Dimitrios Karyampas, PhD
College of Management of Technology, Financial Engineering

FIN-413: Financial applications of blockchains and distributed ledgers

Dimitrios Karyampas, PhD
February 19, 2024

Outline

1. Introduction into blockchains

2. TradFi

Outline

1. Introduction into blockchains

2. TradFi

Where it all starts....

Money

"Money in fact is the most successful story, ever invented and told by humans, because it is the only story everybody believes." Yuval Harari

Money is made of:

- Story: people believe in it
- Trust: security and sound governance
- Features:
  - store of value: maintains its value over time
  - unit of account: a standard numerical unit of measurement of market value of goods and services
  - medium of exchange: can be used to transact goods and services

Money features

Additional features:

- Fungible: one unit is interchangeable with another
- Durable: must be able to last while being used repeatedly
- Portable: can be easily carried
- Uniform: all versions of the same denomination have the same purchasing power
- Acceptable: everyone must be able to use it for transactions
- Divisible: can be divided into smaller units of value
- Limited in supply: the supply of money in circulation ensures values remain “relatively” constant

Digital money

- Speed: today it typically take days to clear traditional cross border transactions; can we achieve transactions made in seconds, with $t + 0$ settlement?
- Trust: no single entity that can control the system; hard to hack
- Transferability and access: programmable or smart money based on fully executable code and easy to integrate in various applications

History of blockchain

- **1982 David Chaum** proposal for a blockchain protocol; later (1995) becoming DigiCash /eCash
- **1991 Stuart Habel & Scott Stornetta** chain of blocks - Merkel Tree
- **1994 Nick Szabo** smart contracts & a decentralized digital currency Bit Gold (1998)
- **1997 Adam Back** Hashcash a proof-of-work system used to limit E-mail spam
- **1998 Wei Dai** B-Money an anonymous and distributed electronic cash system
- **2008 Satoshi Nakamoto** Bicoin: A peer-to-peer electronic cash system

History of blockchain

Principles and features:

- Auditable database
- Time stamp applies to all transactions; append only logic on entries
- Cryptography to secure accounts and transactions
- Decentralized consensus mechanism
- Publicly available - anyone being able to run nodes, execute and view transactions, etc
- Rewards for those participants security the network and processing transactions
- Gradual introduction of supply
- Limited supply (cap - 21mln for bitcoin)

Bitcoin supply

Decentralized network

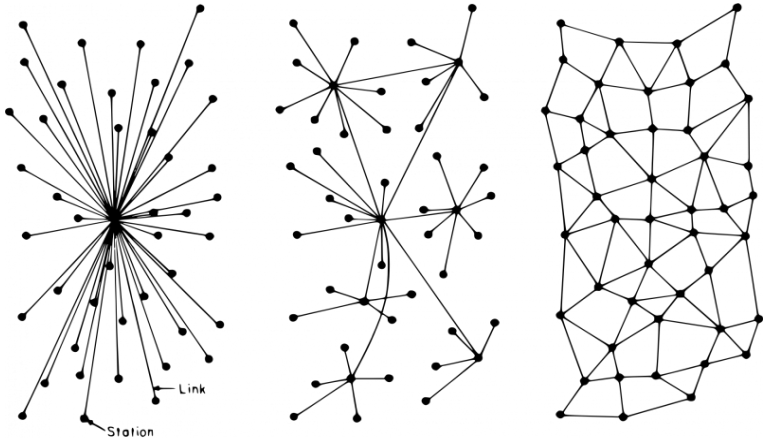


FIG. 1 — Centralized, Decentralized and Distributed Networks

Few terms...

- Hash Function - digital fingerprint of data; a function that can be used to map data of arbitrary size to fixed-size values
- Private / Public key - used to create digital signatures to approve transactions
- Node - computer running Blockchain software. It can simply be a “listener” or contribute to the consensus
- Distributed Ledger - A non-centralized database
- Append only - values are only added one after another
- Consensus mechanism - procedure by which nodes agree and validate transactions
- Mining - consensus mechanism in Proof-of-Work blockchains. A node solves a computationally challenging task and adds to the chain a block

and few more...

- Permissionless DLT - no authority required to allow access and usage
- Private DLT - the exact opposite of permissionless
- Wallet - software that stores public & private key; a secure way for users to keep cryptocurrency balances and engage into transactions
- Cold storage - a wallet which is disconnected from the internet and connects only when a transaction needs to take place
- On- and off-ramp - conversion of fiat currency to crypto and vice versa
- Smart contracts - programs stored on a blockchain with executable code
- Oracles - on-chain data feeds DeFi apps use to reference prices
- Layers
  - Layer 0 - hardware, internet, connection
  - Layer 1 - foundation layer in charge of consensus process, block time, dispute resolution, etc
  - Layer 2 - scalability solutions to the base layer (L1); L1 is decentralized ecosystem while L2 is a third-party integration on top of L1 to enhance the number of nodes and the transactions/fees

Consensus layer

Consensus layer

- a public append-only data structure
- once data added, can never be removed
- all (honest) participants have the same data
- participants can add data
- anyone can add data (openess or not)

Compute layer

Compute layer

- DAPP is encoded in a program that runs on blockchain
- no single trusted 3^{rd} party exists and all source code is publicly available
- the program is executed by the parties who create new blocks
- and everybody can verify the state transitions

Application layer

Application layer

- user applications sit on top of the L1/L2
- examples:
  - aave
  - compound
  - uniswap
  - curve
  - dYdX
  - panoptic
  - ...

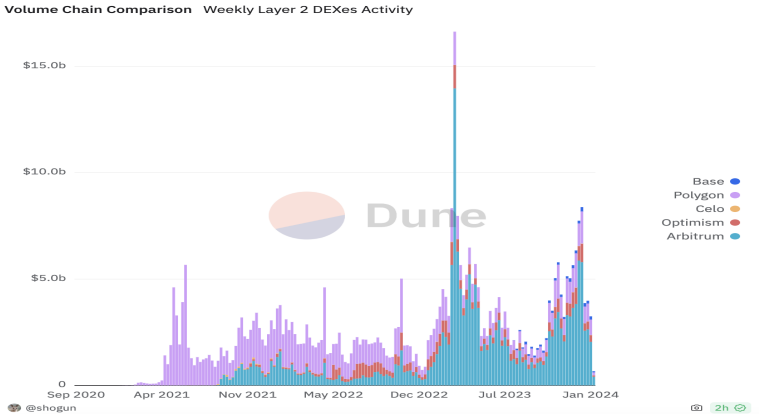
Layer 2s

Comparing Layer 2 Launches

company	layer 2	start	stage
OP Labs	**Optimism**	Jul. 13, 2021 18:00 UTC	Optimism announces Uniswap's launch on the L2 network.
Arbitrum	**Arbitrum One**	Aug. 31, 2021 21:00 UTC	Arbitrum One mainnet launches.
Matter Labs	**zkSync Era**	Mar. 24, 2023 10:00 UTC	zkSync Era mainnet opens to general users following a closed devnet period.
Polygon	**Polygon zkEVM**	Mar. 27, 2023 10:00 UTC	Polygon zkEVM beta mainnet launches.
Bybit / BitDAO	**Mantle**	Jul. 17, 2023 06:00 UTC	Mantle alpha mainnet launches.
Coinbase	**Base**	Aug. 09, 2023 00:00 UTC	The Base mainnet opens 'publicly' following a devnet period.
Consensys	**Linea**	Aug. 16, 2023 00:00 UTC	Linea mainnet launches publicly after a parnter-restricted alpha period.

KEYROCK

Layer 2s



Source: dune - shogun

Proof-of-Work vs. Proof-of-Stake

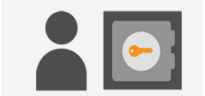
PROOF OF WORK

The probability of mining a block is determined by how much computational work is done by the miner.

A reward is given to the first miner to solve the cryptographic puzzle of each block.

Network miners compete with one another using computational power. Mining communities tend to become more centralized over time.

PROOF OF STAKE



The probability of validating a new block is determined by how large of a stake a person holds (how many coins they possess).

The validators do not receive a block reward, instead they collect network fees as their reward.

Proof of Stake systems can be much more cost and energy efficient than Proof of Work systems, but are less proven.

Gas

Each transaction has to pay a gas.... (for Ethereum)

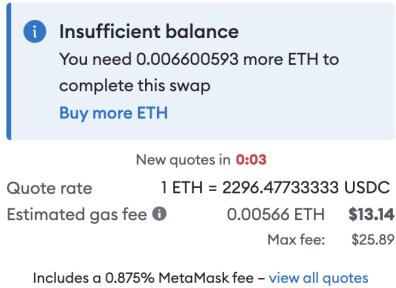
- Gas is the fee required to perform a transaction or execute a contract on the Ethereum blockchain.
- Fees are priced in fractions of ETH - denominations called gwei (10^{-9} ETH)
- Gas is used to pay validators for the resources needed to conduct transactions
- The price of the gas is determined by supply, demand, and network capacity at the time of the transaction

Some analytics can be found etherscan - gastracker or more visualizations in dune - 21co / Ethereum Key Metrics...

Gas

Each transaction specifies a gas limit and a price for the gas, in ETH

- ETH equivalent for the gas must be reserved up-front
- Following the transaction/contract execution, unused gas is refunded by to the wallet



Running out of Gas

- Any changes made to storage variables, any account transfers, are reverted to their state before this method call
- Gas fee for every instruction leading up to the exception are charged
- Like other exceptions, it can be caught by a handler function
- Methods can be invoked with just a portion of available gas

Smart contracts

dutchAuction.sol 1

```
// SPDX-License-Identifier: MIT
pragma solidity >=0.6.12 <0.9.0;

contract DutchAuction {
  /**
   * Implement the dutch auction for a token
   */
  uint public initialPrice;
  uint public bidPeriod;
  uint public offerDelta;
  uint public startTime;
  NFToken public token;
  address payable public seller;
  address payable winningAddress;

  function winAuction() public payable {
    uint timeElapsed = block.timestamp - startTime;
    uint currentPrice = initialPrice - (timeElapsed * offerDelta);
    uint retrieveBid = msg.value;
    require(winningAddress == address(0));
    require(timeElapsed < bidPeriod);
    require(retrieveBid >= currentPrice);

    winningAddress = payable(msg.sender);
    winningAddress.transfer(retrieveBid - currentPrice);
    seller.transfer(currentPrice);
    token.transferOwnership(winningAddress);
  }
}
```

NB: The contract code execution automatically makes transfer of the digital asset in the same transaction as the payment

Outline

1. Introduction into blockchains

2. TradFi

Traditional financial services (TradFi)

Finance is the management and movement of money. It builds products and services around:

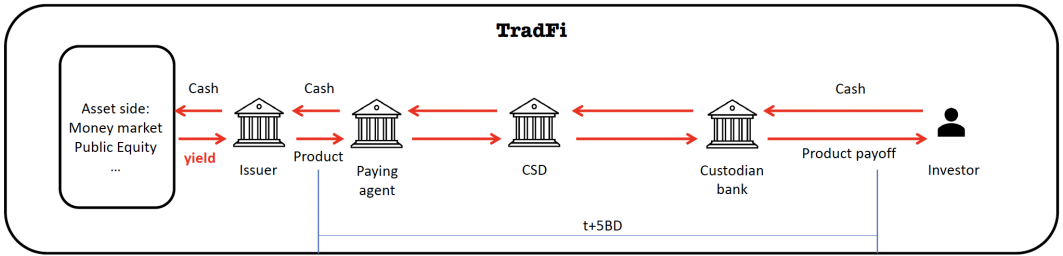
- pay
- invest
- trade
- save
- borrow
- risk manage

TradFi participants

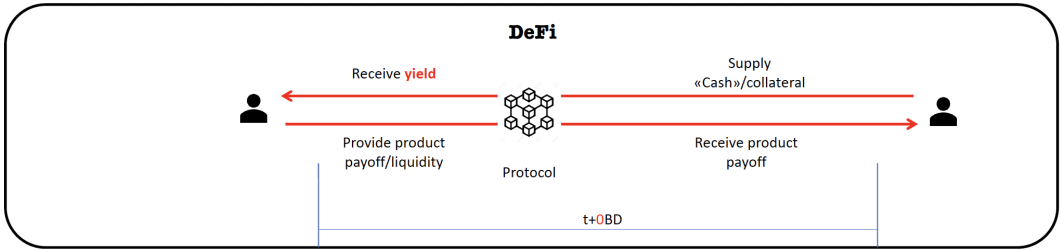
The system is organized in the following way and actors:

- Exchanges
- Custodians
- Brokers
- Clearing houses
- Security trustees
- Portfolio/Asset managers
- Banks (Retail/Commercial, Private, Investment)
- Auditors
- Regulators

TradFi - financial (structured) product life cycle



...teaser on how this works in Decentralized Finance (DeFi)



TradFi vs. DeFi

	Traditional Finance	DeFi
Custody	Held by institution or custody provider	Held directly by users in non-custodial accounts or via smart contract
Unit of Account	Fiat Currency	Denominated in digital asset or stable coin
Execution	Facilitated via intermediaries	Facilitated via smart contract
Settlement	~3-5 business days depending on transaction, during M-F business hours.	Seconds to minutes depending on blockchain, 24/7 operating times.
Clearing	Facilitated via clearinghouses	Facilitated via blockchain transaction
Governance	Specified by exchanges & regulators	Governed by the protocol developers & users
Auditability	Authorized third-party audits	Open source code & public ledger, can be audited by anyone
Collateral	Transactions may involve no collateral, intermediates take on risk	Over-collateral generally required.
Risks	Vulnerable to hacks and data breaches	Vulnerable to hacks and data breaches of smart contracts

Source: https://medium.com/racecapital/defi-infrastructure-101-overview-market-landscape-78e096a85834

Financial products of focus

Financial products

- Lombard loans
- Interest rate swaps
- Structured products
- Digital bonds

Contact details

Dimitrios Karyampas, PhD
Lecturer
dimitrios.karyampas@epfl.ch

EPFL
College of Management of Technology
Financial Engineering