Decentralized Finance

Introduction and Overview of DeFi

Instructors: Dan Boneh, Arthur Gervais, Andrew Miller, Christine Parlour, **Dawn Song**





Stanford University
Imperial College London
UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN
Berkeley UNIVERSITY OF CALIFORNIA

What Is Finance?

- Finance is the process that involves the creation, management, and investment of money and financial assets
- Financial assets/financial instruments:
  - a non-physical asset whose value is derived from a contractual claim
  - Bank deposits, stocks, bonds, loans, derivatives
- Financial services
  - banking, lending/borrowing, securities, insurance, trusts, funds
- Financial markets: marketplace for trading financial assets

Traditional Finance (CeFi)

(Centralized) financial institutions provide financial services

- Banks, securities/insurance/trust investment/fund management companies, etc. (title 31 of the United States Code)
- Hold custodies of customers' funds/assets
  - Can freeze accounts
- Serves as intermediaries for transactions
  - Can censor transactions
  - Take fees (rent seeking)
- Adhere to strict on-boarding & continuous compliance rules (regulation)
  - KYC (know your customer)
  - AML (anti-money laundering)
  - CFT (combat the financing of terrorism)
- Customer has no privacy to service provider
  - Service provider knows real identity and full account/transaction information of customer
- Opaque, siloed databases and applications
- Need to be trusted to operate correctly and securely

Bitcoin: Birth of (Public) Blockchain

Bitcoin P2P e-cash paper

Satoshi Nakamoto | Sat, 01 Nov 2008 16:16:33 -0700

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

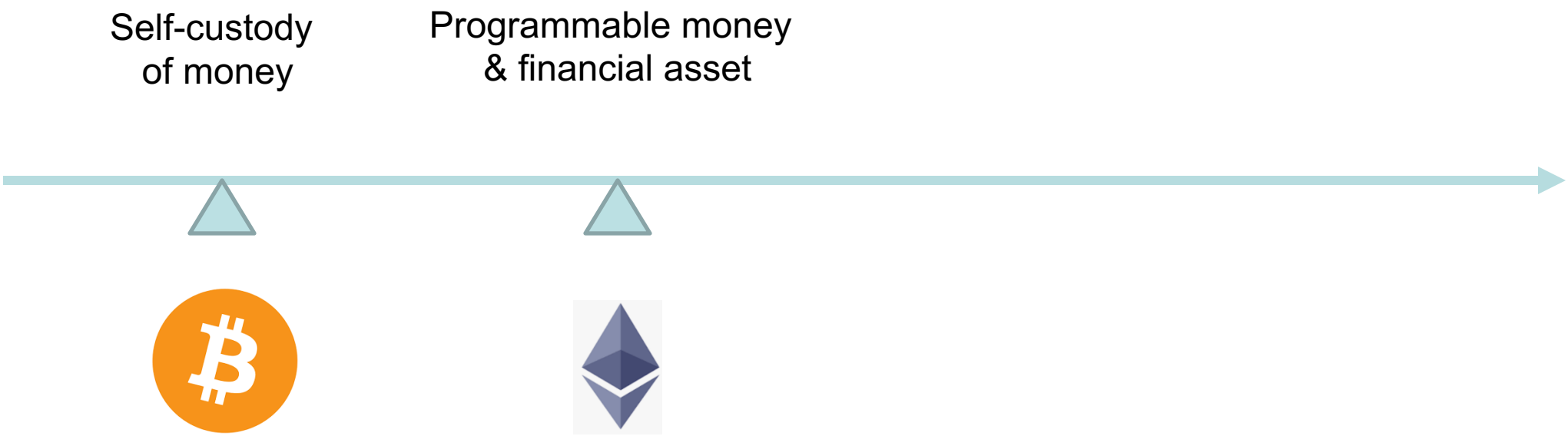
The main properties:
- Double-spending is prevented with a peer-to-peer network.
- No mint or other trusted parties.
- Participants can be anonymous.
- New coins are made from Hashcash style proof-of-work.
- The proof-of-work for new coin generation also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of

Ethereum: Birth of Smart Contract Platform



What is Decentralized Finance (DeFi)?

- Financial infrastructure as an open, permissionless, and highly interoperable protocol stack built on public smart contract platforms

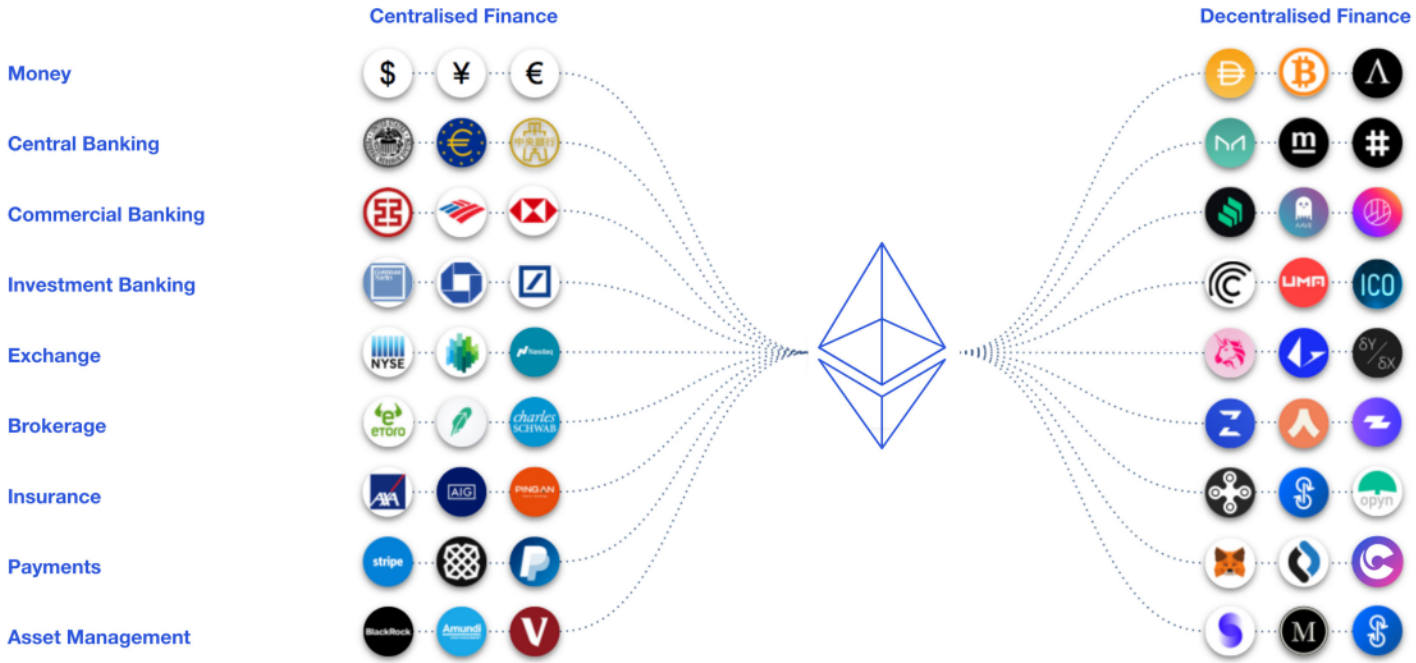
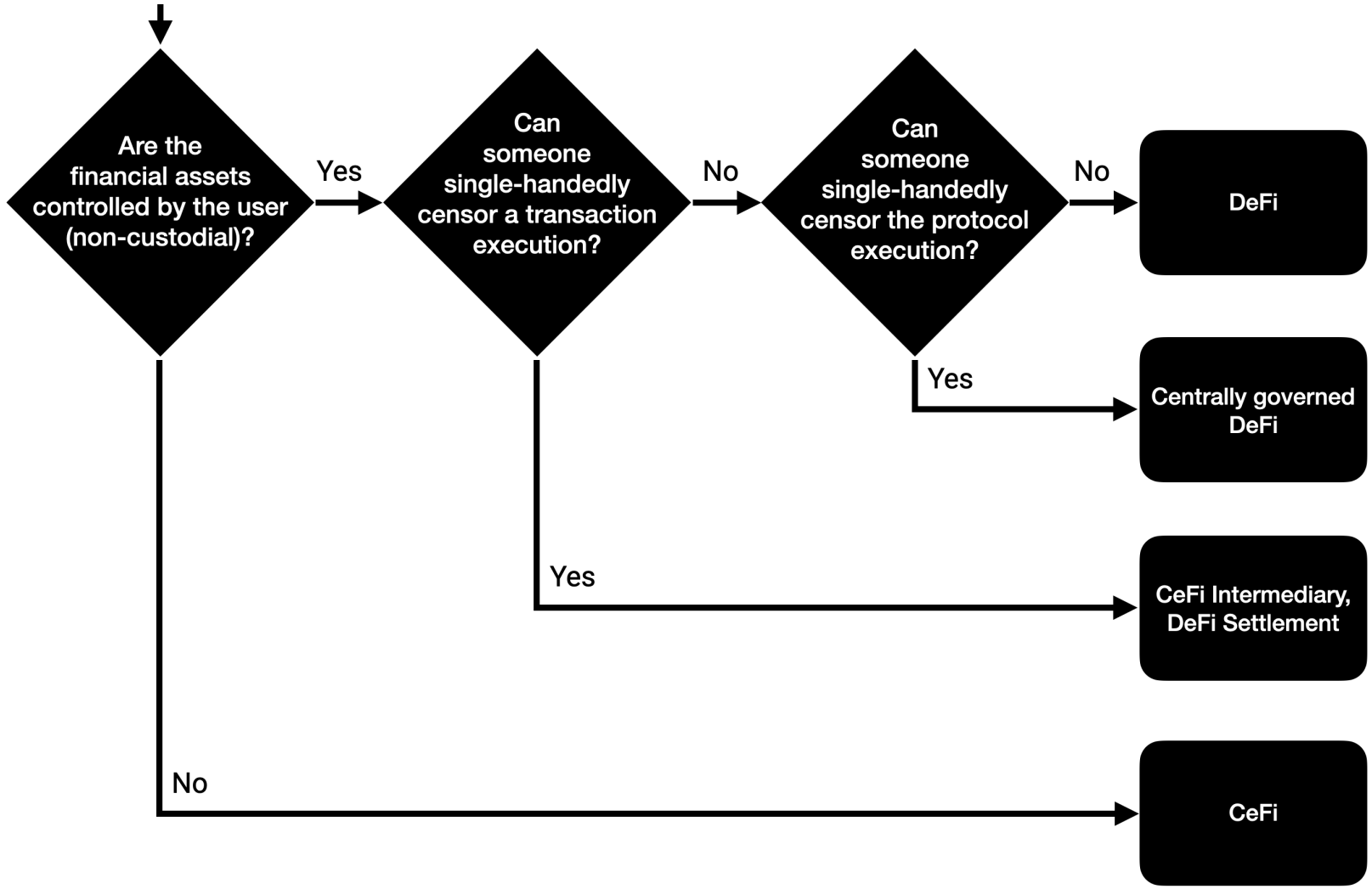


Image credit: Consensys Codefi

What is Decentralized Finance?

- Custody & settlement
- Transaction execution
- Protocol governance




Why DeFi?
https://defi-learning.org

CeFi vs. DeFi

Traditional finance (CeFi)

- Permissioned
  - Closed-source system, built on top of centralized databases
  - Needs approval & agreement for third-party to use & build on
- Custodial
  - Assets are custodied by licensed third-parties
- Centralized trust & governance
  - Single entity responsible for upgrade decisions & admin privileges
- Real identity
  - Users register with real identity, e.g., for KYC/AML compliance

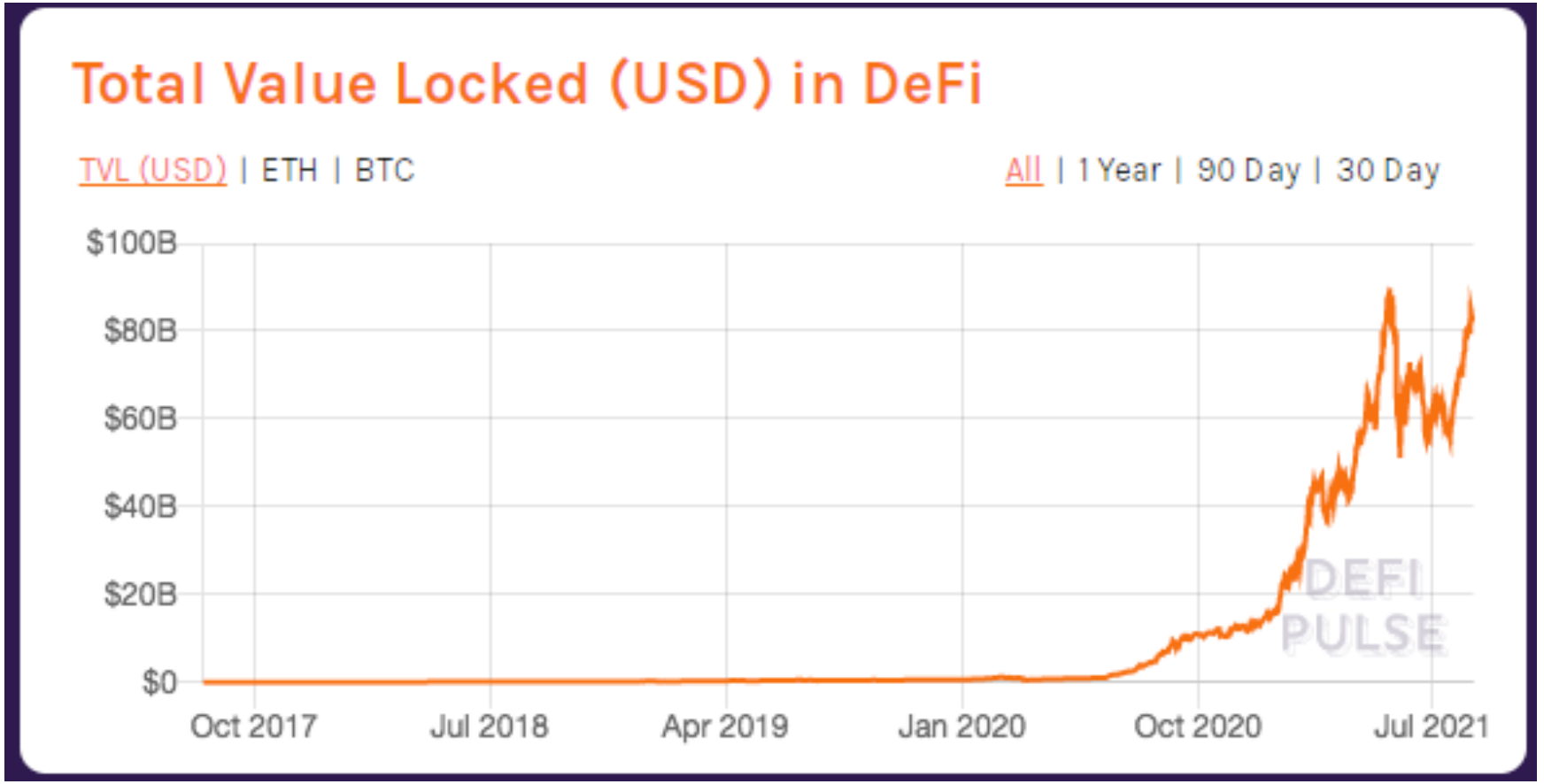
Decentralized finance (DeFi)

- Permissionless
  - Open-source system; built on top of permissionless blockchains
  - Anyone can use/ interoperate or build on top without third-party approval & agreeement
- Non-custodial
  - Assets are not custodied by a single third-party
- Decentralized trust & governance; Trustless
  - No single entity responsible for upgrade decisions & admin privileges
- Pseudonymous; privacy
  - Users usually do not provide real identities

DeFi Advantages

- Efficiency
  - Removing rent-seeking intermediaries
- Open finance and universal accessibility
  - Inclusive
- Transparency and public verifiability
  - Anyone can inspect the smart contract code and verify the execution and state of the system
- Self custody and censorship resistant
- Automation & programmability
- Composability and interoperability
- Innovation
  - DeFi applications often are much simpler and faster to develop than CeFi counterparts
    - E.g., Uniswap vs. CEX
  - Atomic composability
    - E.g., Flash loan

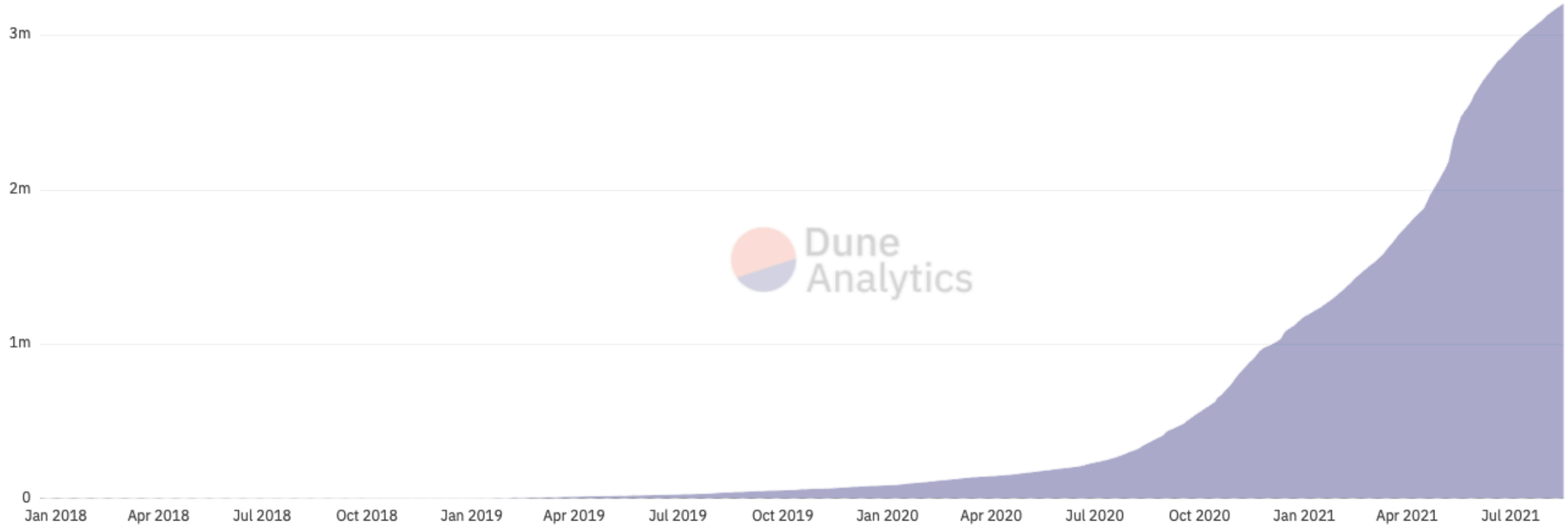
Fast Growth


Total Value Locked (USD) in DeFi
TVL (USD) | ETH | BTC
All | 1 Year | 90 Day | 30 Day
$100B
$80B
$60B
$40B
$20B
$0
Oct 2017
Jul 2018
Apr 2019
Jan 2020
Oct 2020
Jul 2021
DEFI PULSE

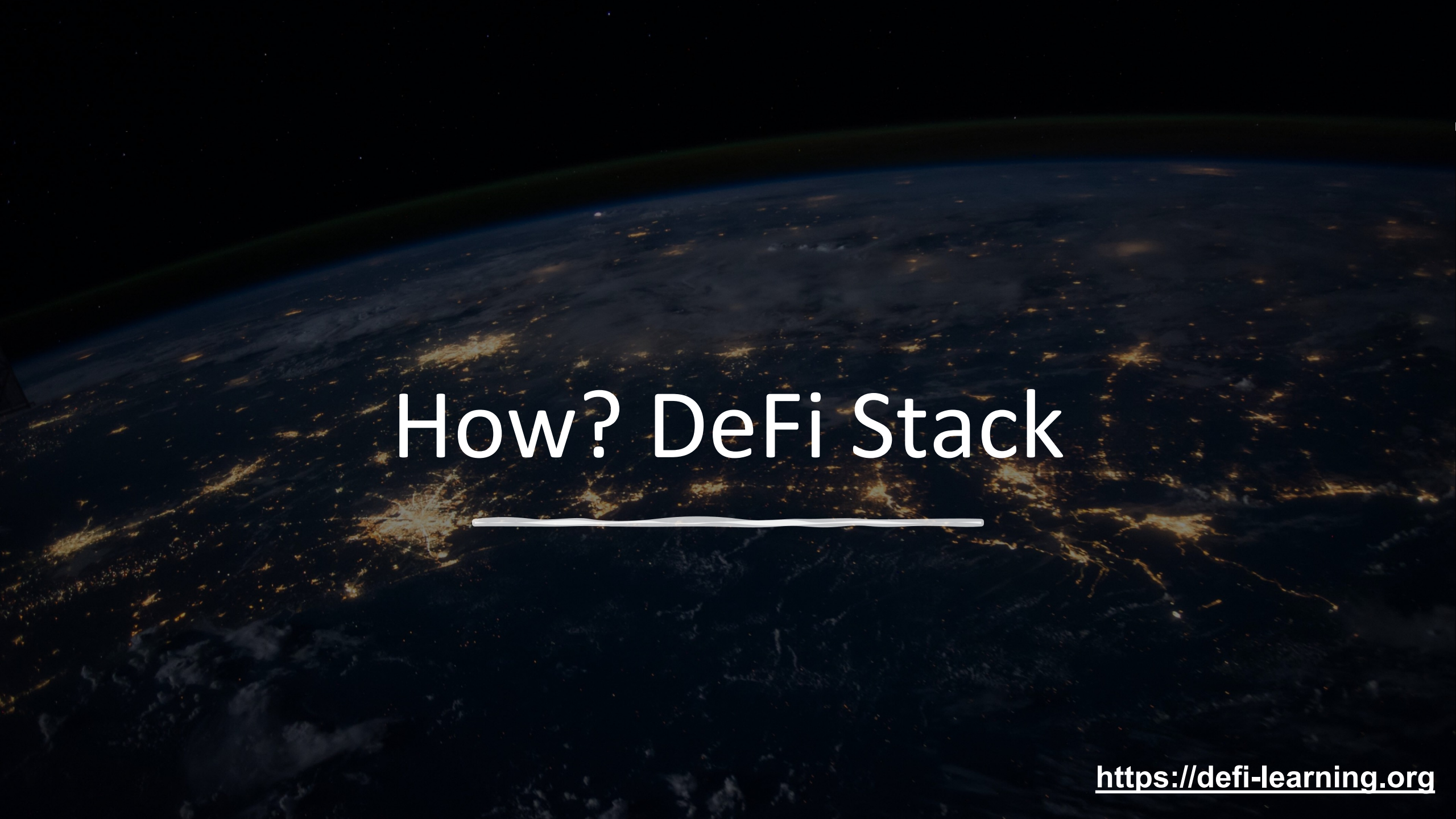
Fast Growth

Total DeFi users over time

Users = unique addresses. Since a user can have multiple addresses the numbers below are overestimates. Source: @richardchen39

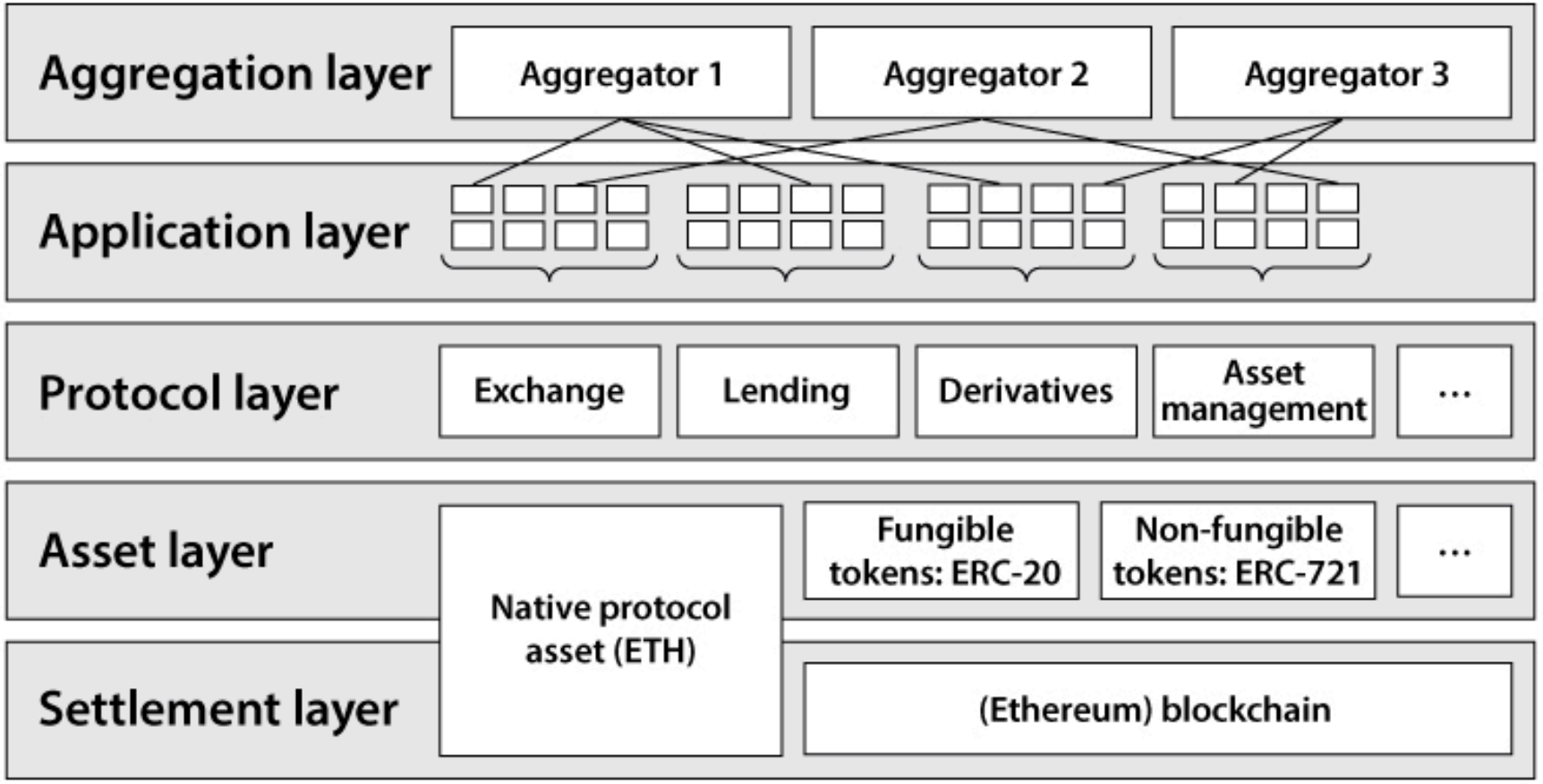


source


How? DeFi Stack
https://defi-learning.org

DeFi Stack

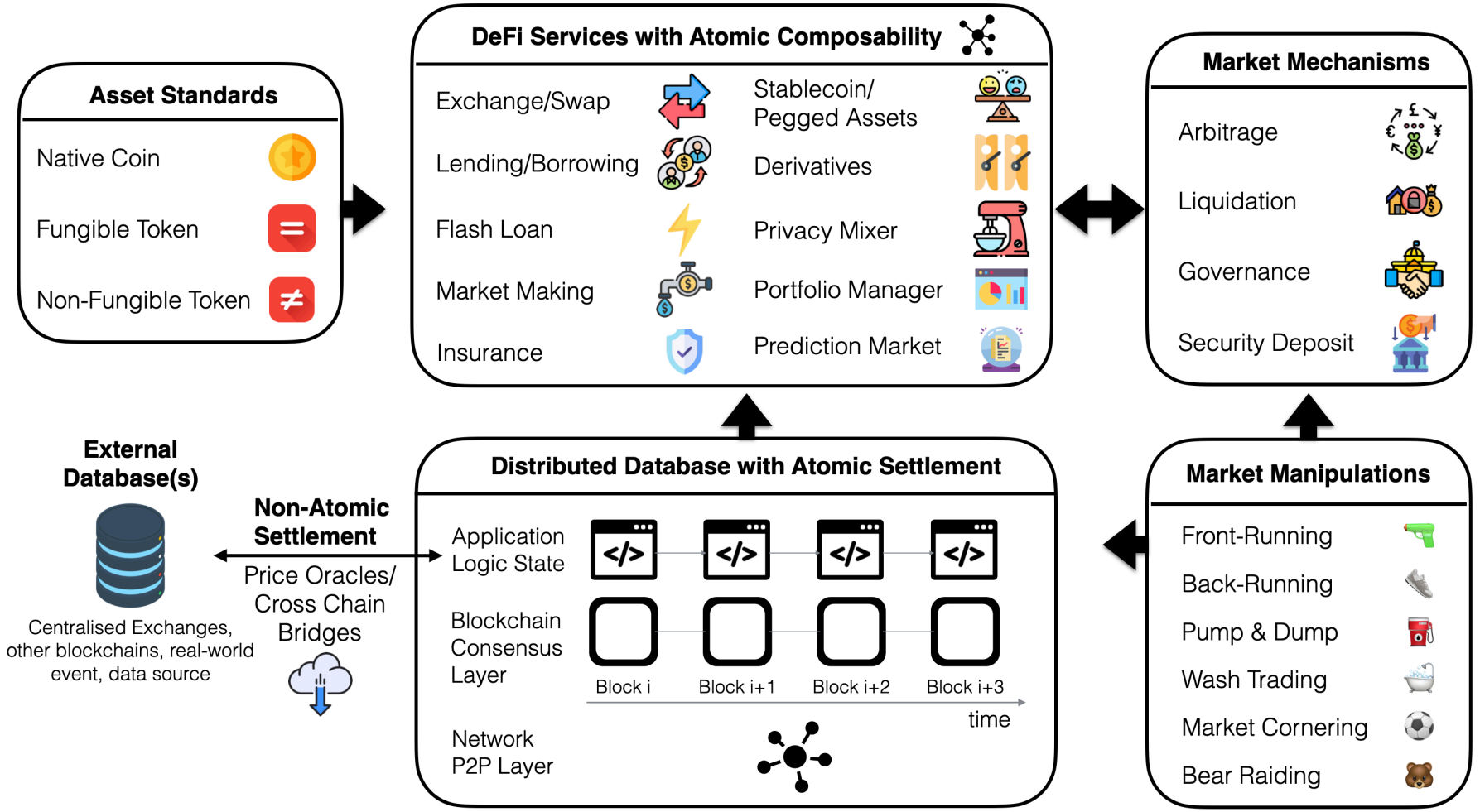
- DeFi is enabled by a decentralized smart contract platform
- Roles
  - User
  - Protocol (smart contract)
    - Governance



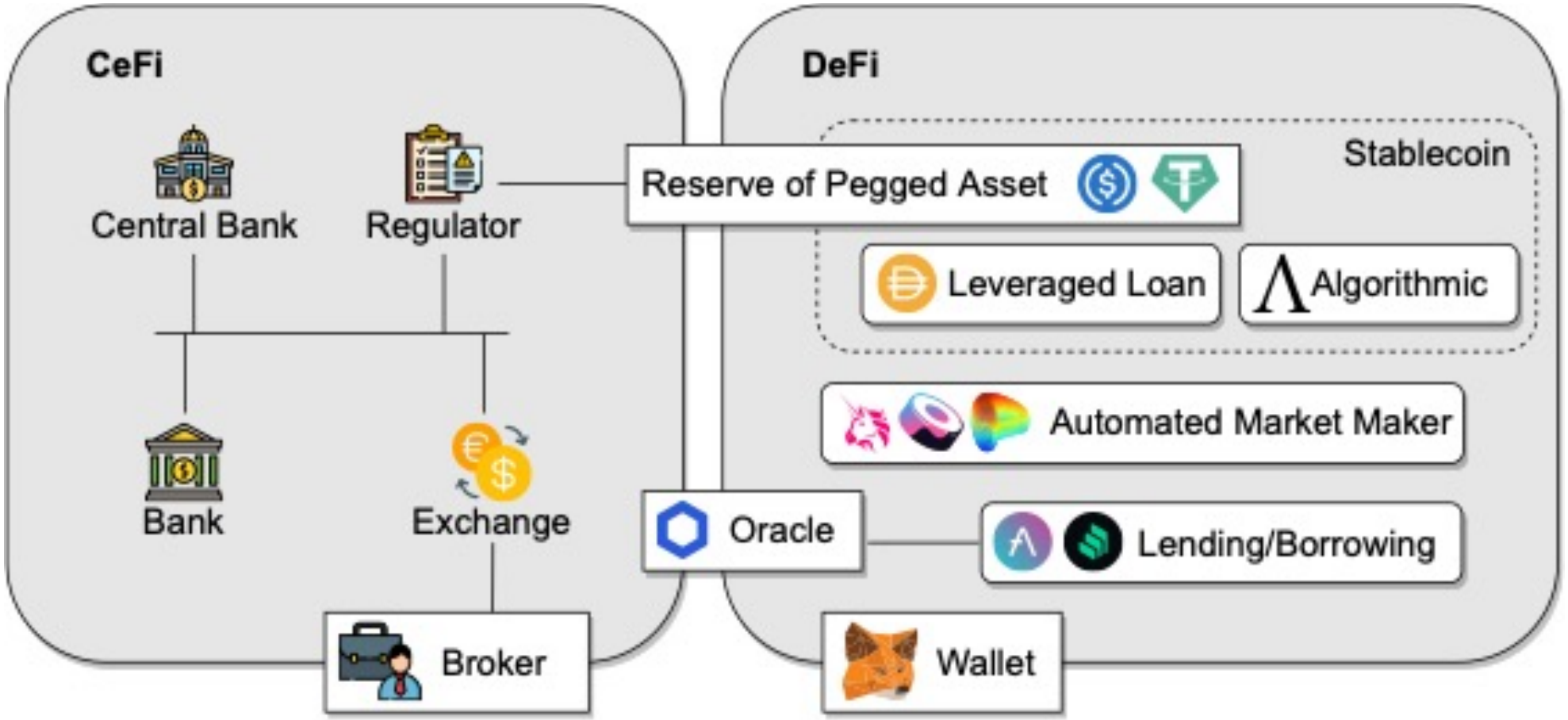
source

DeFi Stack

- Roles
  - User
  - Protocol
  - Keeper
  - Oracle
  - Bridge

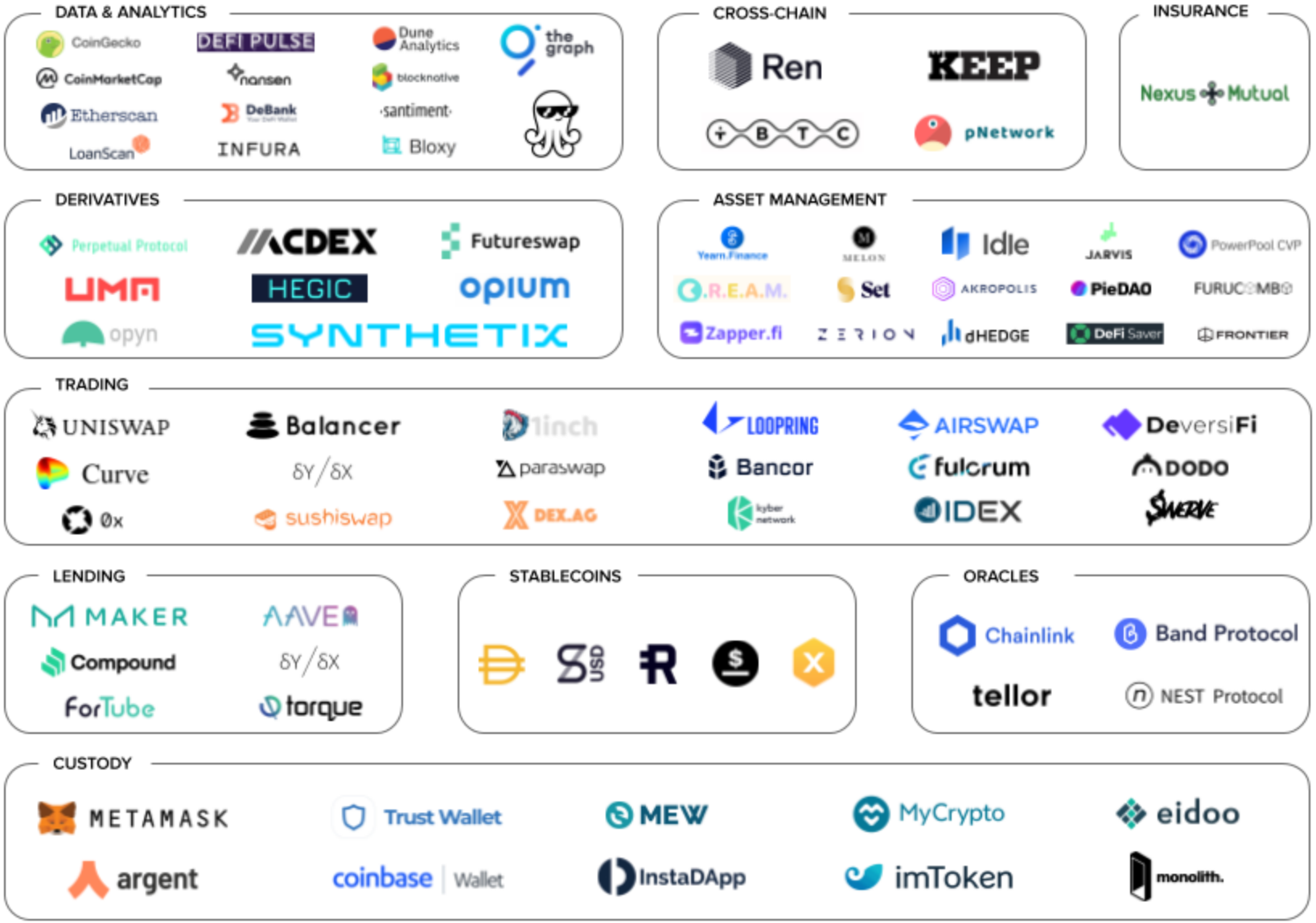


High-Level Service Architecture of CeFi, DeFi




DeFi Services and Innovations
https://defi-learning.org

ETHEREUM DeFi Map by Simone Conti



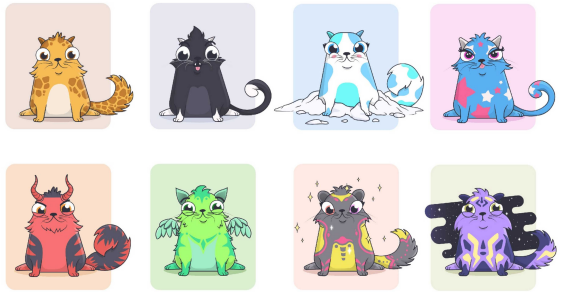
ethereum

DeFi Building Blocks and Services (I): Asset Tokenization

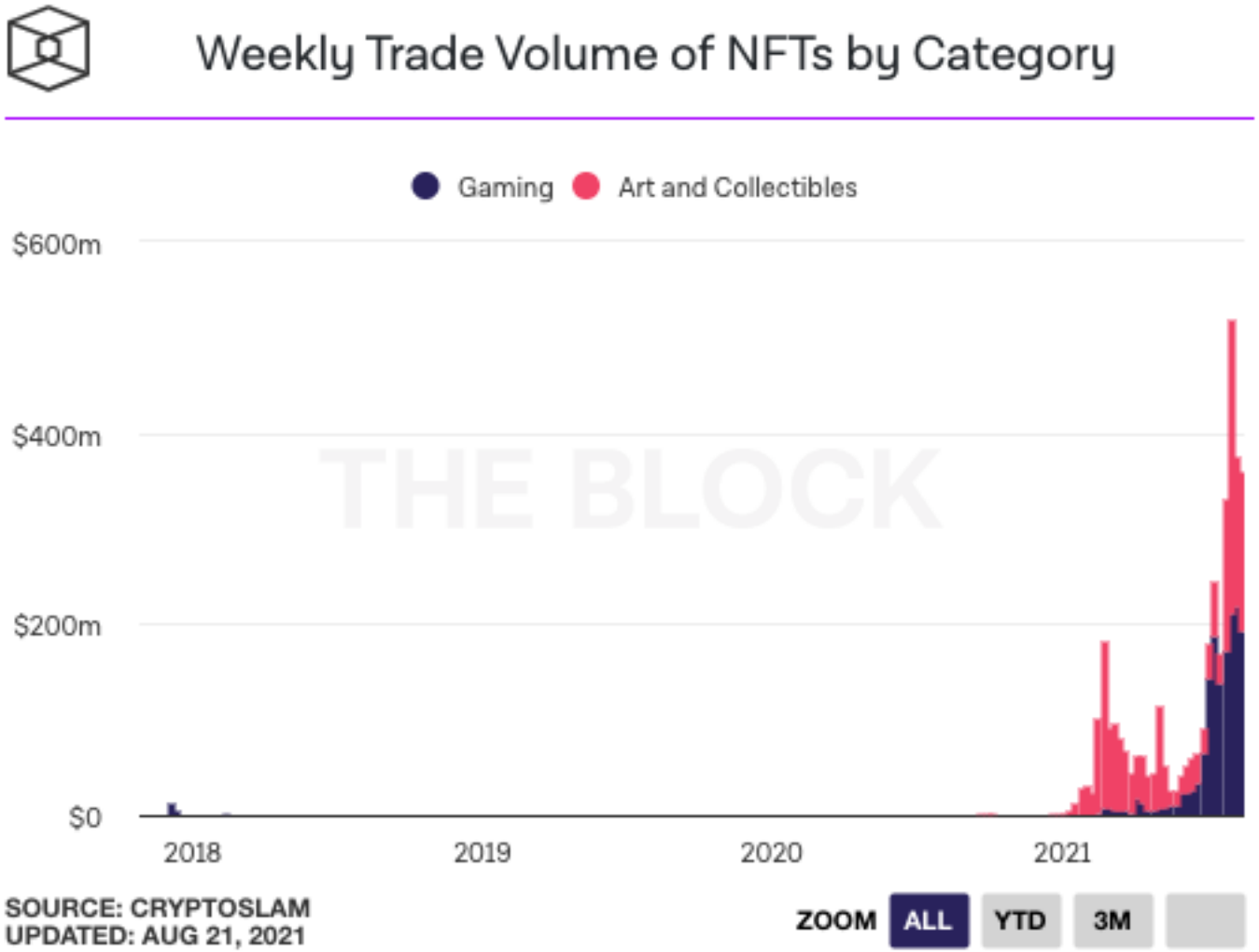
Asset Tokenization

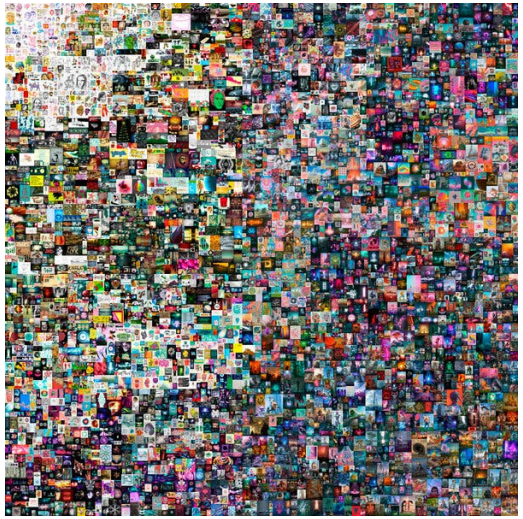
- Tokenization: process of adding new assets to a blockchain
- Token: the blockchain representation of the asset
- Make assets more accessible, easy to transfer, programmable
- Governance token, security tokens (tokenized real estate), Non-fungible token (NFT), stablecoin

NFT



Cryptokitties
Fall 2017





“Everydays — The First 5000 Days”
by Beeple, sold for $69.3M, 03/11/2021

Stablecoin

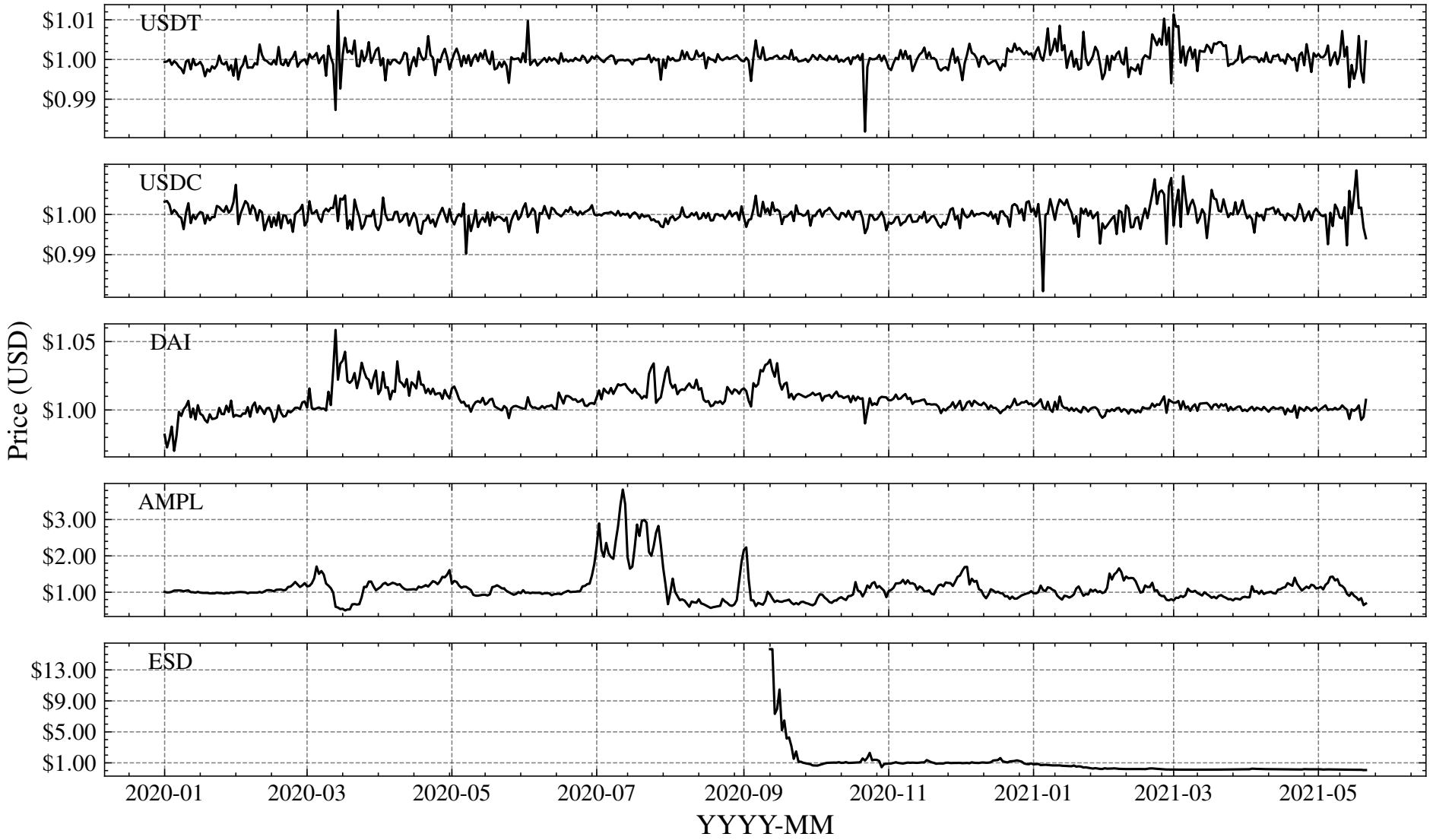
- Offchain (centralized) collateral [fiat, precious metal]
- Onchain (decentralized) collateral [crypto assets]
- Algorithmic (non-collateral) stable coin

CURRENCY	MARKET CAPITALIZATION	COLLATERAL TYPE
Tether	$64,209,563,142	Fiat
USD Coin	$27,450,355,929	Fiat
Binance USD	$11,923,057,774	Fiat
Dai	$5,724,814,479	Crypto
TrueUSD	$1,292,072,149	Fiat
Paxos Standard	$944,424,017	Fiat
HUSD	$489,713,563	Fiat
PAX Gold	$318,754,237	Precious metals
sUSD	$310,485,789	Crypto
Gemini Dollar	$253,561,503	Fiat

Aug 2021

source

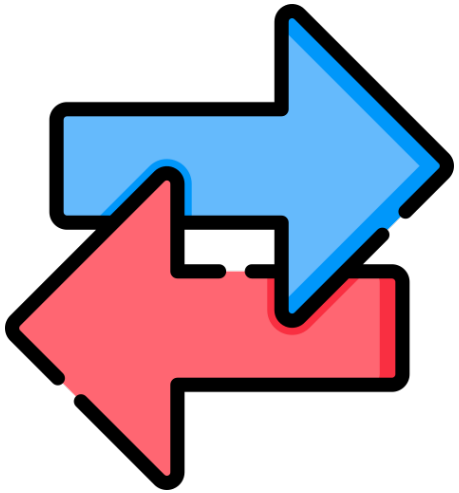
Stablecoin (In-)stability



DeFi Building Blocks and Services (II): Decentralized Exchange

DEX vs. CEX

- Centralized exchange (CEX)
  - Custodial
    - attacks on CEX
      - Mt. GOX (2014): over 800,000 bitcoins stolen (over $450M at the time, over $30B currently)
      - 2019: over 12 CEXes attacked, $300M crypto stolen
    - Rogue CEX
  - Non-transparency
- Decentralized exchange (DEX)
  - Non-custodial
  - Transparency



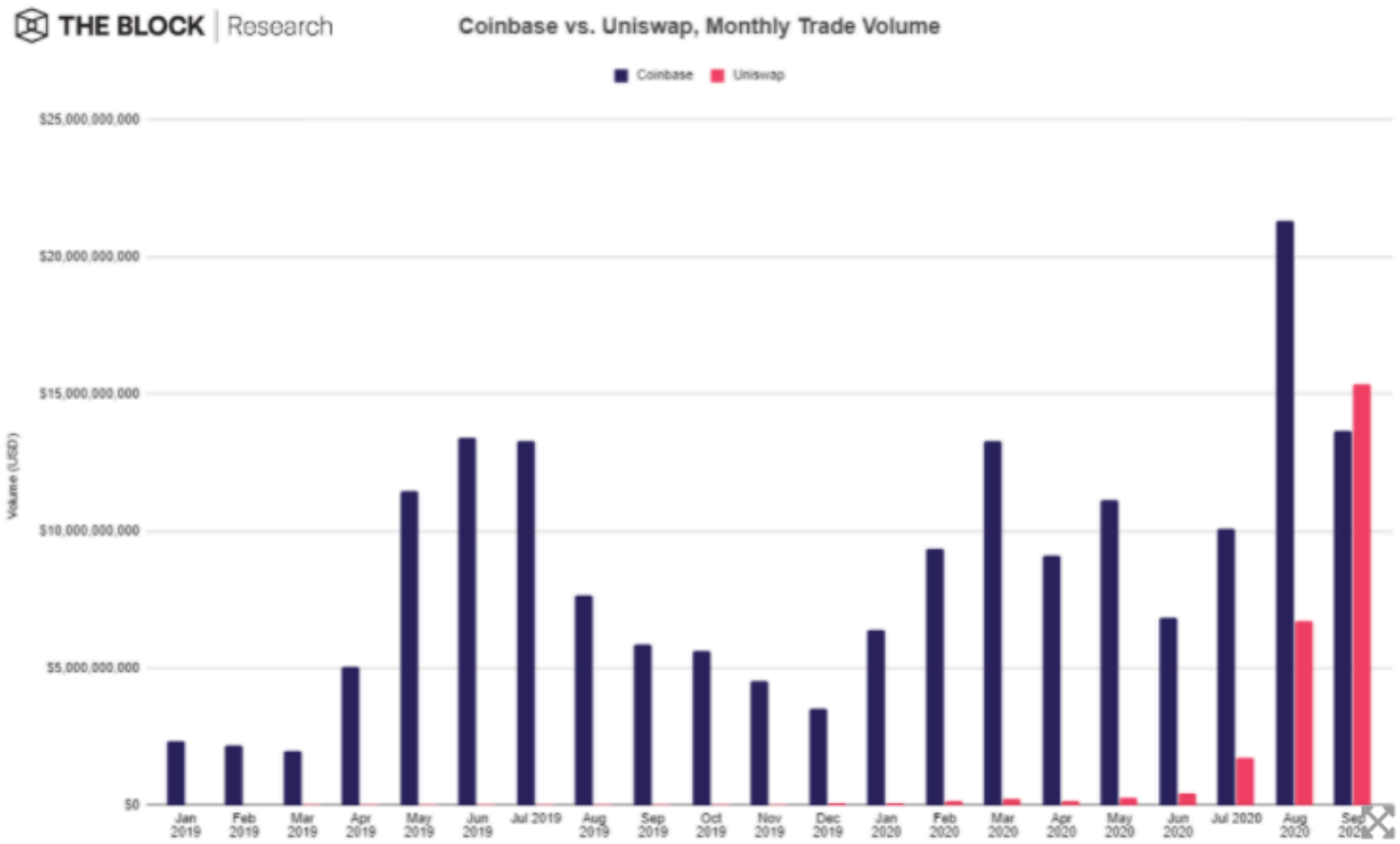
DEX vs. CEX

- CEX:
  - Order book
- DEX:

Protocol name	Protocol type	Price discovery
0x	Exchange	Off-chain order books
(Air)Swap	P2P / OTC	P2P negotiation
Bancor	CFMM	Smart contract
Balancer	CFMM	Smart contract
Curve	CFMM	Smart contract
Kyber Network	Reserve aggregator	Proposal by maker
UniSwap	CFMM	Smart contract

NOTE: CFMM, constant function market maker.

DEX vs. CEX



Source: Dune Analytics, CryptoCompare

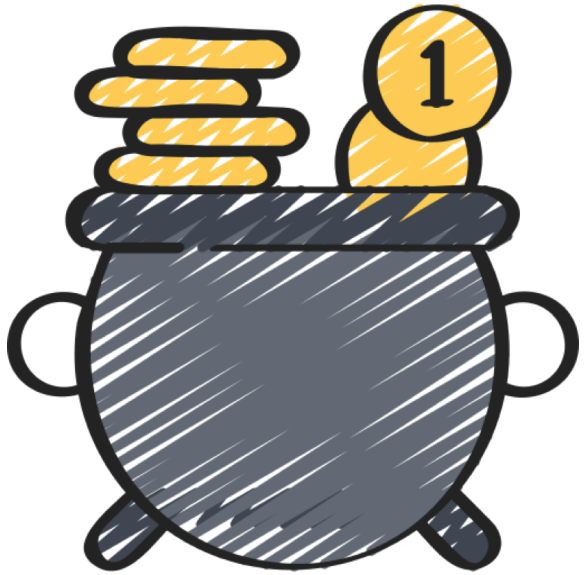
DeFi Building Blocks and Services (III): Decentralized Lending

Decentralized Lending

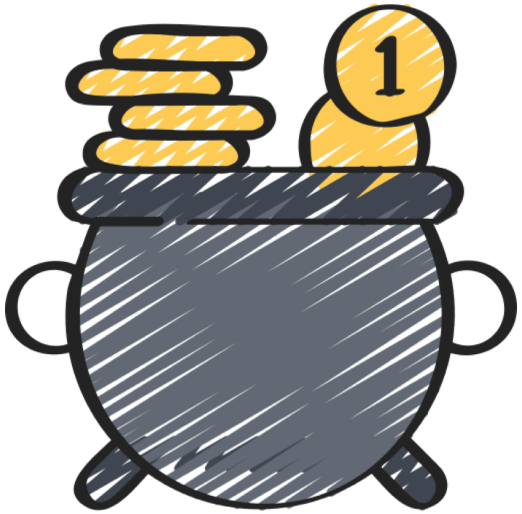
- Lending in CeFi:
  - Processing default is expensive; under-collaterization
  - Credit-worthiness
- Collateralized loans in DeFi
  - Over collateralization; not based on credit
    - Collateralized debt positions: creating new tokens using collateral
      - E.g., MakerDAO
    - Collateralized debt markets:
      - Pooled collateralized debt markets: e.g., Compound, Aave
      - P2P collateralized debt markets
  - Under collateralization

Flash Loans

- Blockchains enable *atomic* transactions
  - The actions within a transaction are *executed entirely in sequence*, or *fail collectively*
- Pools lend assets within one transaction
  - Under the condition that the assets
    - are paid back by the end of the transaction
    - plus interests on the lent amounts
  - Can grow to Billions of USD
    - without upfront costs (only transaction fees)
- Does not exist in CeFi!



Flash Loans

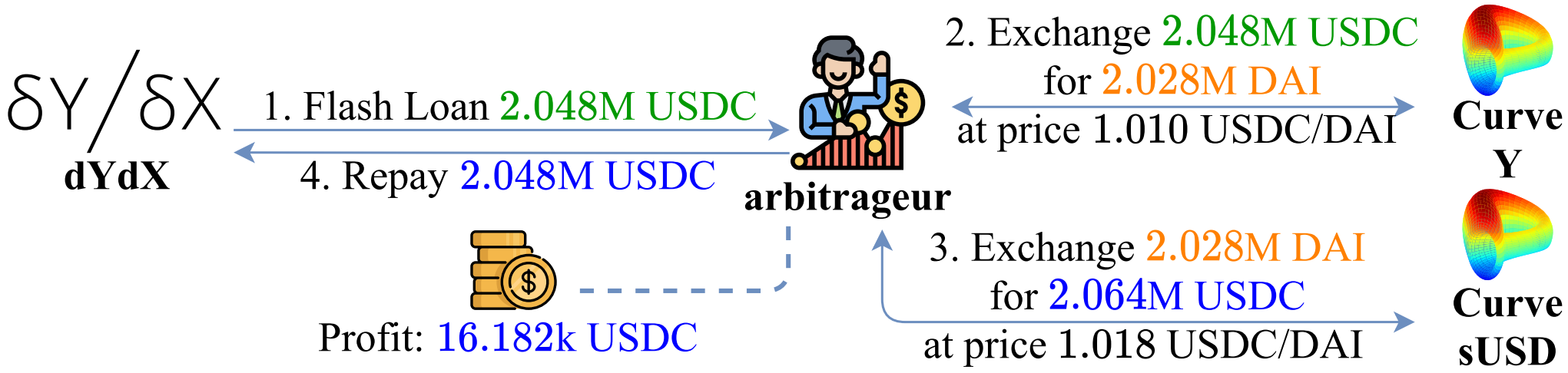


1. Take flash loan

2. go-Wild(loan);

3. Repay loan + interest

Flash Loan Example



Other DeFi Building Blocks and Services

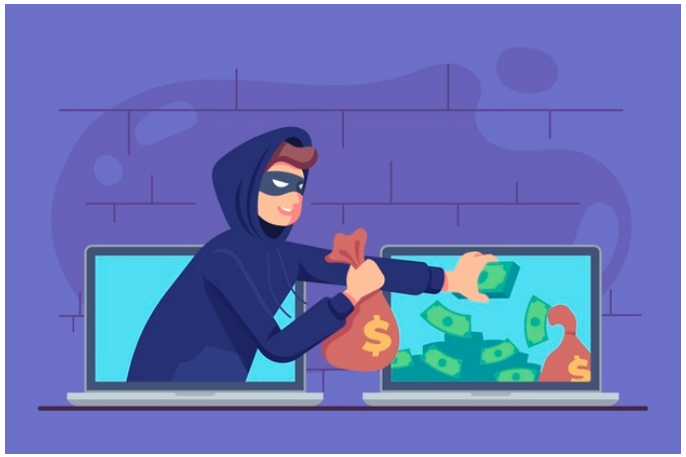
- Decentralized derivatives
  - Asset-based derivatives: e.g., Synthetix, Mirror
  - Event-based derivatives: e.g., Augur
- On-chain asset management
  - Non-custodial, different from traditional asset management
  - Semi-automatic rebalancing of portfolio, trend trading
  - E.g., Yearn, Set protocol
- Decentralized insurance


Risks in DeFi
https://defi-learning.org

DeFi Security

DeFi Security - Issues on all Layers

- Network attacks
  - Eclipse/Dos attacks
- Consensus attacks
  - 51% attacks/Double-spending/Selfish mining
- Smart Contract code bugs
  - Reentracy/Authorization/etc
- DeFi Protocol Composability attacks
  - Excessive arbitrage between pools, flash loans
  - Oracle attacks
- Bridge attacks
- Governance attacks



DeFi attacks stole over $1B in 2021

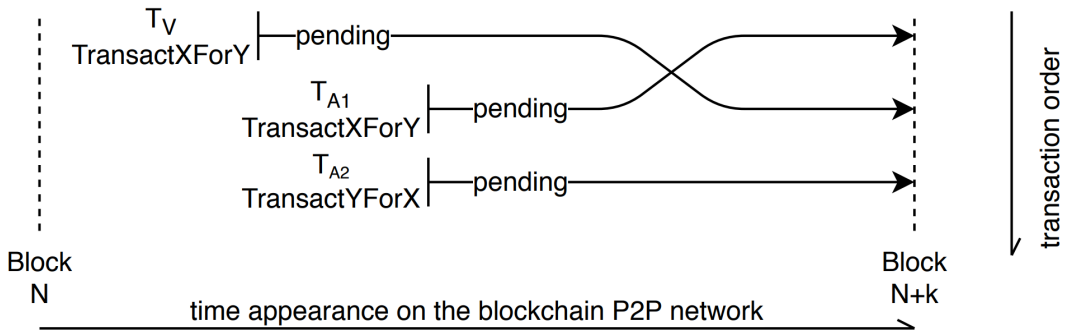
DeFi Security

- Technical structure security
  - Risk-free profit by exploiting technical structure of blockchain systems
- Economic incentive security
  - Exploit the incentive structure of the protocol to realize unintended profit at the expense of the protocol or its users

Front-running Attacks

1. Adversary ($\mathcal{A}$) observes a transaction $\mathcal{T}$ on the blockchain P2P network
2. $\mathcal{A}$ creates a transaction $\mathcal{T}2$ that pays a higher transaction fee (gas)
3. Miners mine transactions based on their paid fee, execute $\mathcal{T}2$ before $\mathcal{T}$
4. Same technique can be used to back-run a transaction

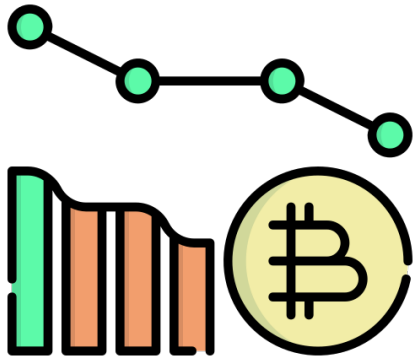
   → Sandwich attacks 🥪



Miner Extractable Value (MEV)

DeFi Dependencies & Systemic Risks

- Multiple significant price declines in cryptocurrencies
  - -30% on the 12th of March 2020
  - -40% on the 19th of May 2021
- Causing ripple effects
  - Liquidation
  - De-leveraging
- Stock markets have circuit breakers to stop losses
- Transaction fees on blockchains spiked, a regular coin transfer costed over 100 USD

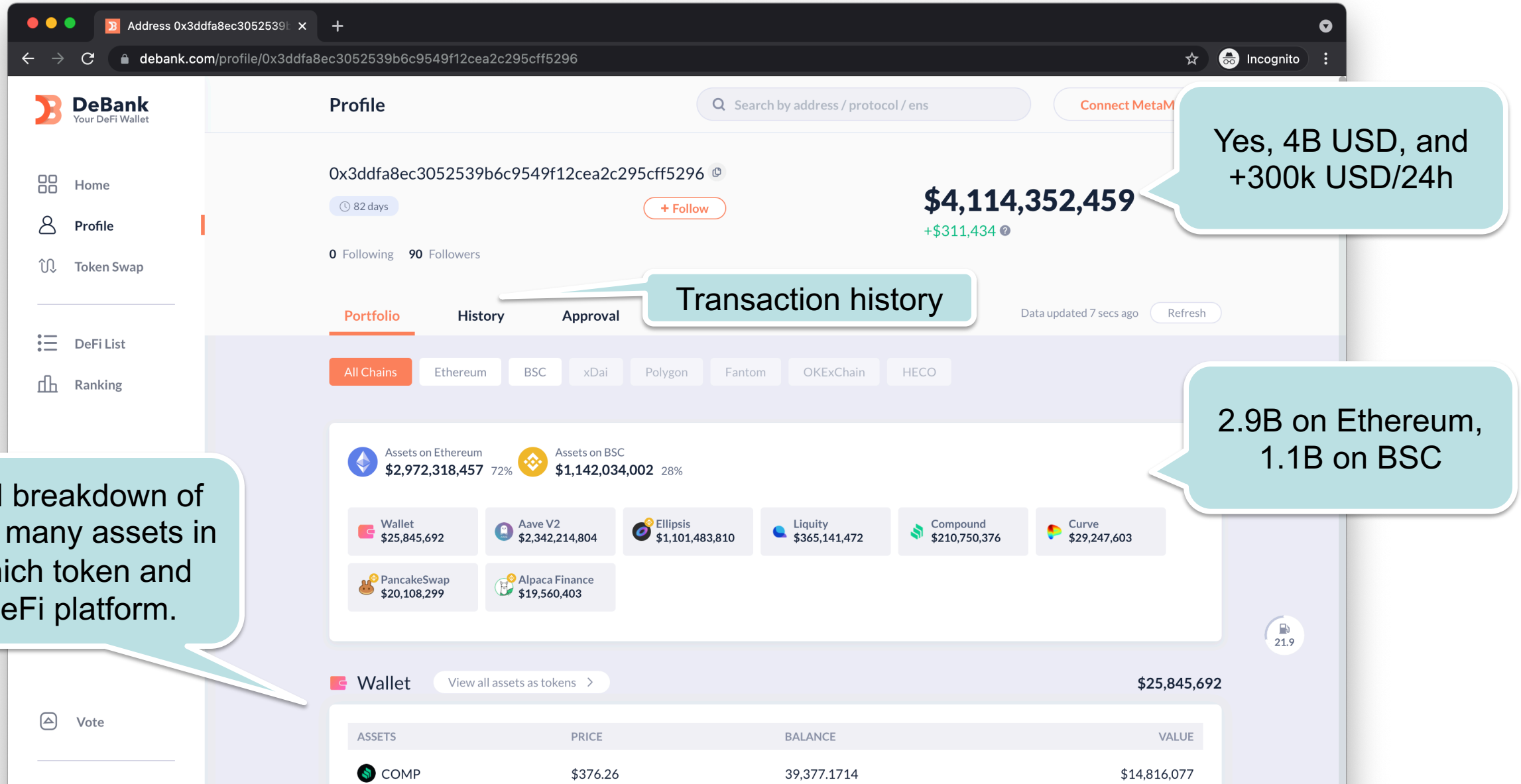


DeFi Privacy

Privacy in DeFi

- Blockchains with DeFi are mostly pseudonymous, not anonymous.
- Balances, transactions, timestamps, amounts are all public.
- See the many super-wealthy DeFi accounts for yourself..

(Non-existent) Privacy in DeFi



https://defi-learning.org

Open Research Challenges

- Scalability
- Universal accessibility; usability
- Privacy (privacy with compliance)
- Security
  - Oracle
  - Program/protocol analysis and verification
    - Protocol security
    - Smart contract security
  - Composability risks/systemic risks
  - Incentive design
  - Miner extractable value
  - Governance
- Legal framework

Interdisciplinary Research

- Explore open questions in DeFi
  - For each financial function, investigating CeFi & DeFi options:
    Is either one of these optimal? We will evaluate both through the lens of CS and finance. Is the application computable (efficiency, decidable), programmable (automatic)? Is the application welfare-enhancing and stable (not a source of systemic risk). How do the new and old systems interact?
- Intersection of Finance & Computer Science
  - Investigate through both lenses
- New questions and challenges in regulation and legal frameworks

Course Syllabus

Date	Topic
08/26	Introduction and Overview of DeFi
09/02	Introduction to Blockchain Technology
09/09	Introduction to Smart Contracts
09/16	Introduction to Traditional Finance
09/23	Stablecoins
09/30	DEX
10/07	Decentralized Lending
10/14	Synthetic And Derivatives; Portfolio Management; Insurance; Information and Data Markets
10/21	Oracles
10/28	Privacy in DeFi; Auditable Privacy; ZKP
11/04	Decentralized Identities
11/11	No Class (Veterans Day)
11/18	DeFi Security I
11/25	No Class (Thanksgiving)
12/02	DeFi Security II
12/09	Regulations and Legal Frameworks


DeFi
Traditional Finance
This is the beginning of the end