Russia Risk Conference

Digital Assets Ecosystem Overview

Sergey Ivliev

Cryptoeconomics and blockchain systems lab, Perm State University

19/11/2020


Russia Risk
Conference

Inefficiencies

2.2 bln people lack access to modern financial system

$14 global average cost of sending $200

27 years average life time of a fiat currency

$19 trln outstanding debt at negative interest rates

92% millennials don't trust financial institutions

Response

```
00000000   01 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD   7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3   88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49   FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00   00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF   FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54   69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39   20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62   72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62   61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73   FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04   67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10   5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6   49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE   5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F   AC 00 00 00 00            ŠLp+kñ._¬....
```

Bitcoin: A Peer-to-Peer Electronic Cash System

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

THE TIMES

Saturday January 3 2009 timesonline.co.uk No 69523

£1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Start collecting tokens today Pullout inside

Israel prepares to send tanks and troops into Gaza

Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes News, page 3

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

99p

Pub chain cuts the price of a pint from £1.69 to 1989 levels

Business, page 47

Continued on page 6, col 1

Leading article, page 2

Michael Sheen
Frost, Nixon and me

Magazine

Working mums
So that's how she does it

Body&Soul

Detox in style
The best spas on the planet

Travel

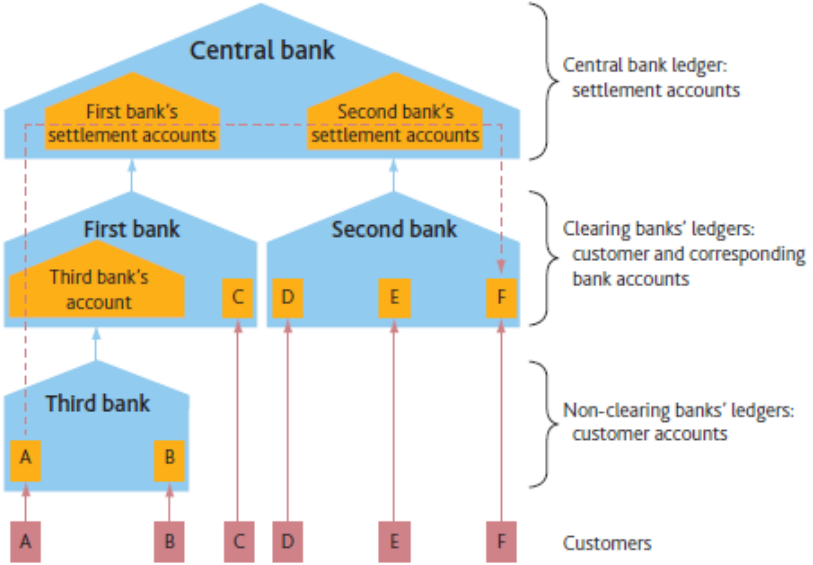
Salman Rushdie
I won't marry again

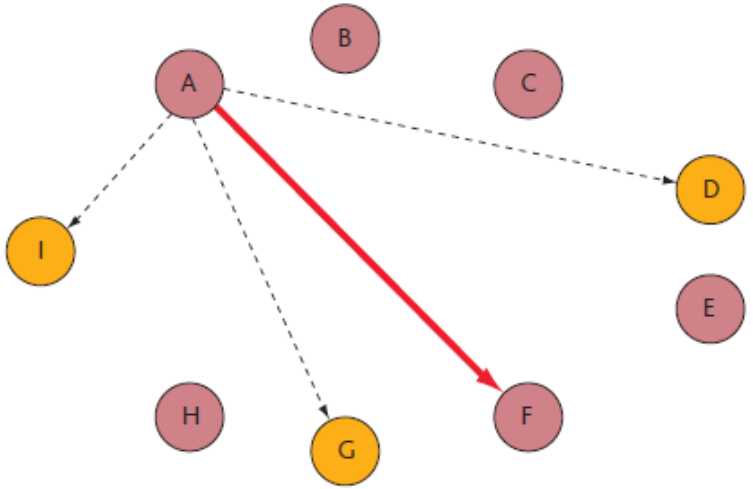
Pages 22, 23

Giant killing?
Guide to the FA Cup third round

Sport

Centralized vs. Decentralized





Centralized system

- Trusted third party
- Censorship power
- Hard to access globally

Decentralized system

- No single point of failure
- Censorship-resistant
- Global instant access

Decentralization

On average, 8-10 thousand full nodes are active daily

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Sat Sep 08 2018 19:51:29 GMT+0000 (Среднее время по Гринвичу).

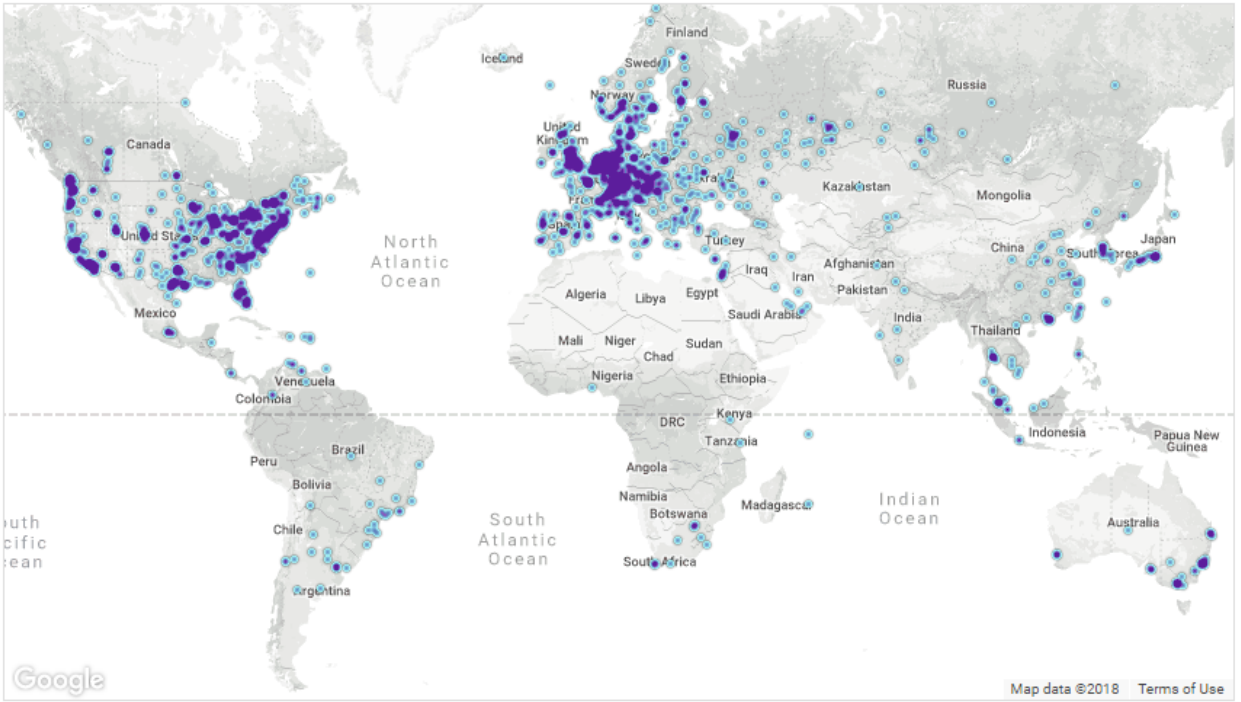
9740 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2330 (23.92%)
2	Germany	1804 (18.52%)
3	France	670 (6.88%)
4	China	657 (6.75%)
5	Netherlands	488 (5.01%)
6	n/a	450 (4.62%)
7	Canada	364 (3.74%)
8	United Kingdom	285 (2.93%)
9	Russian Federation	275 (2.82%)
10	Singapore	242 (2.48%)

More (99) »

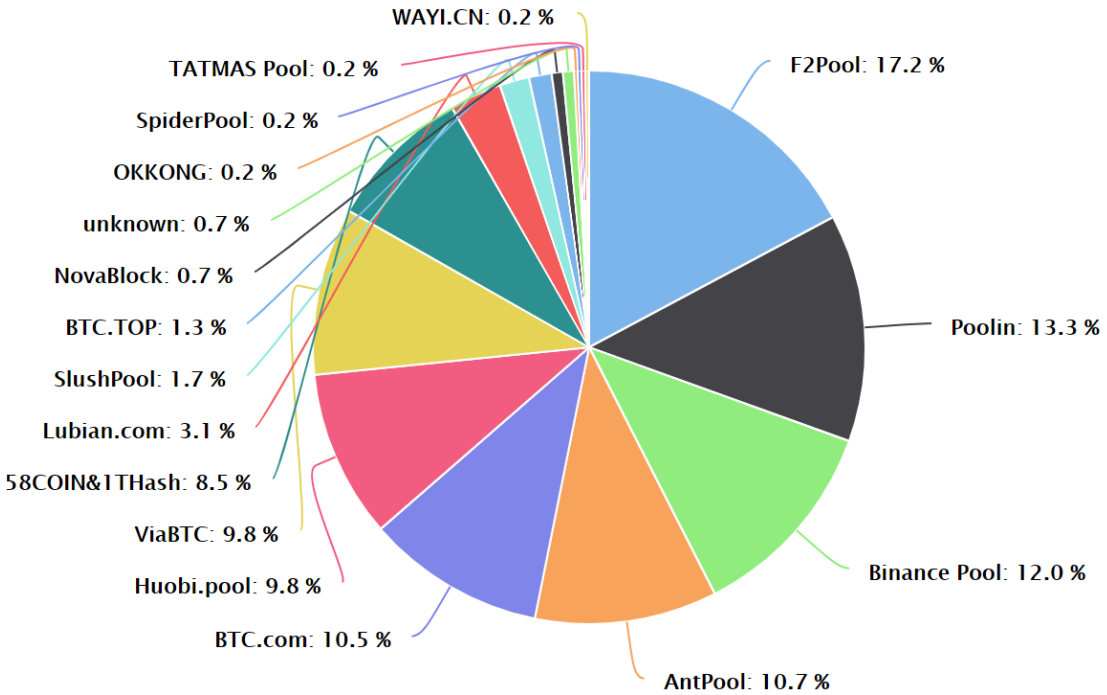


Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

Mining

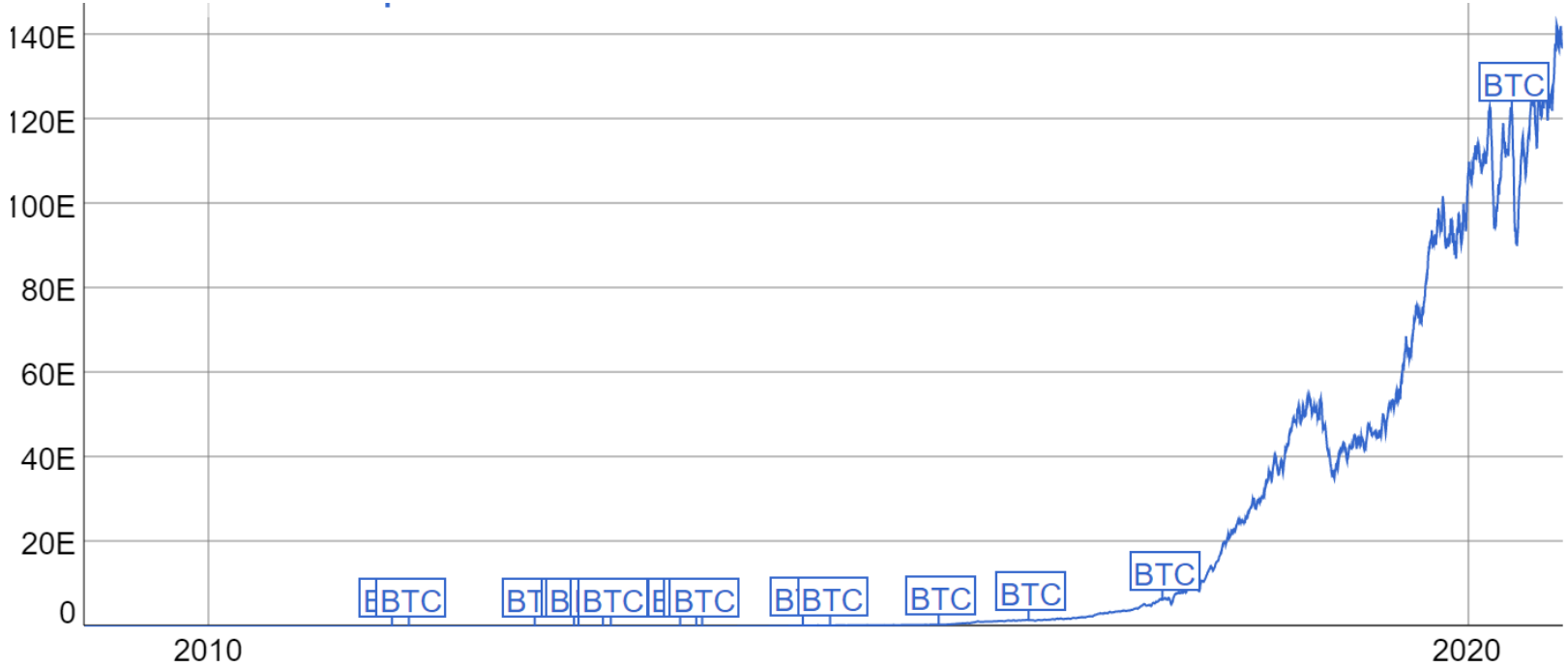
Consolidation of miners into pools



https://btc.com/stats/pool

Mining

Hashrate 140 EH/s = $140 \cdot 10^{18}$



https://bitinfocharts.com/ru/comparison/hashrate-btc-sma7.html

Mining

The hashrate ~140 million TH/s. Power consumption ~6.6 GWh

Energy cost 6.6 GW * $0.05/KWh = $330k /hour ($2.8b /yr)

Equipment replacement cost 1.2 mln S19 * $3000 = $3.6b

Mining award for 6 blocks * 6.25 BTC = 37.5 BTC / hour

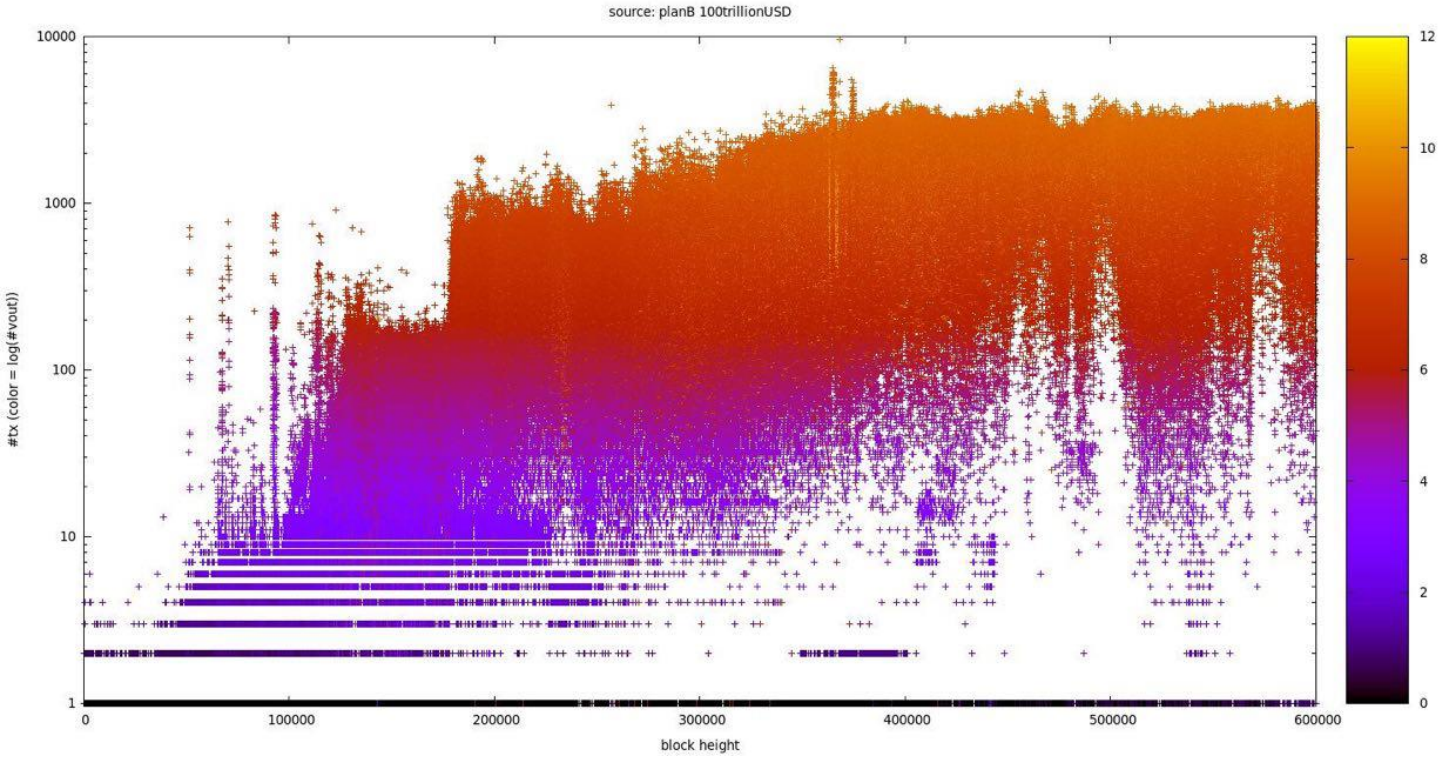
Transaction fee for 6 blocks * 1400 tx * 0.0001 BTC = 1 BTC / hour

Revenue of miners of 38.5 BTC * $17.5k ~ $673k / hour ($6b /yr)

https://www.cbeci.org/

Uptime

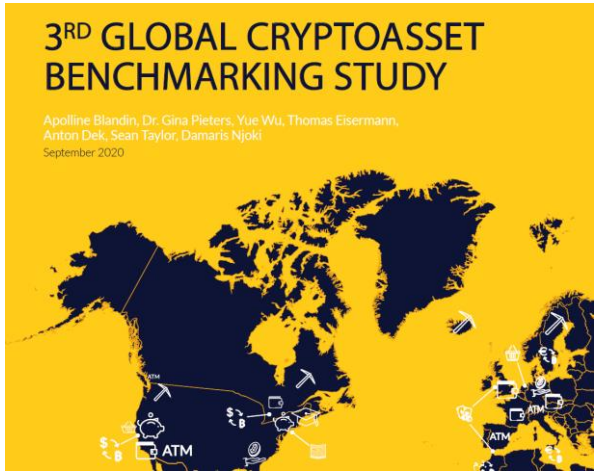
14 hours total downtime, 99.9986% uptime



Adoption

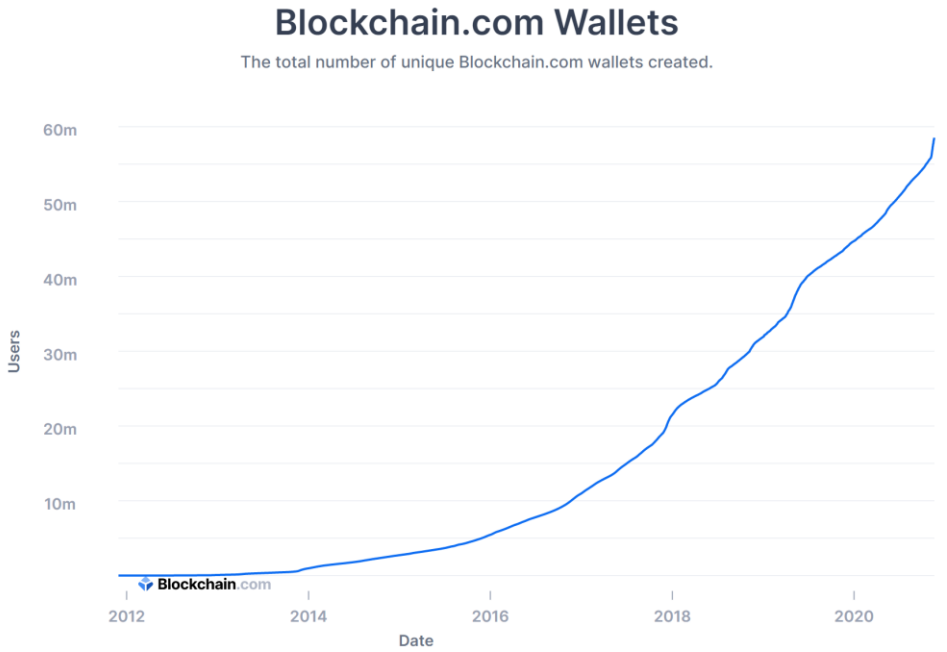
191 mln total accounts

101 mln ID-verified users



https://www.jbs.cam.ac.uk/wp-content/uploads/2020/09/2020-ccaf-3rd-global-cryptoasset-benchmarking-study.pdf

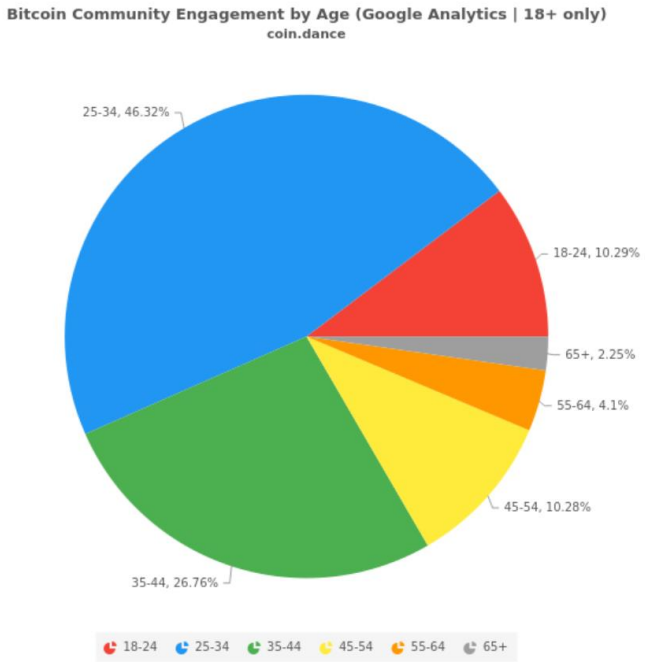
58 mln Blockchain.com wallets



https://www.blockchain.com/charts/my-wallet-n-users

Adoption

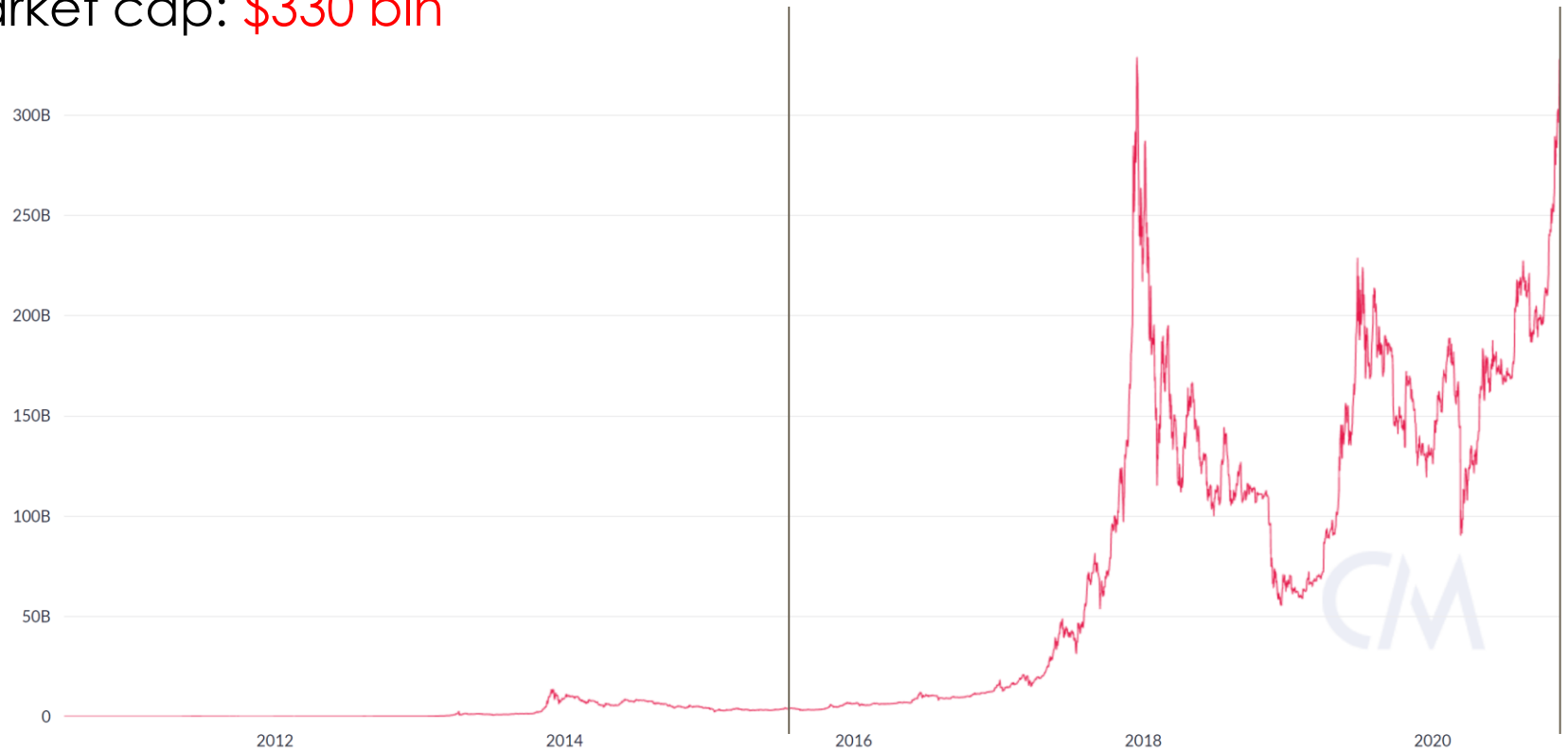
New generation money (57% under 34)



https://coin.dance/stats

Store of value

Market cap: $330 bln

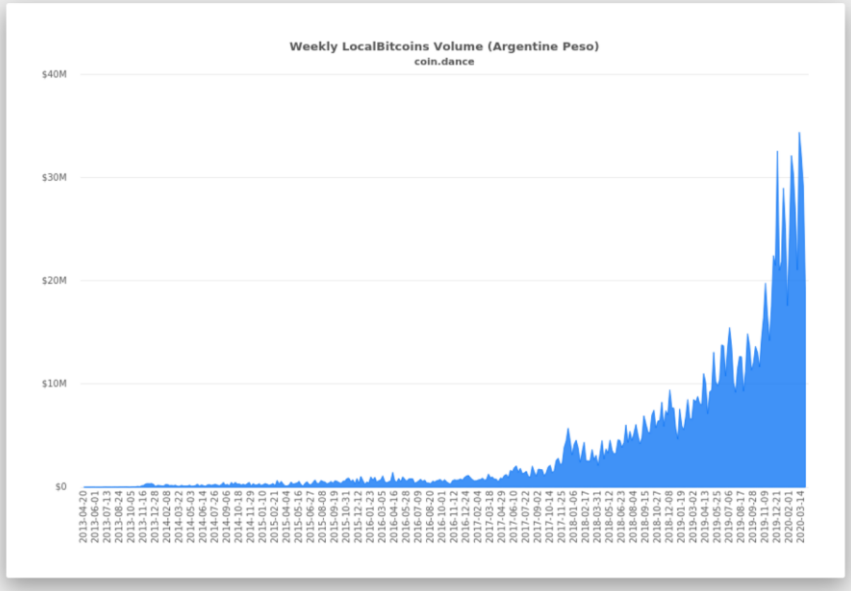


https://network-charts.coinmetrics.io/

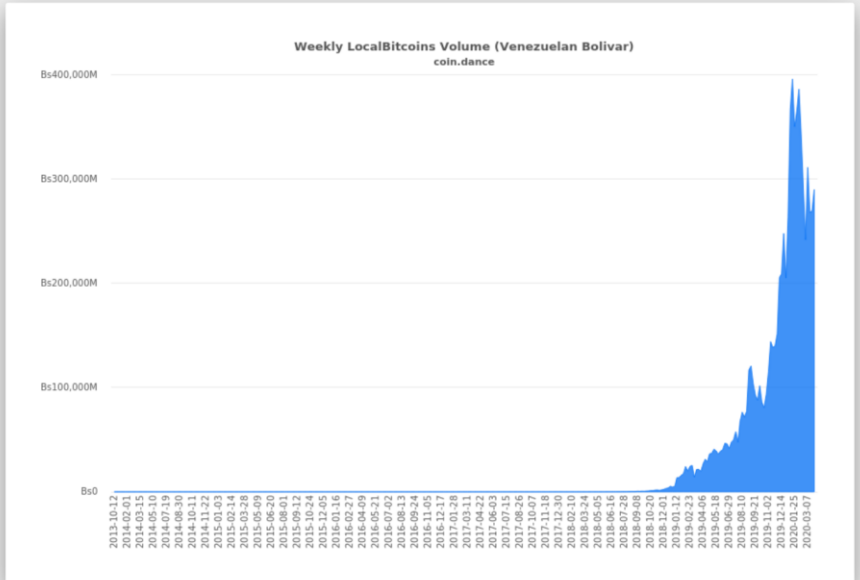
Store of value

Escape from the devaluation of the national currency

Argentina



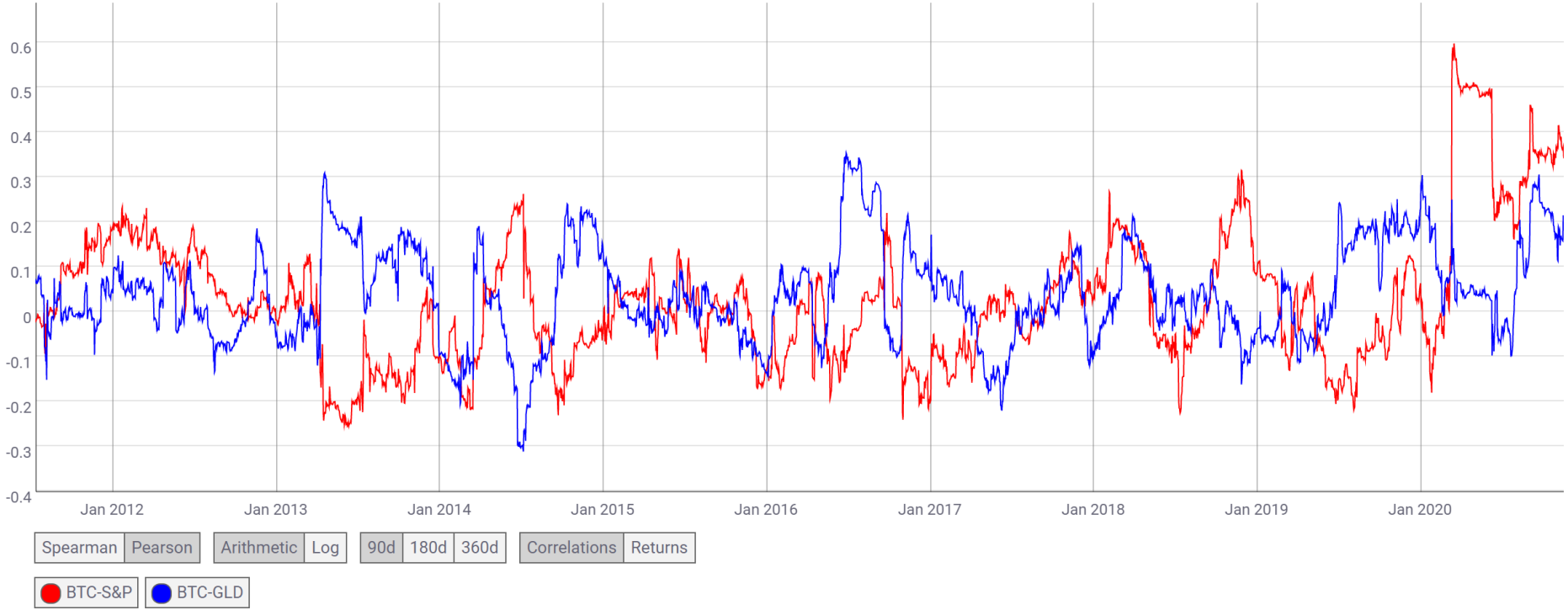
Venezuela



https://coin.dance/volume/localbitcoins

Diversification

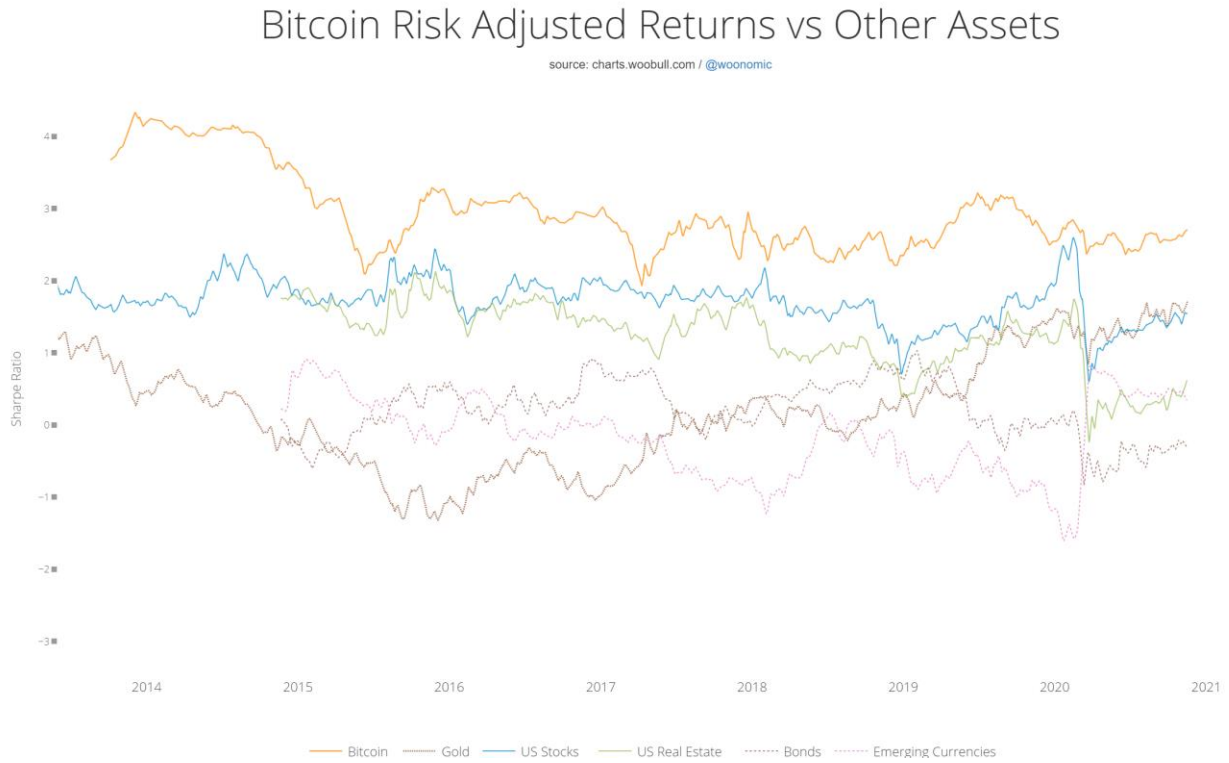
Non-correlated asset class



https://coinmetrics.io/correlation-charts/#assets=btc-s&p,btc-gld_period=90_spearman=false

Performance

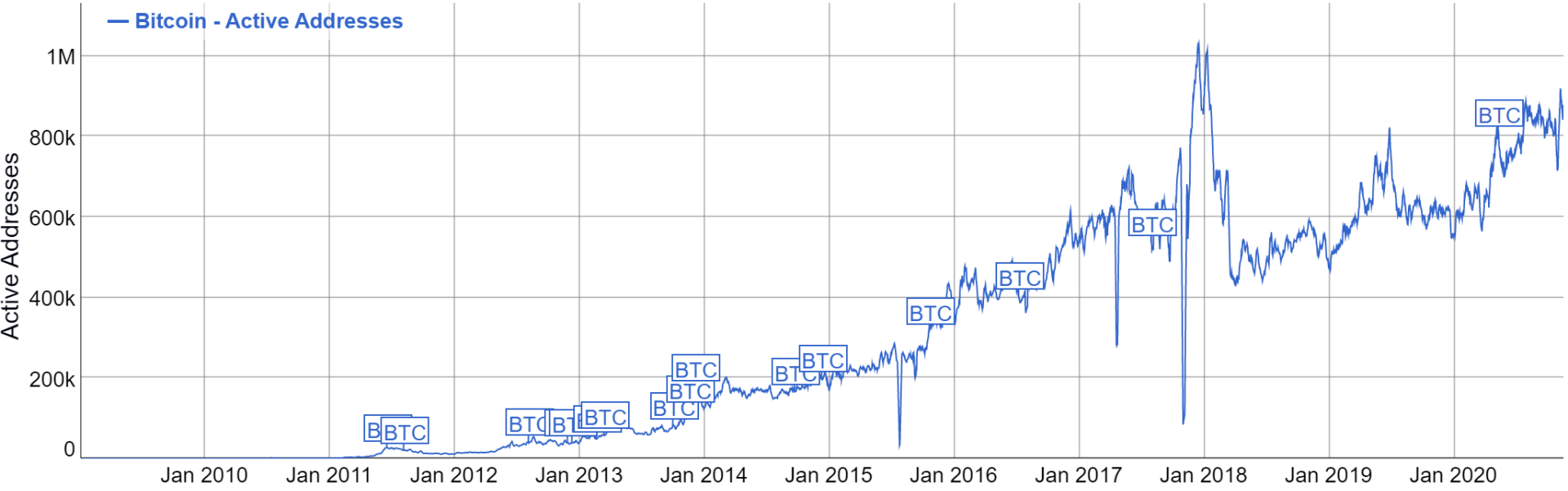
Long-term risk-adjusted performance: sharpe-ratio 2.7



https://charts.woobull.com/bitcoin-risk-adjusted-return/

Payments

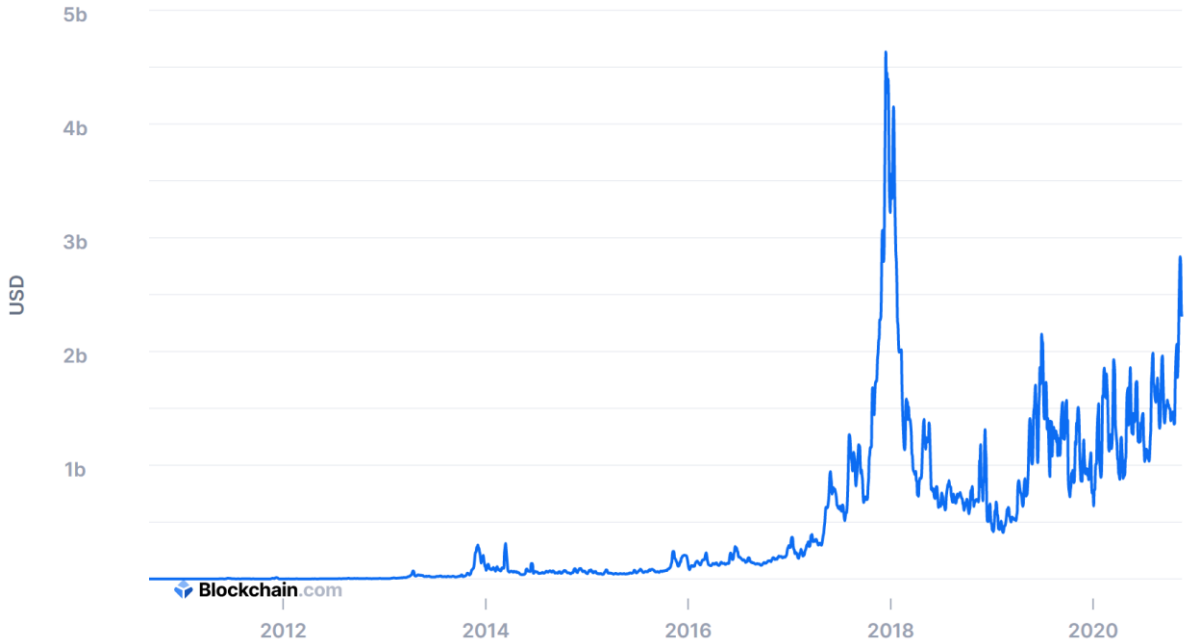
Alternative payment system: ~870k daily active addresses



https://bitinfocharts.com/comparison/bitcoin-activeaddresses.html

Payments

Transaction volume: ~$2.5 bln/day



WU	$0.2 bln/day (2016)
Paypal	$1.3 bln/day (2017)
VISA	$24 bln/day (2016)
SWIFT	$5 trln/day (2016)

https://blockchain.info/charts/estimated-transaction-volume-usd?timespan=all

Scalability

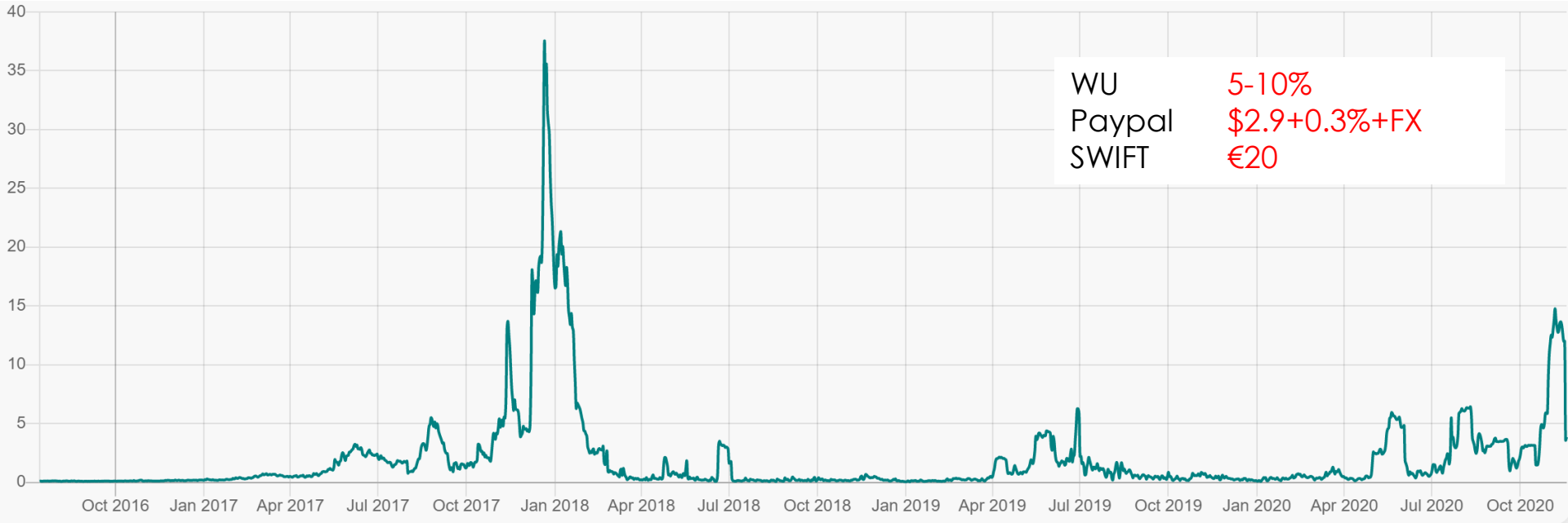
Transaction rate: ~3.5 tps

WU	9 tps (2016)
SWIFT	130 tps (2016)
Paypal	200 tps (2016)
Visa	4470 tps (2017)

https://blockchain.info/charts/n-transactions?timespan=all

Cost of sending

Transaction fee: ~$5



https://bitcoinfees.info/

"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."

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

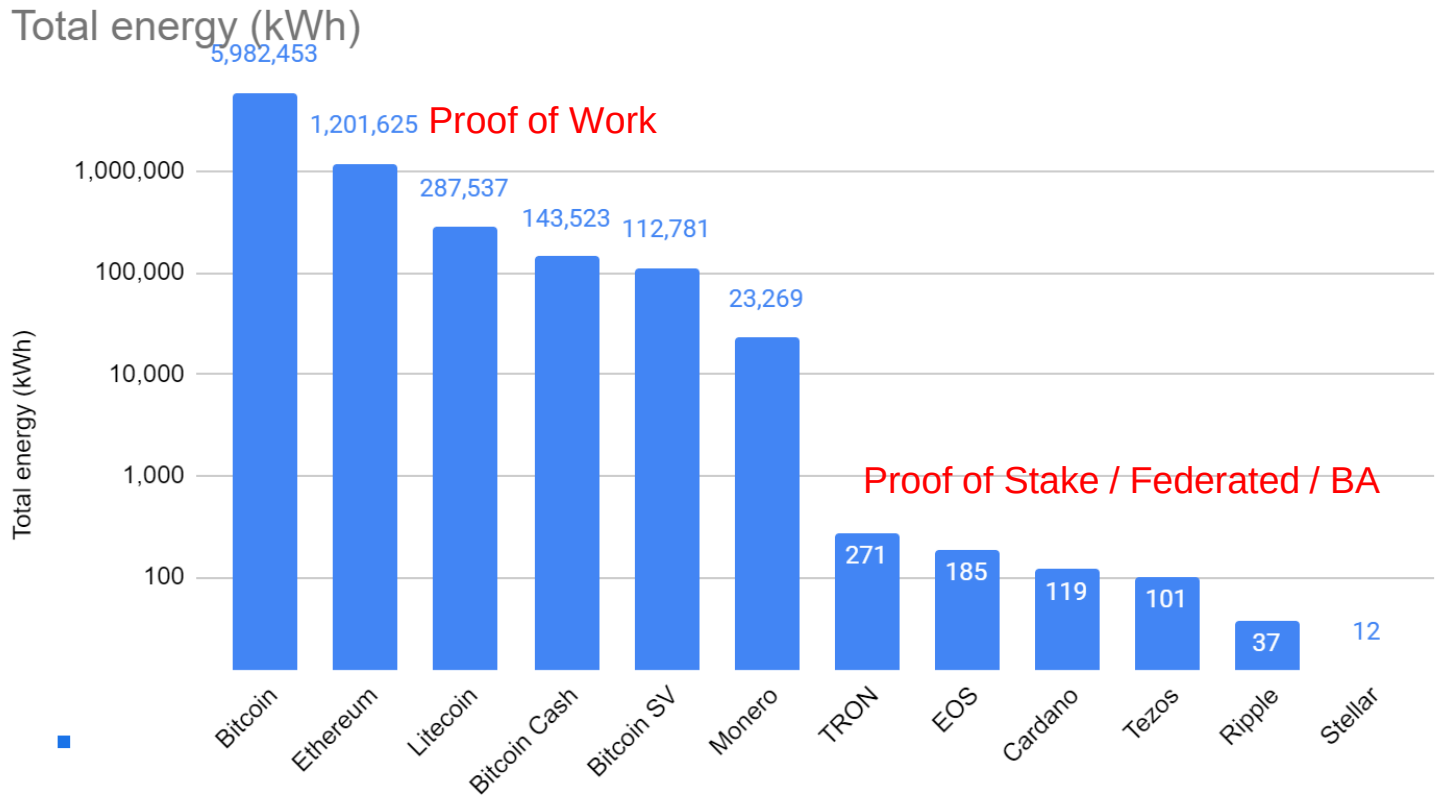
Too energy intensive?

~70 TWh/yr energy consumption, $4 bln cost, 32 Mt CO_2 footprint

https://www.cbeci.org/

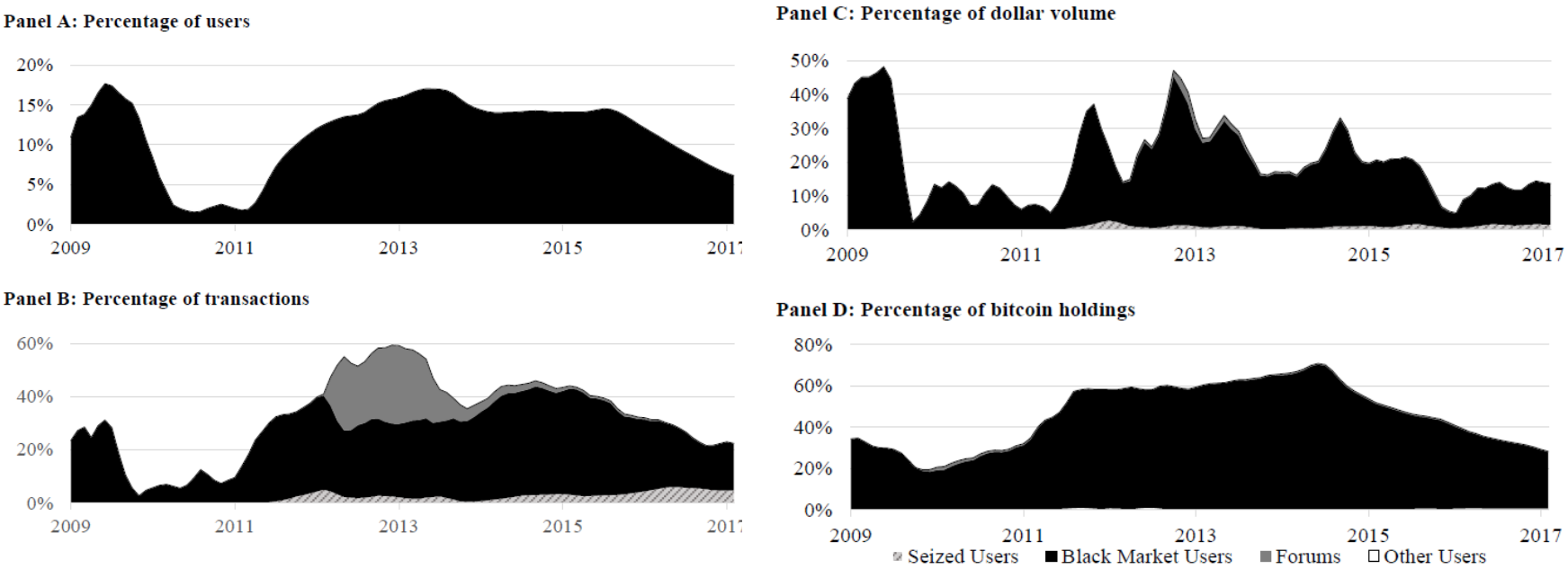
https://digiconomist.net/bitcoin-energy-consumption

Too energy intensive?



Too risky?

Purchase of illegal goods (~10% of payments)



Foley, Sean et al. Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? (January 15, 2018).

https://papers.ssrn.com/abstract=3102645

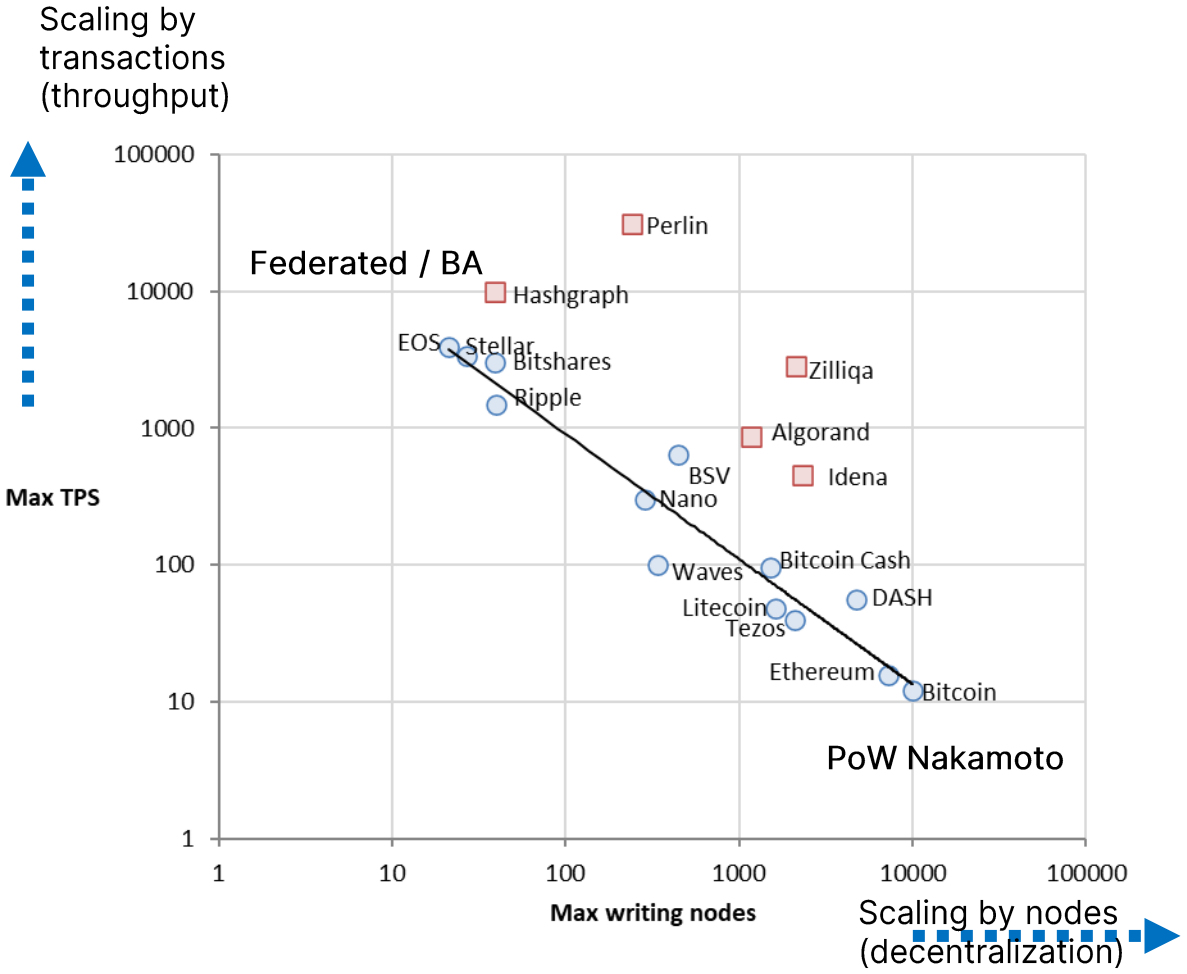
Not yet scalable?

Layer-1 (Horizontal):

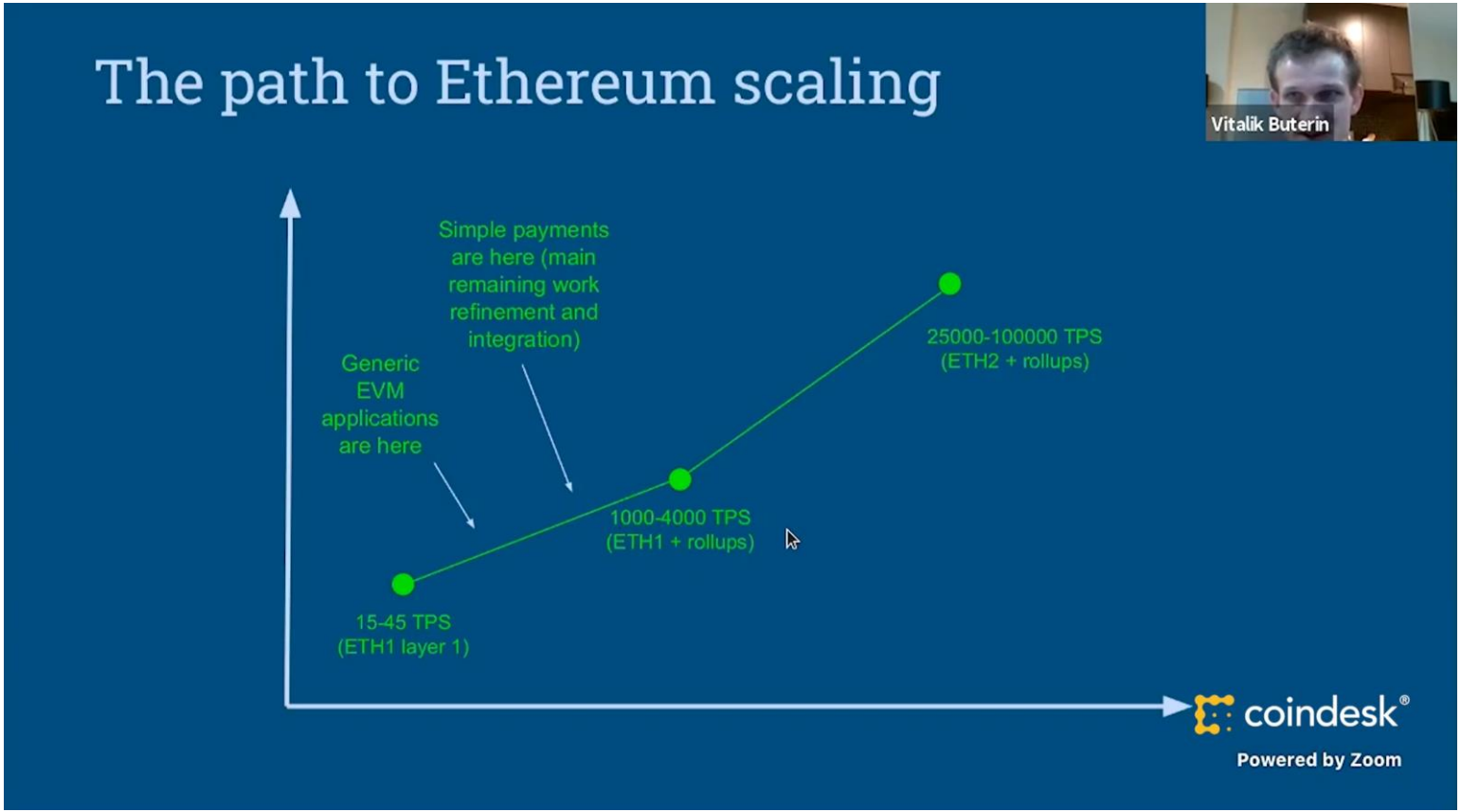
- **Sharding**: Zilliqa, NEAR, Polkadot
- **Committee consensus**: Algorand, Idena, ETH2.0
- **DAG**: Hashgraph, Perlin

Layer-2 (Vertical):

- **Sidechains:** POA, xDai, Quorum
- **Payment channels:** Lightning network, Raiden, Plasma
- **ZK:** Rollups, Optimistic rollups

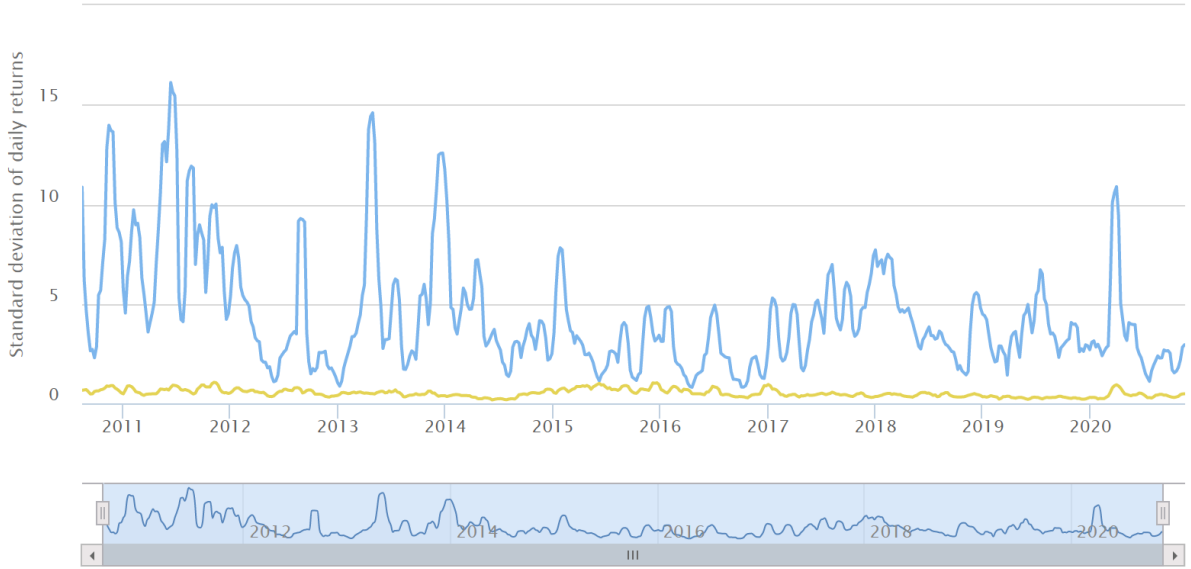


Not yet scalable?



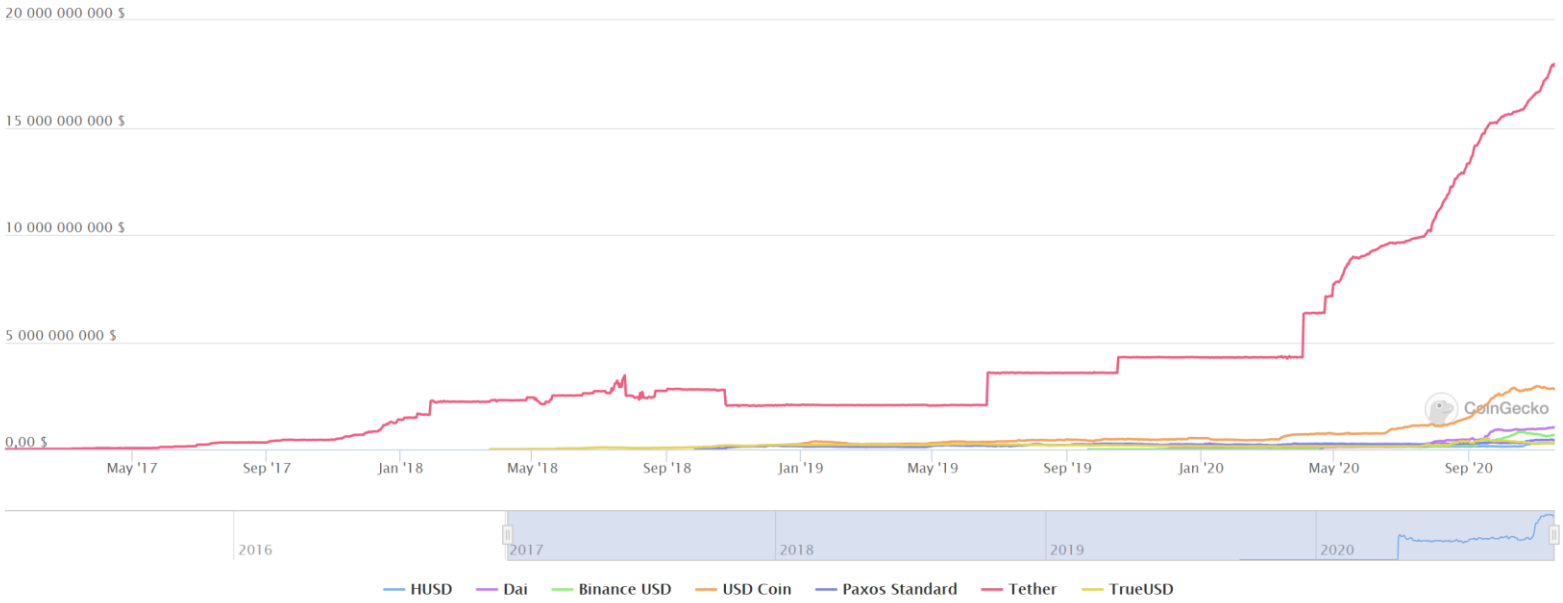
Too volatile?

- 3% daily volatility of BTC/USD recently
- 6x compared to EUR/USD



Stablecoins

Total stablecoins supply >$23 bln



https://www.coingecko.com/ru/stablecoins

Consortia stablecoins

libra

The Coins

The Libra payment system will support single-currency stablecoins (e.g., ≋USD, ≋EUR, and ≋GBP) and a multi-currency coin (≋LBR).

Anchorage · Andreessen Horowitz · BisonTrails · Blockchain Capital · Breakthrough Initiatives · checkout.com · coinbase · Creative Destruction Lab · novi from Facebook · Farfetch · Heifer International · iliad · kiva · lyft · Mercy Corps · Paradigm · PayU · Ribbit Capital · shopify · Slow Ventures · Spotify · Temasek · Thrive Capital · Uber

The Libra Blockchain

Zachary Amsden, Ramnik Arora, Shehar Bano, Mathieu Baudet, Sam Blackshear, Abhay Bothra, George Cabrera, Christian Catalini, Konstantinos Chalkias, Evan Cheng, Avery Ching, Andrey Chursin, George Danezis, Gerardo Di Giacomo, David L. Dill, Hui Ding, Nick Doudchenko, Victor Gao, Zhenhuan Gao, François Garillot, Michael Gorven, Philip Hayes, J. Mark Hou, Yuxuan Hu, Kevin Hurley, Kevin Lewi, Chunqi Li, Zekun Li, Dahlia Malkhi, Sonia Margulis, Ben Maurer, Payman Mohassel, Ladi de Naurois, Valeria Nikolaenko, Todd Nowacki, Oleksandr Orlov, Dmitri Perelman, Alistair Pott, Brett Proctor, Shaz Qadeer, Rain, Dario Russi, Bryan Schwab, Stephane Sezer, Alberto Sonnino, Herman Venter, Lei Wei, Nils Wernerfelt, Brandon Williams, Qinfan Wu, Xifan Yan, Tim Zakian, Runtian Zhou *

Note to readers: This report was published before the Association released White Paper v2.0, which includes a number of key updates to the Libra payment system. Outdated links have been removed, but otherwise, this report has not been modified to incorporate the updates and should be read in that context.

Abstract. The Libra Blockchain is a decentralized, programmable database designed to support a low-volatility cryptocurrency that will have the ability to serve as an efficient medium of exchange for billions of people around the world. We present a proposal for the Libra protocol, which implements the Libra Blockchain and aims to create a financial infrastructure that can foster innovation, lower barriers to entry, and improve access to financial services. To validate the design of the Libra protocol, we have built an open-source prototype implementation — *Libra Core* — in anticipation of a global collaborative effort to advance this new ecosystem.

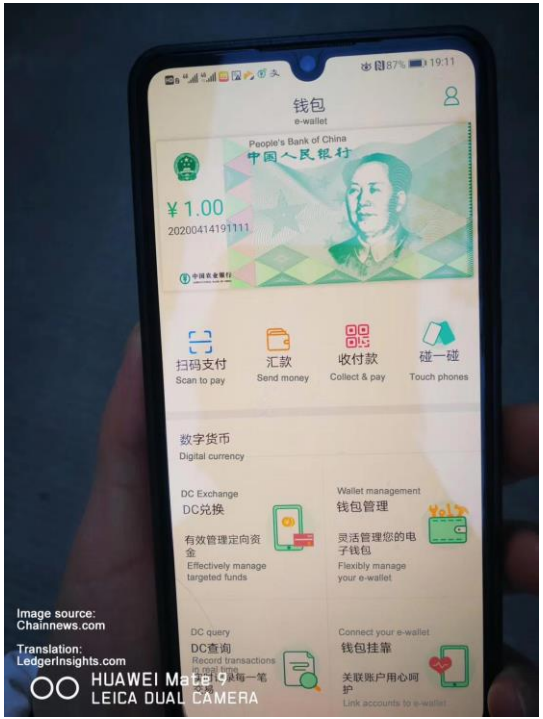
The Libra protocol allows a set of replicas — referred to as validators — from different authorities to jointly maintain a database of programmable resources. These resources are owned by different user accounts authenticated by public key cryptography and adhere to custom rules specified by the developers of these resources. Validators process transactions and interact with each other to reach consensus on the state of the database. Transactions are based on predefined and, in future versions, user-defined smart contracts in a new programming language called *Move*.

We use Move to define the core mechanisms of the blockchain, such as the currency and validator membership. These core mechanisms enable the creation of a unique governance mechanism that builds on the stability and reputation of existing institutions in the early days but transitions to a fully open system over time.

CBDC

*"Whether the **digital Yuan** can become the dominant form of currency and mainstream payment means, depends on whether it has greater efficiency, lower transaction costs, enough economic scale with commercial value, and people' acceptance."*

Li Lihui, Former President of the Bank of China



Use of China's Digital Yuan Nears $300 Million

More than 2 billion digital yuan has been spent in approximately 4 million separate transactions so far.

By Scott Chipolina — 2 min read • Nov 2, 2020

Huawei Mate 40 comes with a hardware cryptocurrency wallet for the digital yuan

The Huawei Mate 40 anticipates the needs of Chinese cryptocurrency investors with its built-in hardware crypto wallet.

Image by: Huawei

Sun, 01 Nov 2020, 16:00 pm UTC

CBDC

	Модель A		Модель B		Модель C		Модель D	
Функции	Центральный банк	Банк/финансовый посредник	Центральный банк	Банк/финансовый посредник	Центральный банк	Банк/финансовый посредник	Центральный банк	Банк/финансовый посредник
Осуществление ПОД/ФТ/ФРОМУ по операциям с ЦВЦБ	✓ В отношении банков/финансовых посредников		✓			✓		✓
Открытие кошельков клиентам	✓ Открывает кошельки банкам/финансовым посредникам		✓		✓	Инициирует открытие кошельков клиентам	✓ Открывает кошельки банкам/финансовым посредникам	✓ Открывает кошельки клиентам
Проведение платежей и расчетов по кошелькам клиентов	✓ Между кошельками банков/финансовых посредников		✓		✓	Инициирует проведение платежей и расчетов		✓
Доступ к кошельку клиента из другого банка/финансового посредника	—		—			✓		✓

https://www.cbr.ru/StaticHtml/File/112957/Consultation_Paper_201013.pdf

Summary

- Crypto has emerged into $500 bln asset class
- Alternative financial system: store of value, stablecoins, tokens, DeFi, DAO,… => Money and financial markets of the next generation
- Advantages: Global, Inclusive (zero KYC), Non-custodial (no counterparty risk), Transparent, Low cost, Fast finality
- Cambrian explosion of new protocols: scalable, decentralized, private and inclusive financial services
- Central banks and corporate digital currencies are catching up…