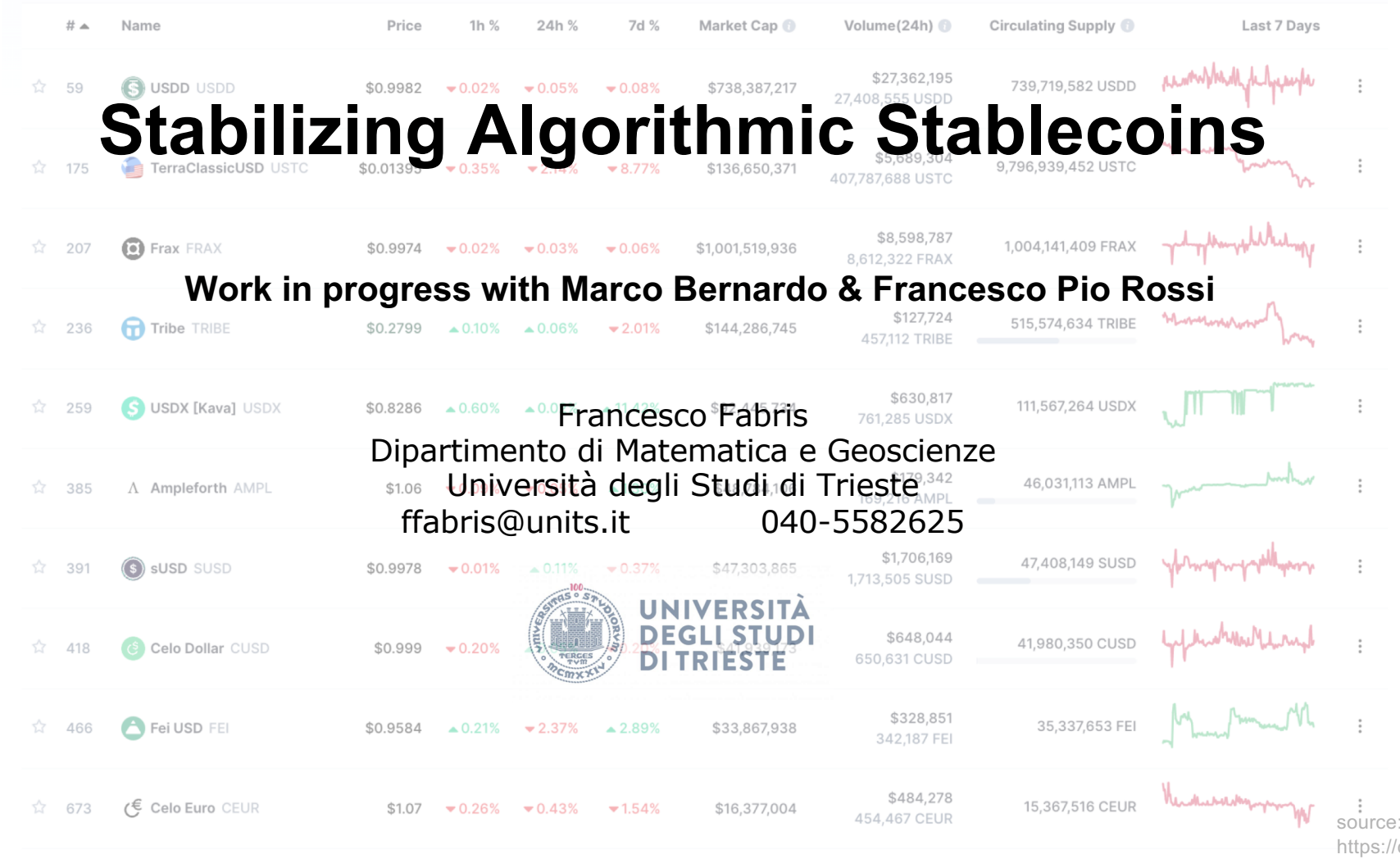


Stabilizing Algorithmic Stablecoins

Work in progress with Marco Bernardo & Francesco Pio Rossi

Francesco Fabris
Dipartimento di Matematica e Geoscienze
Università degli Studi di Trieste
ffabris@units.it 040-5582625

source:
https://coinmarketcap.com/

Outline of the talk:

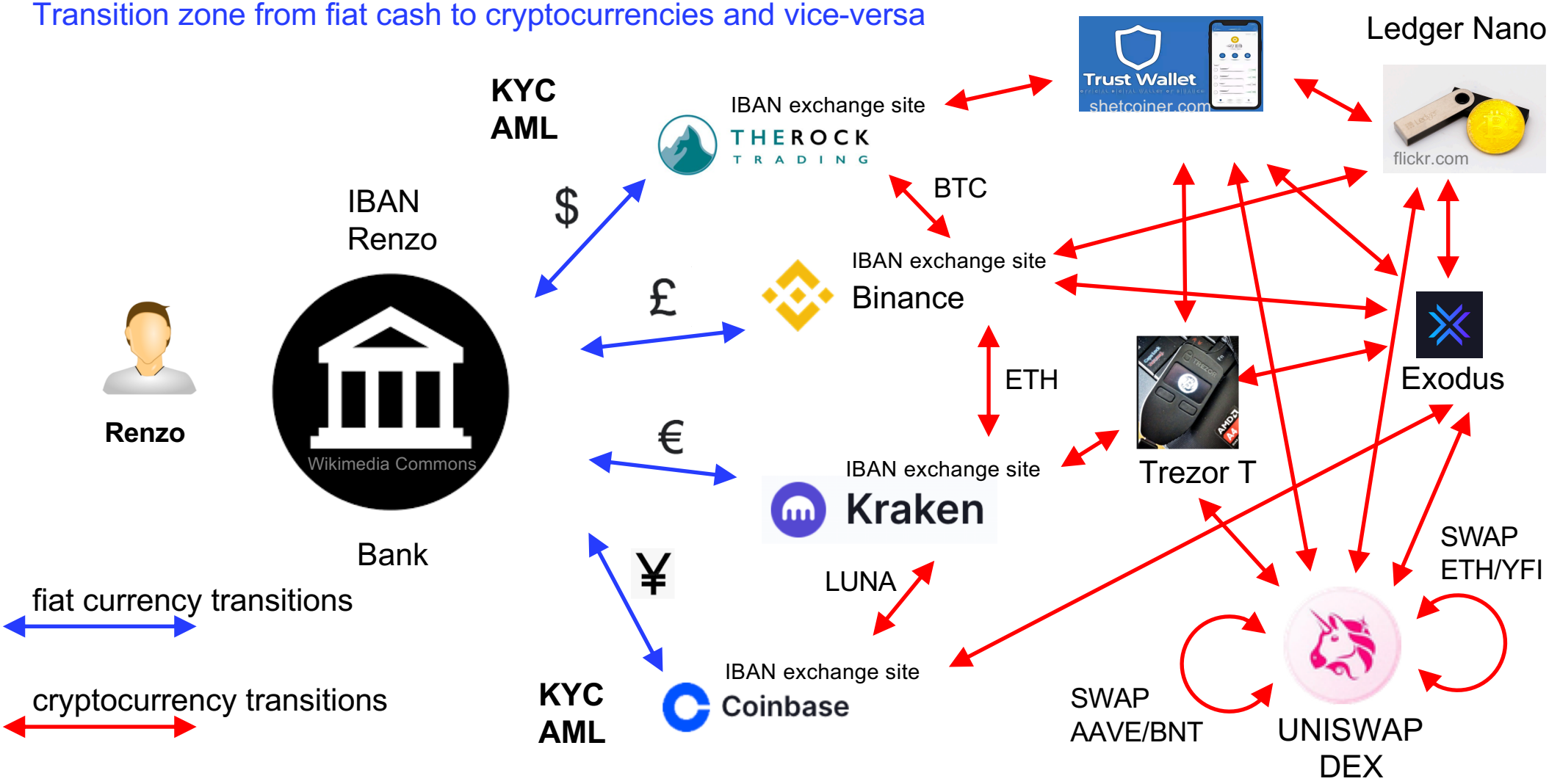
1. Why stablecoins
2. Why *algorithmic* stablecoins
3. The Terra-Luna collapse
4. Proposals for improving the stability of algorithmic stablecoins

Why stablecoins?

It is all in relation with the high volatility of crypto-market

source:
https://www.tradingview.com

Transition zone from fiat cash to cryptocurrencies and vice-versa



Why introducing stablecoins?

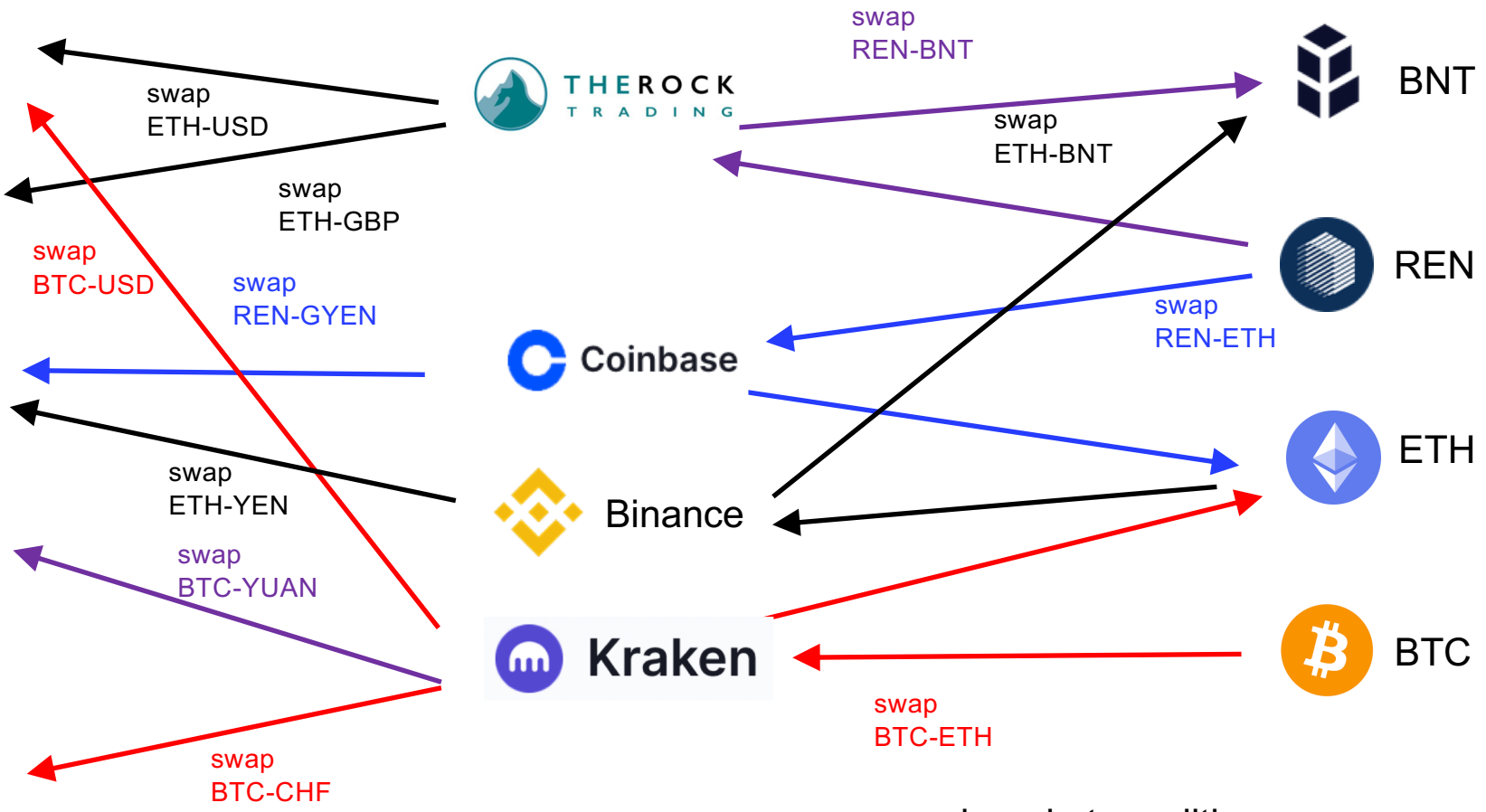
During time of high or extreme volatility in cryptocurrencies, people prefer to come back to fiat money, to preserve the value of their assets

ETH

BTC

Stablecoins trading on CEX exchanges

Fiat money



high volatility market conditions!

normal market conditions

Looming problem:

Who trust CEX, i.e. centralized exchanges?
(almost) nobody!

Main losses on CEX

FTX:	$ 7.4 Billion	Nov. 2022 (bankruptcy)
FTX:	$600 Million	Nov. 2022 (hacked)
Coincheck:	$534 Million	Jan. 2018
Mt. Gox:	$473 Million	2011 e 2014
Ku Coin:	$285 Million	Sept. 2020
BitMart:	$196 Million	Dec. 2021
BitGrail:	$170 Million	Feb. 2018
:	:	:

Consequence

Holding assets (fiat money and cryptocurrencies) in centralized exchanges (CEX) is ***highly dangerous***

Idea:

develop a ***stable*** cryptocurrency, i.e. a ***stablecoin***, backed by fiat money (USD, GBP, YEN,...)


USD Coin - USDC


Tether USD - USDT


Tether EUR - EURT


CryptoYen - GYEN


DAI


CryptoFranc - XCHF

Cryptocurrencies with a (hopefully) stable value

Introduced to have protection towards the strong price volatility of cryptocurrencies.

Stable value maintained through a seigniorage mechanism.

Pegged to the value of a real asset, typically a fiat currency (usd, euro, chf, yuan, ...)

Based on an equivalent value to the capitalization, deposited in a bank and (hopefully) certified.

An equivalent amount of real USD $ are deposited in a bank

USD Coin - USDC

Capitalization
$ 29 Billion

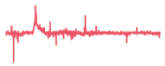
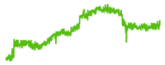
Bank

Cerificate of deposit

$29 Billion

source:
https://www.tradingview.com

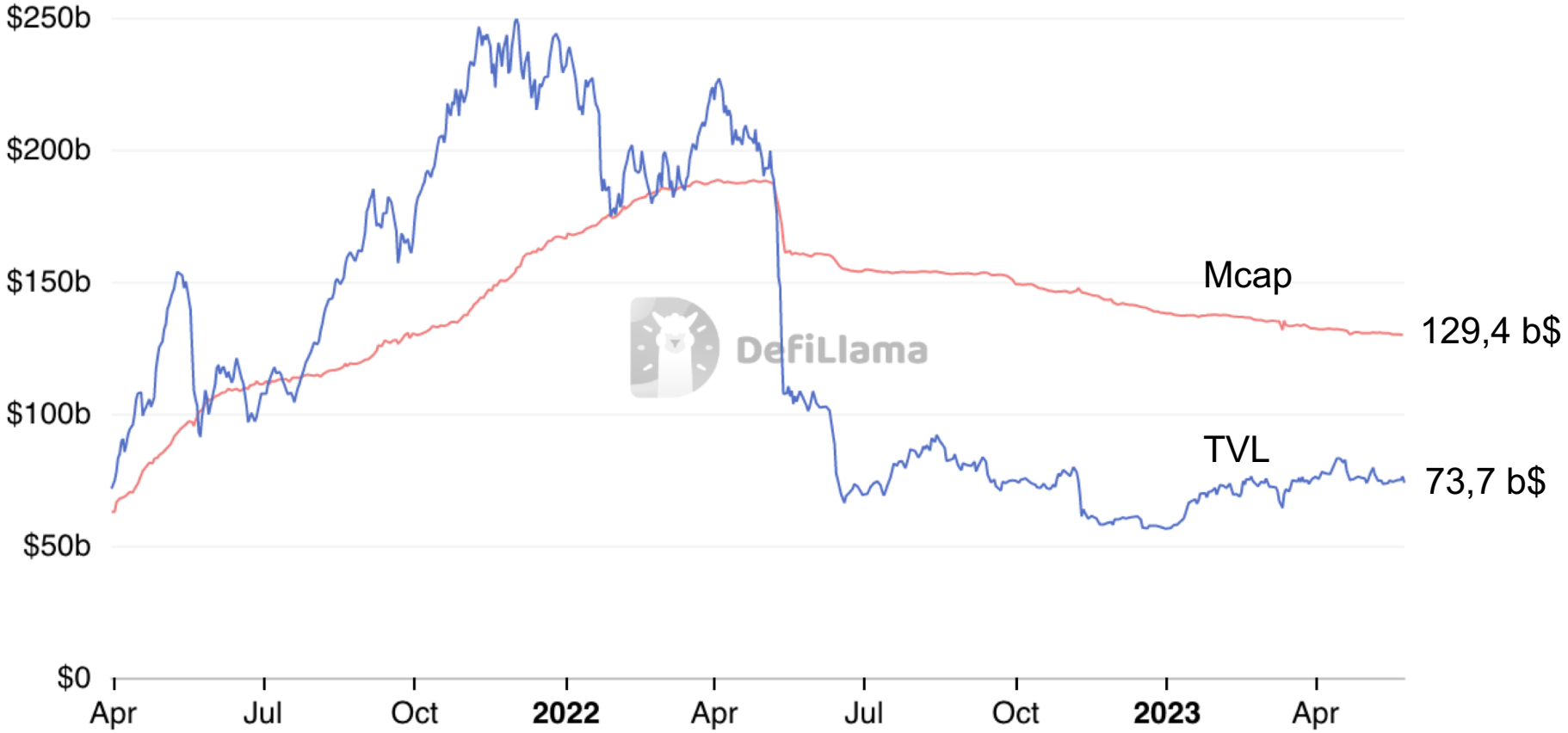
Top Stablecoin Tokens by Market Capitalization

#	Coin	Price	24h Volume	Exchanges	Market Capitalization	30d	Last 30 Days Circulation
1	Tether USDT	$1.00	$23,439,293,724	409	$83,008,861,043	1.8%	
2	USD Coin USDC	$1.00	$4,213,950,681	393	$29,114,653,439	-5.2%	
3	Binance USD BUSD	$1.00	$1,612,962,204	134	$5,323,284,353	-16.9%	
4	Dai DAI	$0.998893	$126,636,285	202	$4,617,083,117	-3.5%	
5	TrueUSD TUSD	$1.00	$226,747,926	53	$2,039,066,165	0.0%	
6	Pax Dollar USDP	$1.00	$30,715,549	20	$1,017,790,744	-2.7%	
7	Frax FRAX	$0.999478	$7,958,172	35	$1,001,726,741	-3.7%	
8	USDD USDD	$1.00	$28,480,915	21	$738,914,540	3.2%	
9	Gemini Dollar GUSD	$1.00	$707,696	9	$574,832,199	26.0%	
10	PAX Gold PAXG	$1,973.01	$9,393,499	34	$518,421,197	-0.1%	
11	Tether Gold XAUT	$1,963.55	$6,421,481	14	$482,982,495	-1.8%	
12	Liquity USD LUSD	$1.01	$6,742,224	12	$282,133,321	3.3%	
13	Euro Tether EURT	$1.07	$2,457,355	17	$220,767,735	-2.8%	

142 of them in all

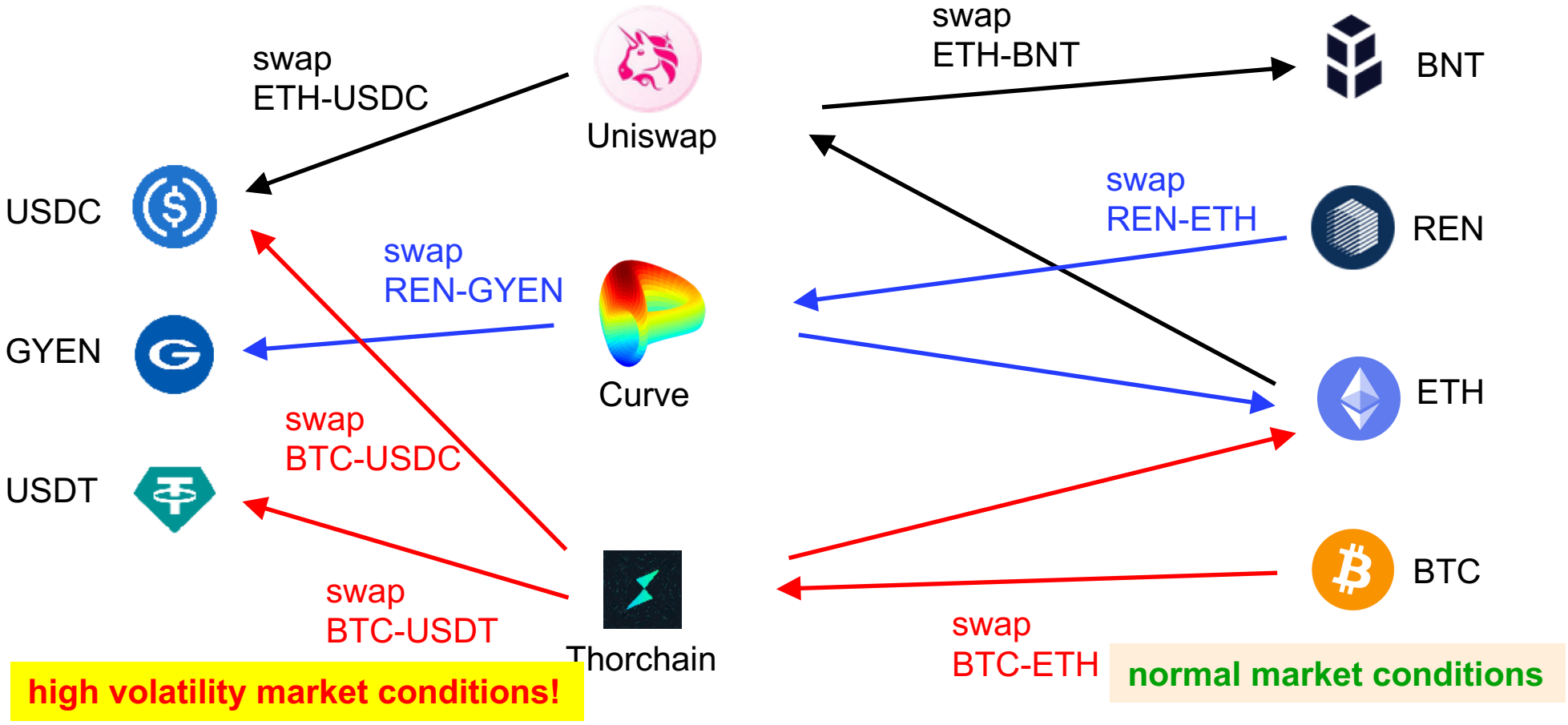
source:
https://coinmarketcap.com/

Total market cap: **129,4 b$** (25 May 2023)

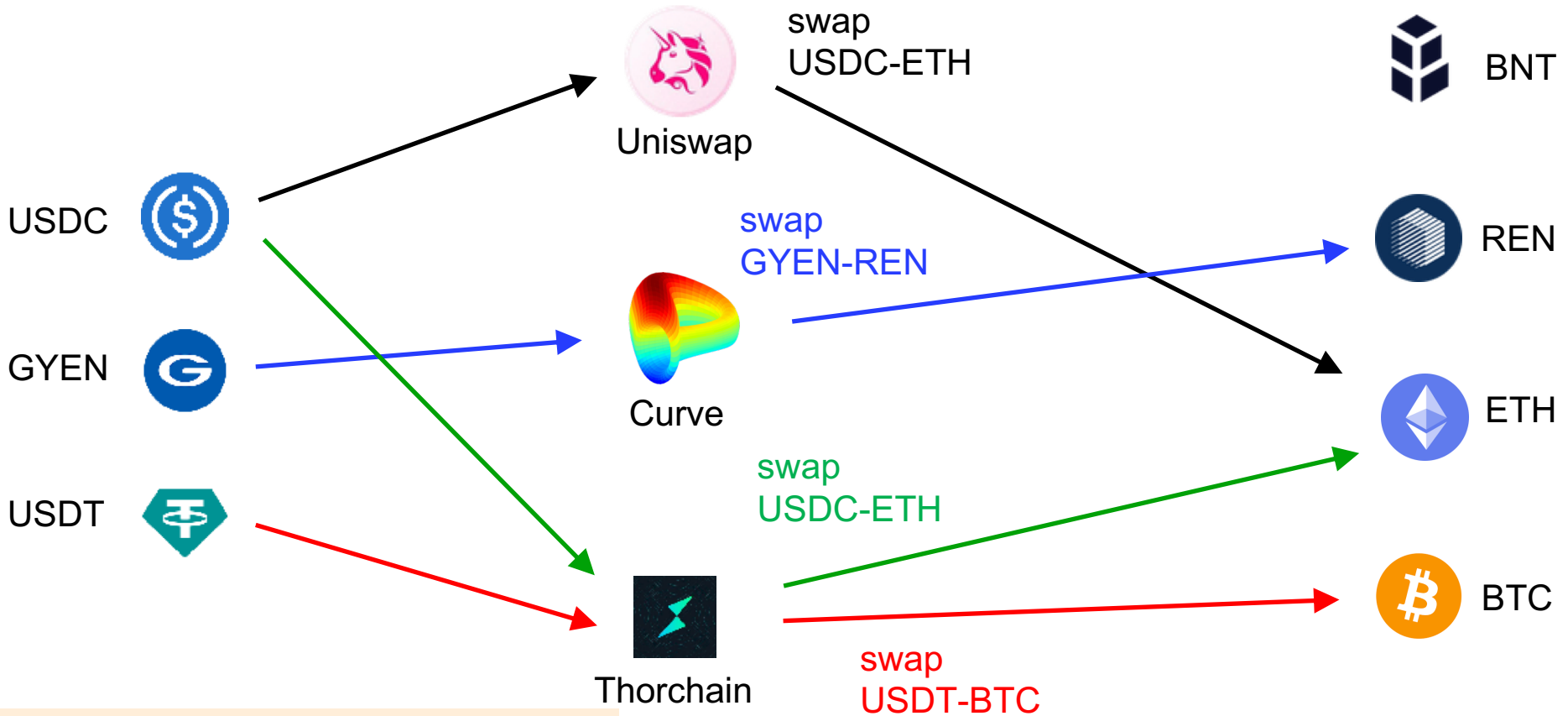


source:
https://defillama.com

Stablecoins trading on DEX exchanges



Stablecoins trading on DEX exchanges



the market comes back to normality

Why algorithmic stablecoins?

Decentralized finance (De-Fi) aims at:

1. building an entire banking, stock and financial system, 24/7/365, decentralized, anonymous and uncensorable independent from institutional finance;

2. making this system available to people who for various reasons are excluded from banking/financial services (financial inclusion)

3. reducing bank/financial intermediation costs

Consequence:

If one wants De-Fi to be independent from istitutional finance

one cannot use fiat money to build the De-Fi ecosystem !

Idea:

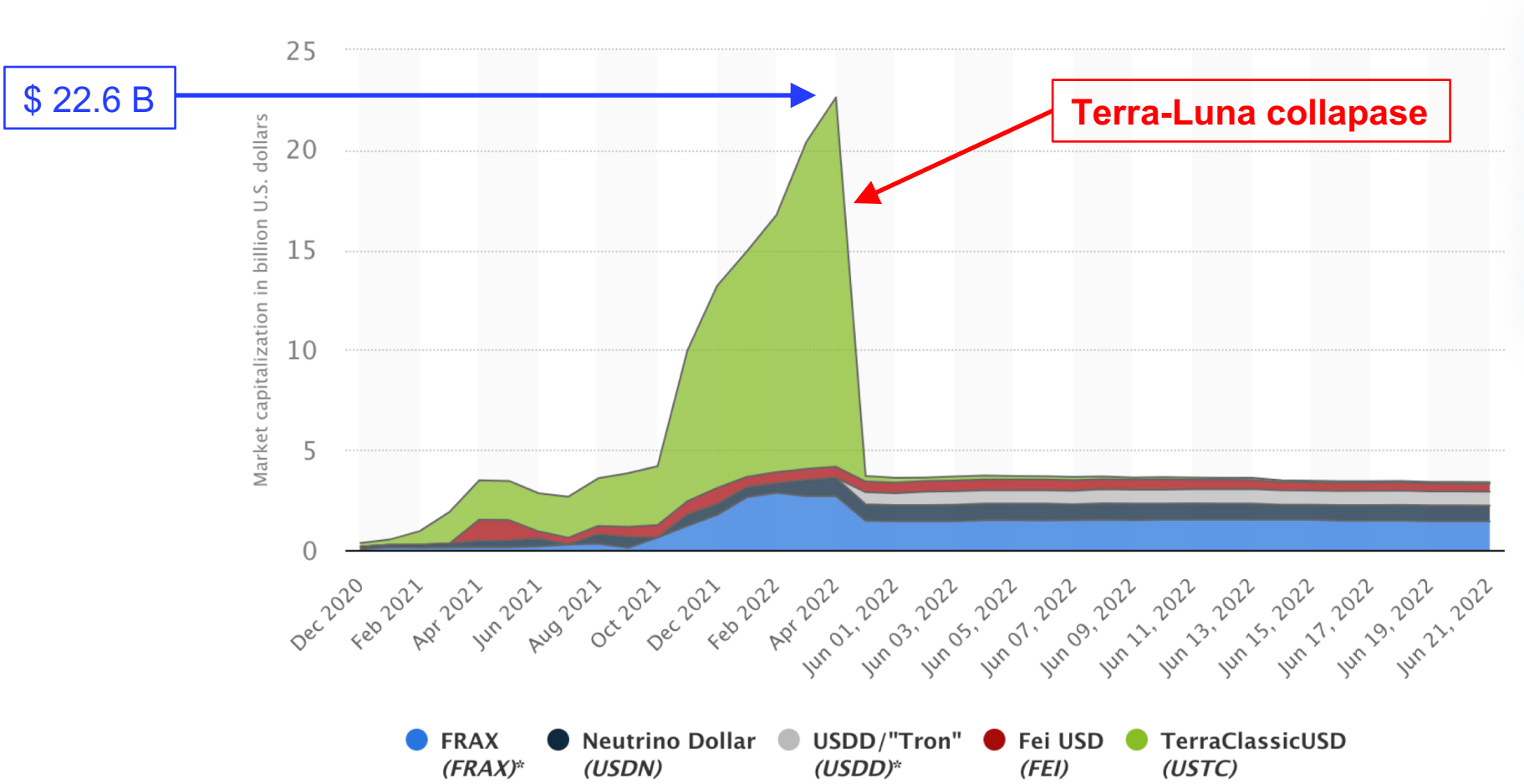
develop a stablecoin **NOT** backed by fiat money,
that is build an ***algorithmic stablecoin***

Top algorithmic stablecoins by market cap

Name	Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
Frax FRAX	$0.9978	0.04%	0.05%	0.04%	$1,001,939,989	$17,748,305 17,784,141 FRAX	1,004,141,409 FRAX	
USDD USDD	$0.9988	0.01%	0.01%	0.03%	$738,797,757	$30,244,272 30,276,780 USDD	739,717,928 USDD	
Tribe TRIBE	$0.2786	0.23%	0.11%	2.44%	$143,618,398	$118,834 426,063 TRIBE	515,574,634 TRIBE	
TerraClassicUSD USTC	$0.01395	0.39%	0.45%	8.05%	$136,624,809	$5,099,841 365,586,707 USTC	9,796,919,879 USTC	
USDX [Kava] USDX	$0.8236	0.02%	0.85%	15.71%	$91,885,639	$619,972 752,884 USDX	111,567,264 USDX	
Ampleforth AMPL	$1.07	0.12%	1.09%	2.35%	$49,124,496	$167,423 156,942 AMPL	46,031,113 AMPL	
sUSD SUSD	$0.9982	0.10%	0.03%	0.49%	$47,267,498	$1,426,718 1,429,489 SUSD	47,354,526 SUSD	
Celo Dollar CUSD	$0.9972	0.32%	0.17%	0.19%	$41,891,606	$533,647 535,217 CUSD	42,007,588 CUSD	
Fei USD FEI	$0.9323	0.10%	3.05%	0.18%	$32,944,909	$314,601 337,473 FEI	35,337,653 FEI	
Celo Euro CEUR	$1.07	0.16%	0.09%	0.86%	$16,327,386	$320,710 300,742 CEUR	15,311,295 CEUR	

23 of them in all

source:
https://coinmarketcap.com/



source:
https://statista.com

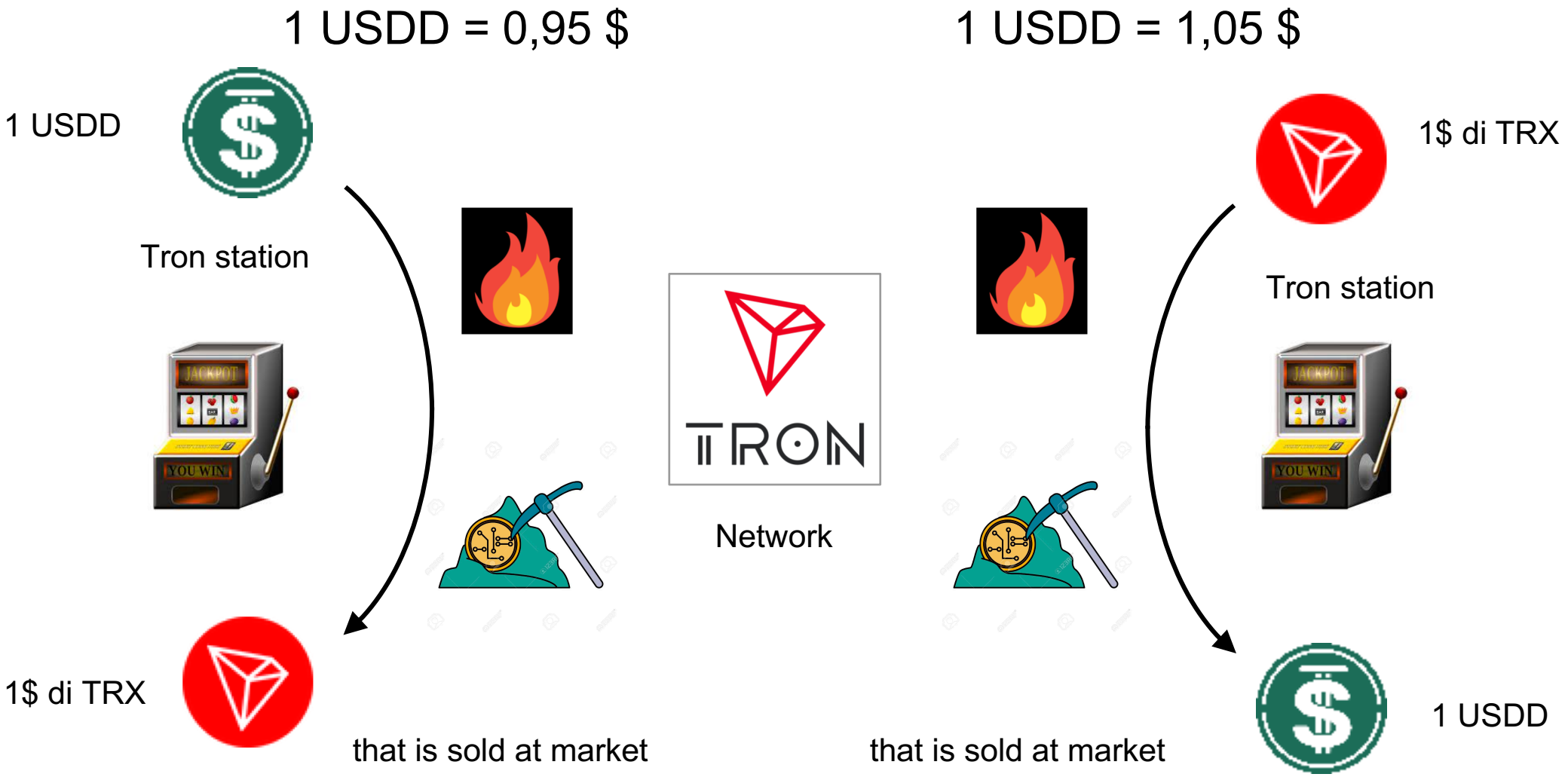
Algorithmic Stablecoin

They maintain the peg with the underlying asset through an algorithm, essentially based on a seigniorage linked to a native token of the network

Example: **USDD** of the Tron network, native token **TRX**

If the price of USDD drops below parity, i.e. $0.95, users can send to the Tron network 1 USDD of Tron to burn it and mint $1 of TRX. Doing so decreases the availability of USDD and its price increases.

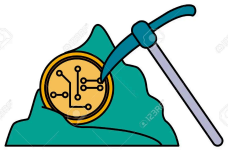
If the price of USDD rises above the parity, i.e. $1.05, users can send to the Tron network $1 of TRX to burn it and mint 1 USDD. This increases availability of USDD and its price decreases.


1 USDD = 0,95 $
1 USDD
Tron station
1$ di TRX
that is sold at market
TRON
Network
1 USDD = 1,05 $
1$ di TRX
Tron station
1 USDD
that is sold at market

1 UST = 0,95 $

1 UST

Terra station



1$ LUNA

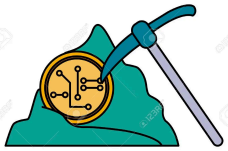
that is sold at market

Terra Luna

1 UST = 1,05 $

1$ LUNA

Terra station



1 UST

that is sold at market

TheTerra-Luna collapse

source:
https://www.tradingview.com

The Terra-Luna collapse, 9 May 2022

Swap of **85M$** UST->USDC on Curve - 9 May 2022
Withdrawal of **2B$** of UST from Anchor. Peg with USD drops to **0.987-0.995$**.
An attacker borrows **100,000** BTC from Gemini (**3B$**) and shorts them
The attacker buys **$1B** UST on the OTC market
LFG moves **150M$** in UST from liquidity pool to Curve
Attacker uses **350M$** of UST to deplete Curve's pool of liquidity
Parity with USD drops to **0.97-0.98$**.
Bank run on Anchor, at a rate of **$10M/minute**
S&P500 and Nasdaq are at a loss, the price of BTC and LUNA lose ground
The attacker still has **650M$** UST which he sells on Binance.
Massive loss of parity
LFG sells BTC of reserves to buy UST in an attempt to regain parity
The spiral of death has begun
In panic, everyone tries to sell UST, which collapses in price and totally loses parity
UST selling = UST burning = LUNA minting = LUNA price crash
Traders start shorting LUNA, which causes its price to plummet even more
On May 17, 2022, LUNA is trading at **$0.0002** and UST at **$0.09**.

The attack on the Terra-Luna ecosystem was successful because:

1) short selling had an immediate impact on the price;

2) the LFG (*Luna Foundation Guard*) support team *did not have the physical time to react*; when they sold strategic BTC reserves to buy UST it was too late;

1) the ecosystem did not have sufficient *internal structural mechanisms*, beyond seigniorage, to *discourage deviation* from the 1 USD parity.

Three proposals at the blockchain level

Terra station

for improving the stability of an algorithmic stablecoin so as to mantain parity and avoid depegging.

We use the couple UST-LUNA as a case study:

1. ***artificially disfavor toxic transactions*** that would tend to cause UST depeg;
2. artificially **slow down the speed** of **toxic transactions** that would tend to cause UST depeg;
3. implement an **internal auto-refill policy** that tends to restore parity.

1. Artificially disfavor toxic transactions

UST = 0,85 $

Toxic transactions

Transactions requiring minting of UST, i.e. burning of LUNA

Healthy transactions

Transactions requiring minting of LUNA, i.e. burning of UST

1$ LUNA

Terra station

UST = 1,15 $

Healthy transactions

Transactions requiring minting of UST, i.e. burning of LUNA

Toxic transactions

Transactions requiring minting of LUNA, i.e. burning of UST

1$ LUNA

Terra station

1. Artificially disfavor toxic transactions

The UST<->LUNA exchange of current transactions at Terra Station **is divided into two queues**, each organized in a time order:

q1) *transactions for minting UST*

1 UST

q2) *transactions for minting LUNA*

1$ LUNA

At each instant, **the choice between** which transaction of **queues q1) and q2)** will be processed **is made on the basis of a probabilistic function** dependent on:

i) the **value of UST** on the market, taken from an oracle;

ii) the **volume** of the transaction

If the trading price falls within an acceptable range of parity, e.g.

0.995<=UST<=1.005

the probability p is 0.5 for both q1) and q2). **Everything is alright.**

When the price leaves the parity range

UST<0.995 o UST>1.005

the probability of processing a toxic transaction is decreased with a suitable probabilistic law, which also depends on the volume of the toxic transaction, with p → 0 as the extreme limit.

The more toxic the transaction – in terms of transaction volume and parity deviance – the lower the probability assigned to the transaction.

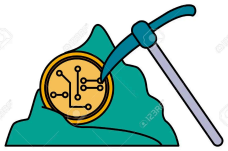
1 UST = 0,95 $

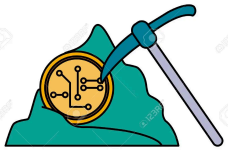
1 UST = 1,05 $

1 UST

1$ LUNA

Terra Luna





1$ LUNA

that is sold at market

that is sold at market

1 UST

Toxic transactions

UST = 0,85 $

q1)

Transactions requiring minting of UST, i.e. burning of LUNA

1 UST

$p(q1) = \mathbf{0,3}$

q2)

Transactions requiring minting of LUNA, i.e. burning of UST

1$ LUNA

$p(q2) = \mathbf{0,7}$

UST = 1,15 $

Toxic transactions

q1)

Transactions requiring minting of UST, i.e. burning of LUNA

1 UST

$p(q1) = \mathbf{0,7}$

q2)

Transactions requiring minting of LUNA, i.e. burning of UST

1$ LUNA

$p(q2) = \mathbf{0,3}$

2) **Slow down the speed of toxic transactions**

When a toxic transaction, chosen by the random mechanism described above, is still going to be processed, **the network hashing functions are slowed down** by using some *password-based key derivation functions*, such as **PBKDF2** or **Bcrypt**, with the **number of iterations increasing with size of the toxic transaction** and the **deviation from parity**.

Hence, toxic transactions tend to slow down the network, giving more time for the support team to study countermeasures, e.g. to sell strategic reserves to buy USTs from the market, raising the price or vice-versa.

PBKDF2 or **Bcrypt** are ***Key Derivation Function***

The classic hash functions (MD5, SHA, RIPEMD) are designed to be very fast in execution.

If the hash function computes very fast, with some specific GPUs one can execute billions of hashes/s, thus attempting a massive brute-force attack (exhaustive search).

In some cases it is therefore preferable to have **hash functions** that are calculated **using important computational resources**, in order to discourage attacks based on the exhaustive search.

A typical use case is that of hash functions for the management of the passwords in a database (DB), which must recognize the user passwords. These will not be stored on the DB as they stay, since a forcing of the DB would allow uncovering all user passwords.

It is then customary to store on the DB only the hashes of the passwords.

We also want the difficulty to be modulated, making it eligible for technology-based upgrades of new generations of computers.

In our use case the difficulty (# of iterations) is modulated based on the transaction toxicity and the deviance from parity.

PBKDF2:
RSA *Laboratories' Public-Key Cryptography Standards*

used in:

Kerberos
WPA-WPA2
Microsoft Windows Data Protection API
Mac OS X Mountain Lion
Apple iOS
Cisco IOS

Kerberos (2005) recommanded 4096 iterations

Apple used 2000 iterations for iOS 3 and 10000 for iOS 4

LastPass (2011) used 5000 for *JavaScript* clients and
100000 on the server side

WPA2 uses 4096

Bcrypt:

used in:

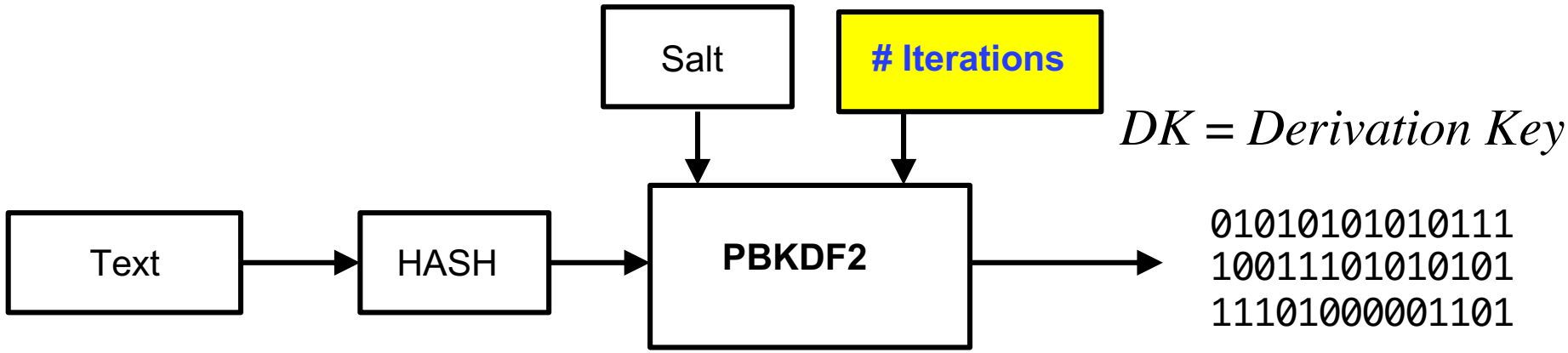
OpenBSD
Unix
Linux

PBKDF2
Password-Based Key Derivation Function

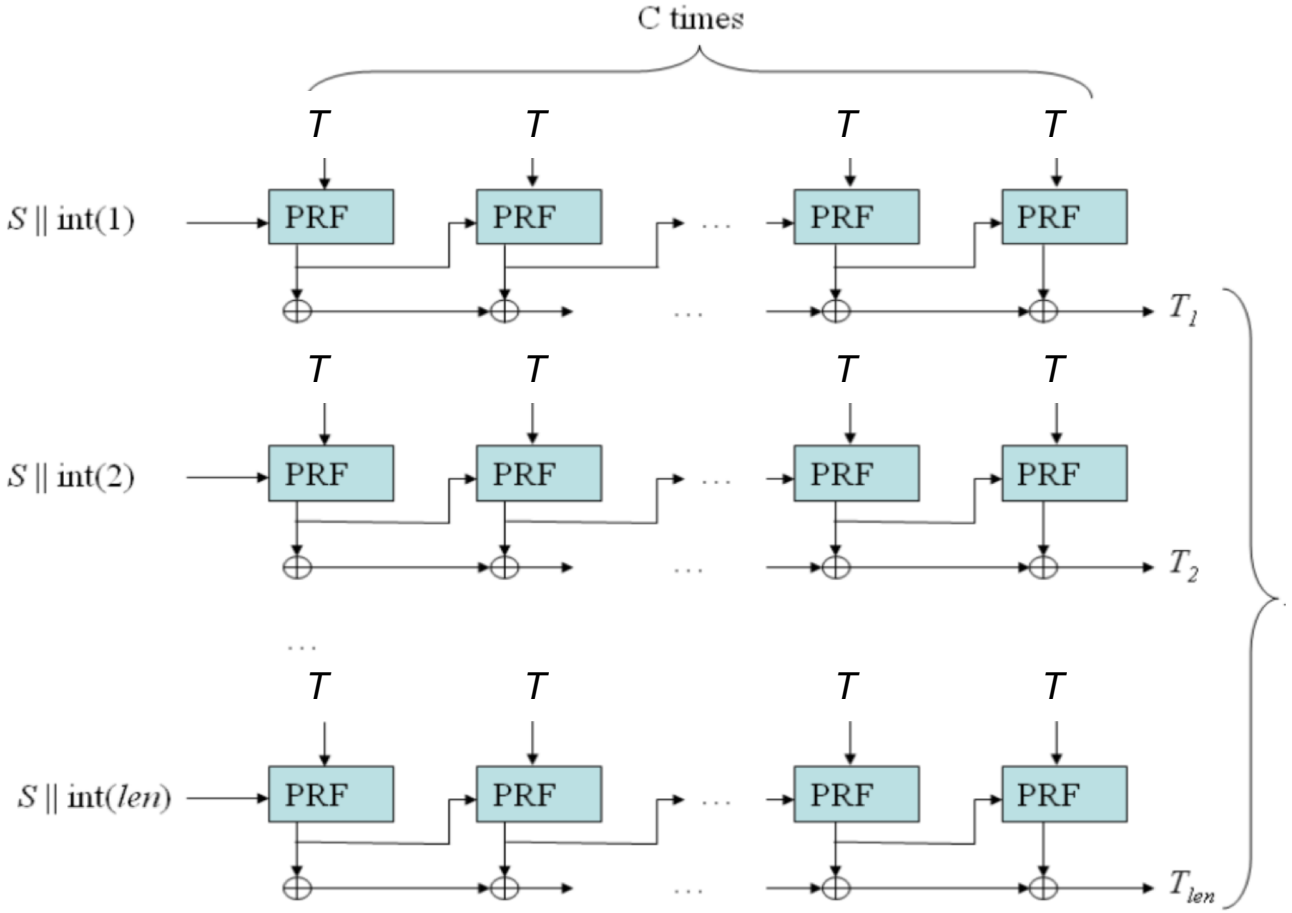
$$DK = \mathrm{KDF}(Password, Salt, Iterations)$$

DK = *Derivation Key*

Salt = random string



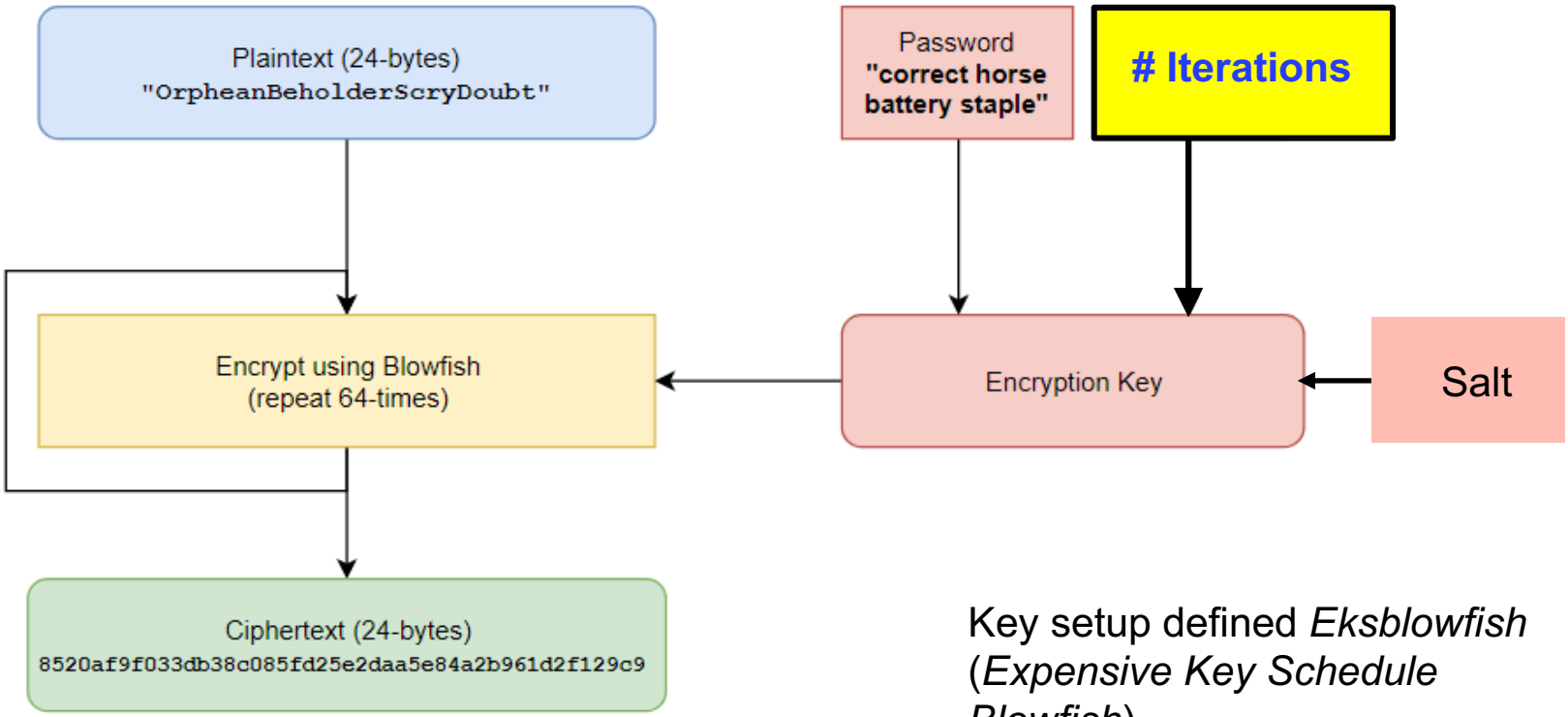
Structure of PBKDF2



C = # iterations
T = Text
S = Salt
int(i) = 32 bit BE number i

slowed-down hash

Structure of Bcrypt



Key setup defined *Eksblowfish* (*Expensive Key Schedule Blowfish*)

192 hash length

3) **Internal auto-refill policy**

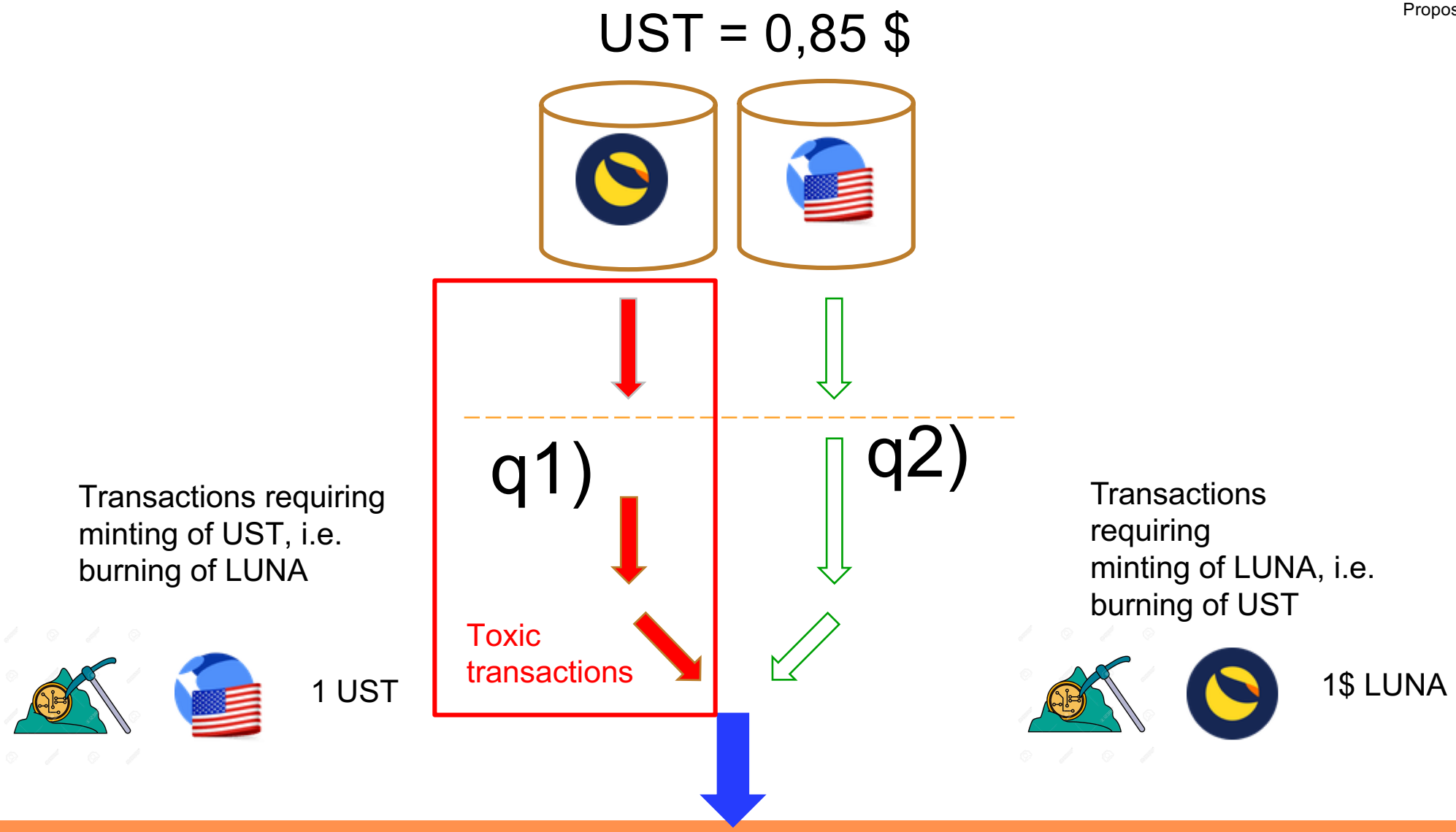
Luna Foundation Guard (*LFG*) was not able to use the $1B BTC reserves to re-peg UST due to **lack of time**, **difficulties in handling several wallets** in real-time, and so on.

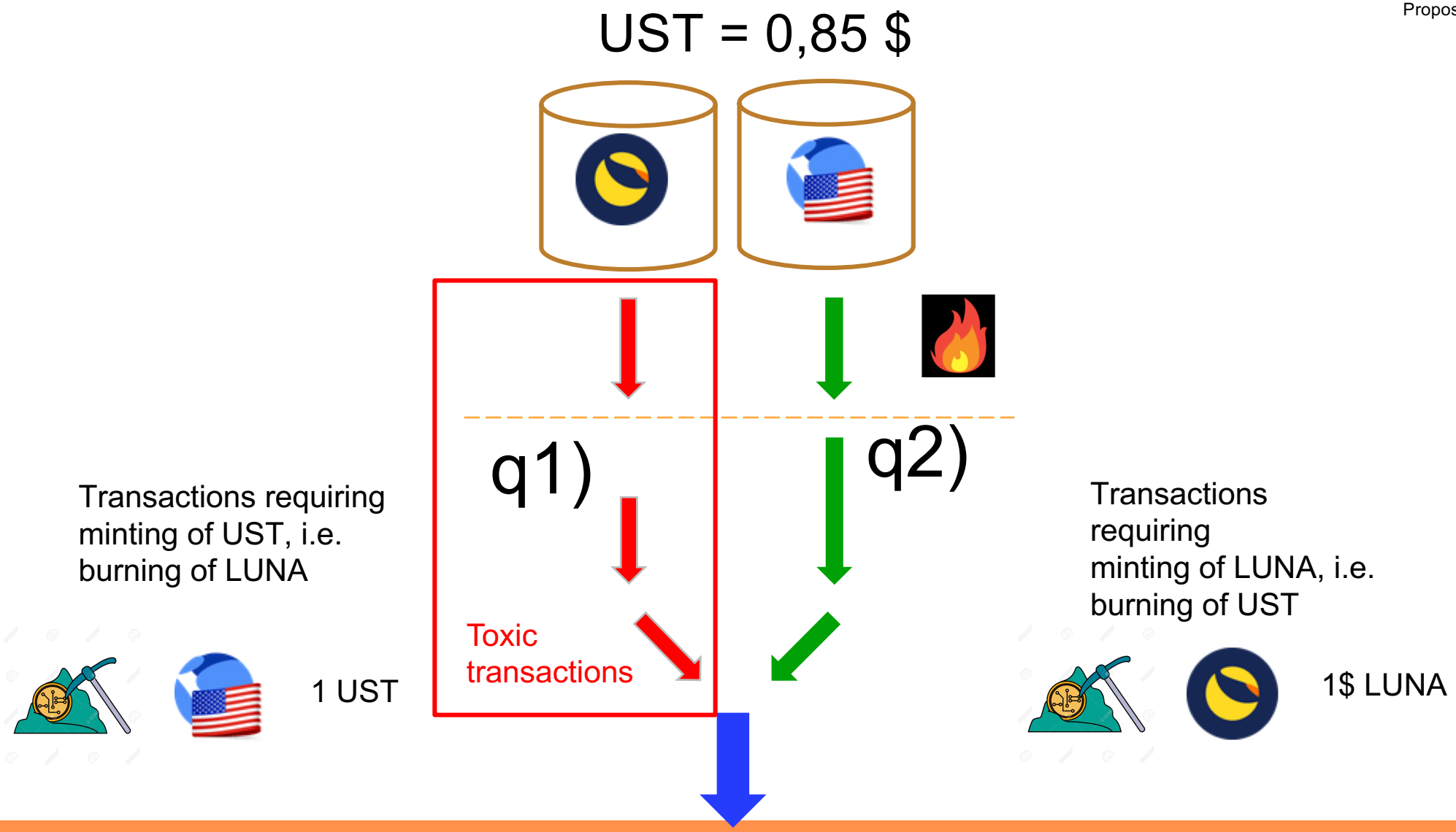
In the proposal the ecosystem has **two strategic reserves** previously acquired, **one with LUNA** and **one with UST**. They are similar to the BTC reserves used by *LFG* during the collapse to try to stabilize the price.

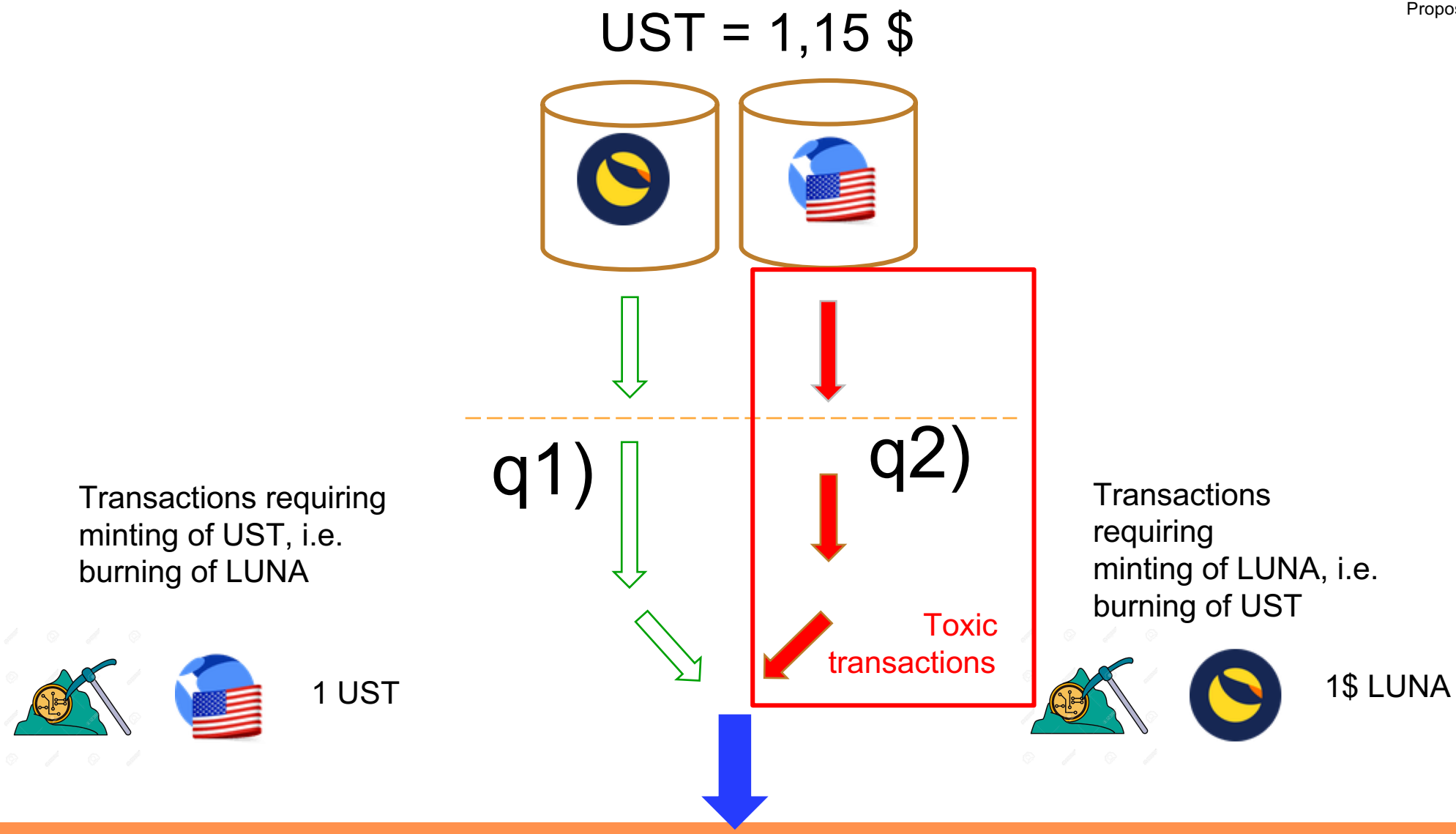
Reserves are used automatically when, during an attack to parity, **no one is booking healthy transactions** that tend to restore the peg (one of the two queues q1)-q2) is empty).

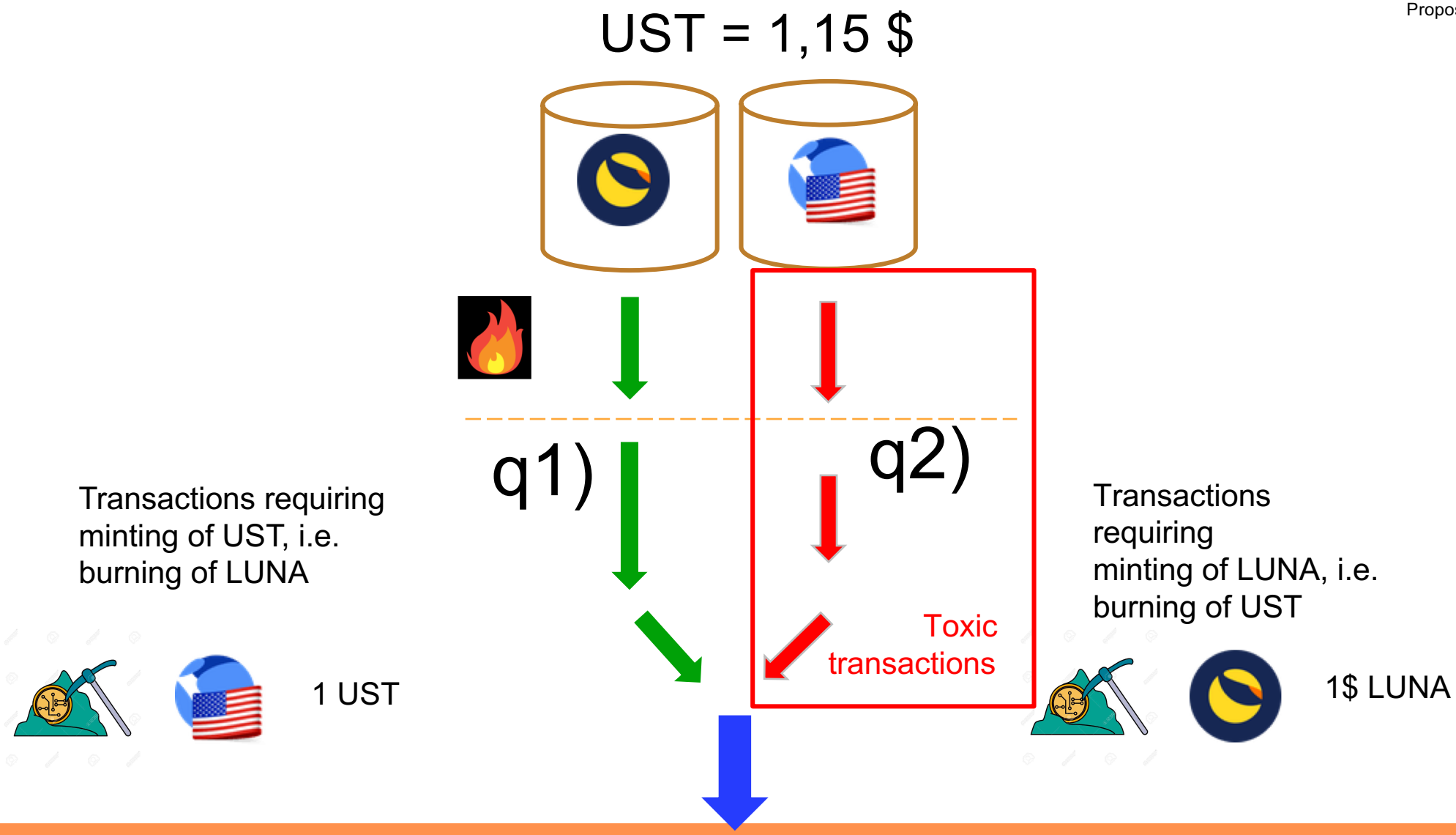
The **size** of the top-up **depends on the deviation from parity** and the **amount of volume**, up to a certain level, accumulated by queued **toxic transactions**.

For example, if UST = $0.85 and queue q2) is empty, the protocol starts automatically a top-up transaction, which enters fresh LUNA to the queue.


UST = 0,85 $
q1)
q2)
Transactions requiring minting of UST, i.e. burning of LUNA
Toxic transactions
Transactions requiring minting of LUNA, i.e. burning of UST
1 UST
1$ LUNA


UST = 0,85 $
q1)
q2)
Transactions requiring minting of UST, i.e. burning of LUNA
Toxic transactions
Transactions requiring minting of LUNA, i.e. burning of UST
1 UST
1$ LUNA


UST = 1,15 $
q1)
q2)
Transactions requiring minting of UST, i.e. burning of LUNA
Toxic transactions
Transactions requiring minting of LUNA, i.e. burning of UST
1 UST
1$ LUNA

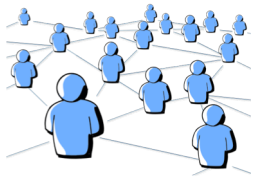

UST = 1,15 $
q1)
q2)
Transactions requiring minting of UST, i.e. burning of LUNA
Toxic transactions
Transactions requiring minting of LUNA, i.e. burning of UST
1 UST
1$ LUNA

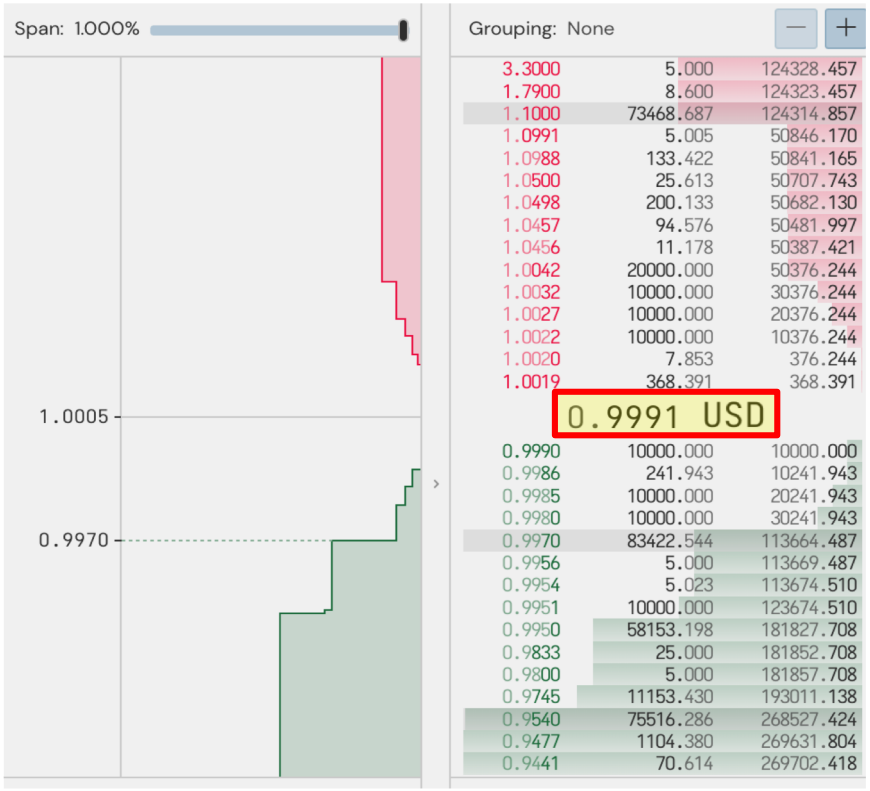
What could be the connection point with NiRvAna project and all of this stuff?

There could be a use case in the CBDC context:

Traditional financial system

Digital Euro Network





source:
https://www.kraken.com