Decentralized Finance & Blockchain Technology

Tutorial delivered at SIAM FM23, Philadelphia, on June 7th 2023

In preparation (sept.23): Book on quantitative issues

Emmanuel Gobet, École Polytechnique

Anastasia Melachrinos, Kaiko

07/06/2023

ABOUT

Kaiko

Founded in 2014, Kaiko is a global company providing financial institutions and corporate clients with **actionable** and **reliable** crypto-assets market data solutions.

- 2021 **revenues tripled** & doubled in 2022
- Successfully **acquired two companies**

Our four business units — **Market Data**, **Analytics, Indices**, and **Research** — empower our clients' use cases across the entire investment lifecycle.

AICPA SOC aicpa.org/soc4so

EU BMR Compliant

New York - London - Paris - Singapore

Market Data

Redistribution of tick level data and aggregates from 100+ CEX, patented proprietary DeFI data

BMR-Compliant Rates and Indices

shaping the market in an investable universe.

Quantitative Analytics

proprietary quantitative models & solutions to price and assess risk.

Research

industry-leading data driven research publications and market analysis

smart data

More advanced presentations during the conference

- ***Maxim Bichuch***: *Pricing by Stake in Decentralized Insurance*
- **Zachary Feinstein**: *Implied Volatility in Decentralized Finance from Automated Market Makers*
- **Andrew Papanicolaou**: *Manoeuvring and Investing in Yield Farms*
- **Philippe Bergault**: *Automated Market Makers: Mean-Variance Analysis of LPs Payoffs and Design of Pricing Functions*
- **Pierre-O Goffard**: *Mining Pool and Centralization in Proof-of-Work Equipped Blockchain*
- **Michael Allouche**: *Statistical Error Bounds for Weighted Mean and Median, with Application to Robust Aggregation of Cryptocurrency Data*
- **Anne-Claire Maurice**: *Unbiasing and Robustifying Implied Volatility Calibration in a Cryptocurrency Market with Large Bid-Ask Spreads and Missing Quotes*
- **Sebastian Jaimungal**: *Optimal Execution in Automatic Market Making Pools: Deep Reinforcement Learning and Galerkin Approaches*
- **Fayçal Drissi**: *Decentralised Finance and Automated Market Making: Predictable Loss and Optimal Liquidity Provision*
- **Ronnie Sircar**: *A Mean Field Games Model for Cryptocurrency Mining*
- **Agostino Capponi**: *The Adoption of Blockchain-Based Decentralized Exchanges*
- **Deborah Miori**: *DeFi: Data-Driven Characterisation of Uniswap v3 Ecosystem & an Ideal Crypto Law for Liquidity Pools*
- **Ciamac C. Moallemi**: *Automated Market Making and Loss-Versus-Rebalancing*
- **Marcello Monga**: *Decentralised Finance and Automated Market Making: Execution and Speculation*
- **Anastasia Melachrinos**: *Impermanent Loss in Automated Market Making*
- **Matheus V. Xavier Ferreira**: *Credible Decentralized Exchange Design via Verifiable Sequencing Rules*

Agenda

1. **Everything you need to know about Blockchains**
   a. Bitcoin: the blockchain revolution
   b. Ethereum: the blockchain evolution
   c. Blockchains Consensus
2. **How Cryptocurrency Exchanges Shape the Value of Digital Assets**
   a. Centralized and Decentralized Exchanges
   b. Exploring Automated Market Makers as a Novel Method for Asset Price Discovery
   c. Cryptocurrency Market Inefficiencies and Opportunities for Arbitrage Trading
   d. Valuing Cryptocurrencies in a multi-exchange world
3. **Cryptocurrency Derivatives Markets**
   a. Futures
   b. Perpetual Futures
   c. Options
4. **Lending & Borrowing Cryptocurrencies**
   a. Collateralized Debt Positions
   b. Pooled Collateralized Debt Markets
   c. Liquidations

Part 1

Everything you need to know about blockchains

a. **Bitcoin: the blockchain revolution**
   i. Bitcoin’s Goal
   ii. What’s a user in Bitcoin ?
   iii. The use of cryptography in Bitcoin
   iv. Signatures
   v. Hash functions
   vi. Why is it a chain ?
   vii. What does decentralization means ?
   viii. How are blocks created ?
   ix. How are bitcoins created ?
   x. Bitcoin’s added value

b. **Ethereum: the blockchain evolution**

c. **Blockchains Consensus**

Bitcoin's Goal

Bitcoin: A Peer-to-Peer Electronic Cash System

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

2009

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 hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

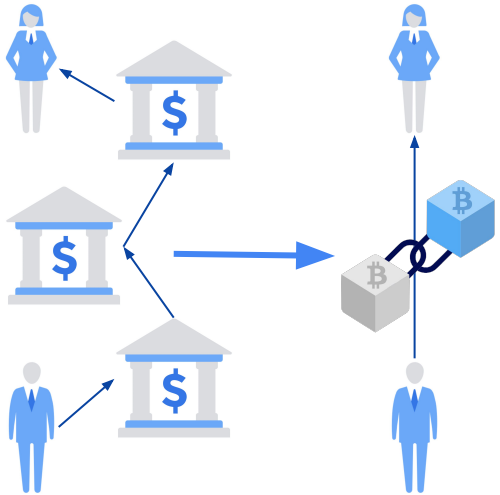
Source: Nakamoto, S. (2008). Bitcoin whitepaper. URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019).

Genesis

Introduced in the "Cypherpunks" Mailing list (Group of individuals interested in cryptography and privacy) in 2008

What is bitcoin about ?

Bitcoin is a peer-to-peer form of digital cash, enabling one individual to **transfer value** to another digitally **without the need for specific third-party intermediaries** to approve or deny the transaction.



A Revolution for trust, privacy, and security.

What do blocks contain ?

Blocks contain a simple list of transactions

Sender	Receiver	Amount
Nicolas	Bob	1 btc
Julien	Emilie	10 btc
Antoine	Emilie	5 btc
...	...	...
Emilie	Adrien	3 btc

Decentralized data ledger made out of blocks of transactions.

What is a user on Bitcoin ?

Traditional Digital Account

User: paul.dubois@gmail.com

Password: Pa55w0rd!!

The two values are not linked in any way, they can be modified independently

Pseudo anonymity & Security

Blockchain Account

Public key (or address):
031e7bcc70c72770d....75bf706

Private key:
60cf347dbc59d31c1...9818477

The two values are connected mathematically, but the private key cannot be deduced from the public key.

What do blocks contain ?

Blocks contain a simple list of transactions

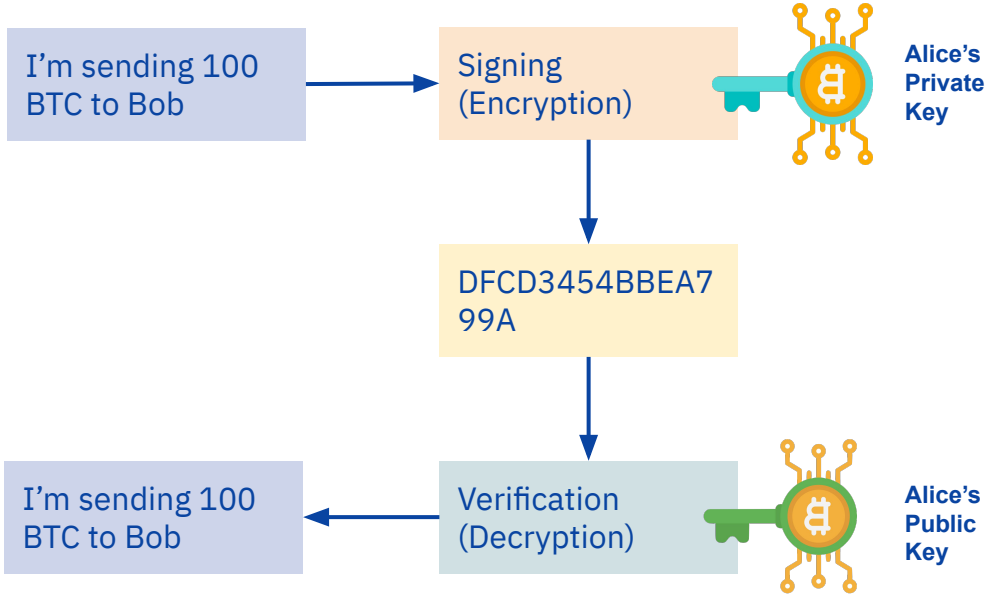
Sender	**Receiver**	**Amount**
0x123	**0x345**	1 btc
Julien	Emilie	10 btc
Antoine	Emilie	5 btc
...	...	...
Emilie	Adrien	3 btc

Signatures

Prove account ownership

(How do you know that the transaction has been actually initiated by this public key ?)

Manual signatures are meant to be unique to each individual in the world. However, they can be easily copied.



The signature demonstrates that a specific message was created by the holder of the public and private key pair, thereby authenticating a transaction by providing account ownership.

What do blocks contain ?

A block contains a simple list of **signed** transactions.

Sender	Receiver	Amount	Signature
bcc70c7…	79a9ef…	1 btc	**bc12…**
779a9e…	c59d31c…	10 btc	**a345…**
bc59d31…	c59d31c…	5 btc	**d63f…**
…	…	…	**…**
c59d31c…	06902a7…	3 btc	**f835…**

The signature allows anyone to check that the transaction has been created by the sender.

Hash Functions

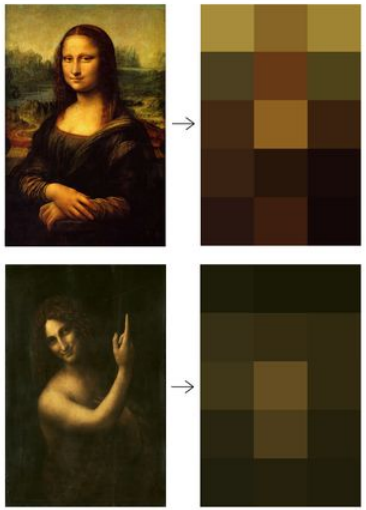
Hash involves applying a cryptographic **hash function (SHA-256)** to data, generating a relatively unique output for an input of almost any size.

Blockchain utilize cryptographic hash functions for various tasks, including:

(i) Generating unique identifiers (addresses)

(ii) Securing block data; a mining node hashes the block data, creating a hash stored within the block header

(iii) Securing previous blocks;



Example of hash function output:

Raw value	Hash value
Kaiko	6A4E1D47C2C35306DEB1E3168E80122B
Kaiko.	63B60AD7EF3AE3EC7BB0B529E6224A9C
Kaiko has awesome data	490B47C9D4761CEBC9AF4CA1BB4FD49A
"The entire official doc of Kaiko"	0BFA1B3EB9D22BFBA107990CBDC2D660

What do blocks contain ?

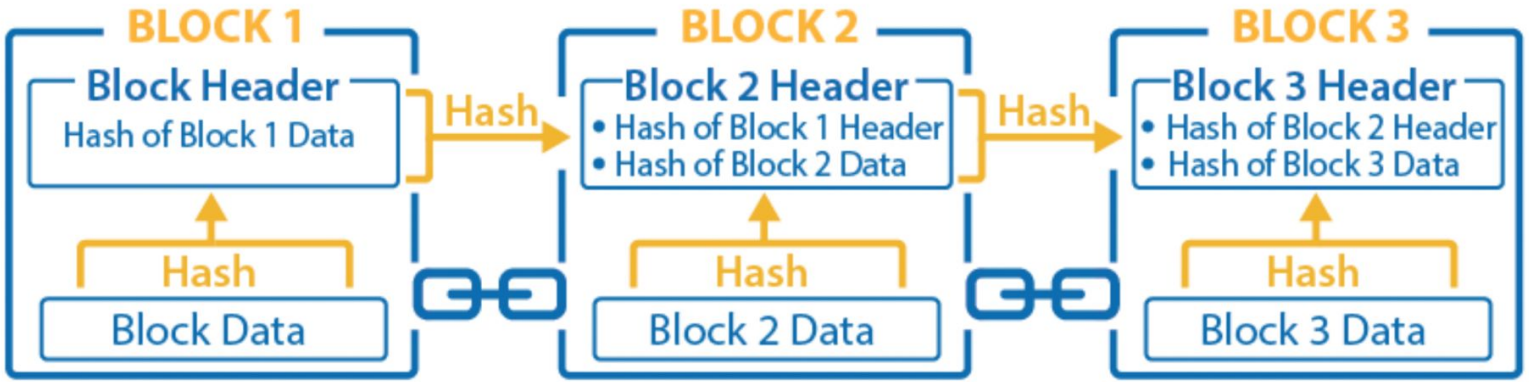
A block contains a simple list of **signed** transactions.

Sender	Receiver	Amount	Signature
bcc70c7...	79a9ef...	1 btc	**bc12...**
779a9e...	c59d31c...	10 btc	**a345...**
bc59d31...	c59d31c...	5 btc	**d63f...**
...	...	...	**...**
c59d31c...	06902a7...	3 btc	**f835...**

... and the mathematical summary (**hash value**) of this entire list

3fgd357fhgkv7

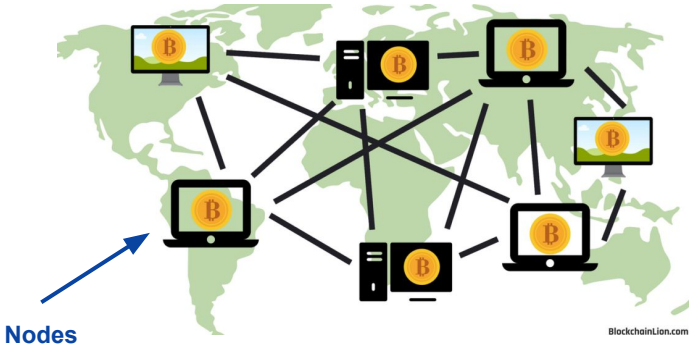
Why is it a chain ?

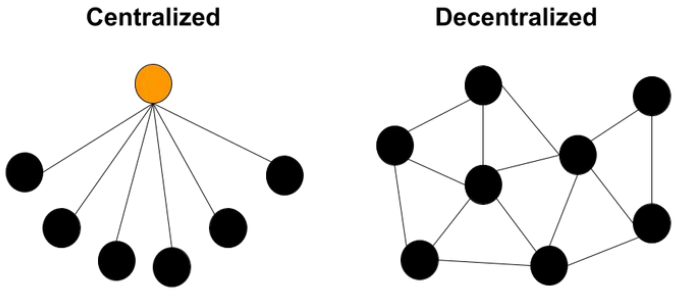


The current block header's hash will be incorporated within the next block's header. This link between blocks prevent any modification of the history.

Decentralization

When a block is created, it is sent to all the nodes of the network that check if this block is valid (transactions/hashes/signatures) or not before adding it to their chain.

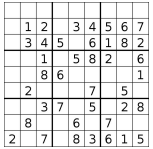




- Ethereum: 11,400 physical nodes in 80 countries
- Bitcoin: ~17000 nodes

How are blocks created ?

Some actors of the network are called **miners** and create the blocks.
In exchange, they receive bitcoin tokens as rewards.

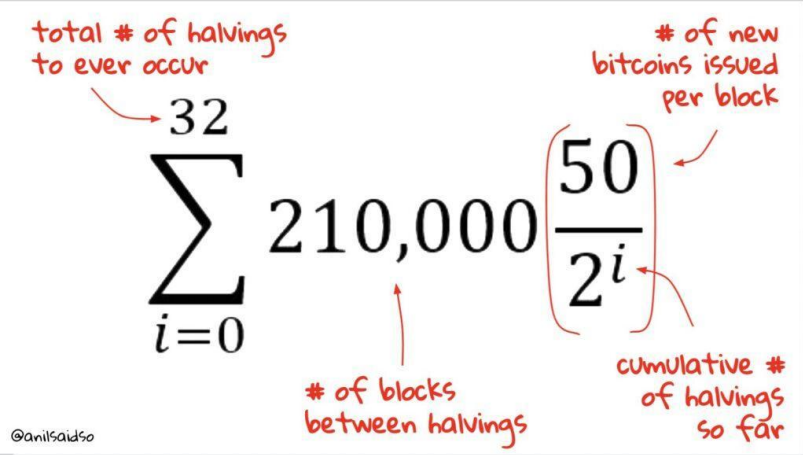


They compete against each other to solve a **mathematical puzzle**, similar to sudoku: time consuming to find a solution but very easy to verify.

The consensus used is called **Proof-Of-Work (POW)**

How are bitcoins created ?

Miners are paid in **newly created bitcoin** when they manage to create a block. The number of earned bitcoin per block is halved every 4 years in an event called **halving**.



The total number of bitcoin that will exist is **known and fixed** by an algorithm.

= 21 millions BTC

Part 1

Everything you need to know about blockchains

a. **Bitcoin: the blockchain revolution**
b. **Ethereum: the blockchain evolution**
    i. Why Ethereum ?
    ii. What is a smart contract ?
    iii. Example of a simple smart contract
    iv. Smart contract vulnerabilities & consequences
    v. ERCs
    vi. Blockchain Layers
    vii. Decentralized Finance
c. **Blockchains Consensus**

Why Ethereum ?

Bitcoin

Bitcoin allows transfers between users. It is like having a software that can do only one thing: **transactions**

Would be possible to have more features ? To allow more actions than simple transactions ?

Ethereum

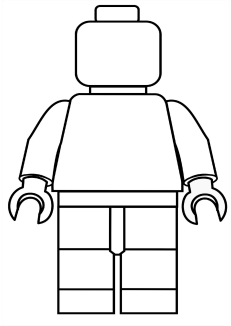
The Ethereum blockchain was born a few years after bitcoin, in **2014**.

The native crypto of that chain is called ether **(ETH)**.

Ethereum also allows direct **transactions** between users, but there is a major change: **Ethereum allows computer programs to run directly on the blockchain !**

What is a smart contract ?

Those **programs** are called smarts contracts
A smart contract has an **address** (just like a user) that users can interact with
A smart contract can **have, send and receive ethers.**



Hey, I'm a smart contract.

I promise you the following

1. **Immutable.** I will never modify or change your code.
2. **Authenticated calls.** I will always run the function you tell me too (assuming the code allows me!).
3. **Atomic.** I will never let code execution "stop half way" it is ALL or NOTHING with me.
4. **No privacy.** I like to gossip and I can't keep secrets - Everything you tell me will be public knowledge.

Example of a simple smart contract

```
1  pragma solidity ^0.5.1;
2
3  contract Timelock {
4    address payable public beneficiary;
5
6    uint256 public releaseTime;
7
8    constructor(
9      address payable _beneficiary,
10     uint256 _releaseTime
11   )
12     public
13     payable
14   {
15     require(_releaseTime > block.timestamp);
16     beneficiary = _beneficiary;
17     releaseTime = _releaseTime;
18   }
19
20   function release() public {
21     require(block.timestamp >= releaseTime);
22     address(beneficiary).transfer(address(this).balance);
23   }
24 }
```

Time lock contract

Idea: send ethers to a beneficiary that will be able to get them only after a certain date chosen by the sender.

ERCs

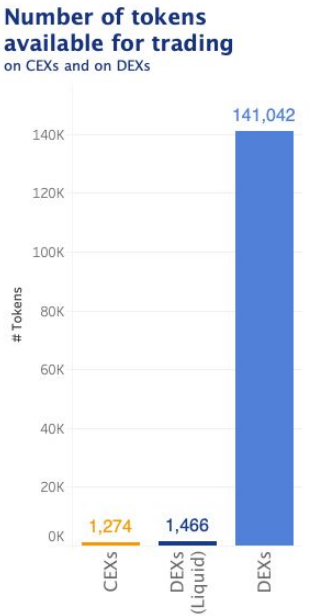
ERC = **E**thereum **R**equest for **C**omments

ERCs are equivalent to standards that the smart contract should follow, most famous examples:

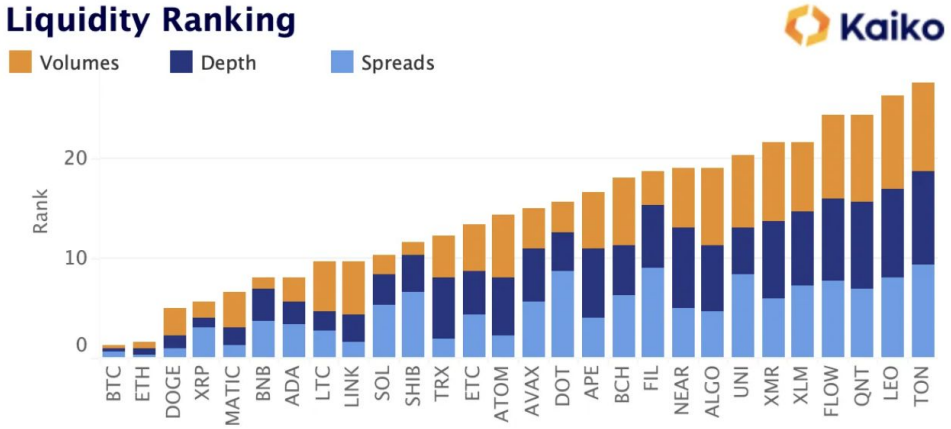
- **ERC-20**: creation of tokens on Ethereum. Examples: USDT, WETH, etc.

- **ERC-721**: creation of non fungible tokens on Ethereum (NFTs)

Tokens Diversity



180 fiat currencies in the world
vs
+ 100k tokens (cryptocurrencies)

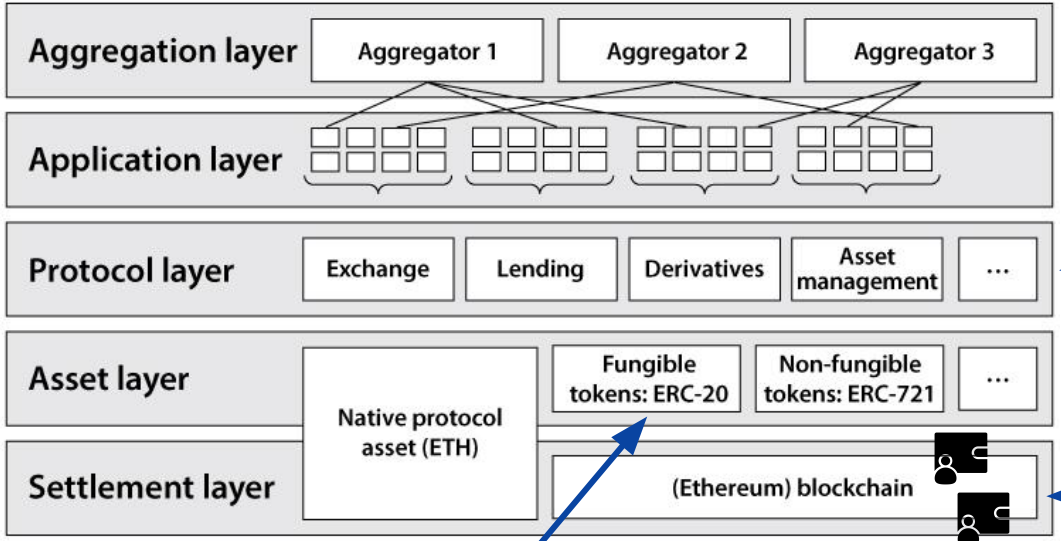


Source: Kaiko exchange data. Ranking for Average Daily Volume, Average 2% Daily Market Depth and Average Daily Spreads

Source: Ryder C. (2022). A New Model for Assessing Crypto Asset Liquidity. URL: https://blog.kaiko.com/a-new-model-for-assessing-crypto-asset-liquidity-d2f27af0ec8e.

ETH and BTC are currently the top two cryptocurrencies in terms of liquidity on crypto markets. However, occupying the third spot is DOGE, a meme coin that lacks a specific utility like BTC and ETH.

Blockchain Layers



Source: Schär, F. (2021). Decentralized finance: On blockchain-and smart contract-based financial markets. FRB of St. Louis Review.

Uniswap

Curve

DeFi is here
(DeFi = Smart Contracts)

Blockchain
infrastructure is here

People's **wallets**
(accounts) are here

Tradable Cryptocurrencies are here

Part 1

Everything you need to know about blockchains

a. **Bitcoin: the blockchain revolution**
b. **Ethereum: the blockchain evolution**
c. **Blockchains Consensus**
    i. Proof of Work
    ii. Proof of Stake
    iii. Blockchains Environmental Impact

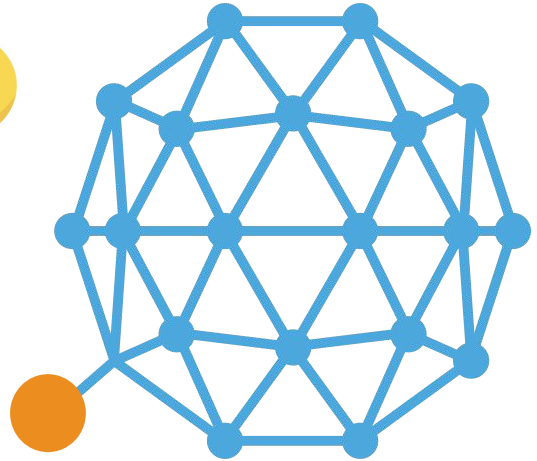
Proof of Work

Miners in competition
for validating a block

All miners except one,
fail = **Energy Waste**

THE WINNER TAKES IT ALL !

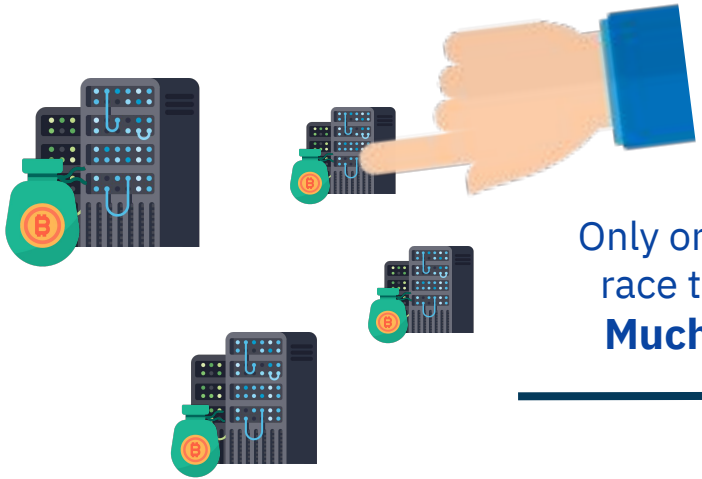
Bitcoin Blockchain



NEW BLOCK

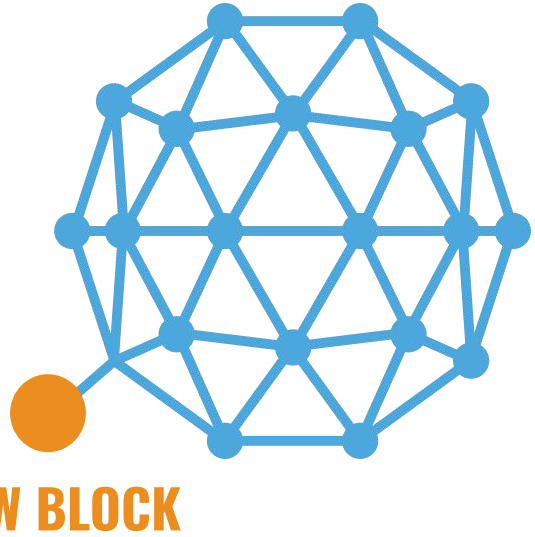
Proof of Stake

Stakers, Picked Randomly
to Create / Validate Blocks



Only one machine runs the
race to validate a block !
Much energy is saved

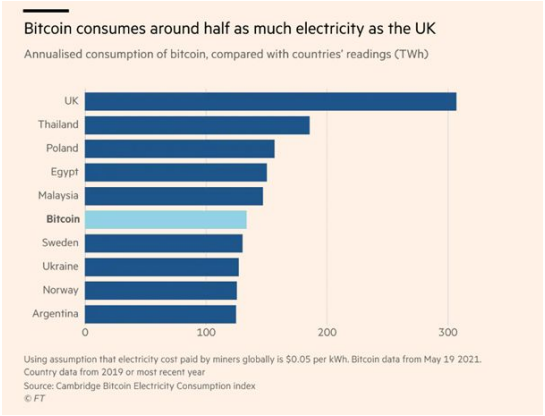
**Another Blockchain based
on Proof of Stake**



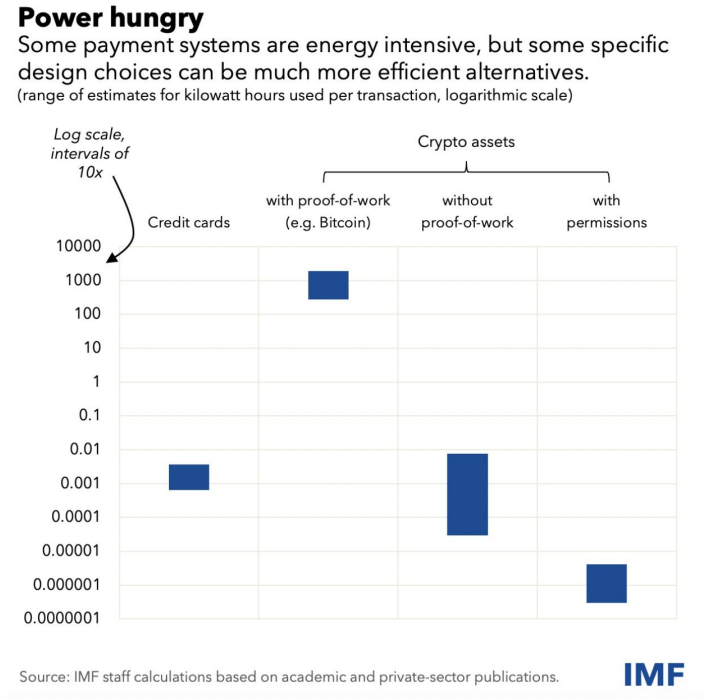
NEW BLOCK

Blockchains environmental impact

- In 2019, 65% of the crypto mining came from China, where coal made up around 60% of the energy mix
- In 2019, Bitcoin consumed as much electricity as Sweden, Ukraine, Norway, and Argentina.



Blockchains environmental impact



The research shows that proof-of-work crypto uses vastly more energy than credit cards. Replacing proof-of-work with other consensus mechanisms is a first green leap for crypto, and using permissioned systems is a second.

Agur, M. I., Deodoro, J., Lavayssière, X., Peria, S. M., Sandri, M. D., Tourpe, H., & Bauer, M. G. V. (2022). Digital Currencies and Energy Consumption. International Monetary Fund.

Blockchains environmental impact

40%-60%

Share of mining using renewable energy

In 2019

The Merge: Ethereum's switch from proof of work, to proof of stake

Blockchains environmental impact

WISE MINING

Get paid in Bitcoins to heat your house

VOLCANO MINING

Volcano-powered bitcoin mining

PROOF OF STAKE

A greener consensus mechanism

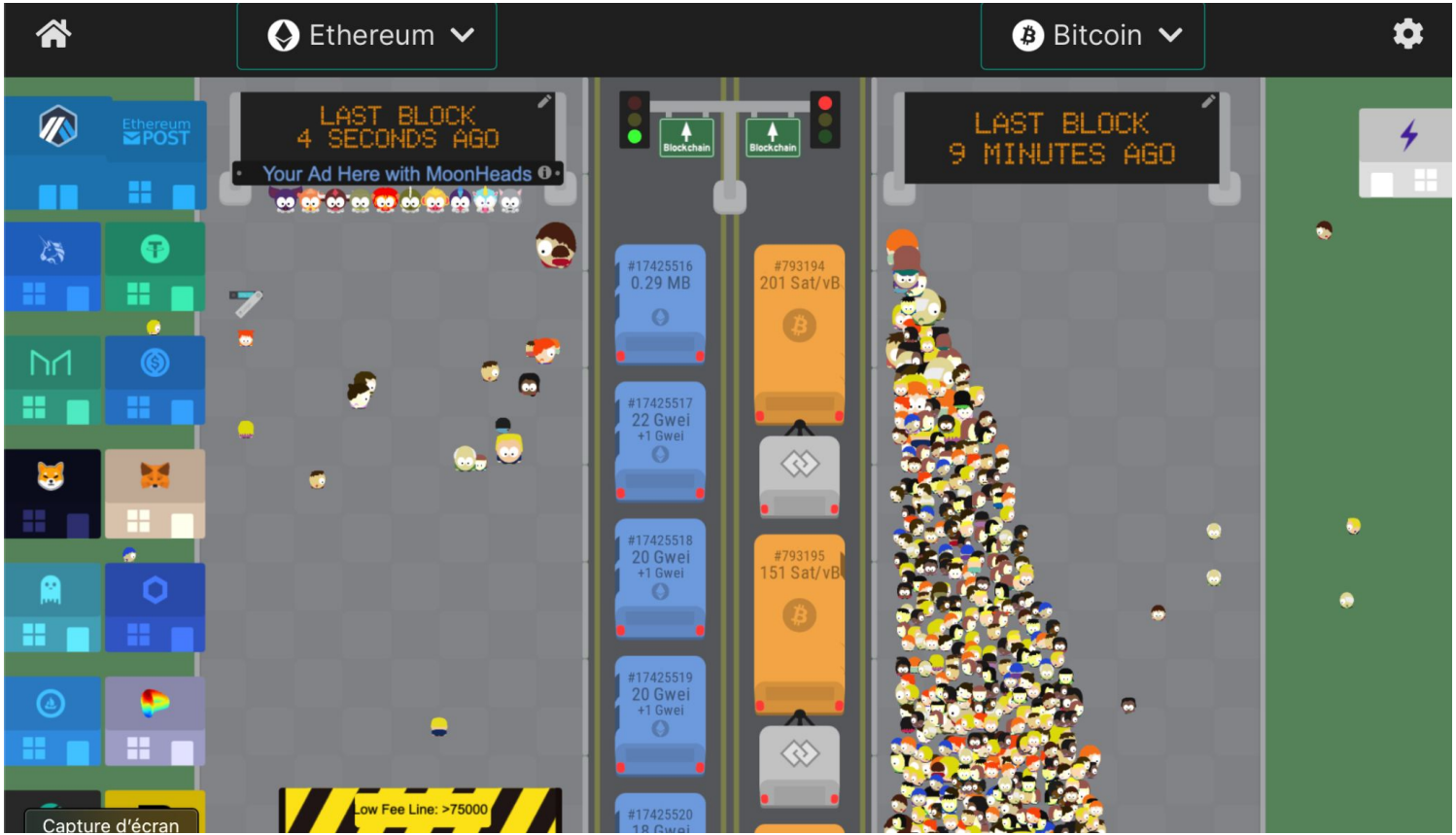
ALGORAND

The first neutral carbon footprint blockchain

MINT GREEN

Efficient capture and transfer of the heat generated by crypto mining

The Blockchain, now at https://txstreet.com

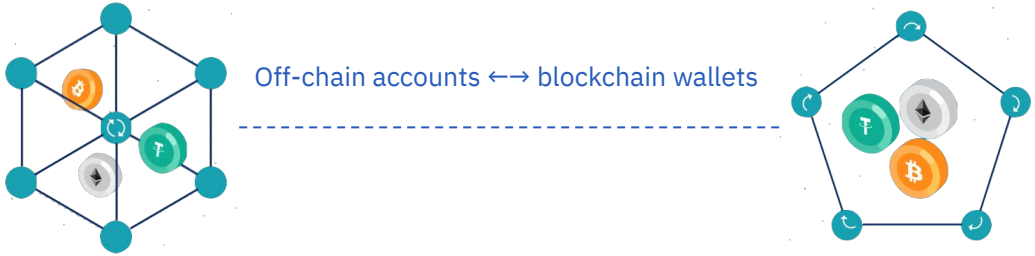


Part 2

How Cryptocurrency Exchanges Shape the Value of Digital Assets

a. **Centralized and Decentralized Exchanges**
   i. Differences Overview
   ii. Users Accessibility & Regulatory Challenges
   iii. Price Discovery Mechanisms Confrontation: Order books vs AMMs
   iv. The first DEX used an order book
b. **Exploring Automated Market Makers as a Novel Method for Asset Price Discovery**
c. **Cryptocurrency Market Inefficiencies and Opportunities for Arbitrage Trading**
d. **Valuing Cryptocurrencies in a multi-exchange world**

Differences Overview



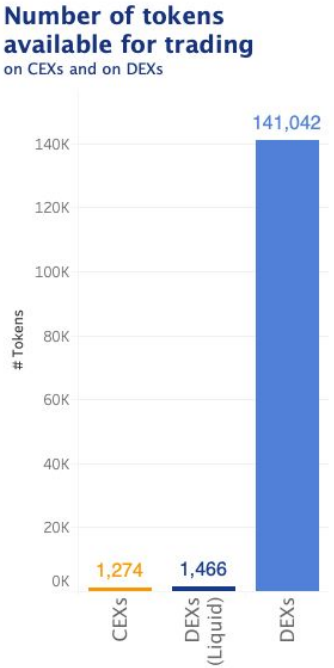
Centralized Exchanges (CEXs)

- Centrally managed (off-chain)
- Exchange controls your assets
- Listing fees and due diligence for new trading pairs
- Regulatory jurisdictions and KYC
- Barriers to market making
- Uses an order book
- You cannot trade if the exchange is down

Decentralized Exchanges (DEXs)

- Decentralized protocol (on-chain)
- You control your assets
- Anyone can list a pair by creating a new liquidity pool
- No regulation or KYC
- Anyone can be a market maker
- Automated Market Maker
- Data recorded directly on the blockchain

Differences Overview

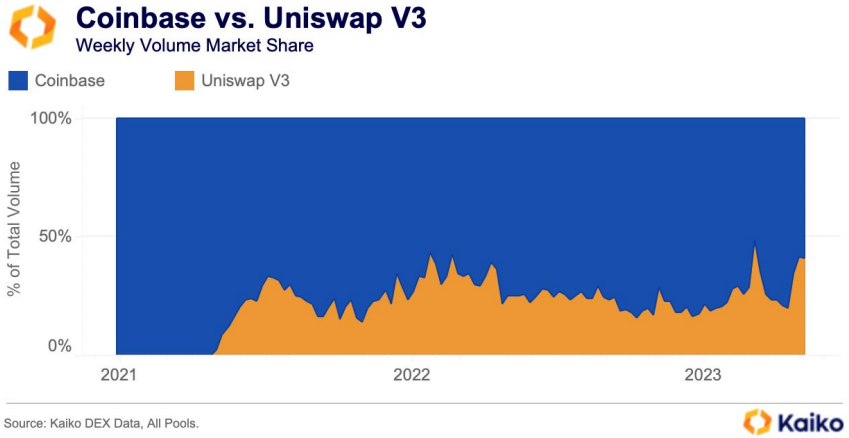


DEXs provide a larger tokens coverage than CEXs

DEXs facilitate trading of any cryptocurrency without requiring token issuers to pay for listing fees.

However, the majority of tokens available for trading on DEXs (98%) are non-liquid altcoins.

Despite this, DEXs offer more liquid tokens than centralized exchanges, with over 200 more assets.

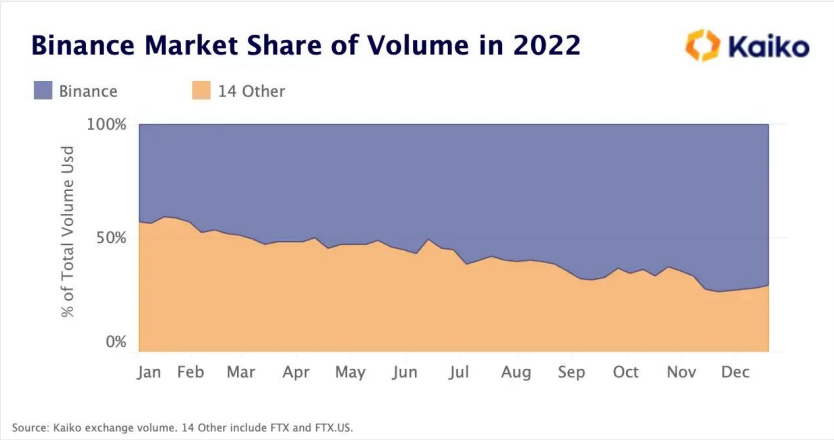


DEXs compete with CEXs on trading volume

Uniswap, the largest Ethereum DEX, emerged as a strong competitor to centralized exchanges in 2022 with its trade volumes nearly matching Coinbase's.

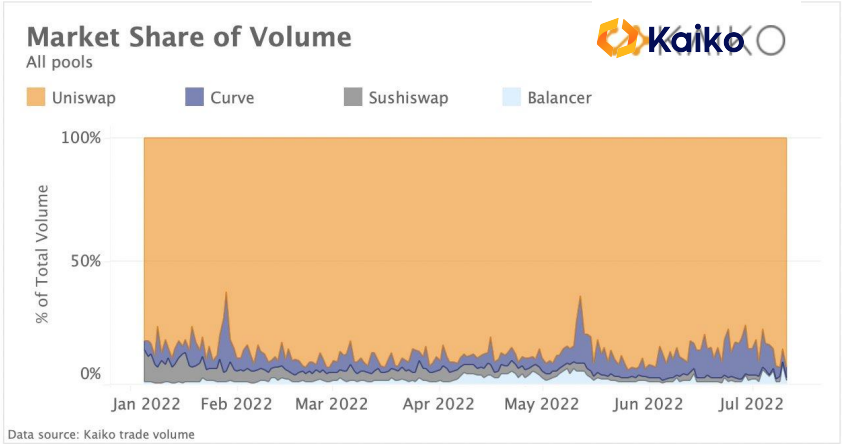
Differences Overview

High Market Concentration in Cryptocurrency Exchanges



CEXs

Binance removed fees for 13 BTC pairs in July, causing a surge in trading on its platform and market share to 72% compared to 14 other exchanges.



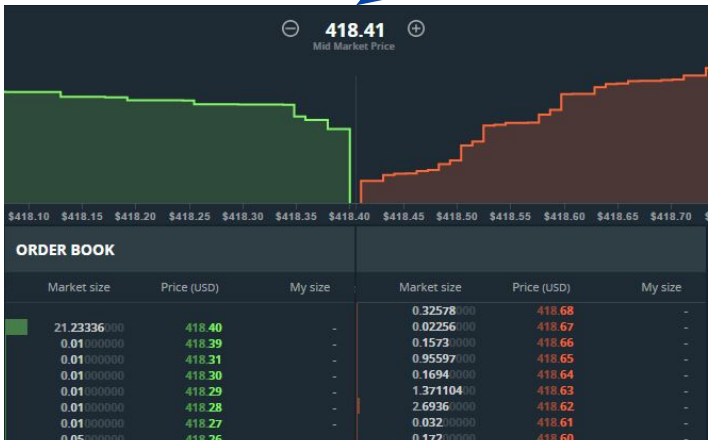
DEXs

Within the DEX category, Uniswap V3 accounts for between 80–90% of all daily volume

Price Discovery Mechanisms Confrontation:

Order books vs AMMs

Mid Price

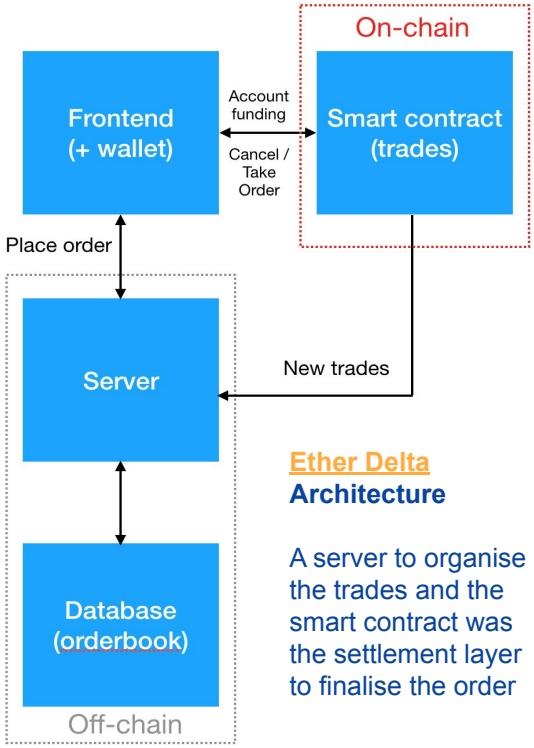


Makers
Provide liquidity by placing sell orders

Takers
Take liquidity by placing buy orders

A trade occurs if the buy / sell orders match up

The first DEX used an Order Book



Ether Delta
Architecture

A server to organise the trades and the smart contract was the settlement layer to finalise the order

U.S. SECURITIES AND EXCHANGE COMMISSION

EtherDelta still had a human component:

Gathering and presenting the list of orders

That was enough for the SEC to go after them

Why not just post all the orders to the smart contract?

Users will need to place a buy or sell order without any guarantee it is filled

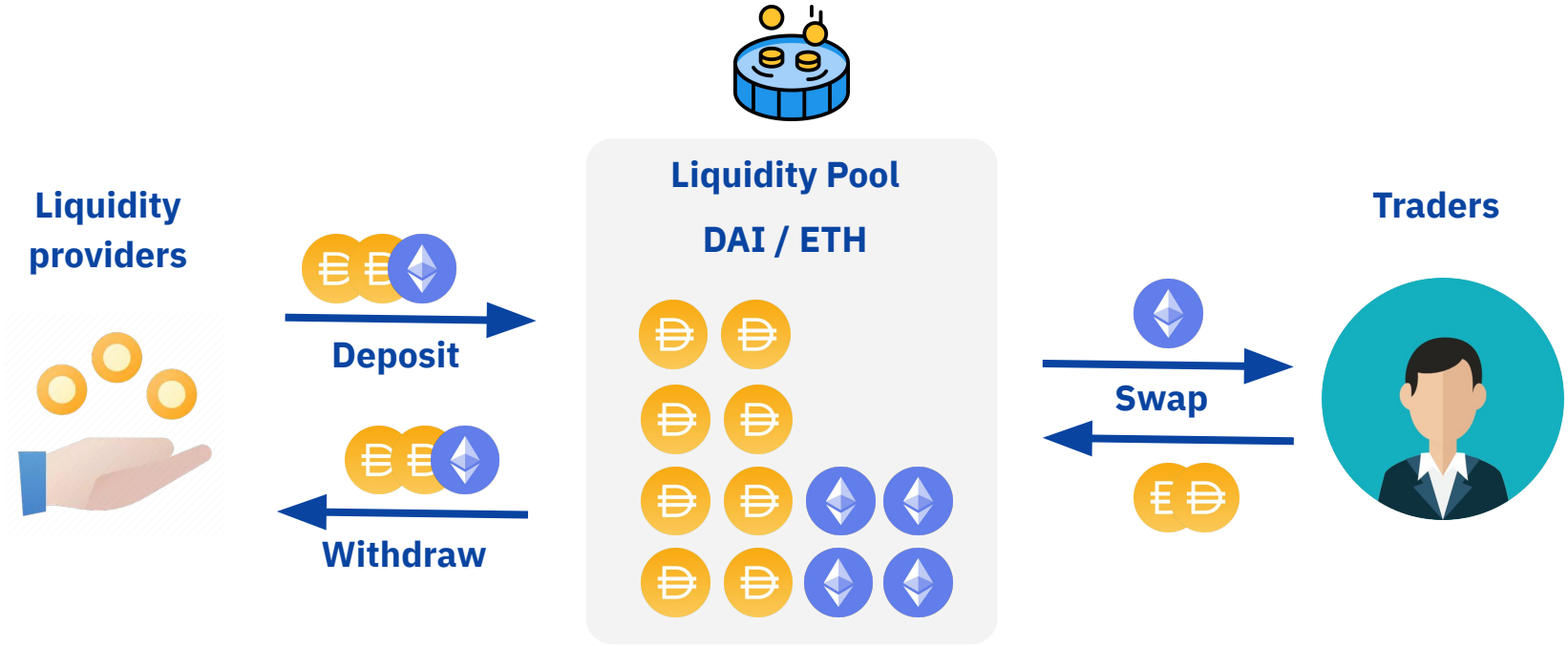
That is **financially expensive** and a network like Ethereum is **too slow** to handle orders bookkeeping.

Part 2

How Cryptocurrency Exchanges Shape the Value of Digital Assets

a. **Centralized and Decentralized Exchanges**
b. **Exploring Automated Market Makers as a Novel Method for Asset Price Discovery**
    i. Pools based DEXs General Functioning
    ii. The first AMM: Uniswap and its CPMM
    iii. Concentrated Liquidity on DEXs
c. **Cryptocurrency Market Inefficiencies and Opportunities for Arbitrage Trading**
d. **Valuing Cryptocurrencies in a multi-exchange world**

Pools based DEXs General Functioning



The amount of tokens for each trade is decided by the **algorithm of the pool.** Rules according to a Constant Function Market Making

Automated Market Makers (AMM)

Definition: **Automated Market Makers** are protocols that permit the automated execution of buy and sell orders in a blockchain.

- We can exchange tokens X and Y (**swap traders**), up to paying fees
- **Liquidity providers** mint/burn liquidity and collect fees
- For automation, used a **Constant Function Market Makers** (CFMMs):

$$I(x \pm \Delta x\,,\, y \mp \Delta y) \geq I\,(x, y)$$

- **Constant Sum MM:** $I(x\,,\,y) = \omega_x\, x\, + \omega_y\, y$
  See mStable (https://mstable.org/)
- **Constant Product MM:** $I(x\,,\,y) = x\,.\,y$
  See Uniswap [Adams et al. 2021] or Sushiswap (https://www.sushi.com/)
- **Constant Mean MM:** $I(x\,,\,y) = \; x^{\omega_x}\,.\,y^{\omega_y}$

The first AMM: Uniswap v2 and its CFMM

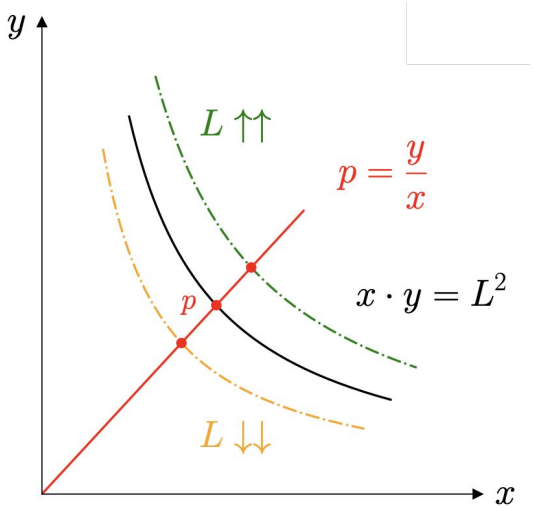
Based on the Constant Product Market Makers:

$$I(x, y) = x \cdot y \;, \quad p = y/x$$

Price/tokens/liquidity relations:

$$x = \frac{L}{\sqrt{p}} = \frac{L}{\pi} \quad \text{and} \quad y = L\sqrt{p} = L \cdot \pi.$$

where p and π are price and square root price.



What happens when a liquidity provider adds / removes liquidity from a liquidity pool ?

What happens when a trader swaps tokens?

Figure: How prices and quantities evolve in a Uniswap v2 protocol

The black hyperbola represents the possible quantities of tokens X and Y that can be in the liquidity pool. Traders who swap these tokens are constrained to make the quantities move along this hyperbola. The price for some given quantities (x, y) is the slope of the line connecting (0, 0) to (x, y).

Trader swap: details

Fee amounts: φ = 0.3%

- **The case d=+1**: when the trader **retrieves Δx tokens X by paying Δy tokens Y** (price increase), from which **φ · Δy are used to pay the fees**

$$(x - \Delta x)\,.\,(y + (1-\varphi)\Delta y) \;=\; x.y$$

- **The case d=-1**: when the operation is symmetric (price decrease) and fees are paid using tokens X

$$(x + (1-\varphi)\Delta x)\,.\,(y - \Delta y) \;=\; x.y$$

- **At the time of swap, the trader** can choose to Uniswap v2 to specify Δx or Δy, independently of the directions.
- The **current liquidity** L increases $(L+\Delta L)^2 = (x+\Delta x).(y+\Delta y)$
- The **supplied liquidity** $\mathcal{L}$ (net of fees) remains the same

Liquidity events (mint/burn)

Principle: The price before and after a liquidity event is the same.

Thus, **when adding**, $\frac{y+\Delta y}{x+\Delta x} = \frac{y}{x} = p$

We deduce $\Delta y = p\,\Delta x$ and thus the ***current liquidity*** is such

$$(L+\Delta L)^2 = (x+\Delta x)(y+\Delta y)$$

from which we get $\Delta L = \Delta x \,.\, \pi = \frac{\Delta y}{\pi}$

Supplied liquidity (net of fees): $\Delta \mathcal{L} = \mathcal{L}\,\frac{\Delta L}{L}$

When withdrawing, the LP owns a fraction $\frac{\Delta \mathcal{L}}{\mathcal{L}_{current}}$ of tokens X and Y.

Exemplification of transactions

$$p = \frac{y}{x}$$

1) Consider a liquidity pool containing 4118 tokens X and 1772610 tokens Y. The current price in the liquidity pool is thus $p_0 = 430.45\ldots$. Assume that no swaps have taken place in the pool, so that the total amount of supplied liquidity $\mathscr{L}$ coincides with L, the actual liquidity available in the pool. Then we have $\mathscr{L} = L = 85437.7\ldots$. Consider an LP wishing to deposit $\Delta x = 500$ tokens X into the pool.

The number of tokens Y to deposit at the same time is $\Delta y = p_0 \cdot \Delta x = 215227.0\ldots$. The price after both quantities of tokens have been deposited remains unchanged, and the resulting liquidity in the pool is $L_0 = L + \Delta L = \sqrt{(x + \Delta x) \cdot (y + \Delta y)} = L + \Delta x \cdot \pi_0 = 95811.4\ldots$. The additional liquidity $\Delta\mathscr{L} = 10373.69\ldots$ is marked to the LP, who owns around 10.8% of the supplied liquidity in the pool.

$$\Delta\mathcal{L} = \mathcal{L}\frac{\Delta L}{L}$$

$$x.y = L^2$$

Exemplification (Cont'd)

2) Consider a trader wishing to transfer tokens Y into the pool and receive $\Delta x = 660$ tokens X in exchange, after the LP added liquidity to the pool. This swap operation will cause the price to increase ($d = 1$ in our formalism). Assuming the price is still $p_0 = 430.45$, the amount Δy of tokens Y to transfer into the pool is $\Delta y = 332470.99\ldots$. After the swap operation, the price in the pool is $p_1 = 586.23\ldots$ and the liquidity is $L_1 = 95832.0\ldots$. Note that this amount differs from the supplied liquidity which is still $\mathscr{L} = 95811.4$.

$$p = \frac{y}{x}$$

(supplied liquidity is net of fees)

$$x.y = L^2$$

$$\Delta y = \frac{y}{(1-\varphi).(x-\Delta x)}.\Delta x$$

$$\Delta y = \frac{(1-\varphi).y}{(x+(1-\varphi).\Delta x)}.\Delta x$$

Now assume another trader wishes to transfer back $\Delta x = 660$ tokens X into the pool in exchange for tokens Y. The swap will cause the price to decrease ($d = -1$). The amount Δy of tokens Y transferred out of the pool is $\Delta y = 330763$. After the swap operation, the price in the pool is $p_2 = 430.82\ldots$ and the liquidity is $L_2 = 95852.5\ldots$.

Exemplification (Cont'd)

$$10.8\% \,.\, (4118 + 500 - 660 + 660)$$

3) Assume the initial LP, who owned around 10.8% of the supplied liquidity, wishes to withdraw all their liquidity. The amounts received by the LP are 215411.96… tokens Y and 500 tokens X. The additional 185 tokens Y they received come from the fees of the two previous swaps.

$$10.8\% \,.\, (1772610 + 215227 + 333470 - 330763) > 215227$$

The first AMM: Uniswap and its CPMM

If liquidity providers withdraw their tokens at t where pt≠ p0, it may result in a lower global value (net of fees)
⇒ **Impermanent Loss**, or Divergence Loss. See [Pintail, 2020].

Compare 2 strategies:

1. **HODL strategy:** VH = the value of a portfolio where tokens are held in a separate wallet
2. **Liquidity providing strategy:** VP = the value of a portfolio where tokens are invested in a liquidity Uniswap v2 pool.

As a convention we take Y as reference numéraire.

The Impermanent Loss is given by: $$\mathrm{IL} = \frac{V_P - V_H}{V_H}$$ or, Absolute IL $$V_P - V_H$$

More results on MS talks.

The first AMM: Uniswap and its CPMM

The case without fees.

From

$$V_H = \Delta x_0 \cdot p_1 + \Delta y_0 = \Delta x_0 \cdot p_1 + \Delta x_0 \cdot p_0,$$

$$V_P = x_1 \cdot p_1 + y_1$$

$$= \frac{(\Delta x_0 \cdot \pi_0)}{\pi_1} \cdot p_1 + (\Delta x_0 \cdot \pi_0) \cdot \pi_1$$

$$= 2 \cdot \Delta x_0 \cdot \pi_0 \cdot \pi_1,$$

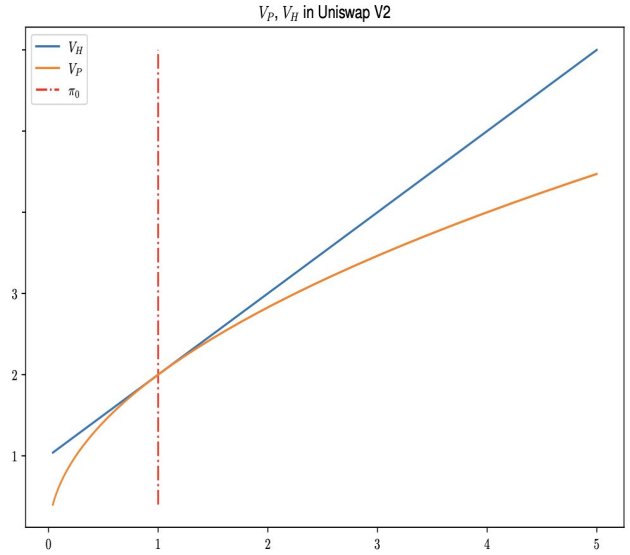
we deduce

$$V_P - V_H$$

$$= 2 \cdot \Delta x_0 \cdot \left(\sqrt{p_0 \cdot p_1} - \frac{1}{2}(p_0 + p_1) \right) \leq 0,$$

$$\mathrm{IL} = \frac{V_P - V_H}{V_H} = \frac{\sqrt{p_0 p_1}}{\frac{p_0 + p_1}{2}} - 1 \leq 0,$$

since the arithmetic mean is always greater than the geometric mean!



The position is Gamma negative (concavity):

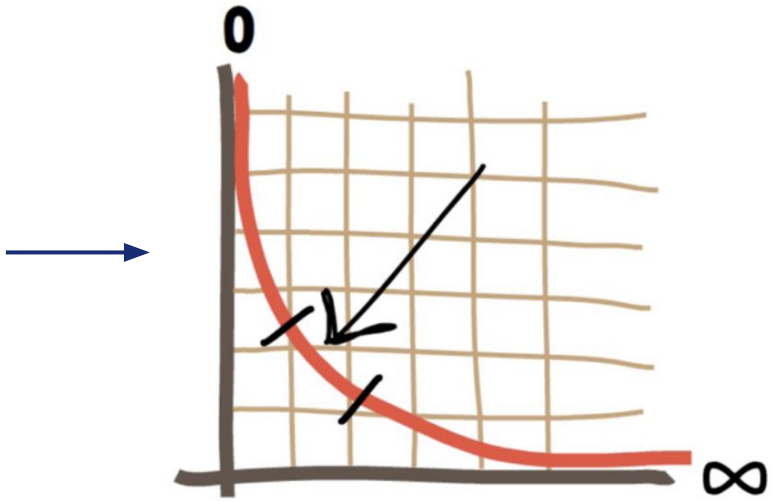
$$\partial^2_{p_1^2} V_P(p_1) = -\frac{\pi_0}{2p_1^{3/2}} < 0$$

- **Without swap fees, no P&L interest for the LP.**
- **The pool behaves as an option with negative gamma**
- **The fees correspond to the positive theta term of an option**

Concentrated Liquidity on DEXs

Uniswap V3,
A revolution for liquidity providers

Problem with simple CPMMs
Most assets usually trade within certain price ranges. Especially in pools with stable assets that trade within a very narrow range (example : DAI/USDC). Uniswap V2 DAI/USDC pool uses around 0.5% of capital for trading between 0.99 USD and 1.01 USD. Only used capital is subject to trading fees, i.e. LPs remuneration.



Solution, Concentrated Liquidity combined to CPMM
Liquidity providers can choose a custom price range when providing liquidity. This allows for concentrating capital within ranges where most of the trading activity occurs.

Concentrated Liquidity on DEXs

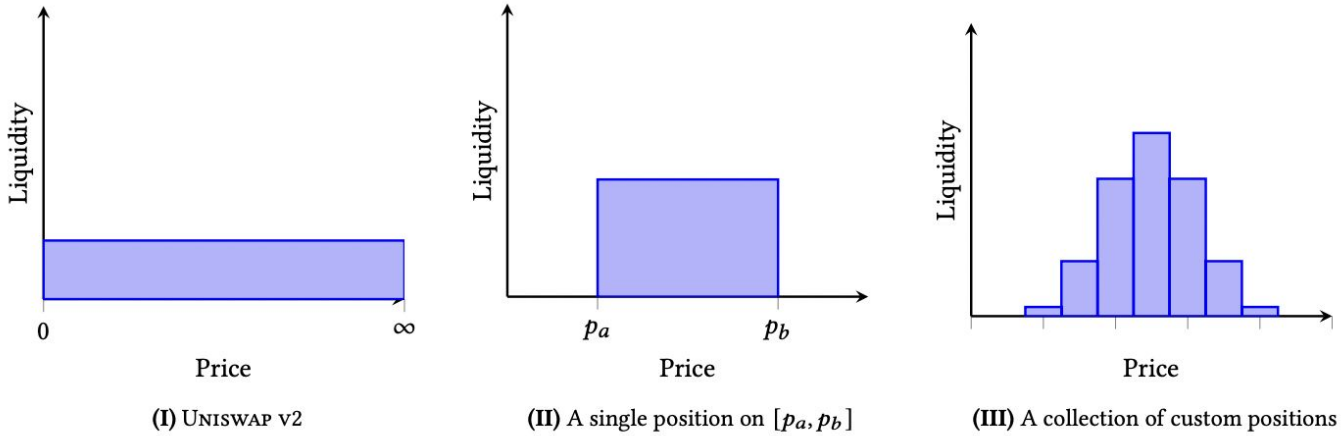
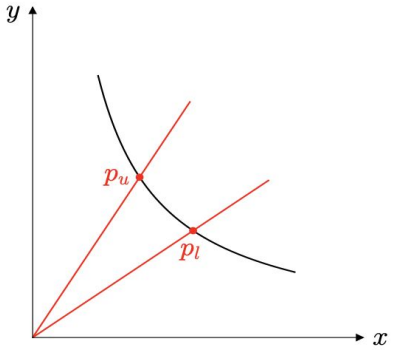


Figure 3: Example Liquidity Distributions. Source: Uniswap V3 white paper

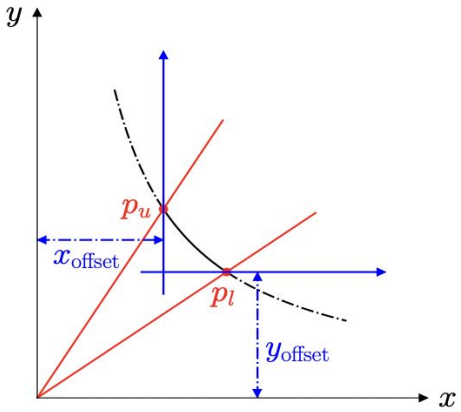
A Liquidity Provider of a Uniswap V3 pool can specify a **lower bound price pa** and an **upper bound price pb**, so that their liquidity can only be used on swaps within the price range [pa, pb].

Constant product formula



Virtual number of tokens:

$$\begin{cases} x = x_r + x_{\text{offset}}, \\ y = y_r + y_{\text{offset}}. \end{cases}$$



CPMM formula: $x.y = L^2$ with **specific offset values**

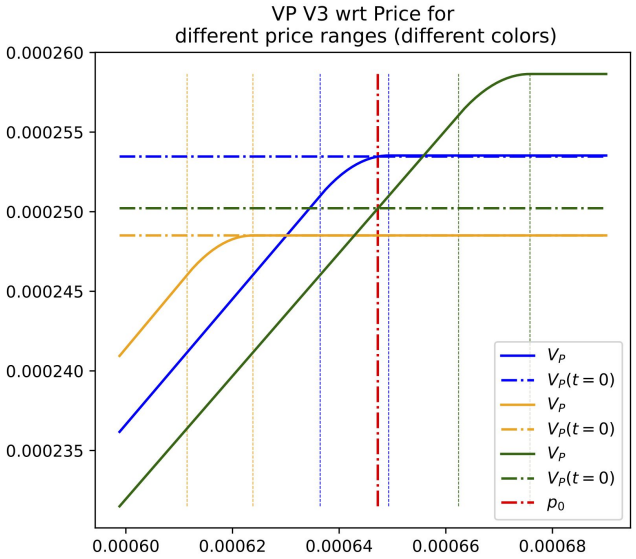
Boundary condition at p_u : $(0 + x_{offset}).\, y_u = L^2, \quad \dfrac{y_u}{x_{offset}} = p_u \implies x_{offset} = \dfrac{L}{\pi_u}$

Boundary condition at p_l : $x_l\,.\,(0 + y_{offset}) = L^2, \quad \dfrac{y_{offset}}{x_l} = p_l \implies y_{offset} = L.\,\pi_l$

Uniswap v3 CFMM formula: $\left(x_r + \dfrac{L}{\pi_u}\right) \cdot (y_r + L \cdot \pi_\ell) = L^2$, on the range

Uniswap v3:

- Amount of Fees depends on the size of the liquidity range
- Negative Impermanent loss.
- As for Uniswap v2, the pool behaves as non-linear product with concave payoff (covered call)
- Collected Fees can be well estimated
- See Anastasia's talk on Friday



Part 2

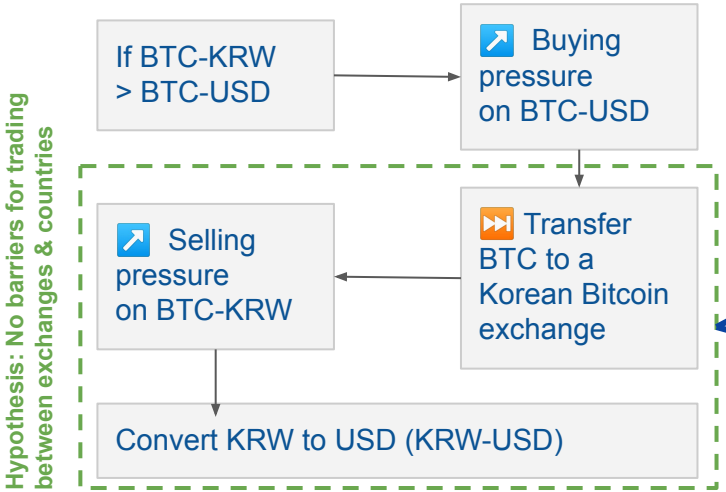
How Cryptocurrency Exchanges Shape the Value of Digital Assets

a. **Centralized and Decentralized Exchanges**
b. **Exploring Automated Market Makers as a Novel Method for Asset Price Discovery**
c. **Cryptocurrency Market Inefficiencies and Opportunities for Arbitrage Trading**
    i. CEXs create price discrepancies due to local capital controls
    ii. Arbitrage opportunities on DEXs
    iii. Arbitrage opportunities between CEXs and DEXs
d. **Valuing Cryptocurrencies in a multi-exchange world**

CEXs create price discrepancies due to local capital controls

In theory, markets are frictionless

Law of one price → Absence of Arbitrage opportunities.
Free Markets tend to the "fair" price (ex: Same price for BTC-USD and BTC-KRW when expressed in USD)



In reality, prices diverge across markets

Arbitrage opportunities, Bitcoin Premium
Makarov and Schoar (2019) and Choi et al. (2020) share those findings.

Costly due to :
- Cryptocurrency Markets Volatility
- Frictions emanating from Bitcoin's network mictrostructure

Cross-border Capital Controls

CEXs create price discrepancies due to local capital controls

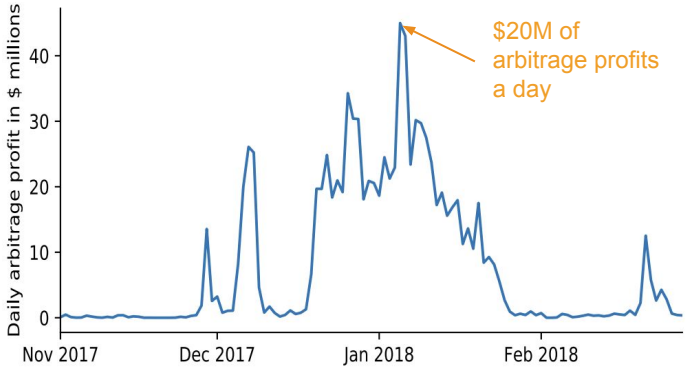
Bitcoin Premium/Discount on Korean Markets

Average price ratio of bitcoin to USD between the US and Korea, from January 2017 to February 28, 2018. Calculated using volume-weighted prices per minute from exchanges in each region, averaged daily.

Source: Kaiko data. Makarov, I., & Schoar, A. (2020).

Daily Arbitrage Profits between the US and Korean for Bitcoin

Daily arbitrage profits calculated from second-level price differences exceeding 2%.



Source: Kaiko data. Makarov, I., & Schoar, A. (2020).

Because of the capital controls arbitrageurs find it difficult to scale up their trading strategies with the intensity of noise-trader activity in a timely fashion. While regulations in some countries make **cross-border transfers** in fiat currencies difficult for retail investors, large institutions are typically able to avoid these constraints. However, the lack of of **regulatory oversight** may create impediments for large public institution to enter the cryptocurrency space and slow down the supply of arbitrage capital.

Arbitrage opportunities on DEXs

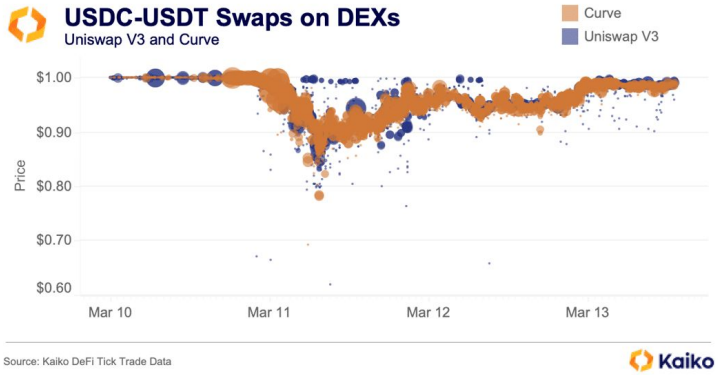
What about the presence of arbitrage opportunities on DEXs ? Lack of academic literature.

On DEXs, no fiat currencies can be used : *“For example, moving trading completely into crypto space by substituting fiat currencies with their digital counterparts, such as tether or Circle’s digital version of the US dollar, can diminish the role of capital controls.”*
- Makarov and Schoar, 2020

What can cause price discrepancies across DEXs ?

For example, between WETH-USDT market on Uniswap V3 on Ethereum and on Binance Smart Chain.

- ➔ Difference in **blockchain latency:** Ethereum (12 seconds/block) vs. Binance Smart Chain (3 seconds/block).
- ➔ Varied **gas fee** levels between blockchains.
- ➔ Liquidity disparities and resulting **slippage**.
- ➔ Vulnerability to **front-running** (dependent on the blockchain).
- ➔ **Microstructure difference** (Curve liquidity pools focus on slippage limitation while Uniswap focuses on capital efficiency)



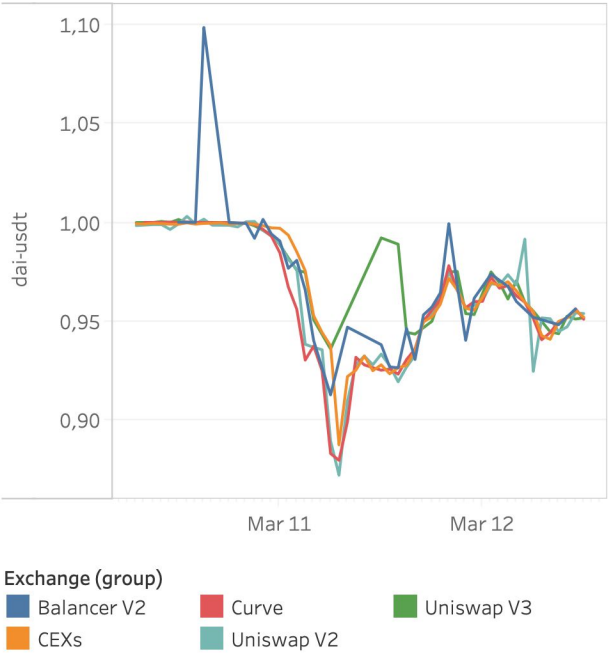
Arbitrage opportunities between CEXs and DEXs

What can cause price discrepancies across DEXs ?

For example, between WETH-USDT market on Uniswap V3 on Ethereum and on Binance Smart Chain.

- ➔ Difference in **blockchain latency** and **off-chain settlement latency :** Ethereum (12 seconds/block) vs. Coinbase (few milliseconds)
- ➔ Difference between **fee structure** (intermediation fees on CEXs vs gas fees on DEXs)
- ➔ **Microstructure difference** (Liquidity pool vs Order book)

Price Discrepencies Across CEXs and DEXs



Part 2

How Cryptocurrency Exchanges Shape the Value of Digital Assets

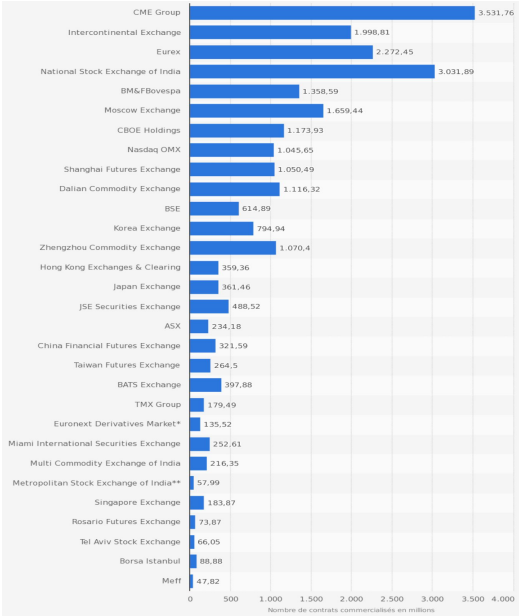
a. **Centralized and Decentralized Exchanges**
b. **Exploring Automated Market Makers as a Novel Method for Asset Price Discovery**
c. **Cryptocurrency Market Inefficiencies and Opportunities for Arbitrage Trading**
d. **Valuing Cryptocurrencies in a multi-exchange world**

Valuing Cryptocurrencies in a multi-exchange world

Context:

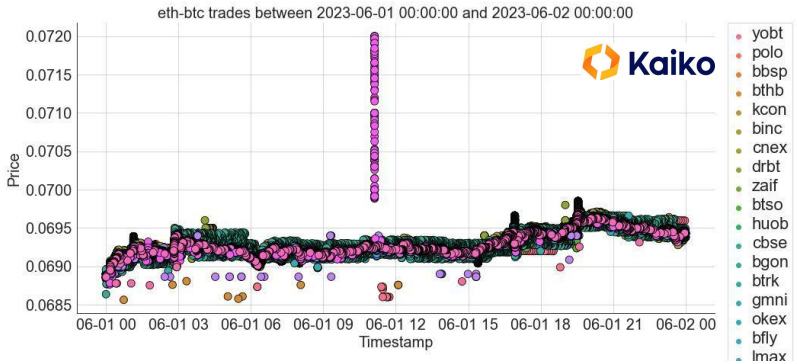
- **Highly fragmented market**: only few exchanges in Traditional Finance vs 200 in DEX, in 200 in CEX, >=170000 pools on Uniswap.
- Data quality: Access to exchanges are controlled in TradFi (rare outliers)
- Latency issues (high-frequency trading vs blockchain trading)

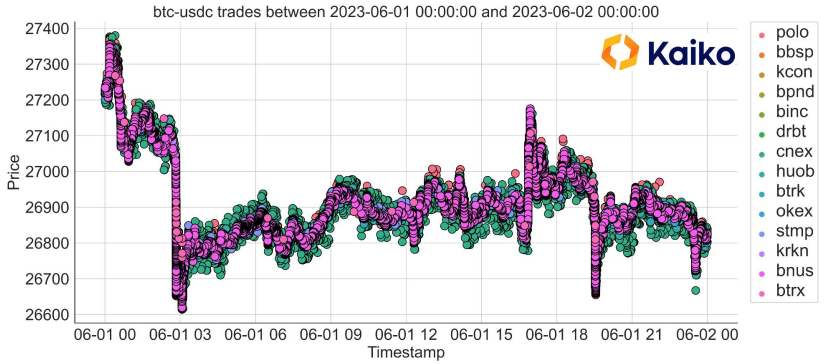
Aggregating (the right) information is really challenging. See examples to come.

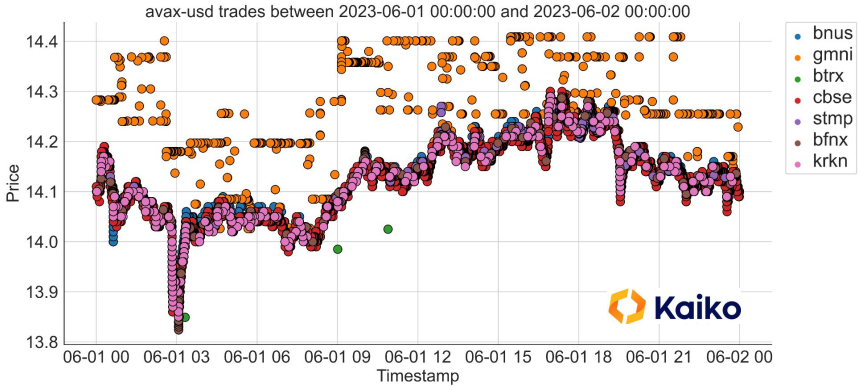


Traditional finance
World exchanges for traditional derivatives - Source: Futures Industry Association

Data samples on June 1st







- Much variability across platforms and exchanges
- Which trades to guess more?
- According to volumes? Or most reliable exchanges?

We need methodologies for having a robust and reliable aggregation rule.

What is the fair price given data points?

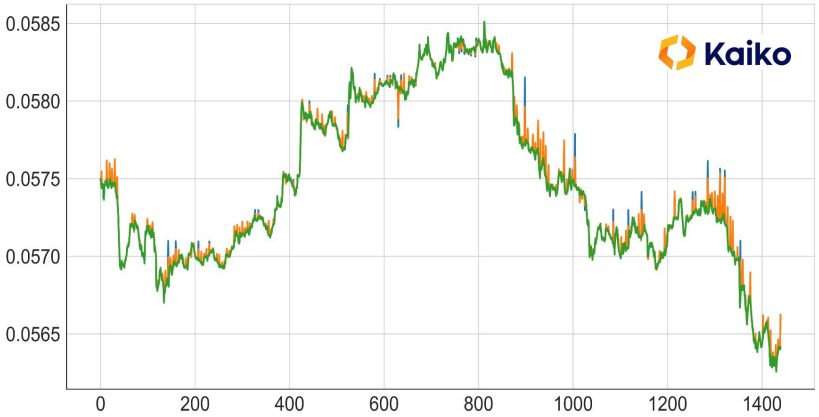
Definition [Paine and Knottenbelt, 2016]: A good price aggregator should fulfills:

- **Relevance** – should reflect the supply and demand, and the resulting true value of the asset
- **Timeliness** – value at a specific point in time or on a time interval as short as possible, quick to compute
- **Manipulation Resistance** – expensive to move the index away from the true value
- **Martingale Property** – not possible to predict patterns
- **Verifiability** – transparent methodology
- **Replicability** – possibility to reproduce the index with minimal tracking error by trading
- **Stability** – robust to outliers and data quality issues
- **Parsimony** – based on small number arbitrary parameters

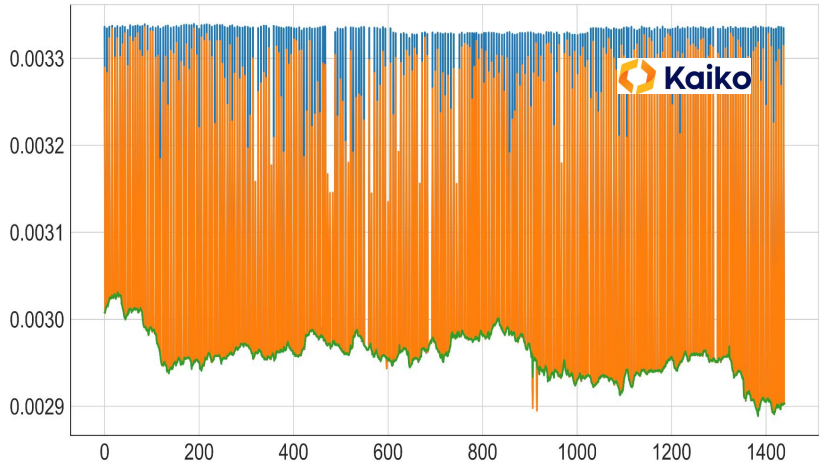
The standard methods: using n volume/price data points

Name	Formulas	Where	Characteristics
Empirical mean:	$\frac{1}{n}\sum_{i=1}^{n} P_i.$	Vinter, 2021	Does not account for volumes (thus can be manipulated)
Volume-Weighted Average Price (VWAP)	$\widehat{\mathrm{VWAP}}_n := \frac{\sum_{i=1}^{n} V_i P_i}{\sum_{i=1}^{n} V_i}.$	Nasdaq, 2022 (Nasdaq Crypto Index - NCI) FTSE Russell, 2022	Many hyperparameters to handle outliers Respect the FX rule "Price of X-Y = 1/ Price Y-X" Replicable
Volume-Weighted Median (VWM)	$\widehat{\mathrm{VWM}}_n := \inf\left\{p : \frac{\sum_{i=1}^{n} V_i \mathbb{1}_{\{P_i \le p\}}}{\sum_{i=1}^{n} V_i} \ge \frac{1}{2}\right\}.$	Fed Reserve Bank of NY, 2015 Chicago Mercantile Exchange 2016 (Bitcoin Reference Rate (BRR)) Bloomberg 2018 Benchmarks 2022	Robust to prices Not robust to volume outliers Several hyperparameters Hardly replicable
Robust Weighted Median (RWM)	See Michael Allouche's talk on Tuesday	Kaiko, 2023	Robust, parsimonious, accurate, reactive, suitable for high-frequency update Hardly replicable

Illustrations on real data: VWAP (orange) / VWM (blue) / RWM (green)



ETH-BTC on June 28, 2022
Frequency: minute

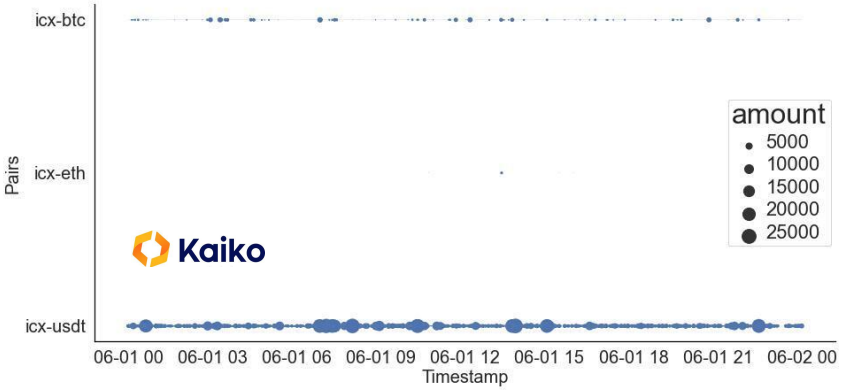


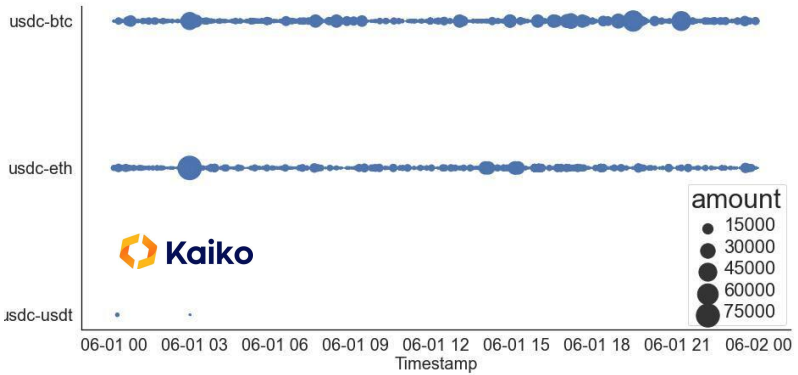
ZEC-BTC on June 28, 2022
Frequency: minute

Perspectives/Open questions

- **Still looking for the ideal aggregator**
  - Respecting the FX rule
  - Replicable
  - Robust to outliers and data quality issues
  - Fast and accurate
  - Works with few data (n=50-100)
- **It can‘t come from usual methods of TradFi**
- **Robust statistics:** Median of Means, Trimmed Mean, Lee-Valiant estimator, Minsker-Ndaoud estimator etc…
- More philosophically, what is a **financial price consensus**?
  - What is a distribution centrality? Median or Average or Mode?
  - Old debate between mathematicians (Galton, Gauss, Fisher…)

What is the rate of a non-traded pair???

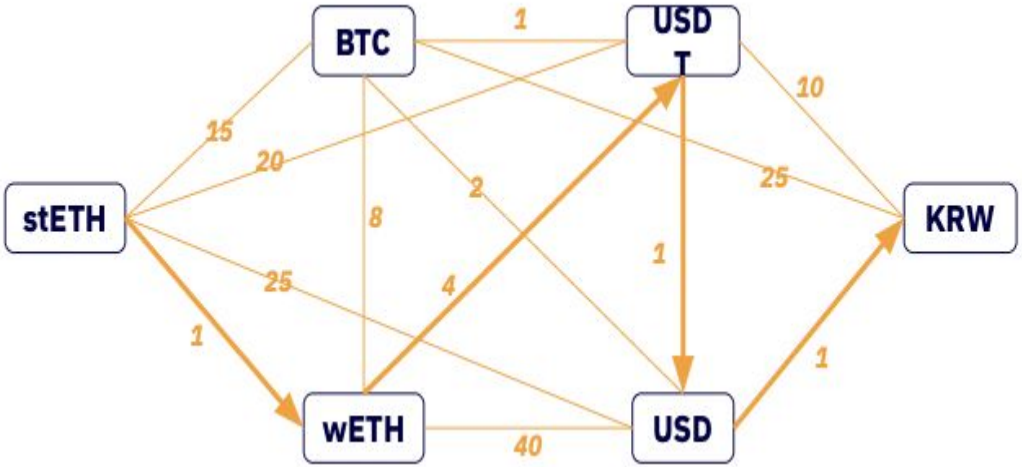




An example with icx-usdc on June 1st

Issues when a pair A-B is not directly traded

- Pair A-B is not traded (stETH->KRW)
- But A-X and X-B is for different X
- What is the fair price of A-B?
- Which X to select now?
- What if X* is changing?
- Notion of shortest path:
  - Volumes
  - Liquidities
  - …
- Shortest path algorithm:
  - Dijkstra's Algorithm
  - A* search algorithm
- Liquidity, market depth



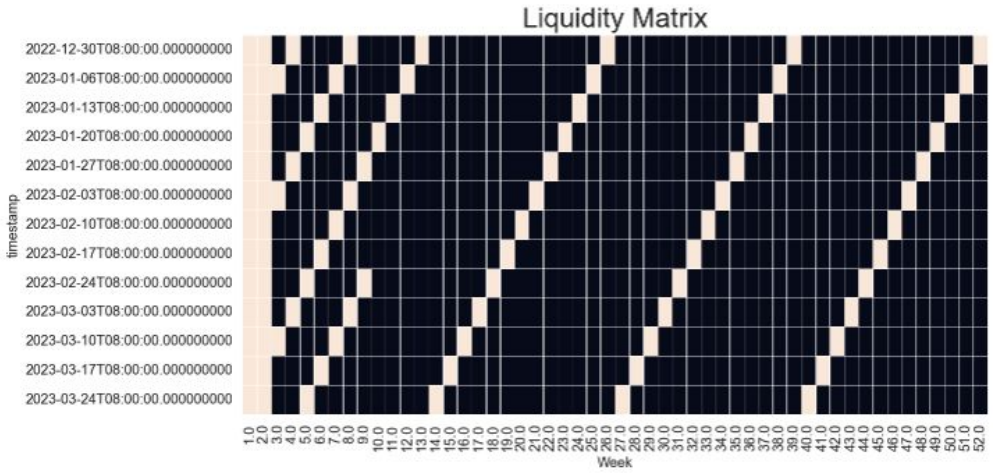
Part 3

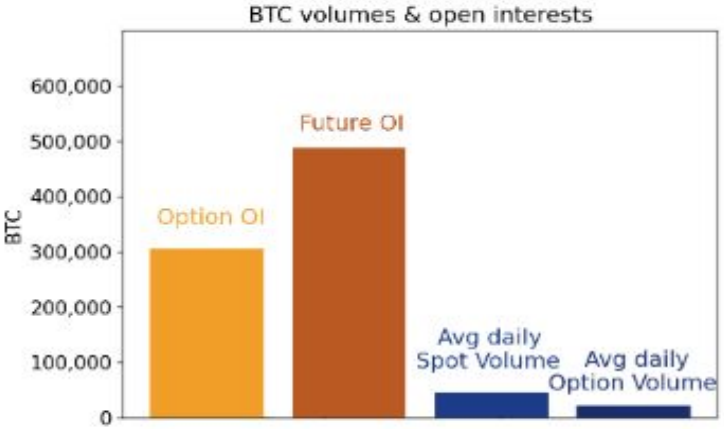
Cryptocurrency Derivatives Markets

a. **Futures**
b. **Perpetual Futures**
c. **Options**

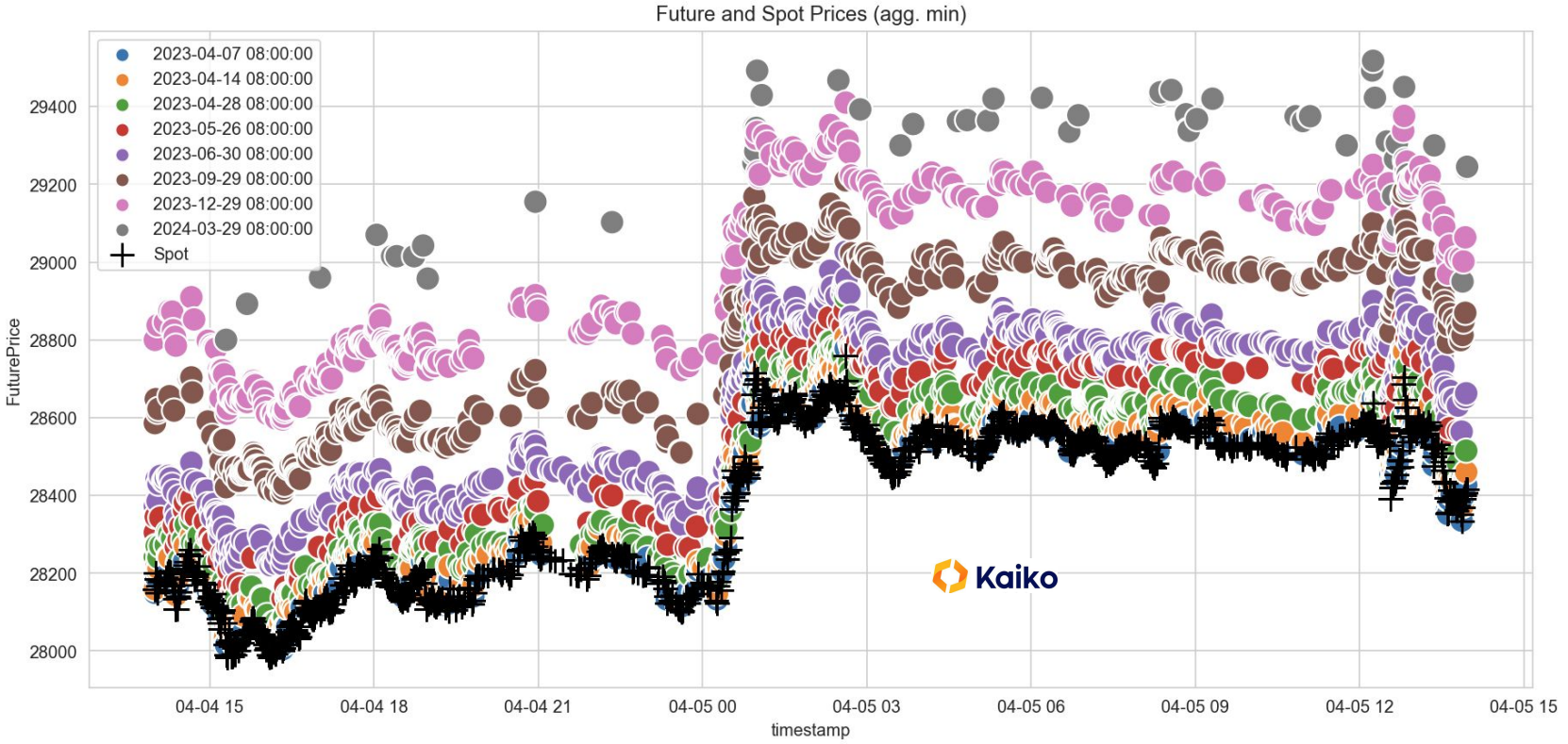
Future contracts

- **Where:** Binance, Bybit, CME, Delta Exchange, Deribit, ErisX, ICE, Gate.io, Huobi, KuCoin, LedgerX, OKX, StormGain…
- **Underlyings:** BTC, ETH, BNB, XRP, LINK, AVAX or MATIC…
- **Lack of standardization (underlying, expiry,...)**
- Still in its infancy





An example of data set (from Deribit on April 4th, BTC-USD)



Statistical model: Principal Component Analysis is possible, but not effective for short tenors.

Perpetual futures:

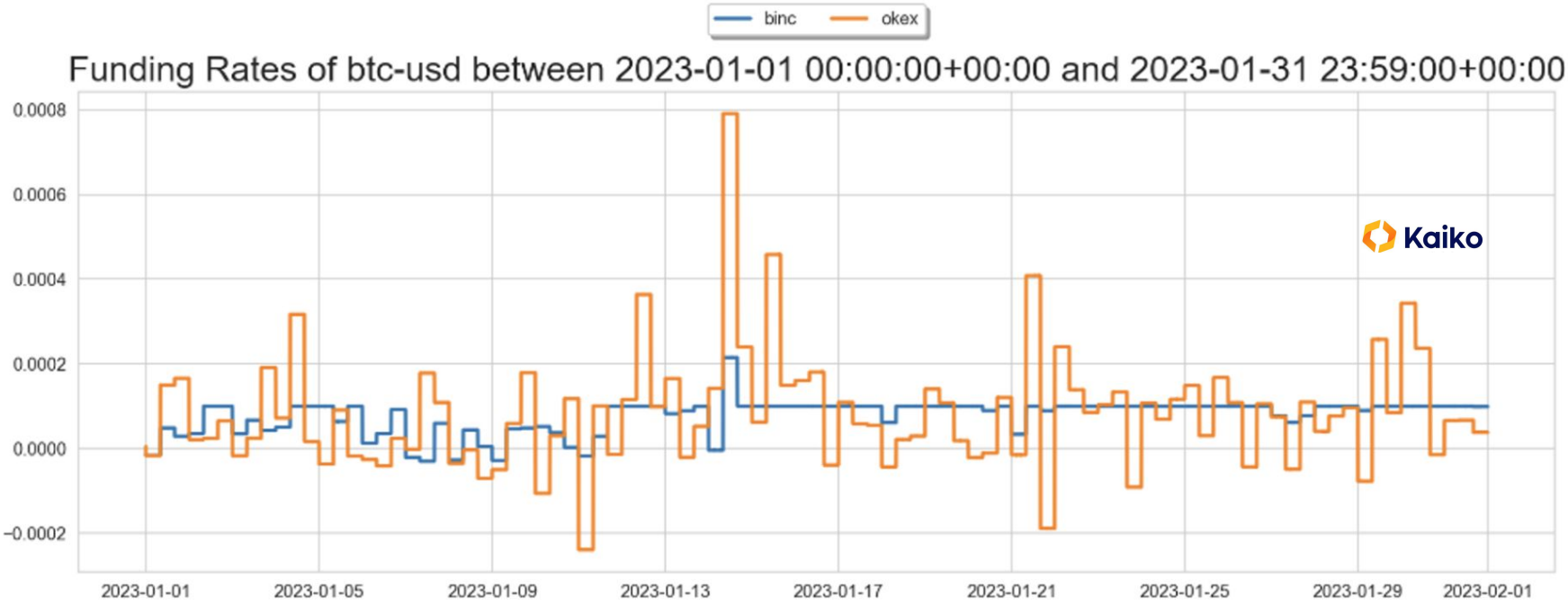
- Concept introduced in **R.J. Shiller**: "Measuring Asset Values for Cash Settlement in Derivative Markets: Hedonic Repeated Measures Indices and Perpetual Futures," Journal of Finance, 1993. Solution for crypto: A. Bragin, 2011.
- Innovative financial product, so far unique to the cryptocurrency markets.
- Funding mechanism to maintain the contract's price in line with the underlying asset: adjusting the contract price through regular payments made between long and short positions based on the difference between the contract price and the underlying asset price.

Example: OKX funding rate

Funding Rate = Clamp(MA(((Best Bid + Best Offer)/2 - Spot Index Price)/Spot Index Price-Interest),a,b)

Currency	a	b
BTC	-0.375%	0.375%
ADA, AVAX, BCH, DOT, EOS, ETC, ETH, FIL, LINK, LTC, SOL, TRX, XRP	-0.75%	0.75%

Data sample:


binc
okex
Funding Rates of btc-usd between 2023-01-01 00:00:00+00:00 and 2023-01-31 23:59:00+00:00
0.0008
0.0006
0.0004
0.0002
0.0000
−0.0002
2023-01-01
2023-01-05
2023-01-09
2023-01-13
2023-01-17
2023-01-21
2023-01-25
2023-01-29
2023-02-01
Kaiko

Future contracts: pricing rule?

- **In TradFi,**
  - Future contracts: “legal agreement to buy/sell a particular asset at a predetermined price at a specified time in the future.”
  - Standardized contracts, daily margins call (we pay the DtD difference everyday).

- **In DigitalFinance,** no such daily margin calls.

EXAMPLE 2.2 (adapted from Deribit version on July 8th 2022) *A trader buys 100 futures contracts on the* BTC *index, at* $\mathrm{Fut}_t^{\mathrm{Der.},T} = 10,000$ USD *per* BTC. *The trader is now long 1,000* USD *worth of* BTC *with a price of 10,000* USD *(100 contracts* $\times$ *10* USD $=$ *1,000* USD*).*

- *At inception, the trader does not pay anything, but is committed to paying 1,000* USD *at expiry; this amount is worth* $1,000\ B_{t,T}^{\mathrm{F}}$ USD *at inception.*
- *At expiry, the trader receives* $1,000/10,000$ BTC, *because of the futures contract.*
- *They can sell this amount in* BTC *at the expiry rate* X_T*; for instance if* $X_T = 12,000$ USD, *then this amount is worth* $\frac{1,000}{10,000} \times 12000 = 1200$ USD.

Writing a *Reverse Cash-and-Carry Arbitrage* in Fiat, we get $\mathrm{Fut}_t^{\mathrm{Der.},T} = \dfrac{C_t^{\mathrm{F}}(X_T, T)}{B_{t,T}^{\mathrm{F}}}.$

The price obeys to a forward pricing rule (not to the “TradFi” future pricing rule).

Other pricing rules

If X the Crypto-Fiat rate (1 unit of C worths X units of F), the **no-arbitrage condition between currencies C and F** yields

$$\frac{1}{X_t} C_t^{\mathrm{F}}(\Phi_T^{\mathrm{F}}, T) = C_t^{\mathrm{C}}\left(\frac{\Phi_T^{\mathrm{F}}}{X_T}, T\right)$$

In particular: $$\mathrm{Fut}_t^{\mathrm{Der.},T} = \frac{X_t C_t^{\mathrm{C}}(1,T)}{B_{t,T}^{\mathrm{F}}} = X_t \frac{B_{t,T}^{\mathrm{C}}}{B_{t,T}^{\mathrm{F}}}.$$

This is the well-know **Interest Rate Parity (IRP)** relationship (Musiela and Rutkowski 2005).

- In theory, gives access to the implied rate use by Future traders on exchanges
- Conceptually interesting since no interest rate available on the exchanges
- However, not much useful because
  - lack of liquidity of futures
  - The underlying to the BTC-future (on Deribit) is not exactly the BTC

Interest rate curve modelling: which data to start with ?

In TradFi:

- The **short-term interest rate** is known (like Euro Short-Term Rate (ESTR), which reflects the overnight borrowing costs of banks within the eurozone).
  Driven by the monetary policy of the central bank attached to a currency.
- **Interest rate derivatives**: Bonds, Swaps, Swaptions, CMS…
- **Forward Rate Agreement** (FRA)

In **DigitalFinance**:

- No central banks
- No Interest rate derivatives
- Mostly, Futures/Forwards

It’s quite challenging to build a complete Interest Rate Curve

Option markets

Where and underlyings: similar to futures

Exercice type: European and American (Huobi)

Payoff:

- vanilla (call/put)
- exotic (Touch Options Double One-Touch and Touch Options Double No-Touch, by Huobi)

80-90% of the activities on **Deribit**

Lack of standardization between exchanges

See Anne-Claire Maurice’s talk on Tuesday.

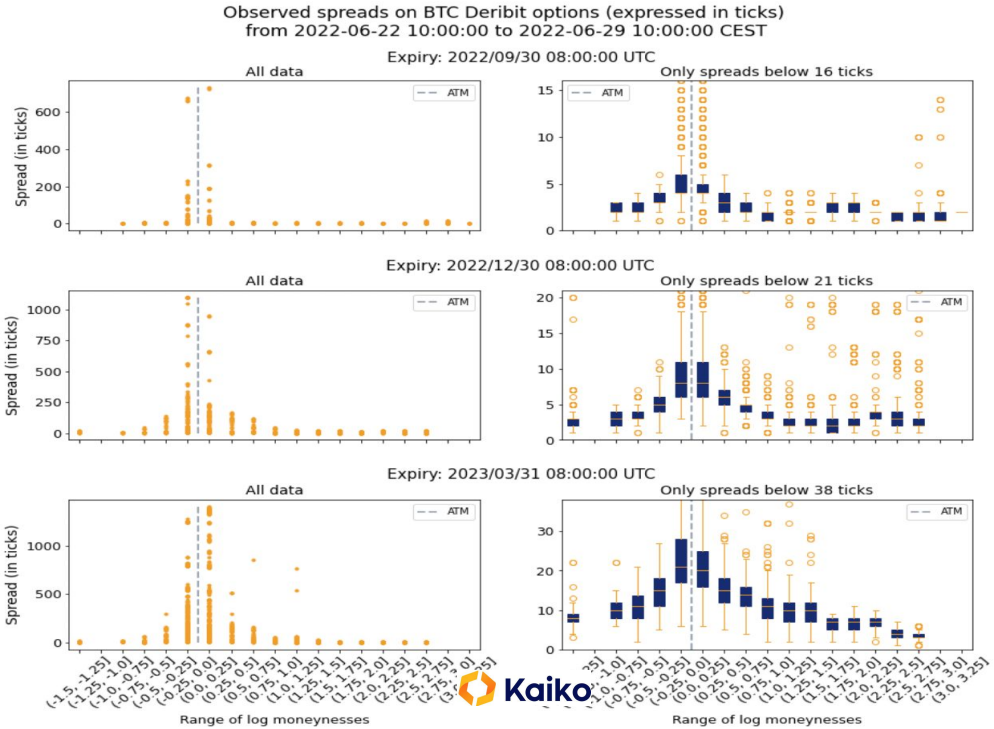
Issues for calibrating the IV

- **Relative tick size for options is 50 larger** than for usual TradFi derivatives market

Option \ Exchange	CBOE	EUREX	EURONEXT	CME	Deribit
Underlying Name	SP500	Eurostoxx	AEX	EUR-USD	BTC-USD
Option tick size	0.05	0.10	0.01	0.00005	0.0005
Underlying Value (close) on 2022, May 24th	3 941.48	3 647.56	679.88	1.0737	1
Ratio in basis points (bps, i.e. 1E-4)	0.127	0.274	0.147	0.466	5

It implies a more important discrepancy between the bid/ask/mid.

Boxplot of spreads (expressed in ticks) BTC-USD options collected over a period of a week (2022-06-22 10:00 to 2022-06-28, 10:00 CEST). Option expiries are: 2022 Sept 30th (top), 2022 Dec 30th (middle), 2023 March 31th (bottom).



- Large spreads
- Many missing bids
- Links between different IVs across platforms (Deribit, Okex,..) and different implied models?

Part 4

Lending & Borrowing Cryptocurrencies

a. Lending & Borrowing in DeFi: How it works?
b. **Collateralized Debt Positions (CDPs)**
c. **Pooled Collateralized Debt Markets (PCDMs)**
d. **Liquidations**

Lending & Borrowing in DeFi: How it works ?

I have an excess of liquidity

I need extra liquidity

1. **Collateral**: Loan secured with specific assets **(DeFi Mostly)**
2. **Verifiable Identities**: Option to take legal action / Credit score **(TradFi)**
3. **Flash loans** (none of the above), leverage blockchain technology

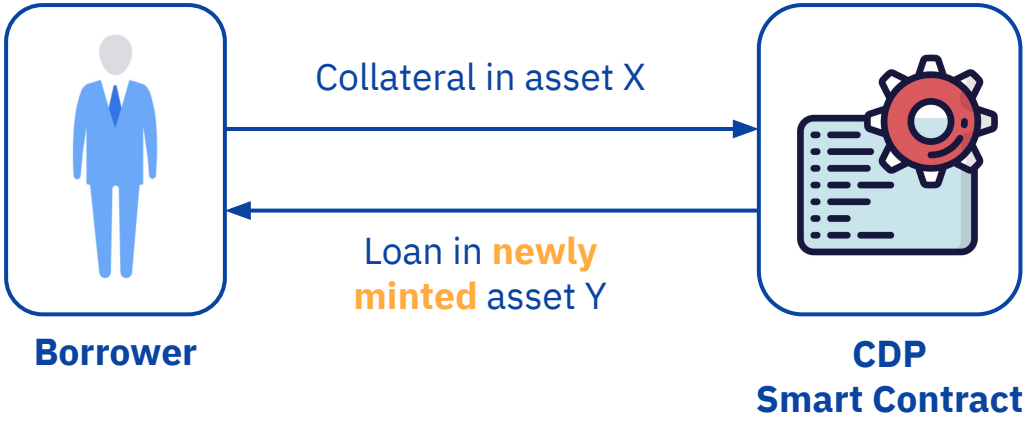
Part 4

Lending & Borrowing Cryptocurrencies

a. **Lending & Borrowing in Crypto: How it works?**
b. **Collateralized Debt Positions (CDPs)**
c. **Pooled Collateralized Debt Markets (PCDMs)**
d. **Liquidations**

Collateralized Debt Positions (CDPs)

Example:
MAKER



Use Cases

1. **Consume** something without selling your assets X
2. **Leverage** : lock up X assets, borrow Y assets, then exchange Y assets for X assets, then lock up those new X assets etc.

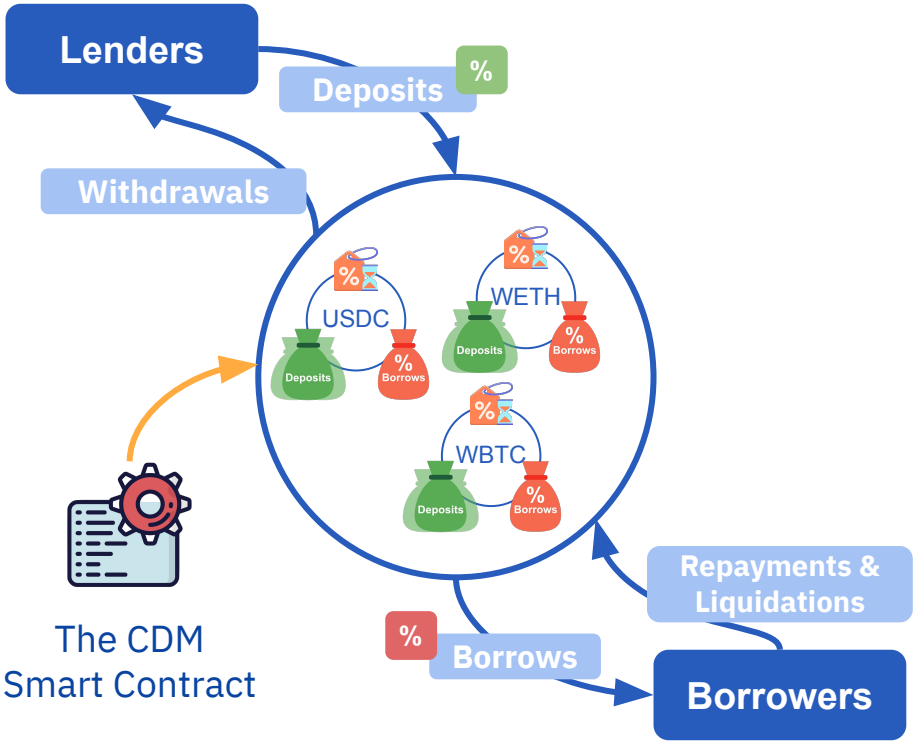
Part 4

Lending & Borrowing Cryptocurrencies

a. **Lending & Borrowing in Crypto: How it works?**
b. **Collateralized Debt Positions (CDPs)**
c. **Pooled Collateralized Debt Markets (CDMs)**
    i. CDMs: Functioning & Interest Bearing Tokens
    ii. Risks of borrowing
d. **Liquidations**

CDMs: Functioning & Interest Bearing Tokens

Example:
AAVE



When one deposits assets in lending pools, he receives **interest bearing tokens** (IBTs).

- *For example, if one provides USDC on AAVE, he gets aUSDC.*
- *IBTs account for interest earned*
- *IBTs represent transferable claims to the collateral*
- *IBTs are burnt to redeem and withdraw the asset including the accrued interest*

Risks of Borrowing

The main risk for taking an over collateralized loan for a borrower, is to get his collateral **liquidated**. The collateral can be liquidated by anyone (generally a liquidation bot) against repayment of the position's debt.

To prevent risk, one has to monitor the borrowed/lent tokens prices to make sure his position stays healthy.

A healthy position is when the sum of the debt of an borrower (Σdi) , is ≤ to the absolute liquidation threshold (aLT). This is often referred to as the **health factor**. This is the ratio between a position's liquidation threshold and the sum of any outstanding debt. We directly see based on the ratio below, that:

- ☹️ when HF ≥ 1
- 🙂 when HF < 1

$$HF = \frac{aLT}{\Sigma d_i}$$

The **Liquidation threshold** refers to the point at which a borrower's collateral value falls below a specified level, leading to the initiation of the liquidation process.

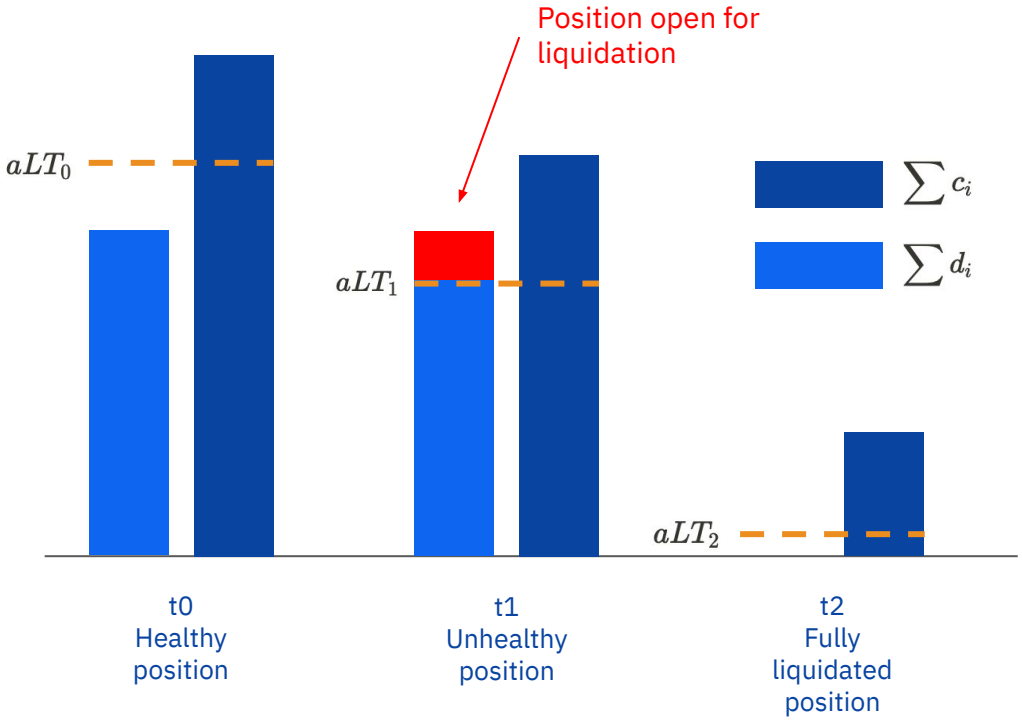
Part 4

Lending & Borrowing Cryptocurrencies

a. **Collateralized Debt Positions (CDPs)**
b. **Pooled Collateralized Debt Markets (PCDMs)**
c. **Liquidations**
    i. Liquidations: How it works ?
    ii. How to incentivize liquidators ?
    iii. What happens when a liquidation fails?

Liquidations: How it works ?

$$rLT_i \in [0,1]$$
$$aLT = \Sigma c_i rLT_i$$



Both **CDMs and CDPs** require a minimum collateralisation for each loan, Σdi≤aLT.

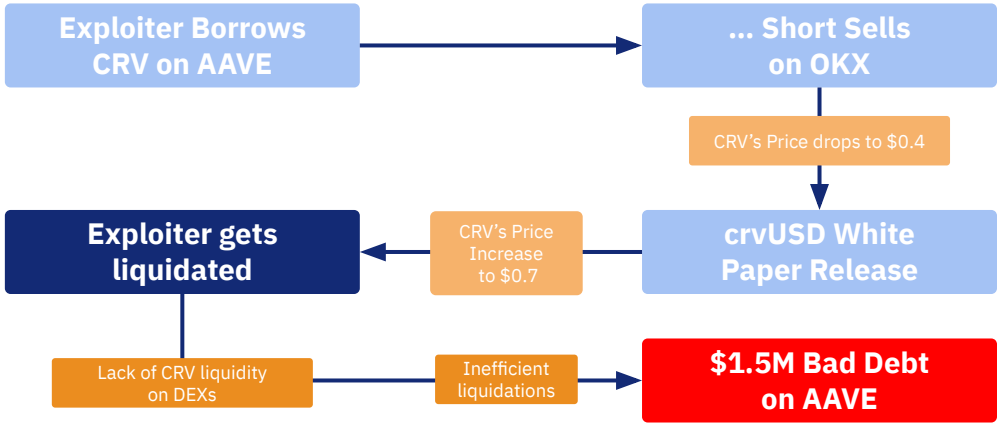
The collateral of a position can be liquidated by anyone, **against repayment of the position's debt.**

However, one can liquidate **part of or all** the position's collateral.

Hypothesis here: All the position in liquidated.

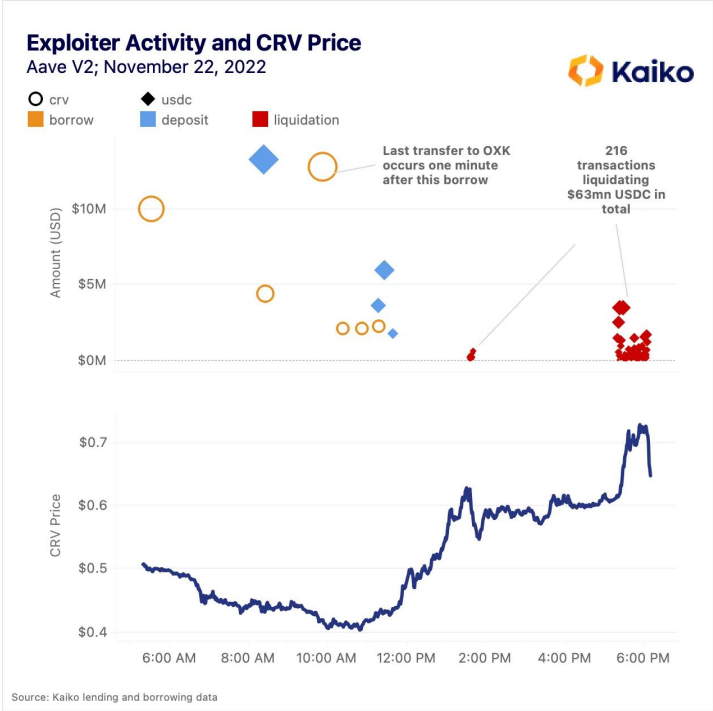
Emmanuel Gobet, Anastasia Melachrinos

What happens when a liquidation fails ? Bad Debt



Conclusion : Reducing Risk with Token Liquidity Data

Liquidity information of tokens from both centralized and decentralized finance markets can be used in lending protocols to **reduce the risk of default and insolvency** by limiting the amount of less liquid tokens that can be borrowed or deposited.



Source: Riyad Carey. (2023). The long and short of AAVE. URL: https://blog.kaiko.com/the-long-and-short-of-aave-d61d5c14ad43

Still many quantitative issues, such as

- Modelling the energy consumption of block-chains
- Arbitrages between DEX and CEX
- More generally, crypto derivatives modelling
- Modelling interest rate curve modelling
- Liquidation and Systemic risk
- Prices aggregation in fragmented market

Need more quantitative research!

References

Decentralized & Centralized Exchanges

Pintail. "Uniswap: A good deal for liquidity providers?" (2020). Available at: https://pintail.medium.com/uniswap-a-good-deal-for-liquidity-providers-104c0b6816.

Makarov, I., & Schoar, A. "Trading and arbitrage in cryptocurrency markets." Journal of Financial Economics, 135(2), 293-319 (2020).

Angeris, G., Kao, H. T., Chiang, R., Noyes, C., & Chitra, T. "An analysis of Uniswap markets" (2019). Available at: https://arxiv.org/pdf/1911.03380.pdf.

Evans, A. "Liquidity provider returns in geometric mean markets" (2020). Available at: https://arxiv.org/pdf/2006.08806.pdf.

Angeris, G., & Chitra, T. "Improved price oracles: Constant function market makers." Proceedings of the 2nd ACM Conference on Advances in Financial Technologies, 80-91 (2020). Available at: https://arxiv.org/pdf/2003.10001.pdf.

Harvey, C. R., Ramachandran, A., & Santoro, J. "DeFi and the Future of Finance." SSRN 3711777 (2020).

Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., ... & Juels, A. "Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges." arXiv preprint arXiv:1904.05234 (2019).

Lin, L. X., Budish, E., Cong, L. W., He, Z., Bergquist, J. H., Panesir, M. S., ... & Zhang, S. "Deconstructing decentralized exchanges." Stanford Journal of Blockchain Law & Policy, 2 (2019).

Hautsch, N., Scheuch, C., & Voigt, S. "Building Trust Takes Time: Limits to Arbitrage in Blockchain-Based Markets" (2018).

Walch, Angela. "Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems." In Crypto Assets: Legal and Monetary Perspectives (Chris Brummer, ed), Oxford University Press, 2019.

Walch, Angela. "In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains." In Regulating Blockchain. Techno-Social and Legal Challenges, edited by Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos & Stefan Eich, Oxford University Press, 2019.

Dodd, N. "The social life of Bitcoin." Theory, culture & society (2017).

Vigna, P. "Regulating cryptocurrencies: Assessing market reactions." VoxEU.org, 2018. Available at: https://voxeu.org/article/regulating-cryptocurrencies-assessing-market-reactions

References

Bitcoin mining and environment

Auer, R. 2019. Beyond the doomsday economics of “proof-of work” in cryptocurrencies, BIS Working Papers No 765

Brunnermeier, M. K. and J. Abadi, 2018. The economics of blockchains, VoxEU

Explore the total electricity use by bitcoin miners: https://ccaf.io/cbeci/index/comparisons

Explore bitcoin mining map: https://ccaf.io/cbeci/mining_map

Explore blockchain charts: https://www.blockchain.com/charts

Makarov, Igor and Schoar, Antoinette, 2021. Blockchain Analysis of the Bitcoin Market, NBER Working Paper

Easley, D. and O'Hara, M. and Basu, S., 2019. From Mining to Markets: The Evolution of Bitcoin Transaction Fees, Journal of Financial Economics

Lehar, A. and C. A. Parlour, 2021. Miner Collusion and the Bitcoin Protocol

First chapter of the The Blocksize War: https://blog.bitmex.com/the-blocksize-war-chapter-1-first-strike/

Benetton, Matteo and Benetton, Matteo and Compiani, Giovanni and Morse, Adair, 2021. When Cryptomining Comes to Town: High Electricity-Use Spillovers to the Local Economy

Paul Roberts, 2018. This Is What Happens When Bitcoin Miners Take Over Your Town. POLITICO Magazine

References

Bitcoin as a payments system

Foley, S., Karlsen, J. R., and Putnins, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? The Review of Financial Studies, 32(5):1798{1853.

Farrel, H. 2015. Dark Leviathan: The Silk Road might have started as a libertarian experiment, but it was doomed to end as a fiefdom run by pirate kings

Graf von Luckner, C., Reinhart, C. M and Rogoff, K. S, 2021. Decrypting New Age International Capital Flows", NBER Working Paper 29337.

Hanna Halaburda, Guillaume Haeringer, Joshua S. Gans, Neil Gandal, THE MICROECONOMICS OF CRYPTOCURRENCIES, NBER Working Paper 27477

Chainanalysis, 2021. The 2021 Crypto Crime Report (first 7 pages)

Max, D.T. 2021. Half a Billion in Bitcoin, Lost in the Dump, the New Yorker