

July 16

2020

REPORT TRIMESTRALE

2020 Q2



Digital Gold Institute: Vision

R&D center of excellence focused on teaching, training, consulting, and advising about scarcity in digital domain (bitcoin and crypto-assets) and the underlying blockchain technology



Bitcoin: Digital Gold

The most successful attempt at creating *scarcity in the digital realm* without a trusted third party. *Bitcoin is the digital equivalent of gold, disruptive for our current digital civilization and the future of money and finance.* More a crypto-commodity than a crypto-currency, Bitcoin aims to be world reserve asset.



Beyond Bitcoin: Timestamping

A timestamp demonstrates that a document existed in a specific status prior to a given point in time. Digital data can be securely timestamped though the attestation of its hash value in a blockchain transaction. *What jewellery is for gold, Timestamping could be for bitcoin: not essential but effective at leveraging its beauty.*



Blockchain: Hype or Reality?

Blockchain requires an intrinsic native digital asset to provide the economic incentives for the blockchain maintainers to be honest. Without the seigniorage revenues associated to its native asset, a blockchain system would need to select and appoint its maintainers, ultimately resorting to central governance.



Financial Services for Crypto

The most promising field, instead of technological applications of blockchain, is the development of financial services for crypto assets: those tools, practices, and facilities needed by institutional investors and high net worth individuals. *Finance might not need blockchain, but the blockchain economy needs new financial services.*

Digital Gold Institute: Services

R&D center of excellence focused on teaching, training, consulting, and advising about scarcity in digital domain (bitcoin and crypto-assets) and the underlying blockchain technology

Partnership Program



Becoming one of our [partners](#) means empowering your business with a proper understanding of Bitcoin, crypto assets, and blockchain technology. It is a strategic choice that will allow you to leverage unique opportunities while avoiding the irrational hype that pollutes these topics.

Research



Our research activity includes quarterly [reports](#) on the bitcoin and blockchain ecosystem and the thesis works of our [students](#). Anyway, the bulk of the activity is happening at the [Crypto Asset Lab](#) (CAL), a joint research initiative with the University of Milano-Bicocca.

Training Program



We offer training and education about Bitcoin, crypto assets, blockchain, distributed ledger, smart contracts, and cryptography: the program is based on the [Bitcoin and Blockchain Technology](#) course taught at Milano-Bicocca and other universities.

Development



We [write code](#) and love to get our hands dirty in programming and technology. Check out our [OpenTimestamps calendar](#) free facility and [btclib](#), an open-source Python library intended for teaching/learning/using bitcoin, its blockchain, and the associated elliptic curve cryptography.

Digital Gold Institute: Partners

Educational Program Partner



Partner



The DGI Quarterly Report

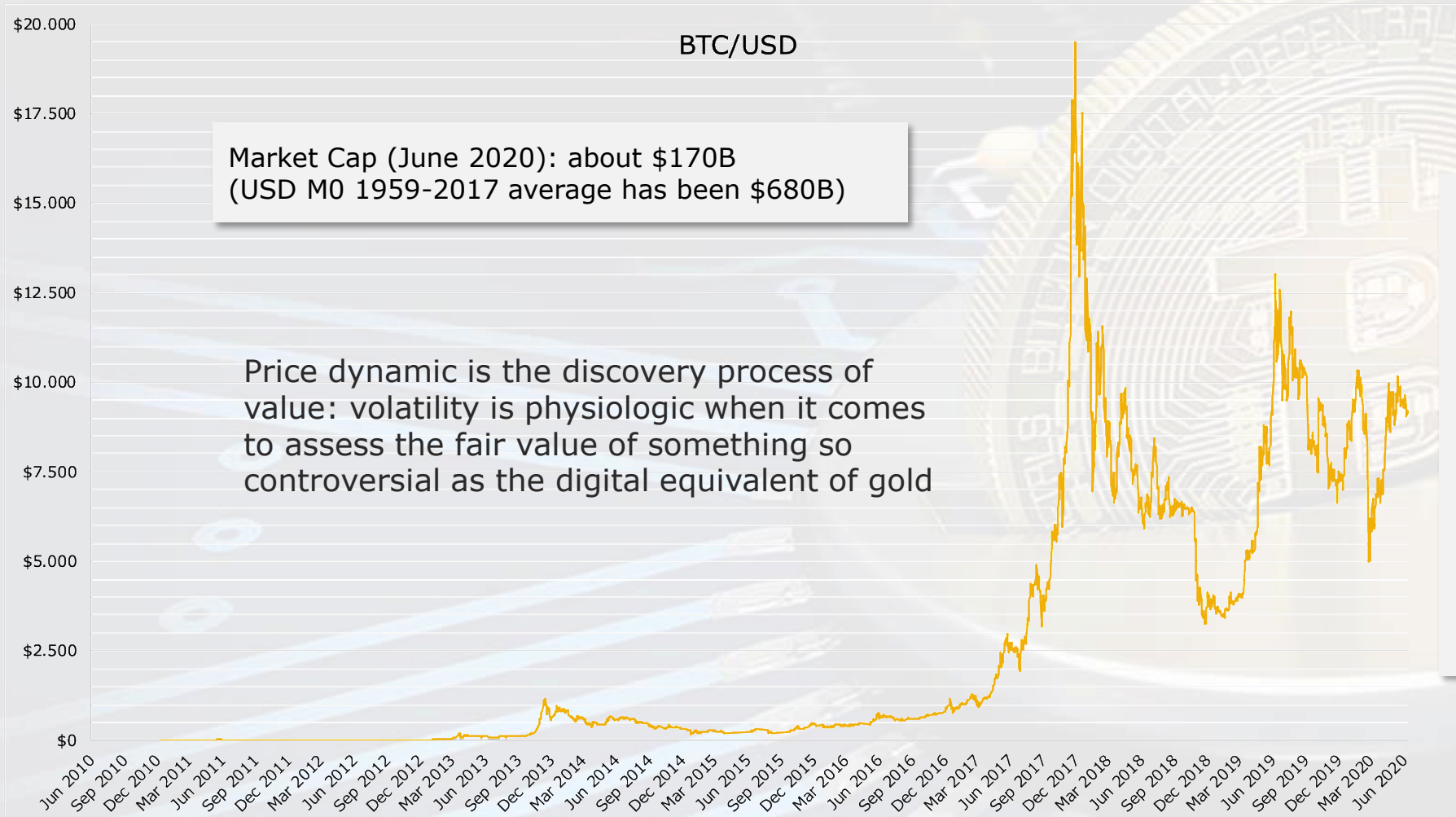
- Exclusive for our partners and their guests
- A quarterly update on the crypto assets world with a focus on:
 1. **Market**
 2. **Technology**
 3. **Regulation**
 4. **Ecosystem**
 5. **Updates from the Institute**



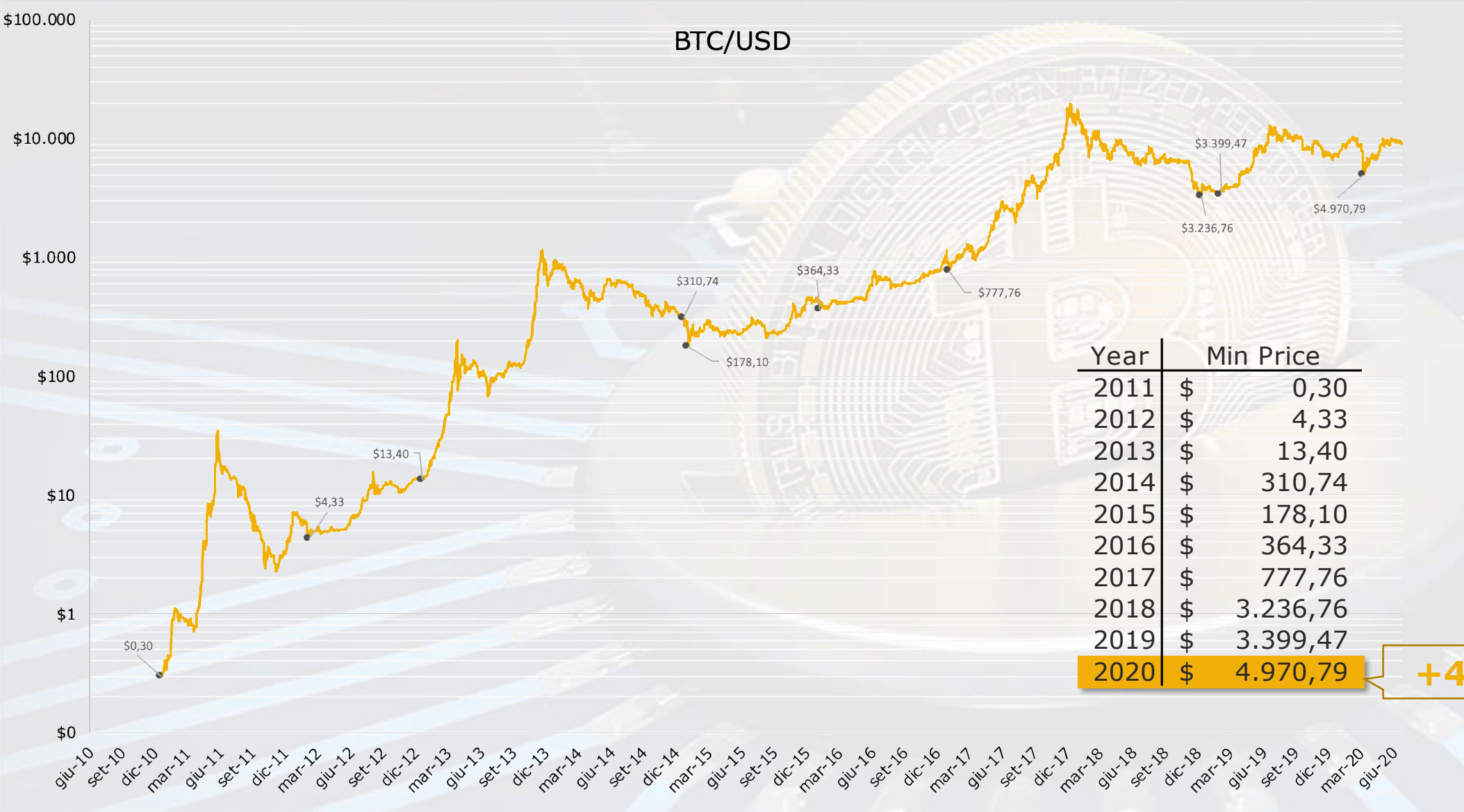


1. MARKET

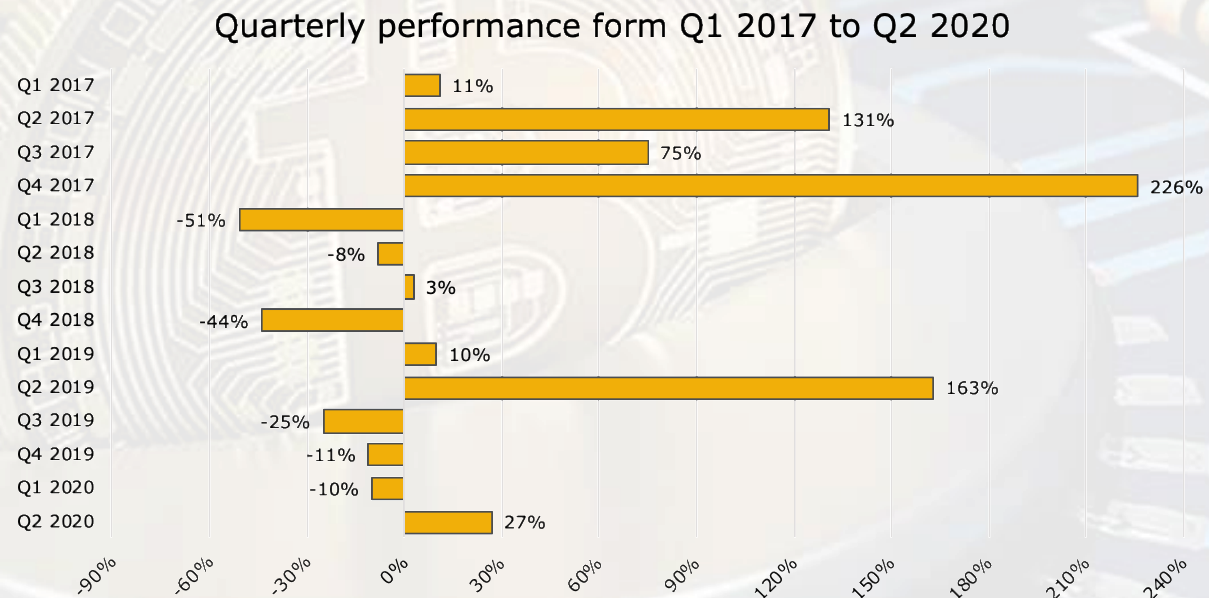
Bitcoin Performance



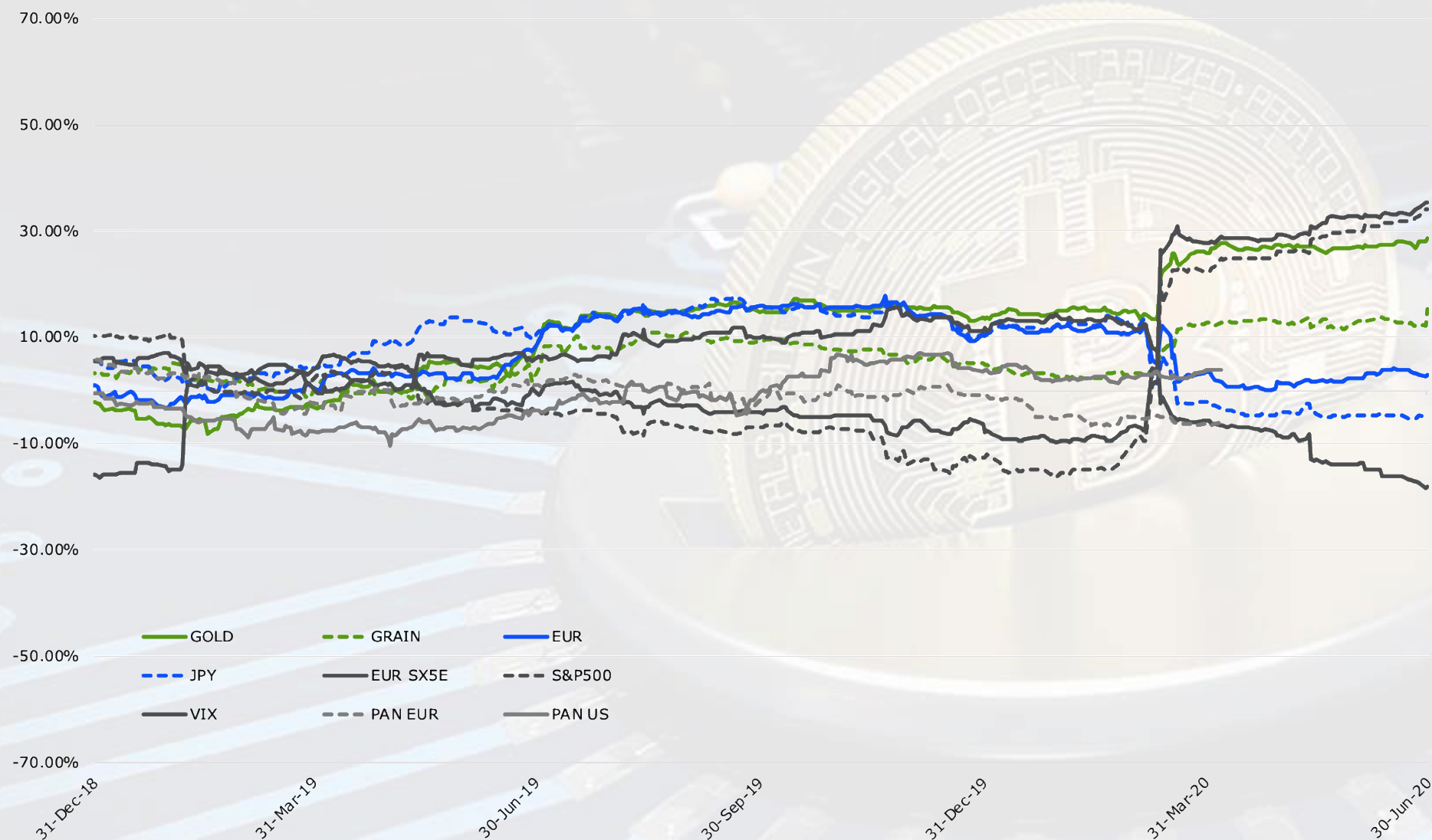
Bitcoin Performance (Log Scale)



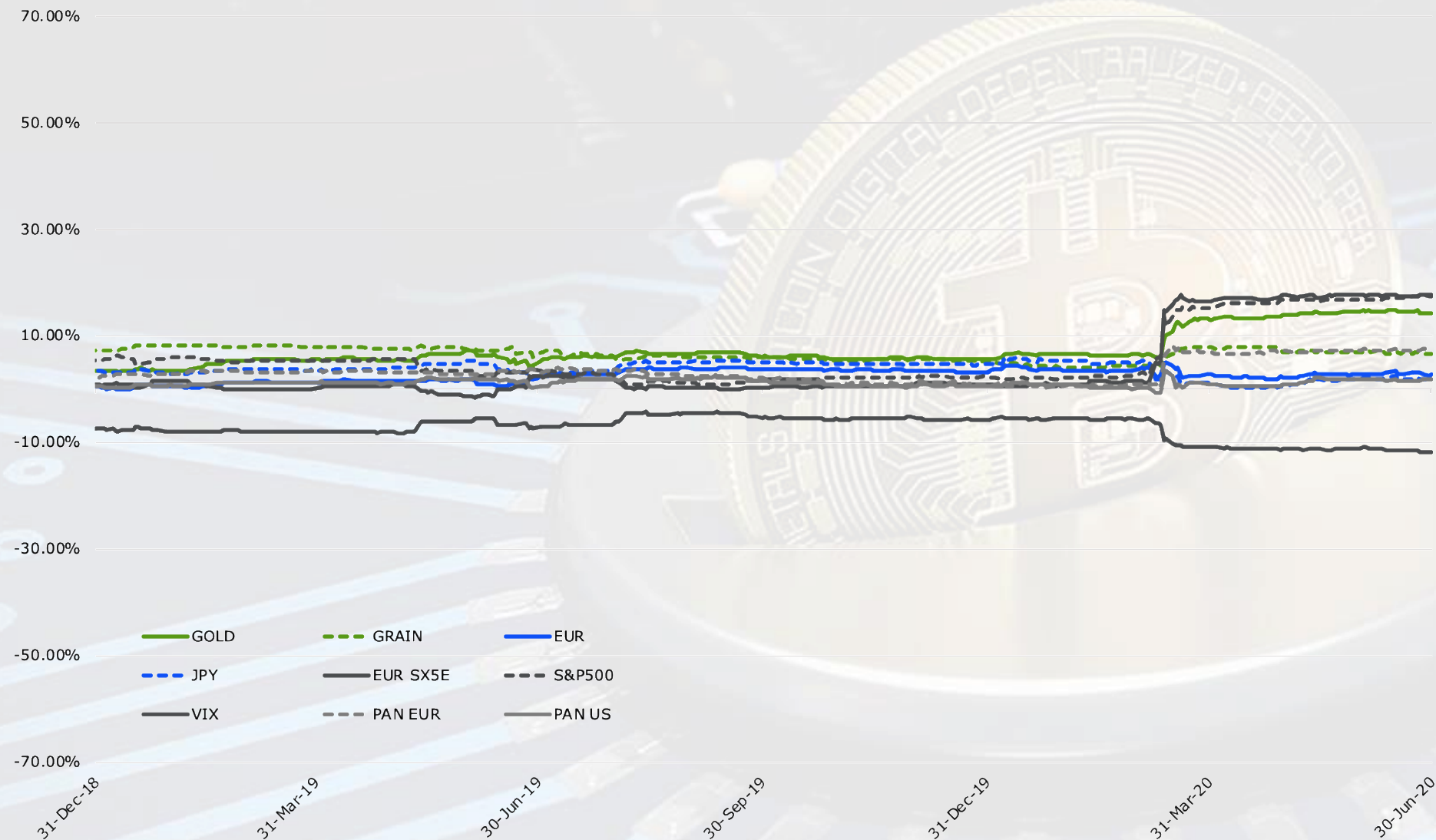
Bitcoin Performance (2020 Q2)



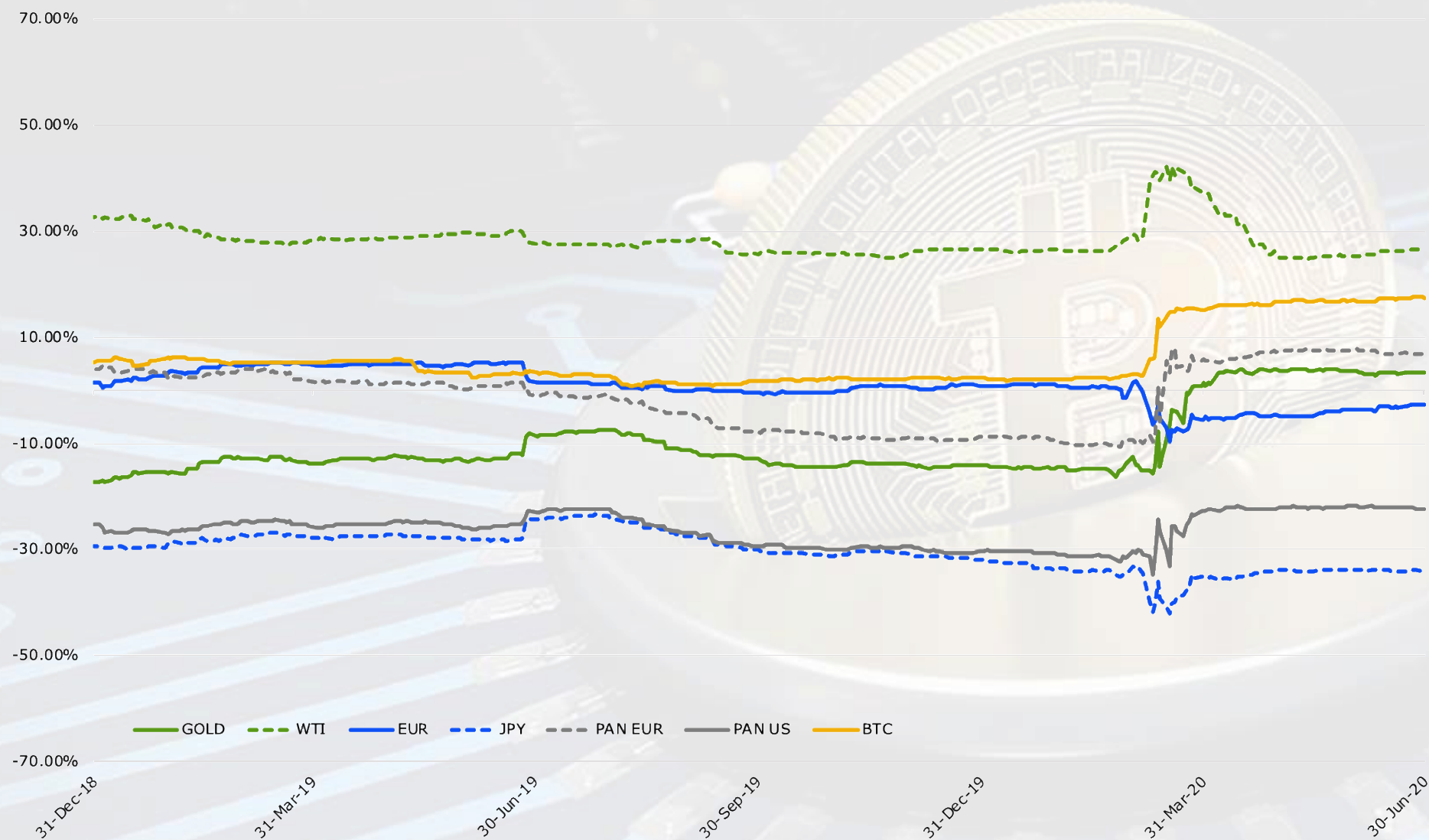
Correlation with Bitcoin: 1Y rolling window



Correlation with Bitcoin: 3Y Rolling Window



Correlation with S&P500: 3Y rolling window



Correlation Matrix (1/3)

3Y																																
BTC	100.00%																			Data set: 2017-07-01 / 2020-06-30												
ETH	16.50%	100.00%																														
LTC	14.58%	78.24%	100.00%																													
XRP	12.99%	68.11%	57.01%	100.00%																												
GOLD	14.30%	7.47%	4.86%	4.31%	100.00%																											
IND MET	3.50%	1.81%	1.41%	8.23%	8.27%	100.00%																										
WTI	11.31%	1.00%	0.91%	2.60%	6.22%	17.37%	100.00%																									
GRAIN	7.06%	0.37%	0.21%	1.15%	4.31%	6.09%	11.71%	100.00%																								
EUR	2.68%	7.50%	5.04%	4.22%	37.09%	21.73%	-4.38%	5.33%	100.00%											Positive												
CHF	2.18%	7.12%	4.12%	2.41%	41.55%	11.19%	-8.18%	3.30%	75.89%	100.00%										Negative												
GBP	5.89%	8.03%	5.04%	2.92%	28.06%	21.03%	6.07%	3.70%	57.83%	44.54%	100.00%																					
JPY	1.86%	8.91%	6.07%	3.66%	41.59%	-7.09%	-18.25%	-6.73%	44.12%	60.34%	27.22%	100.00%																				
NASDAQ	17.40%	-8.18%	-5.83%	-3.24%	3.66%	27.05%	25.52%	11.59%	-4.87%	-15.87%	10.82%	-34.49%	100.00%																			
EURSX5E	17.83%	5.10%	4.88%	4.91%	2.57%	32.97%	20.11%	15.21%	-5.80%	-20.91%	17.39%	-36.21%	61.25%	100.00%																		
S&P500	17.50%	-7.30%	-5.64%	-2.44%	3.34%	28.46%	26.62%	11.58%	-2.56%	-13.97%	14.31%	-34.09%	96.42%	66.59%	100.00%																	
MSCIBRIC	10.91%	4.42%	4.91%	4.67%	5.61%	44.53%	20.87%	13.22%	9.67%	-2.91%	24.33%	-22.90%	58.19%	67.10%	59.01%	100.00%																
VIX	-11.72%	1.64%	4.76%	-3.60%	5.94%	-21.92%	-20.79%	-15.98%	4.50%	17.86%	-5.72%	33.17%	-72.45%	-46.77%	-69.66%	-44.56%	100.00%															
EURAGG	7.70%	1.52%	-0.78%	1.63%	30.40%	-8.31%	7.88%	0.83%	-0.64%	10.51%	10.17%	20.93%	5.55%	10.46%	5.67%	6.06%	-1.48%	100.00%														
PANEUR	7.66%	4.17%	1.65%	2.17%	30.84%	-6.86%	8.60%	0.92%	-6.09%	9.46%	26.61%	22.73%	6.19%	13.66%	6.59%	9.20%	-1.08%	93.11%	100.00%													
PANUS	1.73%	4.58%	4.23%	2.94%	39.39%	-9.32%	-4.29%	-3.67%	21.59%	34.95%	16.78%	51.95%	-21.79%	-12.19%	-22.43%	-14.17%	24.01%	50.89%	53.57%	100.00%												
	BTC	ETH	LTC	XRP	GOLD	IND MET	WTI	GRAIN	EUR	CHF	GBP	JPY	NASDAQ	EURSX5E	S&P500	MSCIBRIC	VIX	EURAGG	PANEUR	PANUS												
	Crypto-currency				Commodity				Currency				Equity				Volatility	Bond														

Data set: 2017-07-01 / 2020-06-30

Positive
Negative

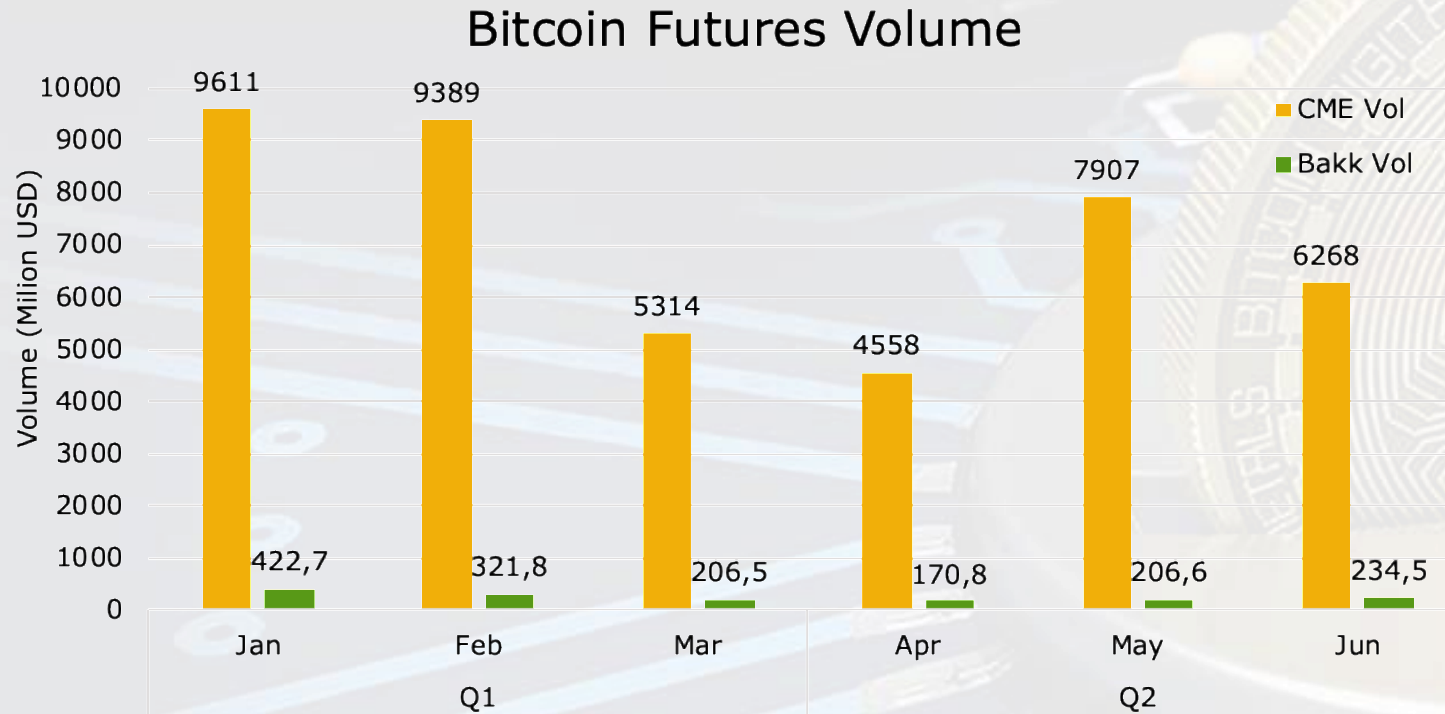
Correlation Matrix (2/3)

1Y																				
BTC	100.00%																			
ETH	18.33%	100.00%																		
LTC	18.30%	92.01%	100.00%																	
XRP	18.20%	88.08%	86.68%	100.00%																
GOLD	27.20%	13.79%	8.80%	7.28%	100.00%															
IND MET	8.00%	2.35%	-0.28%	4.62%	-15.45%	100.00%														
WTI	22.52%	-1.02%	2.12%	3.59%	6.67%	19.42%	100.00%													
GRAIN	12.96%	0.56%	-4.79%	-3.02%	3.47%	12.00%	17.97%	100.00%												
EUR	1.20%	15.70%	12.02%	9.83%	21.38%	16.10%	-9.84%	6.60%	100.00%											
CHF	-1.93%	15.57%	12.36%	9.42%	29.30%	2.99%	-12.90%	1.95%	84.57%	100.00%										
GBP	14.28%	24.56%	18.16%	17.56%	20.88%	29.54%	7.73%	7.13%	56.25%	47.26%	100.00%									
JPY	-6.19%	17.64%	13.62%	13.60%	27.56%	-15.08%	-24.24%	-16.69%	52.61%	67.21%	31.47%	100.00%								
NASDAQ	36.65%	-20.96%	-17.79%	-17.62%	8.77%	42.18%	26.59%	22.27%	-12.63%	-22.36%	15.24%	-42.50%	100.00%							
EURSX5E	36.55%	6.16%	4.75%	6.08%	11.88%	47.80%	18.50%	24.09%	-2.49%	-18.47%	27.24%	-34.04%	69.45%	100.00%						
S&P500	35.44%	-18.91%	-15.87%	-15.48%	8.01%	43.49%	26.23%	21.32%	-8.40%	-18.99%	19.33%	-39.53%	97.74%	72.65%	100.00%					
MSCIBRIC	21.94%	5.54%	3.00%	5.87%	3.07%	57.81%	20.92%	19.89%	2.61%	-10.50%	30.65%	-31.09%	65.31%	77.90%	67.77%	100.00%				
VIX	-19.29%	15.74%	14.11%	11.84%	8.53%	-35.96%	-24.36%	-26.22%	15.64%	30.25%	-7.11%	45.54%	-74.76%	-54.79%	-71.88%	-48.69%	100.00%			
EURAGG	16.29%	8.07%	1.67%	7.29%	38.31%	-8.09%	10.60%	4.62%	10.55%	20.76%	25.63%	20.86%	7.41%	13.64%	8.34%	11.46%	-1.07%	100.00%		
PANEUR	16.07%	13.65%	6.22%	11.61%	38.93%	-3.37%	11.58%	4.80%	8.52%	19.53%	41.74%	22.71%	9.89%	18.76%	10.99%	17.64%	-3.97%	94.57%	100.00%	
PANUS	3.61%	12.52%	11.24%	9.25%	41.81%	-10.52%	-1.68%	-9.70%	38.94%	48.83%	31.39%	58.16%	-21.58%	-7.26%	-21.08%	-13.17%	25.35%	53.25%	56.13%	
	BTC	ETH	LTC	XRP	GOLD	IND MET	WTI	GRAIN	EUR	CHF	GBP	JPY	NASDAQ	EURSX5E	S&P500	MSCIBRIC	VIX	EURAGG	PANEUR	PANUS
	Crypto-currency				Commodity				Currency				Equity				Volatility	Bond		

Data set: 2019-07-01 / 2020-06-30

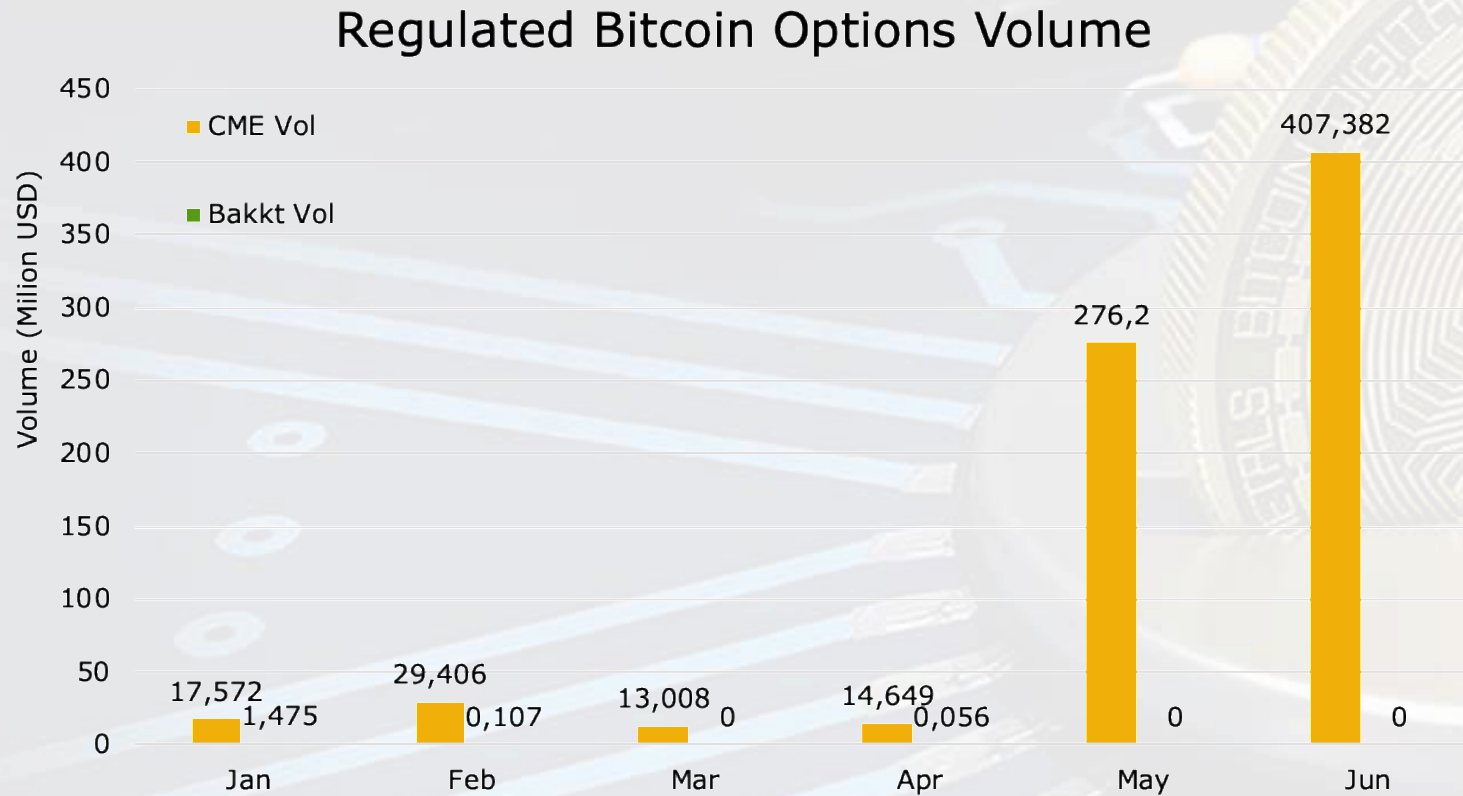
Positive
Negative

Bitcoin Listed Futures



- After a drop in volumes due to Covid-19 in May the CME Futures market restarted
- CME is still the market leader
- Bakkt physically settled Futures continue to show low volumes

Bitcoin Listed Options

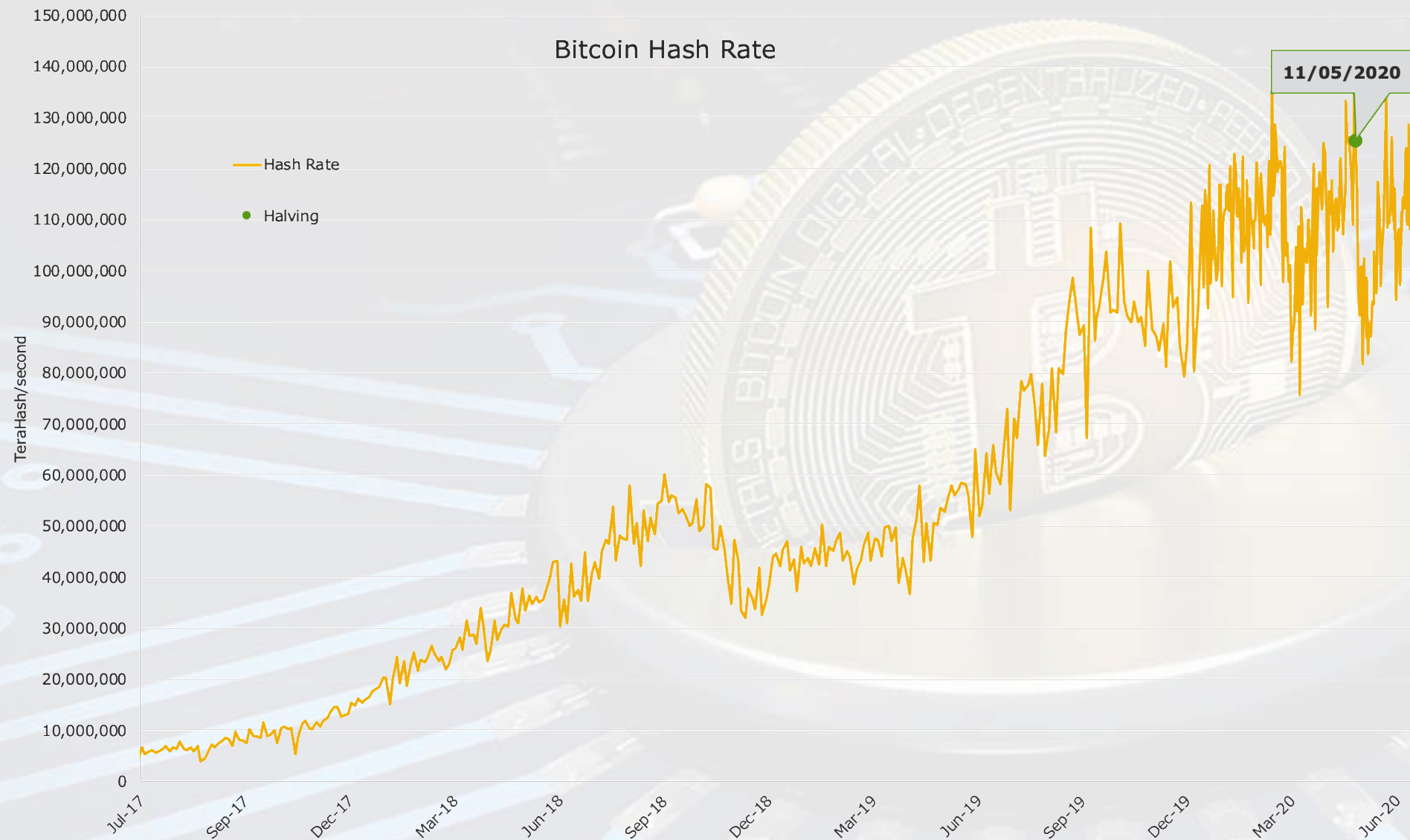


- CME Options traded volumes exploited in May
- Bakkt options instead had zero volume
- The option market is starting gaining interest and a lot of new player are approaching this market
- Not regulated options, like the one proposed by Deribit, are still by far the most traded



2. TECHNOLOGY

Bitcoin Network Hash Rate



Bitcoin – Halving & Mining (1/2)

- Mining difficulty reached almost an All-Time High (ATH) in the adjustment before the halving (May 11)
- Then, it had two consecutive declines on May 20 and June 4, dropping down to January levels
- After that, on June 16 there has been a 14.95% increase, the biggest difficulty increase in nearly 2.5 years
- Finally, it set a sequence of ATHs peaking at 17.35 trillion difficulty on July 1 (about 124 EH/s)

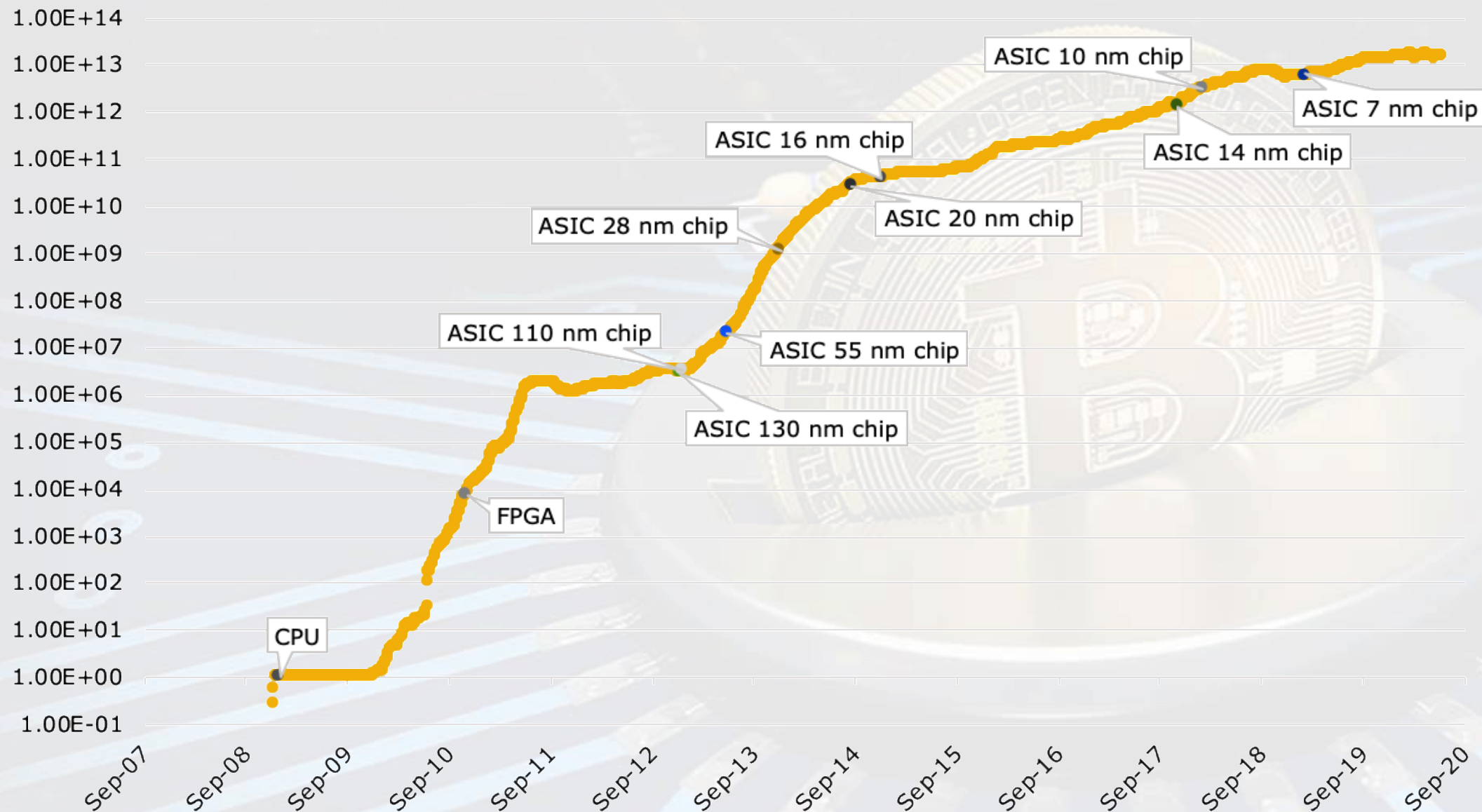
Bitcoin – Halving & Mining (2/2)

- Halving has been a non-event
- Covid-19 has interfered with supply of new hardware
- China remains, by far, the leading region for bitcoin mining, contributing roughly 60 percent of the global hash-rate, followed by Russia with 15 to 20 percent and North America with roughly 15 percent



Bitcoin mining farm (CoinDesk archives)

Mining is Hitting Semiconductor Limits



Bitcoin - Protocol Update

Bitcoin 0.20 protects against potential nation-state/large-ISP attacks

- An *Erebus* attack allows nation-states and/or large internet providers such as Amazon Web Services to spy, double-spend or censor bitcoin transactions
- The *Asmap* configuration protects the peer-to-peer architecture of bitcoin nodes by limiting the connections made to any single Internet Tier 1 or larger Tier 2 Autonomous Systems
- Bitcoin core all time high: 510 commits in April
- Over 800 contributors to the protocol



Bitcoin: Second Layer



In June the holders of the network's emergency two-of-three multisig wallet moved 870 bitcoins that had been stuck in a queue since June 11



Researchers used a privacy vulnerability to construct snapshots of the Lightning Network at different time intervals, detecting payment movements, their senders, recipients, and amounts

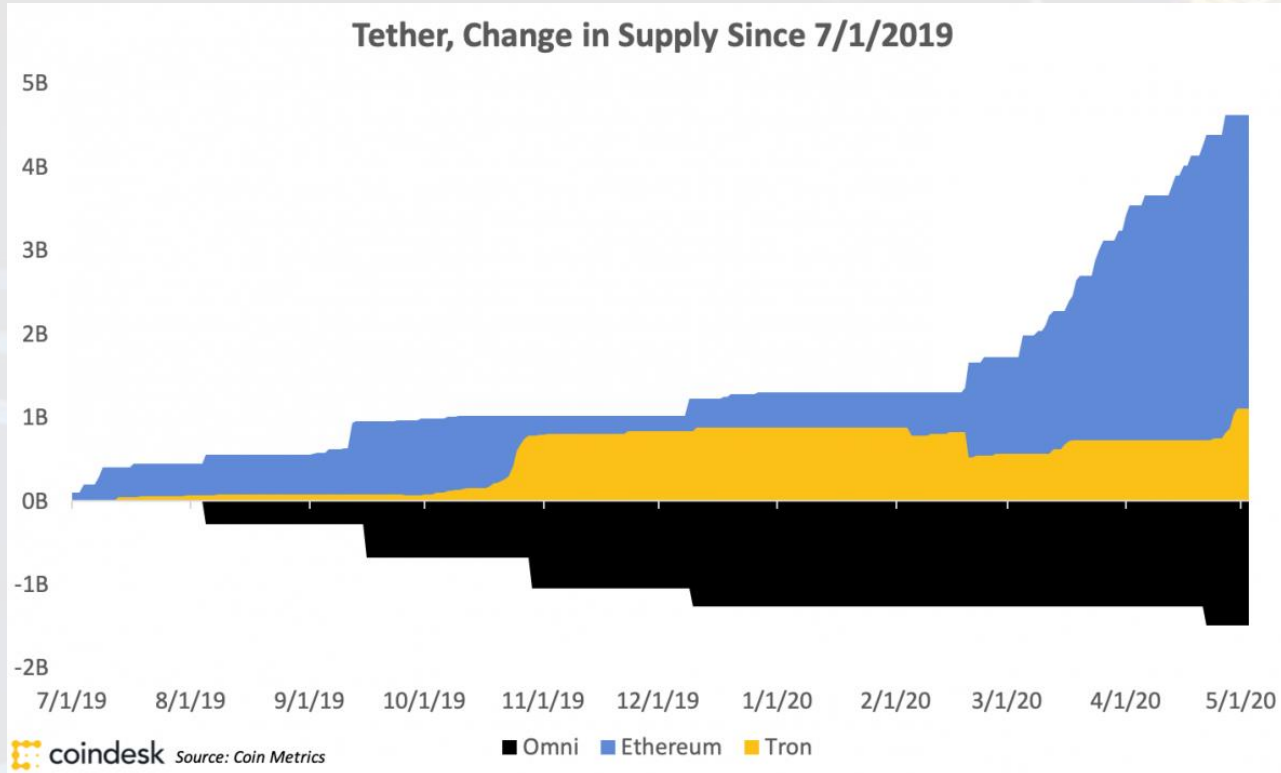


Ethereum



- *The Good:*
 - total value transferred on the Ethereum network, including ether and ERC-20 stablecoins, now matches that of the Bitcoin network
- *The Bad:*
 - Berlin hard fork has been delayed to give clients other than Geth (79% of Ethereum nodes run on it) a chance to increase their share of the network
 - Gavin Wood, an original co-founder of Ethereum, founder of Parity Technologies (the maintainer of the second most relevant client) is touting Polkadot instead of Ethereum
- *The Ugly:*
 - At the *Consensus: Distributed* event Vitalik Buterin said that Ethereum 2.0 (PoS) will launch in July
 - Afri Schoedon countered on Twitter: “Going on stages or panels and putting out dates is not helpful at all. The final spec is not implemented in any client and we didn't launch a coordinated testnet yet.”

Tether



- Volume growth is hitting new all-time highs
- Ethereum is the main platform for Tether
- Or maybe one should say Tether is the only real driver of the Ethereum growth

Coin Centralization



- The community that drove the Steem blockchain largely broke off to form Hive, to stop Justin Sun take-over
- Steem blockchain hard forked to seize the tokens of the dissenters
- Exchanges (Binance, Bittrex) had to take a camp in supporting hard forks, confiscations, and counter-measures in the fight between opponents involving millions of dollars



- Block.one, the Cayman Island based company which controls 10% of EOS tokens, has requested geographic location of the block producer candidates to support and vote for, to fight back the "Chinese oligarchy"

Telegram TON

- Telegram has agreed to pay \$18.5M penalty in SEC settlement over failed TON offering
- In a letter to Telegram Open Network (TON) investors, the company said American investors are not eligible for a 110% loan refund option in April 2021 and should take a 72% refund amount
- Investors are in discussion to sue Telegram



Blockchain Hype

- IBM, Oracle and the World Health Organization (WHO) are among the collaborators on an open-data hub that will use blockchain technology to check the veracity of data relating to the coronavirus pandemic
- The World Economic Forum (WEF) is still pitching blockchain as the savior of failing global supply chains and says its blockchain deployment toolkit
- Amazon has patented the use of DLT to infuse “digital trust from the first mile of an item’s supply chain”
- China is leading POC on supply chain, DLT interoperability, etc.

Blockchain for Financial Markets



- Nasdaq has partnered with R3 to offer a platform for digital asset marketplaces on the Corda blockchain

DTCC

Securing Today. Shaping Tomorrow.SM

- Depository Trust & Clearing Corporation (DTCC), a giant of financial markets infrastructure, is **still** studying whether distributed ledger technology (DLT) could accelerate its processing of securities

Blockchain Voting

- American Association for the Advancement of Science's Center for Scientific Evidence in Public Issues: *"At this time, internet voting is not a secure solution for voting, nor will it be in the foreseeable future"*
- *"Blockchains are a data structure, they're a way of storing data, but they don't deal with the main security issues of internet voting"*, added Barbara Simons, a fellow with the Association for Computing Machinery and the American Association for the Advancement of Science
- Online voting is "high risk" because ballots can be manipulated "at scale", without a paper trail as recourse mechanism
- Constitutional changes will be blockchain voted in Russia, also including the change to allow Vladimir Putin to stay in power for more than the current limit of two consecutive six-year terms



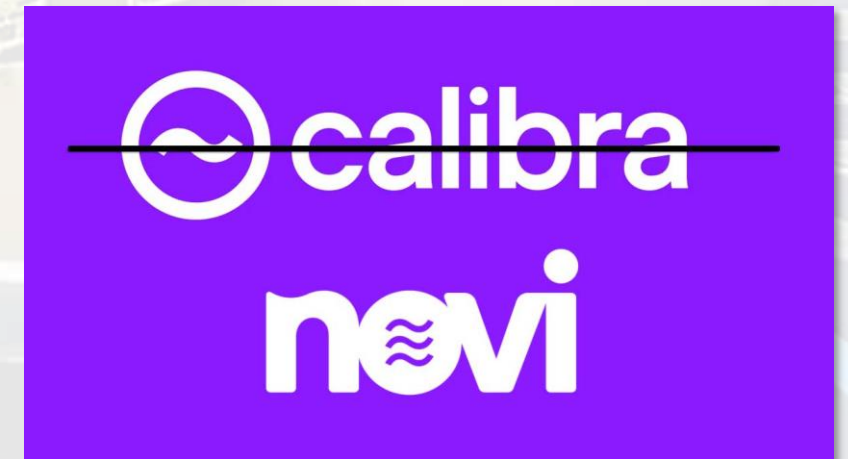
3. REGULATION

Libra Scales Back Its Ambitions


New White Paper

1. Offering single-currency stablecoins in addition to the multi-currency coin
2. Enhancing the safety of the Libra payment system with a robust compliance framework
3. Forgoing the future transition to a permissionless system while maintaining its key economic properties
4. Building strong protections into the design of the Libra Reserve

The *Calibra* wallet has been renamed as *Novi*



Central Bank Digital Currency (1/2)

- BIS: *CBDC is not a reaction to Libra* 
- March 2019, three months before Facebook unveiled the Libra cryptocurrency, BIS chief Agustín Carstens said central banks “are not seeing the value” of CBDCs. By July he had changed his tune, saying CBDC issuance might come “sooner than we think”
- China is a driving force
- In EU the Dutch Central Bank is pushing for CBDC more programmable than bitcoin, not using DLT
- FED paper points out the risks for commercial banks

Central Bank Digital Currency (2/2)



- The rationale for issuing e-krona in the digital era
- Need for convertibility between commercial bank money and publicly available central bank money
- Competitive aspects of e-krona
- The Riksbank's seigniorage and the e-krona
- Adverse effects on the supply of bank loans and thereby macroeconomic activity of the issuance of a CBDC
- E-krona design models

InterVasp Messaging Standard 101 (1/2)

- Crypto Industry adopts messaging standard to comply with Travel Rule
- Developed by the Joint Working Group for interVASP Messaging Standards (JWG)
- CAL joined the JWG



A New Standard For The Crypto Industry IVMS101

Universal common language for communication of required originator and beneficiary information between virtual asset service providers.

ESTABLISHED BY LEADING INDUSTRY BODIES:

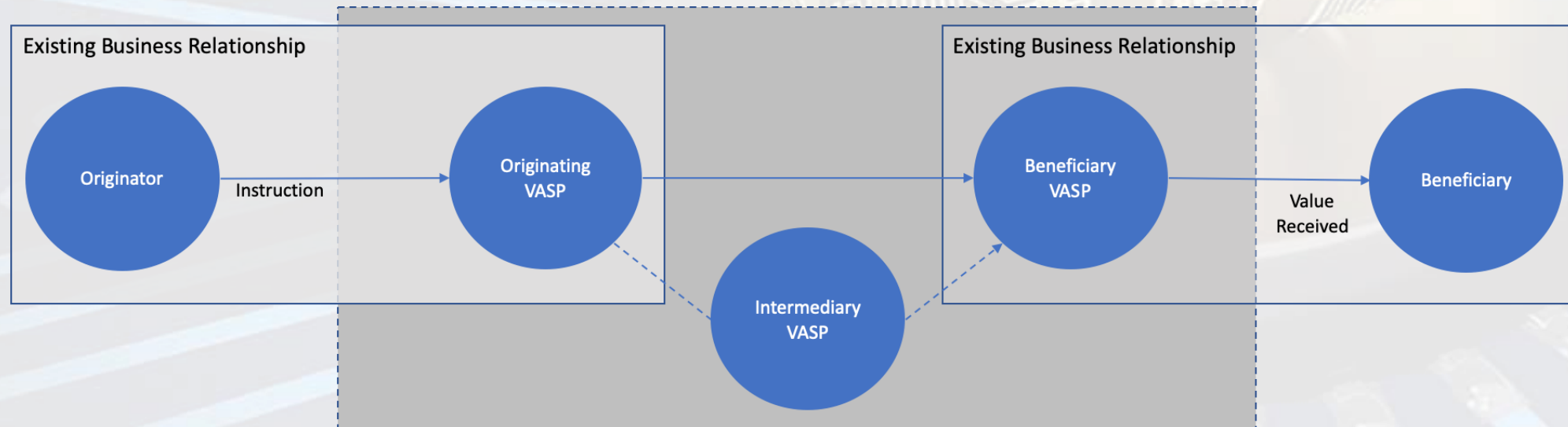


visit:
intervasp.org

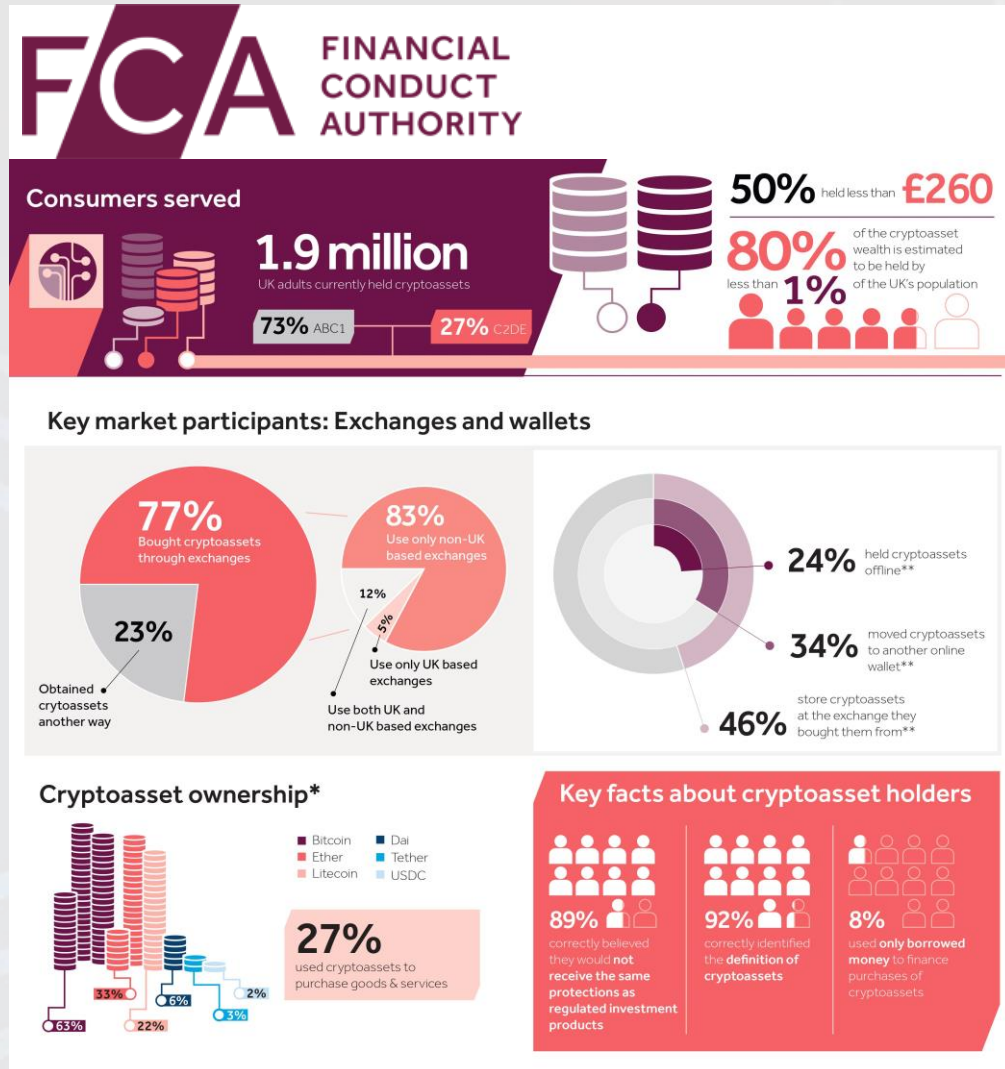


InterVasp Messaging Standard 101 (2/2)

- The new technical standard aims to facilitate exchange of data between Virtual Asset Service Providers (VASPs)
- IVMS101 is a data model to enable a universal common language for communication of required originator and beneficiary information between VASPs.
- Data model payload:

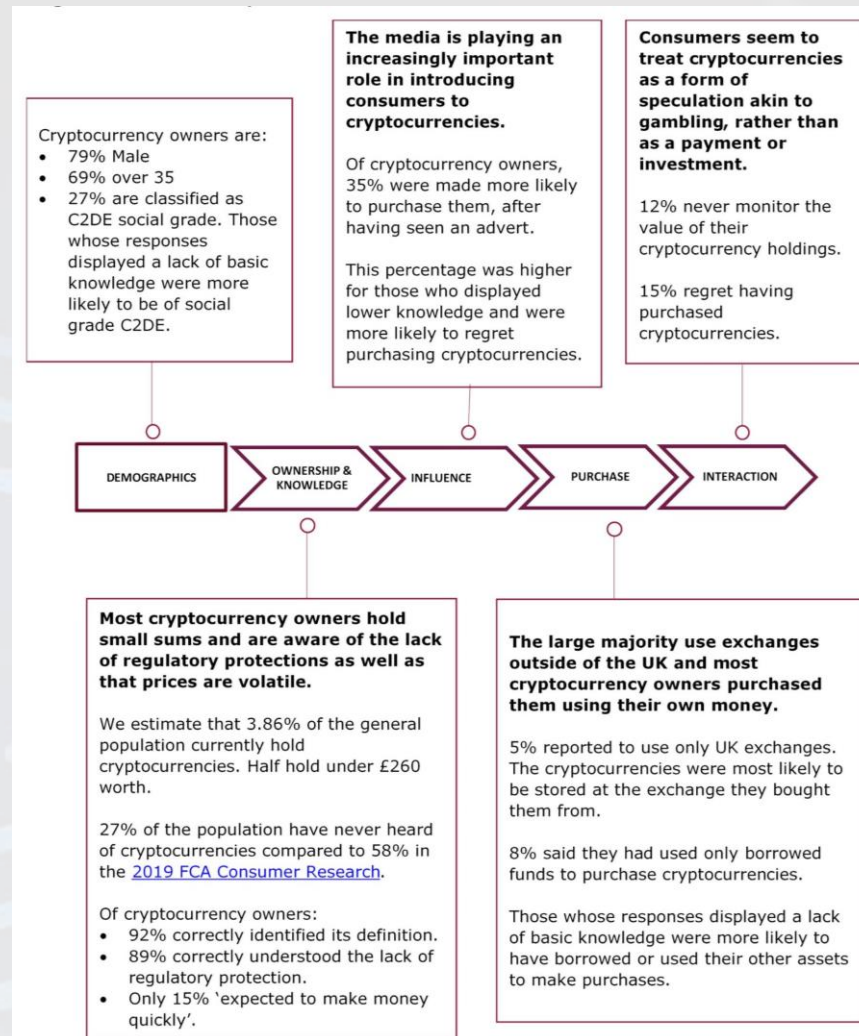


Crypto Asset Consumer Research 2020 (1/3)



- **Demographics:**
 - 79% male
 - 69% over 35 years old
- **Ownership & Knowledge:**
 - the typical cryptocurrency owner holds small sums of cryptocurrencies
 - 3.86% of the general population currently hold cryptocurrencies
 - Most of them appear to understand the lack of regulatory protection

Crypto Asset Consumer Research 2020 (2/3)



■ Influencers:

- News media is playing an increasing role
- those influenced by advertising were more likely to subsequently regret the purchase

■ Purchase:

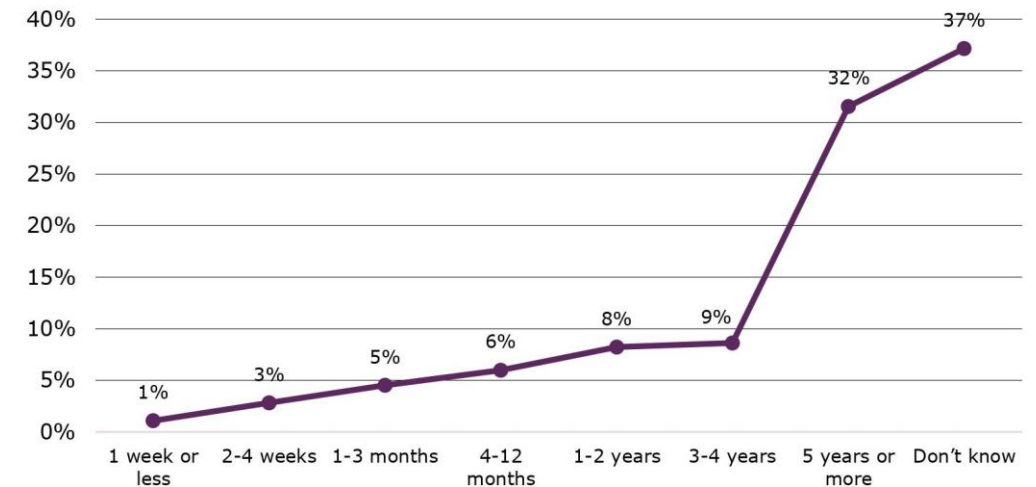
- Those with lack of knowledge have financed their purchases of crypto with borrowed money and/or other assets

Crypto Asset Consumer Research 2020 (3/3)

Interaction:

- Most treat crypto as a form of speculation akin to gambling
- Payment: 25% use crypto to purchase goods and services
- Investment: most current crypto owners intend expect to hold them for long periods of time.

How long do you expect to hold your cryptocurrencies?



Base: Current cryptocurrency owners N = 491



4. ECOSYSTEM

Crypto-Assets Custody

- The industry keeps moving toward insurance guarantees and (SOC) attestations:
 - Bakkt has onboarded more than 70 clients for its custody services and given them the option to tap more than \$600 million in insurance coverage overall
 - Gemini has completed the SOC 1 Type 1 examination in March
- The Bitcoin community and ecosystem is moving too:
 - Bryan Bishop has released a prototype for its secure on-chain storage *Bitcoin Vaults*
 - Kevin Loaec of Chainsmiths took it and modified it as *Revault*, a product for companies who need to move the funds often and relatively fast
 - CheckSig goes live in July with its protocol; the protocol will go public in early 2021

CheckSig

Decentralized Finance

- Coinbase has deposited \$1.1 million of USDC stablecoins into the pools powering two of the most popular decentralized finance (DeFi) applications on Ethereum: Uniswap and PoolTogether
- AVA Labs COO Kevin Sekniqi: *“There is nothing about [DeFi] that is decentralized”*, just as susceptible to fallible people and relationships built on trust as traditional finance
- AVA Labs hope to conduct a “brain merge” that will bring those in traditional finance and blockchain together

European Cybercrime Centre: Wasabi Bits



- Wasabi is a very effective decentralized method of mixing bitcoin using a «coinjoin» with many privacy-focused options
- Possibly the most convenient and secure way to mix bitcoins
- Increasing number of cases featuring Wasabi Wallet, also involving criminal activities
- ECC law enforcement-relevant considerations:
 - Easy to visually identify Wasabi wallet transaction;
 - Tracing tools identify most of the addresses but do not demix the transactions;
 - Possible to follow the money but high probability of staying undetected

Craig Wright: Controversial Credibility



“Craig Steven Wright is a liar and a fraud. He doesn't have the keys used to sign this message.”

This message was signed with a private key allegedly under the control of Craig Wright



5. UPDATES FROM THE INSTITUTE

Crypto Assets in Asset Allocation



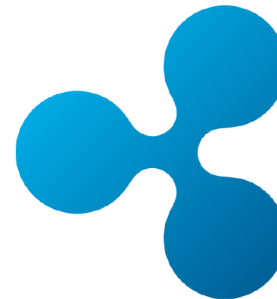
The first protocol to solve the problem of **double-spending** without the need for a centralized party and to achieve **scarcity** in the digital realm



Backed by a blockchain, the technology is aimed at a specific use case: **smart** contracts



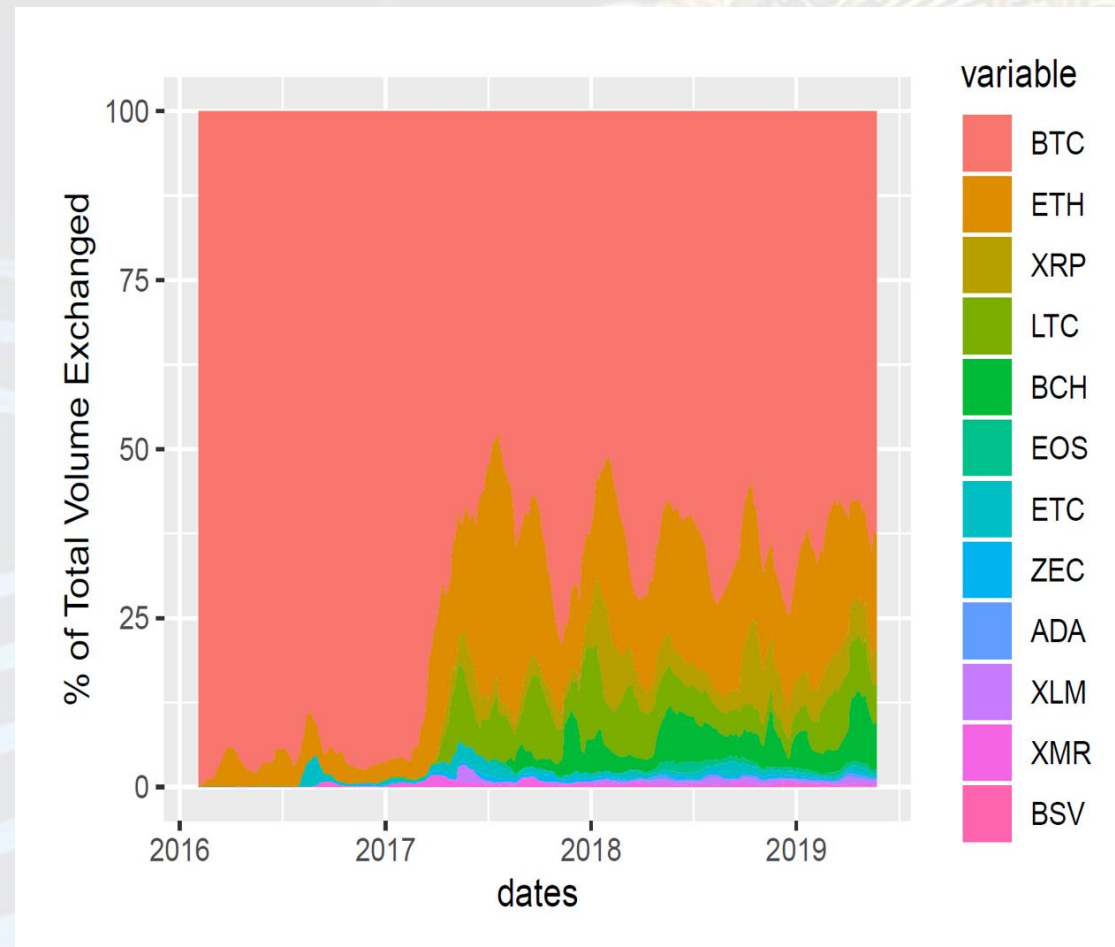
Bitcoin's closest rival in terms of the use case. There is a **limited supply** of 84 million litecoins, compared to 21 million bitcoins



A cross-border **payments solution** for large financial institutions based on blockchain technology. A transaction of XRP can be settled in 4 seconds

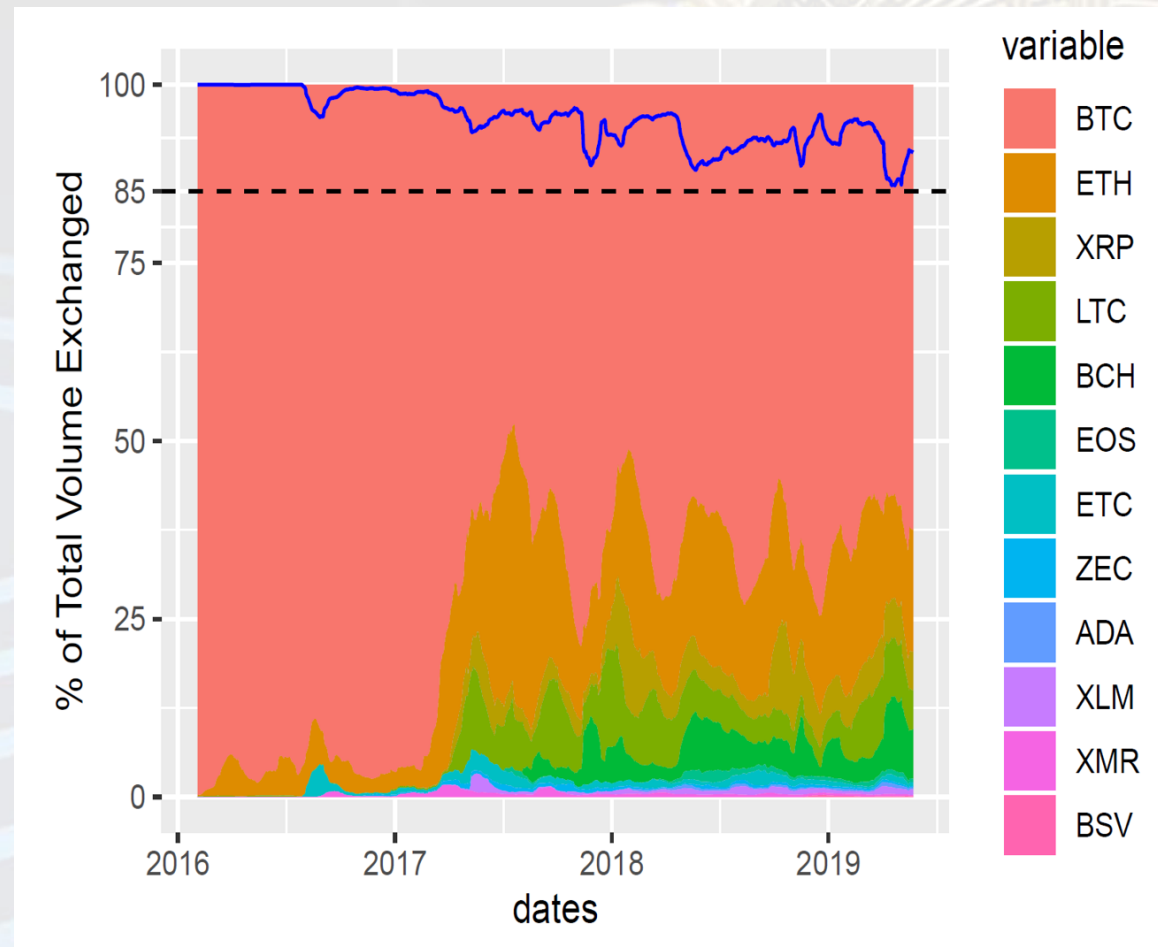
Traded Volumes (1/2)

Bitcoin was more than 85% of total volumes until 2017, more than 50% until the middle of 2019

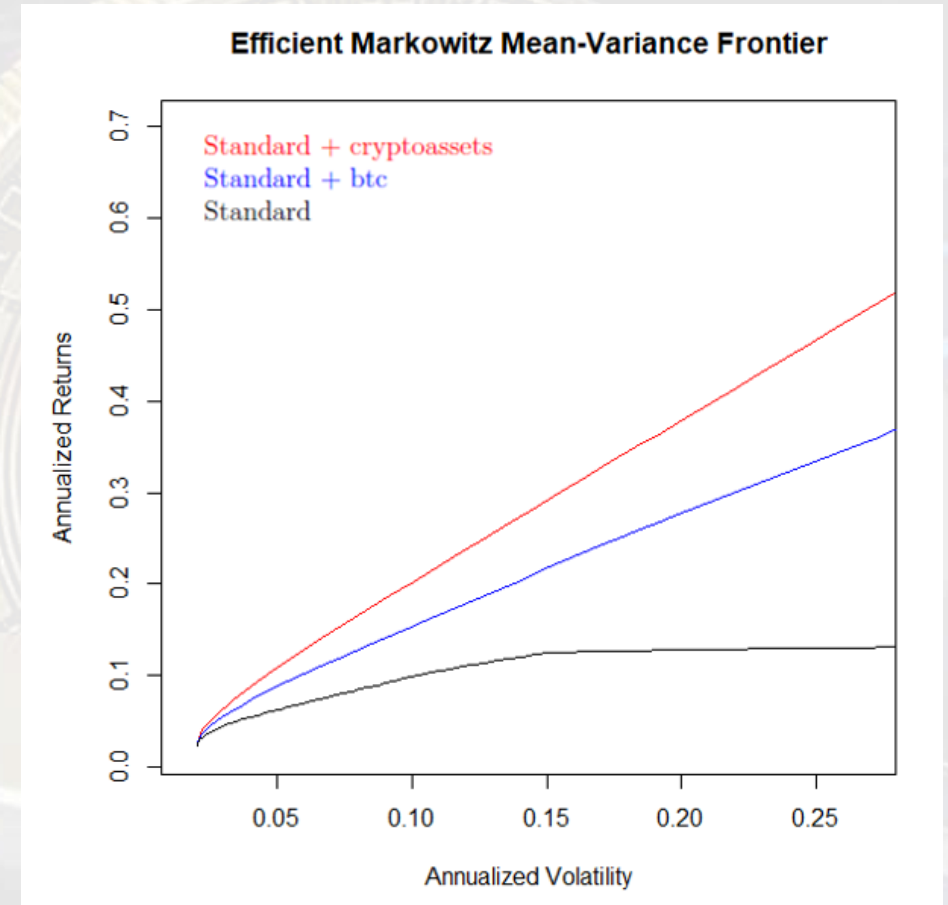
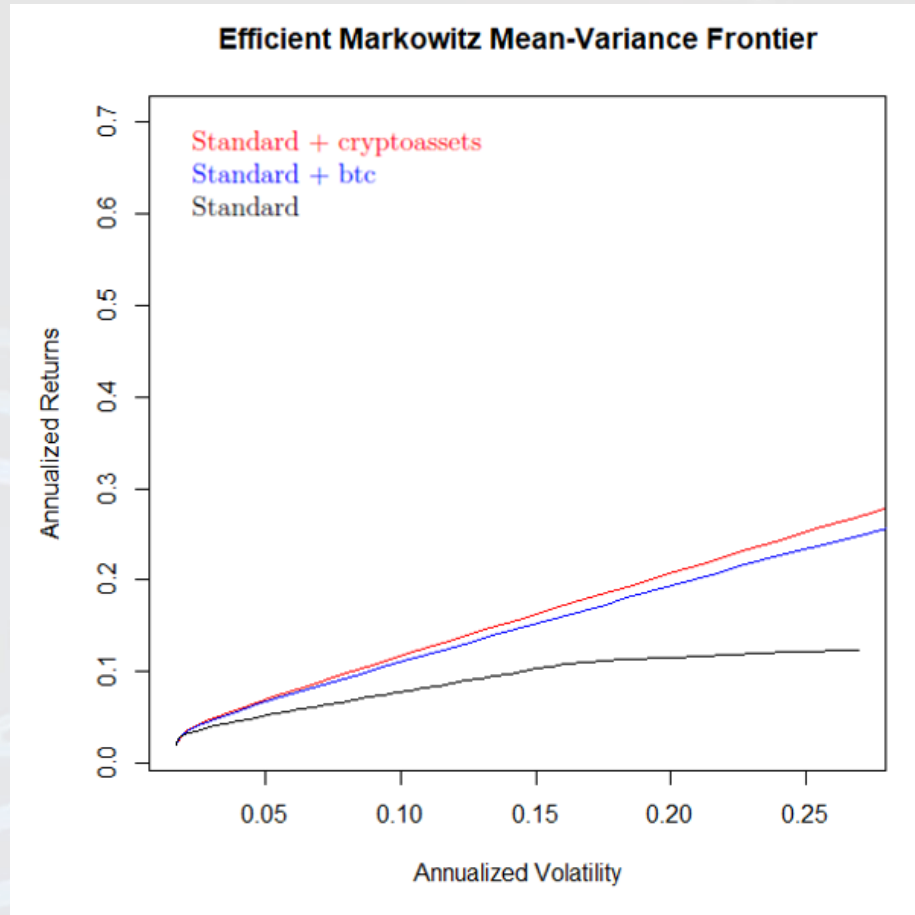


Traded Volumes (2/2)

More than 90% of total volumes exchanged is covered by the 4 major digital assets



Crypto Assets: a New Asset Class

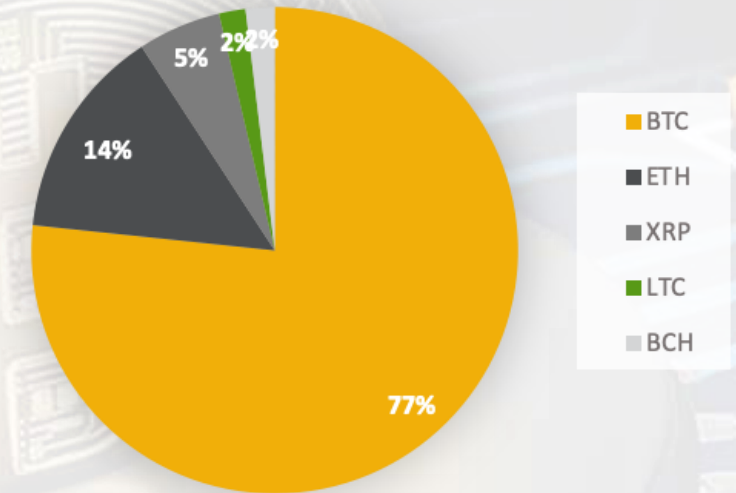


Analysis by **Matteo Avigni**, *alumnus* DGI

Research Activity: Crypto Index



Index Weights as of July 1st, 2020



- Implementation started in 2019 by Digital Gold Institute
- It explains the relevance of Bitcoin, as it accounts for about the 77% of the index composition
- The index is developed in collaboration with CheckSig
- Available by the end of 2020

btclib: new release



- Latest released: v2020.5.11
- Major changes includes:
 - switched to tox testing, gradually moving to pytest testing
 - adopted black formatter and added compatible flake8 and isort configurations
 - added Integer as hex-string or bytes representation of an int
 - adopted the function signature of dsa.sign for rfc6979.rfc6979
 - added CURVES dictionary of all elliptic curves
 - moved all entropy functions into the entropy module
 - entropy.generate has been renamed as entropy.randbinst

<https://btclib.org/>

Workshops

A&C Law has promoted a series of three webinars:

- Bitcoin's legal qualification
- Bitcoin as asset eligible for portfolio allocation
- Technological and regulatory requirements for investments in Bitcoin



Save The Date

**Bitcoin, blockchain e crypto-assets:
impatti nei settori finanziari e assicurativi**

September 15

<https://www.lseg.com/it/Blockchain2020>

2nd Crypto Asset Lab Conference

October 27

<https://cryptoassetlab.diseade.unimib.it/cal2020/>

Bitcoin and Blockchain

July 21-22

<https://dgi.io/workshop/>

2020-Q3 Report Presentation

October 15

<https://dgi.io/reports/>



Guest Speaker

Guido Maria Brera

Co-founder of the Kairos Group, he is a Director and Head of Collective Management at Kairos Partners SGR

Author of short stories and financial books including "Everything is broken up and dances" and "The Devils. Finance told by its black box", as well as the creator of the website www.idiavoli.com



L'insostenibile leggerezza del *Quantitative Easing*



Digital Gold Institute

Scarcity in the Digital Realm

Nothing in this document constitutes an offer to buy or sell, or a solicitation of an offer to buy or sell, any financial instruments. It is not intended to represent the conclusive terms and conditions of any security or transaction, nor to notify you of any possible risks, direct or indirect, in undertaking such a transaction. No entity in Digital Gold Institute shall be responsible for any loss whatsoever sustained by any person who relies on this document.

Nessun contenuto presente in questo documento costituisce e deve essere inteso come offerta all'acquisto o alla vendita o sollecitazione all'investimento in relazione a strumenti finanziari e non è inteso a rappresentare i termini e le condizioni definitivi di ogni strumento finanziario ovvero di ogni offerta avente ad oggetto strumenti finanziari, né i rischi diretti od indiretti connessi alla stessa offerta. Nessuna entità di Digital Gold Institute è responsabile delle perdite sostenute da una persona che si affida a questo documento.