



Understanding Cryptocurrencies

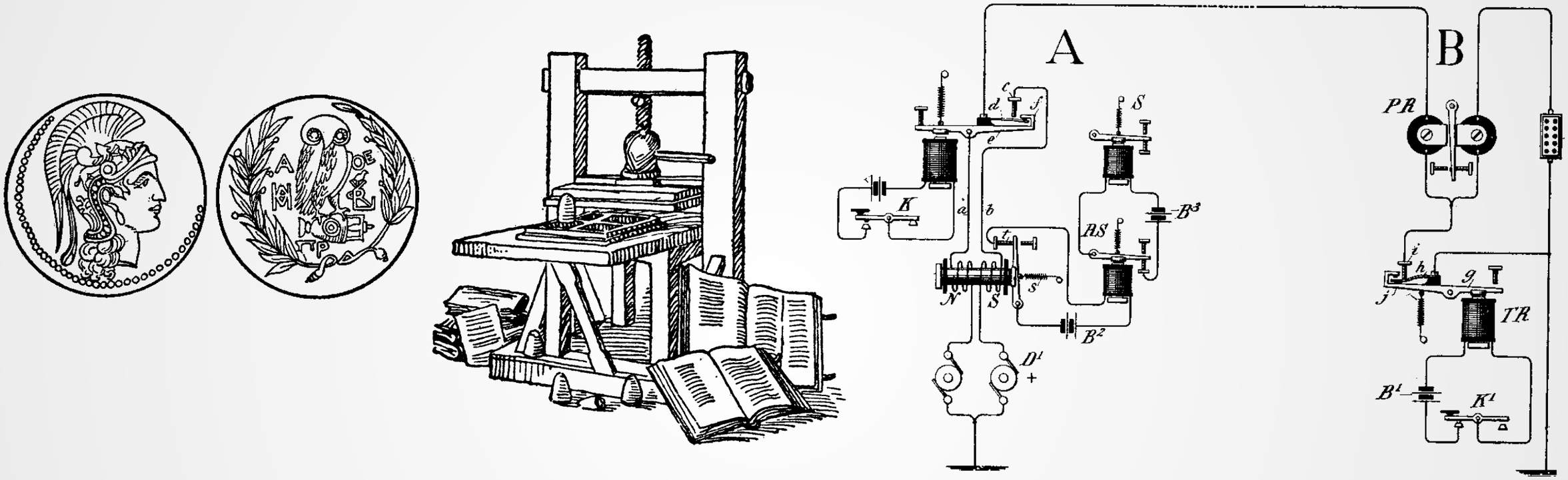
Wolfgang Karl Härdle

Campbell R. Harvey

Raphael C. G. Reule

20200326 Glasgow U

The role of money



Greek Coin, Gutenberg Paper Printing, Telegraphy Circuit

Allocation of scarce (appropriable, non-abundant, non-rivalrous) resources

Commodity (Gold) - Fiat (EUR) - Cryptocurrencies (CC)

Financial Inclusion

Homeostasis

Financial illiteracy
Corruption
Suboptimal governance
Inefficient monetary institutions
Insecurities about fiat currency (forgery …)

Mass-1st-World-Evolution

1970s: Mainframe
1980s: PC
1990s: Internet
2000s: Social Media
2010s: Blockchain

Smartphone ownership

43% in 2013, 60% in 2018

56% in 2013, 77% in 2018

41% in 2013, 78% in 2018

13% in 2013, 34% in 2017

Source: statista.com

In total, 53% of the worlds' adult population is unbanked (2 455 million)
Source: "Half the world is unbanked", McKinsey & Company

Traditionally
with intermediary

Now
permissionless, decentralized, 24/7

Berlin - Room 77

Beer for Bitcoin, 2011

„Murderers, drug dealers and North Koreans“

James Dimon

chairman, president and CEO of JPMorgan Chase & Co.

„It’s a lot more“

Christine Lagarde

Managing Director of the International Monetary Fund

Both statements are from fall 2017.

Exiting the “Nerd”-Space

Institutional incentives (**ECB**, Bundesblock, DB, CoBa, …) to

- lower the **risk** and cost of entrepreneurship across economic systems and costs associated with contracting.

- provide **chances** for improved economic coordination and governance.

- present **opportunities** for economic discovery, financial / governmental policy innovation and coordination, geared toward adoption and usage of the BC tech.

- What is the reason for the rise of interest in CCs ?
- Can and will it be part of Industry 4.0 ?
- What are the differences between CC variants ?
- Traditional HF econometrics versus 24/7 data ?
- New research areas and evolution of CC research ?

Myths vs. Facts

Need of **empirically perceived**
and **scientifically proven answers**!

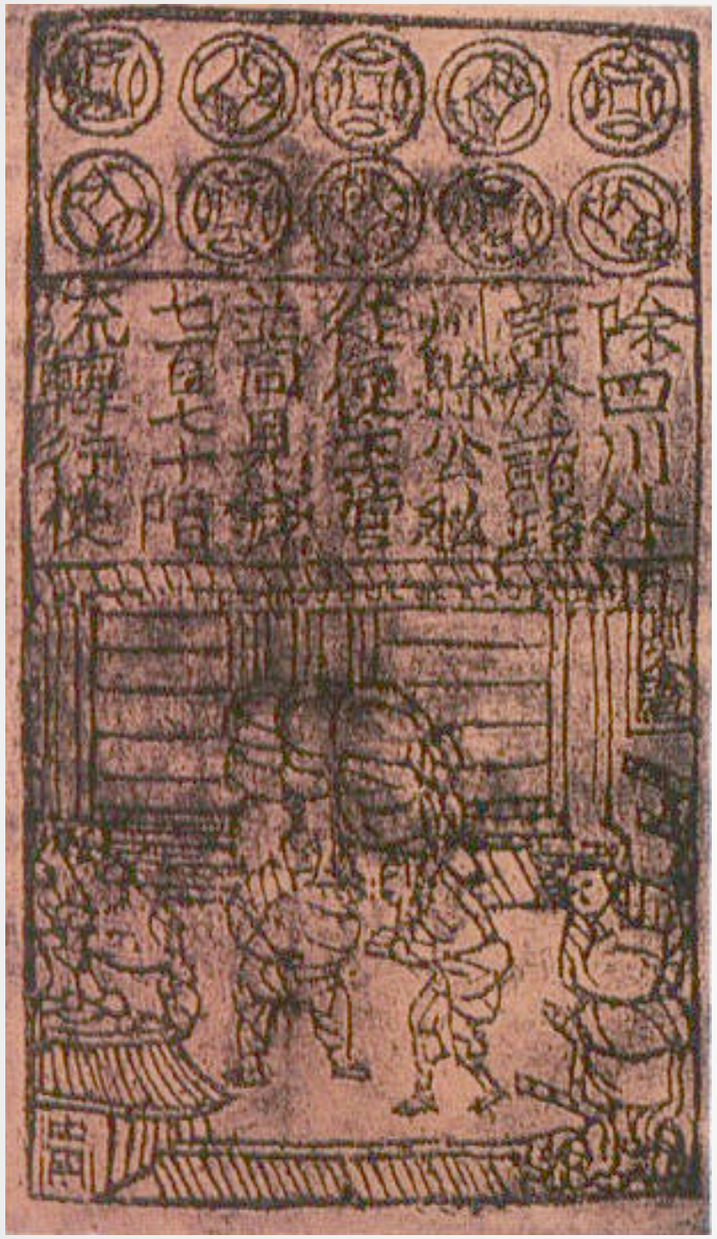
- What are we dealing with ?
- How does it work ?
- Why and how do people participate ?
- How do CCs develop in target groups ?
- How can this be researched ?

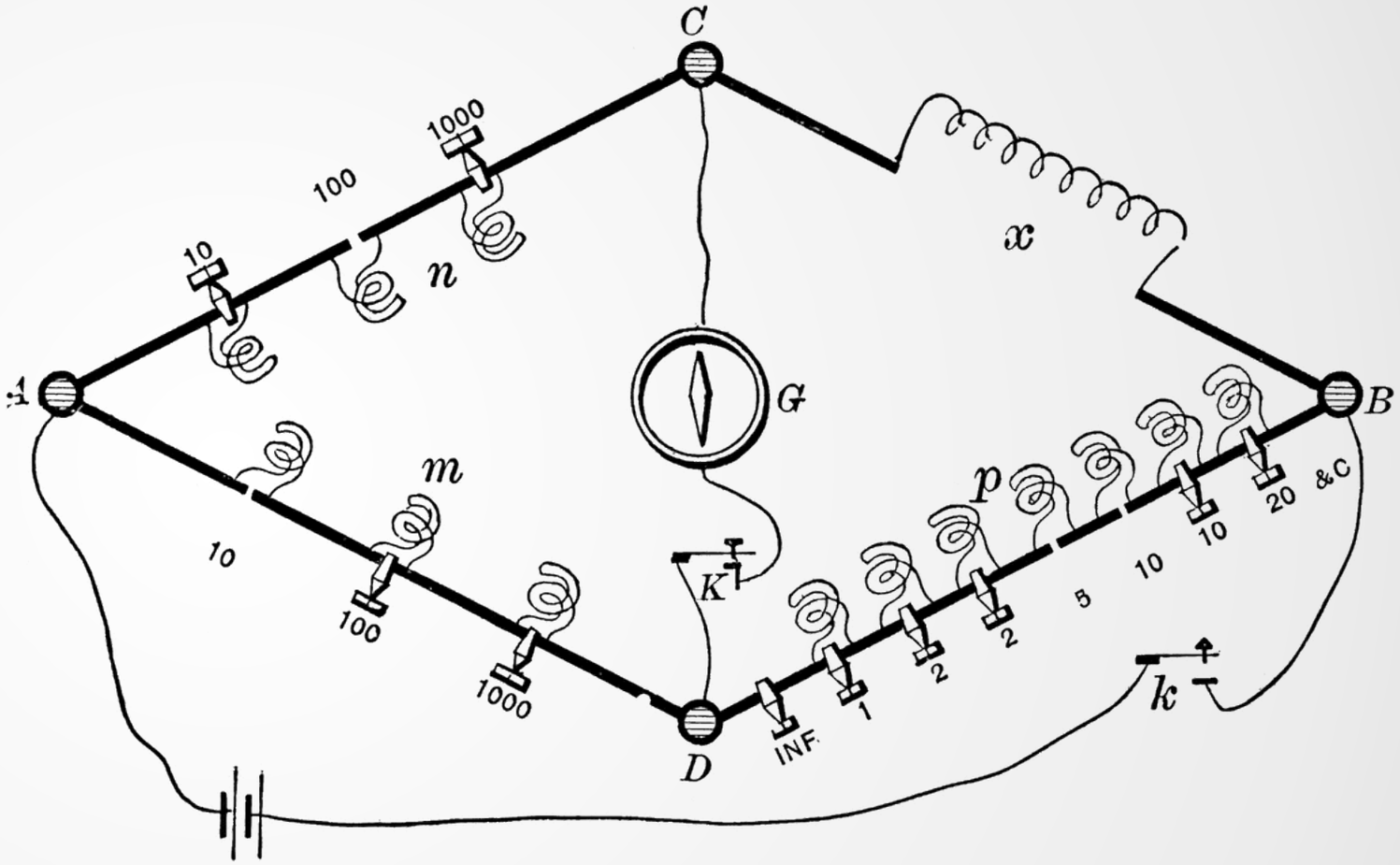
Pythia
High Priestess at the
Oracle of Delphi

Outline

1. Motivation ✔
2. Background information
3. Blockchain mechanisms
4. Cryptocurrency markets
5. Research areas
6. Chance, Risk and Opportunities
7. Understanding Cryptocurrencies (?)

Transition from homeostasis





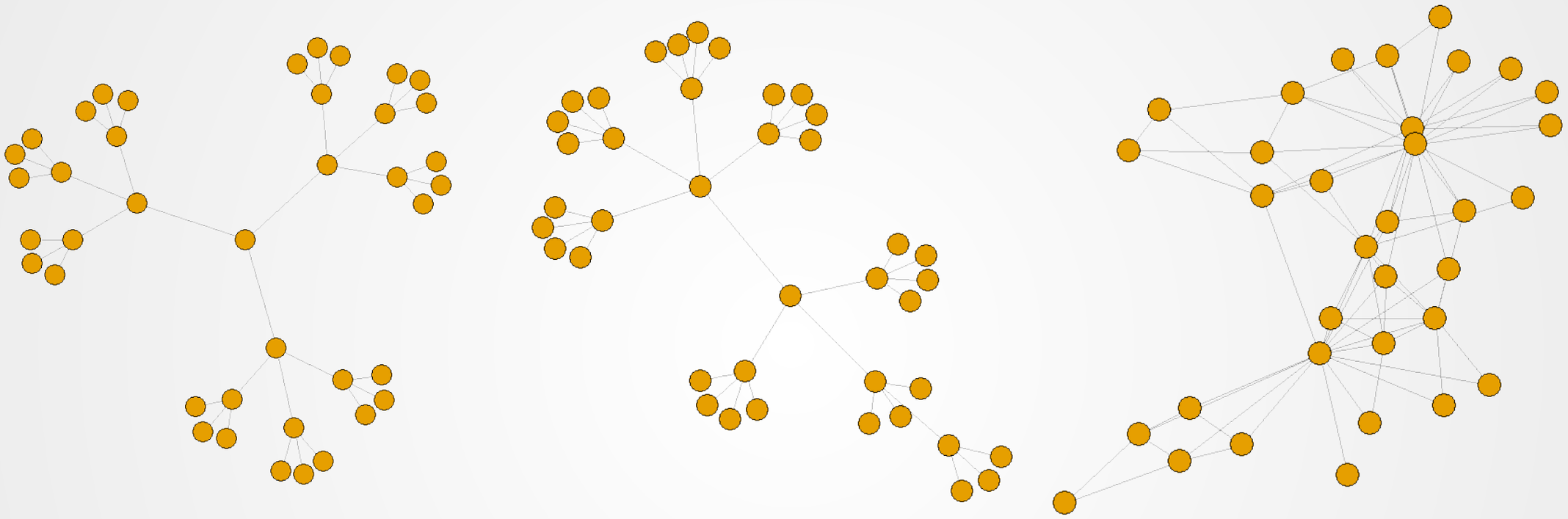
Physical proof

Song Dynasty Jiaozi, the world's earliest paper money.
Source: 社会历史博物馆 (Museum of Social History, Henan)

Algorithmic proof

Wheatstone bridge
Avery 1895

Network Fundamentals



(a) Centralized (b) Decentralized (c) Distributed

Types of networks

How to run a network with increasing nodes/participants?
Consensus, Trust, Incentives for participation

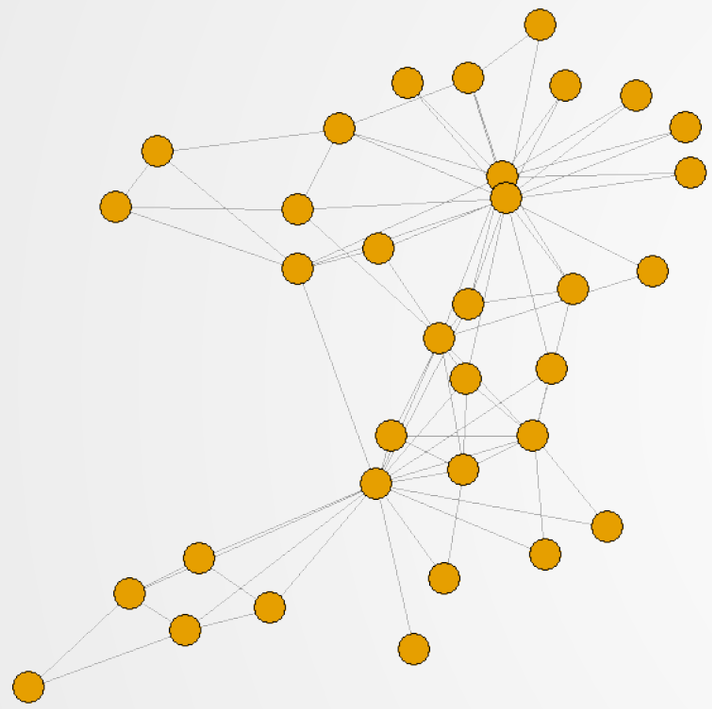
CrixToDate

Consensus

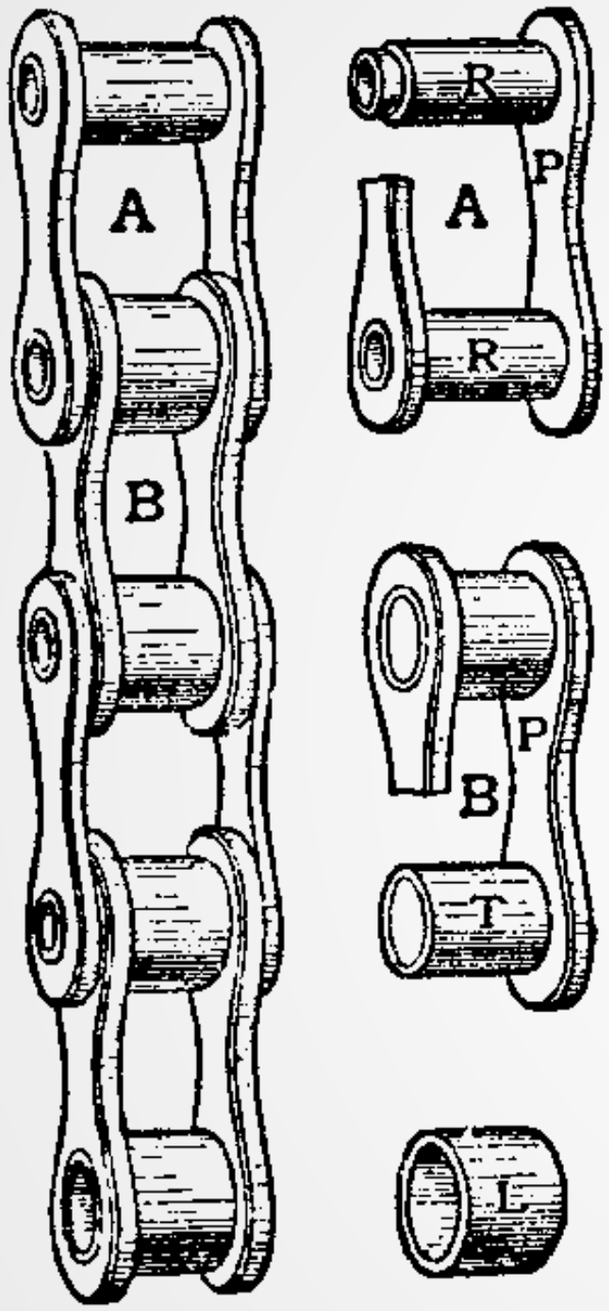
Lynch, Dwork, Stockmeyer, 1988

Protocols for
solving consensus in a (distributed) network of unreliable processors, called „Paxos“ or „Paxos Consistence“ (greek Παξός)

Consensus is the process of agreeing on one result.



Distributed Network



Bicycle chain made of chainblocks

Trust & Validation Systems

Haber & Stornetta, 1991

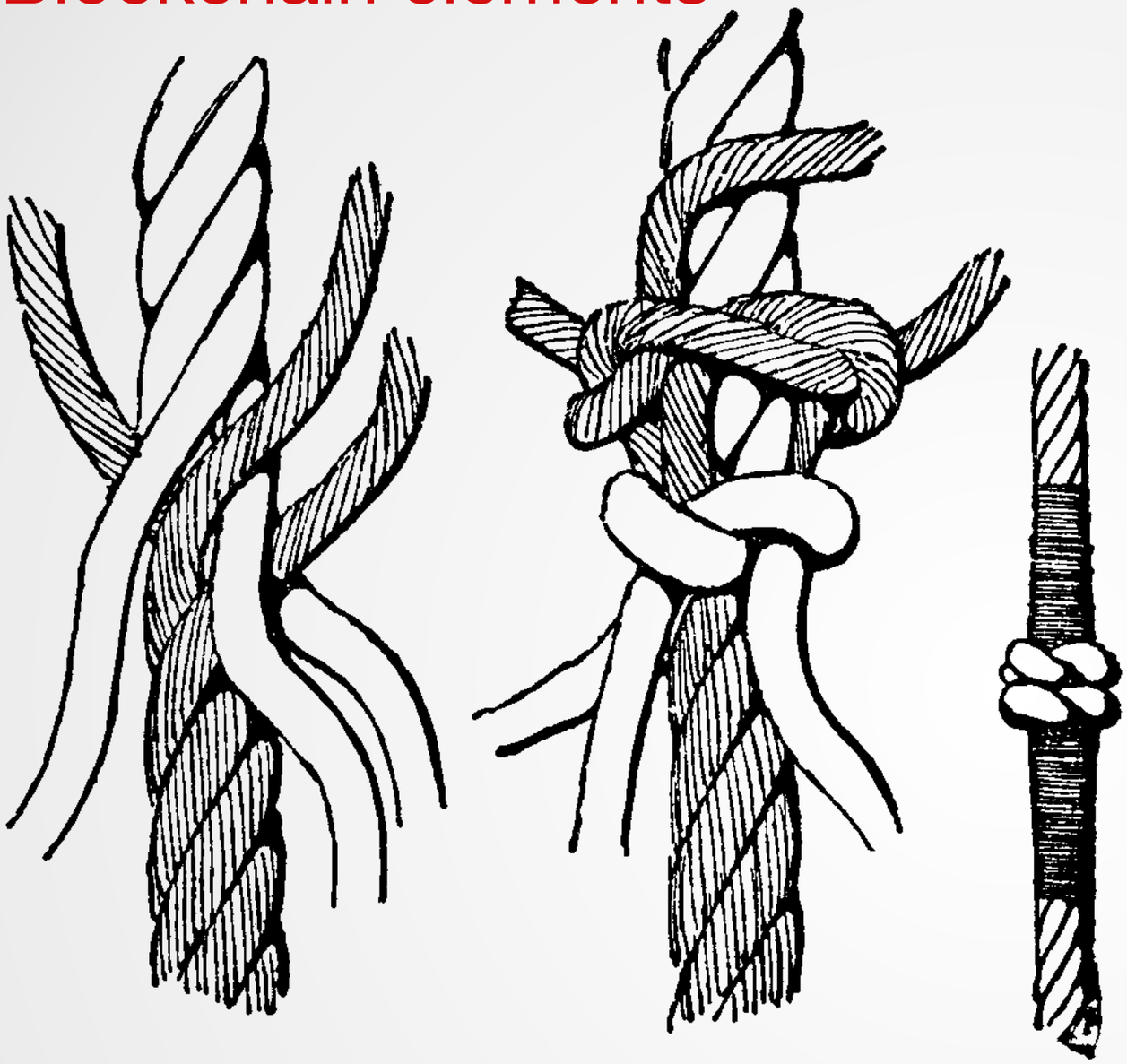
Solved problems of collusion and trust by using **either linking hash values** together **or** providing distributed trust via **signatures**

Dwork & Naor, 1992

provide each eMail with a header containing the ”**virtual postage**” („**proof-of-work calculation**“) to combat junk mails / spam-

cost of the stamp = cost in computational power

Blockchain elements



Hashing

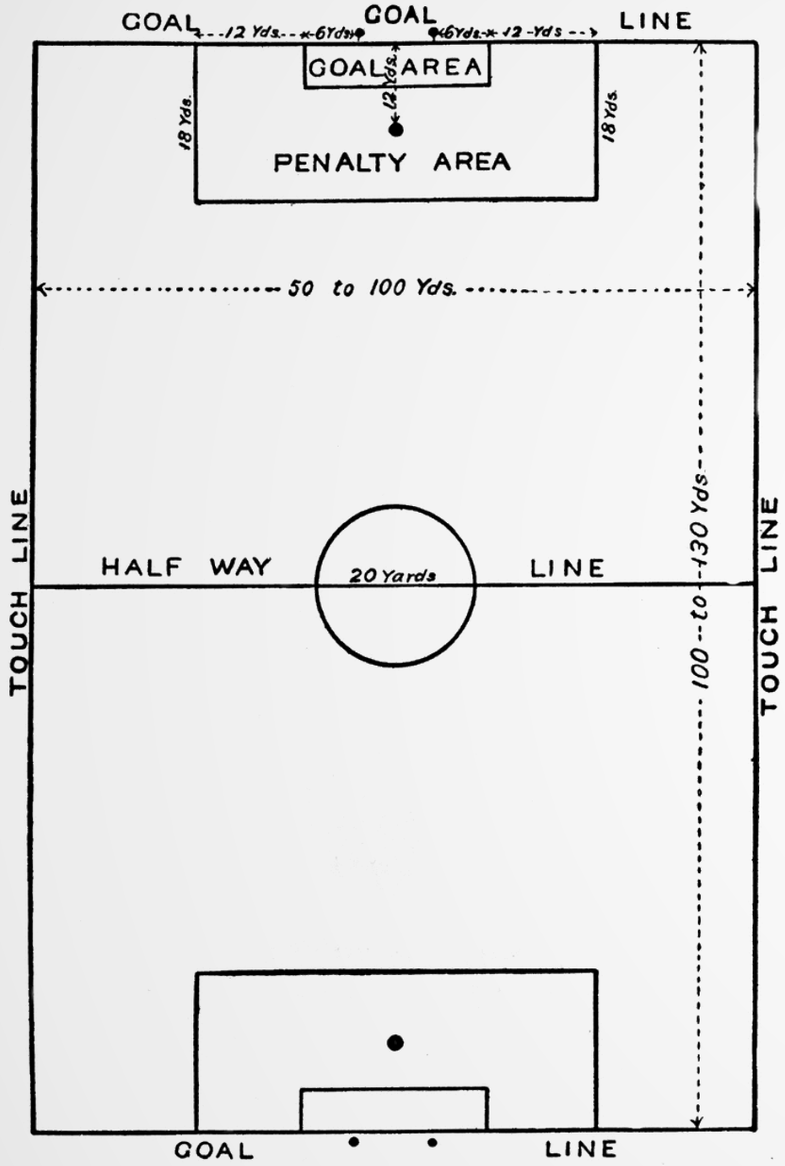
Input message **m**
Output message **h**
Specific **hashing** function **H**

h = H (m)

(Hashing ≠ Encryption)

BTC = SHA-256 algorithm (maximum input size is 2^{64}-1 bits = Word, Phrase, Book etc.; SHA = Secure Hash Algorithm)

SHA-256 output is 64 numbers and characters (a to f and 0 to 9 = hexadecimal) for a plethora of input (sentence, speech, the Bible etc.)



SHA-256 Maximum Theoretical Input

- Assume that **1 bit equals to 1 mm²**.

- A **soccer field** has the dimensions of **7 140 m²**.

  Then **2^64-1 bits fill 2 583 577 601,36 soccer fields**.

- The whole surface of the earth equals to

  510 000 000 000 000 m².

  The maximum theoretical input is therefore 36 170

  times the earth surface with the theoretical input size.

In 1: Hello CRIX
Out 1: 4e0f6bbff658b4b12b01e5b5dc766316104b5cbbd1666284a61ee6ab39185823

In 2: Hallo CRIX
Out 2: 0f2de5d947b5780ab1b0cc4bae36268f4481eafa24b5bf7c6527bda7758ef2df

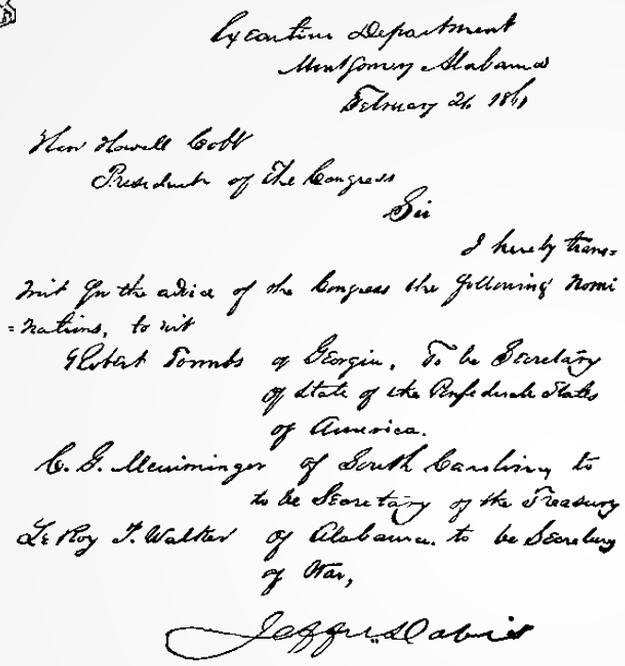
In 3: Asia is wonderful!
Out 3: d77146c8ca175d408173938a1b0568f6baae10ba46518b93682b3284dce85ff2

R package = **digest(„sha256“)**

```
library(digest)
digest("Asia is wonderful!",algo="sha256")
```

thecrix.de

Hashes as Checksum



By authority Department
Montgomery Alabama
February 25. 1861

Hon Howell Cobb
President of the Congress

Sir

I hereby transmit for the advice of the Congress the following Nominations, to wit

Alexander Toombs of Georgia, To be Secretary of State of the Confederate States of America.

C. G. Memminger of South Carolina to be Secretary of the Treasury

Le Roy P. Walker of Alabama. to be Secretary of War,

Jeffn Davis

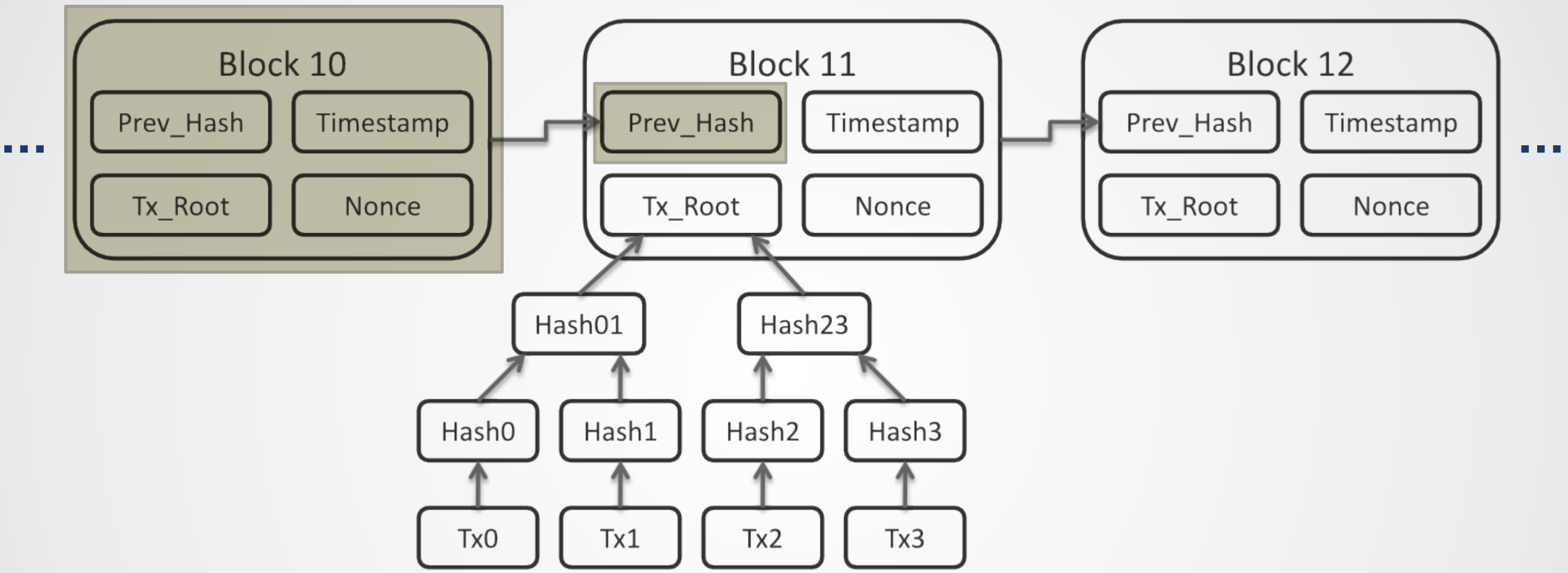
Message A = unique Hash A
Message B = unique Hash B
…

Sender / Receiver can check, if messages are the same by looking at the hash.
Recall: Minor/any changes = Hash changes completely

Blockchain

- information put together in „blocks“
- „chained“ together via hashes (of the information)
- sequential distributed database
- shared across all participants (network nodes)
- replication & consistency

Exemplary contents of a BTC block



First line in block = Hash of last block

Last line in block = Hash of all block contents, e.g. Transactions (Tx) = First line in next block

$$h = H(m_{\text{Prevhash+Timestamp+List of transactions+etc.}})$$

„Controls allow a quarrelsome species,

ill-suited to organizations larger than tribes,

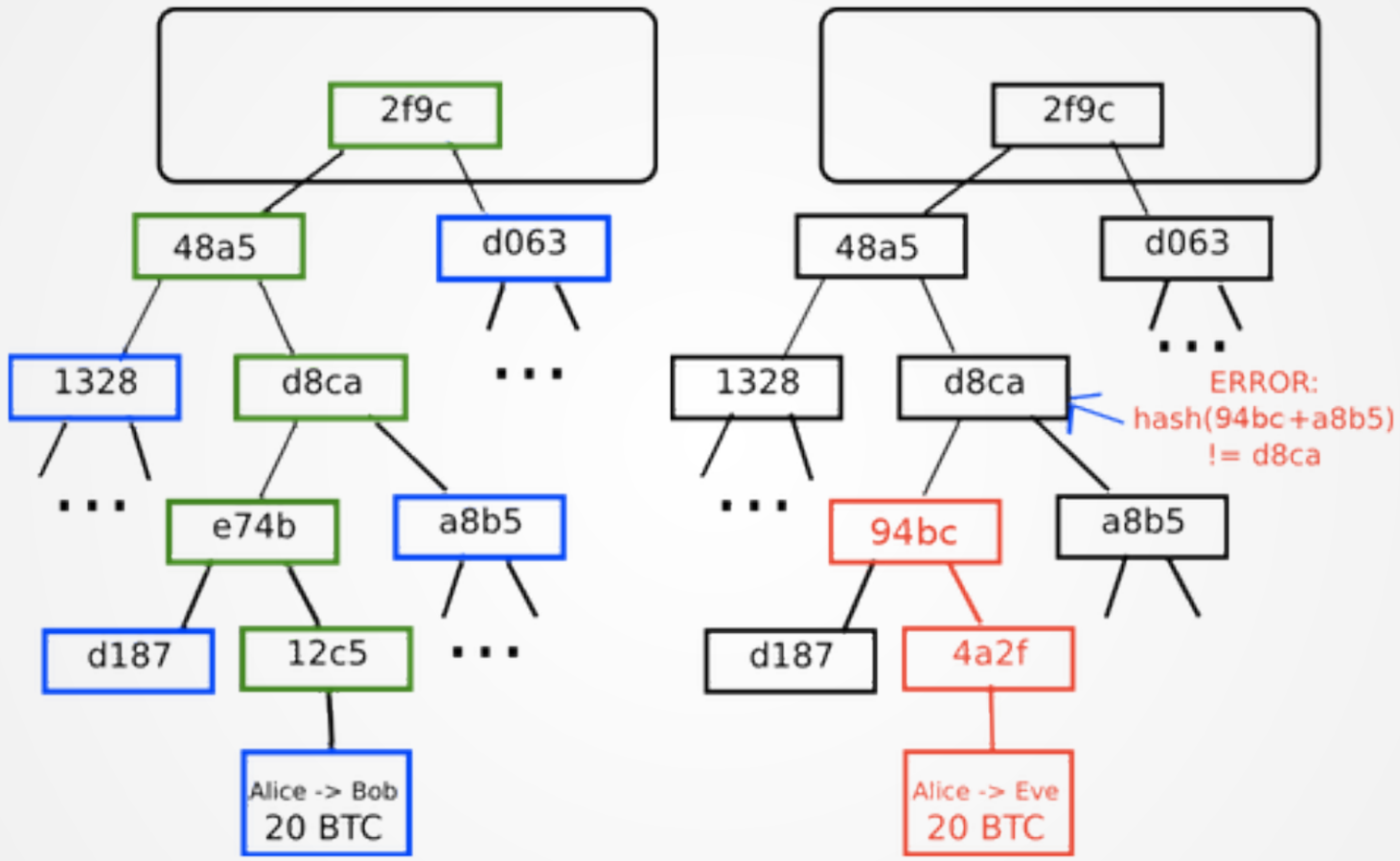
to work together on vast projects

like manufacturing jumbo jets and running hospitals.“

Nick Szabo „Smart Contracts“, 1997

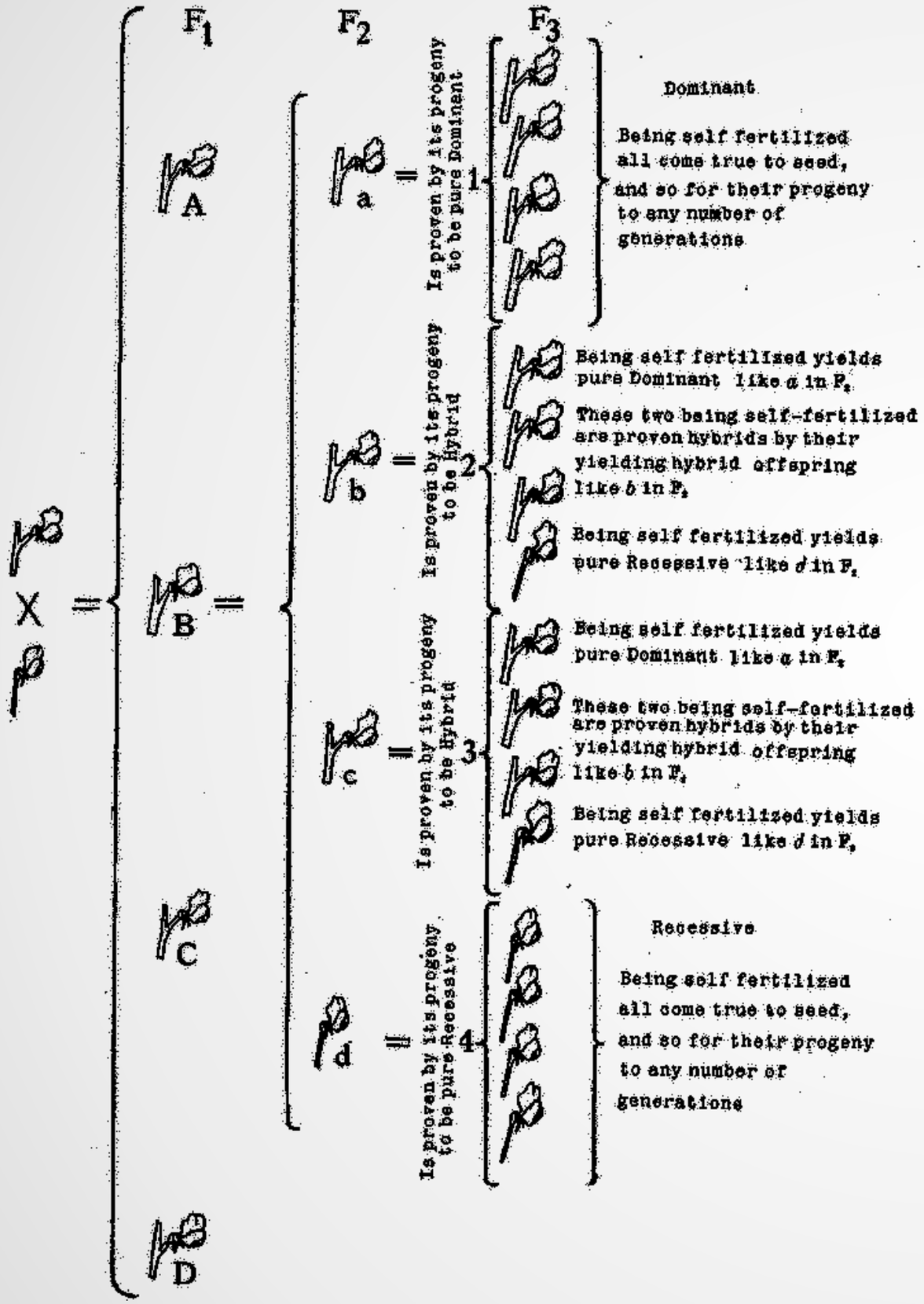
Quarrelsome species being in controlled

Blockchain - the Unchangeable Game Changer



History can not be rewritten.

https://andersbrownworth.com/blockchain/blockchain



Hundreds of CCs share the same „genes“ (active/dead).

Yet they often develop (drastically) different.

But all CCs are algorithms based on the blockchain technology.

BTC
Block Time ~ 10 min

(Block Time = Block Latency)

LTC
Block Time ~ 2.5 min

ETH
Block Time ~ 10 sec

XRP
Block Time ~ 3.5 sec

(! BC ≠ „=CC“)
(! CC ≠ „=Token“)

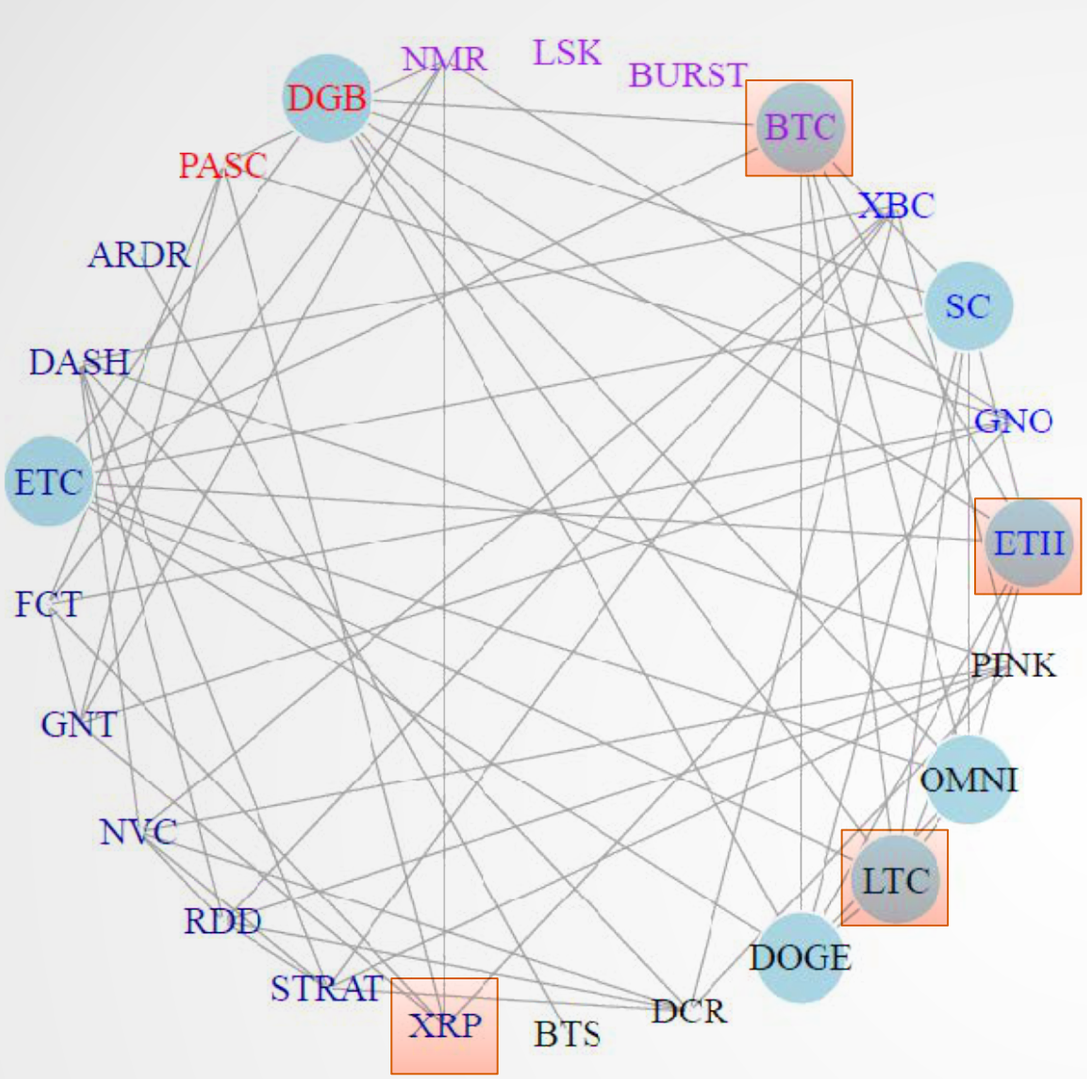
Some differences as highlights:

- Target groups (e.g. Ripple/XRP = bankers)
- System constructions and intentions (e.g. Block Latency)
- System management (e.g. BTC vs. XRP)
- Proof-of-work, proof-of-stake, proof-of-brain, proof-of-burn …
- Value supply (e.g. „premined“ vs. „mined“)
- Reward systems

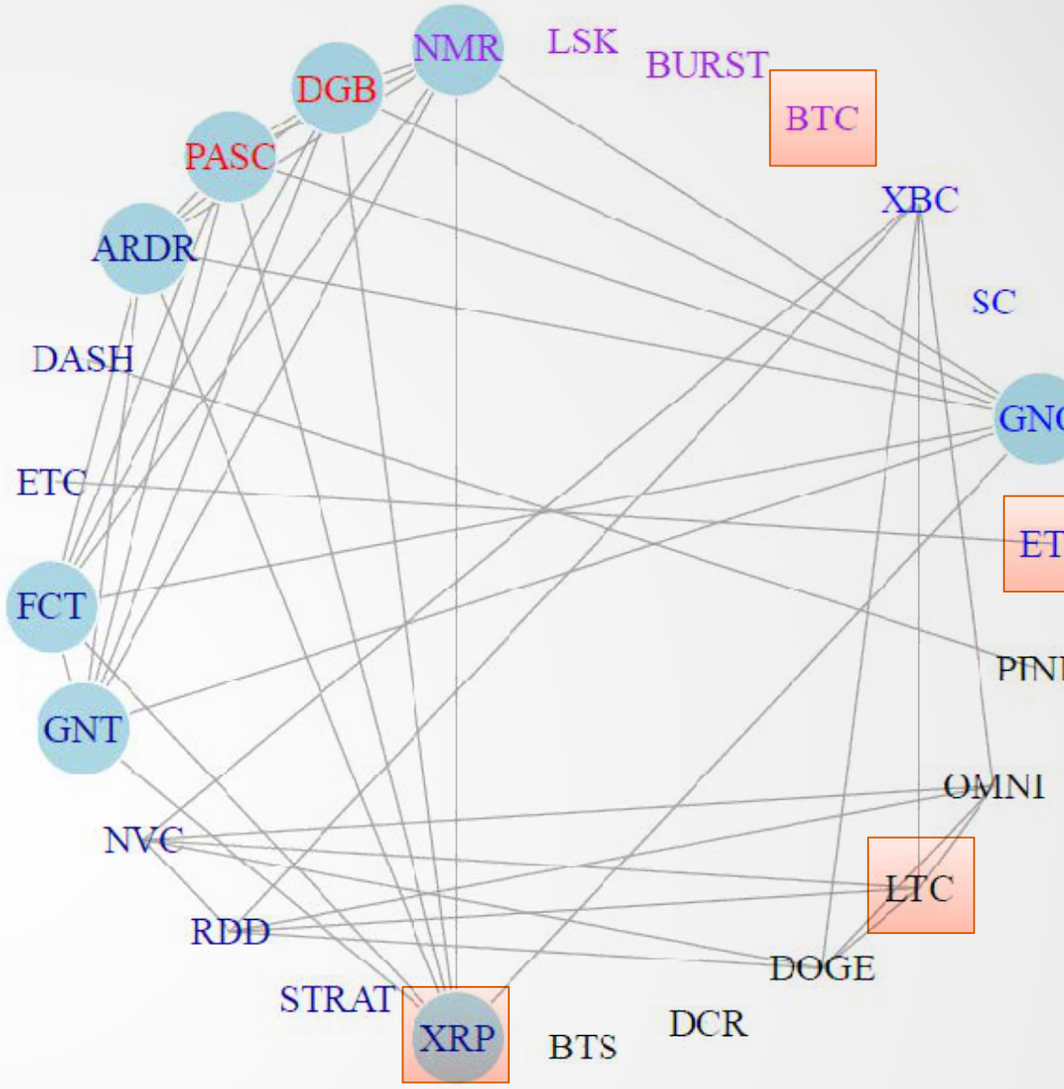
  (e.g. BTC = proof-of-work, ETH planned = proof-of-stake)
- System „reaction time“, Block-Build-Time (e.g. BTC vs. ETH)

Broad **Classification**

- Transaction (e.g. BTC, LTC)
- Distributed Computation (e.g. ETH)
- Utility Token (e.g. FileCoin, Golem)
- Security Token (e.g. DX.Exchange)
- Fungible Token (e.g. ETH's ERC-20)
- Non-Fungible Token (e.g. ETH's ERC-721)
- Stablecoins (e.g. collateralized w/ fiat, real assets, cryptocurrencies)



(a) Type of proof mechanism



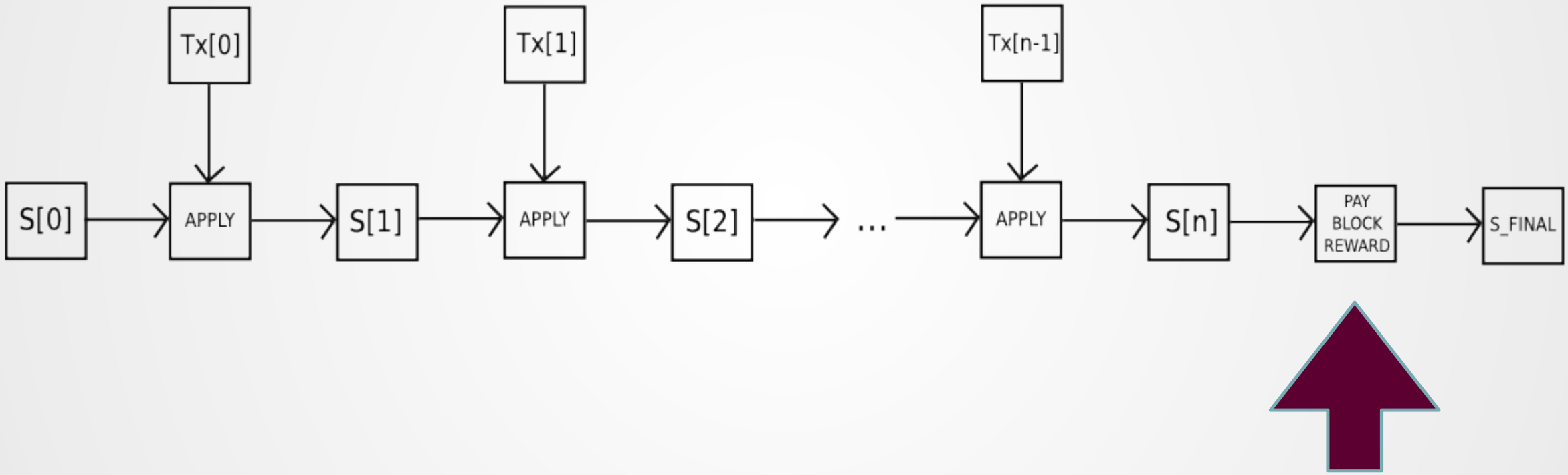
(b) Type of algorithm

Dynamic return-based network with coin attributions used to develop a dynamic covariate-assisted spectral clustering method to detect communities.

Li G, Tao Y, Härdle WK (2019)

Cause of participation/Reward System

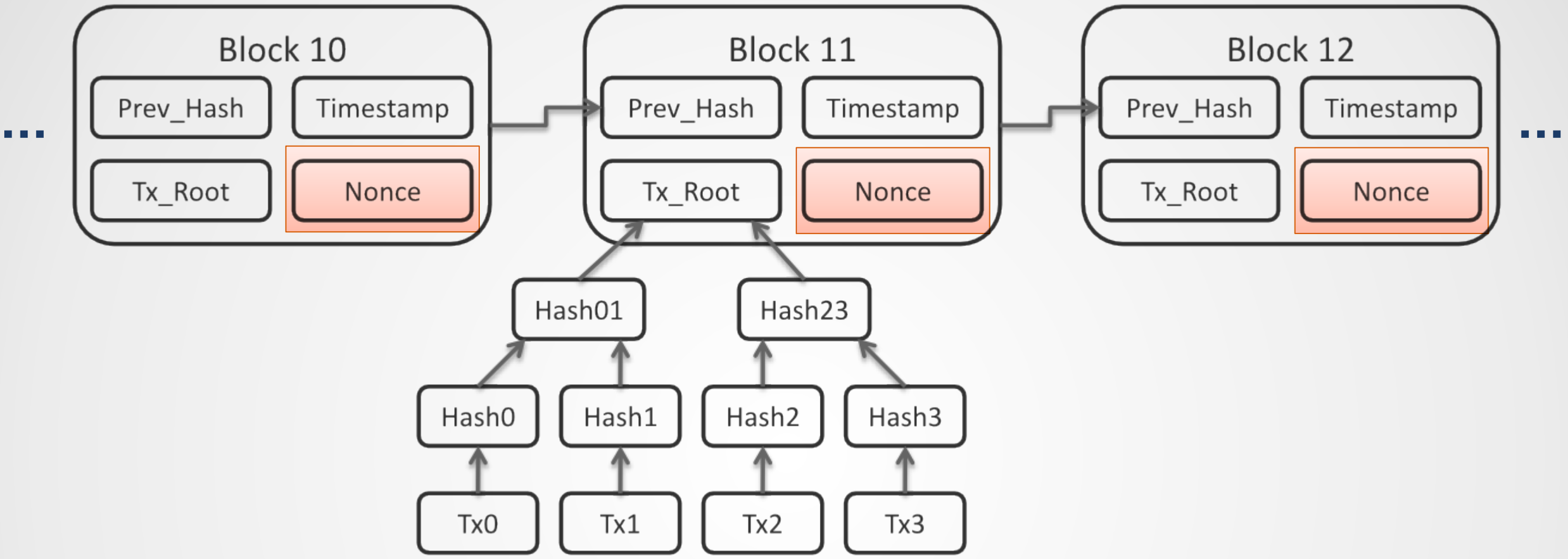
Miners create „fitting“ hashes to chain the blocks



Block reward started at 50 BTC in block #1 and halves every 210,000 blocks

http://www.bitcoinblockhalf.com

„Fitting“ BTC hash creation via the nonce



- **BTC** = **proof-of-work** (everybody can participate) = nonce **N &** target value **t**
- **Nonce** = **random number, which leads to a value lower than the target value given**

  Target value = number of leading zeroes in a hash
- **Search for the „right“ nonce = brute force lottery**

  immense amounts of computing power, single or „pooled“ **needed** to find the right nonce as fast as possible before the competition finds it

- **„Difficulty“ = „Find a hash with specified number of leading zeroes“**

  i.e. here „find 12 leading zeroes“ (before the competition does)

- **Aim = Block creation every 10 minutes on average (BTC System)**

  If blocks are being created too fast or too slowly, then the difficulty (the number of leading zeroes) is adjusted

- **„right“ hash = hard to find, easy to validate with given nonce (POW)**

In: h + N_1
Out: **00**da7e9f36f14c85a242a8113e53033ee5a9453d57dc7af26a6444a8e2704e99

In: h + N_2
Out: **0000000**dbae88544b993330777f448112f7df2daa12227143a74821bb315b9de

...

In: h + N_{356}
Out: **000000000000**38b6ad3811370fe06b9a5854ebc62280e54a7dd6cf001a3505e3

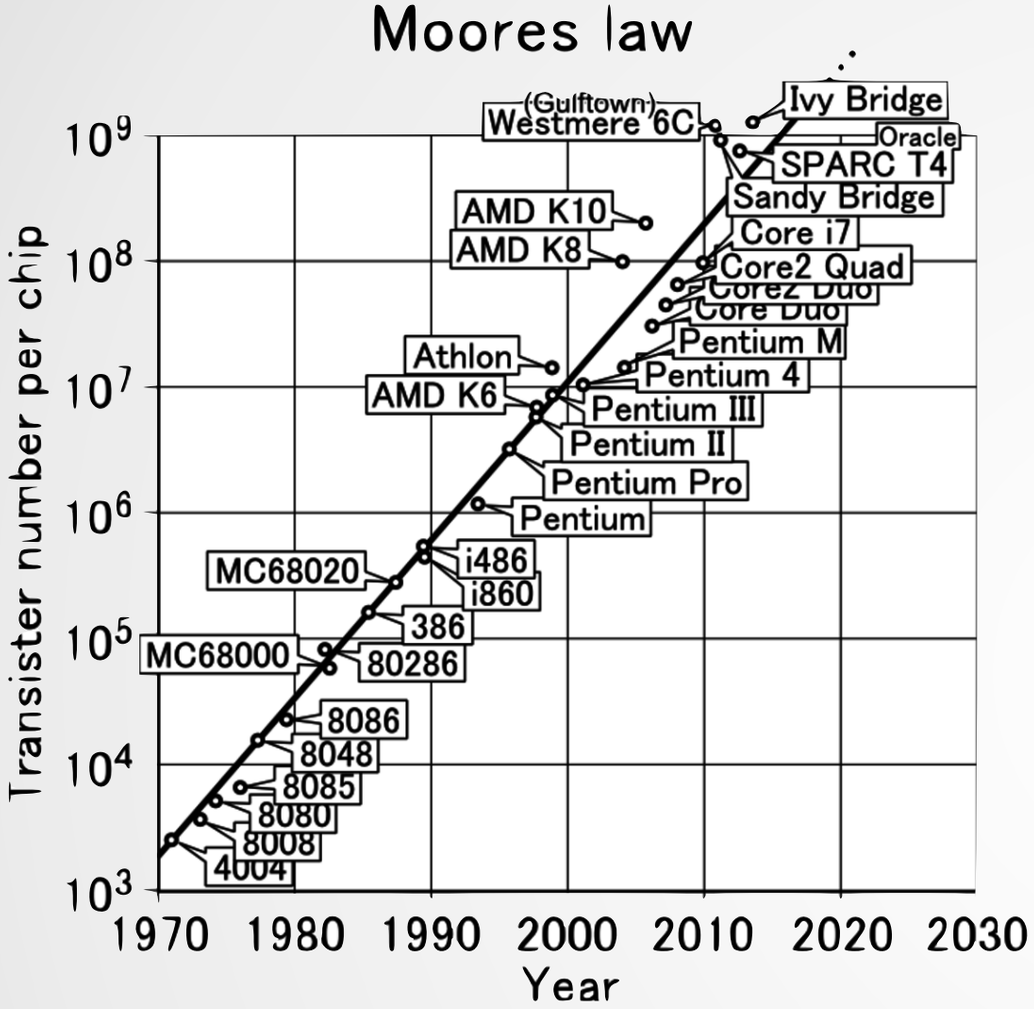
In: h + N_{357}
Out: **0000000**db5e8d544b993a30737eae8112f7df2daa122f7143a74821bb315b911

$$\mathbf{h}_{BTC} = \mathbf{H}_{BTC}\,(\,\mathbf{m}_{Prevhash+Timestamp+List\ of\ transactions} + \mathbf{N}) \leq \mathbf{t}$$

Pooling of Computational Power

Bigger Hashrate = Faster possibly fitting results / hashes

Different systems: e.g. evenly split reward amongst the participants, or via listing.



- „Cray 2“ fastest supercomputer: 1985-1990
- 1.9 GFLOPs*

- „Summit“ fastest supercomputer: June 2018
- 200 PFLOPS**

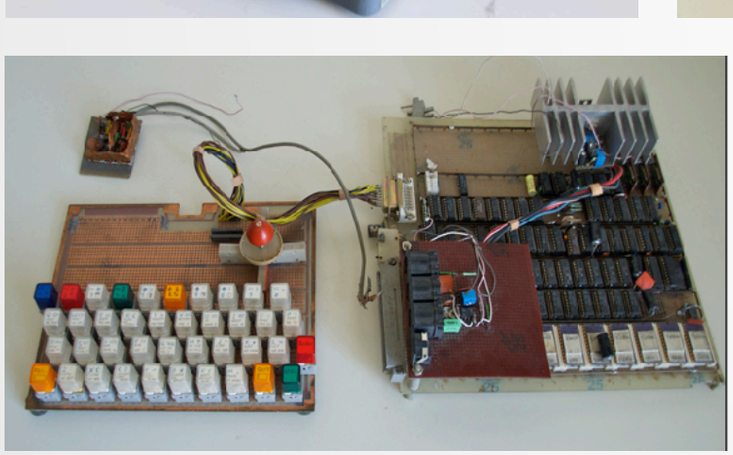
*10^9 **FL**oating point **OP**erations per **S**econd **10^15 FLOPS

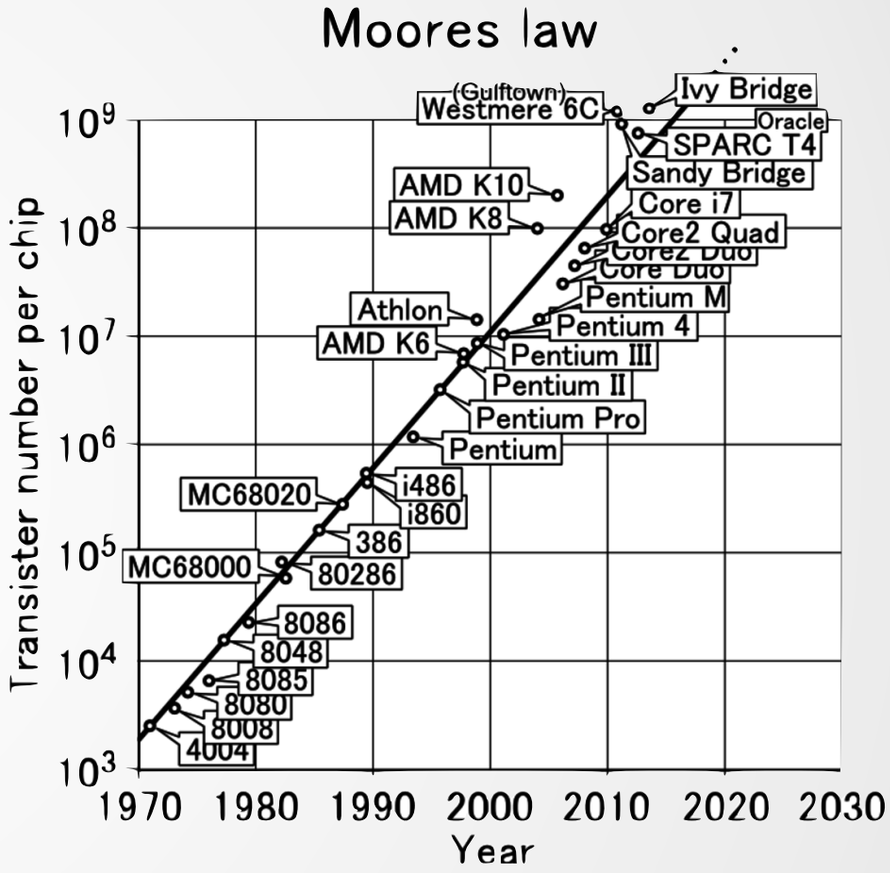
Pooling computing power to outperform more powerful single agents/computers („hash power“)

Rise of the machines

Mechanical calculator MADAS
H.W. Egli S.A., Zurich, 1965

VEB Röhrenwerk Mühlhausen, 1975
8 digits



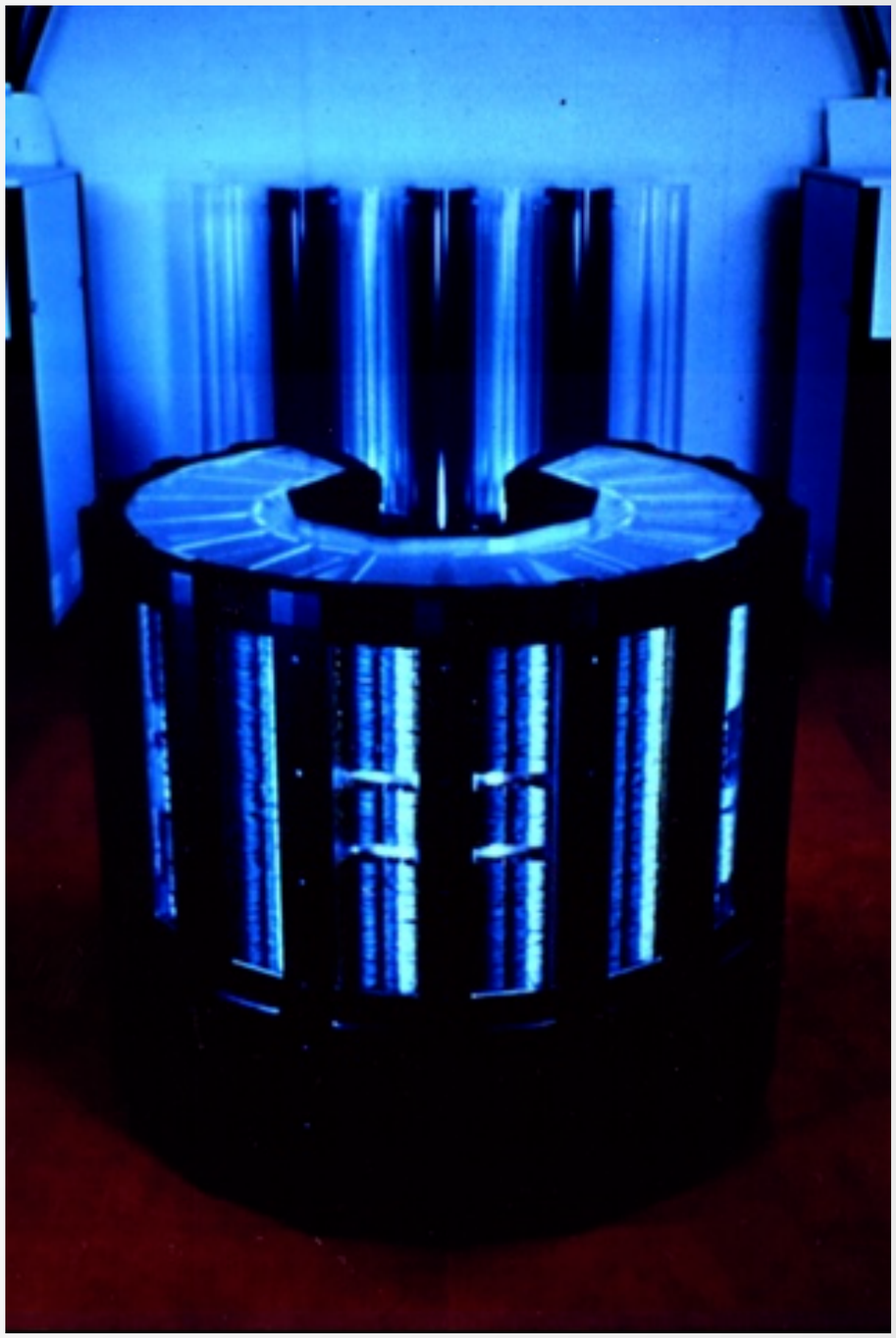


ZX Spectrum East / West 1982

https://phys.org/news/2015-08-silicon-limits-power-electronics-revolution.html

- http://computermuseum.wiwi.hu-berlin.de

- Cray 2 is the world's fastest supercomputer: 1985-1990
- 1.9 GFLOPs*
- 5,500 pounds
- $32 million (current $)
- 舞 锡市 太湖之光, (wu3xi1shi4tai4hu2zhi1guang1) 95 PFLOPS**

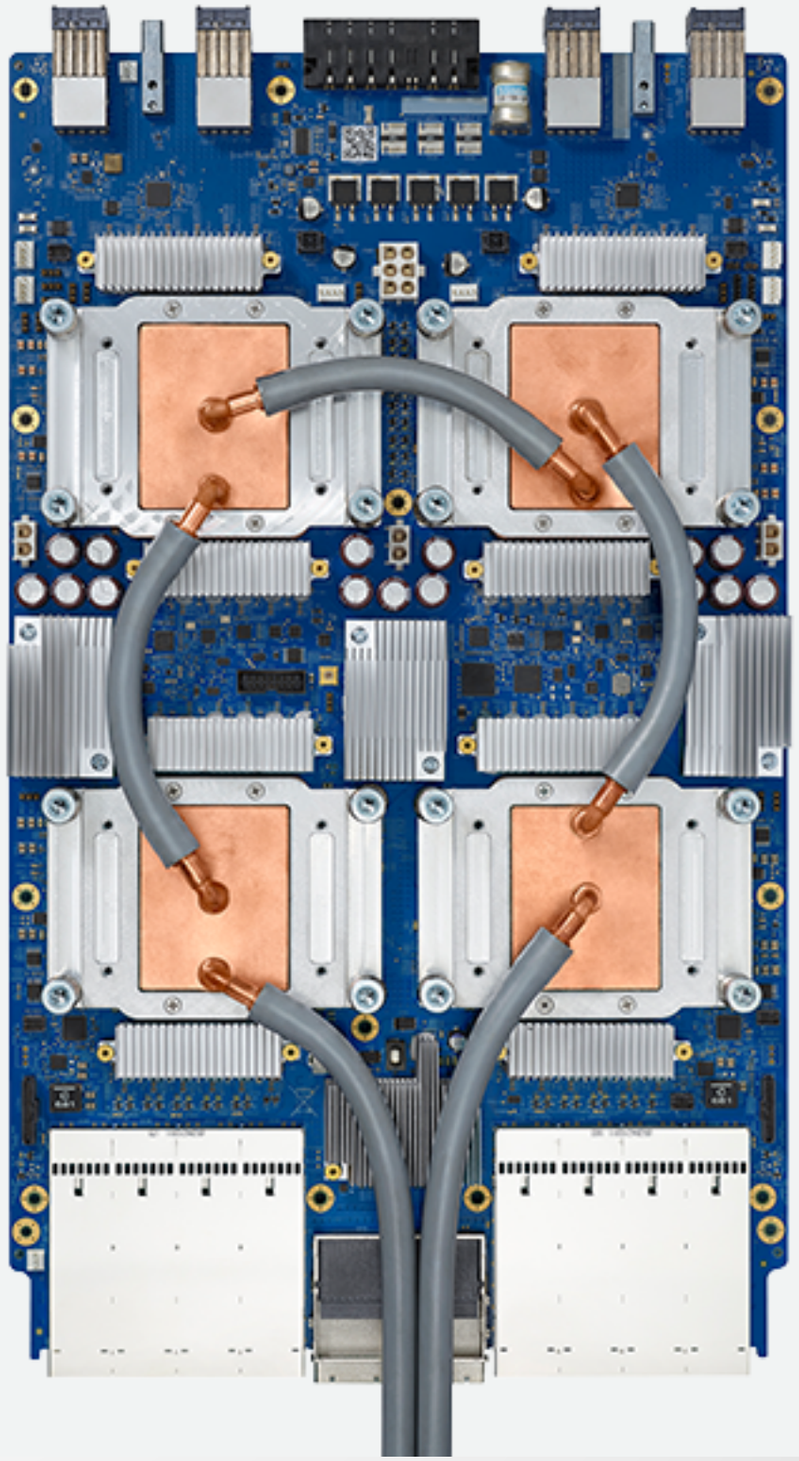


*10^9 FLoating point OPerations per Second **10^15 FLOPS

- 2016 iPhone 7* , 178 GFLOPs
- 2019 iPhone XS Max* , 1300 GFLOPs
- A12 Bionic Chip w/ Neural Engine, 256 GB storage
- 138 g
- 1.3 K EUR

*A10 Fusion. The Apollo guidance system had only 4K of RAM.

- 2017 Nvidia Titan Xp
- 125 TFLOPs, 16 GB
- 1.1 K USD
- ASICS, Antminer
- Google’s Tensor Processing Unit (TPUv2)
- 180 TFLOPs, 64GB per TPU
- TPUs important for MLE*



*MLE = „Maximum Likelihood Estimation“ (age>=45)
MLE = „Machine Learning in Economics“ (age<=45)

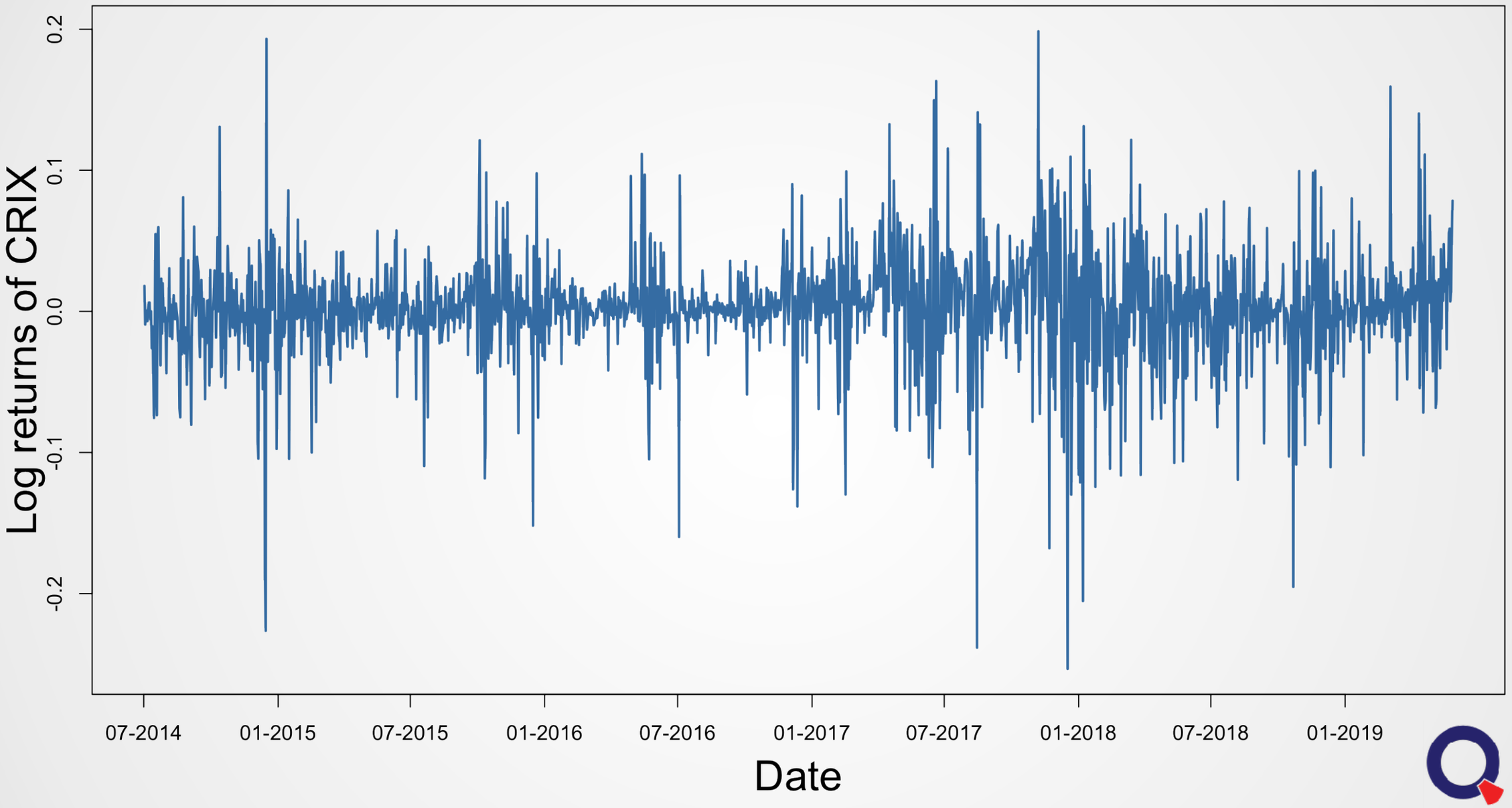
- **Bitcoin (BTC) = leader, proof-of-work**
  (also XBT, as the abbrv. BTC violates ISO 4217 in regards to the Kingdom of Bhutan's Ngultrum, BTN)

- **Ethereum (ETH) = different system & proof-of-stake**

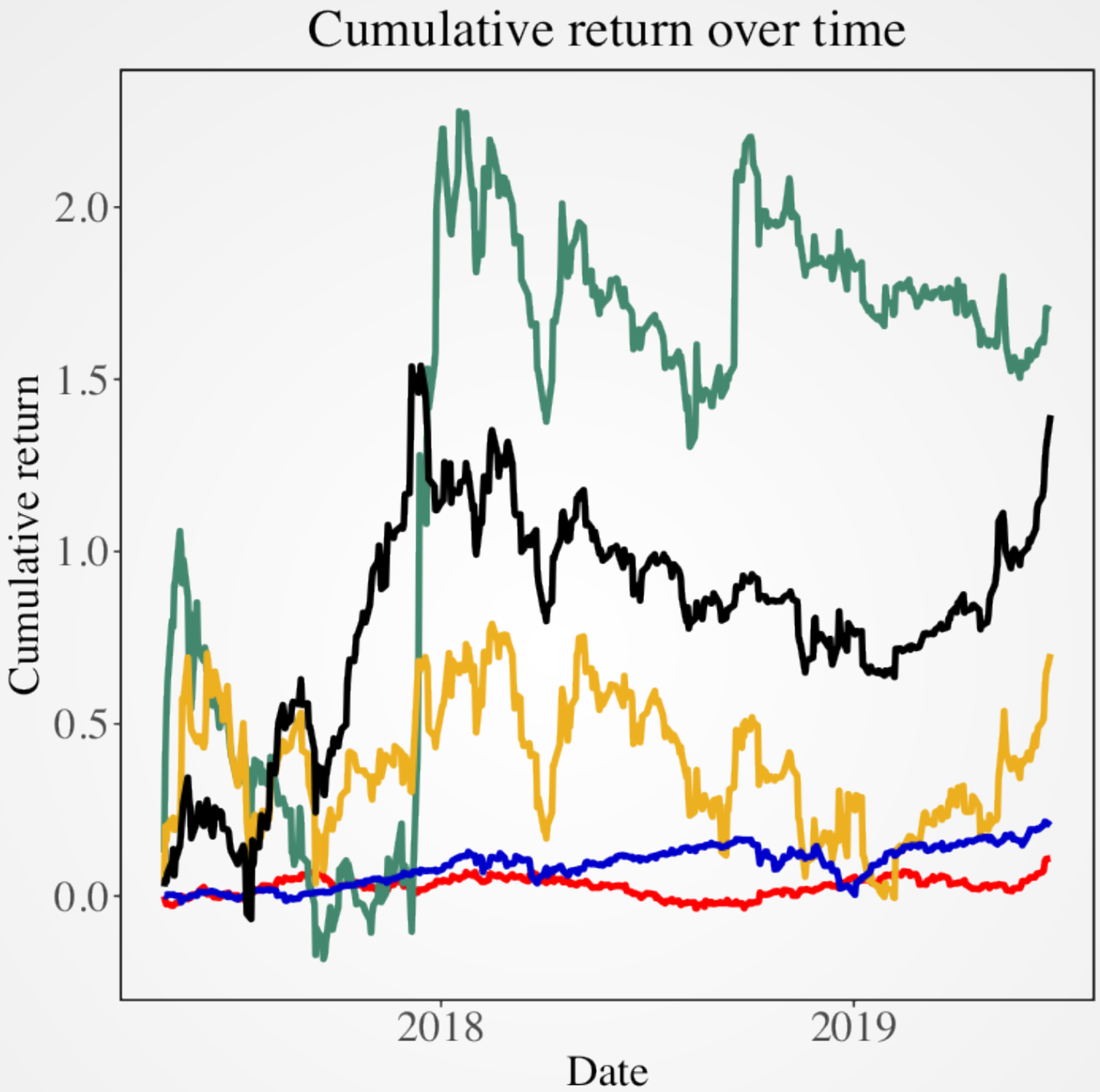
- Ripple (XRP) = target group are bankers
- Litecoin (LTC) = better clone of BTC

- **CC systemic risk** (historical/systemic), high **illiquidity** (market share, maturity, acceptance and trading volume) or not secure

Cryptocurrency markets



CRypto currency IndeX thecrix.de crix.berlin



Cumulative return over time between May 1, 2017 and Jun. 26, 2019 of BTC, XRP, ETH, GOLD and S&P 500.

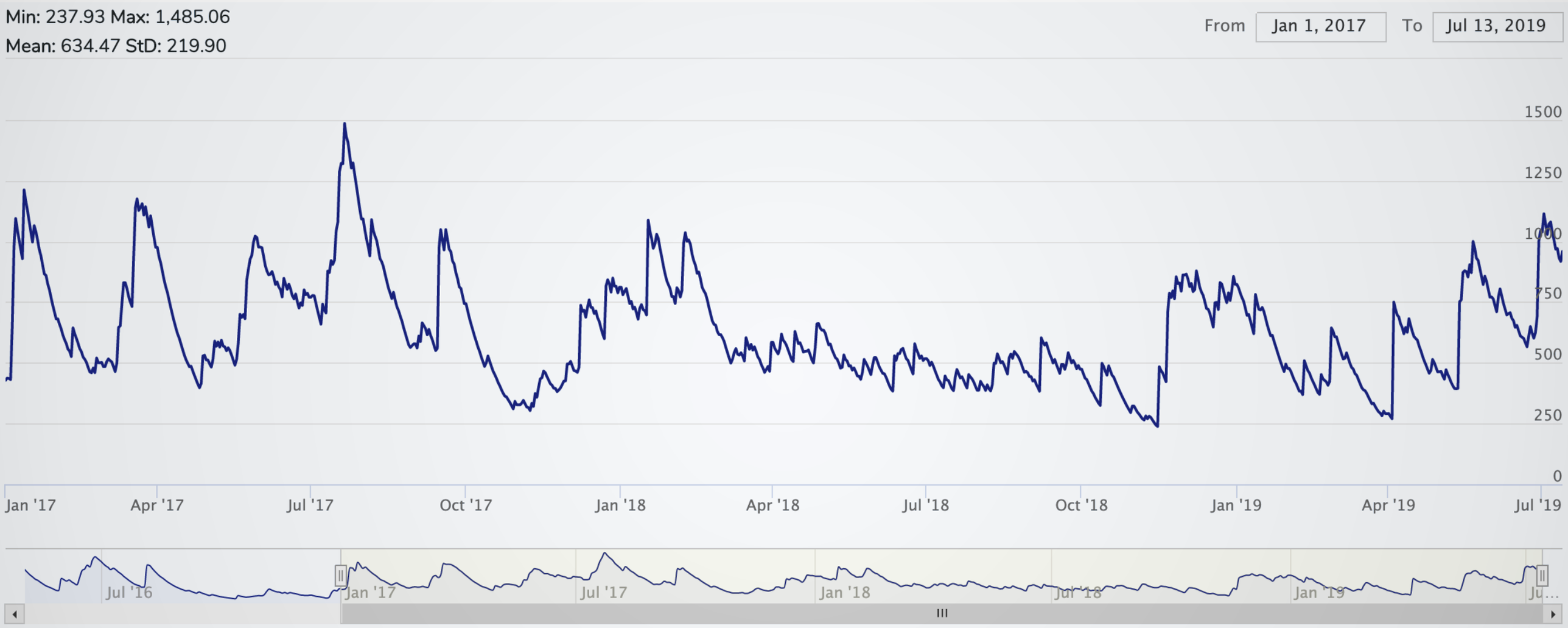
Daily	BTC	ETH	XRP	GLD	SP500	VIX
BTC		0.42	0.21	0.04	0.04	-0.06
ETH	0.42		0.20	0.06	0.01	-0.01
XRP	0.21	0.20		0.04	-0.01	-0.02
GLD	0.04	0.06	0.04		-0.15	0.13
SP500	0.04	0.01	-0.01	-0.15		-0.80
VIX	-0.06	-0.01	-0.02	0.13	-0.80	

Daily Correlation 2016-2019

	BTC	ETH	XRP	GLD	SP500	VIX
BTC		0.48	0.45	0.08	0.13	-0.08
ETH	0.48		0.58	0.26	0.12	-0.19
XRP	0.45	0.58		0.15	-0.08	0.02
GLD	0.08	0.26	0.15		-0.10	0.17
SP500	0.13	0.12	-0.08	-0.10		-0.75
VIX	-0.08	-0.19	0.02	0.17	-0.75	

Monthly Correlation 2016-2019

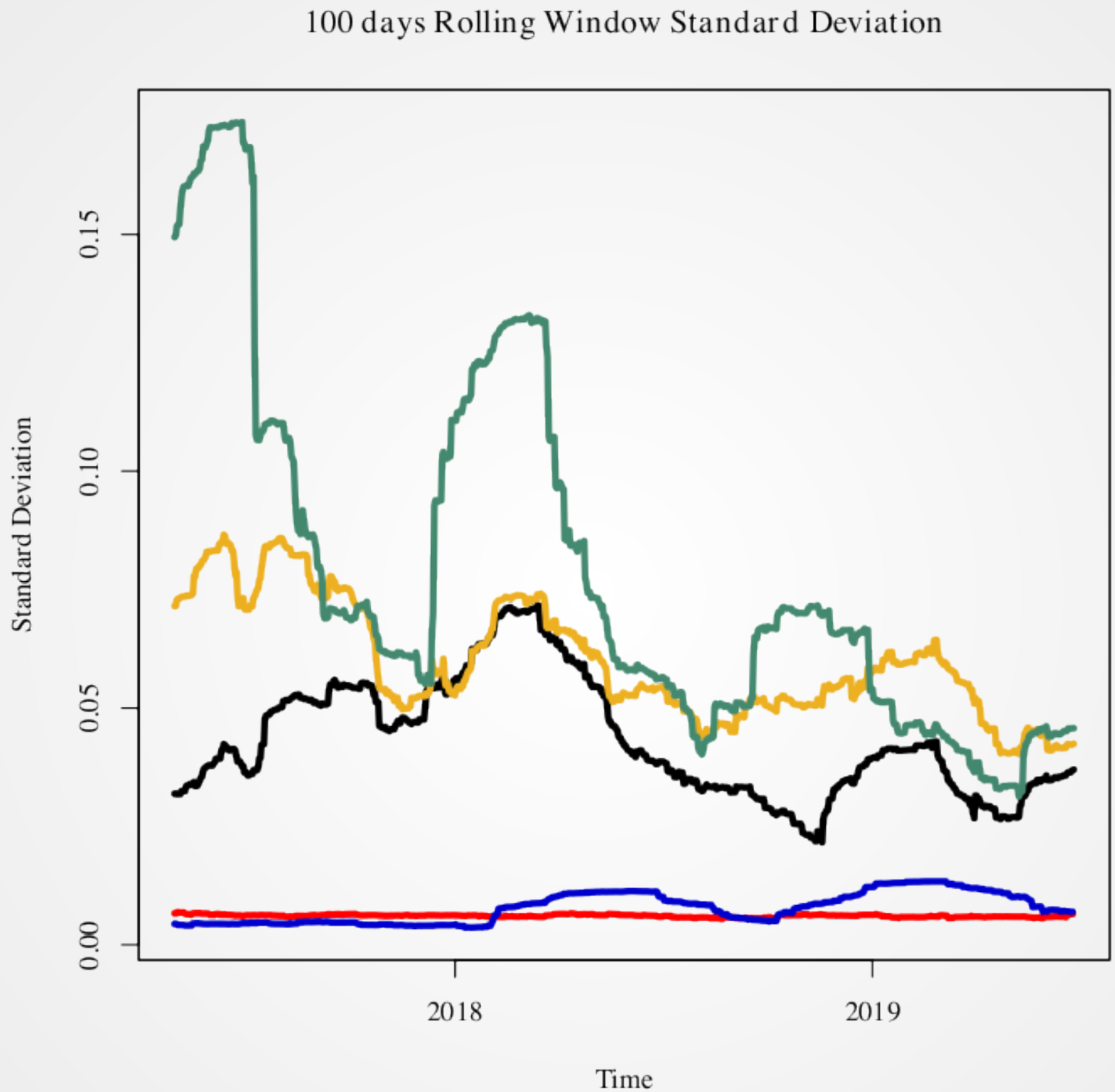
CRIX monthly aggregated returns volatility (VCRIX)
as an analogue to VIX for cryptocurrencies



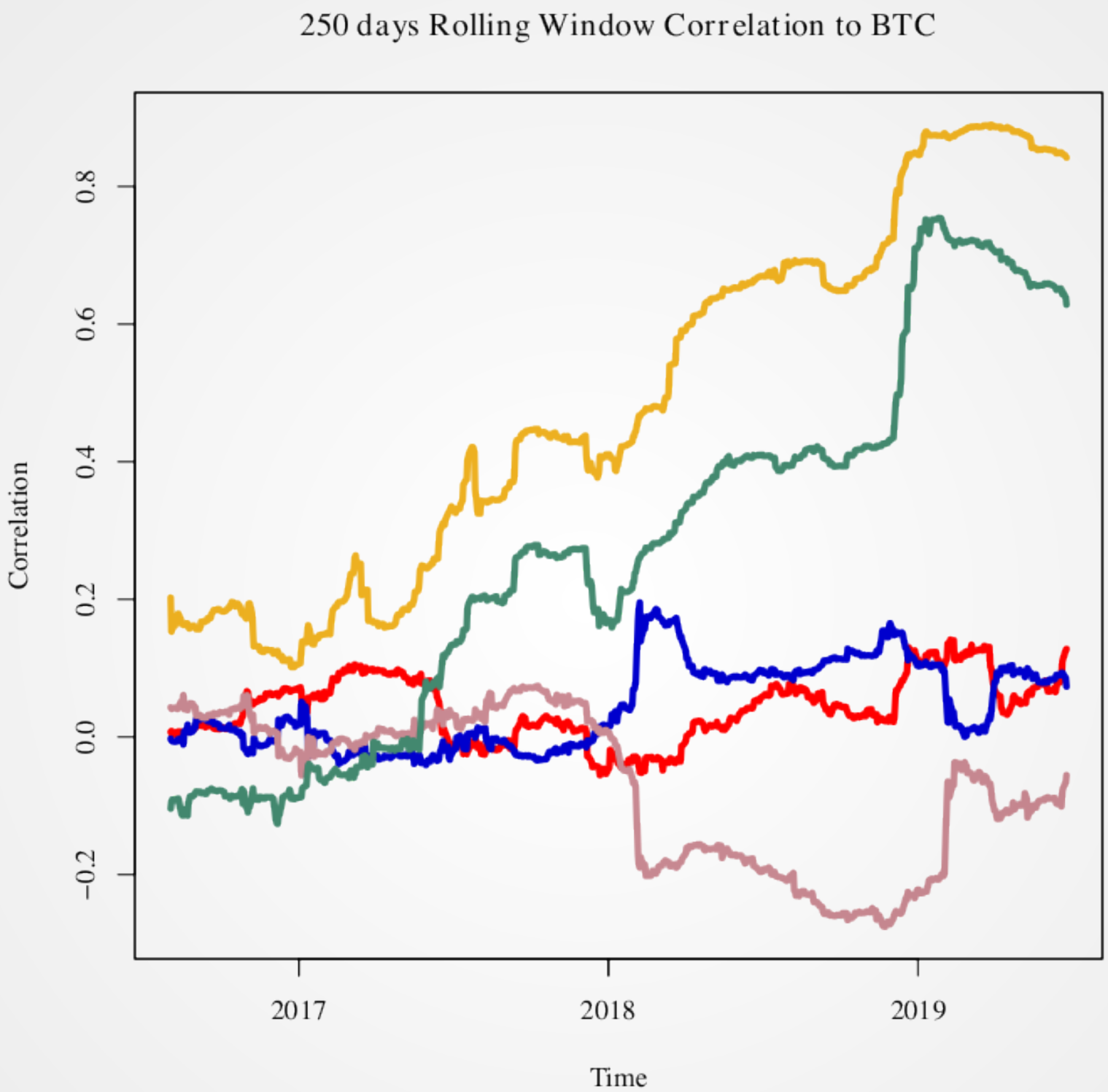
Monthly aggregated returns volatility based on CRIX public JSON data

$$VCRIX = \frac{\sqrt{\sum_i^n w_i \sigma_i^2 + \sum_i \sum_{i \neq j} w_i w_j \sigma_i \sigma_j \rho_{ij}}}{Divisor}$$

VCRIX



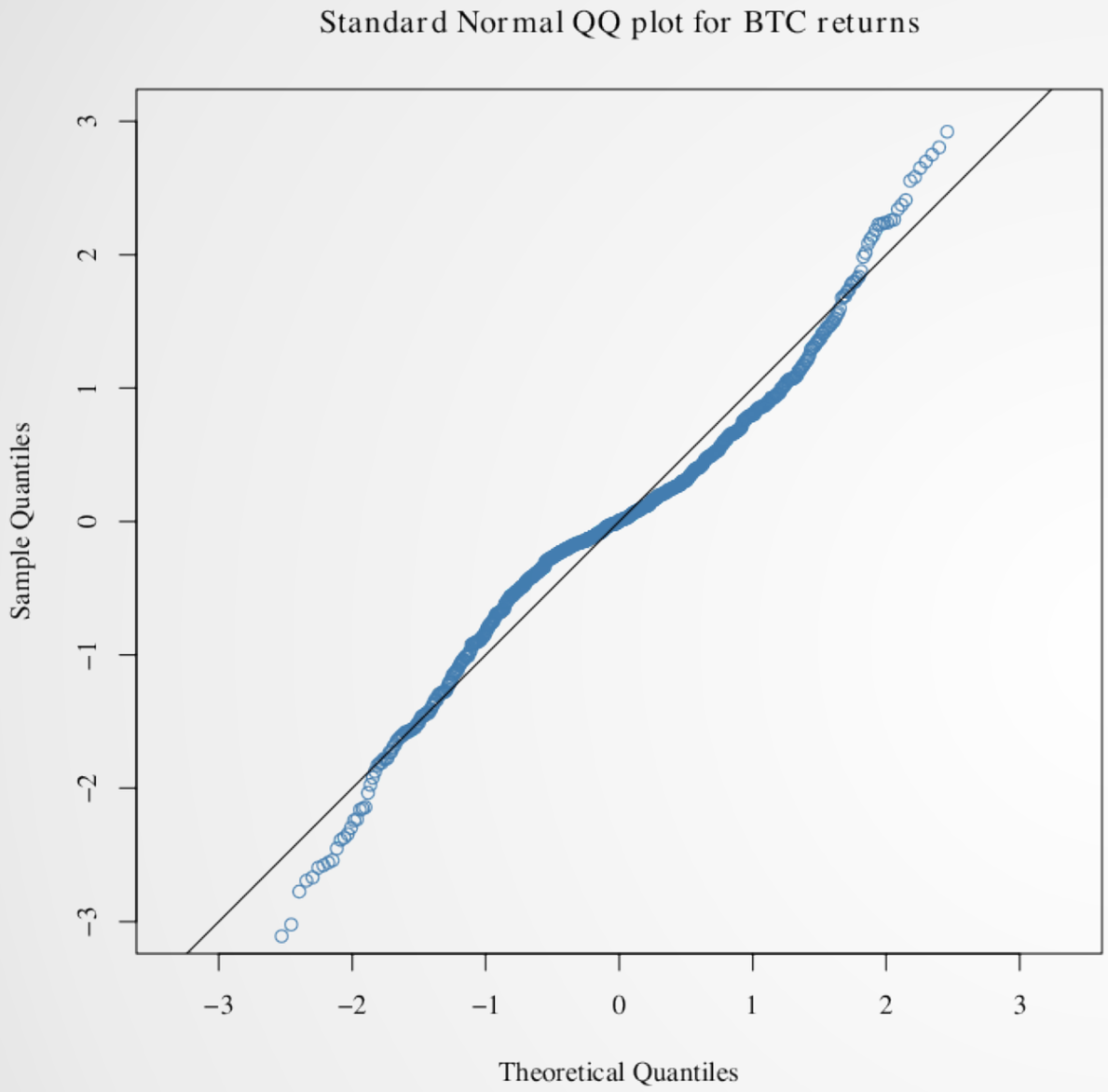
250 days rolling window standard deviation of BTC, XRP, ETH, GOLD and S&P 500.

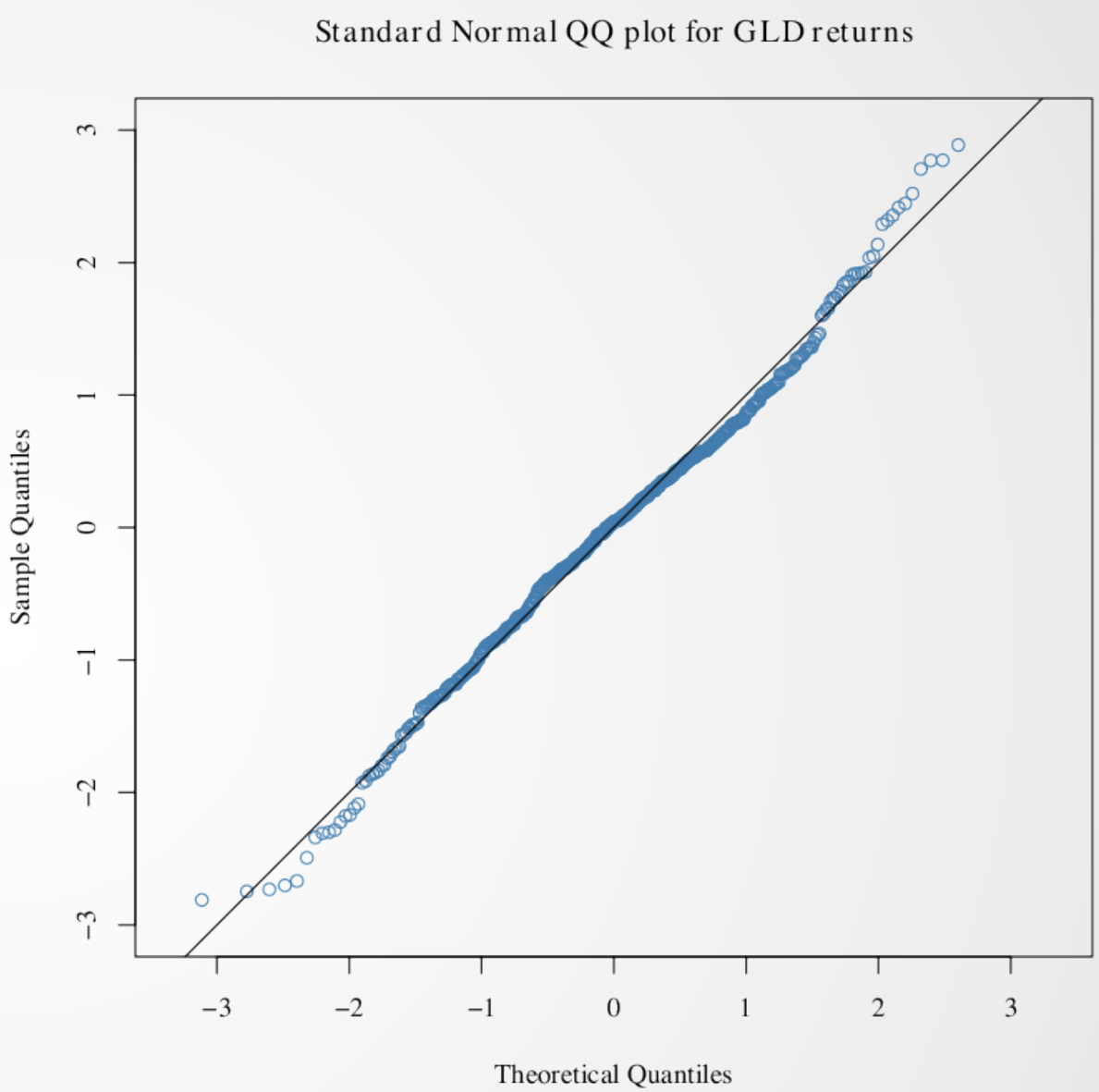


250 days rolling window correlation of of XRP, ETH, GOLD, S&P 500 and VIX to BTC.

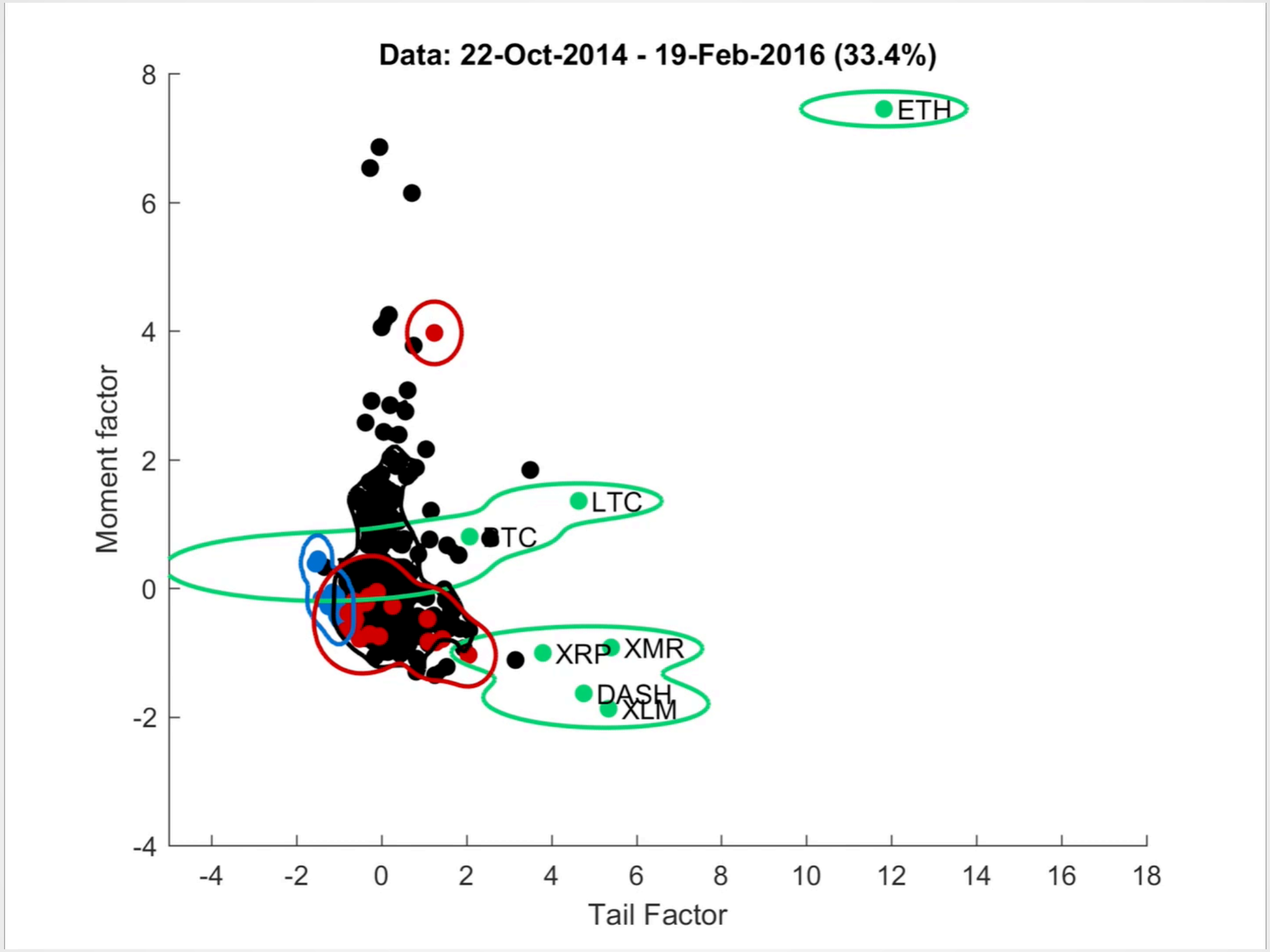
	Mean	Std. Dev.	Skewness	e. Kurtosis	Min.	Max.
BTC	0.0028	0.0454	0.0452	2.8227	-0.1892	0.2276
ETH	0.0019	0.0594	0.1501	2.0517	-0.2228	0.2602
XRP	0.0028	0.0767	1.6053	10.3886	-0.3671	0.6183
GLD	0.0002	0.0062	0.1681	1.0159	-0.0172	0.0254
SP500	0.0004	0.0086	-0.5997	5.1430	-0.0418	0.0484

Log return statistics 2017-2019





Theoretical Quantiles (Standard Normal Quantiles) / Sample Quantiles (Quantiles of Input Sample) of BTC and GOLD (!Weekends cleared) based on 24/7 data.



CC factor analysis

(Heavy-tailedness/Distribution shape)

Research areas

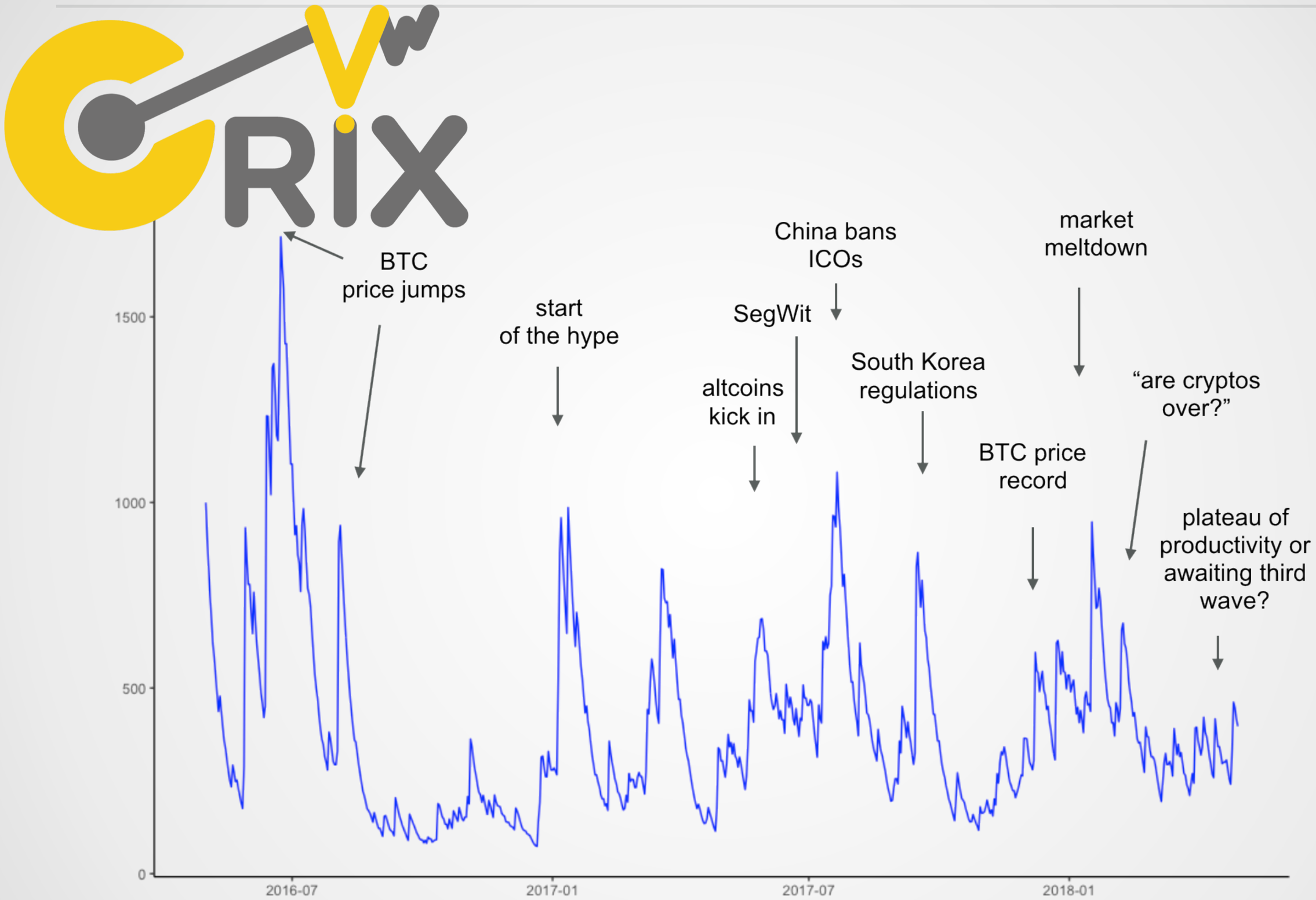
- CC index constructions - CRIX, VCRIX …
- High Frequency Markets - 24/7 data availability
- Specificity for CC markets - Sentiment text mining
- CC Exchanges - Arbitrage possibilities
- Macroeconomy - The role of money and value, ICOs …
- Economic risks - Bubble testing
- Derivative markets - Energy markets and industries
- State reactions - Regulations, Bans …
- Political economy - Public Ledgers …
- Social Sciences - Social Contract Theory …

- CRyptocurrency IndeX / **CRIX**
- CRIX a benchmark index for crypto dynamics
- CRIX as a valuable trading tool providing a benchmark for CCs
- Used by Exchange Traded Funds and Investment funds

crix.berlin, **thecrix.de**

- Econometric Analysis of CRIX (Chen S et al., 2017)
- Crypto Currency (CC) based derivatives emerge
- CRIX dynamics vital for price discoveries
- **VCRIX** a necessary volatility measure
- VCRIX as analogue to VIX from CBOE

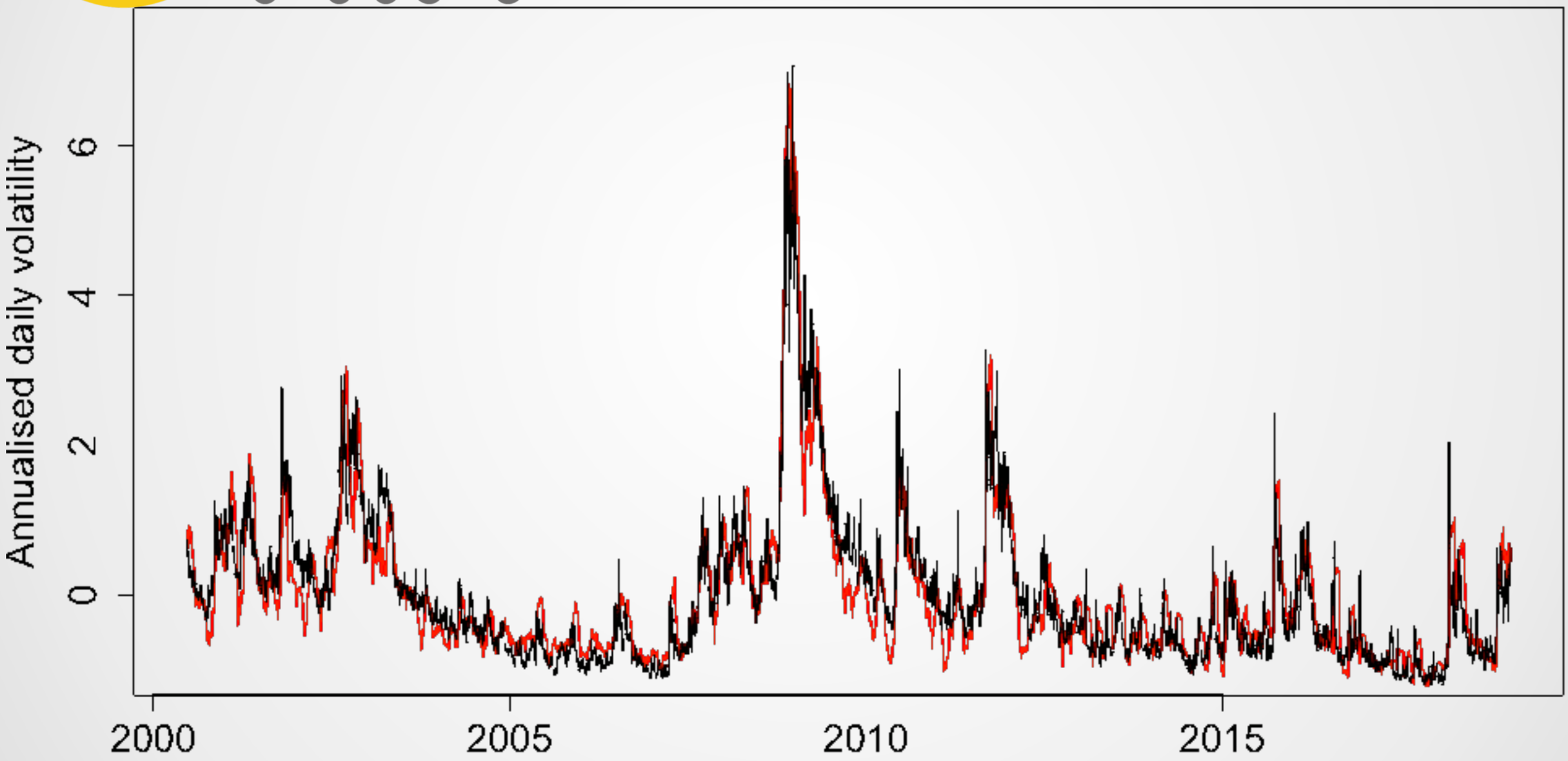
econ_vola



VCRIX

Kim A et al. (2018)

21-day vola S&P 500 ETF (^SPY) for 20 years



Corr(VCRIX_VIX, VIX) = 0.89

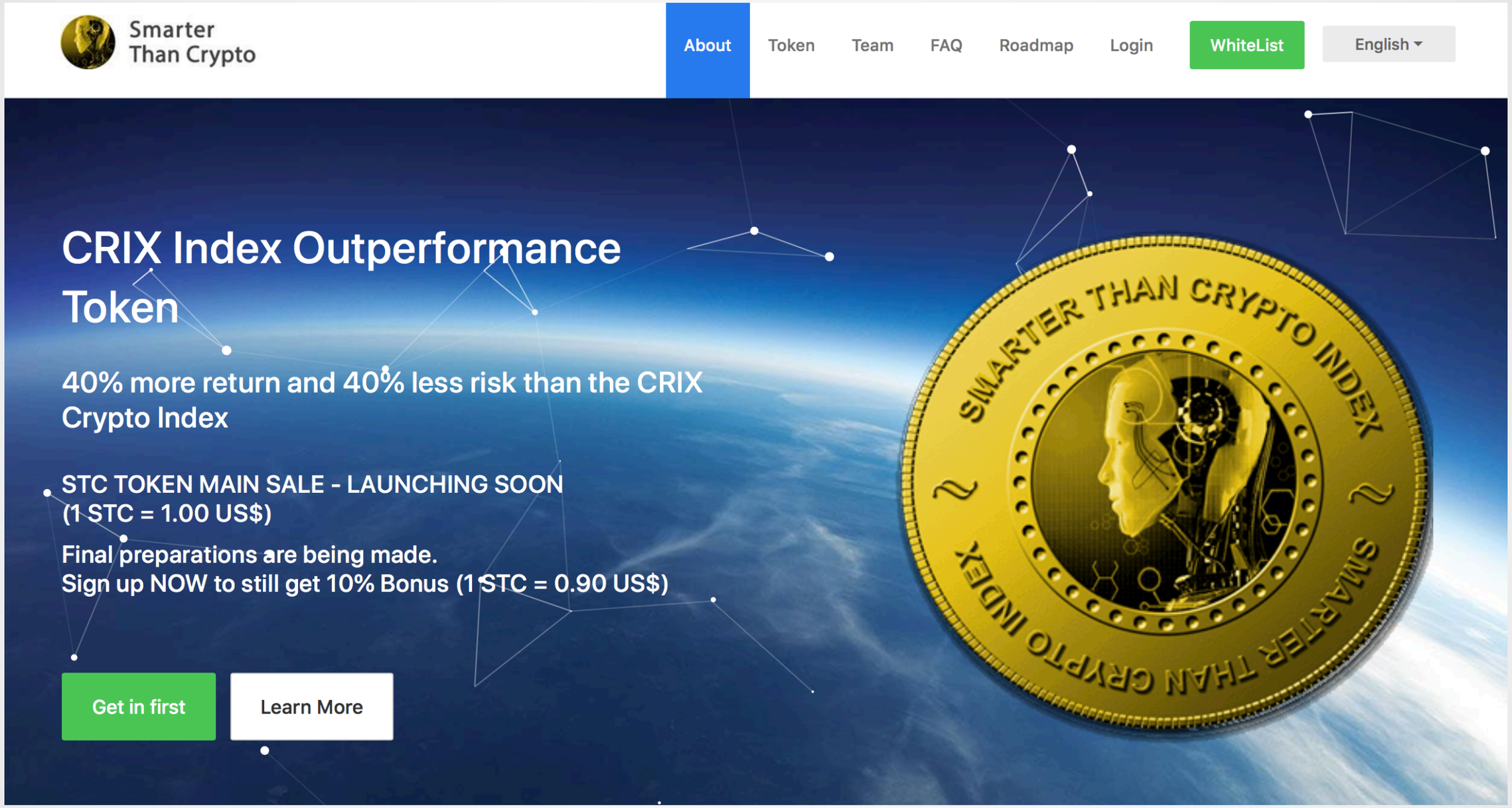
- Option Pricing on CRIX and CCs (Chen CYH et al., 2018)

  as preliminary research to a CC option market

- Stochastic Vola Corr Jump model
- **VCRIX** as a natural component

$$dlogY_t = \mu d_t + \sqrt{V_t} dW_{y,t} + Z_{y,t} dN_t$$

$$dV_t = k(\theta - V_t)dt + \sigma_V \sqrt{V_t} dW_{v,t} + Z_{v,t} dN_t$$



CRIX as reference index for (portfolio) trading tokens

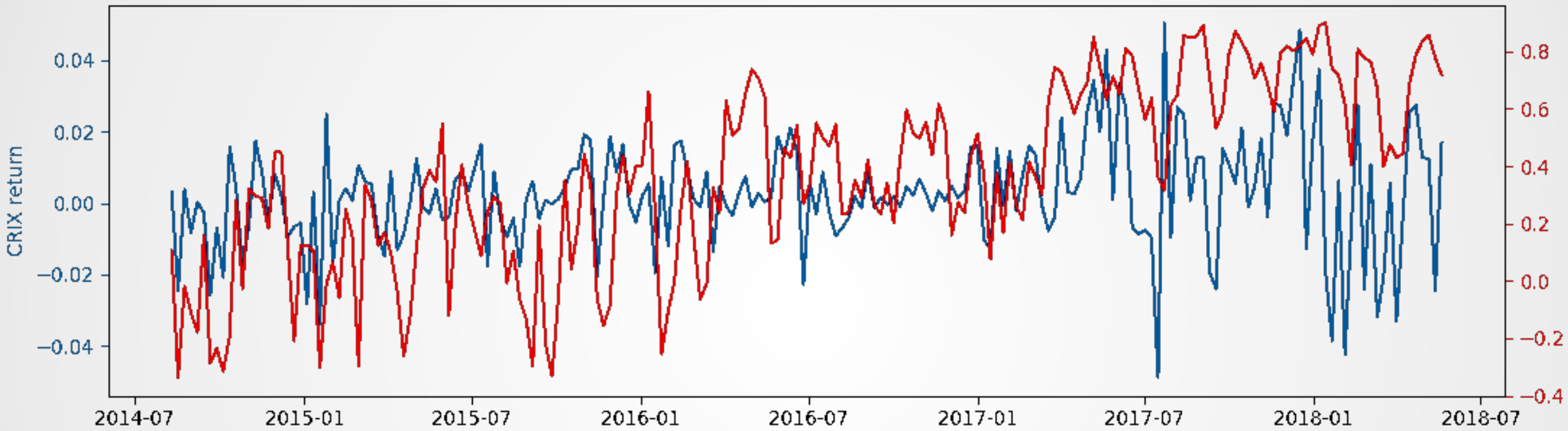
Network design, sentiment, and valuation

- Trading patterns
- Herding effects
- Efficiencies/Failures

  in markets of unprecedented fragmentation

- Economic decision making
- Networks and marketplaces

CRIX and sentiments



Daily CRIX log-return, Daily stock twits sentiment
201407 - 201807

Prediction of CC market movements through investor sentiment derived from social media

Chen CYH et al. (2018)

Term	Sentiment weight
🚀	0.90
hodl	0.54
hodl !	0.85
hackers	−0.74
miner	0.62
bitcoin 😂	−0.73
scam	−0.77
~~fuckingscam~~	−0.86

Crypto specific terms

Emojis and Sentiment Scales 🐿️ 📈

- Tweets data is not in standard language
- **Emojis** appear more and more, especially in personal tweets
- Hard to quantify affective states and subjective information in some cases without emojis
- With emojis, the analysis results might be upside down different

Ni X (wip)

Monetary systems and financial development

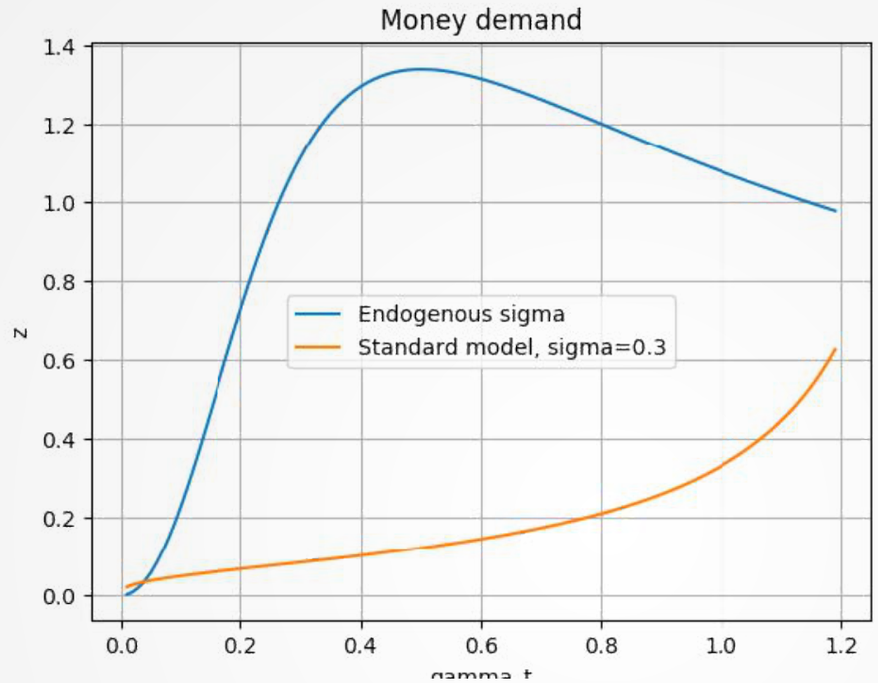
- BC-based monetary system currency provision and currency competition
- Disrupture of the financial institutions and the system of payments (also “Banking the Unbanked”)
- Change in monetary and financial stability questioning the role of central / commercial banks and state / commercially lead financial institutions (Central Bank Digital Currencies, CBDC)

Petro

Petromoneda, Venezuela

Macroeconomics of blockchains

- Endogenous Trade Probability and Hump-shaped Money Demand

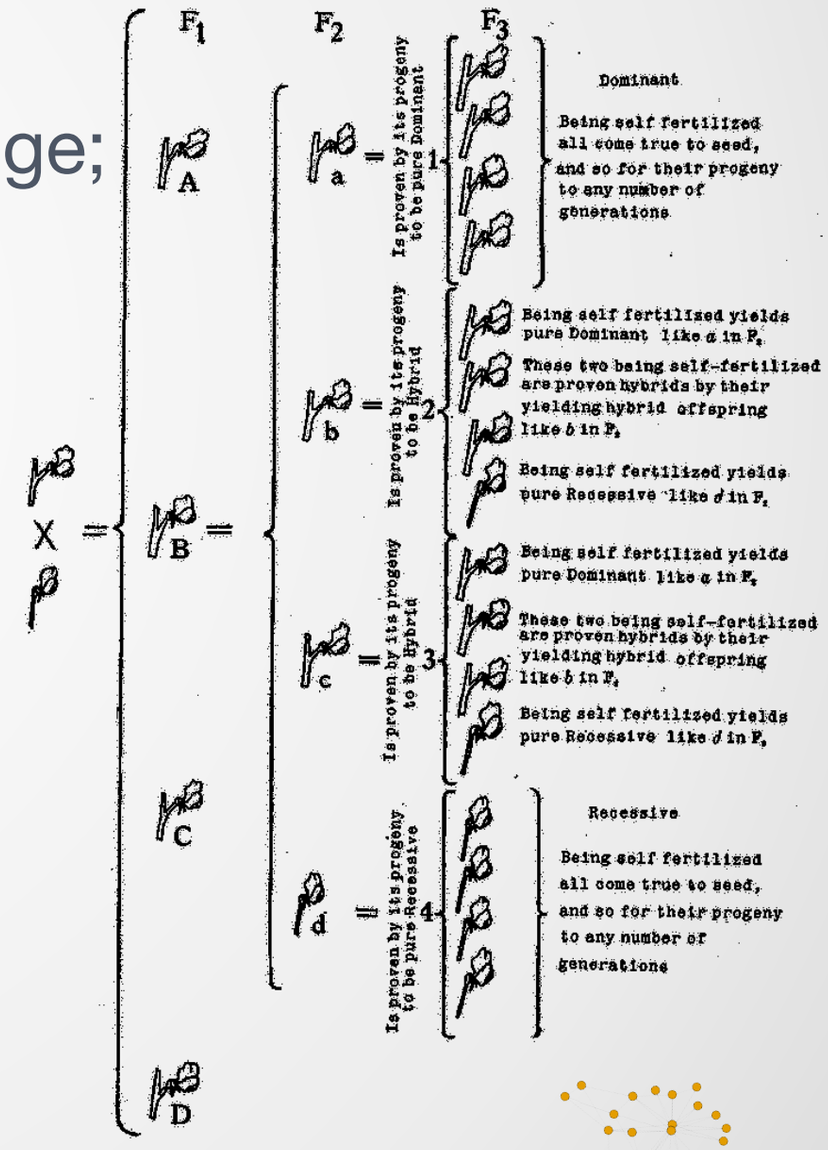


- Steady State Return on Money as a Function of Mining Costs and Rewards
- Cryptocurrency Competition

Almosova A (2018)

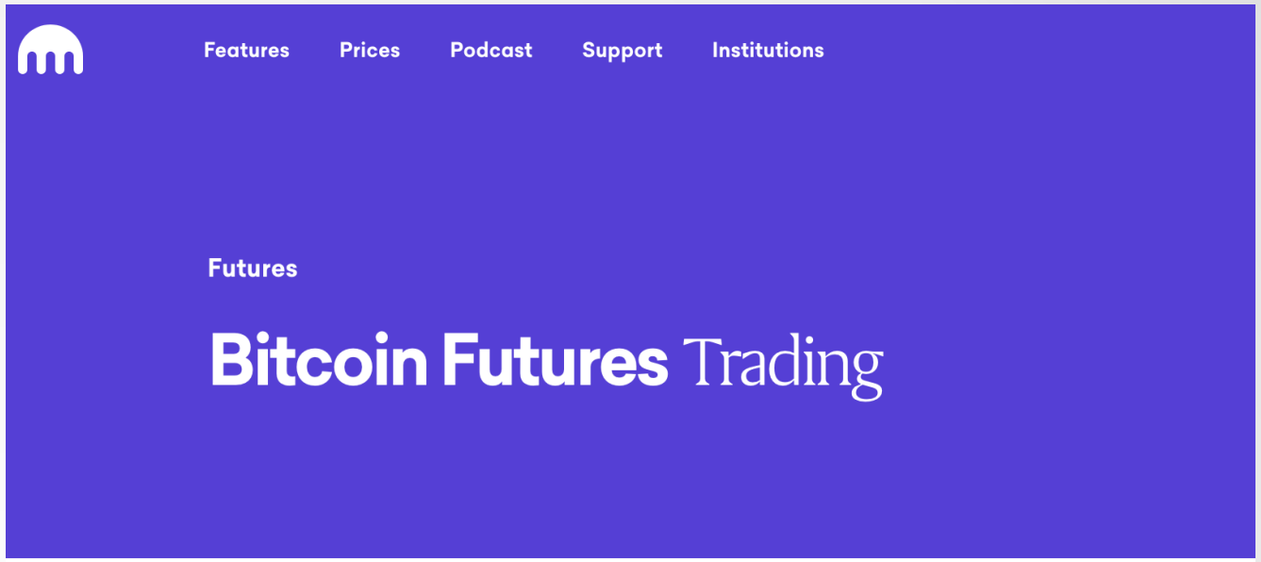
Markets, price discovery and high-frequency data

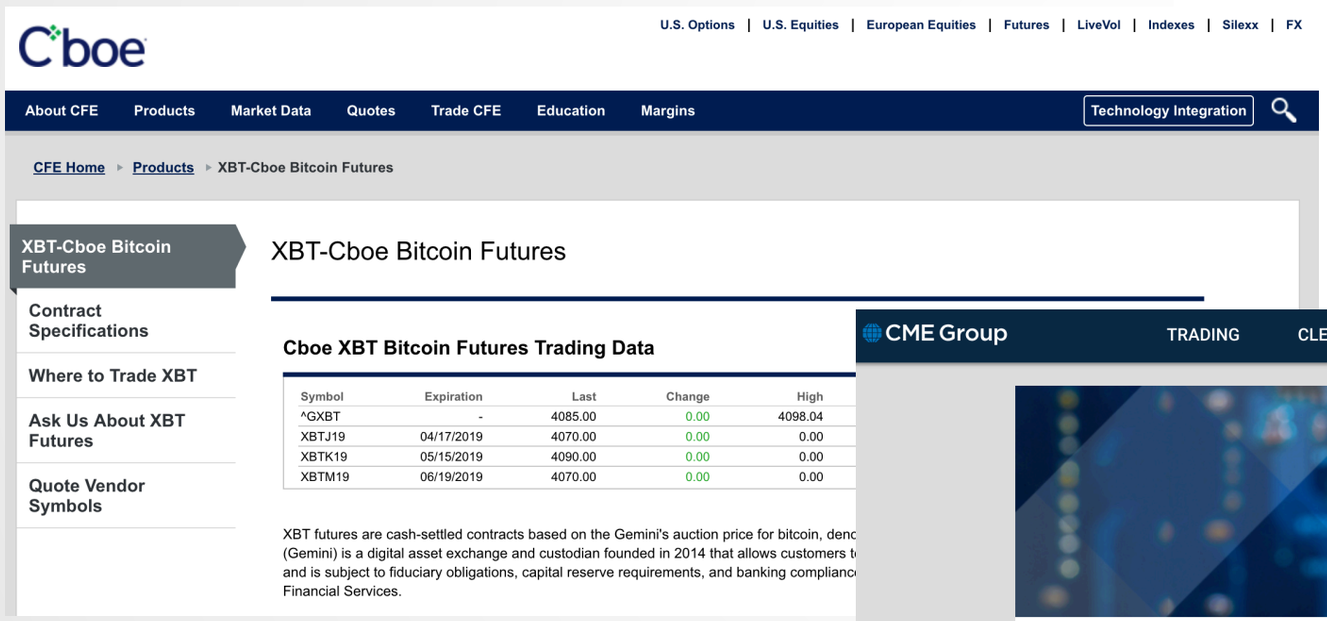
- Hundred of CC exchanges,
  (Binance, Bitfinex, Kraken etc.)
- Specialisations
  (e.g. Kraken is the biggest CC-EUR exchange;
  Gemini being fully US-regulated)
- Arbitrage Opportunities
- Fake trading volumes
  (SEC found only 10 out of 81
  BTC exchanges with actual volume)



Cryptocurrency Futures

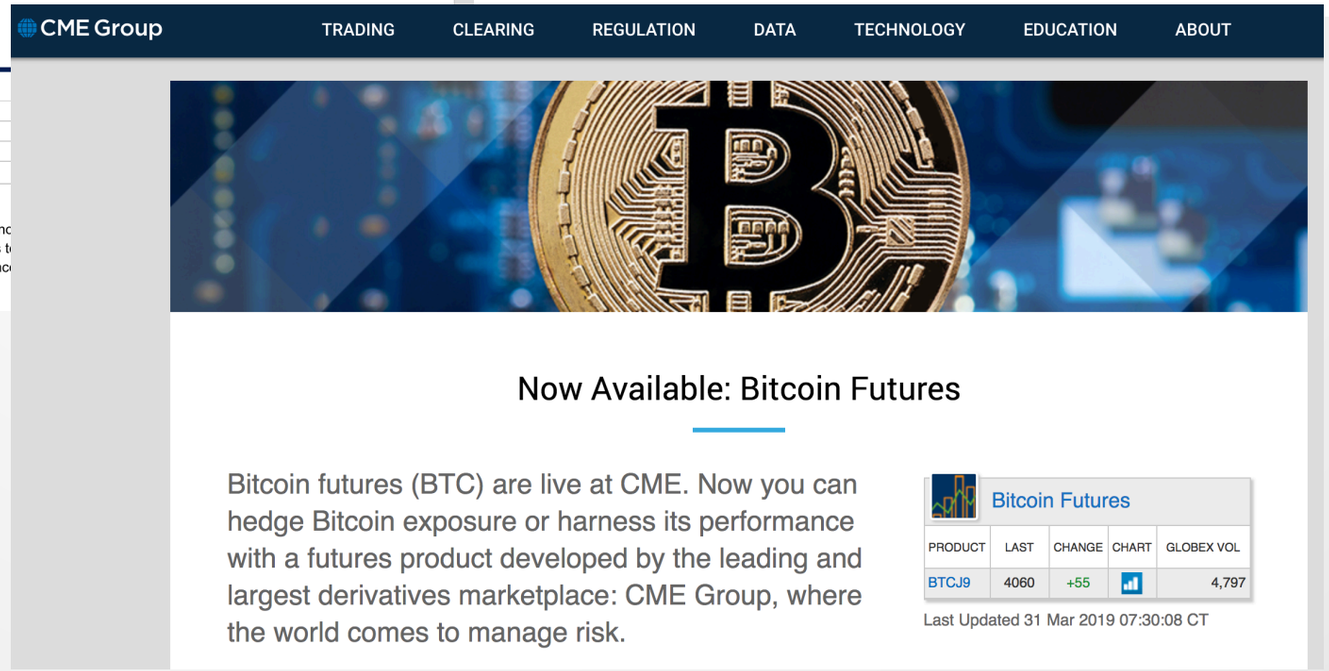
- CME
- CBEO
- Exchanges (e.g. Kraken)



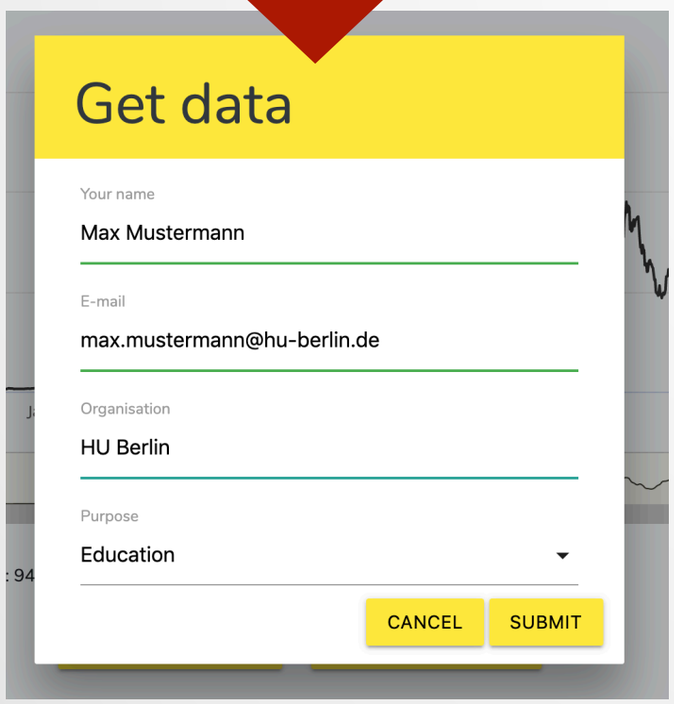


Next Level Trading with Cryptocurrency Futures

Bitcoin and digital assets are volatile investments. Many traders attempt to manage their risk simply by buying an asset when the price drops or selling it when the price goes up. The downside of this tactic is that oftentimes money is left on the table after you leave the market. If the price continues to rise after you sell, for example, you're missing out on profits you could've earned had you left your position open. A key benefit of futures trading is that you can hedge existing spot



High-frequency data



You are now a member of the CRIX-Network

Congratulations Max Mustermann!

You are now a member of the CRIX-Network. As such, you will have permanent access to the latest data available. Below you can find the access-link to the indexes data in several formats. Please Note, that the files containing the data are updated regularly and can easily be accessed by our members through opening the link provided below:

JSON

CRIX closing data

CRIX 24h data

VCRIX closing data

CSV

CRIX closing data

VCRIX closing data

Need help? Feel free to contact us any time.
Sincerely, CRIX-Team

crix.berlin, thecrix.de

Bubbles

- **Phillips et al., 2011**
  Biased in the presence of non-stationary volatility.

- **Harvey et al., 2015**
  For cryptocurrencies we may expect volatilities to be nonstationary for various reasons, one of them being the typically high volatility shortly after the initial coin offering (ICO) and a possible decline once the crypto is becoming more mature and accepted as a payment medium.

- **Hafner, 2018**
  Empirical application using eleven of the largest cryptocurrencies and the CRIX index. General evidence in favor of bubbles is confirmed, but much less pronounced than under constant volatility.

A bubble of hot glass

...

Portfolio diversification

Cryptocurrency	F-Test	F-Test1	F-Test2	Cryptocurrency	F-Test	F-Test1	F-Test2
aur	1.66	2.96	0.36	nav	1.69	2.88	0.49
	(0.19)	(0.09)	(0.55)		(0.19)	(0.09)	(0.48)
btc	4.97	9.41	0.52	neos	2.54	4.87	0.20
	(0.01)	(0.00)	(0.47)		(0.08)	(0.03)	(0.66)
btcd	3.77	4.74	2.75	nxt	2.43	4.70	0.16
	(0.02)	(0.03)	(0.10)		(0.09)	(0.03)	(0.69)
btm	2.04	3.21	0.87	pot	1.96	3.37	0.55
	(0.13)	(0.07)	(0.35)		(0.14)	(0.07)	(0.46)
bts	5.44	9.75	1.10	ppc	2.00	2.86	1.13
	(0.00)	(0.00)	(0.30)		(0.14)	(0.09)	(0.29)
burst	1.95	3.86	0.04	spr	3.18	2.16	4.19
	(0.14)	(0.05)	(0.84)		(0.04)	(0.14)	(0.04)
cann	3.18	3.80	2.54	sys	3.23	6.45	0.02
	(0.04)	(0.05)	(0.11)		(0.04)	(0.01)	(0.90)
dash	5.92	11.12	0.70	uno	1.50	2.86	0.14
	(0.00)	(0.00)	(0.40)		(0.23)	(0.09)	(0.71)
dgb	1.87	3.71	0.04	via	3.04	5.33	0.75
	(0.16)	(0.06)	(0.85)		(0.05)	(0.02)	(0.39)
dmd	1.80	3.59	0.00	vtc	4.81	9.06	0.54
	(0.17)	(0.06)	(0.95)		(0.01)	(0.00)	(0.46)
doge	1.76	3.28	0.23	xmg	1.92	3.70	0.15
	(0.17)	(0.07)	(0.63)		(0.15)	(0.06)	(0.70)
emc2	3.84	7.48	0.20	xmr	1.53	3.04	0.03
	(0.02)	(0.01)	(0.66)		(0.22)	(0.08)	(0.85)
ftc	2.35	3.03	1.66	xrp	3.50	6.45	0.54
	(0.10)	(0.08)	(0.20)		(0.03)	(0.01)	(0.46)
ltc	3.48	6.66	0.29	xst	3.07	3.54	2.58
	(0.03)	(0.01)	(0.59)		(0.05)	(0.06)	(0.11)

CCP

Spanning Test for Cryptocurrencies Effect on Portfolios Constructed from Traditional Investment (p-value is given in brackets)

Petukhina A et al. (2018)

Alternative methods to raise capital

ICOs as grand scale crowd funding

Coins or Tokens - „CCs IPOs“

Blockchain Nights #1, #2, #4, #5 - **blockchainnights.com**

Porsche, Volkswagen and Daimler introduce blockchain to cars

collaboration with the Berlin-based XAIN.io

XAIN.

The role of energy in consensus mechanisms

Country	Systems
China	206
United States	124
Japan	36
United Kingdom	22
Germany	21
France	18
Netherlands	9
Korea, South	7
Ireland	7
Canada	6
Australia	5
India	5
Italy	5
Poland	4
Russia	4
Saudi Arabia	4
Switzerland	3
Sweden	3
Singapore	2
Spain	2
South Africa	1
Taiwan	1
Norway	1
Brazil	1
New Zealand	1

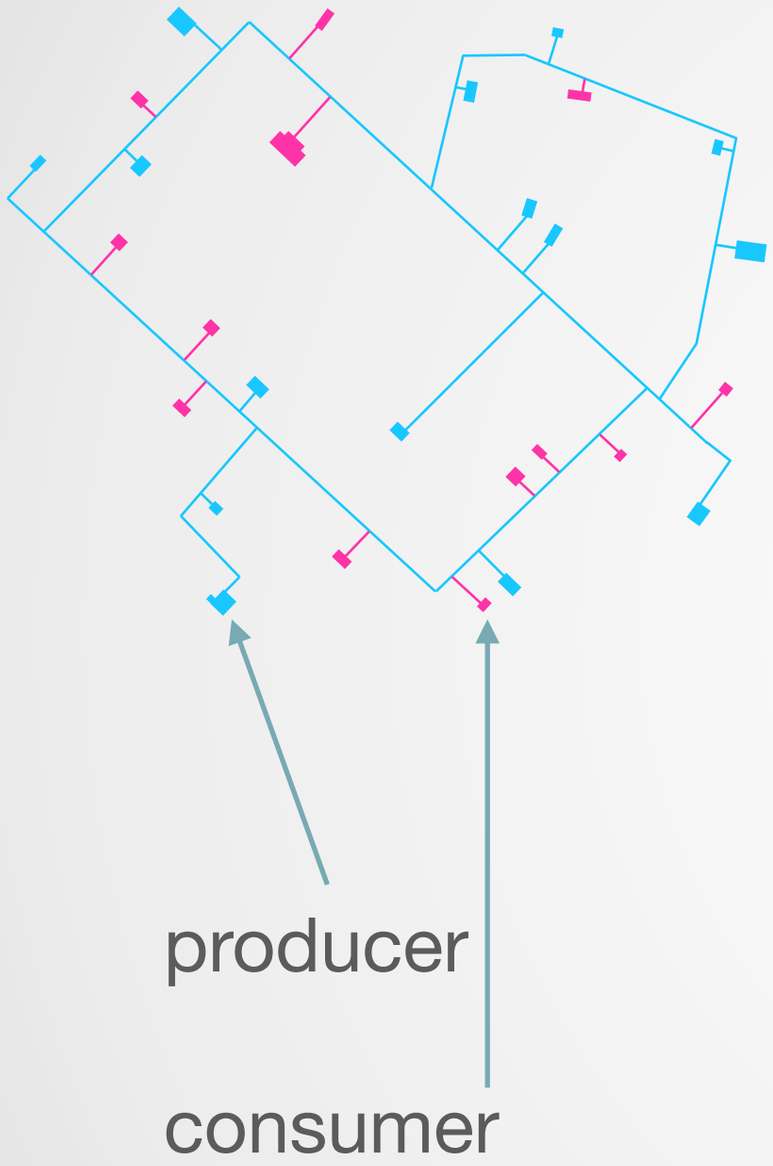
Supercomputers

China mines most Bitcoins and therefore “exports” the most bitcoins.

Electricity in China is very cheap and allows Bitcoin miners to gain a large hash power (computing power).

China is home to many of the top Bitcoin mining companies: F2Pool, AntPool, BTCC, and BW.

Energy trading is implemented through smart contracts on a DLT



- Every smart grid participant has a **smart meter**
- A **smart contract** matches supply and demand bids through an **auction**
- The smart contracts **settles financial transactions** according to the actual readings

Kostmann M (2018)
Mengelkamp E et al. (2017)

Grand-Scale Adaptions

- XRP TipBot
  Already usable via MS Outlook, Reddit, Twitter, Discord and Googlemail to e.g. grant κῦδος to other users (to tip them).

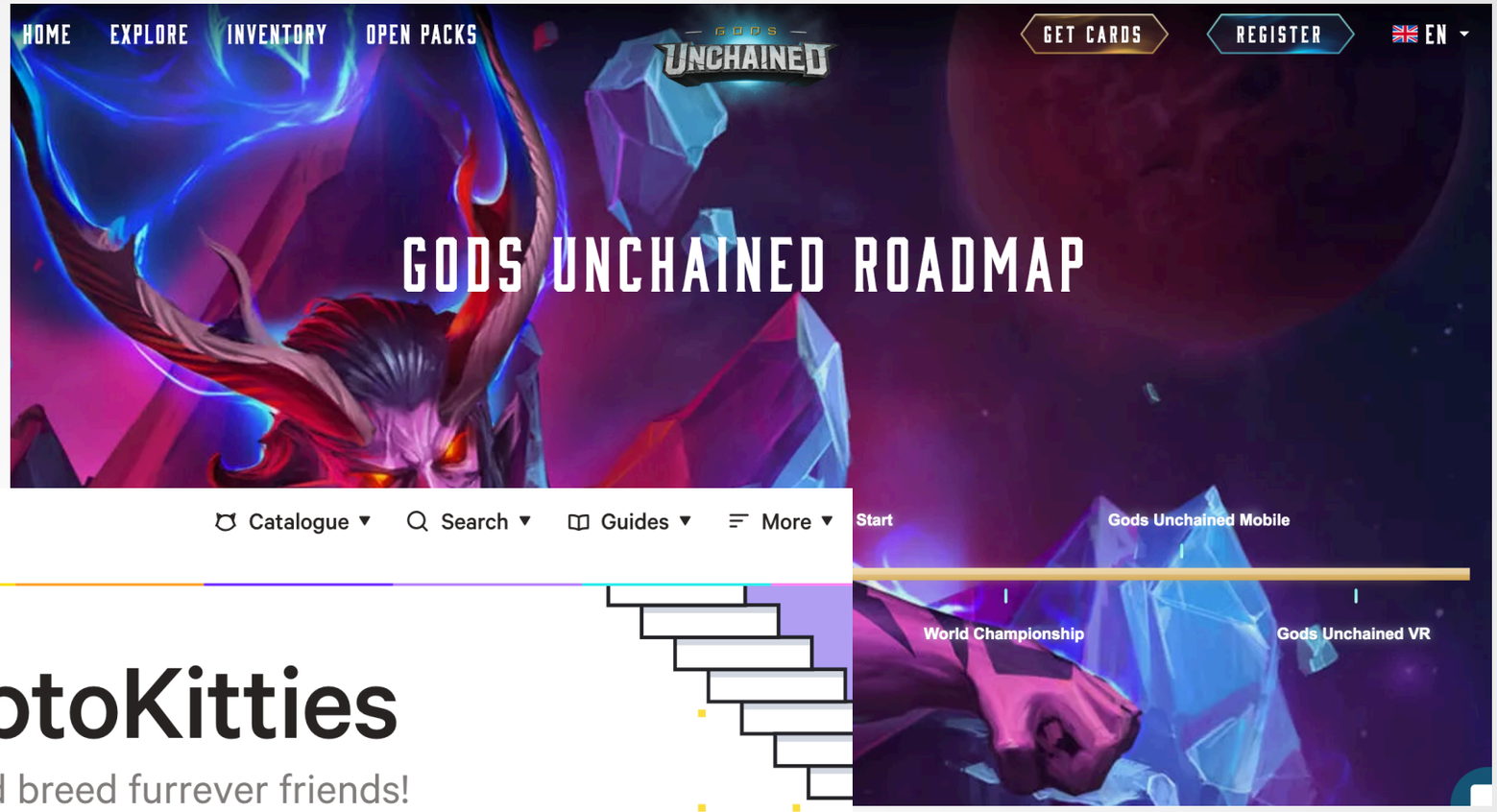
- Skype explores micropayment systems
  e.g. most prominently the XRP TipBot.

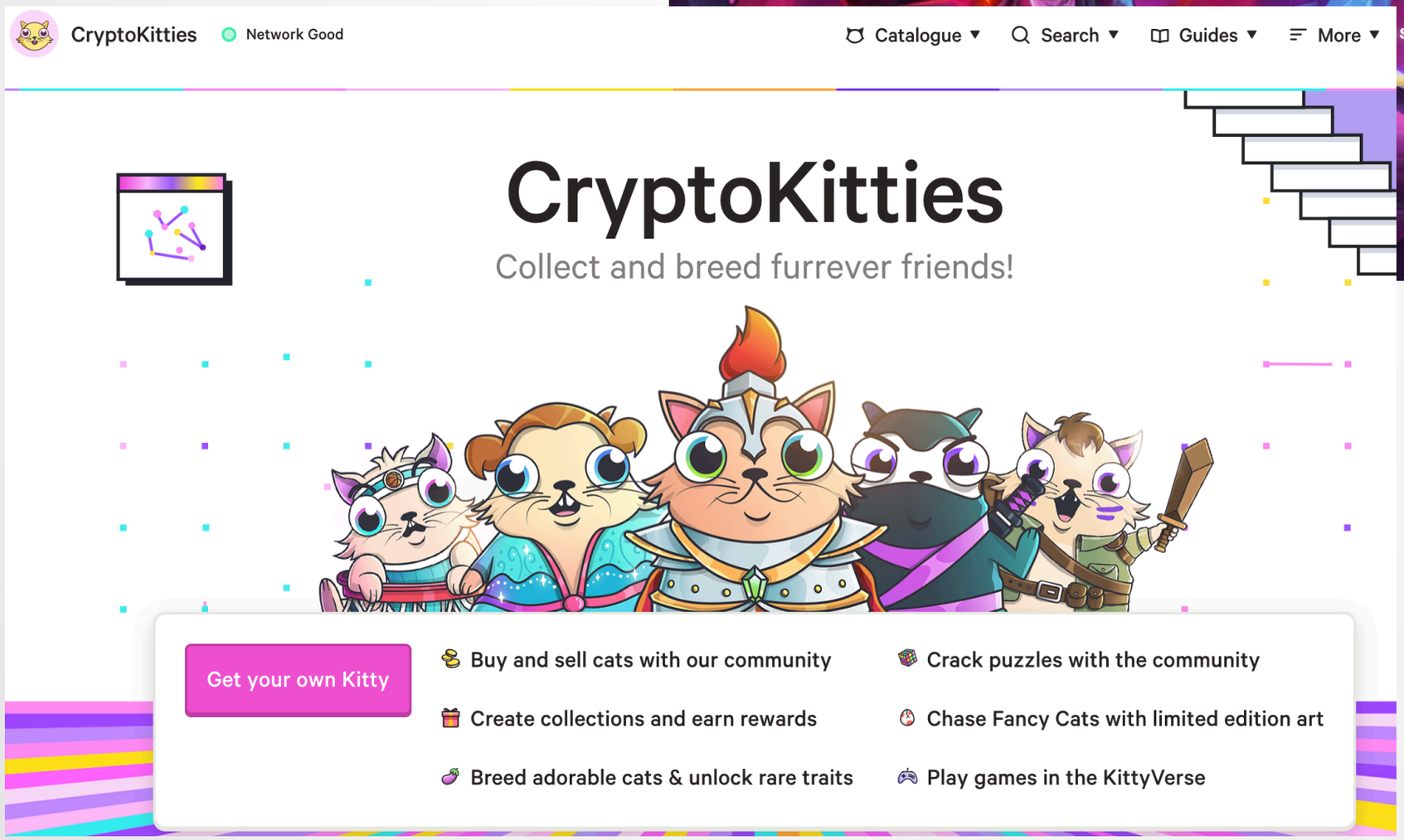
- Facebook / WhatsApp Pay
  Urged by deficiencies in contrast to competitors like WeChat etc.

...

Recreational Industry

Digital collectible card games (think “Magic the Gathering”, “Pirelli Football Cards” etc.); possibility to play, share and trade the games’ cards.





CryptoKitties once “took down” the ETH network, as too many requests were sent by this specific applications’ users.


libra
FB 8382047 F
FB
IN ZUCK WE TRUST
FB 8382047 F
Chief Executive Officer of Facebook
FACEBOOK

Myths vs. Facts

- What are we dealing with ✔
- How does it work ✔
- Why and how do people participate ✔
- How do CCs develop ✔
- How can this be researched ✔

Listen to the Myths;

But reach for the Facts.

Pythia
High Priestess at the
Oracle of Delphi

Donald J. Trump 
@realDonaldTrump

Follow

I am not a fan of Bitcoin and other Cryptocurrencies, which are not money, and whose value is highly volatile and based on thin air. Unregulated Crypto Assets can facilitate unlawful behavior, including drug trade and other illegal activity....

5:15 pm - 11 Jul 2019

13,661 Retweets **46,033** Likes

14K 14K 46K

Donald J. Trump @realDonaldTrump · 14h

....Similarly, Facebook Libra's "virtual currency" will have little standing or dependability. If Facebook and other companies want to become a bank, they must seek a new Banking Charter and become subject to all Banking Regulations, just like other Banks, both National...

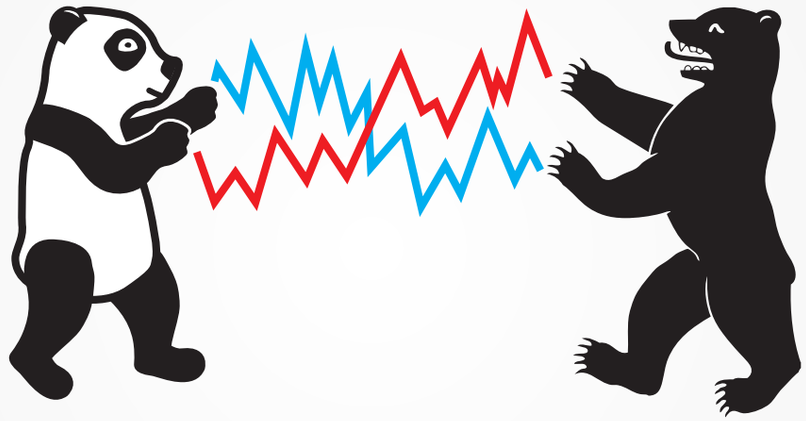
1.5K 8.7K 35K

Donald J. Trump @realDonaldTrump · 14h

...and International. We have only one real currency in the USA, and it is stronger than ever, both dependable and reliable. It is by far the most dominant currency anywhere in the World, and it will always stay that way. It is called the United States Dollar!

Thank you!

谢谢



irtg1792.hu-berlin.de

Ladislaus von Bortkiewicz Group of Statistics
Humboldt-Universität zu Berlin
lvb.wiwi.hu-berlin.de

References

Almosova A (2018) “A Monetary Model of Blockchain.” Annual Conference 2018 (Freiburg, Breisgau): Digital Economy 181502, Verein für Socialpolitik / German Economic Association.

Back A (2002) “Hashcash - A Denial of Service Counter-Measure.” Retrieved on the 24.12.2017 from http://www.hashcash.org/papers/hashcash.pdf.

Chen S, Chen CYH, Härdle WK, Lee T, Ong B (2017). “A first econometric analysis of the CRIX family.” Handbook of Blockchain, Digital Finance and Inclusion, Vol 1, Cryptocurrency, FinTech, InsurTech, and Regulation. LEE KCD, Deng CR, eds. ISBN: 9780128104415, Academic Press, Elsevier .

Chen K, Lei J (2017) “Network cross-validation for determining the number of communities in network data.” Journal of the American Statistical Association, Volume 113, 2018 - Issue 521, pp. 241-251.

Chen Y, Trimborn S, Zhang J, Wang W (2018) “Discover Regional and Size Effects in Global Bitcoin Blockchain via Sparse-Group Network AutoRegressive Modeling.” SSRN. Retrieved on the 17.10.2018 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3245031.

Chen CYH, Després R, Guo L, Renault T (2018) “What makes cryptocurrencies special? Investor sentiment and price predictability in the absence of fundamental value.” IRTG 1792 Discussion Paper. ISSN: 2568-5619. Forthcoming.

Dwork C, Naor M (1992) “Pricing via Processing or Combatting Junk Mail.” Annual International Cryptology Conference. CRYPTO 1992: Advances in Cryptology. CRYPTO 92, pp. 139-147.

Guo L, Li X (2017) “Risk Analysis of Cryptocurrency as an Alternative Asset Class.” In Härdle, W., Chen, C. YH., Overbeck, L. (Eds.). Applied Quantitative Finance. Third edition. Springer-Verlag Berlin Heidelberg. ISBN 978-3-662-54485-3, e-ISBN 978-3-662-54486-0, DOI:10.1007/978-3-662-54486-0, pp. 309-329.

Guo L, Tao Y, Härdle WK (2019) “A Dynamic Network for Cryptocurrencies.” Retrieved on the 15.03.2019 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3185594. J Amer Stat Assoc, submitted

Haber S, Stornetta W (1991) “How to Time-Stamp a Digital Document.” Journal of Cryptology. Volume 3, Issue 2, pp. 99–111.

Hafner, Ch (2018) “Testing for Bubbles in Cryptocurrencies with Time-Varying Volatility.” SSRN. Retrieved on the 15.10.2018 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3105251.

Härdle WK, Trimborn S (2015) “CRIX or evaluating Blockchain based currencies. Oberwolfach Report No. 42/2015.” The Mathematics and Statistics of Quantitative Risk\. DOI:10.4171/OWR/2015/42

Härdle WK, Lee D, Nasekin S, Petukhina A (2018) “Tail Event Driven ASset allocation: evidence from equity and mutual funds' markets.” Journal of Asset Management. January 2018, Volume 19, Issue 1, pp. 49-63.

Hou A, Wang W, Chen CYH, Härdle WK (2019) “Pricing Cryptocurrency options: the case of CRIX and Bitcoin.” Journal of Financial Econometrics. Revise and Resubmit.

Klein T, Hien PT, Walther T (2018) “Bitcoin Is Not the New Gold: A Comparison of Volatility, Correlation, and Portfolio Performance.” Retrieved on the 25.03.2018 from http://dx.doi.org/10.2139/ssrn.3146845.

Kim A, Trimborn S, Härdle WK (2018) “VCRIX - Cryptocurrency Volatility Index.” Forthcoming.

Kostmann M (2018) “Forecasting in blockchain-based smart grids: Testing a prerequisite for the implementation of local energy markets.” Humboldt-Universität zu Berlin, Wirtschaftswissenschaftliche Fakultät, Masterarbeit. http://dx.doi.org/10.18452/19578.

Linton M, Teo E, Bommes E, Chen CYH, Härdle WK (2017) “Dynamic Topic Modelling for Cryptocurrency Community Forums.” In Härdle, W., Chen, C. YH., Overbeck, L. (Eds.). Applied Quantitative Finance. Third edition. Springer-Verlag Berlin Heidelberg. ISBN 978-3-662-54485-3, e-ISBN 978-3-662-54486-0, DOI 10.1007/978-3-662-54486-0, pp. 355-372.

Mengelkamp E, Notheisen B, Beer C, Dauer D, Weinhardt Ch (2017) “A blockchain-based smart grid: towards sustainable local energy markets.” Computer Science - Research and Development. February 2018, Volume 33, Issue 1–2, https://doi.org/10.1007/s00450-017-0360-9, pp. 207–214.

Petukhina A, Trimborn S, Härdle WK, Elendner H (2018) “Investing with cryptocurrencies evaluating the potential of portfolio allocation strategies.” SSRN. Retrieved on the 25.10.2018 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3274193.

Trimborn S, Härdle WK (2018) “CRIX an Index for cryptocurrencies.” Journal of Empirical Finance. https://doi.org/10.1016/j.jempfin.2018.08.004.

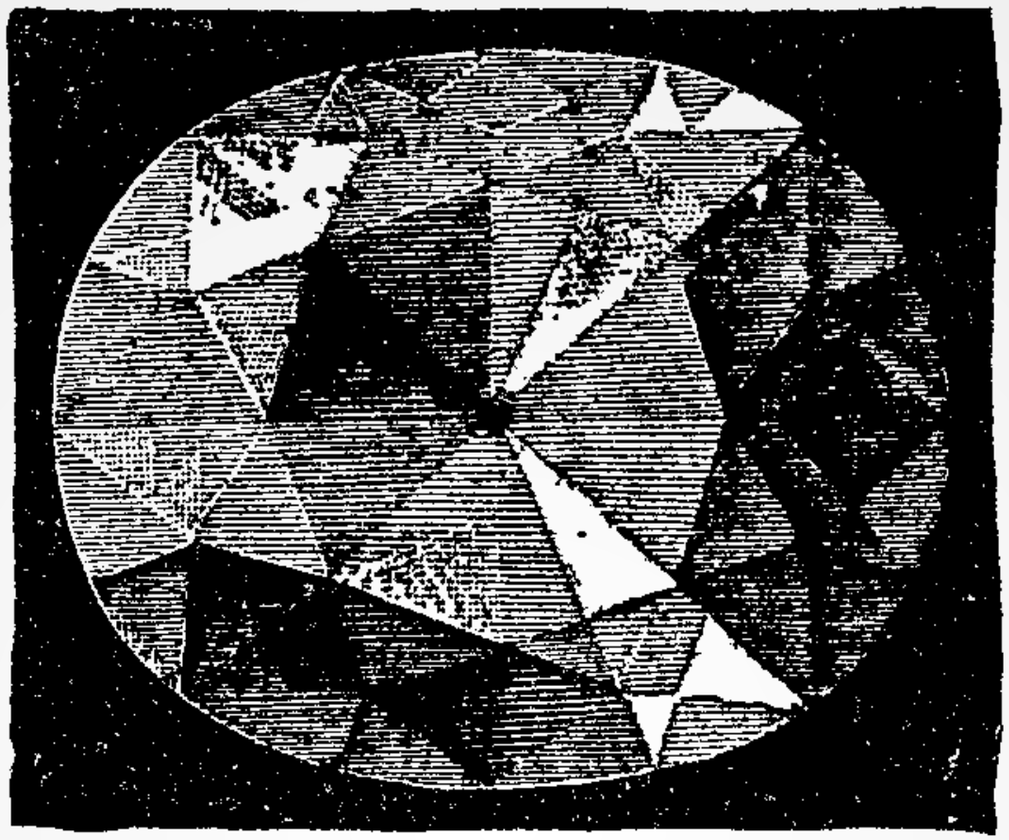
Trimborn S, Li M, Härdle WK (2019) “Investing with cryptocurrencies - A liquidity constrained investment approach.” Journal of Financial Econometrics. In print.

FIN

„Dangerous‘ systems ?

‚Special‘ systems ?

‚Democratic‘ systems ?



Koh-i-Noor (Persian: كوه نور), also spelt Kohinoor and Koh-i-Nur
is one of the largest cut diamonds in the world, weighing 105.6 carats (21.12 g), and part of the British Crown Jewels.

Cryptocurrencies = Value or First-World-Entertainment ?

Bitcoin: charting a crazy 2017 - BBC News

Bitcoin: financial revolution or modern day tulipmania? - BBC Newsnight

Bitcoin: My 400 bitcoin bet paid off, but is it too late for others? - BBC News

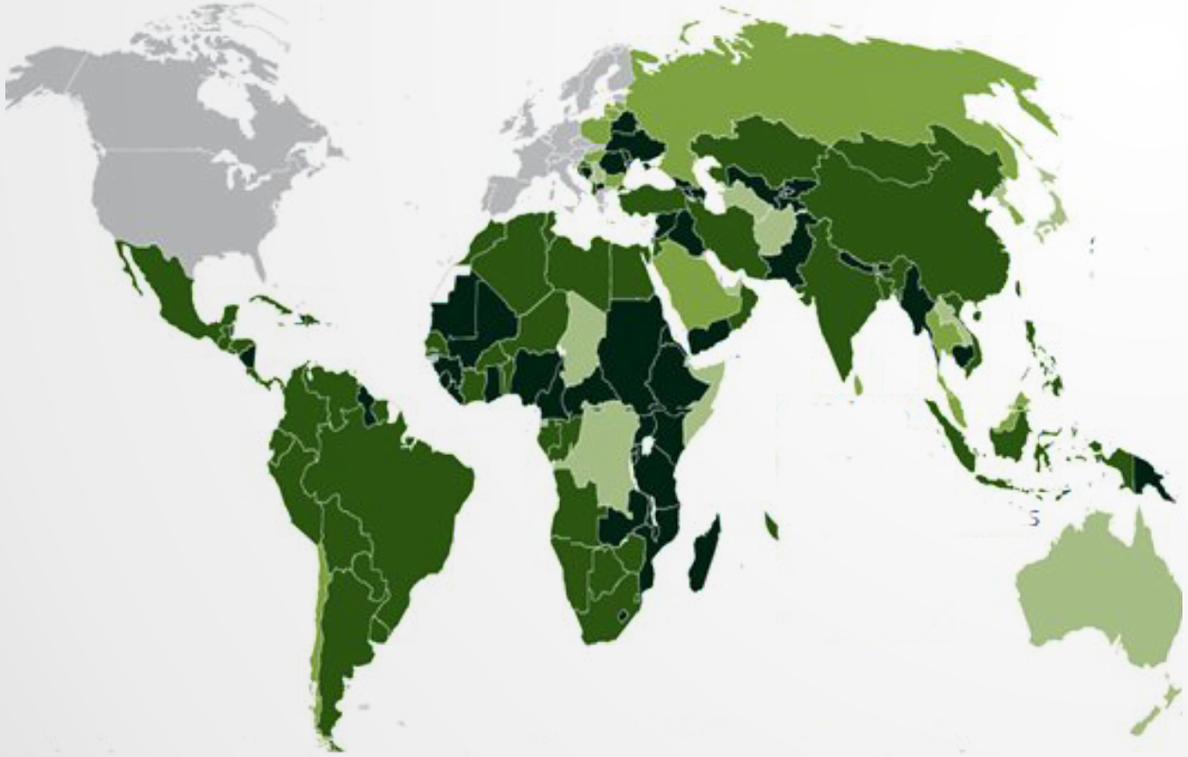
Financial Inclusion

Homeostasis

Financial illiteracy
Corruption
Suboptimal governance
Inefficient monetary institutions
Insecurities about fiat currency (forgery …)

Mass-1st-World-Evolution

1970s: Mainframe
1980s: PC
1990s: Internet
2000s: Social Media
2010s: Blockchain



In total, 53% of the worlds' adult population is unbanked (2 455 million)
Source: "Half the world is unbanked", McKinsey & Company

Smartphone ownership

🇨🇳 43% in 2013, 60% in 2018

🇺🇸 56% in 2013, 77% in 2018

🇩🇪 41% in 2013, 78% in 2018

🇸🇳 13% in 2013, 34% in 2017

Source: statista.com

Transition from homeostasis

Type	Now Systems	New Systems
Data	Local Storage	Cloud / Blockchain
Assets	Physical	Smart Contracts
Provenance	Physical Proof	Algorithmic Proof
Data Models	EDI, XML	JSON, Graph
Connectivity	Point-to-Point, VPN	API, SDK, Cloud
Processing	Mostly Manual	Async, real-time

Transition of control

	Now Systems	Blockchains
Records	Errare humanum est	Immutable
Consensus	Centralized	Decentralized
Visibility	Mostly inter partes	Transparent, Auditable
Security	Mostly Centralized	Verifiable via Hashes

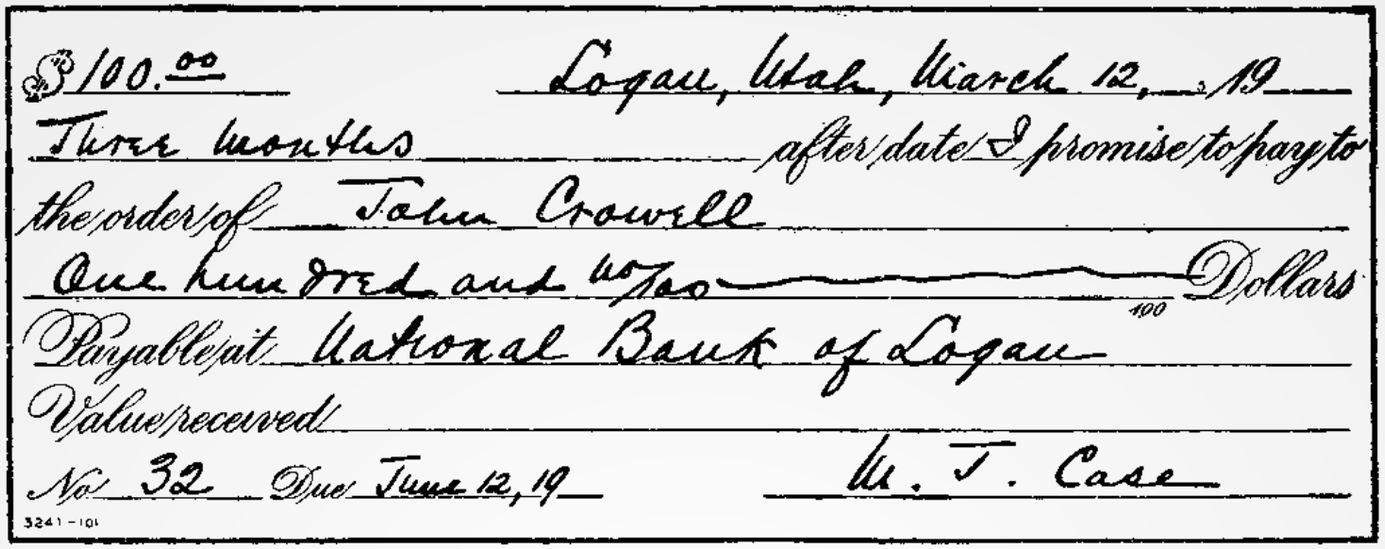
Trust / Reward systems for participation

British Bechuanaland One Penny Stamp, 1887

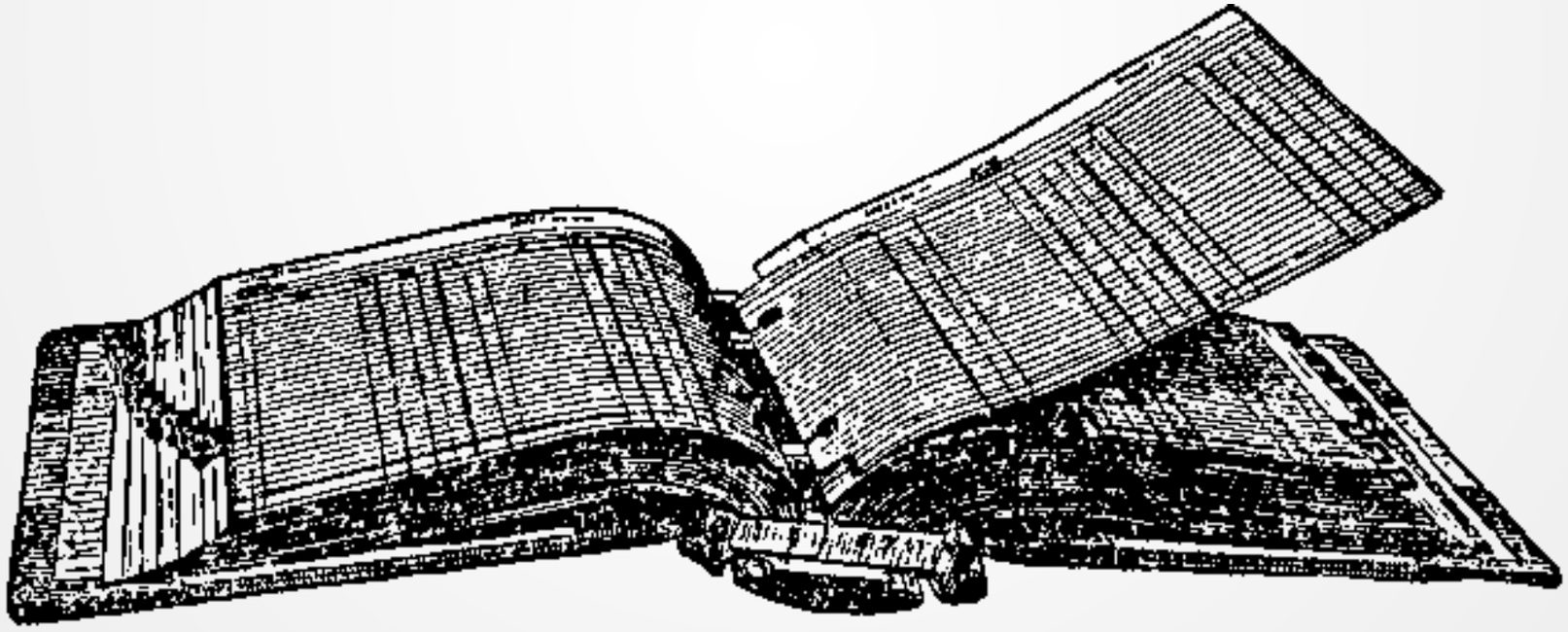
Dwork & Naor, 1992

provide each eMail with a header containing
the "**virtual postage**" („**proof-of-work calculation**")
to combat junk mails / spam-

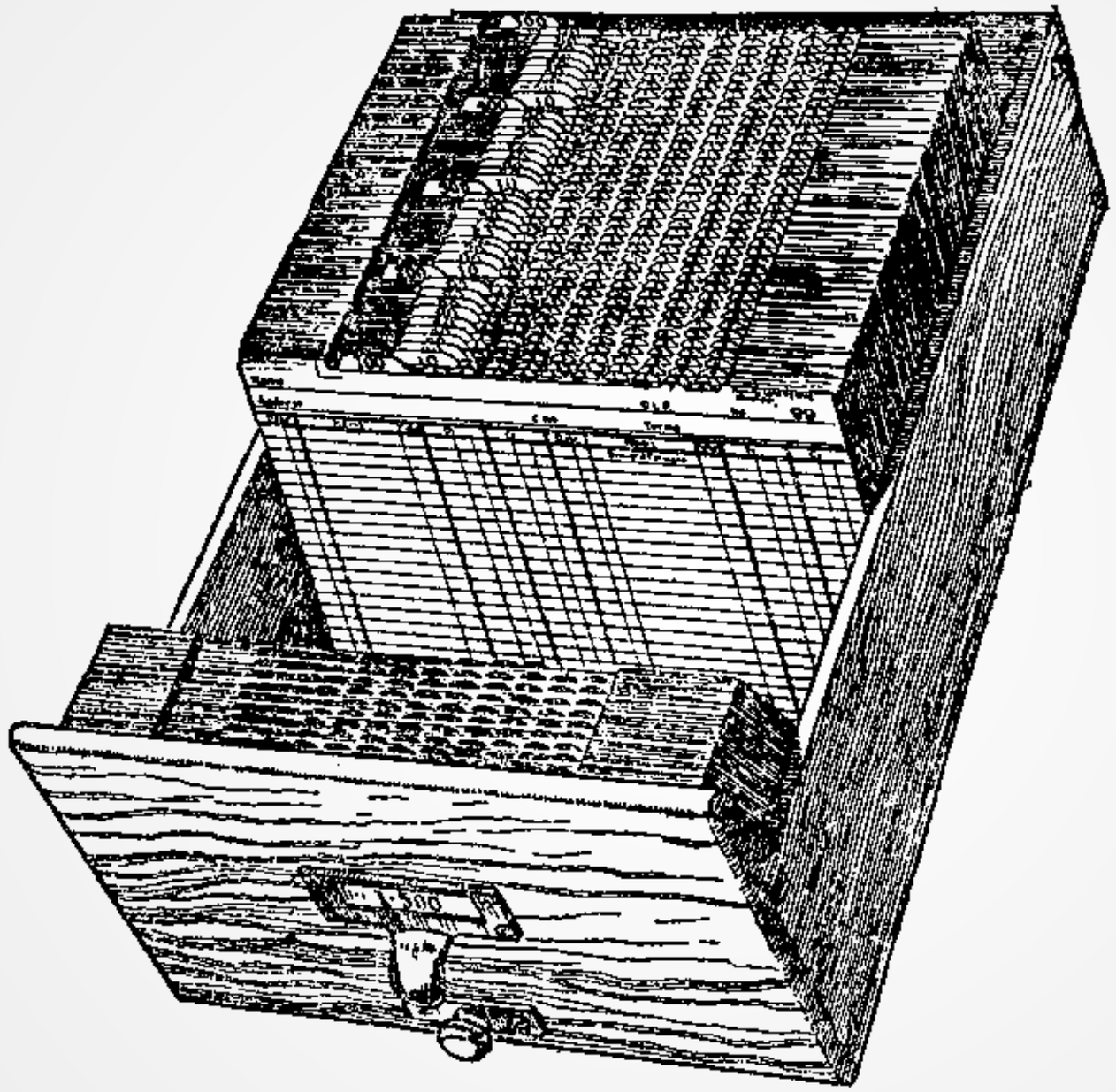
cost of the stamp = cost in computational power


$100.00 Logan, Utah, March 12, 19
Three months after date I promise to pay to
the order of John Crowell
One hundred and 60/100 Dollars
Payable at National Bank of Logan
Value received
No 32 Due June 12, 19 W. J. Case
3241-101

A typical ledger block, used in transactions



Goal: **Create** chain of ledger blocks
= Transparency, Consensus, Impermutable …

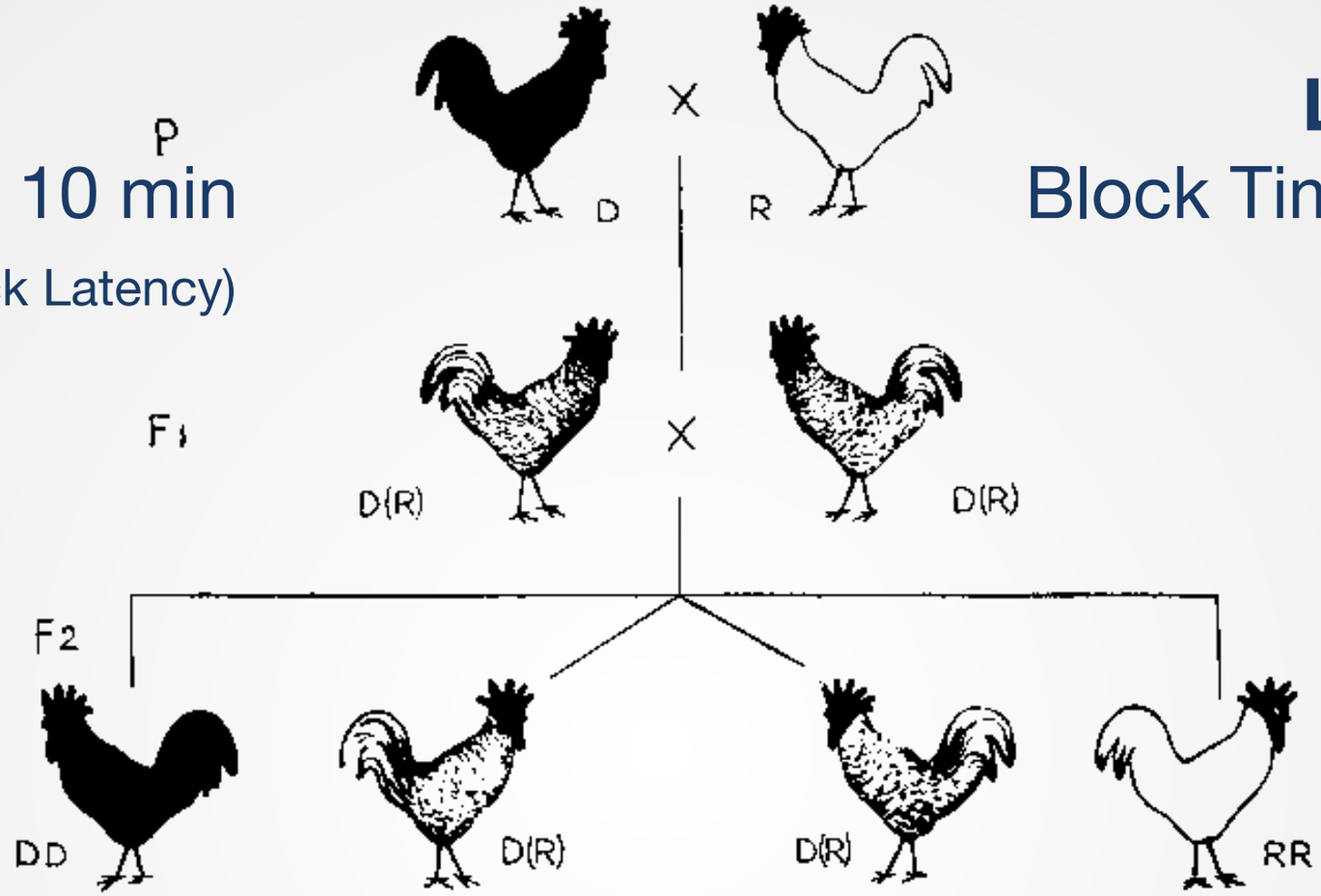


A Blockchain (BC) application, e.g. (public) ledger

BTC
Block Time ~ 10 min
(Block Time = Block Latency)

LTC
Block Time ~ 2.5 min

...



...

ETH
Block Time ~ 10 sec

...

XRP
Block Time ~ 3.5 sec

Hundreds of CCs share the same „genes“ (active/dead).
But all CCs are algorithms based on the blockchain technology.

(! BC ≠ „=CC“)
(! CC ≠ „=Token“)

The „genes“ of Cryptocurrencies

„**Satoshi Nakamoto**“, 2008

the

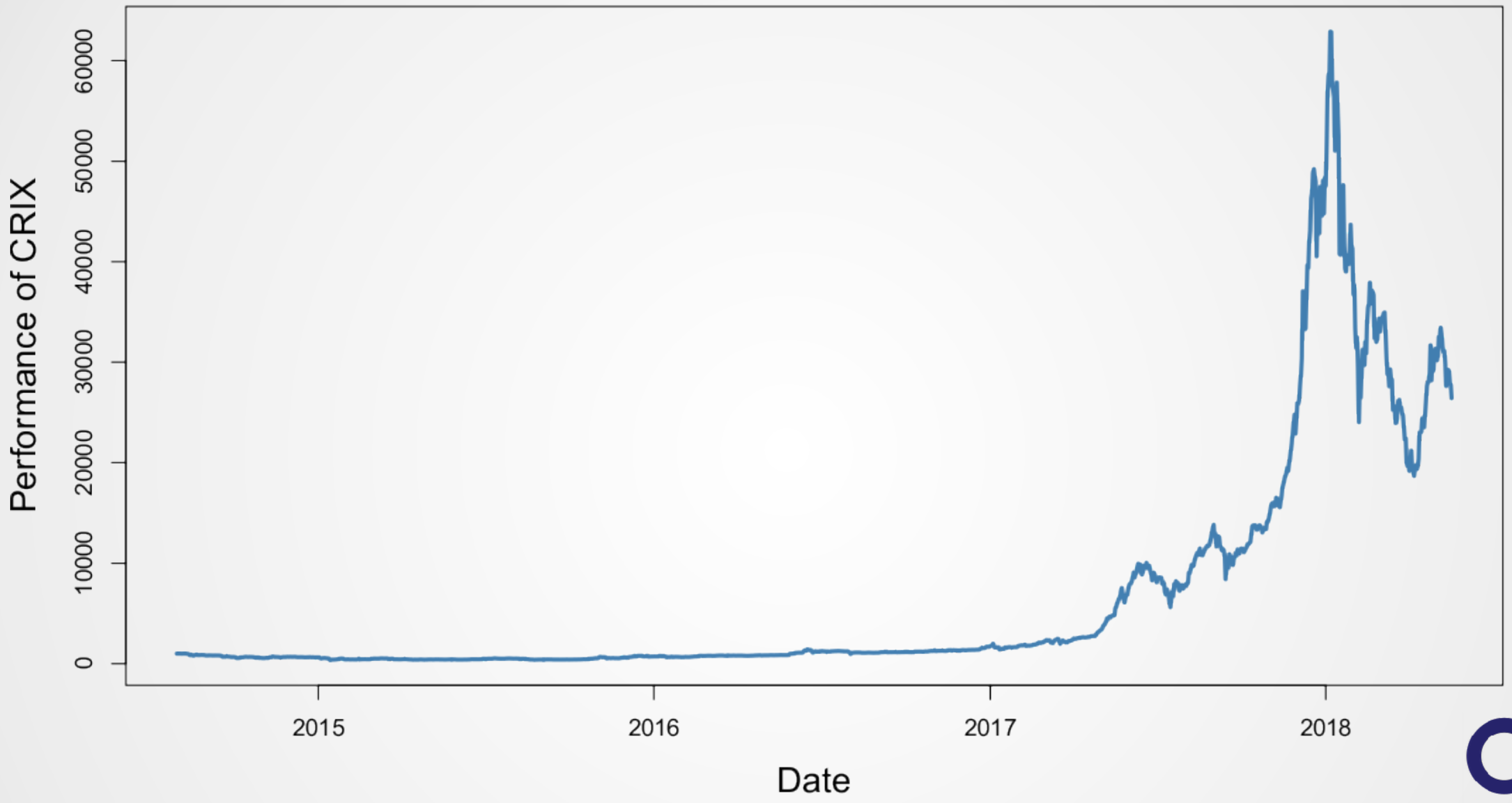
Gregor Mendel of Cryptocurrencies

and „developer“ of

Bitcoin

BTC = Marketleader

Cryptocurrency markets



CRypto currency IndeX, CRIX

thecrix.de

crix.berlin

2014	NXT	PPC	XPY	CNMT	BTS	LTC	XRP	BTC	GOLD	S.P100
NXT	1.00	0.19	0.15	0.16	0.11	0.16	0.09	0.36	0.02	0.07
PPC	0.19	1.00	0.29	0.00	0.18	0.43	0.07	0.44	-0.03	0.08
XPY	0.15	0.29	1.00	0.15	0.59	0.28	0.16	0.23	-0.22	-0.24
CNMT	0.16	0.00	0.15	1.00	0.03	0.01	0.00	0.10	0.00	0.09
BTS	0.11	0.18	0.59	0.03	1.00	0.19	0.00	0.28	-0.05	0.00
LTC	0.16	0.43	0.28	0.01	0.19	1.00	0.09	0.59	-0.07	0.05
XRP	0.09	0.07	0.16	0.00	0.00	0.09	1.00	0.05	-0.07	0.08
BTC	0.36	0.44	0.23	0.10	0.28	0.59	0.05	1.00	-0.02	0.01
GOLD	0.02	-0.03	-0.22	0.00	-0.05	-0.07	-0.07	-0.02	1.00	-0.16
S&P100	0.07	0.08	-0.24	0.09	0.00	0.05	0.08	0.01	-0.16	1.00

Yearly correlation of the TOP-8 cryptocurrencies, S&P100 and GOLD

NXT = more than just a CC, but bad management

XPY (Paycoin) = how to not run a CC

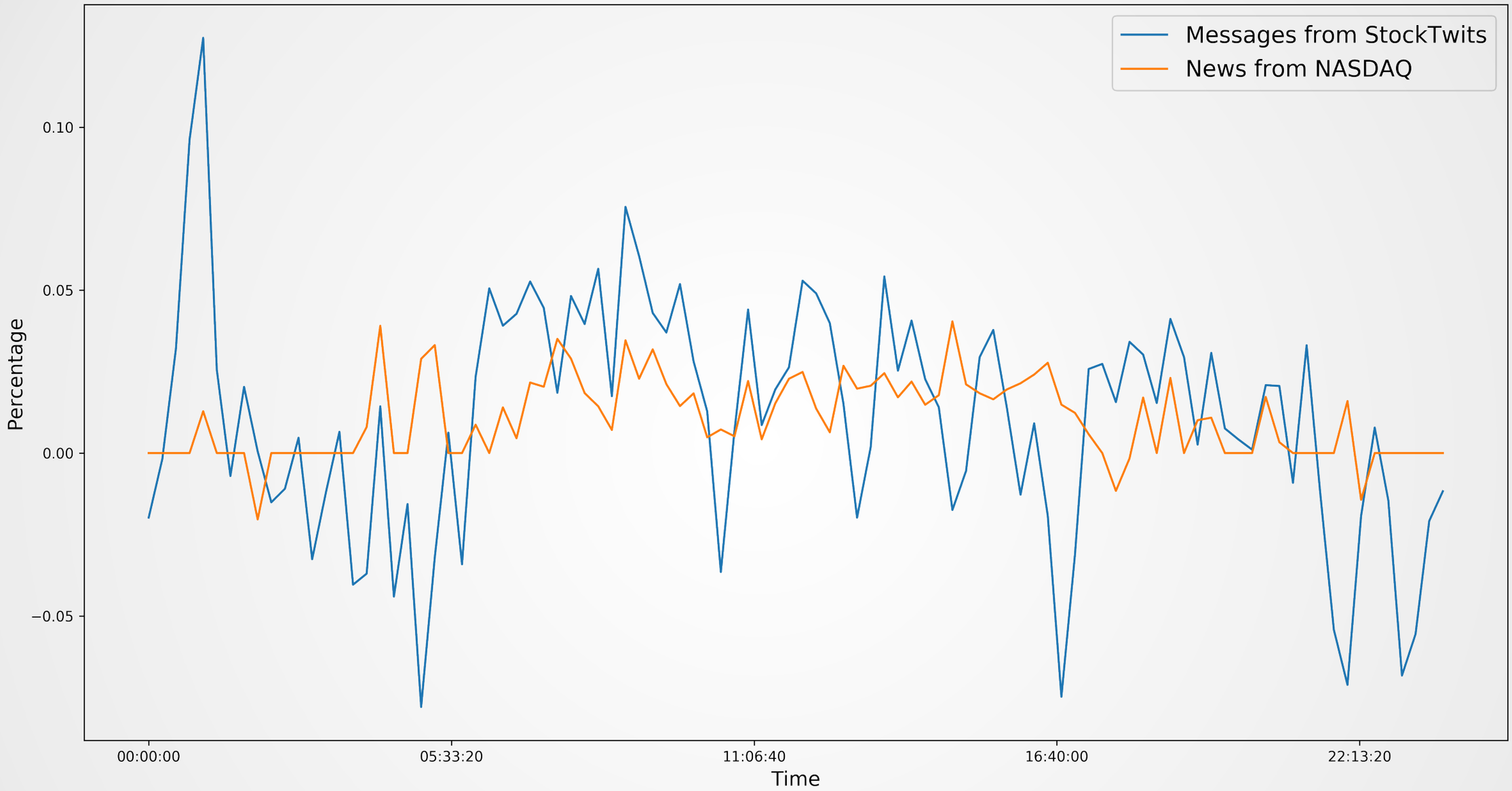
CrixToDate

2015	MAID	DOGE	BTS	DASH	LTC	XRP	ETH	BTC	GOLD	S.P100
MAID	1.00	0.30	0.18	0.30	0.17	0.29	0.28	0.42	-0.04	-0.04
DOGE	0.30	1.00	0.48	0.40	0.51	0.35	0.18	0.67	0.10	-0.02
BTS	0.18	0.48	1.00	0.23	0.28	0.29	0.23	0.36	0.07	-0.02
DASH	0.30	0.40	0.23	1.00	0.22	0.23	0.19	0.53	0.04	0.01
LTC	0.17	0.51	0.28	0.22	1.00	0.22	0.19	0.54	0.02	-0.07
XRP	0.29	0.35	0.29	0.23	0.22	1.00	-0.02	0.36	0.06	0.02
ETH	0.28	0.18	0.23	0.19	0.19	-0.02	1.00	0.24	-0.03	0.00
BTC	0.42	0.67	0.36	0.53	0.54	0.36	0.24	1.00	0.04	-0.01
GOLD	-0.04	0.10	0.07	0.04	0.02	0.06	-0.03	0.04	1.00	-0.06
S&P100	-0.04	-0.02	-0.02	0.01	-0.07	0.02	0.00	-0.01	-0.06	1.00

2016	XMR	STEEM	ETC	DASH	LTC	XRP	ETH	BTC	GOLD	S.P100
XMR	1.00	-0.02	-0.16	0.11	0.12	0.03	0.15	0.17	-0.05	0.04
STEEM	-0.02	1.00	0.09	0.02	-0.01	-0.04	0.04	0.11	-0.05	0.11
ETC	-0.16	0.09	1.00	0.17	-0.15	0.00	-0.21	-0.30	0.06	0.05
DASH	0.11	0.02	0.17	1.00	0.06	0.03	0.10	0.13	-0.01	0.13
LTC	0.12	-0.01	-0.15	0.06	1.00	0.01	0.03	0.74	0.11	-0.06
XRP	0.03	-0.04	0.00	0.03	0.01	1.00	0.07	0.03	0.00	0.11
ETH	0.15	0.04	-0.21	0.10	0.03	0.07	1.00	0.09	0.01	-0.05
BTC	0.17	0.11	-0.30	0.13	0.74	0.03	0.09	1.00	0.08	-0.02
GOLD	-0.05	-0.05	0.06	-0.01	0.11	0.00	0.01	0.08	1.00	-0.35
S&P100	0.04	0.11	0.05	0.13	-0.06	0.11	-0.05	-0.02	-0.35	1.00

CrixToDate

Sentiment construction



Nature language processing techniques (SVM model) distilling sentiment

shown here: from NASDAQ news

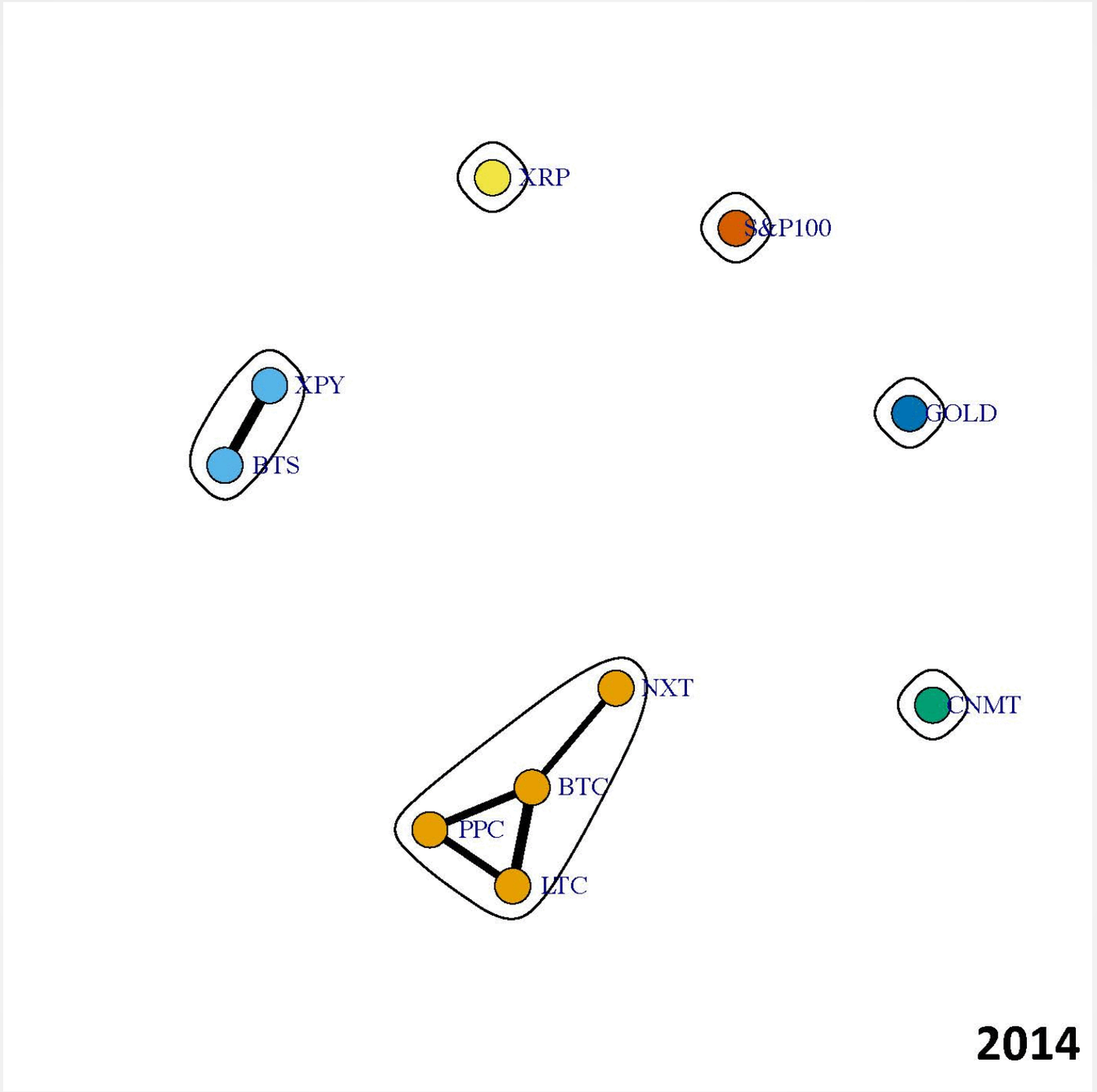
Junji Hu, Wolfgang K. Härdle

2017	BCH	NEO	ADA	XLM	LTC	XRP	ETH	BTC	GOLD	S.P100
BCH	1.00	0.29	-0.05	0.04	0.19	0.13	0.27	0.07	-0.04	-0.08
NEO	0.29	1.00	0.29	0.34	0.35	0.29	0.50	0.31	0.10	-0.01
ADA	-0.05	0.29	1.00	0.57	0.20	0.43	0.26	0.16	0.00	0.19
XLM	0.04	0.34	0.57	1.00	0.35	0.50	0.27	0.27	0.00	0.01
LTC	0.19	0.35	0.20	0.35	1.00	0.28	0.39	0.41	-0.10	0.11
XRP	0.13	0.29	0.43	0.50	0.28	1.00	0.19	0.14	0.06	-0.06
ETH	0.27	0.50	0.26	0.27	0.39	0.19	1.00	0.39	0.07	0.06
BTC	0.07	0.31	0.16	0.27	0.41	0.14	0.39	1.00	-0.02	0.01
GOLD	-0.04	0.10	0.00	0.00	-0.10	0.06	0.07	-0.02	1.00	-0.23
S&P100	-0.08	-0.01	0.19	0.01	0.11	-0.06	0.06	0.01	-0.23	1.00

Focus on LTC, XRP, ETH, BTC, GOLD, S&P 100 correlations.

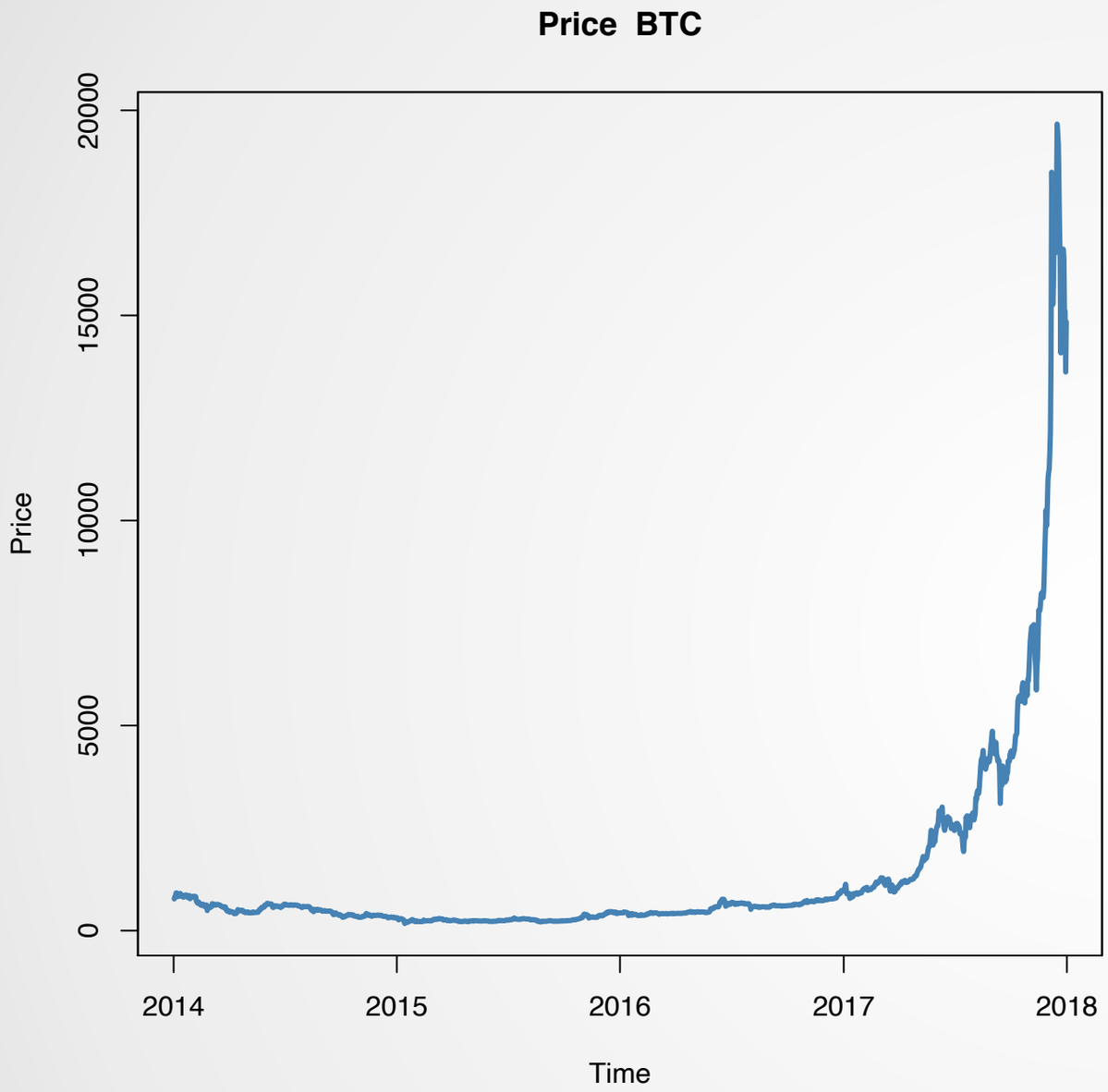
CCs attract interest of
more risk friendly investors,
compared to GOLD investors.

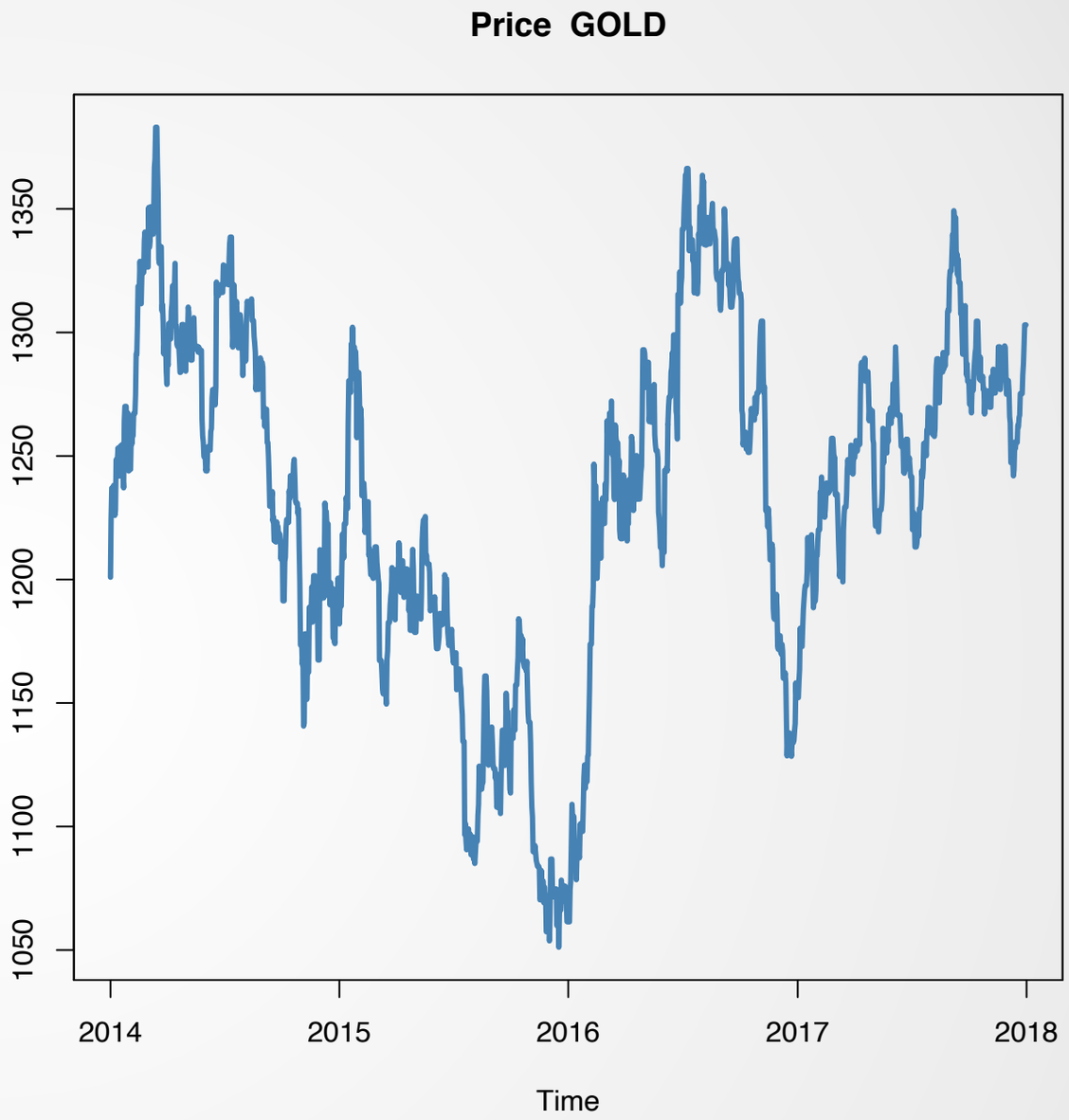
CrixToDate



Animation: Yearly correlation of the TOP-8 cryptocurrencies, S&P100 and GOLD

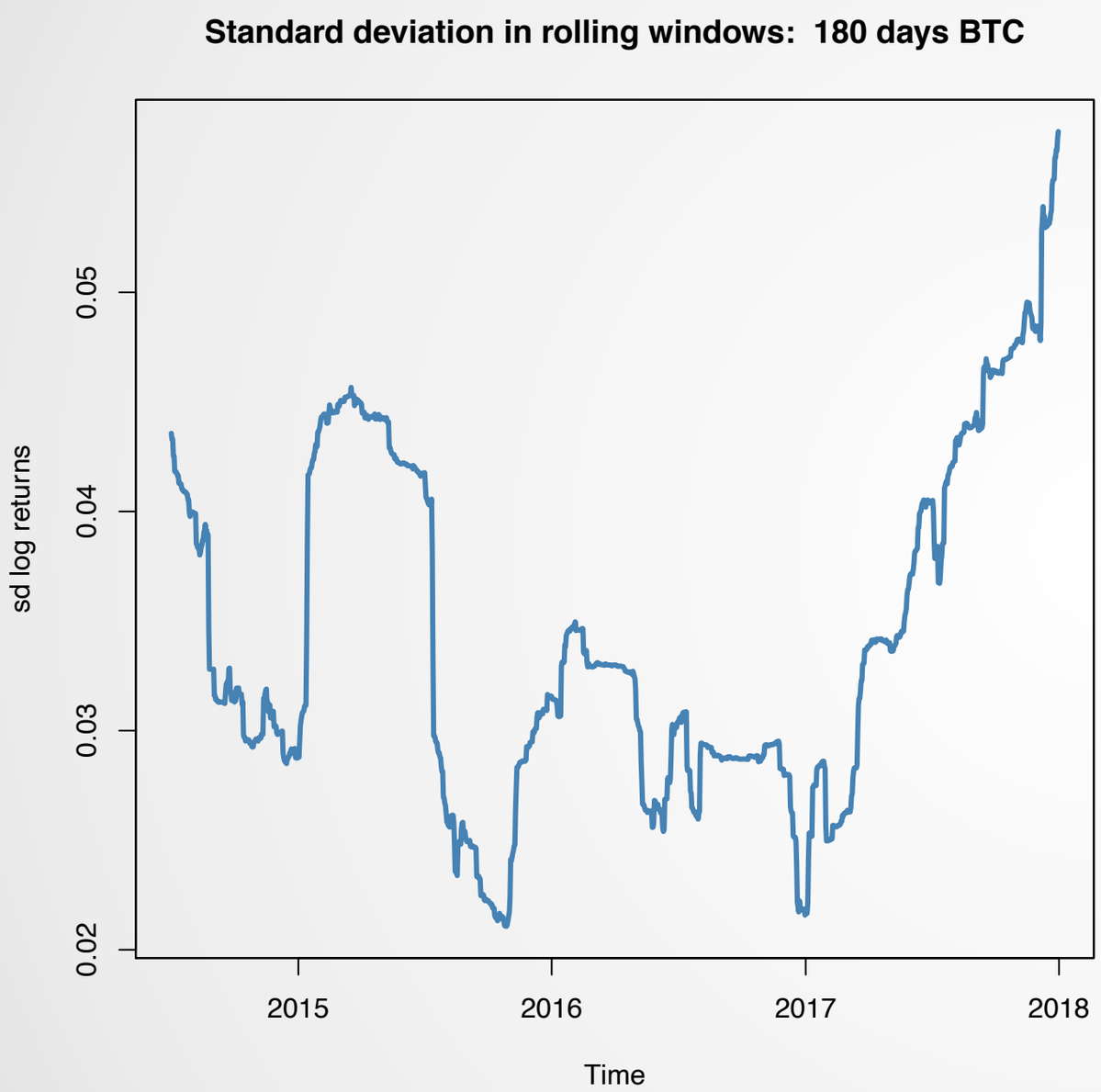
CrixToDate

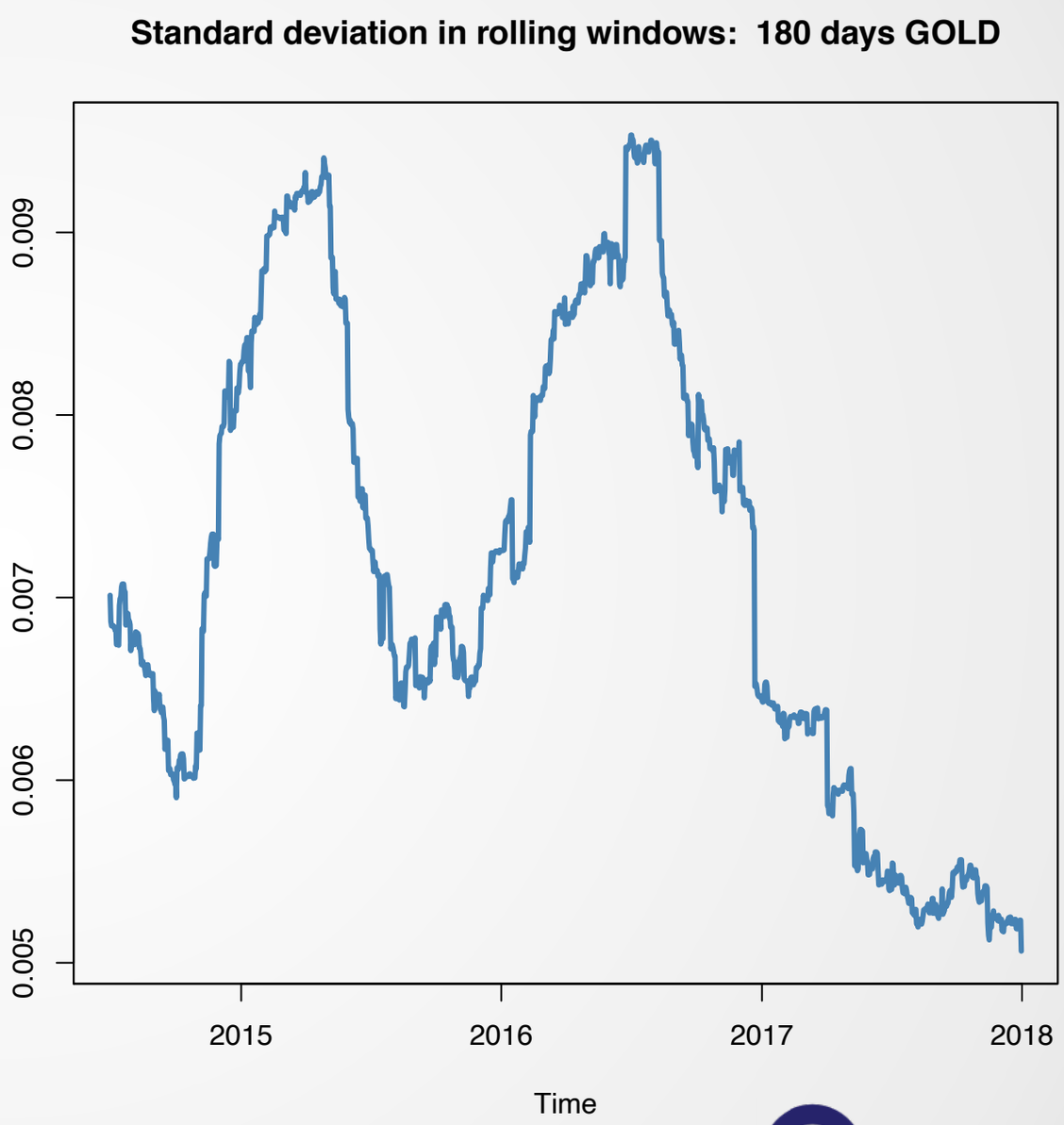




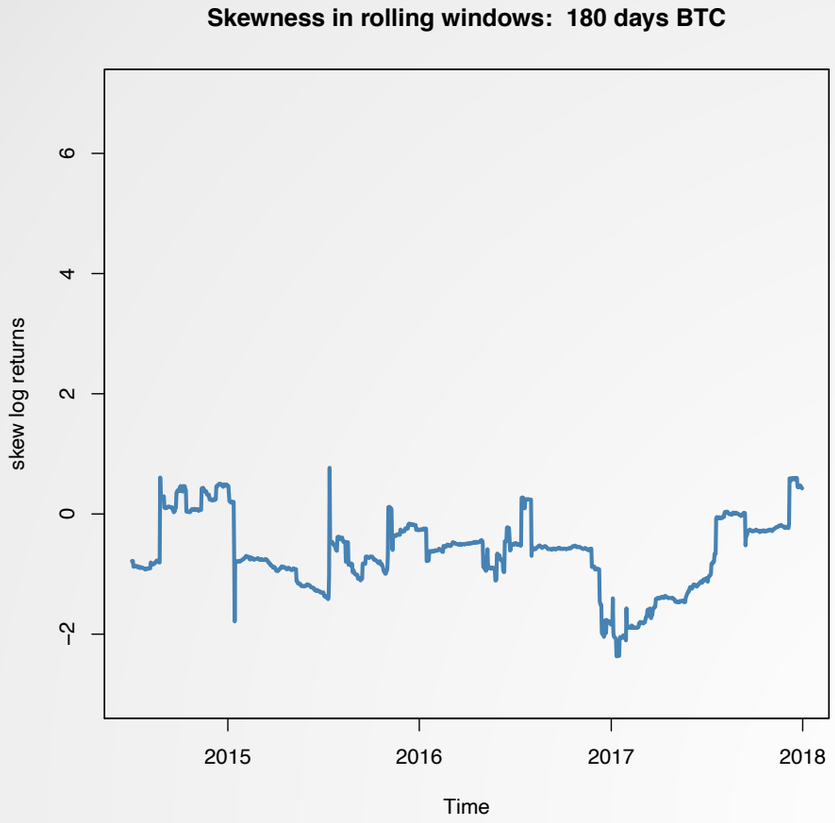
Finding: BTC to GOLD Correlation = negative
However: Both assets are highly driven by psychological factors.

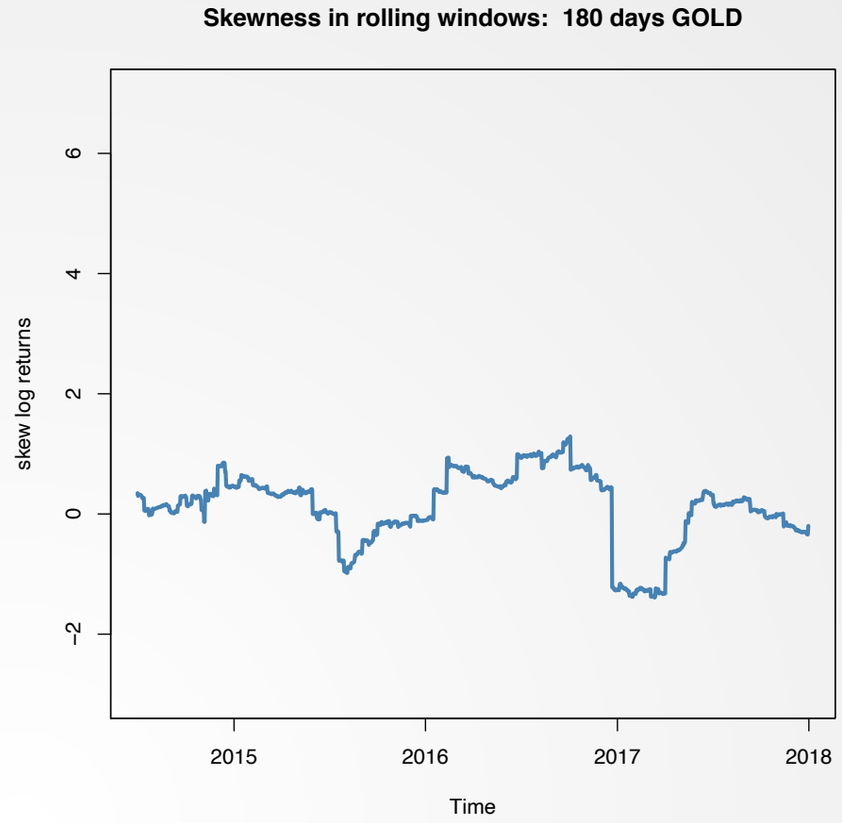
CrixToDate

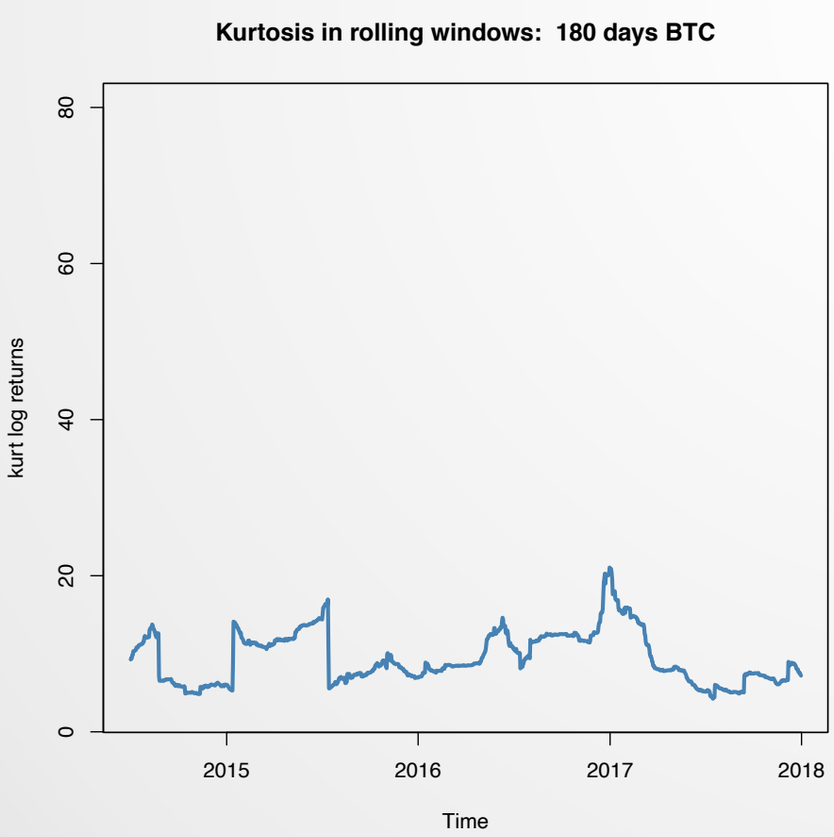

Standard deviation in rolling windows: 180 days BTC
sd log returns
0.02
0.03
0.04
0.05
2015
2016
2017
2018
Time

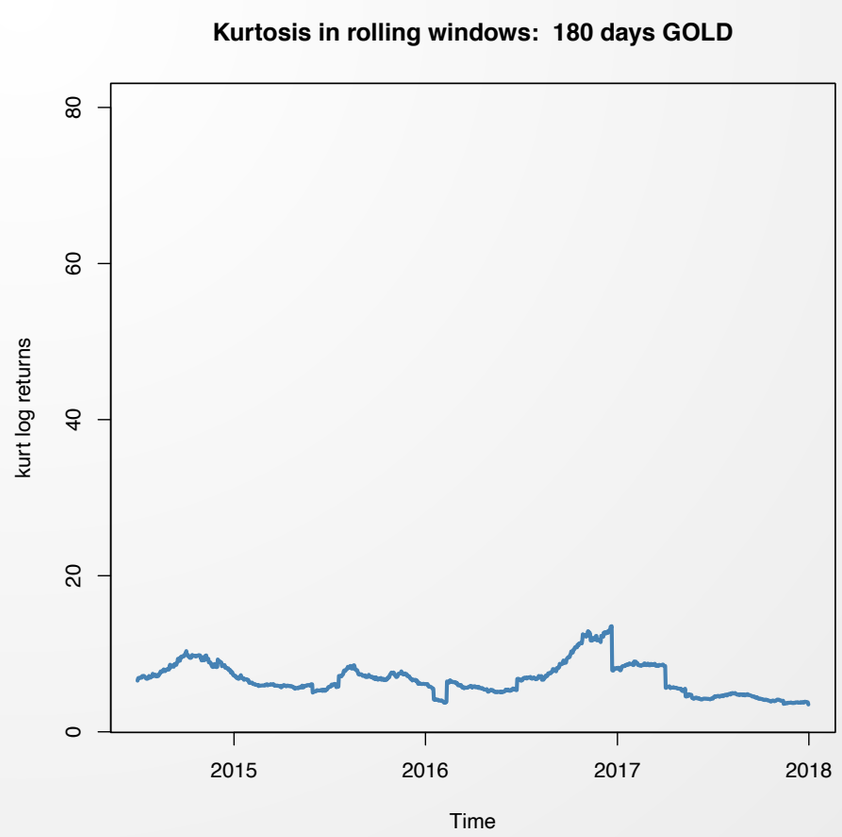

Standard deviation in rolling windows: 180 days GOLD
0.005
0.006
0.007
0.008
0.009
2015
2016
2017
2018
Time

CrixToDate


Skewness in rolling windows: 180 days BTC
skew log returns
6
4
2
0
−2
2015
2016
2017
2018
Time


Skewness in rolling windows: 180 days GOLD
skew log returns
6
4
2
0
−2
2015
2016
2017
2018
Time

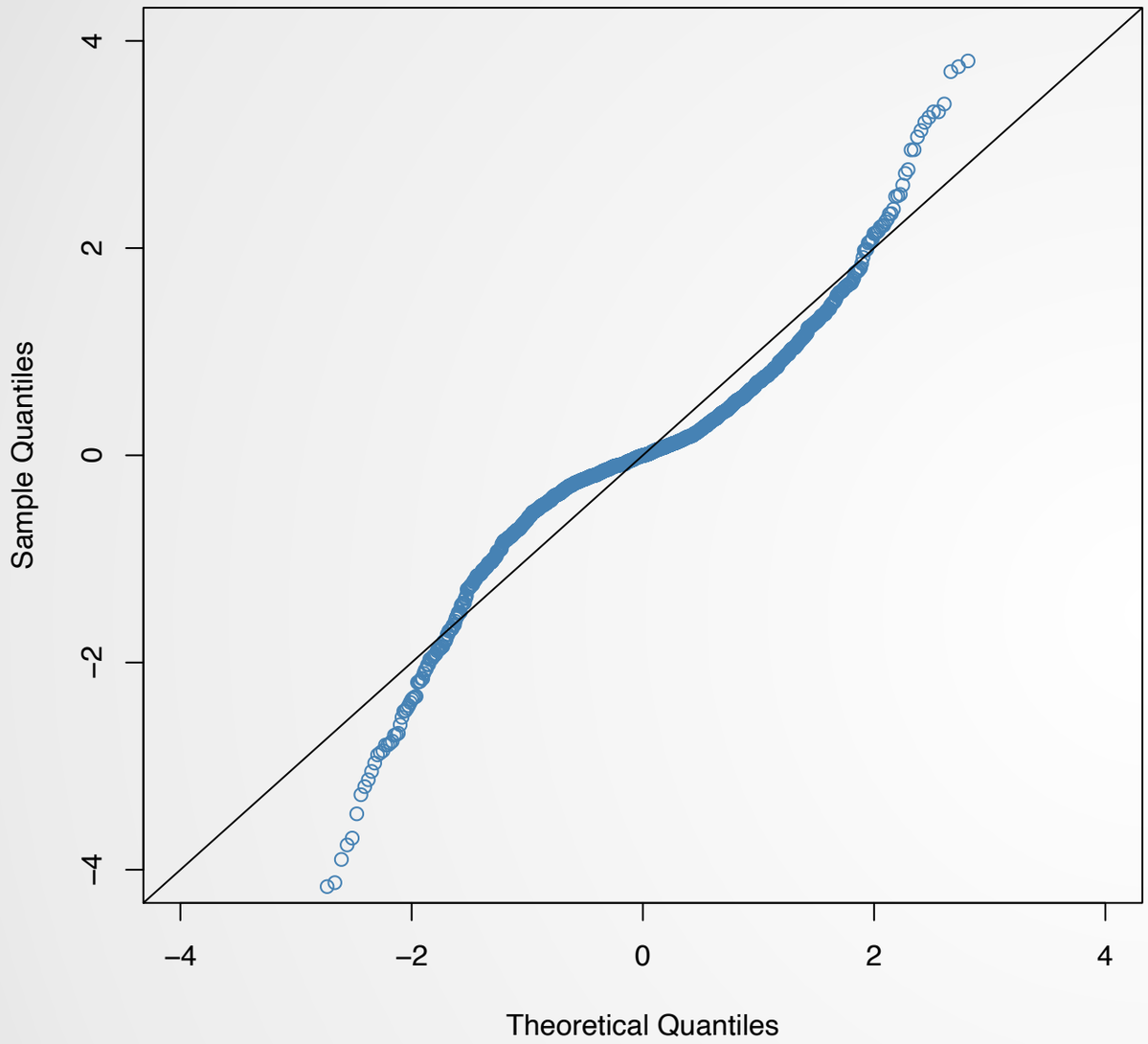

Kurtosis in rolling windows: 180 days BTC
kurt log returns
80
60
40
20
0
2015
2016
2017
2018
Time

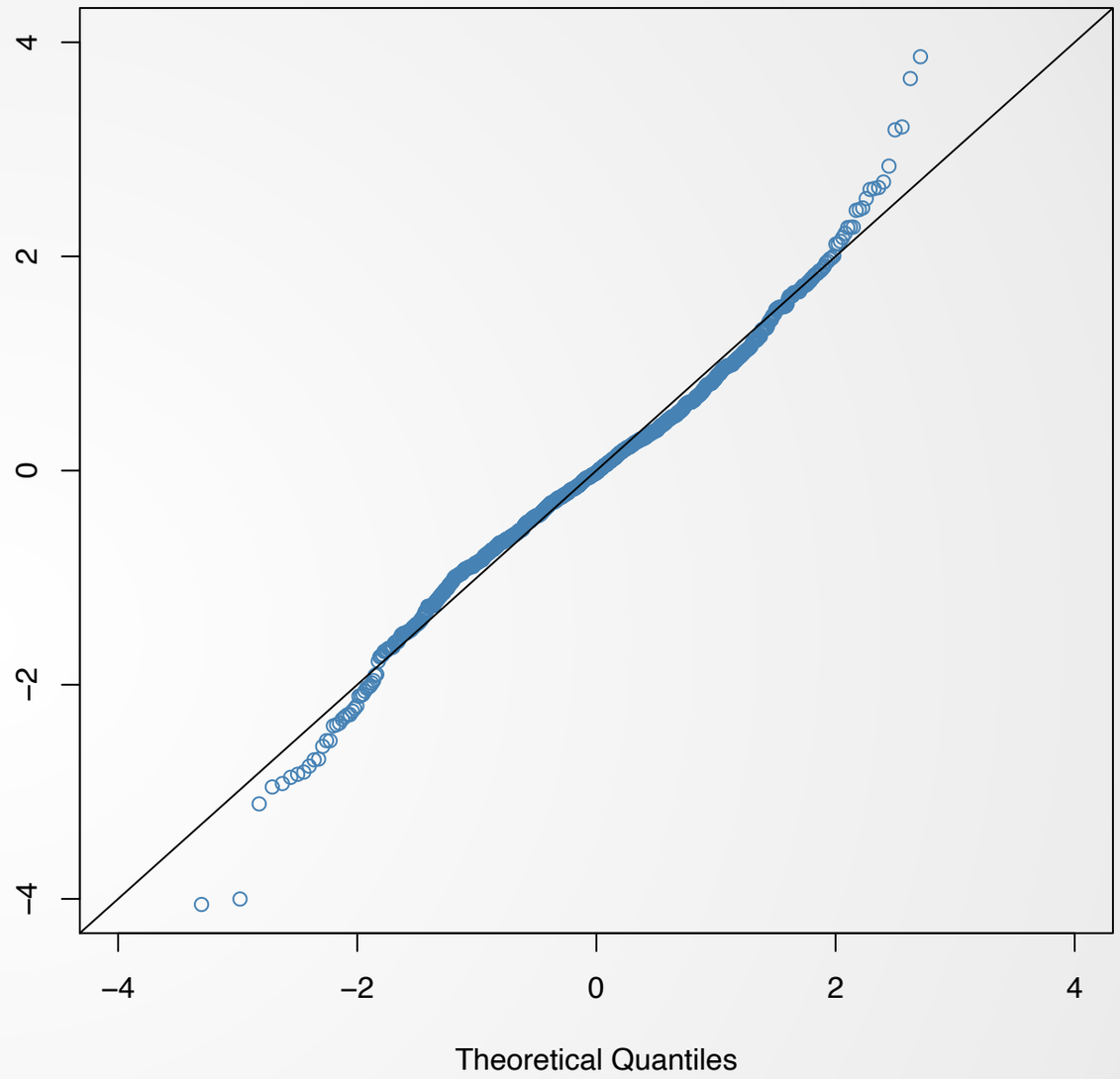

Kurtosis in rolling windows: 180 days GOLD
kurt log returns
80
60
40
20
0
2015
2016
2017
2018
Time

CrixToDate

- **Skewness** of BTC and GOLD are
- close to 0, therefore the distributions are close to symmetry
- tend to a negative skewness, thus a right-leaning curve

- **Kurtosis** for BTC and GOLD are
- bigger than 4 and thus leptokurtic (heavy-tailed).





CrixToDate

Theoretical Quantiles (Standard Normal Quantiles) / Sample Quantiles (Quantiles of Input Sample) of BTC and GOLD (!Weekends cleared) based on 24/7 data.

Appendix

Abbrev.	CC	Website
ADA	Cardano	`cardano.org`
BCH	Bitcoin Cash	`bitcoincash.org`
BTC (XBT)	Bitcoin	`bitcoin.com`, `bitcoin.org`
BTS	BitShares	`bitshares.org`
CNMT	Coinomat	`coinomat.com`
DASH	Dash	`dash.org`
ETH	Ethereum	`ethereum.org`
ETC	Ethereum Classic	`ethereumclassic.github.io`
GOLD	SPDR Gold Shares	`spdrgoldshares.com`
LTC	Litecoin	`litecoin.com`, `litecoin.org`
MAID	MaidSafeCoin	`maidsafe.net`
NEO	NEO	`neo.org`
NXT	Nxt	`nxt.org`
PPC	Peercoin	`peercoin.net`
STEEM	Steem	`steem.io`, `steemit.com`
XLM	Stellar	`stellar.org`
XMR	Monero	`getmonero.org`
XPY	PayCoin	`paycoin.com`
XRP	Ripple	`ripple.com`

Political economy

CCs beyond CCs (e.g. Tokens)

Governance

- e-estonia.com
- United Kingdom (smart permits)

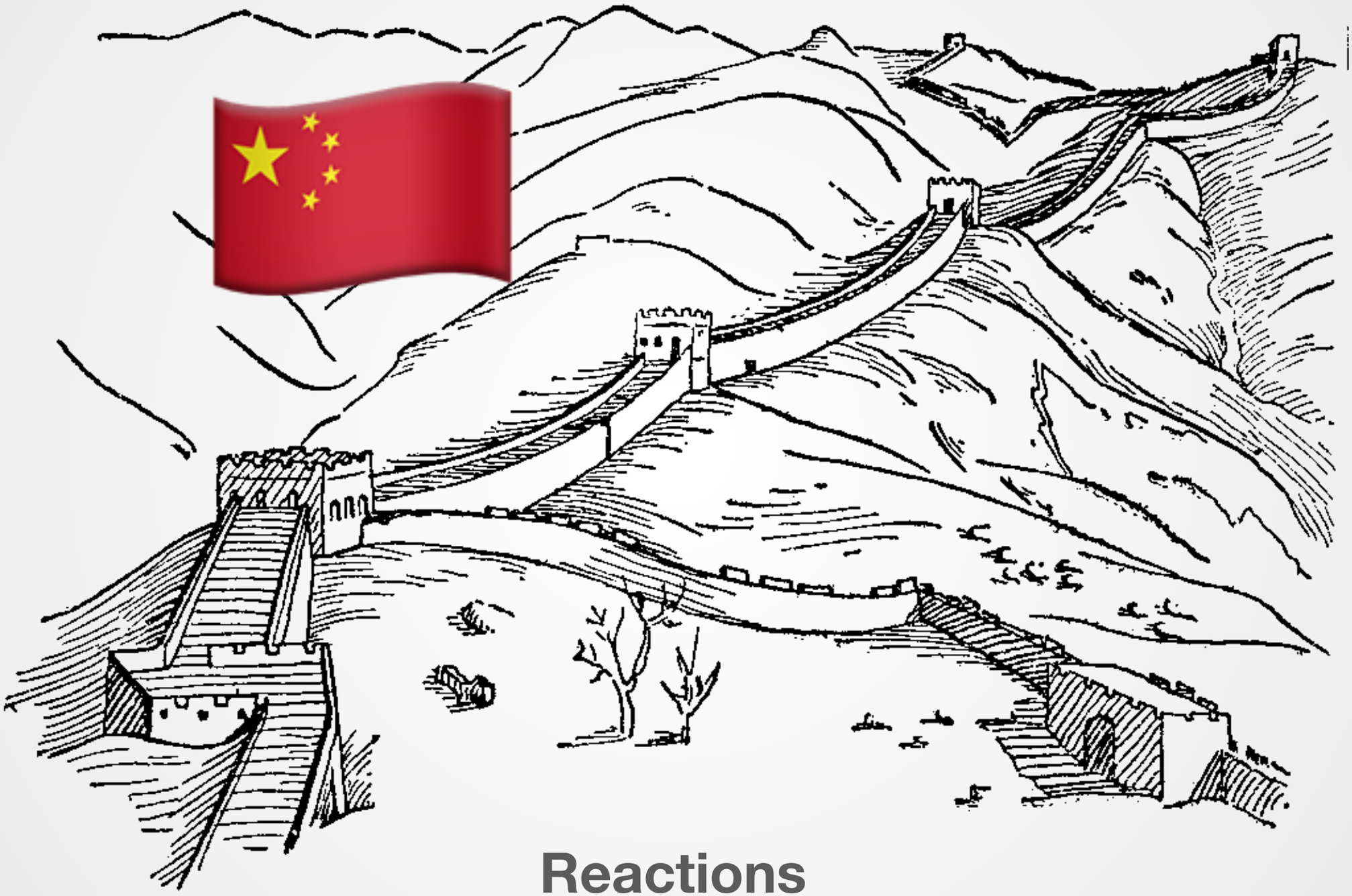
…

Public Ledgers

- Deutsche Bundesbank
- Russian Federation state agencies and banks

…

REPUBLIC OF ESTONIA
E-RESIDENCY



Reactions

People’s Republic of China - South Korea - United States of America …

or: Venezuela’s „Petro"

Chance, Risk and Opportunities

What we have at hand:

- Highly dynamic systems and networks
- High dimensional and high frequency data
- Unclear legislative status, e.g. for ICO's
- No established businesses or precedents
- …

Silicon Valley didn't have smarter people;

they just **had people** who were wired to take different risks,

who actually came out to California

to take risks and to get away from the status quo.

Steve Blank
(Interview with Harvard Business Review, [1]. 3 August 2017)