrad

- Also blockchain should have **smart contract** compatibility
  - To write DeFi business logic
- Blockchain should not be vulnerable to **attacks** like **51% attack**, i.e it needs good mining community
- Blockchain should have less transaction **fee** as there will be lot of transaction and users have to pay the fee from their wallet
- **Bitcoin** can not be used as it does not have smart contract capability
- Either **Ethereum** or **Binance** Chain (Fork of ethereum) can be used for DeFi
- Both supports **solidity** programming language for smart contract
- Since **Ethereum** has good community support and completely **decentralized**, it becomes the most obvious choice for DeFi

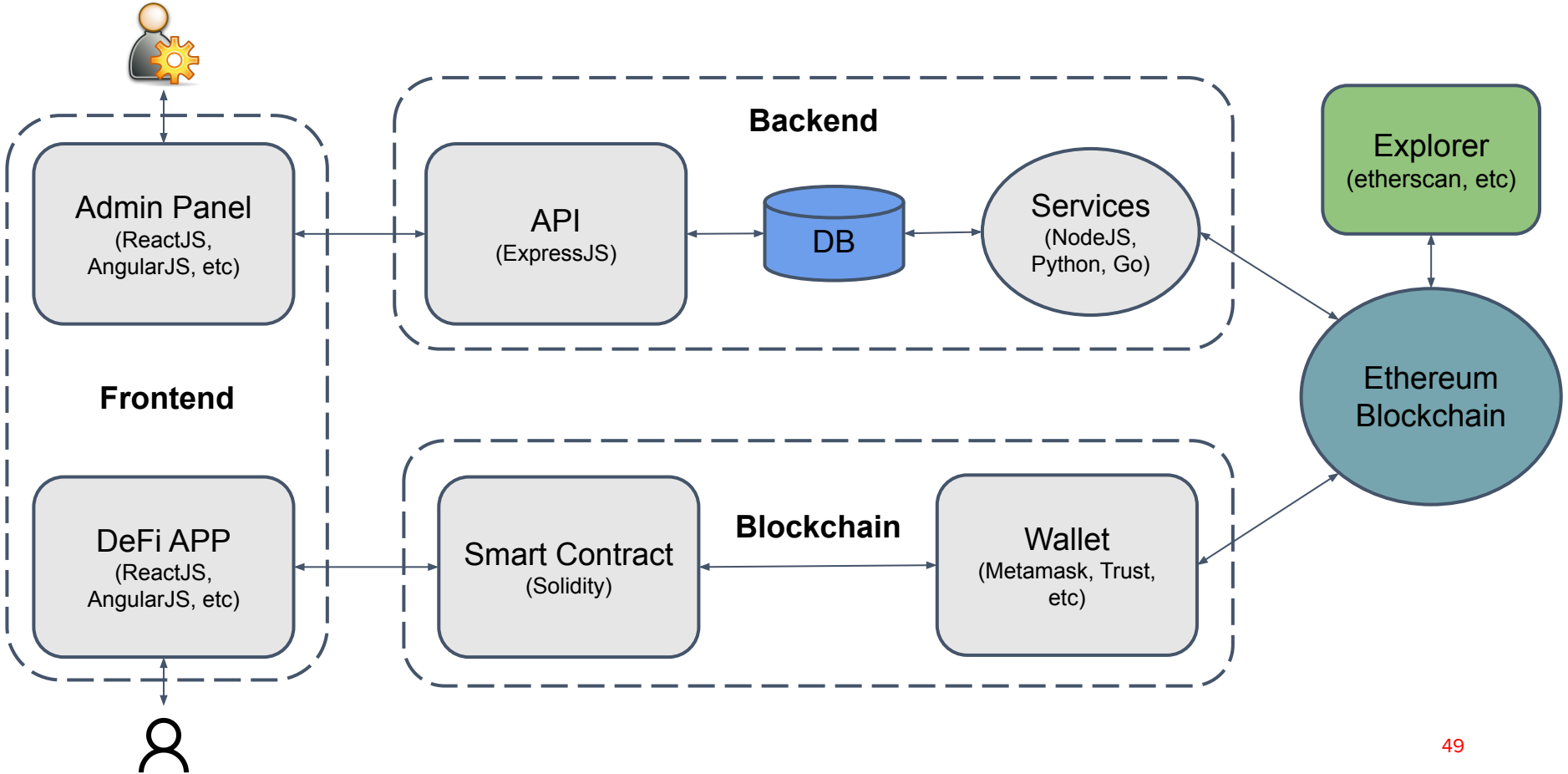
P2P LENDING AND BORROWING

upGrad

- A decentralized, smart contract based platform for p2p lending and borrowing of any **existing ERC20 Token** on the Ethereum Blockchain with ETH as **collateral**.
- The open ecosystem of the p2p lending and borrowing platform has the potential to offer cheaper lending contracts than the current centralized institutions, while also enabling people to profit from a fair and transparent portfolio of products.

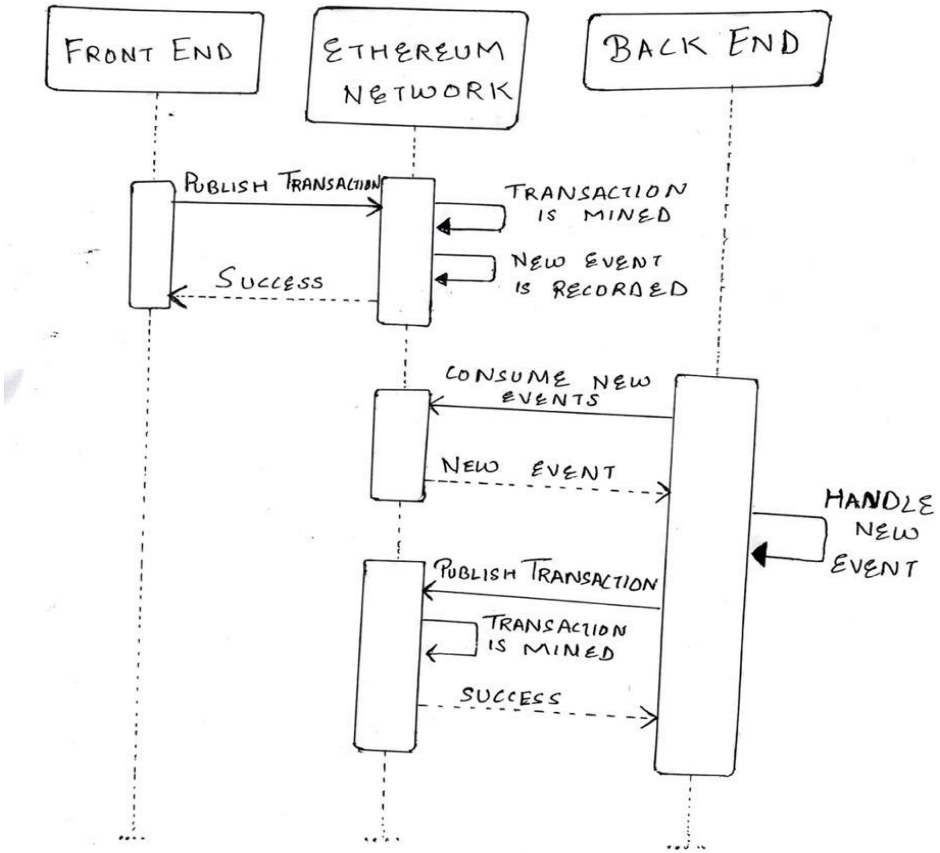
DeFi ARCHITECTURE

upGrad



DeFi ARCHITECTURE

upGrad



APPLICATION LAYERS

upGrad

- **Blockchain**

  Ethereum blockchain can be used for P2P Lending and Borrowing DeFi App.

- **Smart Contract**

  Holds the business logic of DeFi

  - ERC20 token
  - Ask Token (With Collateral)
  - Lend Token
  - Payback
  - Collect Collateral
  - Cancel Request

APPLICATION LAYERS

upGrad

- **Wallet**

  For transaction signatures and broadcasting to blockchain

  - Metamask
  - Trust
  - Custom (if any)
- **Frontend**

  Below User Interfaces are required :

  - DeFi APP (For End Users)
  - Admin Panel (For Administration and tracking transactions)

APPLICATION LAYERS

upGrad

- **Backend**
  - Services
    - To store our DeFi App blockchain transaction in local DB
  - API
    - For both Admin and DeFi APP
    - To view Blockchain Transaction data
    - Analytics
- **Explorer**
  - To Verify and Publish smart contract (For trust)

What are we going to develop?

upGrad

- Smart Contract
  - Creating
  - Deploying
- DeFi Backend API with Wallet
- Understand how to achieve it with frontend and external wallets like Metamask, etc.

Poll 2 (15 seconds)

Which of the below steps can be taken if your transaction is not included in the block for a long time?

A. Cancel that transaction and rebroadcast it

B. Broadcast a new transaction with same nonce and higher transaction fee

C. Broadcast a new transaction with next nonce and higher transaction fee

D. It's not possible

Poll 2 (15 seconds)

Which of the below steps can be taken if your transaction is not included in the block for a long time?

A. Cancel that transaction and rebroadcast it

B. Broadcast a new transaction with same nonce and higher transaction fee

C. Broadcast a new transaction with next nonce and higher transaction fee

D. It's not possible

upGrad

DOUBT CLEARANCE WINDOW

In this class, you learnt that:

upGrad

1. What is Decentralized Finance
2. Difference between Centralized and Decentralized finance
3. Live use cases
    a. Uniswap
    b. Aave
    c. MakerDAO
    d. Compound
    e. Binance
4. Understand DeFi app architecture

HOMEWORK

upGrad

1. Do some research on existing live DEFI products and understand their smart contract on explorers
2. Think other ways/opportunities in which we can incorporate decentralized finance.
3. Read solidity style guide
4. Research different DAPP design pattern

   (https://medium.com/@i6mi6/solidty-smart-contracts-design-patterns-ecfa3b1e9784)

NEXT STEPS

- Create and Build a Defi App from scratch
  - Smart Contract
  - Backend
  - Frontend
- Further scope
  - Administration
  - Scalability

upGrad

#RahoAmbitious

Thank You!