Stablecoins:

an elusive dream of stability

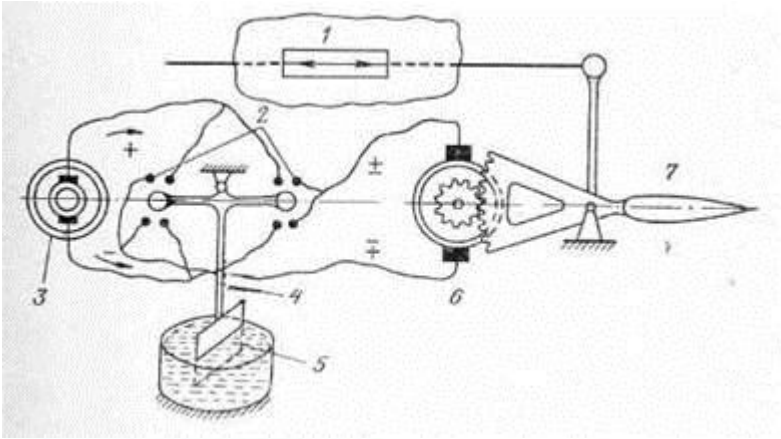
Sergey Ivliev,
Lykke, Perm State University
Perm Winter School 2018

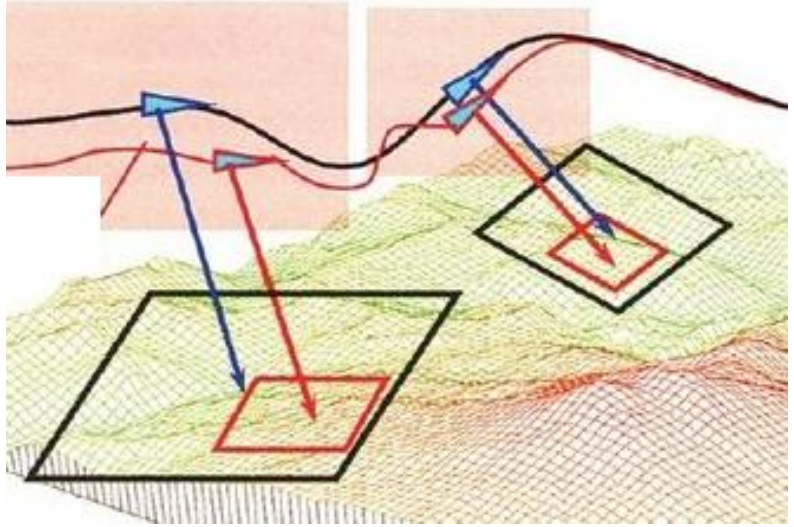
What is Stability?

- **Stability**, a situation in which something is not likely to move or change
- **Chemical stability**, occurring when a substance is in a dynamic chemical equilibrium with its environment
- **Stability of solutions of differential equations** and of trajectories of dynamical systems under small perturbations of initial conditions
- **Economic stability**, the absence of excessive fluctuations in the macroeconomy

What is Stability?

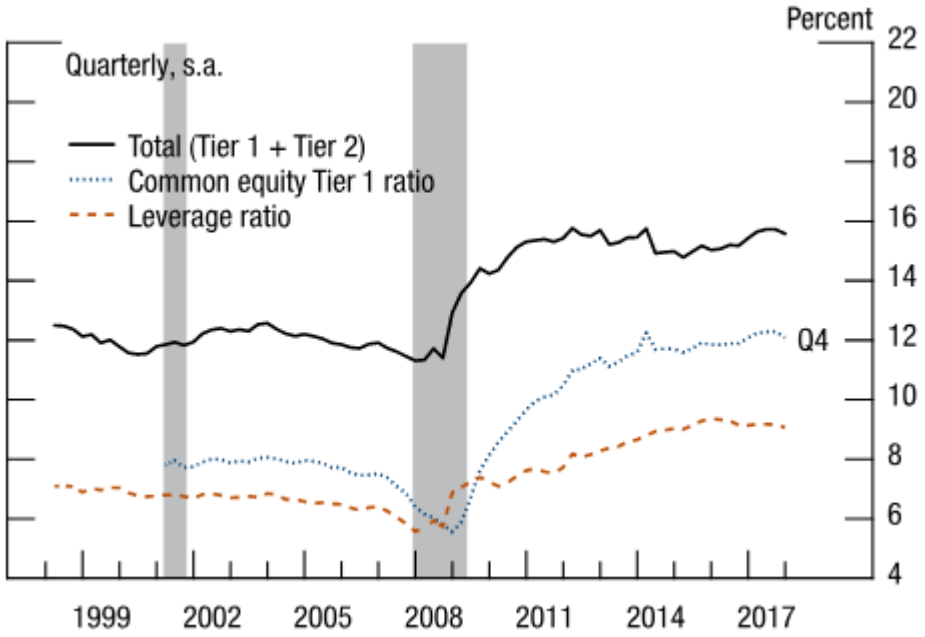
- **Control Theory**, operating dynamical systems using a control action in an optimum manner without delay or overshoot and ensuring control stability
- **Flight stabilization,** taking into account external (e.g. wind) and internal (e.g. resonance) disturbances and compensating them with allowance for the maximum values acceptable by an aircraft / rocket





What is Stability?

- **Financial stability** can be broadly defined as "a condition in which the financial system can facilitate real economic activities smoothly and is capable of unravelling financial imbalances arising from shocks"
- **Financial stability** is about building a financial system that can function in good times and bad, and can absorb all the good and bad things that happen in the economy at any moment



‘Good money’ fundamentals

Lykke

Money use cases:

- Store of value
- Medium of exchange
- Unit of account: Price discovery/signalling

MONEY IS
THE ROOT OF
ALL GOOD

Good money is:

- Durable
- Divisible
- Fungible
- Portable
- Relatively scarce
- Resistant to counterfeiting

…also…

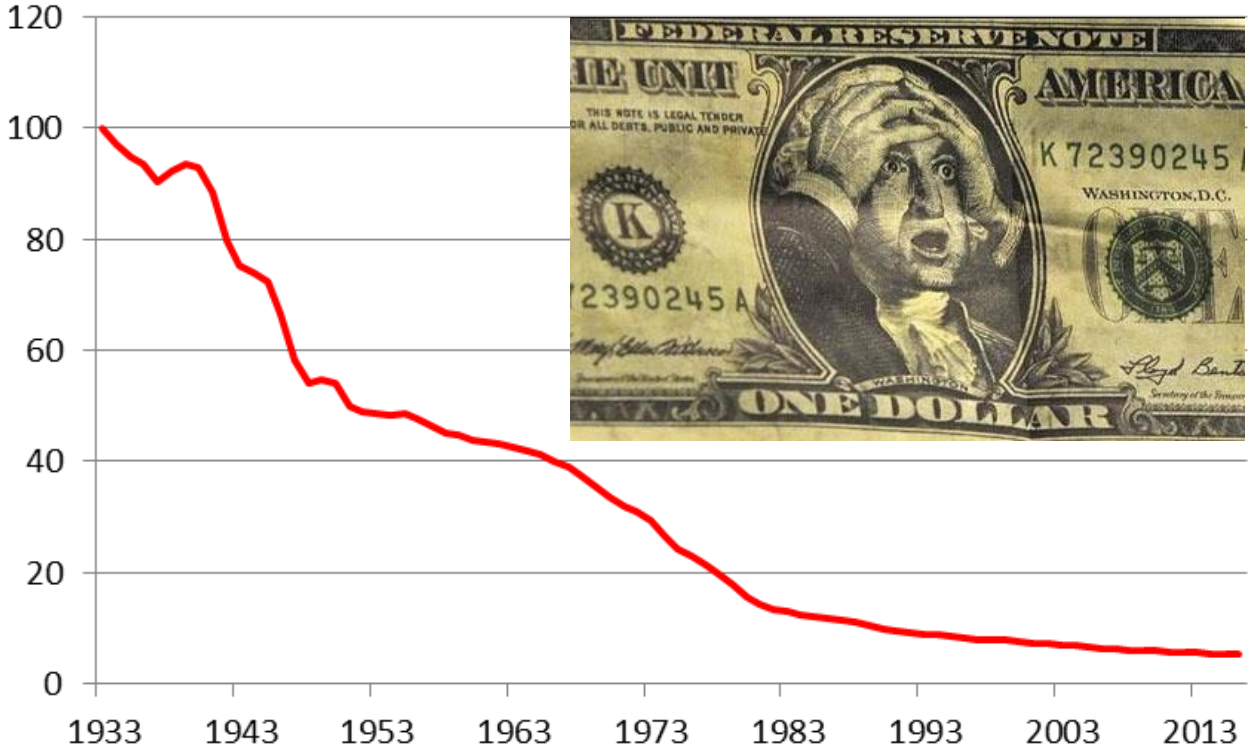
- Private
- Censorship resistant
- Socially scalable

US Dollar

- Short-term stable: **0.18%** 90-d volatility to basket (SDR)
- Store of value: >**63%** of currency reserves
- Payment method: **>50%** of payments (SWIFT)
- Unit of account of choice

…but

- Long term inflation (halving every **20** yrs)
- Not private (except for $ cash)
- Not resistant to censorship
- Not suitable for microtransactions

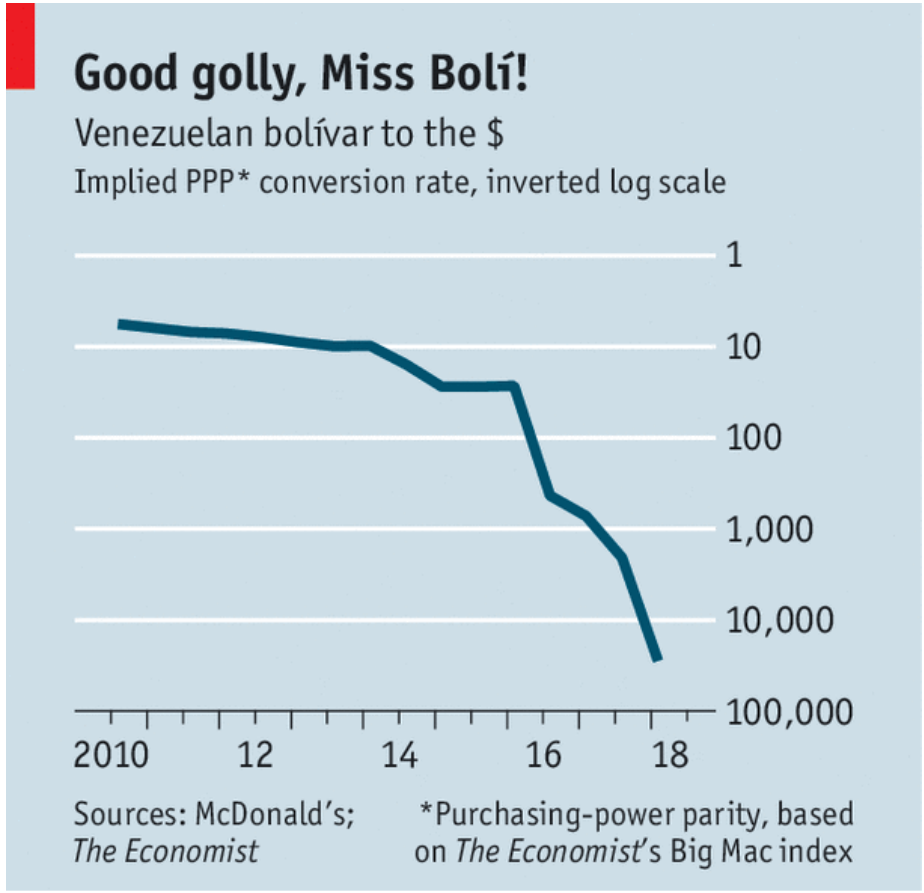


https://www.swift.com/node/19186

http://www.imf.org/en/News/Articles/2017/03/31/pr17108-IMF-Releases-Data-on-the-Currency-Composition-of-Foreign-Exchange-Reserves

Fiat currencies

- **27 years** average life expectancy of a fiat currency
- **20%** failed through hyperinflation, **21%** destroyed by war, **12%** destroyed by independence, **24%** were monetarily reformed

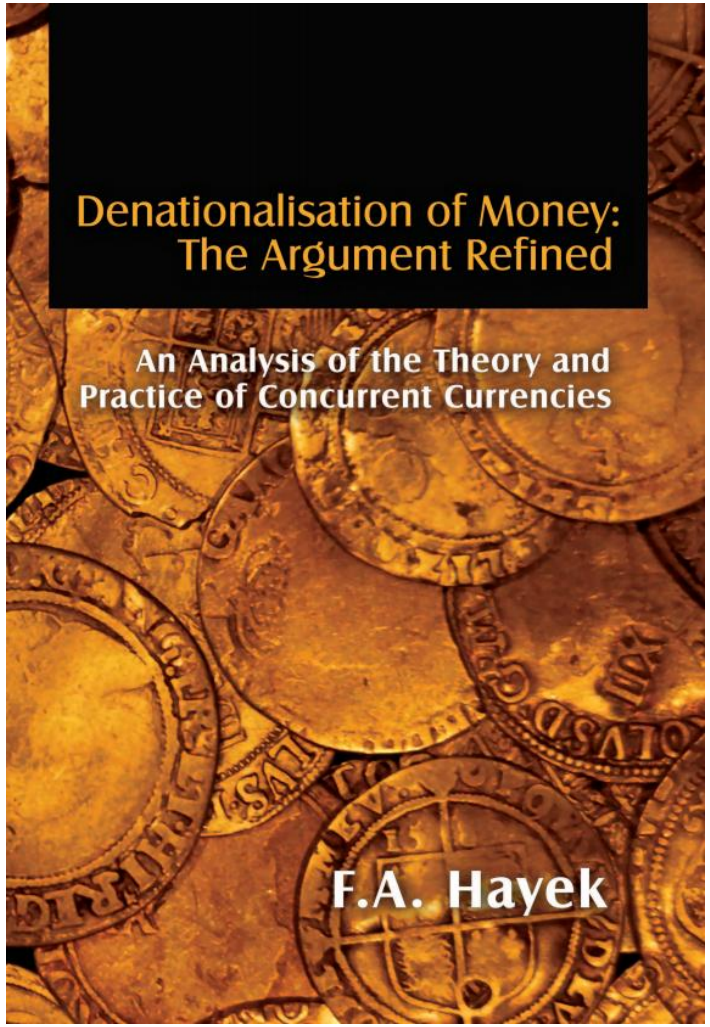


Economist.com

http://georgewashington2.blogspot.com/2011/08/average-life-expectancy-for-fiat.html

Private money

- **Price level stability** can be achieved only by removing from national governments their monopoly of money creation
- **Private businesses** should be allowed to issue their own forms of money, deciding how to do so on their own
- **Competition** will favour currencies with the greatest stability in value



https://nakamotoinstitute.org/static/docs/denationalisation.pdf

Cryptocurrencies

‘Magic Internet Money’:

- Decentralized consensus on monetary policy => **Relatively scarce**
- Expensive double-spending (cost of 51% attack) => **Resistant to counterfeiting**
- Fast finality => **Portable, Transferable**
- **Divisible**
- **Fungible**
- Pseudoanonymous, difficult to trace => **Private**
- Direct ownership => **Censorship-resistant**
- **139m** total accounts, **35mln** ID-verified users, 3Q18

  25% expect to own, adoption 2x in 2018

  => **Socially scalable**

Why didn’t we all switched to BTC then?

Cryptocurrencies

"…cryptocurrencies such as Bitcoin, Ethereum, and Ripple are vying for a spot in the cashless world, constantly reinventing themselves in the hope of offering more stable value, and quicker, cheaper settlement"

"For now, virtual currencies such as Bitcoin pose little or no challenge to the existing order of *fiat* currencies and central banks. Why? Because they are **too volatile**, too risky, too energy intensive, and because the underlying technologies are **not yet scalable**.
But many of these are *technological* challenges that could be addressed over time."

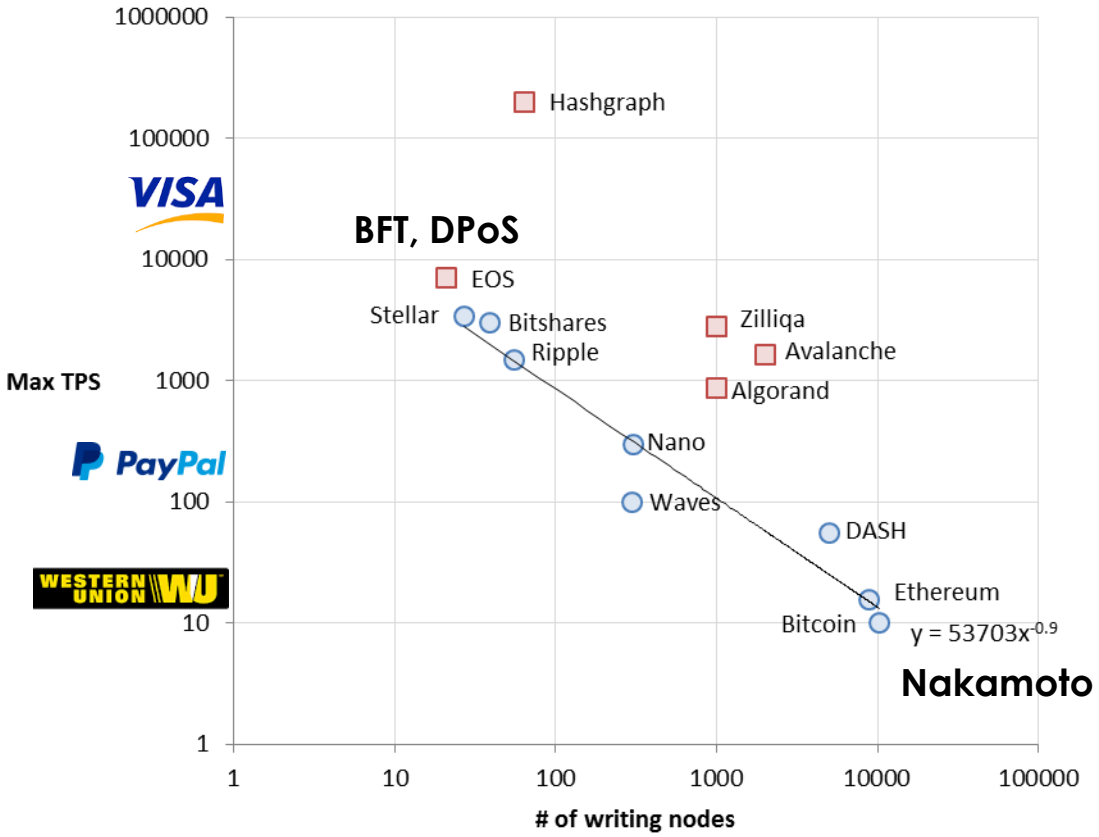
And it's not a legal tender yet

https://www.imf.org/en/News/Articles/2018/11/13/sp111418-winds-of-change-the-case-for-new-digital-currency

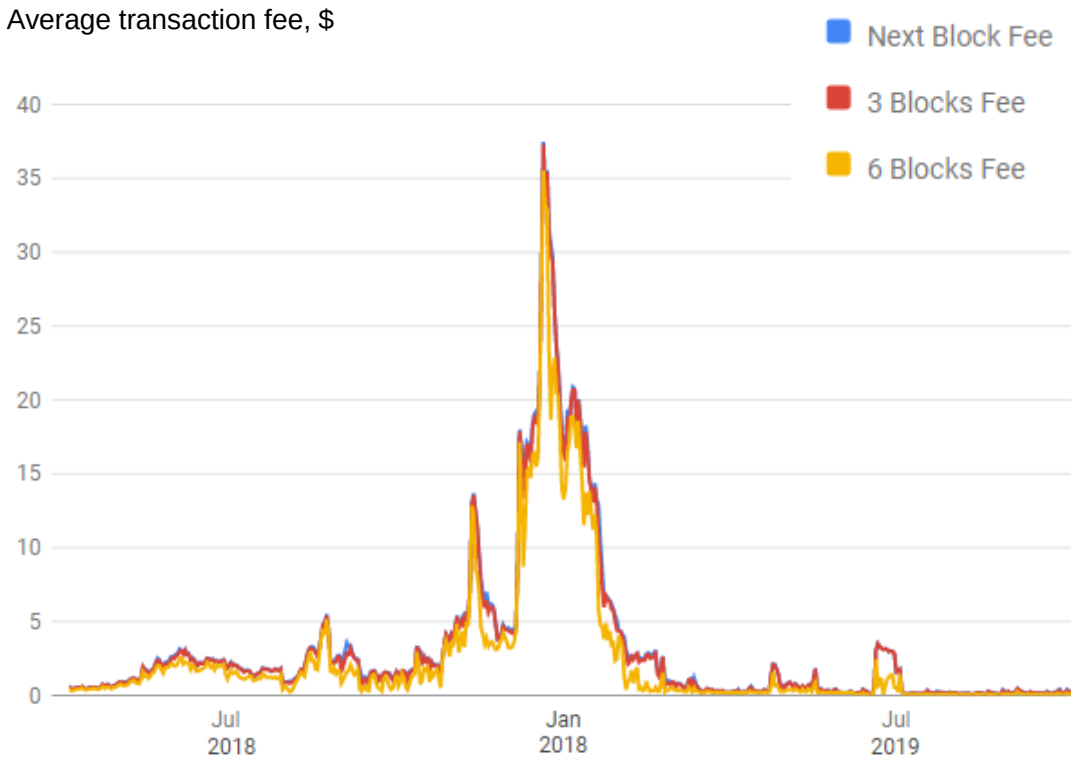
https://www.imf.org/en/News/Articles/2017/09/28/sp092917-central-banking-and-fintech-a-brave-new-world

Cryptocurrencies

- **Scalability** problem



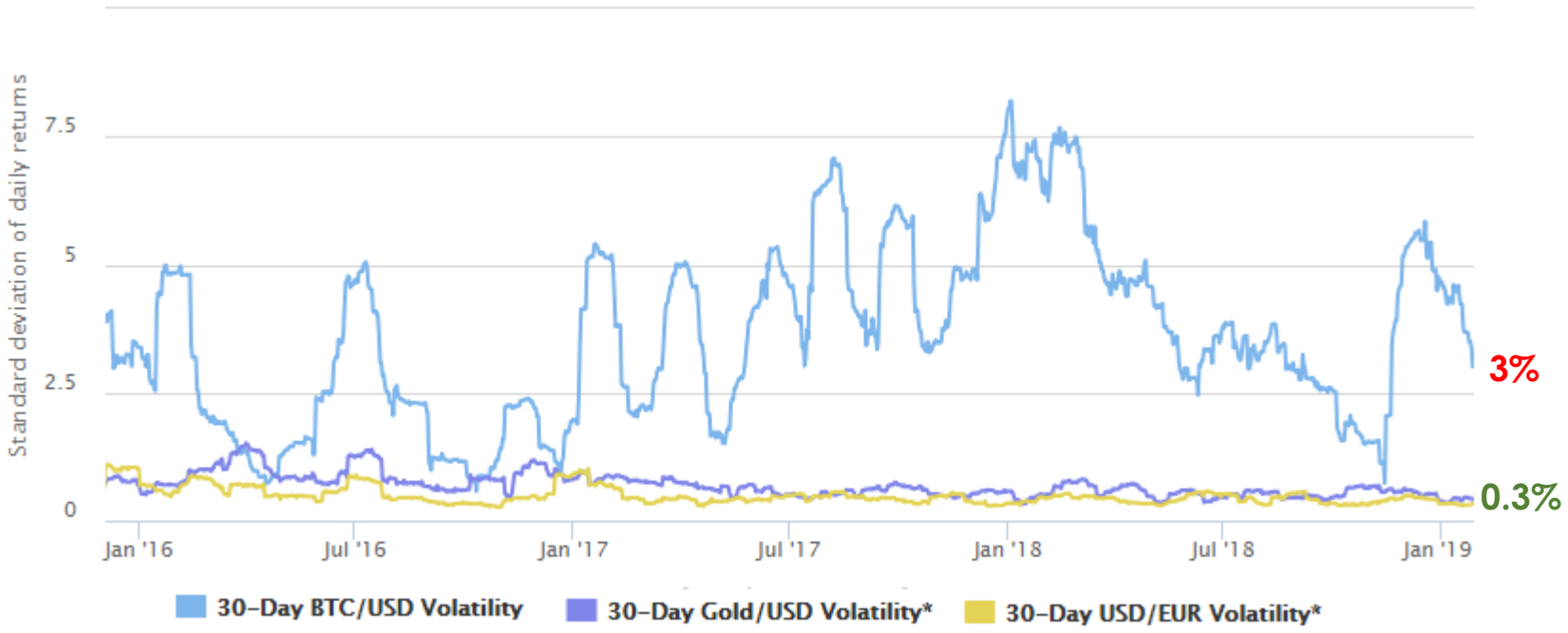
- **Expensive to transact** when congested



Horizontal (sharding) and vertical (L2-networks) scaling

Cryptocurrencies

- **3%** 30-d volatility of BTC/USD, up to **7.5%** (**>100%** annual)
- **10x** compared to EUR/USD and Gold volatility (**0.3-0.4%**, up to **1-3%** daily)

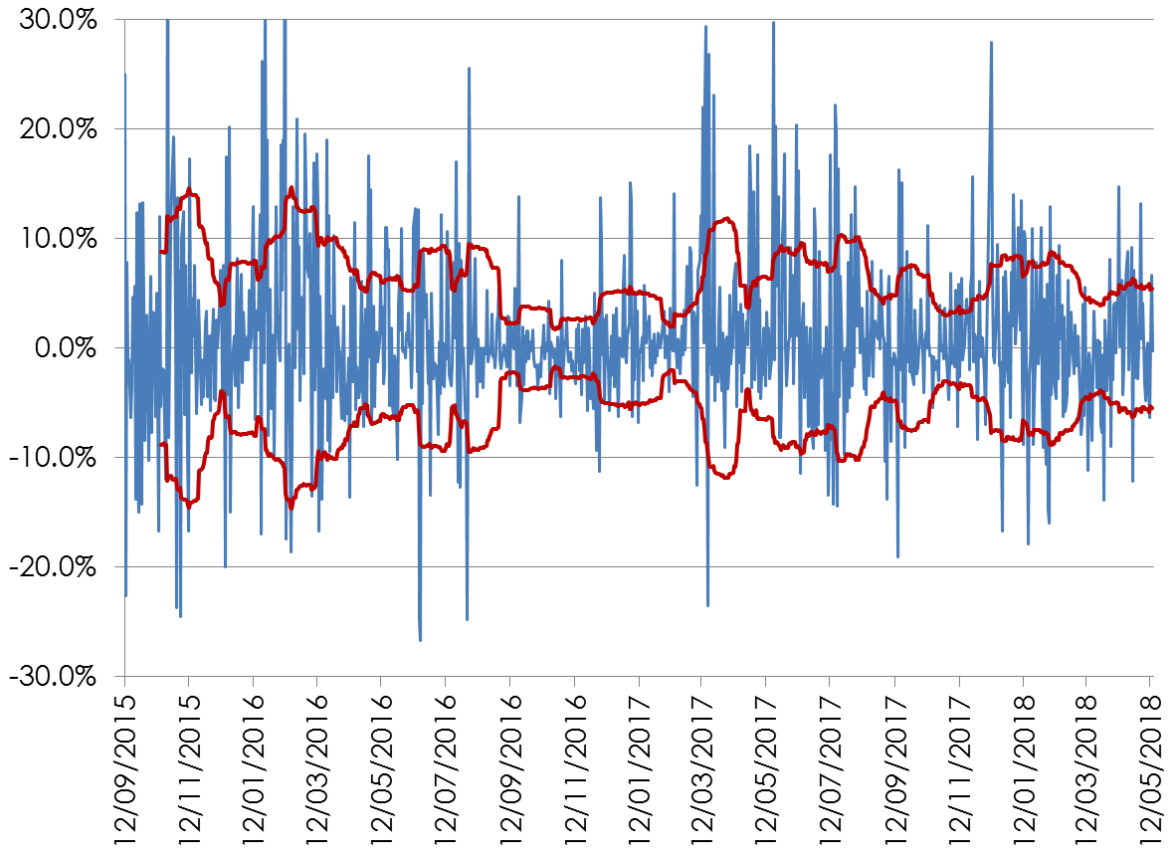


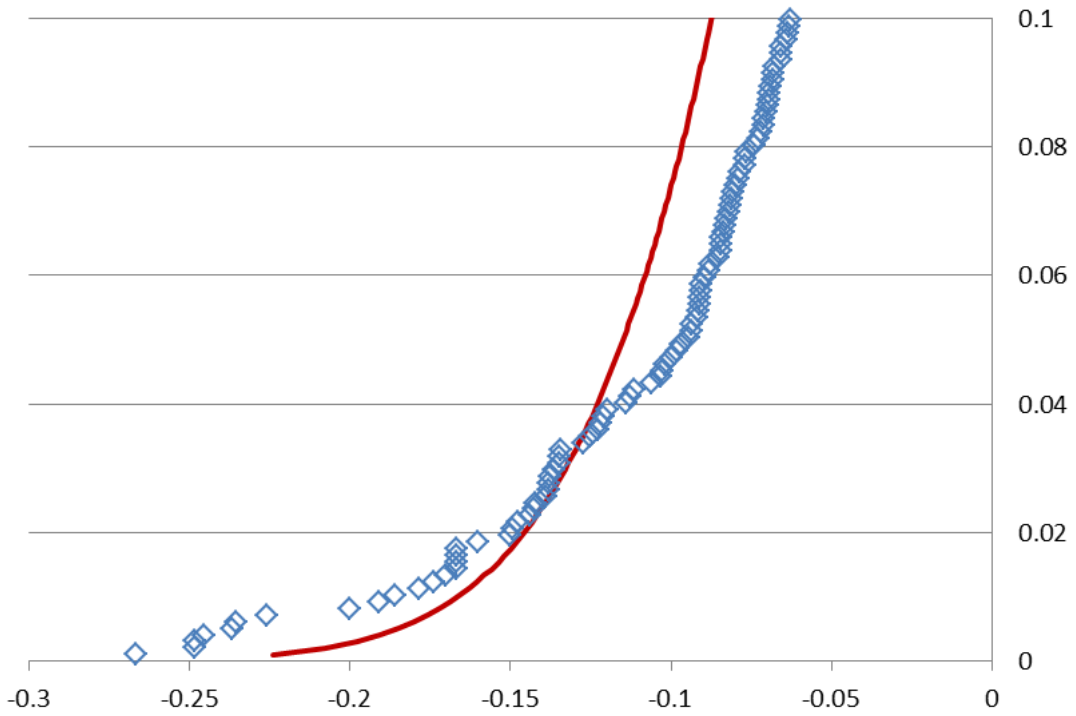
https://www.buybitcoinworldwide.com/volatility-index/

Too volatile for Means of Payment

Cryptocurrencies

- Other cryptos are even more volatile
- **7.5%** sample std.dev for ETH returns, **8.2%** sample volatility for Bitshares, etc.
- Heavy tails: **3x** sigma price drops are pretty frequent





Fat tails

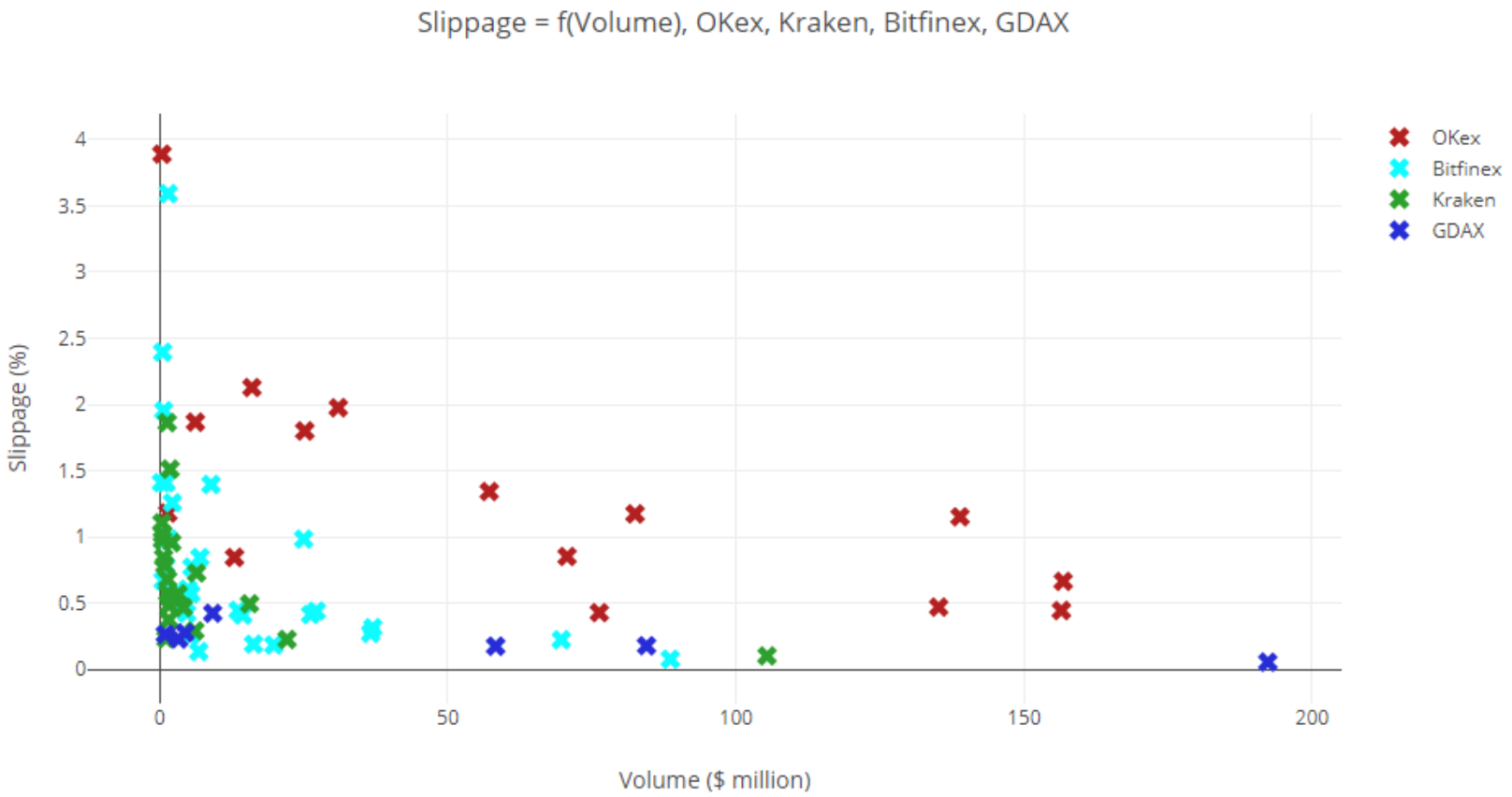
Cryptocurrencies

- Intraday price jumps (shocks) are severe: **>10%** in less than 1 hour

Other cryptos are even worth

Cryptocurrencies

- Liquidity is spurious on many exchanges (slippage **> 0.25%** for $50k order)



Fake volume, low liquidity

https://medium.com/@sylvainartplayribes/chasing-fake-volume-a-crypto-plague-ea1a3c1e0b5e

Stablecoins

Must have's

- Price stability

Nice to have's

- Transparent structure and governance
- Insignificant tail event risk (e.g. collateral risk)
- Market liquidity
- Scalability
- Privacy
- Censorship resistance
- Adoption (exchanges, wallets)

Holy Grail of Crypto

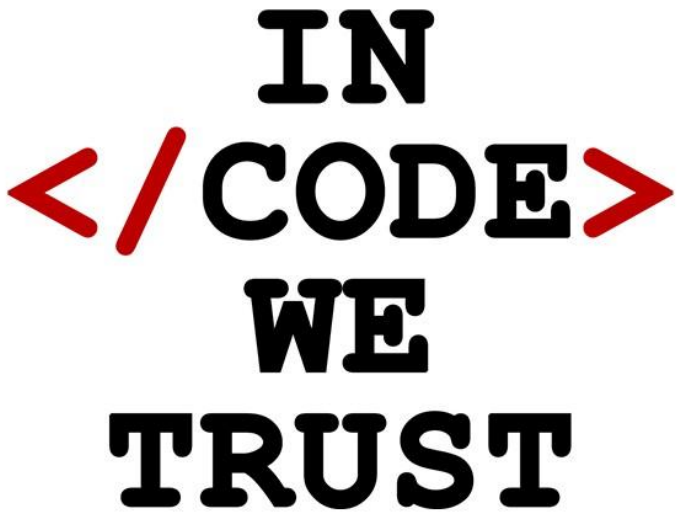
Stablecoins

Lykke

3 types of Stablecoins:

- Centralized IOUs (“*I-Owe-You*”)
- Decentralized collateral-backed
- Algorithmic-stable

What do we trust in?



Centralized IOUs

Tether

- Symbol: USDT
- Colored coin (OMNI protocol)
- Issuer: Tether International Limited
- Launched: 2014 (Realcoin)
- Redeemable for fiat (Kraken, OTC)
- Close ties with Bitfinex

	TetherUS created by 5ed3694e8a4fa8d3ec5c75eb6789492c69e65511522b220e94ab51da2b6dd53f
Total	**3,020,000,000.00 Tokens**
Name	**TetherUS**
PropertyID	**#31**
Created	10/6/2014 9:39:15 PM
Data	The next paradigm of money.
Sender	3MbYQMMmSkC3AgWkj9FMo5LsPTW1zBTwXL
Category	Financial and insurance activities
Divisible	True
URL	https://tether.to
Raw Data	Click here for raw info

Centralized IOUs
Tether

- Proof of reserve

USD₮	
Total Assets	**$2,075,761,771.12**
Liabilities (Tether in Circulation on Omni)	
Total Authorized	$2,520,000,000.00
Less: Authorized but not issued	- $462,239,404.48
Less: Quarantined Tether	- $30,950,010.00
Liabilities (Tether in Circulation on Eth)	
Total Authorized	$60,057,493.36
Less: Authorized but not issued	- $35,066,902.33
Total Liabilities	**$2,051,801,176.55**
Shareholder Equity	**$23,960,594.56**

https://wallet.tether.to/transparency

MONITOR AND REVIEW:

Pursuant to the above terms of Engagement, and the discretion provided by Tether, FSS selected the date of June 1st, 2018, and received the following balance information from Tether's two banks as of the close of the banking day. FSS received the following confirmations from the respective banks by sworn and notarized statements provided by duly authorized personnel.

BANK 1: $1,968,538,584.82 USD (unencumbered)

BANK 2: $576,528,652.00 USD (unencumbered)

TOTAL: $2,545,067,236.82 USD

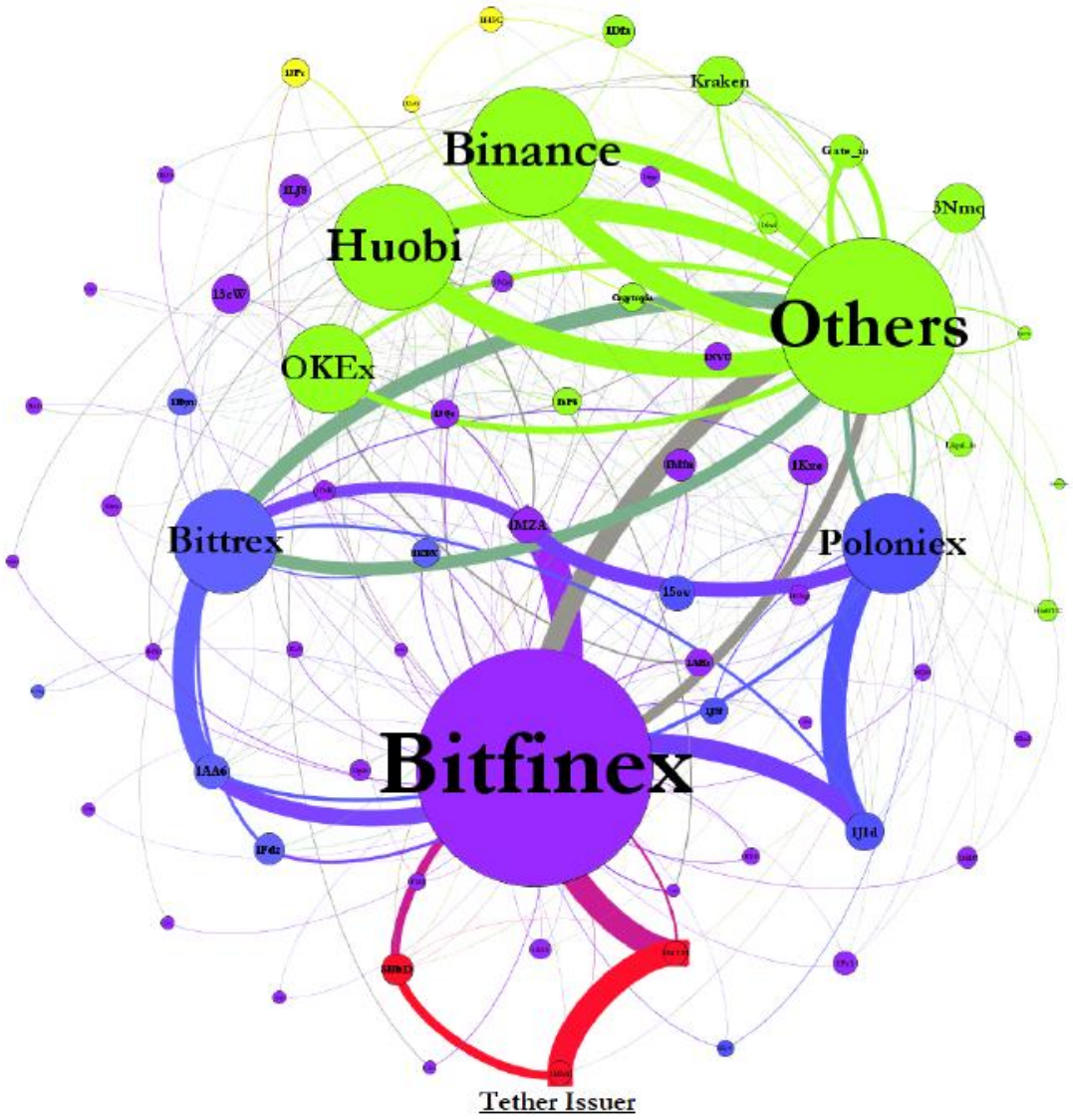
In conjunction with receiving the above balance information, FSS requested the Chief Financial Officer and the General Counsel of Tether to certify, by sworn statement, the amount of fully-backed USD Tethers that were in circulation as of the close of business on June 1st, 2018. The amount certified to FSS was $2,538,090,823.52 USD Tethers. According to Tether's transparency page (https://wallet.tether.to/transparency), the amount of fully-backed USD Tethers in circulation as of June 1st, 2018 was equal to $2,538,090,823.52 USD Tethers. FSS did not provide the Tether personnel with any advance notice, nor did FSS provide Tether the account balance information gathered from the two banks prior to receiving the Tether balance information.

https://tether.to/wp-content/uploads/2018/06/FSS1JUN18-Account-Snapshot-Statement-final-15JUN18.pdf

Centralized IOUs

Tether

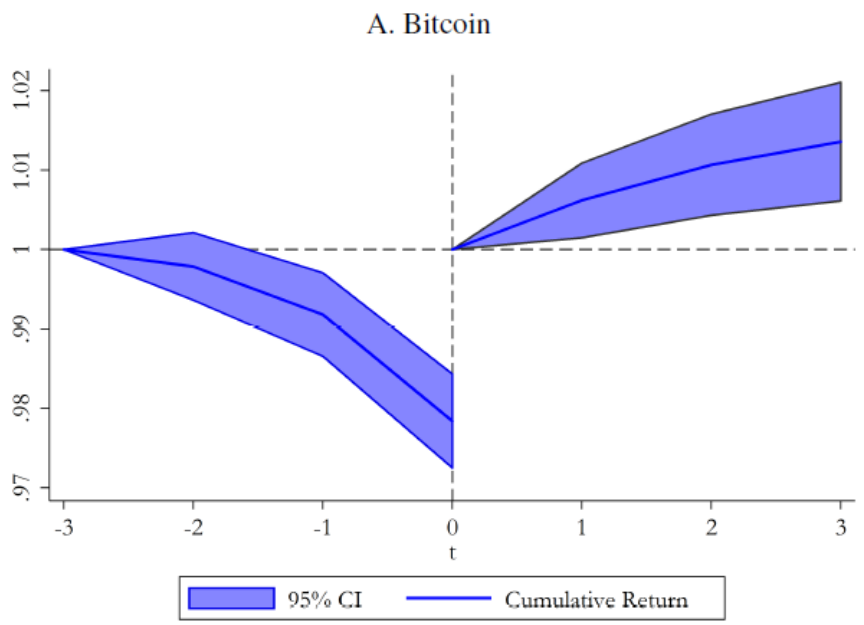
- Aggregate flow between major addresses
- USDT are issued at private address
- Sent to Bitfinex
- Bittrex and Poloniex are close allies



Griffin, John M. and Shams, Amin, Is Bitcoin Really Un-Tethered? (June 13, 2018). SSRN: https://ssrn.com/abstract=3195066

Centralized IOUs
Tether

- Controversy: "*Less than 1% of hours with such heavy Tether transactions are associated with 50% of the meteoric rise in Bitcoin and 64% of other top cryptocurrencies.*"



Markets

Bitcoin-Rigging Criminal Probe Focused on Tie to Tether

By Matt Robinson and Tom Schoenberg

20 ноября 2018 г., 14:00 GMT+5 *Updated on 20 ноября 2018 г., 19:10 GMT+5*

- DOJ investigating whether Tether was used to prop up Bitcoin
- U.S. case part of broader review of possible coin manipulation

Griffin, John M. and Shams, Amin, Is Bitcoin Really Un-Tethered? (June 13, 2018). SSRN: https://ssrn.com/abstract=3195066

https://www.bloomberg.com/news/articles/2018-11-20/bitcoin-rigging-criminal-probe-is-said-to-focus-on-tie-to-tether

Centralized IOUs

TrueUSD

- Symbol: TUSD
- ERC20 token
- Launched: Jan 2018
- Issuer: TrueCoin LLC
- Custodian: Prime Trust LLC
- Audited by: Cohen & Co
- Redeemable for fiat (>$10k)

Backers

a16zcrypto
BLOCKTOWER
DISTRIBUTED GLOBAL
foundation capital
FOUNDERS FUND
GGVCAPITAL
JumpCapital
SIGNIA VENTURE
SLOW VENTURES
Stanford University
Stanford-StartX Fund
ZhenFund

Centralized IOUs
TrueUSD

- Proof of reserve

TrueUSD Attestation Reports

TrustToken has engaged Cohen & Company, a Top 50 public accounting firm with cryptocurrency expertise, to independently confirm that the TrueUSD assets the independent fiduciaries hold in escrow adequately collateralize the outstanding TrueUSD coins that have been issued. **All the attestations that have been published since the launch of TrueUSD can be viewed below.**

Cohen & Co

https://blog.trusttoken.com/trueusd-attestation-reports-86f693b90a4

TRUECOIN LLC
325 9th Street
San Francisco, CA 94103

ESCROW HOLDINGS REPORT

JULY 16, 2018

Balance of Escrow Account(s): $ 79,051,658.66

NOTES

1. The issued and outstanding TrueUSD tokens on the blockchain as of 5:00 pm ET on July 16, 2018 do not exceed the balance of the Escrow Account(s) reported above.
2. The USD balance in the Escrow Account is held at Prime Trust, LLC (the "Escrow Agent") for the benefit of the TrueUSD token holders as agreed to within the Escrow Agreement(s).
3. In the event of Escrow Agent's insolvency, recovery of the USD Balance in the Escrow Account with the Escrow Agent may be limited to account insurance or other protection afforded such deposits.
4. As agreed to within the Escrow Agreement(s), TrueCoin LLC and the Escrow Agent are not entitled to any funds at any time and no amounts deposited into the Escrow Account(s) shall become the property of TrueCoin LLC, the Escrow Agent, or any other entity, or be subject to any debts, liens or encumbrances of any kind of TrueCoin LLC, the Escrow Agent, or any other entity.

https://drive.google.com/file/d/12_p6U3RC8EkVToLAewagcU48_4_-cl7o/view

Centralized IOUs
Runners-up

Lykke

GEMINI dollar

- *Symbol*: GUSD
- ERC20 token
- *Launched*: Sep 2018
- *Issuer*: Gemini Trust Company
- *Custodian*: State Street
- *Auditor*: BPM LLP
- Fiat exchange only at Gemini
- 45 exchanges & wallets

https://gemini.com/dollar

PAXOS STANDARD

- *Symbol*: PAX
- ERC20 token
- *Launched*: Sep 2018
- *Issuer*: Paxos Trust Company
- *Custodian*: N/A
- *Auditor*: Withum
- Min withdrawal: $50K
- 80 exchanges & wallets

https://www.paxos.com/standard/

USD Coin

- *Symbol*: USDC
- ERC20 token
- *Launched*: Sep 2018
- *Issuer*: Centre (Coinbase, Circle)
- *Custodian*: US Bancorp
- *Auditor*: Grant Thornton LLP
- Min withdrawal: $50K
- 92 exchanges & wallets

https://www.circle.com/ru/usdc

Centralized IOUs
Summary

Lykke

Pros

- Easy to understand
- Strong backers
- High adoption

Cons

- Issuer credit risk (*probability of default*)
- Custodial risk (*loss given default*)
- Subject to hard AML requirements
- Not censorship resistant

Decentralized collateral-backed

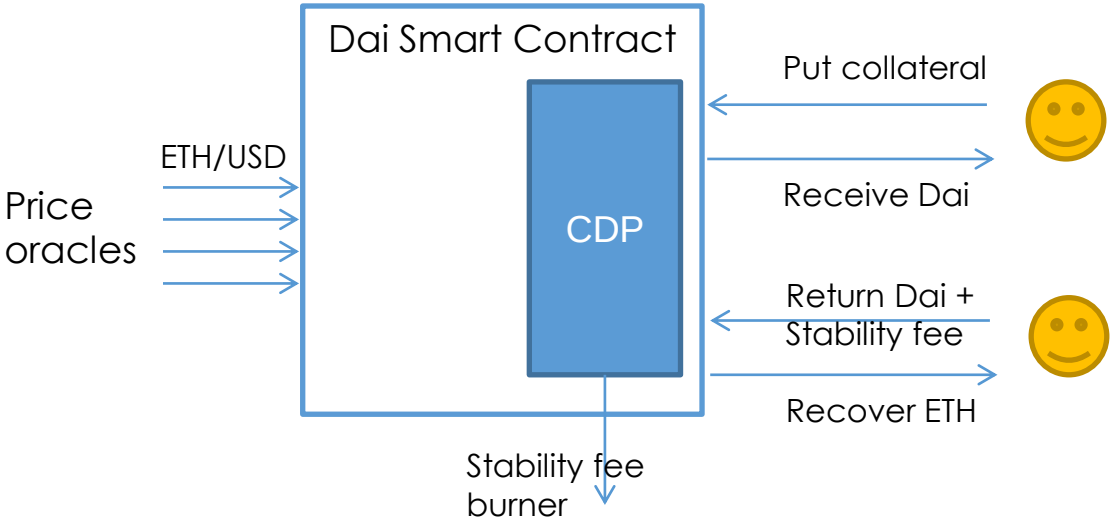
MakerDAO

- Symbol: DAI
- ERC 20
- Issuer: MakerDAO
- Launched in Dec 2017
- Collateralized with Ethers
- Stable to USD
- Coupled with MKR *"Stakercoin"*
    - Governance (voting on parameters)
    - Equity (stake)
    - Tail risk exposure
    - Lender of last resort
    - Fees paid in MKR are burnt

Decentralized collateral-backed
MakerDAO

- Dai is created by locking ETH in smart contract (called *collateralized debt position* or CDP)
- ETH → Wrapped ETH (ERC20 for ETH) → Pooled ETH (allows dilution and burning)
- Locked collateral can be recovered at any time by paying back the borrowed Dai (plus a stability fee in MKR)

- 1 Dai is created as effectively a securitized loan when at least $1.5 worth of Ether is locked (**min 150% collateral**)



1 Collateralize & generate DAI — 2 Confirm details

How much ETH would you like to collateralize?

8,47 ETH

8.141 PETH

Min. ETH required: 7.610 ETH

How much DAI would you like to generate?

600 DAI

Max DAI available to generate: 667.774 DAI

Liquidation price (ETH/USD)	106.257 USD	Collateralization ratio	166.943%
Current price information (ETH/USD)	118.260 USD	Minimum ratio	150.000%
Liquidation penalty	13.000%		

Stability fee @0.5%/year in MKR

⚠ The amount of DAI you are trying to generate against the collateral is putting your CDP at risk.

COLLATERALIZE & GENERATE DAI

MetaMask 0xfa99ab...4f3605

ASSET	BALANCE	SEND	UNLOCK
ETH USD	8.473 $1,002.13		
DAI USD	0.000 $0.00		
MKR USD	0.000 $0.00		

Main Ethereum Network

Price Info

ETH/USD	118.260 USD
PETH/ETH	1.040 ETH
DAI/USD	1.000 USD
MKR/USD	449.190 USD

Global CDP Info

Global CDP Collateralization

311.017 %

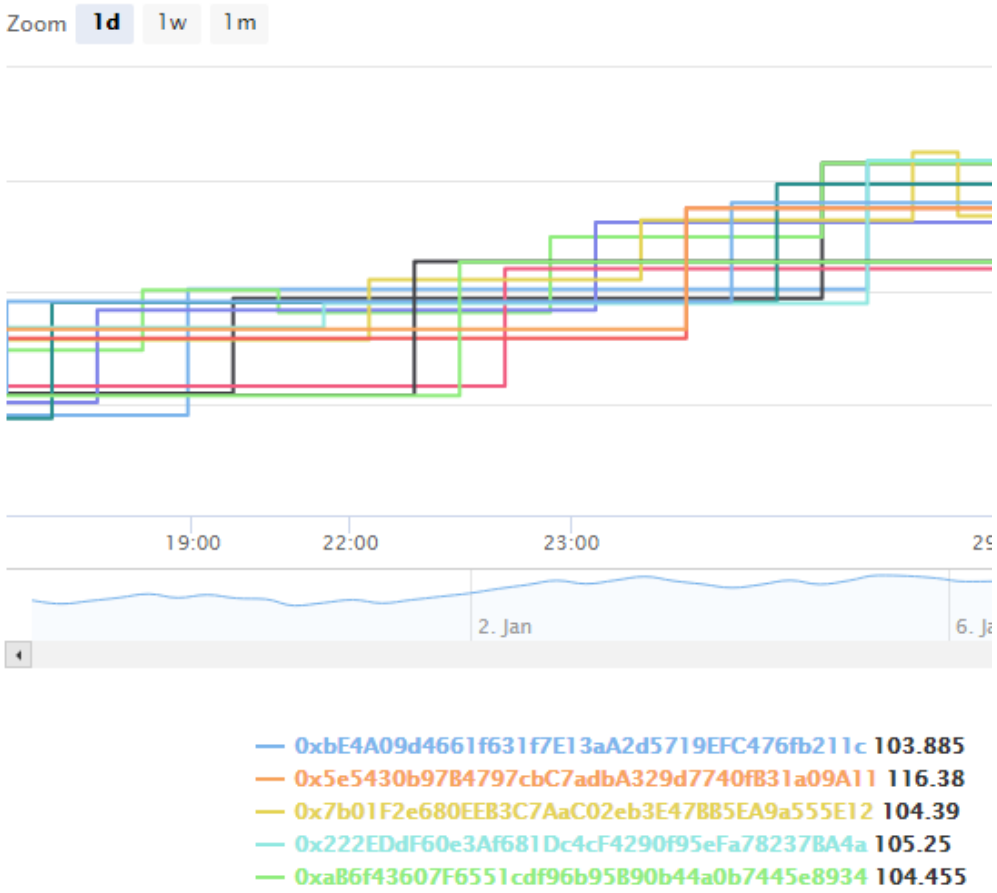
Decentralized collateral-backed MakerDAO

Lykke

Price oracles

- MKR voters choose a **set of trusted oracles** to feed this information to the Dai smart contract (currently – **14**). Oracles submit underlying asset prices to Ethereum blockchain. Median price is taken and delayed 1 hour.

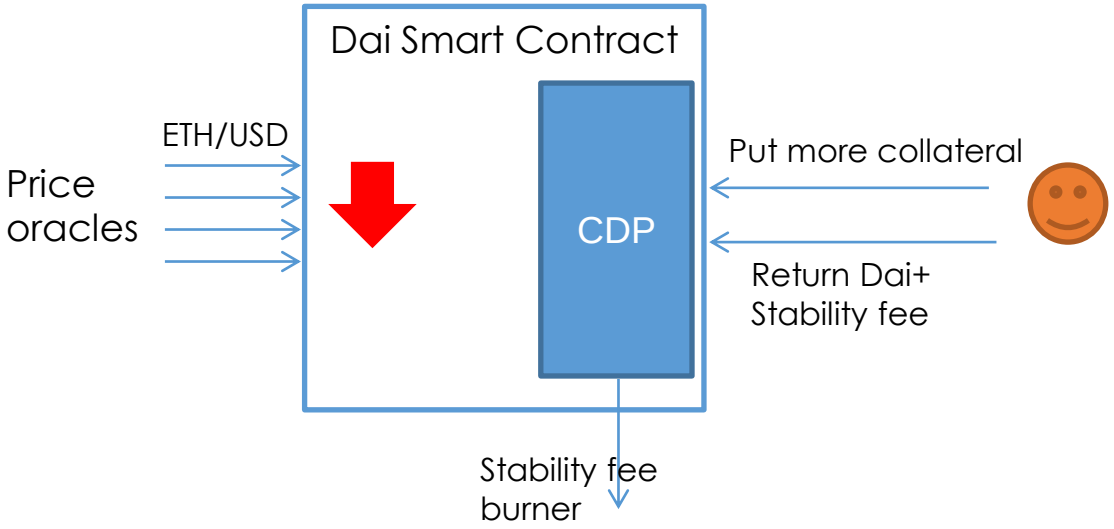
- **Price Feed Sensitivity Parameter** protects oracles from collusion and price manipulation (**"5% in 15 minutes"**). This restriction ensures there is enough time to trigger (by Emergency Oracles or even MKR holders) an **Emergency shutdown** in case of successful attack



Decentralized collateral-backed MakerDAO

CDP Adjustment

- If ETH price goes up, all is good! But, if down, CDP Collateral ratio will decrease.
- It can be adjusted by the CDP holder:
  1) paying back some DAI,
  2) depositing more ETH



Decentralized collateral-backed
MakerDAO

Lykke

CDP Portal

My collateralized debt position #13896

MOVE CDP | CLOSE CDP

Liquidation price (ETH/USD)	62.496 USD
Current price information (ETH/USD)	104.620 USD
Liquidation penalty	13.000 %
Collateralization ratio	251.100 %
Minimum ratio	150.000 %
Stability fee	0.500 %

ETH collateral

Deposited	0.840 ETH 0.807 PETH | 87.885 USD	DEPOSIT
Max. available to withdraw	0.338 ETH 0.325 PETH | 35.385 USD	WITHDRAW

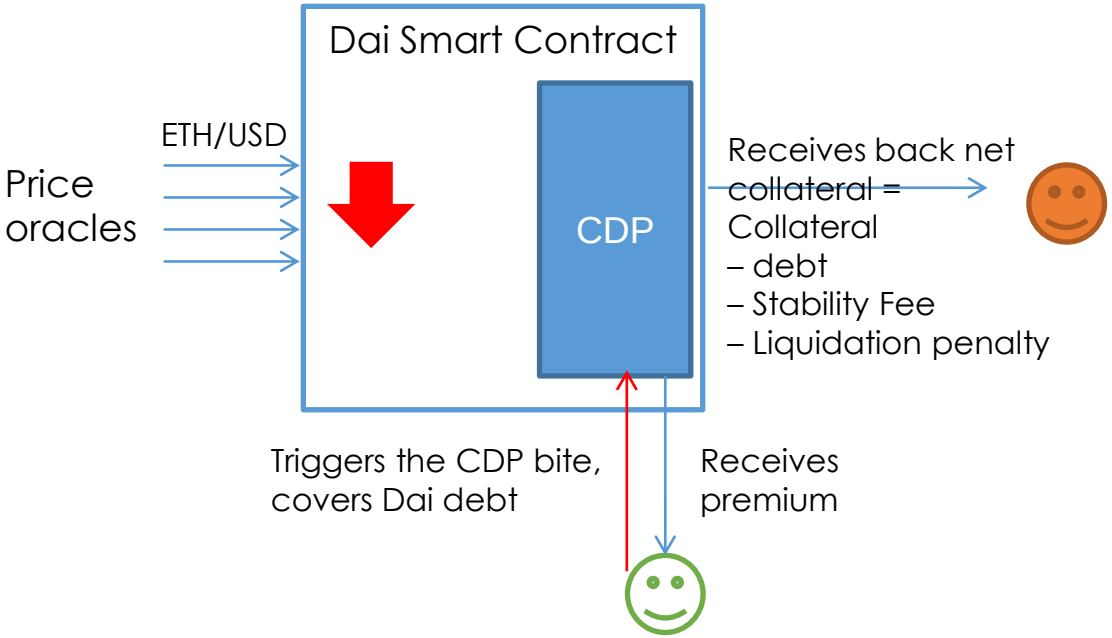
DAI position

Generated	35.000 DAI 35.000 USD	PAYBACK
Max. available to generate	23.590 DAI 23.590 USD	GENERATE

Decentralized collateral-backed MakerDAO

Liquidation

- If CDP reaches Liquidation Ratio (**150%**) the Maker forces to liquidate the collateral
- The CDP owner receives the value of the leftover collateral *minus* the debt, Stability Fee (**0.5% p.a.**) and Liquidation Penalty (**13%**)
- The PETH collateral is set for sale in the Liquidity Providing Contract, and **keepers** can atomically purchase the PETH by paying Dai

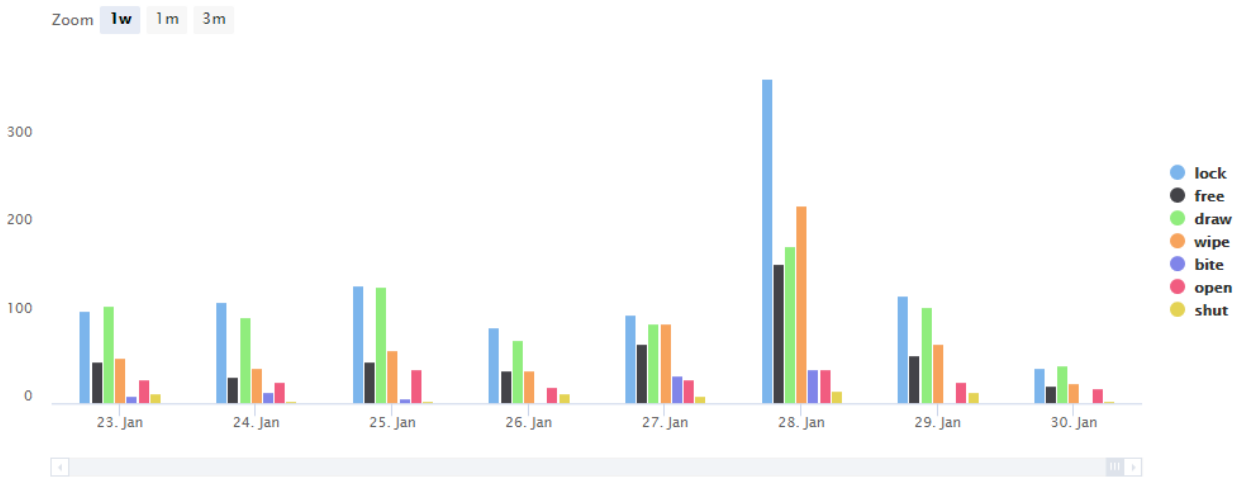


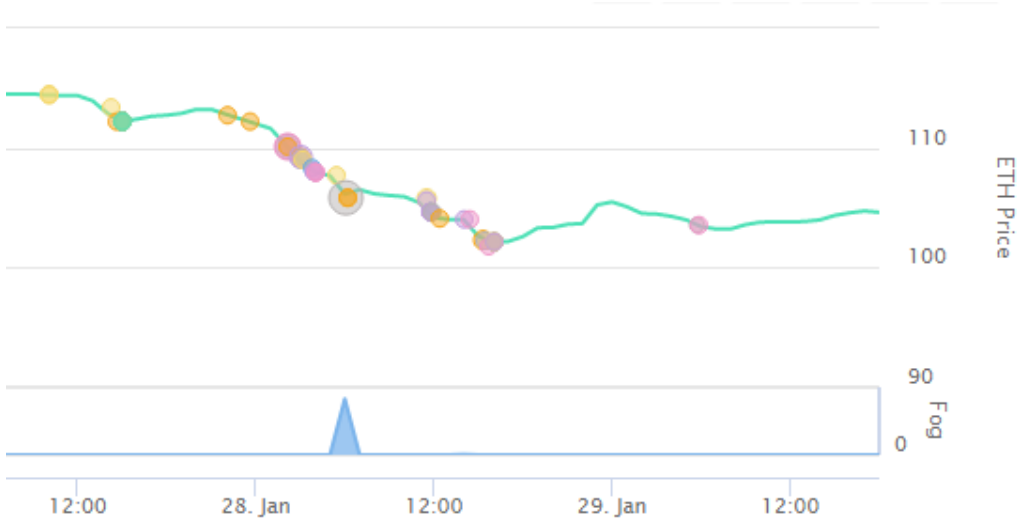
Keepers – independent agents, that explore profit opportunities: "bite" CDPs at risk, market make, explore arbitrage between exchanges

Decentralized collateral-backed
MakerDAO

Liquidation

- Liquidations are rare (~40 last week, ~$100k)
- Largest "Bite" - 54k ETH ($10 mln)





Decentralized collateral-backed MakerDAO

Lykke

Global Settlement (aka "Emergency Shutdown")

- **Global Settlers** are selected by MKR voters and have the authority to trigger global settlement (the last line of defense for the Dai Stablecoin System in the event of an attack)
- GS stops CDP creation, freezes the Price Feed at a fixed value that is then used to process proportional claims for all users (**Settlement price**)
- After GS has been activated, a period of time is needed to allow keepers to process the proportional claims of all Dai and CDP holders based on the Settlement price.
- Each Dai and CDP holder can **call a claim function** to exchange their Dai and CDPs directly for a fixed amount of ETH that corresponds to the calculated value of their assets, based on the target price of Dai. There is no time limit for when the final claim can be made.

Decentralized collateral-backed MakerDAO

Lykke

Risk Management

- **Volatility risk:** the higher the volatility of the collateral value, the less likely we are to recover the full loan in the event of default.
- **Qualitative risk:** the less stable the fundamentals of the organization, the less confident holders will be, and the more volatile the price will become.
- **Liquidity risk:** the less liquidity available in the market, the more likely the price impact will work against realizable value.
- **Exposure risk:** the higher the aggregate relative exposure to total supply, the more risk in trying to realize its value.
- **Price feed risk:** low quality feeds create low confidence in value.

Decentralized collateral-backed MakerDAO

Lykke

Risk Management parameters

- Collateral selection
- Price feed rules
- Maximum Exposure Level (*$100 mln*)
- Liquidation Ratio (*150%*)
- Stability Fee (*0.5% p.a.*)

Decentralized collateral-backed
MakerDAO

Governance

- 3 forms of voting: 1) vote where resolution is required (**Governance Vote**), 2) vote to enact that resolution into the system (**Executive Vote**), 3) polling

Keep the Stability Fee set to 0.5% GOVERNING PROPOSAL

Vote for this proposal to maintain the current state of the system with a Stability Fee of 0.5% per year

Executed on Dec 22, 2018 with 70 316,51 MKR

Vote for no change

62 448,94 MKR in support

Vote YES to the five core principles of the Maker Governance philos...

Voting for this proposal means voting YES to the five core principles of the Maker Governance philosophy as updated on Medium on August 21, 2018

Winning proposal

Approved
on Sep 15, 2018
with 47 601,40 MKR

Decentralized collateral-backed
MakerDAO

Lykke

Statistics (as of 30 Jan 2019)

- **1.9 mln** ETH locked (1.9% of supply), **$208** mln collateral value, **75m** Dai issued
- **14’084** CDPs created, **13’860** Dai holders
- **267%** Collateralization Ratio

Decentralized collateral-backed
MakerDAO

Lykke

Pros

- Decentralized governance and transparent structure
- Battle-tested in 2018
- Anybody can become an issuer of CDP (no KYC)
- Enables ETH leveraged position (up to 1.6x)
- Not e-money, not subject to AML
- Foundation for #DeFi (*Decentralized Finance*)

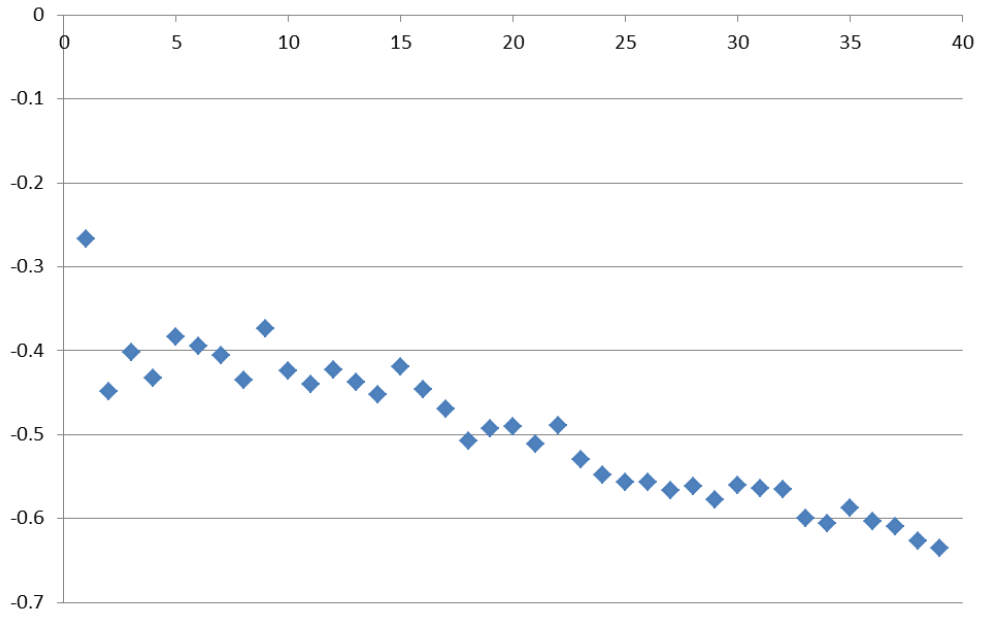
Cons

- Oracles and Global Settlers are points of failure
- "Bug" in the contract?
- Severe intraday shock of Ether can lead to the Global Settlement (like in BitUSD)

Decentralized collateral-backed
MakerDAO

- Worst N-days returns for Ether price:

  -27% in a day, **-45%** in 2 days



- BitUSD unpegged on 4 Dec 2019

Algorithmic-stable

Basis

- Issuer: Intangible Labs
- ERC20
- Raised $133m (VC backed)
- Stable cryptocurrency with algorithmic central bank

Algorithmic-stable
Basis

Lykke

Three-token system:

- *Basecoin*.

  Pegged to the USD and are intended to be used as a medium of exchange.

  Their supply is expanded and contracted in order to maintain the peg.

- *Base Bonds*.

  Auctioned off by the blockchain when it needs to contract Basecoin supply.

  Each bond promises 1 Basecoin at some point in the future under certain conditions.

  Newly-issued bonds are sold on open auction for prices of less than 1 Basecoin (yield curve).

- *Base Shares*.

  Shares supply is fixed at the genesis of the blockchain.

  Their value stems from their dividend policy.

  When demand for Basecoin goes up and the blockchain creates new Basecoin to match demand, shareholders receive these newly-created Basecoins pro rata after all outstanding Base Bonds have been redeemed.

Algorithmic-stable
Basis

Lykke

Expansion:

- Basecoin **>$1**
- Blockchain orders outstanding Base Bonds according to when they were issued, with the oldest first (*Bond Queue*) as well as outstanding Base Shares.
- Blockchain creates N new Basecoin tokens and distributes them as follows:

  1) Bondholders are paid first, and in first-in-first-out (FIFO) order. Blockchain converts bonds into coins, one-for-one, according to their order in the Bond Queue.

  2) Shareholders are paid after bondholders. If there are no more outstanding Base Bonds, the system issues any remaining new coins to shareholders, pro rata, as a dividend.

Algorithmic-stable
Basis

Lykke

Contraction:

- Basecoin < **$1**
- Blockchain tries to lock up existing Basecoins in exchange for future payoff
- Blockchain runs a Dutch auction in which bidders specify a bid and bid size for Base bonds
- Then it chooses the orders with the highest bids and converts the holders' coins into bonds until sufficient Basis has been destroyed
- Price floor is **0.10** Basis per bond
- Bond buyers will have to wait until the the price is back >$1 to receive Basecoins, but no longer than 5 years (when both bonds defaults)

Algorithmic-stable
Basis

Lykke

Pros

- Interesting approach to solve the cryptocurrency deterministic supply problem

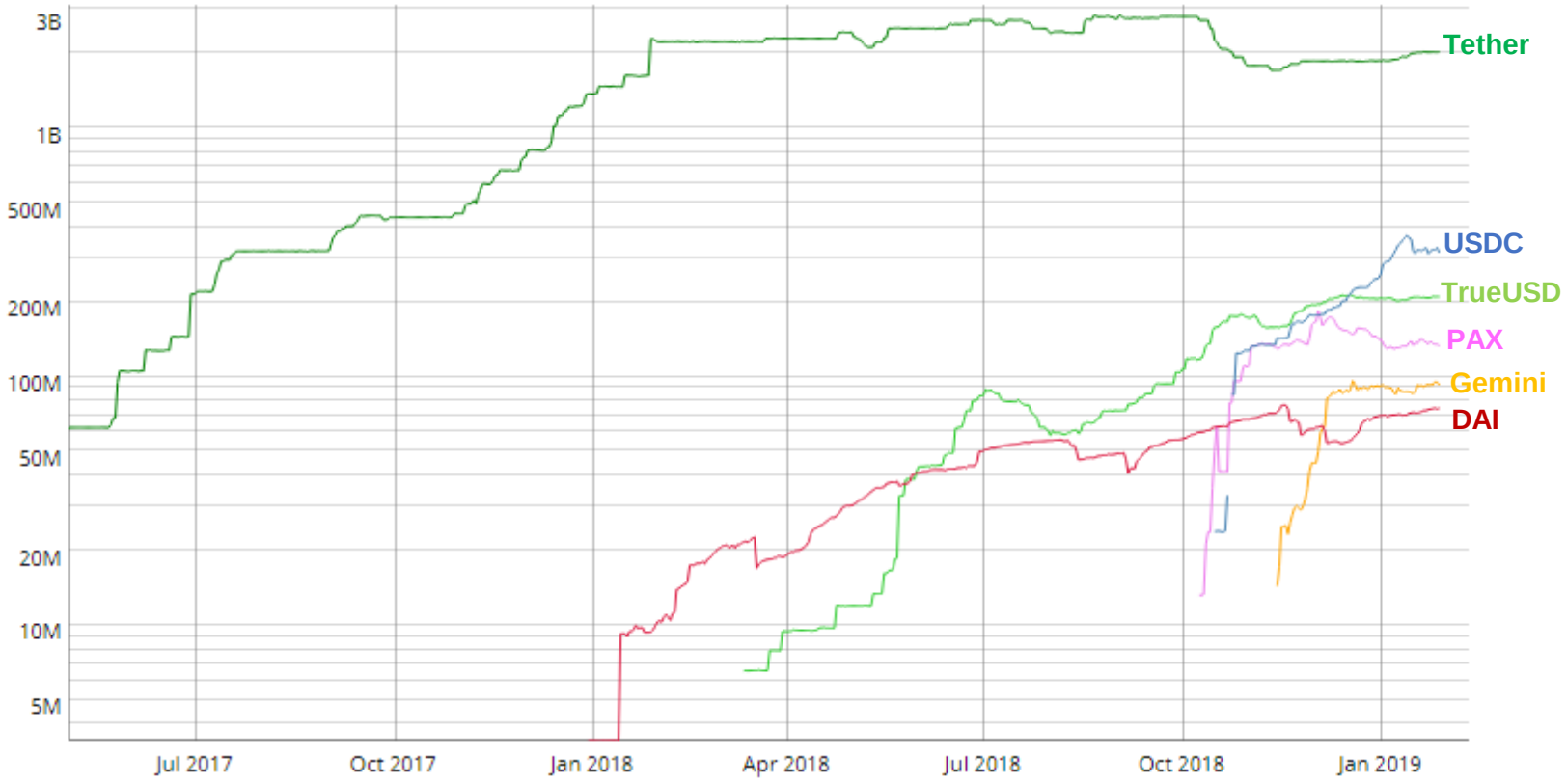
Cons

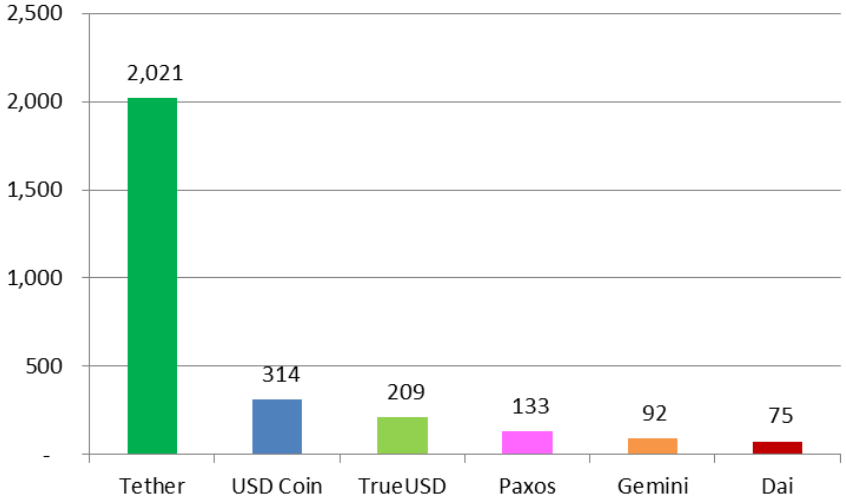
- Bonds, Shares tokens are qualified as securities
- Requires trust in the stablecoin mechanisms
- Not stable when trust is lost

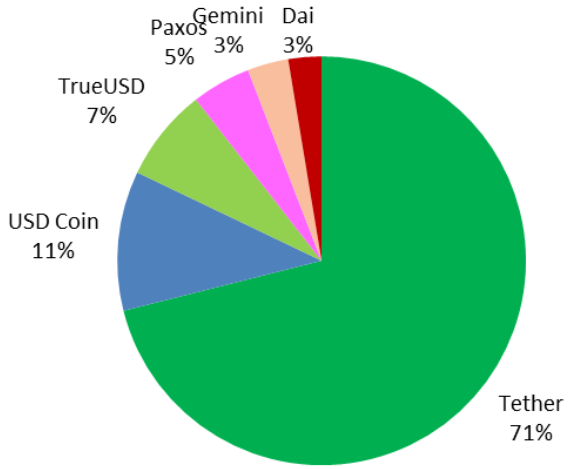
Stablecoins

Circulating supply, mln tokens

Token circulating supply (Source: Coinmarketcap, Coinmetrics)





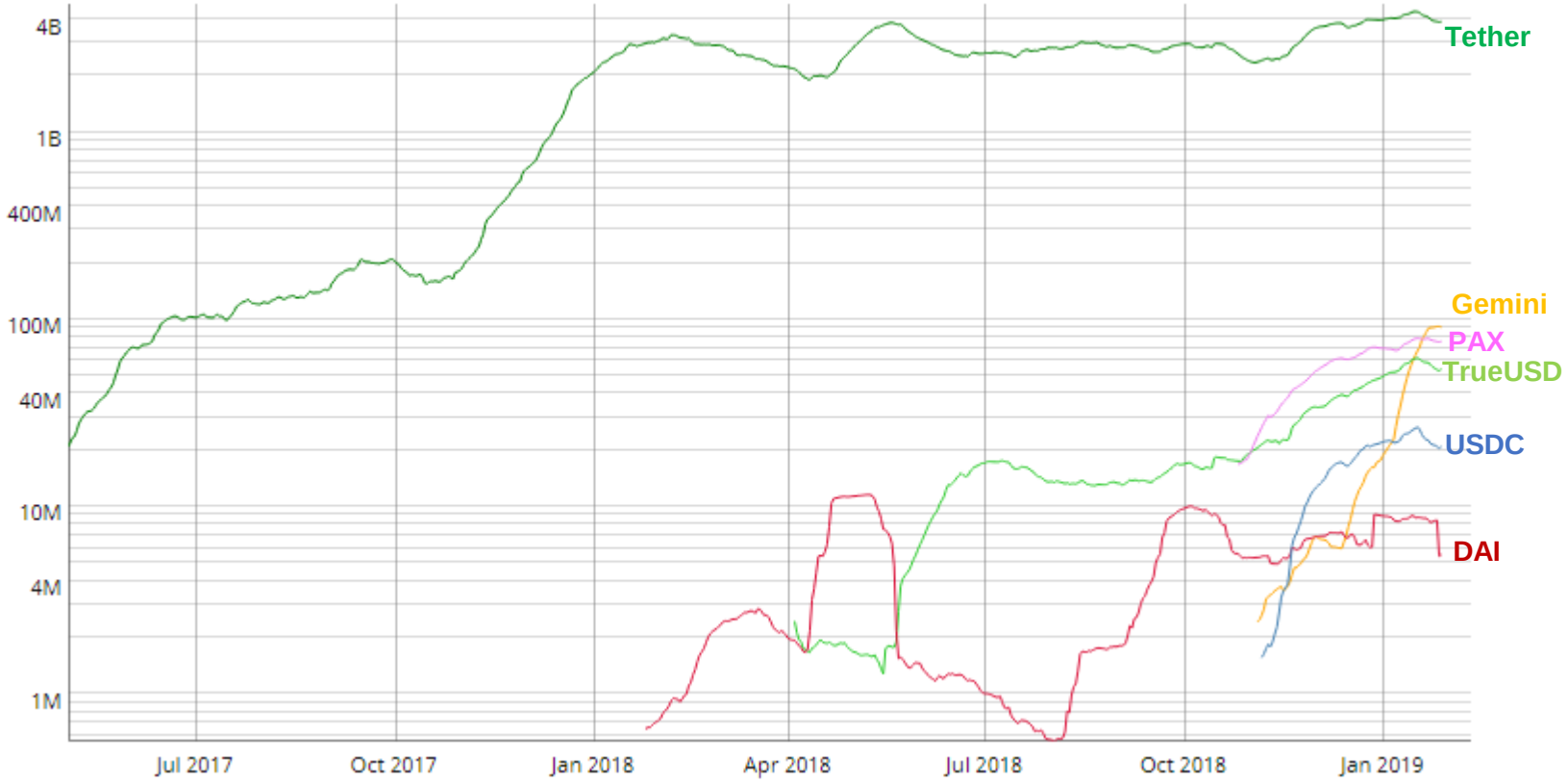


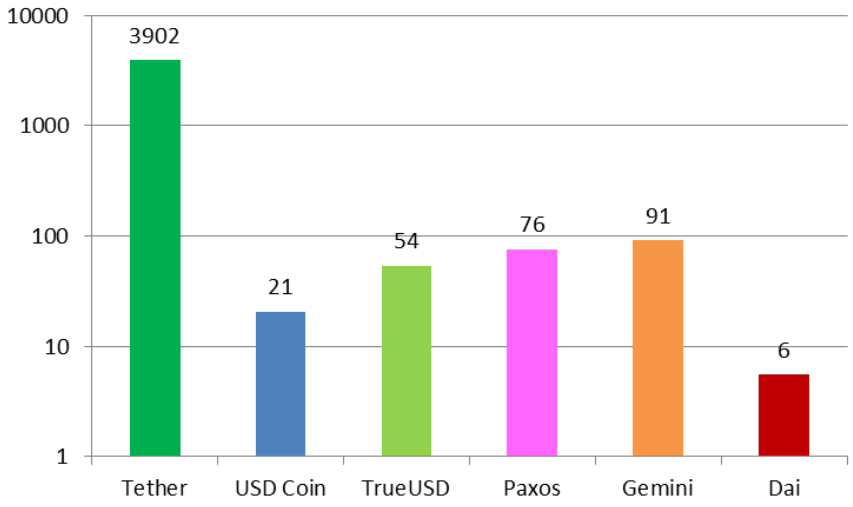
USD Tether share has decreased to 70%, but it's still the King

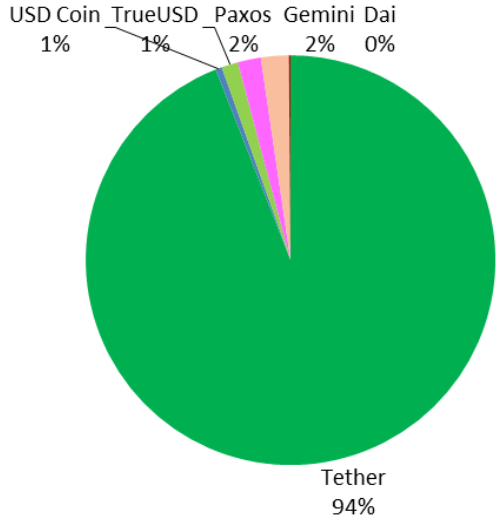
Stablecoins

Trading volume, mln $

30-d average daily trading volume (Source: Coinmetrics)





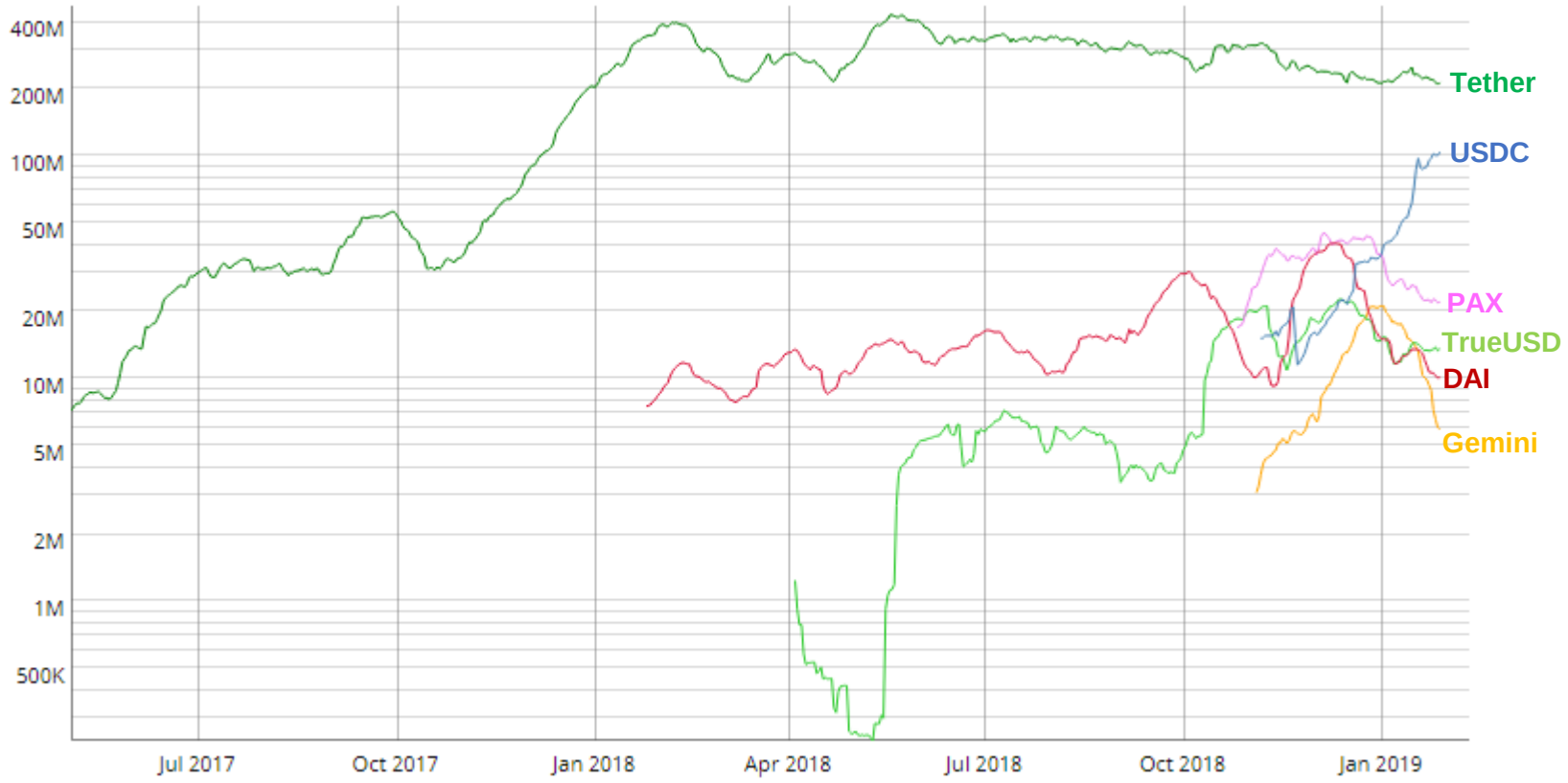


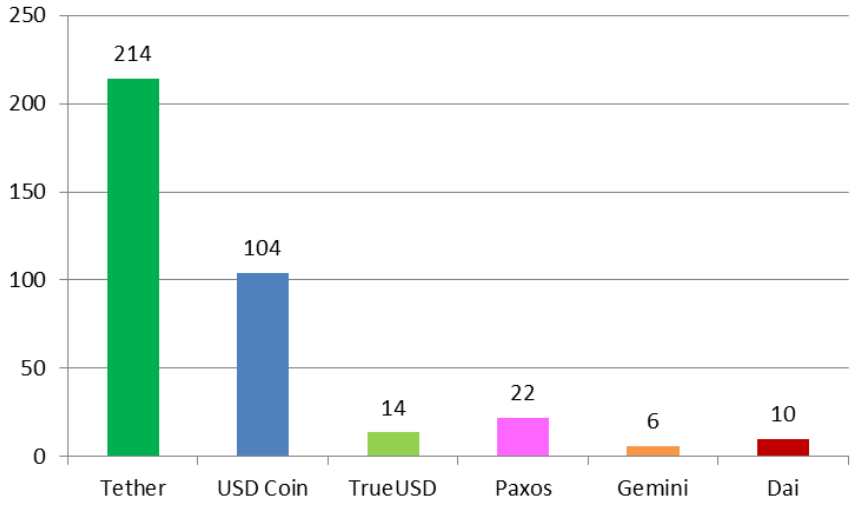
USD Tether is still the currency of choice for crypto-crypto trading

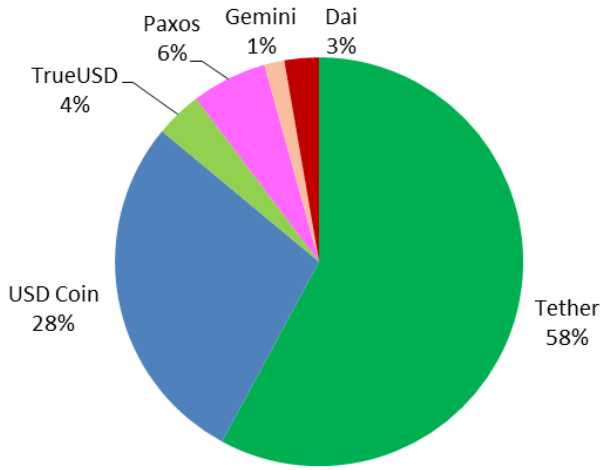
Stablecoins

Transaction volume, mln $

30-d average daily transaction volume (Source: Coinmetrics)



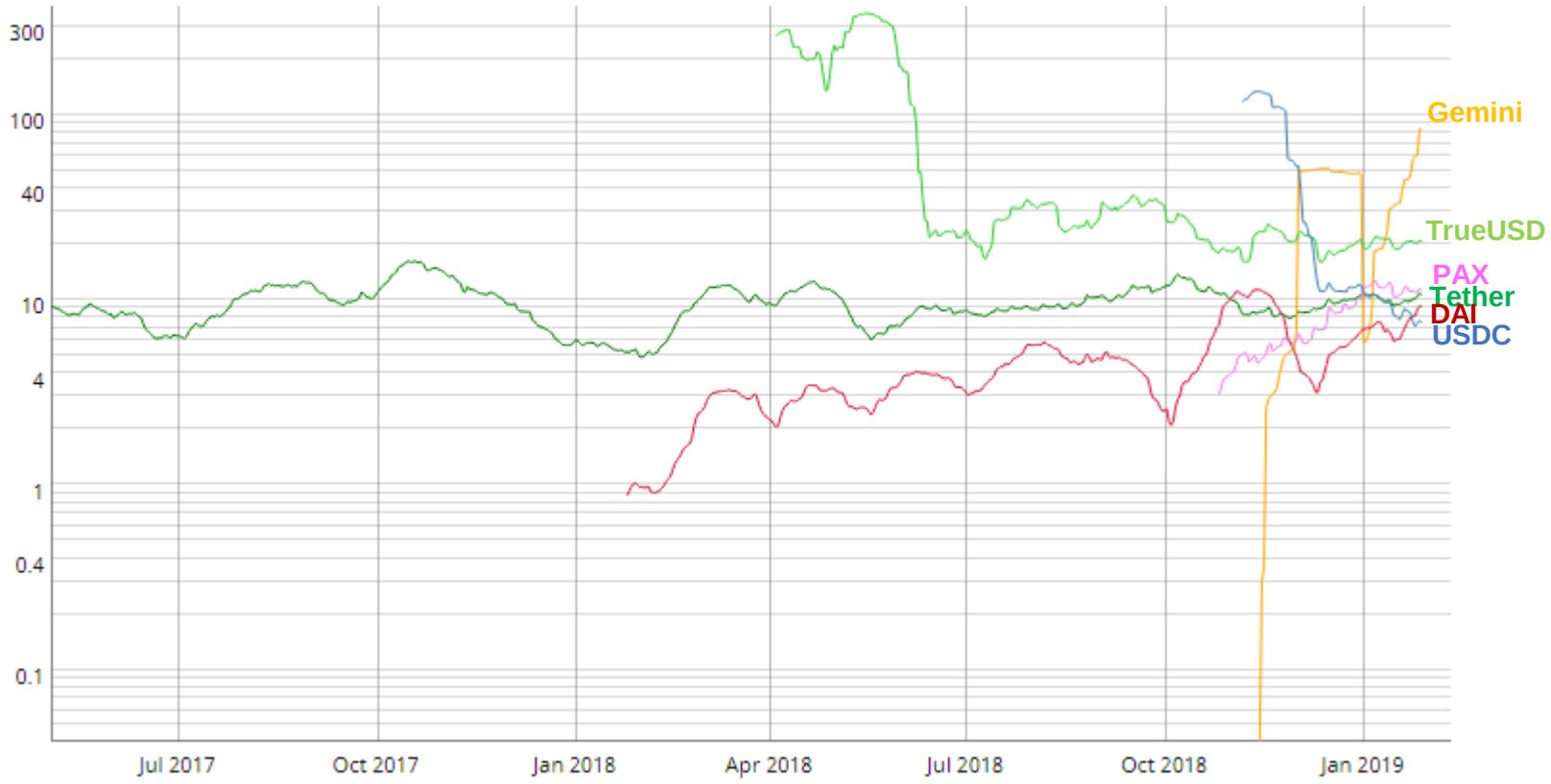




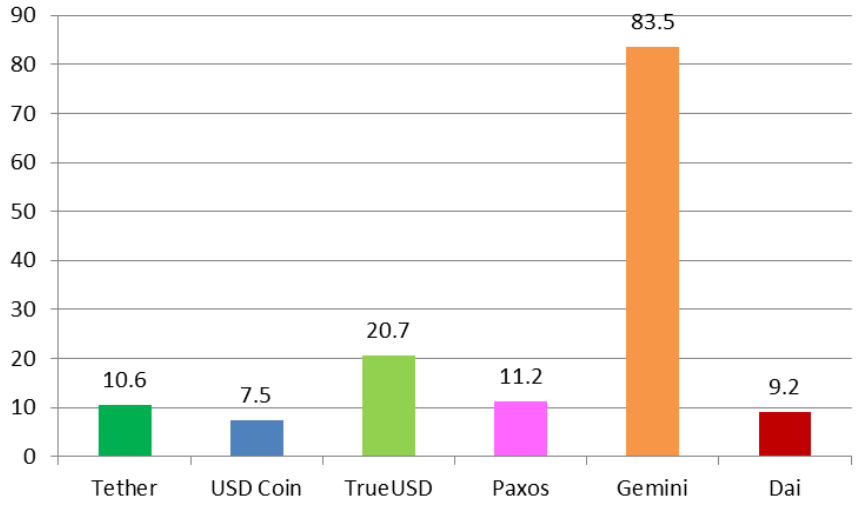
USD Coin is getting close to USD Tether in $ transaction volume

Stablecoins
NVT ratio

Network value to transactions ratio (Source: Coinmetrics)



NVT = network value / the dollar value of cryptoasset transaction activity

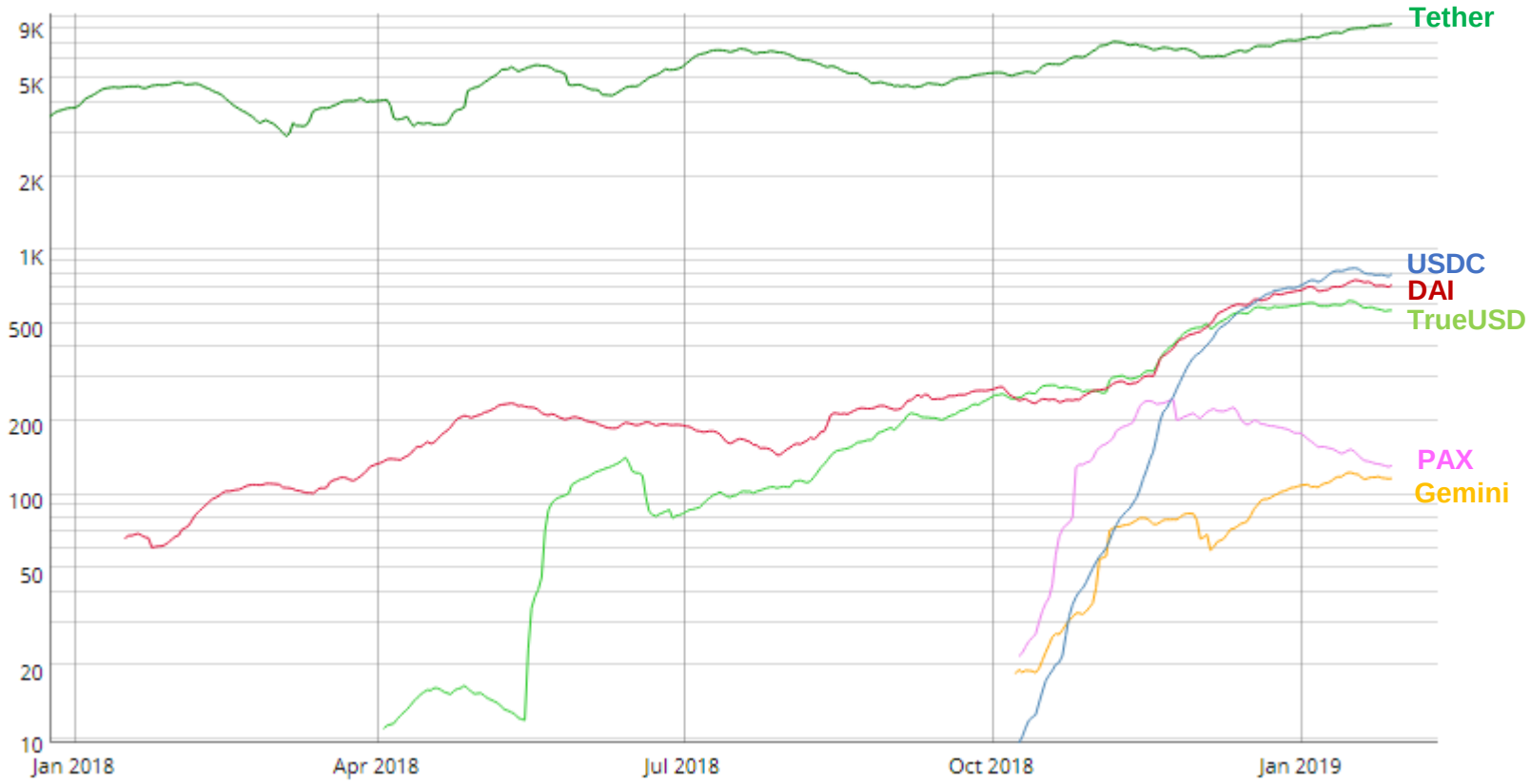


Gemini and TrueUSD are out of normal NVT range

Stablecoins

Active addresses

30-d average of daily active addresses (Source: Coinmetrics)

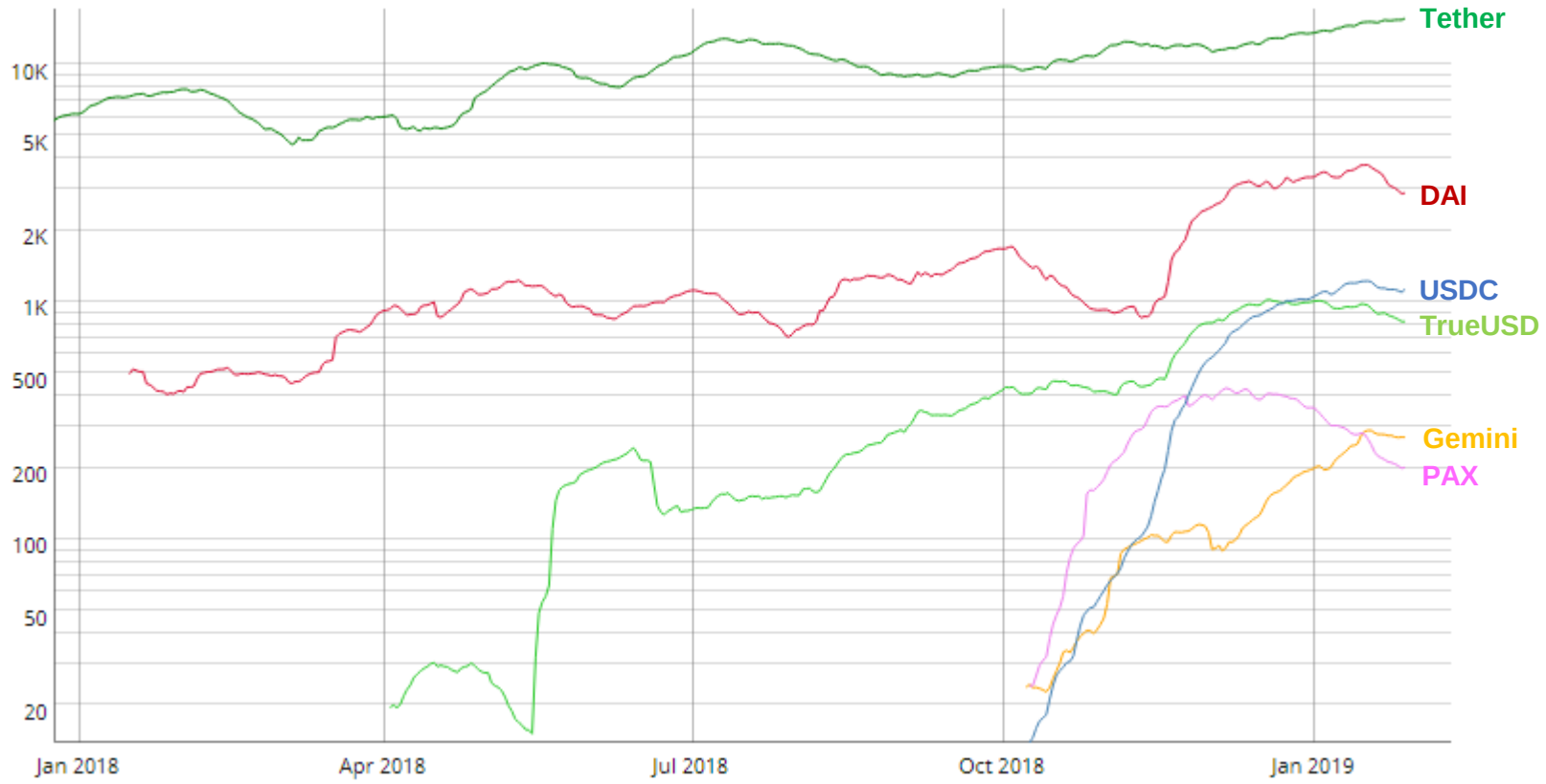


PAX and Gemini are used only at small circle

Stablecoins

Transaction count

30-d average of daily # of transactions (Source: Coinmetrics)

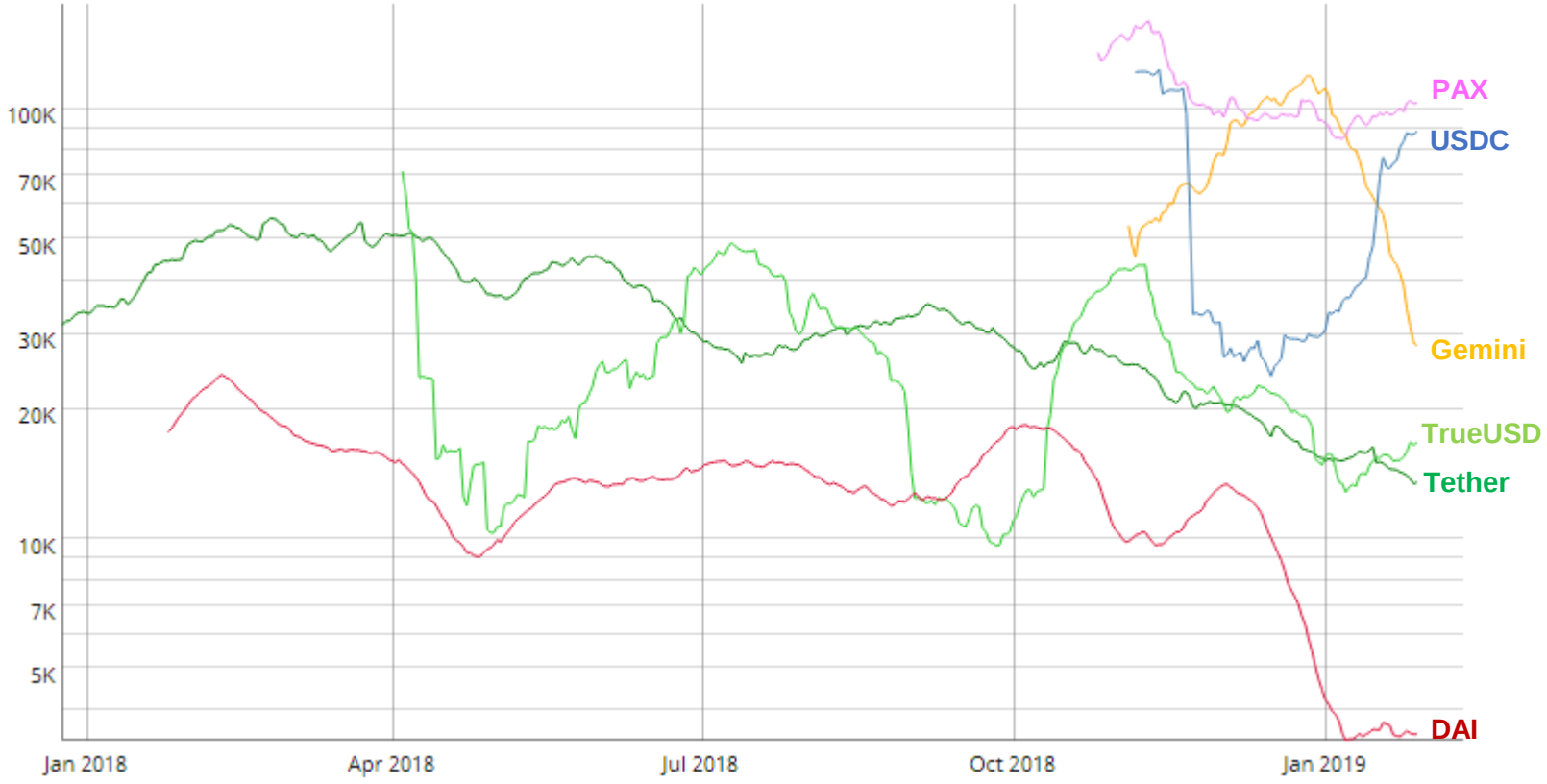


DAI is challenging Tether

Stablecoins

Average transaction, $

30-d average of average transaction value (Source: Coinmetrics)

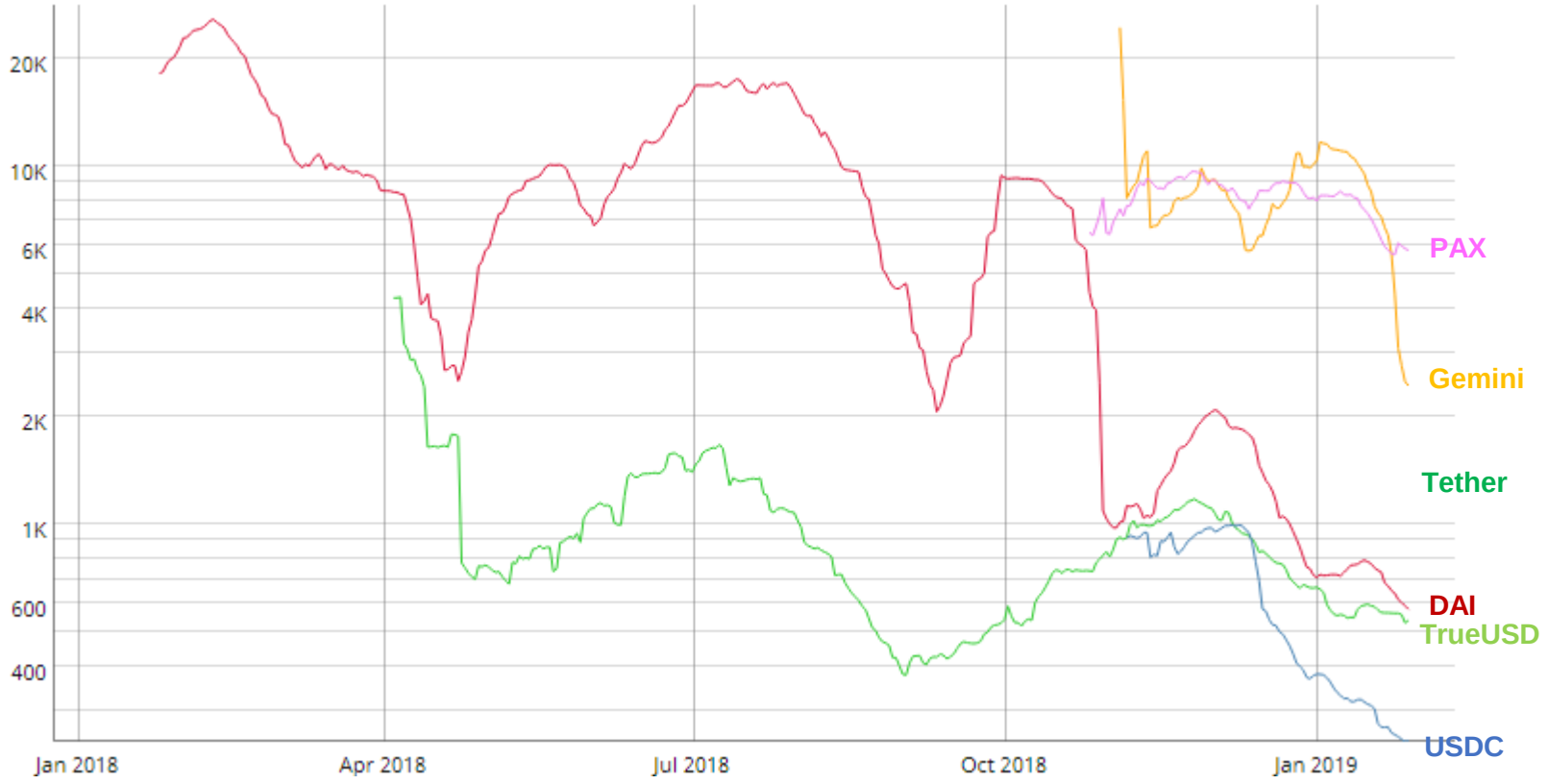


USDC have on of the highest mean tx value (~$100k)

Stablecoins

Median transaction, $

30-d average of average transaction value (Source: Coinmetrics)

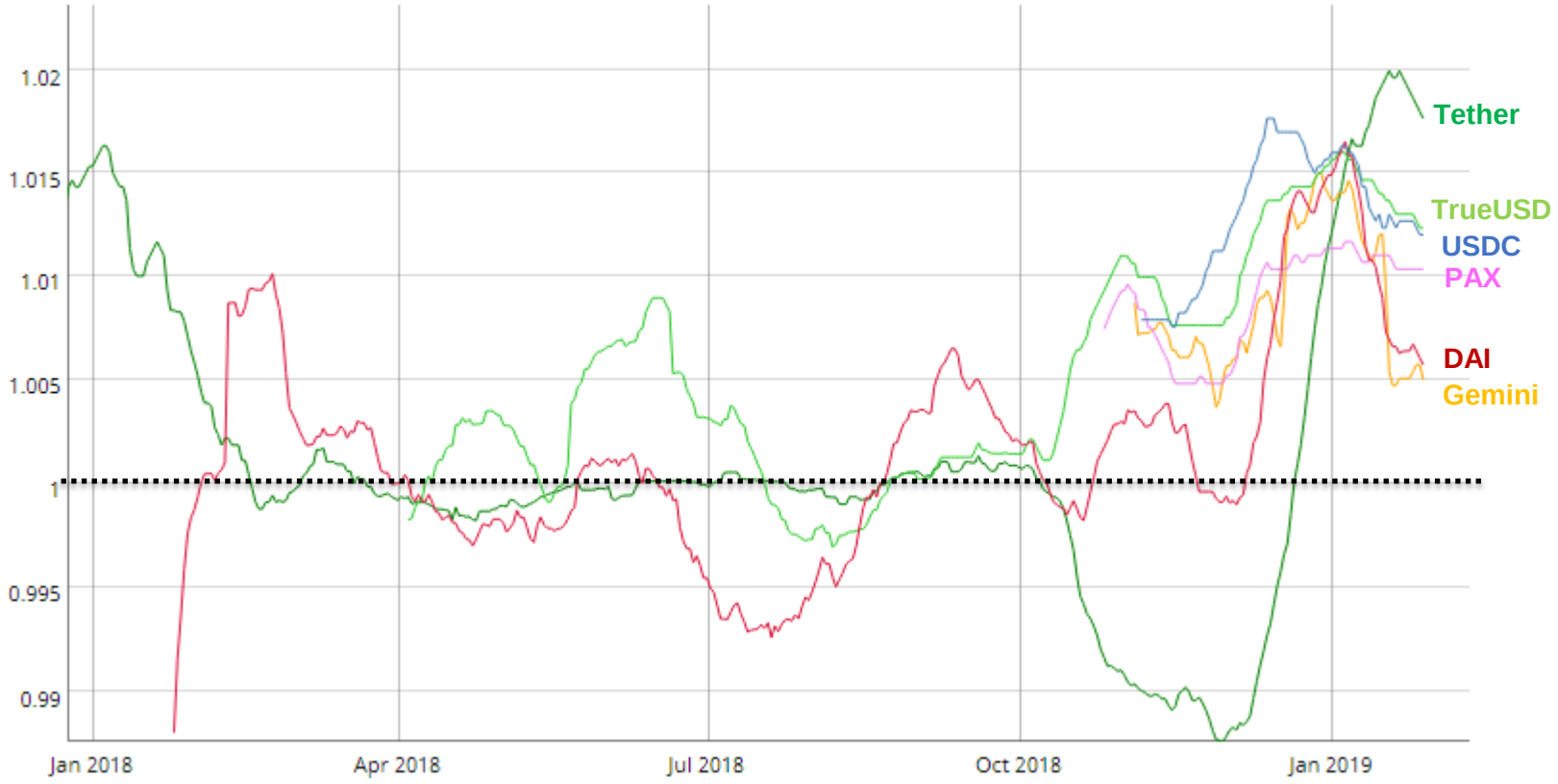


…at the same time the smallest median (~$200)

Stablecoins

Price deviation, $

30-d average of the market price (Source: Coinmetrics)

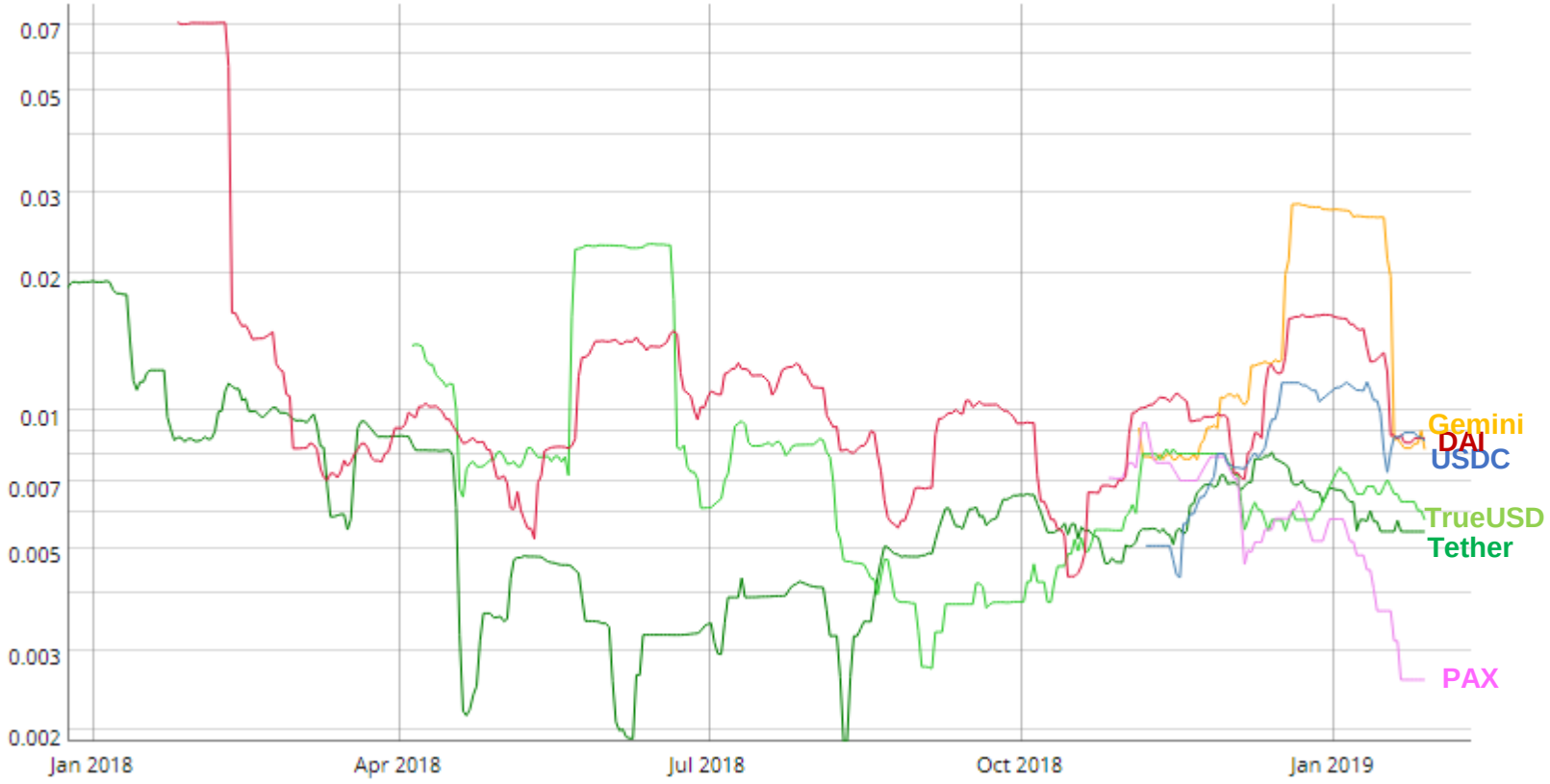


<$1 signals of the increased risk of black swan event, >$1 is typical for the bear market

Stablecoins

Price volatility

30-d standard deviation of daily price returns (Source: Coinmetrics)



Normally less than 1%

Stablecoins
Summary

- Price stability is almost there
- Use cases: transfer between exchanges/wallets, base for price discovery, *#DeFi*
- Transparent structure and governance (*not for Tether*)
- Scalability (~similar to underlying blockchans, *xDai*)
- Privacy (~similar to underlying blockchans, *Aztec+xDAI*)
- Censorship resistance (*not for US-issued stablecoins*)

….BUT…

- Blackswans happen

Stablecoins
Summary

Avenues to explore:

- Stablecoins Basket with Rainy Day Fund (see Ariah Klages-Mundt proposal https://streams.lykke.com/Project/ProjectDetails/lykke-research-hub-call-for-proposals)
- Stablecoins CDO (see Vitalik Buterin proposal https://ethresear.ch/t/collateralized-debt-obligations-for-issuer-backed-tokens/525)
- Coupling with underlying value (e.g. internet traffic)