

# Ethereum and Decentralized Finance

PRANAY ANCHURI

PREPARED FOR  
WINTERSESSION

2022

# CHECK-IN

INTRODUCTION TO BLOCKCHAIN AND  
DECENTRALIZED FINANCE (PART 2 OF 2)

THURSDAY, JANUARY 13 AT 1:00PM



<http://cglink.me/2gi/c1367322102816304>

- 1 Open the My PrincetonU app.
- 2 Select a Hub
- 3 Click on QR Code scanner.
- 4 Scan this QR Code and you are checked-in!



# Logistics

---

CHECK-IN

@ [HTTP://CGLINK.ME/2GI/C1367322102816304](http://cglink.me/2gi/c1367322102816304)

# Outline

---

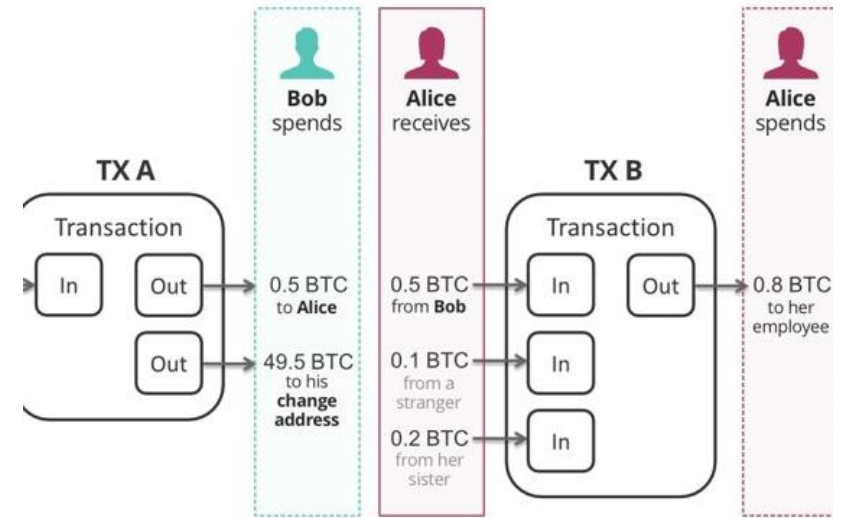
- Bitcoin recap
- Ethereum
- Decentralized Applications (DApps)
- Decentralized Finance
- Conclusions

# Bitcoin recap

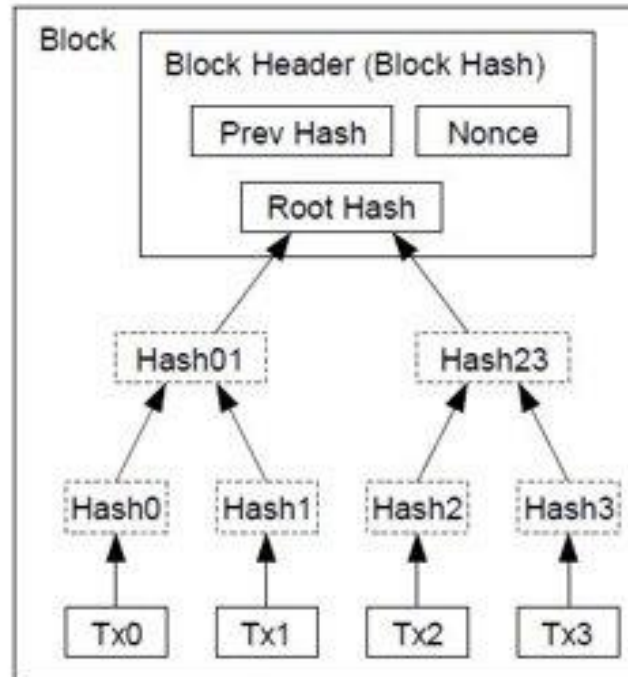
---

# Bitcoin transaction and blockchain

- Users create public key, private key pairs
- Transaction : Private key A Signs a message that transfers a Bitcoin associated with Public key A to Public key B
  - Anyone on the network can verify the digital signature
  - No one on the network can modify the transaction without knowing the private key A
- Miners solve hash-based puzzles to order transactions on the network



# Proof-of-work



## Bitcoin's Proof-of-Work



Find a nonce  $x$  such that:

$$\text{SHA-256}(\text{SHA-256}(r \parallel x)) < T/d$$

$r$  = header

includes  $H(\text{previous block})$   
root of Merkle tree of transactions

# Applications beyond value transfer

---

- Colored coins
- Eternal wall
- Bitcoin is not meant for deploying complex financial applications
  - Limited block size
  - Limited scripting

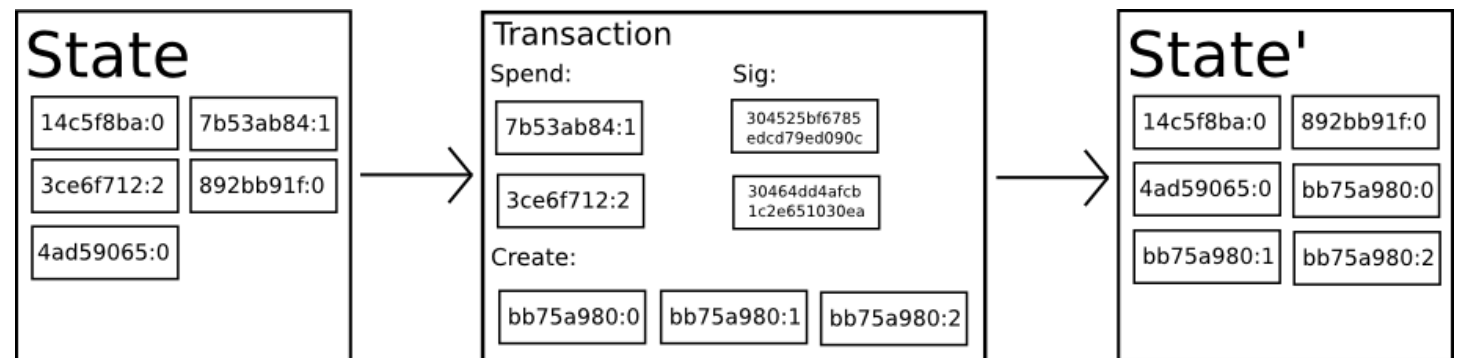
# Ethereum

---



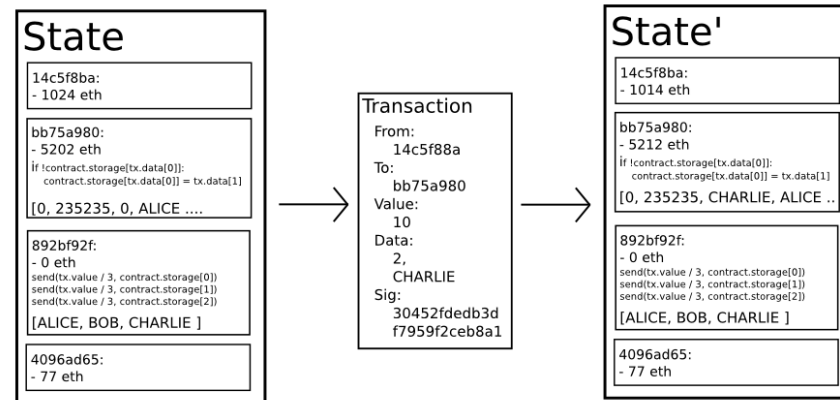
# Bitcoin state transition

- State of Bitcoin is the set of all outstanding coins
- Each transaction consumes few coins and produce new coins
- Transaction is essentially a state transition function
- Mining rewards is a special case none of the existing coins are destroyed



# Ethereum state transition

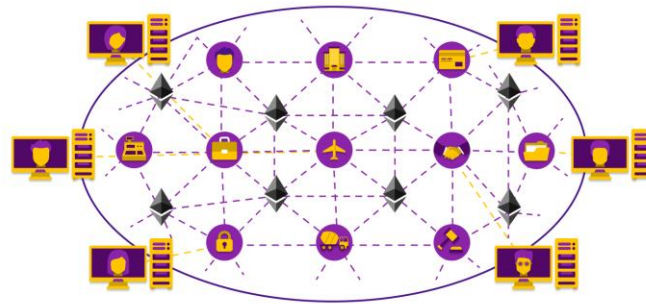
- Ethereum is a generalized version of Bitcoin with accounts, storage and complex logic to modify the storage.
- A global computer that anyone can use, truly interact with other users and applications



# Ethereum world computer

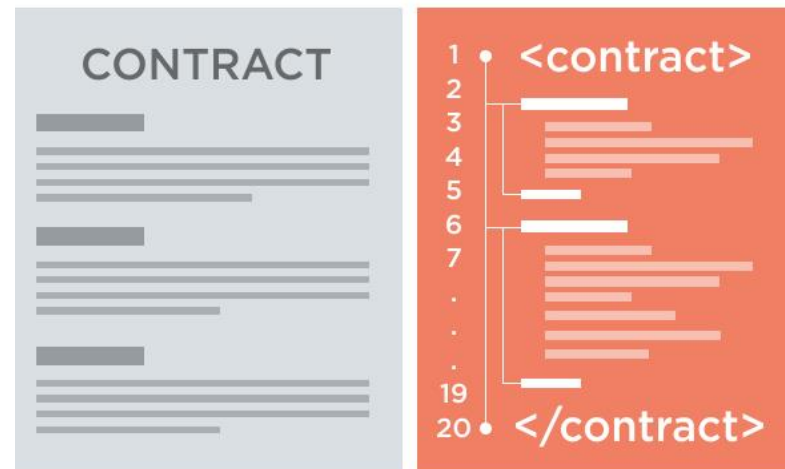
- A blockchain based generalized state transition mechanism enables a world computer
  - Decentralized apps (Dapps) like applications on desktop computer
  - Transactions are like user interactions
- Ethereum is a synchronized, open for all computer that runs forever
- Everyone runs a local copy of this synchronized machine
  - Massive replication

Ethereum platform allows users from all over the world to create and use smart contracts and decentralized applications



# Smart contracts

- Smart contracts are applications that are stored on world computer
- Encodes logic that can modify state of storage via user interaction / transactions
- Reduces the need for intermediaries in person-to-person interactions
  - Example : Rules for auction can be encoded in smart contracts
- Anyone can deploy new smart contracts



# Accounts on Ethereum blockchain

## Externally Owned Accounts (EOA)

- Can be created independently, like bitcoin accounts
- Private and public key
- Can hold Ether tokens

## Contracts

- Can hold Ether
- Can only be triggered in response to a transaction
- Can deploy new contracts

# Transactions on Ethereum

---

- Ether transfer : Transfer from EOA to EOA or contracts
- Contract deployment : EOAs create contracts by sending data and logic
- Contract interaction : EOAs or contracts interact with other contracts by sending appropriate inputs

# Ethereum virtual machine

- Smart contracts are usually written in a specialized high-level language called Solidity
- Smart contracts are compiled into machine interpretable instructions called bytecode
  - Bytecode (not the source code) is stored on blockchain
- Bytecode instructions are executed on Ethereum Virtual Machine (EVM)
- What if the smart contract program has an infinite loop ?

# Ether

---

FUEL FOR THE ETHEREUM WORLD COMPUTER



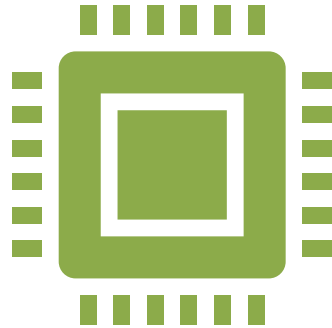
# Halting problem

---

- Undecidable problems are those which can't be answered yes/no
- Halting problem :
  - Given an algorithm and an input return YES if the program terminates and NO otherwise
- Halting problem is an example of undecidable problem
- Undecidability of halting problem means that we can't algorithmically decide termination of all programs
  - Proof by contradiction

# Turing machines and smart contracts

---



We want smart contracts that can represent complex logic and calculations, a Turing machine



Undecidability of halting problem poses a major challenge

# Halting problem in Ethereum

- Ethereum's "solution" for halting problem
  - Transaction initiator pays (in Ether) for every step of execution
  - Limited supply of Ether implies infinite loops can't execute
- Every computation is expressed in Gas
  - Addition is 1 unit, multiplication is 4 etc
- Gas price is not constant
  - Transaction cost = Total gas \* Gas price (Pay what you wish model)
  - Easy to estimate approximately based on operations involved
- 1 Ether =  $10^{18}$  Wei

# Putting it all together

---

- Ethereum is a generalization of Bitcoin blockchain
- Turing complete language to write arbitrarily complex smart contracts - Solidity
- Uses proof-of-work model for ordering transactions
- Miners execute transaction on EVM, update their blockchain state
  - Users set gas limit and gas price
- State synchronization via matching root hash



# Bitcoin vs Ethereum

---

- Primary use : Currency
- Block time : ~ 10 minutes
- Throughput : 1 MB blocks

- Primary use : Platform for decentralized applications
- Block time : ~13 seconds
- Throughput : 21 Million gas

# Decentralized Apps

---

# ERC20 Smart contract

- *Standardized smart contract for issuing, transfer of assets/coins*
- Coins can represent real-world or digital assets
  - In-game currency
  - Digital gold etc
- Ethereum blockchain provides
  - Cross-border transfer
  - Near instantaneous transfers
  - Traceability
  - Security

```
1 // -----  
2 // ERC Token Standard #20 Interface  
3 // https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20-token-standard.md  
4 // -----  
5 contract ERC20Interface {  
6     function totalSupply() public constant returns (uint);  
7     function balanceOf(address tokenOwner) public constant returns (uint balance);  
8     function allowance(address tokenOwner, address spender) public constant returns (uint remaining);  
9     function transfer(address to, uint tokens) public returns (bool success);  
10    function approve(address spender, uint tokens) public returns (bool success);  
11    function transferFrom(address from, address to, uint tokens) public returns (bool success);  
12  
13    event Transfer(address indexed from, address indexed to, uint tokens);  
14    event Approval(address indexed tokenOwner, address indexed spender, uint tokens);  
15 }
```

# Initial coin offering

---

- ICO is a means of fund-raising leveraging the decentralized security and validation offered by blockchain
- Entrepreneurs receive capital (often in the form of cryptocurrencies) not for an equity stake but in exchange for a utility coin or token issued by the company
  - In traditional IPOs, investors receive equity stake (shares) in exchange for the capital (money)
  - Equities are tradable on an exchange (NYSE)
- ICO tokens are tradable on centralized (Coinbase, Gemini) or decentralized exchanges (0x)
- Types of ICO
  - Utility token : These are coins that can be redeemed later for goods or service
  - Security token offering : Like traditional securities and has regulatory oversight



# Decentralized prediction market

---

- Augur is a decentralized betting platform
- Market can be created for any real-world event with a limited and deterministic set of outcomes
- Anyone can create a market
  - Indicates possible outcomes
  - Reporting mechanism
  - Posts a deposit which is returned if the market resolves

# Trading on Augur

---

- Shares of each outcome of market are traded via Ethereum blockchain
- Order book for opening positions and matching buy/sell orders
- Say a market has three outcomes A, B, C
  - I can place an order for 3 shares of A at 0.6 ETH per share
  - Matching finds open orders for B and C such that each share is exactly 1 ETH.
  - It can match B at 0.3 ETH and C at 0.1 ETH
- At the end of event, the shares of winning outcome is 1 ETH and other shares are worthless
- Ethereum is a closed system i.e., it only knows about Ethereum accounts and state
  - How to bring external facts ? Time, Stock prices, Weather etc

POLITICS TAGS / DEMOCRATIC

## How Democratic Caucuses Win

65.00% ▼ Joe Biden 24.99% ▼

OPEN INTEREST

313.7598 ETH

EST. FEE

1.0100 %

REPORTING START TIME

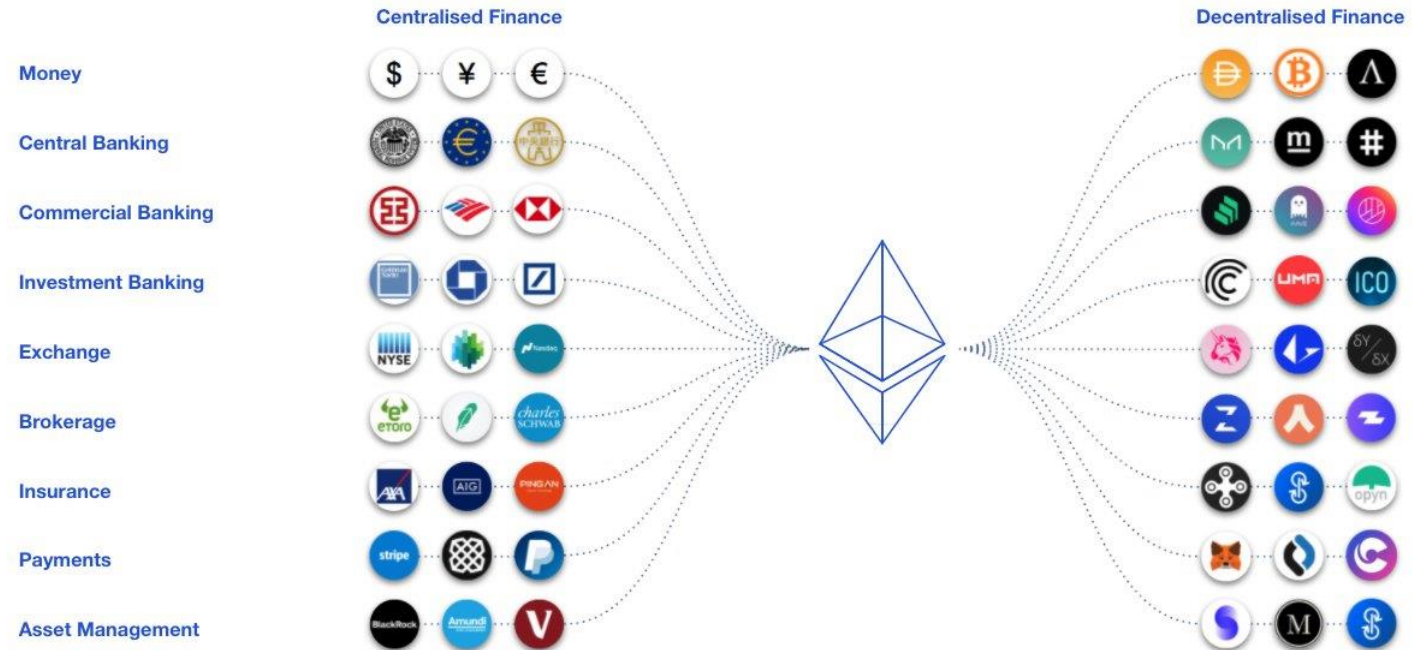
February 7, 2020 5:00 PM (E)  
February 7, 2020 12:00 PM (E)

# Decentralized Finance

---

# Centralized Finance -> Decentralized Finance

- Ethereum provides base infrastructure to replicate complex centralized finance products
- Users on Ethereum have access to financial products (no need for onboarding onto each platform)



# Why DeFi

---

Global participation

---

Transparent

---

Low infrastructure costs

---

Composable products

---

Fast settlement

---

Automated market makers

---

Total Value Locked (USD)

**\$95.28B**

Maker Dominance

**17.94%**

DeFi Pulse Index

**250.91** +4.64  
(+1.88%)

## Total Value Locked (USD) in DeFi

[TVL \(USD\)](#) | [ETH](#) | [BTC](#)

All | 1 Year | [90 Day](#) | 30 Day



# DeFi market size

# Stable currencies

---

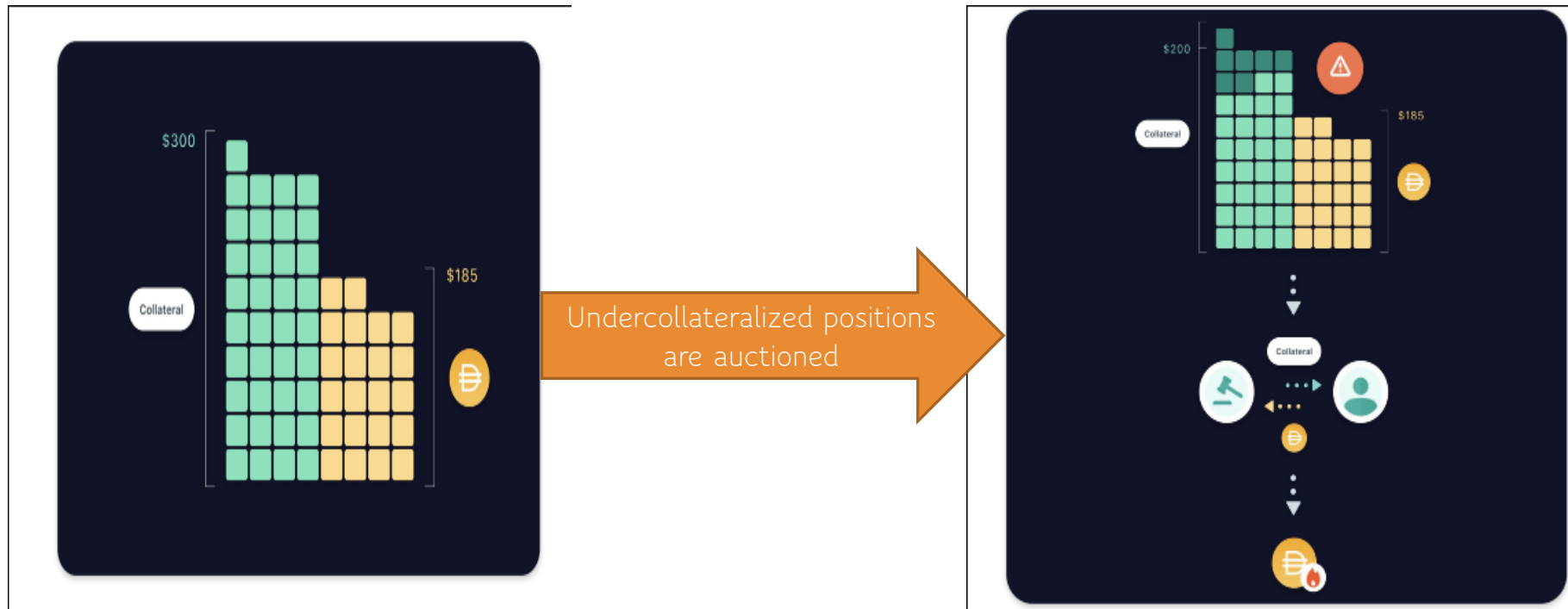
# Why blockchain based stable currencies ?

---

- Volatile (10x in ~ 1 year) cryptocurrencies like Bitcoin, Ethereum are 1) Not an ideal medium of exchange 2) Can't be used as a unit to value other items
- **Stable cryptocurrency** : A decentralized, unbiased, collateral-backed cryptocurrency that is soft-pegged to an offline currency like USD.



# DAI Stable coin



# Decentralized exchanges

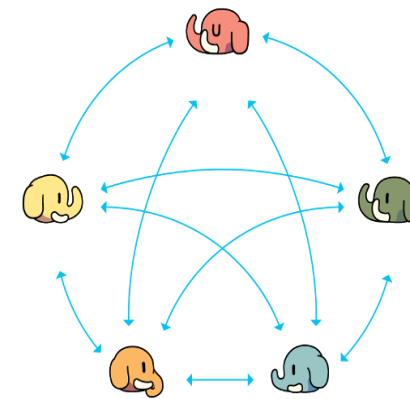
---

# Centralized vs decentralized exchanges

---



- Exchange controls user funds
- Not anonymous
- Regulatory compliance



- User hold funds in their wallet
- Anonymous
- Underlying network provides security
- No regulatory oversight

# Automated market makers

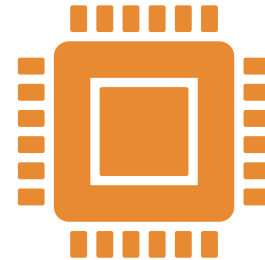
---



Automated Market Makers : Algorithmic agents that act as counterparty to any trade







Providers of liquidity

Used in prediction markets



Smart-contract platforms like Ethereum provide ideal platform for deploying AMMs

Useful for exchange, lending, derivatives etc

Contract	Latest Yes Price	Best Offer	Best Offer
 Donald Trump	29¢ <small>1¢↓</small>	30¢	<div>Buy Yes</div> <div>Buy No</div> 71¢
 Kamala Harris	16¢ <small>NC</small>	17¢	<div>Buy Yes</div> <div>Buy No</div> 84¢
 Joe Biden	13¢ <small>NC</small>	13¢	<div>Buy Yes</div> <div>Buy No</div> 88¢
 Bernie Sanders	11¢ <small>1¢↑</small>	11¢	<div>Buy Yes</div> <div>Buy No</div> 90¢
 Beto O'Rourke	10¢ <small>2¢↑</small>	10¢	<div>Buy Yes</div> <div>Buy No</div> 91¢
 Elizabeth Warren	8¢ <small>NC</small>	8¢	<div>Buy Yes</div> <div>Buy No</div> 93¢

# AMM – Prediction markets

Actor	Goals	Actions
Liquidity providers	Earn trading fee, long term speculation	Deposit funds
Users	Short term loans, liquidity (exchange volatile for stable coins), speculation, illegal trading	Exchange tokens
Arbitrageurs	Make money from price differences	Positions on AMM and reference markets
Governance tokens	Invest in the vision, direction of protocol	Invest to change to control protocol parameters
Market maker contract	Facilitate exchange	Design appropriate incentives
Decentralized oracles	Provide market prices	Track AMM reported prices

# Actors in decentralized exchanges

Total Value Locked (USD)

**\$30.4B**

Curve Finance Dominance

**47.39%**

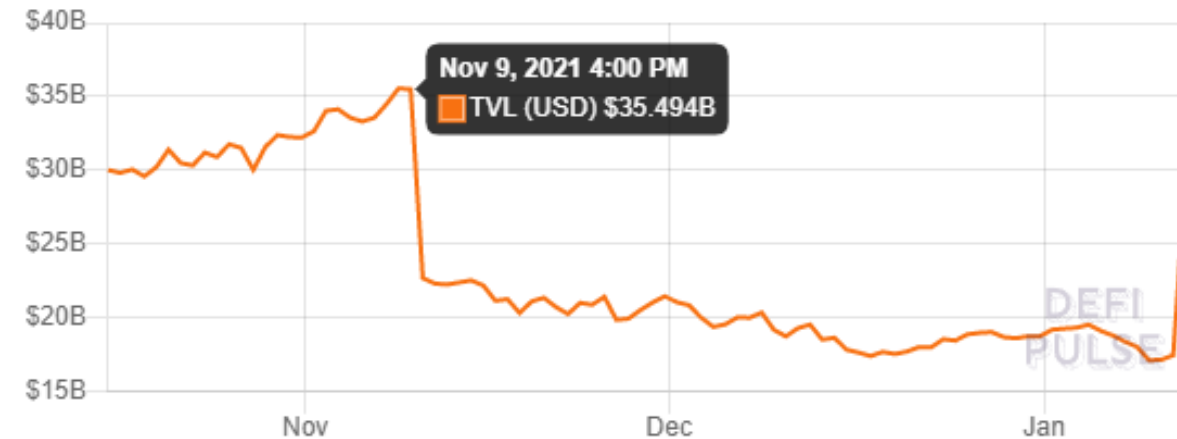
DeFi Pulse Index

**250.91** +4.64  
(+1.88%)

## Total Value Locked (USD) in DEXes

[TVL \(USD\)](#) | ETH | BTC

All | 1 Year | [90 Day](#) | 30 Day

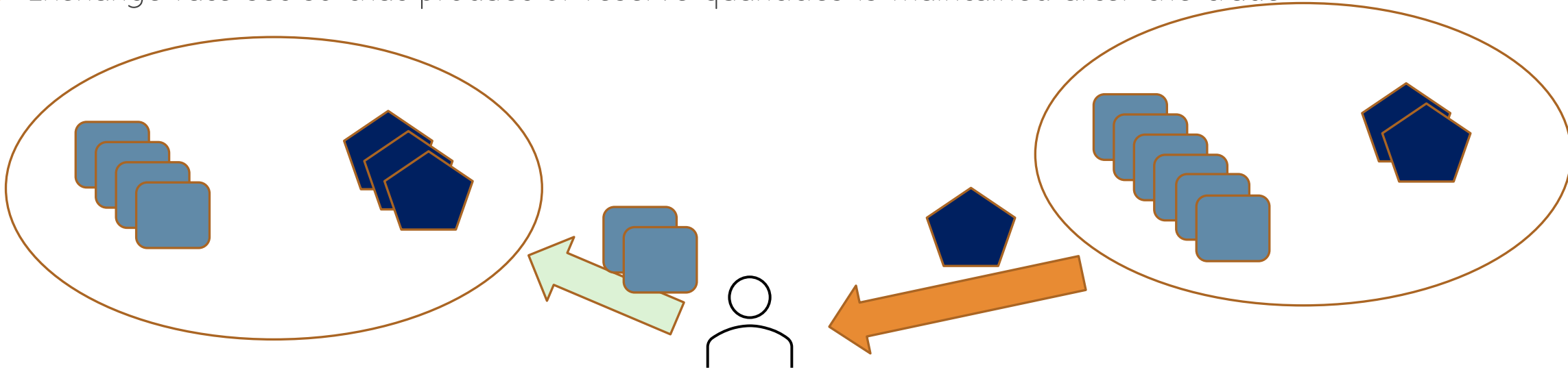


# Volume on decentralized exchanges

# AMM – Constant function market makers

---

- Pair of tokens are deposited into a pool (smart contract)
- Users buy and sell against the pool; Examples : Uniswap, SushiSwap
- Exchange rate set so that product of reserve quantities is maintained after the trade





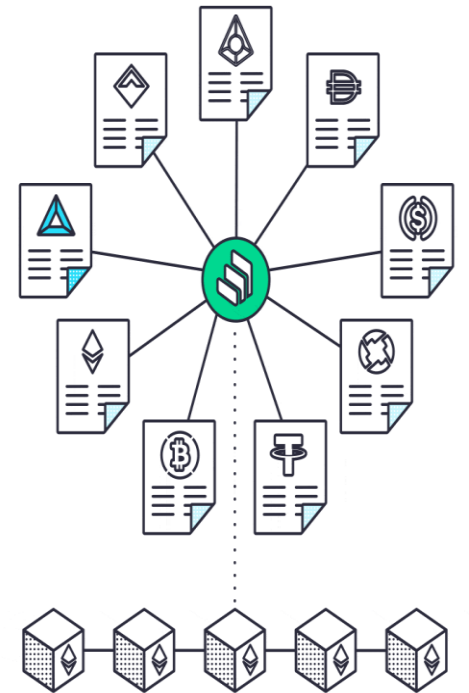
# Lending and borrowing on blockchain

---

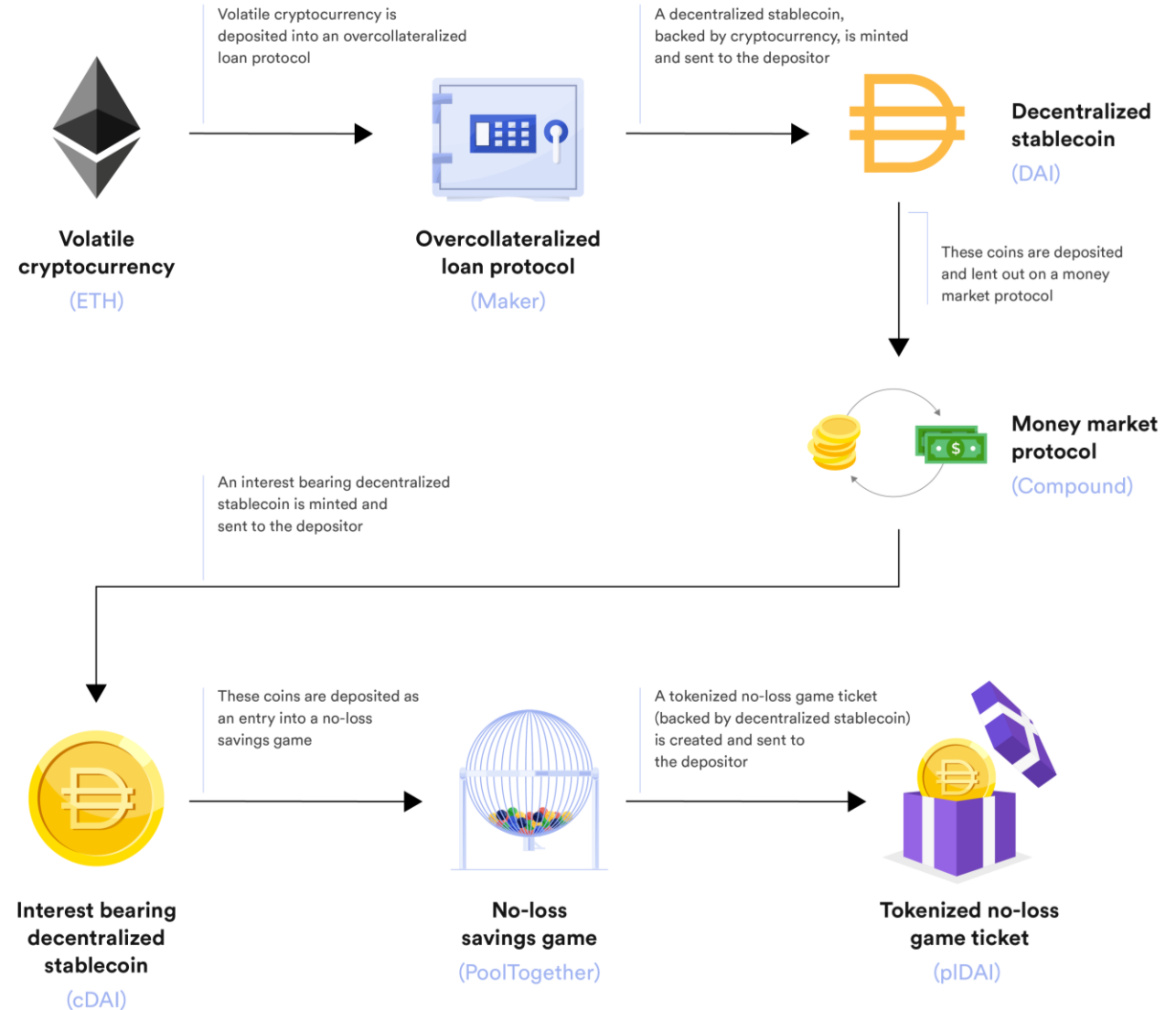
# P2p lending of crypto assets - Compound

---

- Users can post collateral in any of the 9 supported cryptocurrencies and in-turn receive cTokens
  - Can borrow up to a certain fraction
- Earn interest per block (cTokens become more valuable)
- Exchange prices fed into the protocol



# Composability of DeFi protocols



# Demo

---

INTERACTING WITH DECENTRALIZED EXCHANGES AND LENDING  
PROTOCOLS

# Developing DApps

---

# Deploying a smart contract

Write smart contract in solidity

- Requires minimal programming experience
- Lots of tools

Compile

- Bytecode
- ABI

Test for bugs

- Contract once deployed can't be "upgraded"

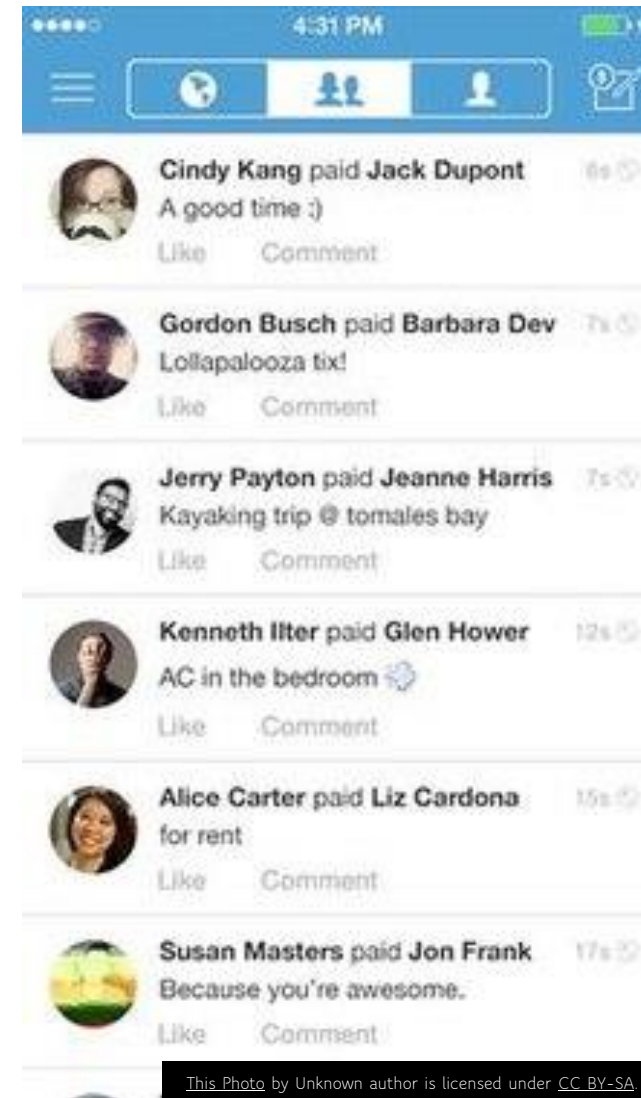
Deploy the bytecode

Interact with the contract via new transactions

# VenmoLite

---

- Users pay each other Ether via contract
  - Contract may provide additional functionality like splitwise, request payments etc.
- Payments are public



# Other aspects

---

- Technical :
  - Scaling
  - Proof-of-stake
  - Layer-2 solutions
- Adoption and societal impact
- Privacy and legal



# Conclusions

---

- Ethereum provides decentralized infrastructure for deploying applications beyond value transfer
- Applications range from creating stable currencies to DeFi products



## CHECK-IN

INTRODUCTION TO BLOCKCHAIN AND  
DECENTRALIZED FINANCE (PART 2 OF 2)

THURSDAY, JANUARY 13 AT 1:00PM



<http://cglink.me/2gi/c1367322102816304>

- 1 Open the **My PrincetonU** app.
- 2 Select a Hub
- 3 Click on QR Code scanner.
- 4 Scan this QR Code and you are checked-in!



# Announcements

---

- [HTTPS://FORMS.GLE/D2WVGyKCHKU1TjVF9](https://forms.gle/D2WVGyKCHKU1TjVF9)
- [HTTPS://GITHUB.COM/PRANAYANCHURI/WINTERSESSION-2022](https://github.com/PRANAYANCHURI/WINTERSESSION-2022)

Thank you 😊