Latest Insights & Analytics

March-May 2019 selection

We provide in-depth analysis and data-driven insights of digital assets and the overall crypto market by generating unbiased, institutional-grade research reports for investors in the crypto space.

Disclaimer
This report has been prepared solely for informative purposes and should not be the basis for making investment decisions or be construed as a recommendation to engage in investment transactions or be taken to suggest an investment strategy in respect of any financial instruments or the issuers thereof. This report released by Binance Research is not related to the provision of advisory services regarding investment, tax, legal, financial, accounting, consulting or any other related services and are not recommendations to buy, sell, or hold any asset. The information contained in this report is based on sources considered to be reliable, but not guaranteed, to be accurate or complete. Any opinions or estimates expressed herein reflect a judgment made as of this date, and are subject to change without notice. Binance Research will not be liable whatsoever for any direct or consequential loss arising from the use of this publication/communication or its contents.
Our views

Binance Trading Desk - Market commentary

Can JPM Coin Disrupt the Existing Stablecoin Market?

KEY TAKEAWAYS

1. What are stablecoins?
   - Definition of Stablecoins
   - Functions of Stablecoins
   - Timeline of Stablecoins
   - Ever-increasing Volume: Contribution of Stablecoin Volume to Total Industry Volume
     Chart 1 - 7-day rolling stablecoin volume contribution to total volume

2. Stablecoin Market Structure
   - Fiat-Collateralized Stablecoin Snapshot
     Chart 2 - Backed Stablecoin 7-Day Rolling Trading Volume Breakdown
     Chart 3 - Backed Stablecoin 7-Day Rolling Trading Volume Breakdown (Excluding USDT)

3. Fiat-collateralized Stablecoin Business Models and Risks

4. Description of JPM Coin and its Blockchain
   - JPM Coin Overview
   - Use Cases & Design
   - JPM Coin Core Functions: Issuance, Transfer and Redemption
   - JPM Coin Technology - Quorum Blockchain
     Raft consensus
     Istanbul Byzantine Fault Tolerance Consensus
   - Blockchain Privacy Architecture
   - Initial Applications
     Figure 3 - 0.1 %/1 % of J.P. Morgan’s existing balance sheet (in $bn) relative to stablecoin market size
   - Future Applications
     1. Clearing house in the derivatives industry
     2. Stablecoin providers through public-private cross-chain atomic swap

5. How does JPM Coin Compare to Ripple (XRP)?

6. What Implications does JPM Coin have for the Existing Stablecoin Market?

7. Stablecoins and Private Blockchains: An Illustration of the Industry Change

8. Conclusion

References

Are Cryptoassets Highly Correlated?

KEY TAKEAWAYS

1. Three-month correlations within the cryptoasset market
   1.1 Cryptoassets exhibited high correlations in USD terms at the beginning of 2019
     Chart 1 - Large-cap asset 3-month daily return correlation matrix (USD) Dec 1 2018 - Mar 1 2019
   - Possible idiosyncratic factors and events influencing correlations over this period:
     "Binance Effect"
   - Consensus Mechanism

1.2 BTC returns exhibited lower correlations at the beginning of 2019
   Chart 2 - Large-cap asset 3-month daily return correlation matrix (BTC) Dec 1 2018 - Mar 1 2019
   - Idiosyncratic factors
     "Binance Effect"
   - Consensus Mechanism

2. Did stablecoins impact market structure?
2.1 USD 3-month Snapshots
Chart 3 - Dec 1 2018 - Mar 1 2019: Large-cap assets 3-month correlation matrix (USD)
Chart 4 - Dec 1 2017 - Mar 1 2018: Large-cap assets 3-month correlation matrix (USD)
Chart 5 - Jun 1 2018 - Sep 1 2018: Large-cap assets 3-month correlation matrix (USD)

2.2 BTC 3-month Snapshots
Chart 7 - Dec 1 2017 - Mar 1 2018: Large-cap coins 3-month correlation matrix (BTC)
Chart 8 - Jun 1 2018 - Sep 1 2018: Large-cap assets 3-month correlation matrix (BTC)

2.3 Does the Rise of Stablecoins Explain Increased Correlations?
Chart 9 - 2018: Evolution of the total crypto market cap (USD bn)
Chart 10 - Increasing Volume: Contribution of Stablecoin Volume to Total Industry Volume
Chart 11 - NEO trading volume on Binance - Feb 28 2018 vs. Feb 28 2019
Table 1 - Existence of stablecoin pairs on Binance

Conclusion

Examining the Implications of Monero’s Latest Fork

KEY TAKEAWAYS
Monero’s XMR Fork in March 2019
Consequences of Monero’s March 2019 fork
  - Added privacy features and improved security
  - Knocked out pre-fork ASIC miners
    1. Sudden drop in hash rate
    2. Increasing block profitability
    3. A brief spike in blocktime
Conclusion - The Fork’s Outcomes
  - Outcome 1 - Mining remains fairly unprofitable for household miners
  - Outcome 2 - Lower hashrate = higher probability of 51% attack

Binance Academy - ASICs

A look at irregularities discovered on Augur

KEY TAKEAWAYS
Brief description of Augur
  - Figure 1 - Simplified outline of the lifetime of a prediction market (Augur whitepaper)
Existing issues
  1. General issues
    - Image 1 - IPFS-hosted version (accessed as of 3/31/2019 at 10am UTC)
    - Image 2 - “Augur.Casino” version displaying a warning (accessed as of 3/31/2019 at 10am UTC)
    - Image 3 - Warning displayed on “Augur.Casino” (accessed as of 3/31/2019 at 10am UTC)
  2. Technical Issues
    - Market illiquidity
    - Incentive Problems
    - Voting & Possible Forks
A Controversial Market
Outcomes for the settlement of the current case
  - Outcome 1 - Market resolves as invalid
  - Outcome 2 - Market disputed but doesn’t resolve as invalid
  - Outcome 3 - Market is not disputed
Past example of a “design flaw attack” 53
Potential improvements 53
  1. A Price-Based Refunding Mechanism 54
  2. Clear references in the definition of a market 54
  3. Market validators with nontrivial stakes prior to the inception of any new market 55
A note on Governance Tokens 55

Binance Academy - Design Flaw Attack 56

Investigating Cryptoasset Cycles 57
KEY TAKEAWAYS 57
1. Market Turning Points and Cyclical Movements in Correlations 58
  Chart 1 - Correlation between the smoothed market cap of Bitcoin and Altcoins (excluding stablecoins) 58
  Table 1 - Historical crypto-correlation periods over 0.8 (Data from 2013/8/26 to 2019/3/14) 59
2. Irrational Cognition: Are Crypto Market Correlations Prone To Extremes? 60
  2.1 High proportion of retail investors 60
    Chart 2 - Investor structure comparison: crypto (estimated) vs. stock markets 60
    Chart 3 - 2018 Annual turnover rate comparison: crypto vs. stock markets 61
  2.2 HODLing - another feature of the crypto investors 62
    Chart 4 - "UTXO market cap" and the spot price of Bitcoin 63
    Table 2 - Recent cryptoasset products by traditional institutions and regulatory progress 66
    Table 3 - The status of cryptoasset regulations around the world 67

Litecoin’s 2019 Halving Scenarios 68
KEY TAKEAWAYS 68
1. Why are halvings important? 69
  Chart 1 - Realized and expected annual inflation rates (%) on Litecoin 70
  Chart 2 - Transactions fees (%) relative to block rewards 71
2. A look at past halving events 71
  2.1 Litecoin’s August 2015 halving 71
    2.1.1 Price rallies before the event 71
      Chart 3 - Evolution of the price (USD) before/after the 2015’s halving 71
    2.1.2 Hashrate barely dropped 72
      Chart 4 - Litecoin’s hashrate (in THash/s) 72
    2.1.3 Permanent drop in mining profitability 72
      Chart 5 - Litecoin’s mining profitability (in USD/day for GHash/s) 72
  2.2 Bitcoin’s previous halvings 72
    Table 1 - Bitcoin’s historical halving figures 73
3. Halving scenarios 73
  Outcome 1 - price rallies before stabilizing at a new high 73
    Chart 6 - Litecoin’s year-to-date prices in USD 74
  Outcome 2 - hashrate increases before the halving 74
    Chart 7 - Litecoin’s year-to-day hashrate (THash/sec) 74
  Outcome 3 - mining profitability adjust as miners exit the market 74
  Outcome 4 - permanent drop in mining profitability 75
Conclusion 75
Binance Academy - A look at consensus algorithms

Consensus Algorithm
Definition
Consensus Algorithm vs Protocol
Different Types of Consensus Algorithms
Proof of Work (PoW)
Proof of Stake (PoS)
Delegated Proof of Stake (DPoS)
Delayed Proof of Work (dPoW)
Proof of Burn (PoB)
Proof of Authority (PoA)

Why Consensus Algorithms Matter to Cryptocurrencies

Categorizing Cryptoassets: A Return-Driven Cluster Analysis

KEY TAKEAWAYS
1. Methodology
   1.1 Dataset
   1.2 Algorithm selection
      Table 1 - Comparison between K-Means and Hierarchical clustering methods
      1.2.1 Hierarchical clustering methodology
      1.2.2 K-means clustering methodology
2. Results
   2.1 Selection of assets
      Chart 1 - 30-day 10 largest average market capitalizations (USDbn) as of March 31st 2019
      Chart 2 - 30-day 11-30 largest average market capitalizations (USDbn) as of March 31st 2019
   2.2 52-week returns correlation matrix
      Figure 1 - Weekly return correlation matrix
   2.3 Hierarchical clustering results
      Figure 2 - Dendrogram based on correlation matrix (based on squared euclidean distances)
   2.4 K-means analysis
      Figure 3 - Elbow curve - Selecting the optimal amount of clusters
      Table 2. Risk-return profiles for first cluster (A)
      Table 3. Risk-return profiles for second cluster (B)
      Table 4 - Risk-return profiles for the 4 other clusters (C-F)
3. Conclusion

The Evolution of Stablecoins

KEY TAKEAWAYS
1. Ever-increasing popularity in USD-collateralized stablecoins
   1.1 Year-On-Year Volume Breakdown comparison on Binance
      Chart 1 - Comparison of 24h Quote Asset volume between May 1st 2018 and May 1st 2019 on Binance
   1.2 Stablecoin pair additions on Binance over first 4 months of 2019
      Table 1 - Addition of new stablecoin pairs on Binance for existing assets over the first four months of 2019 *
   1.3 Net inflows: more deposits than redemptions over the first four months of 2019
      Table 2 - 2019 first 4-month redemptions & deposits for main USD-backed stablecoins
      Chart 2 - Evolution of total monthly net inflows (USD million) in non-USDT stablecoins in 2019
2. Trading environment overview
   2.1 Untethered stablecoins have small differences
Table 3 - Statistics about stablecoin trading pairs on Binance (over April 2019)  
2.2 Tether volatility: low but recent spike in late April  
   Chart 3 - Kraken USDT/USD daily OHLC from January 1st 2019 to April 30th 2019  
3. Axes of differentiation  
   3.1 Addition of new blockchains  
      3.1.1 Tether: OMNI is not the end-all-be-all  
         Chart 4 - Breakdown of all USD Tether issued across blockchains as of April 30th 2019  
         Table 4 - Exchanges supporting non-OMNI versions of USD Tether  
         Chart 5 - Breakdown of all USD Tether issued across chains as of December 31st 2018  
      3.1.2 Ontology’s support of the PAX stablecoin  
         Chart 6 - To-be-issued Ontology-based PAX compared to existing Ethereum-based PAX (as of April 30th 2019)  
3.2 Additional support of new collaterals: Trust Token’s expansion to a wide range of fiat currencies  
3.3 Increasing participation of non-financial institutions: could Facebook Coin and Samsung Coin become future game changers?  
   3.3.1 Facebook Coin  
   3.3.2 Samsung Coin  
Conclusion  
Quick insights
Our views

May 31st 2019

One step at a time.

As correlations in USD returns increased in Q1-Q2 between all major cryptocurrencies and digital assets, stablecoins will further become the primary quote currency for cryptoassets in the future, taking over the historical role of Bitcoin as the leading quote currency. Yet, despite Tether’s recent turmoil, other stablecoins are lagging in terms of trading volume and market capitalization, affecting their liquidity profile. As a result, competition is heating up for existing stablecoin providers fighting for market share, using different strategies such as diversification on new blockchains, additional support of non-USD fiat currencies, and targeting a wider range of financial use-cases such as USDC’s recent integration into many Decentralized Finance (ie. DeFi) applications (e.g. Compound, Dharma).

Specifically, Open Finance - aka DeFi - applications have also become increasingly popular, with Ethereum being the go-to programmable blockchain for most developers today. We expect this trend to continue with new platforms being launched and new protocols and dApps being developed on Ethereum. Similarly, other decentralized applications such as prediction markets have also received wide market coverage, with the development of both layer-2 solutions built on top of Augur, despite its flaws, such as Veil, who also recently launched their own fork of Augur called AugurLite.

Korean crypto-appetite seems to have cooled down with local exchange premiums (commonly referred to as the “kimchi premium”), which may exist owing to domestic capital restrictions, being at low historical levels. Though the premium has remained at historically-low levels, we do not see this as a negative signal, and instead, consider it as a sign of growing market maturity.

Meanwhile, all-time high volumes on the CME, which recorded more than USD1bn traded over 24 hours in May, send a clearer signal of institutional demand entering the space. Institutional investors, currently representing (in our conservative assumptions) less than 10% of all long-term investors, are growing their exposure to digital assets and
cryptocurrencies, as illustrated by a premium of nearly 40% for Grayscale Bitcoin Trust (GBTC) over BTC spot price at the end of May.

On the contrary, permissioned blockchains are also being built by large corporations, with widely-covered initiatives from Facebook (“WorldCoin” and “Project Libra”) and JP Morgan (“JPM Coin”). Despite these initiatives running on private (or partially private) closed systems, we expect these projects to be stepping stones in the blockchain industry for everyday users to enter the blockchain world. Thanks to their large user-bases comprised of both retail and institutional clients, these initiatives could ultimately benefit the whole cryptoasset industry, with new users moving onto decentralized, permissionless and non-custodial platforms.

Furthermore, amidst the growing institutional interest in this industry, privacy and decentralization-focused tokens remain a relevant niche in the blockchain sphere. New protocols such as MimbleWimble and the never-ending battle to fight ASIC miners (“cat and mouse game”), illustrated by Monero’s recent hard fork, present proof that market participants have been concerned about both the lack of fungibility of some cryptocurrencies and the concentration of mining pools.

Initial Exchange Offerings (IEO) will continue over the course of 2019, with many exchanges following the example of Binance to organize public sale of new tokens. This fast-follower effect may also be replicated again down the road with the development of native blockchains built by other trading platforms, echoing the launch of the Binance Chain in Q1 2019.

In short, the cryptocurrency and digital asset industry will continue to evolve over 2019, with the pace of evolution potentially accelerating even further if market prices decide to hit the gas pedal.

Binance Research
May has been very exciting for the markets. First we had the move higher in BTC from 5000 to 9000, immediately back down, and in between we had a few ‘liquidation fueled moves’, most of all the ‘Bitstamp flash crash’ of May 17th. Compared to March and April, which were relatively quiet in altcoin space, May was a much more active month in terms of OTC trading. The initial move higher in BTC was likely fueled by Blockchain week in NY (Consensus, Magical Crypto Conference and other events) and led to a lot of renewed interest in buyers of BTCUSD.

We had hoped for the inflow to extend into altcoins especially the large-cap coins, until the Bitstamp ‘flash crash’ occurred and shook out a lot of would-be investors. However the market did recover after a few days and we see renewed interest in the altcoin space again on two-way flows. Sellers were there to take profit, and others were putting on new positions. Most interest so far has been on the large cap altcoins and we are slowly seeing volumes for smaller cap coins building. We do see much larger volumes on altcoins compared to March and April.

We have definitely seen more interest from the non-crypto public this month, and hope that the market ‘behaves’ such that the interest continues to build. However as the May 17th event showed, some large players can come in to move the markets and trigger a lot of big moves. The liquidation mechanisms on futures exchanges are such that, if liquidation is triggered, the engine aggressively sells more contracts into the market, exacerbating any moves. We have seen a few more attempts at this in the later half of the month. We do believe the market will learn from these events and will be better equipped to respond going forward.

June promises to be eventful - there seem to be a number of developments and releases on various altcoins, and we are excited to see positive momentum continue to build in the space.

On our side, we will keep building out our infrastructure and connecting more buyers and sellers globally. We also continue to see people learn more about our pricing - great to see more appreciation of the liquidity we can provide, especially in altcoins.

About Binance Trading

Binance Trading is one of the leading OTC desks to exchange digital assets and cryptocurrencies. If you wish to trade large volumes with efficient settlement and competitive quotes, join Binance Trading Telegram channel. Please reach out to one of the official traders on this channel, confirm your account and get ready to exchange the world.
Can JPM Coin Disrupt the Existing Stablecoin Market?

Binance Research - March 1st 2019

In late 2017, amidst significant media hype surrounding blockchain and distributed ledger technologies, J.P. Morgan CEO Jamie Dimon deemed Bitcoin a fraud. Nonetheless, the company had been extensively researching use cases of blockchain technology since 2015 while building Quorum: a private and permissioned version of Ethereum.

On February 14th 2019, J.P. Morgan introduced the first prototype of its blockchain settlement product: JPM Coin, a stablecoin backed 1:1 by its fiat reserves.

**KEY TAKEAWAYS**

- Fiat-collateralized stablecoins have become increasingly popular in cryptoasset markets as they combine the functions of a blockchain, such as transparency and speed, **without the inherent volatility risk of bitcoin** and other cryptocurrencies.

- The primary business model of fiat-collateralized stablecoin issuers is generating returns through lending collateral in addition to issuance / redemption fees.

- JPM Coin marks the first experiment of a **new type of stablecoin** that would rely on private blockchains, marking a transition from an interest-collecting business model to one that is targeted at improving internal processes (e.g. clearing and settlement).

- Using Quorum blockchain, the JPM Coin model could serve as a **framework for other financial institutions to issue their own stablecoins**. In a similar fashion to tokens created using the ERC-20 standard (built on the Ethereum blockchain), financial institutions could use & issue a wide range of branded stablecoins backed by various fiat currencies.

- JPM Coin and the Ripple ecosystem are currently focusing on improving different aspects of traditional finance. **Minimal direct competition** is expected between the

---

2 https://www.coindesk.com/jpmorgan-ethereum-blockchain-quorum
two in the near term, though this could change depending on how JPM Coin develops to venture out of its current closed network.

- While JPM Coin does have the potential to **materially impact traditional financial services** (related to institutional client use cases such as clearing and settlement), it **will not displace liquid, publicly traded stablecoins in the near-term** given its private, permissioned structure.

- Should this pilot project proves successful as a model for driving institutional adoption of private blockchains, it may be an intermediate stepping stone for crypto mass adoption as clients move toward private distributed ledgers backed by technology providers of enterprise whitelabel solutions; however, a global decentralized economy will not appear overnight with everyone running on public blockchains.

1. What are stablecoins?

Since the inception of Tether in 2014, several stablecoin projects have been launched to address the volatility inherent to cryptoassets. Most existing projects were either established directly (Gemini Dollar) and indirectly (USD Coin, Tether) by cryptocurrency exchanges, or by dedicated companies and foundations (TrueUSD, NuBits). In that regard, JPM Coin represents the first prototype of a stablecoin created by a traditional financial institution.

**Definition of Stablecoins**

Stablecoins have several definitions:

“A stablecoin is a type of cryptocurrency that is designed to maintain a stable value, rather than experiencing significant price changes. Recently, these digital currencies have grown substantially in popularity as an answer to the high volatility associated with the cryptocurrency markets.”

*Binance Academy: What is a stablecoin?*


“Stablecoin refers to a new class of cryptocurrencies which offer price stability and/or are backed by reserve asset(s). In recent times, stablecoins have gained enough traction as they attempt to offer the best of both worlds – the instant processing and security of payments of cryptocurrencies, and the volatility-free stable valuations of fiat currencies.”

*Investopedia: Stablecoin*
Throughout this report, we will refer to stablecoin as a cryptocurrency whose value is designed to follow the value of a specific fiat currency.

Functions of Stablecoins

The primary function of existing stablecoins is to transfer value worldwide efficiently and at minimal cost without the price volatility inherent to Bitcoin or other digital assets.

Additionally, stablecoins provide convenience in conducting arbitrage between trading venues. Before stablecoins were massively adopted by exchanges, it was a complicated process to arbitrage BTC among exchanges as fiat transfers were slow to process (taking up to several days).

Timeline of Stablecoins

The first generation of stablecoins (Tether) aimed to provide a digital currency relying on blockchain without "volatile price swings" (Tether Whitepaper 2014).

While Tether was created as a fiat-collateralized stablecoin pegged to the US dollar, other primitive stablecoins (BitUSD, NuBits) relied on algorithms and/or non-fiat collateralization mechanisms to maintain their peg against a fiat currency.

The second generation of stablecoins (USD Coin, TrueUSD, Dai) is aimed at increasing transparency into the business model of the first generation of stablecoins. It includes the release of audits for stablecoins backed by fiat bank accounts and a clearer collateralization mechanism for non-USD backed collateralized stablecoins, such as Dai.

In comparison, JPM Coin seems to be the precursor of a third generation of stablecoins that targets a particular market segment: financial institutions. Relying on private blockchains, these stablecoins would only serve specific purposes such as improving settlement times and processes within financial institutions. From this perspective, the business model itself shifts from a pure profit-driven model to a business model designated to solve specific business use cases (e.g. improve the client experience for settlement and clearing operations).

Based on the current information provided by J.P. Morgan, JPM Coin might be a direct competitor to Ripple, which currently has a lead in this industry with over 100 institutional clients3 for its blockchain-powered alternative to SWIFT4.

Fiat-collateralized stablecoins have primarily the following features:

---

3 https://www.cnbc.com/2017/10/10/ripple-has-over-100-clients-as-mainstream-finance-warms-to-blockchain.html
4 https://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp
- **Serving as fiat on/off ramps**: for institutional investors, they collateralize their USD assets to stablecoins before transferring on a wide variety of exchanges.

- **Stable prices**: owing to the pegging system, it is convenient to trade stablecoins with other digital assets. Fiat-backed stablecoins are especially popular in OTC trading.

- **Easy to apprehend**: unlike algorithmic stablecoins, investors have more confidence in the fiat-based pegging mechanism as it is more intuitive to apprehend. The break in the peg of some algorithmic stablecoins has made it difficult for institutional investors to consider these assets as low-risk as fiat-pegged stablecoins.

Ever-increasing Volume: Contribution of Stablecoin Volume to Total Industry Volume

**Chart 1 - 7-day rolling stablecoin volume contribution to total volume**

The total share of stablecoin volume continues to increase relative to total volume across the entire cryptoasset market, which reflects increasing demand to manage volatility inherent in other cryptoassets.

2. Stablecoin Market Structure

The stablecoin market continues to evolve as new models emerge, with a particular division between collateralized vs. non-collateralized approaches for maintaining a consistent price peg. Within collateralized models, both fiat and crypto-backed models exist as a way to minimize volatility.

For non-collateralized models, **many leverage algorithmic techniques to maintain price stability**. While we acknowledge the existence of a variety of price stability models, this overview will focus primarily on the fiat-collateralized stablecoins. Many projects have
issued --and will continue to issue -- stablecoins backed by a variety of fiat currencies beyond the US dollar, such as EURS presented in the table below.

**Fiat-Collateralized Stablecoin Snapshot**

*symbol indicates listing on Binance as of March 1st 2019*

<table>
<thead>
<tr>
<th>NAME</th>
<th>BLOCKCHAIN</th>
<th>INCEPTION</th>
<th>COLLATERALIZED BY</th>
<th>CIRCULATING SUPPLY (FEB. 18)</th>
<th>JURISDICTION</th>
<th>ISSUES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tether (USDT)</td>
<td>OMNI</td>
<td>April 2013</td>
<td>Banked USD</td>
<td>2,031,129,386</td>
<td>British Virgin Islands</td>
<td>&gt; Failure to produce quarterly audits⁵</td>
</tr>
<tr>
<td>TrueUSD (TUSD)</td>
<td>Ethereum</td>
<td>Mar 2018</td>
<td>Banked USD, regular audits</td>
<td>205,590,114</td>
<td>US</td>
<td>-</td>
</tr>
<tr>
<td>Paxos Standard Token (PAX)</td>
<td>Ethereum</td>
<td>Sep 2018</td>
<td>Banked USD, regular audits</td>
<td>114,311,518</td>
<td>US</td>
<td>&gt; Recent controversy about discount for clients⁶</td>
</tr>
<tr>
<td>Gemini Dollar (GUSD)</td>
<td>Ethereum</td>
<td>Oct 2018</td>
<td>Banked USD, regular audits</td>
<td>76,490,852</td>
<td>US</td>
<td>&gt; Recent controversy about discount for clients⁵</td>
</tr>
<tr>
<td>USD Coin (USDC)</td>
<td>Ethereum</td>
<td>Oct 2018</td>
<td>Banked USD, regular audits</td>
<td>244,620,016</td>
<td>US</td>
<td>-</td>
</tr>
<tr>
<td>Stasis EUR (EURS)</td>
<td>Ethereum</td>
<td>Aug 2018</td>
<td>Banked EUR, regular audits</td>
<td>30,979,207</td>
<td>Malta</td>
<td>-</td>
</tr>
<tr>
<td>Stable USD (USDS)</td>
<td>Ethereum</td>
<td>Feb 2019</td>
<td>Banked USD, regular audits</td>
<td>5,781,823</td>
<td>US</td>
<td>-</td>
</tr>
<tr>
<td>JPM Coin</td>
<td>Quorum (Ethereum fork)</td>
<td>2019</td>
<td>Fiat currencies on J.P. Morgan deposits</td>
<td>-</td>
<td>-</td>
<td>&gt; Prototype</td>
</tr>
</tbody>
</table>

Source: CoinMarketCap, Mosaic.io, Binance Research, Project Whitepapers

In addition to fiat-collateralized stablecoins currently in circulation, many companies and financial institutions are evaluating issuing their own stablecoins as a way to reduce counterparty / settlement risk and enable instant value transfer. Disclosed examples include **GMO Yen**, a yen-denominated stablecoin expected to be issued by Japanese Internet giant GMO in 2019⁷, and Saga⁸, a stablecoin backed by a basket of fiat currencies.

---

⁸ [https://www.saga.org/currency](https://www.saga.org/currency)
In Japan, Mizuho recently released its prototype of a yen-denominated currency (“J-Coin”); this could impact up to 56 million of clients as a result of its various partnerships with domestic financial institutions. Last year, Mitsubishi UFJ (“MUFJ”) was also reportedly working on its own digital asset backed by Japanese yen.

Despite the increasing number of fiat-collateralized stablecoins in the market, Tether (USDT) is still the dominant asset by trading volume and market cap with a current circulating supply of $2,031,129,386.

Chart 2 - Backed Stablecoin 7-Day Rolling Trading Volume Breakdown

Nevertheless, it appears that new market entrants are slowly gaining share of global trade volume as they continue to be listed on exchanges. Projects also leverage strong industry brands, regulatory approvals, and substantial private investment to bootstrap their networks and initial circulating supplies.

---

9 [https://asia.nikkei.com/Economy/Mizuho-s-digital-currency-to-take-on-payment-rivals-next-month](https://asia.nikkei.com/Economy/Mizuho-s-digital-currency-to-take-on-payment-rivals-next-month)
11 Data as of February 18th 2019. It is worth noting that many no-fee (or transaction mining) exchanges use Tether as their primary quote currency for listed pairs. As a result, these may create some upward bias in the Tether volume share displayed in the chart below.
In February 2019, excluding Tether (USDT), stablecoin volume was primarily spread across PAX, TUSD, USDC, and GUSD.

Whereas fiat-collateralized stablecoins represent a fairly straightforward business model with similar characteristics / mechanics, it is instructive to explore their similarities and differences, and if the nature of their business models impacts the magnitude of risks.

3. Fiat-collateralized Stablecoin Business Models and Risks

Fiat-collateralized stablecoins generally share similar business models and, therefore, are susceptible to similar types of systemic and counterparty risk.

Fiat-collateralized stablecoins typically profit in two ways:

- **Issuance / Redemption Fees**: Stablecoin companies charge fees to issue and redeem stablecoins, generating revenue based on fluctuations in demand, as stablecoins often function as fiat on / off ramps.

- **Yield on Short-term Securities**: Issuers often invest collateral in liquid securities (treasuries, money market funds, etc.) to generate yield. Value captured from this revenue stream is therefore driven by total circulating supply and interest rates (and arguably the reserve ratio of the issuer).

However, interest-bearing stablecoins are likely to exist in the near future (e.g. USDD), and existing companies will be pressed to share at least some of the aforementioned interest payments to their clients and / or offer a discount on face value for new token issuance of new clients. As a result, the entire stablecoin industry will likely face increasing pressure and extremely tight margins in the coming years.

---

12 Example with USD Tether: [https://tether.to/fees/](https://tether.to/fees/)

Given the mechanics and business models of fiat-collateralized stablecoins, the key structural risk is stablecoins breaking their 1:1 peg against underlying fiat currencies.

As fiat-collateralized stablecoins are centralized in nature, several underlying structural and counterparty risks exist, and could potentially break the 1:1 peg of a stablecoin:

- **Counterparty Risk**: Stablecoin holders are susceptible to both Issuer and Custodian / Bank counterparty risk. Examples of such risk include issuers being unable to prove, via reliable audits, that collateral exists to match the outstanding supply.
- **Macroeconomic Risk**: Any type of macroeconomic risk that could negatively affect depository institutions resulting in insolvency, frozen funds, redemption refusal, etc.
- **Technology Risk**: Centralized issuers are susceptible to technology risk within their own smart contracts (e.g., a smart contract flaw could result in printing excess coins that are not backed by collateral); The blockchain of choice is also susceptible to a variety of hacks (e.g., 51% attack of Ethereum blockchain if token is an ERC-20).
- **Regulatory Risk**: Issuers operating in jurisdictions that have become unfavorable towards digital assets could face significant regulatory / political risk (e.g., characterizing stablecoins as securities).

Furthermore, stablecoin holders could potentially face redemption risk should centralized Issuers decide to reject account KYC, seize funds, or act maliciously.

4. Description of JPM Coin and its Blockchain

JPM Coin Overview

JPM Coin is a prototype of a stablecoin that aims at “reducing clients’ counterparty and settlement risk, decreasing capital requirements and enabling instant value transfer” based on innovations in distributed ledger and blockchain technology.

JPM Coin will be backed by fiat reserves from J.P. Morgan client accounts, and will likely initially be limited with US dollars but could theoretically be expanded to any currency on their balance sheet. If the pilot is successful, JPM Coin could conceivably exist in various forms, including JPMUSD (US-dollar backed), JPMJPY (Yen backed) or JPMEUR (Euro backed).

Use Cases & Design

For this pilot project, J.P. Morgan is specifically targeting institutional clients such as banks, brokers, dealers and other large corporations primarily for settlement and value transfer use cases within a closed ecosystem. J.P. Morgan has made it clear that the intent of this pilot is to test stablecoins and blockchain technologies to improve internal processes, ultimately resulting in efficiency gains and cost reductions for its global client base.
While the use cases for JPM Coin differ slightly from that of other fiat-collateralized stablecoins, the mechanism by which coins are issued, transferred and redeemed is similar to those in existence. The core functions of JPM Coin is illustrated in the graphic below.

**JPM Coin Core Functions: Issuance, Transfer and Redemption**

![Step 1 Coin Issuance](Image)

![Step 2 Coin Transfer](Image)

![Step 3 Coin Redemption](Image)

*Source: J.P. Morgan*

**JPM Coin Technology - Quorum Blockchain**

J.P. Morgan, one of the largest members of the Enterprise Ethereum Alliance\(^{14}\), created its own blockchain, Quorum, which is a fork of Ethereum. JPM Coin will be issued on the **Quorum blockchain**, a permissioned network that includes a public / private state separation and allows transfer of private data between participants\(^{15}\).

In contrast to the public Ethereum blockchain that is transitioning to a Proof of Stake consensus from a Proof of Work consensus, Quorum offers the choice of two consensus algorithms, **Raft**\(^{16}\) and **Istanbul Byzantine Fault Tolerance**\(^{17}\).

---

\(^{14}\) [https://entethalliance.org/members/#j](https://entethalliance.org/members/#j)


\(^{17}\) [https://github.com/ethereum/EIPs/issues/650](https://github.com/ethereum/EIPs/issues/650)
Raft consensus

The Raft consensus algorithm is a Crash Fault Tolerance ("CFT") consensus, as opposed to Byzantine Fault Tolerance ("BFT"), as the node leader is assumed to never be malicious. All followers will then blindly replicate the entries proposed by the leader with no questions asked.

If the node leader crashes, the remainder of the network will automatically elect a new leader after a set period of timeout, and the network will continue to function. When the crashed node recovers, it will become a follower and start replicating the blocks it has missed while offline.

The Raft consensus only mints blocks when there are pending transactions, resulting in significant savings on storage when transaction load is low. A theoretical advantage of using Raft is faster possible block times compared to Istanbul BFT, as the former assumes that there are no malicious nodes, thus theoretically requiring less time to validate transactions. However, this may pose as a potential security risk to the network if the node leader turns out to be malicious.

Istanbul Byzantine Fault Tolerance Consensus

Istanbul BFT ("IBFT") is a practical Byzantine Fault Tolerance implementation that allows for greater tolerance in adversarial environments. Thus, banks or counterparties with no previous business relationship can transact freely so long as fewer than 1/3 of the nodes are faulty.

IBFT utilizes multiple rounds of voting per block, and the voting validators also do not trust that the round’s leader or block producer is cooperating. As a result, IBFT has slower block times than Raft as the cost of removing the assumption of a trustworthy block leader.

Though the block time may be theoretically slower, it is always constant. This allows more predictability for reaching certain block heights by a certain time, but also comes with the inefficiency of potentially mining empty blocks with no transactions — thus the choice of block time is a key factor to ensuring optimal network usage.

---

18 https://kaleido.io/consensus-algorithms-poa-ibft-or-raft/
19 https://www.binance.vision/blockchain/byzantine-fault-tolerance-explained
Since Quorum is a fork of the Ethereum blockchain, it does share some core pieces of technology with the Ethereum blockchain:

1. **Core infrastructure:** Quorum, as a fork of Ethereum, shares most of its code with Ethereum.
2. **Future developments:** Quorum can tap into future updates from the Ethereum development community as a fork of Ethereum, potentially adopting future improvements, and bug fixes.
3. **Same standards:** Quorum smart-contracts are written in standard Solidity and are compiled using the Ethereum Virtual Machine (“EVM”), allowing for greater developer familiarity across both Quorum and Ethereum. ERC-20 token equivalents could also be issued on Quorum in a similar structure as those issued on the Ethereum blockchain. These shared standards could lead to the mutualization of resources working on some core functions of Ethereum, thus contributing to the alignment of interests between Ethereum and Quorum.

However, as a private, permissioned network, Quorum delivers a value proposition and design that also differ from the Ethereum blockchain in a few notable ways:

- **Faster Transactions and Improved Scalability:** Quorum is expected to process “dozens to hundreds of transactions per second” with regards to the state of the network and existing smart-contracts.

- **Additional Privacy Features:** there is the ability to select public / private states. Private transactions are encrypted and included in the blocks. However, the data can only be decrypted by members that are a part of a sub-private group. On the other hand, public transactions are included in the blocks, in a similar fashion as Ethereum and could be seen by any trusted participant in the private network.

- **Permissioned Network:** at the initial stage of Quorum, only trusted parties will be accepted into the network and any new party will be manually approved. Yet, J.P. Morgan reportedly is also planning on introducing “smart-contract governance tools” to eventually handle this centralization responsibility / burden.

---

20 [https://www.jpmorgan.com/global/Quorum#section_1320553542030](https://www.jpmorgan.com/global/Quorum#section_1320553542030)
Initial Applications

JPM Coin has the potential to dramatically impact both existing financial institutions as well as the broader cryptoasset market given the size of its balance sheet, industry influence, and extensive global network of partners.

Broadly speaking, J.P. Morgan's stablecoin project will initially target efficiency gains and risk reduction in clearing and settlement functions, as well as cost reductions across core back office functions.

- **Clearing & Settlement**
  - **Greater transparency and faster times:** JPM Coin is expected to cut down processing times for clearing and settlement operations. As transactions occur on the blockchain, they can be cleared and settled regardless of existing business day constraints.

---

22 J.P. Morgan Github’s profile: https://github.com/jpmorganchase/quorum
- **Tail Risk Mitigation:** JPM Coin could decrease *tail risks such as system failure events that can occur in a fully centralized settlement system*. As an example in recent news, Wells Fargo, one of America's largest banks, left its customers unable to access their accounts for days due to internal system issues. Blockchain networks are unlikely to experience a complete shutdown as they generally rely upon a large number of nodes for validation. If a node is disabled, all other nodes will still remain functional.

- **Cost Reduction:** JPM Coin has potential to dramatically reduce costs for institutional clients, as transactions between institutional clients can be executed without pre-established trust given the transparency and auditability of transactions that is native to a blockchain architecture.

  Accenture, one of the largest global management consulting firms, provides an estimation of some additional sources of cost savings:

  1. **Finance-reporting costs could be lowered by 70 percent** as a result of optimized data quality, transparency, and internal processes enabled by a shared and verified database: the blockchain.

  2. **Supporting functions of centralized operations** (e.g. KYC, client-onboarding) could bring *50 percent savings* by establishing more efficient processes for managing digital identities and by “mutualizing” or sharing client data on a blockchain across multiple financial institutions.

  3. **Business operations expenses** from, for instance, middle office, clearing, and settlement activities could be *lowered by up to 50 percent* by reducing or eliminating the need for third-party reconciliation, confirmation and validation of trades.

  4. **Compliance costs could be reduced by 30-50%** owing to higher transparency and easiness to audit financial transactions.

Based on J.P. Morgan’s position as one of the world’s largest banks, even a small portion of total assets locked as fiat collateral for JPM Coin could make the institution the largest stablecoin issuer on a blockchain measured by circulating supply and total market cap.

For an illustration of the potential size of JPM Coin circulating supply, two scenarios were established to put in perspective the size of J.P. Morgan’s balance sheet (**USD2.6 trillion**) with the size of the existing stablecoin markets.

---


Future Applications

Beyond the aforementioned use cases, JPM Coin (or a similar concept) will also possess additional applications beyond traditional institutional banking clients.

1. Clearing house in the derivatives industry

A clearing house is “a financial intermediary responsible for settling trading accounts, clearing trades, collecting and maintaining margin money, regulating delivery of the bought/sold instrument, and reporting trading data.” For instance, they are typically responsible for managing margin calls in the largest segment of the financial industry: derivatives markets.

In the existing system, the clearing process is fairly slow and includes a lot of intermediaries. On top of that, the clearing industry is currently concentrated toward a few entities. As a result, the overall industry is quite obscure, which leads to a lack of public information for market participants.

The advantages of utilizing blockchain in the clearing process might include:

- **Regulatory oversight:** The use of a decentralized ledger, seen and monitored by regulators, could help to prevent future financial crises, since a shared ledger would make it easier for regulators to determine systemic risks (and by extension to create required policies to mitigate them).

---

- **Faster redemption / deposit times:** clearing houses could improve their own margin call system through the use of a permissioned blockchain such as the one offered by J.P. Morgan’s Quorum. Near-instant withdrawal / deposits could help clients to deposit additional collateral to increase their current margins (i.e. matching margin requirements).

- **Increase in transparency:** audit of transactions would become easier owing to the distributed ledger, and the overall linkage between institution positions would become simpler to determine (e.g. allow for new possibilities on how financial institution calculate risk exposures).

In this scenario, the deployment of a blockchain such as Quorum could help the industry to **reduce systemic risks** and make the overall clearing and settlement segment in the derivatives industry more efficient with lower costs, faster redemption/withdrawal time & increasing transparency.

2. **Stablecoin providers through public-private cross-chain atomic swap**

Stablecoin entities (e.g. Trust Token, Circle) could work hand in hand with JPM coins (e.g. JPMEUR, JPMUSD), employing public-private cross-chain atomic swaps to issue their own stablecoins running on public blockchains, with key features such as:

- **Tokenization through atomic swap:** a stablecoin entity with a J.P. Morgan corporate account may rely on the JPMUSD token in more efficiently managing deposits and withdrawals with the bank. Once a client is approved by the stablecoin entity, he would transfer funds to the USD bank account of the stablecoin entity, and the stablecoin issuer could then subsequently tokenize its newly received USD funds to JPMUSD coins.

- **Private proof of reserve:** in the process of placing JPMUSD in reserves, a cross-chain public-private atomic swap could be executed such that the exact amount of JPMUSD in reserve would be created as a public ERC20 token on the Ethereum blockchain that would then be transferred to the client. Because the JPMUSD amount would be locked in the public smart contract, it could serve as a proof of reserve for external auditors.

- **Redemption risk remaining on the stablecoin provider:** when the client wants to redeem his funds, he can simply transfer his tokens back to the stablecoin entity’s Ethereum wallet. The stablecoin issuer would then be able to apply its AML procedures and evaluate where the money comes from. If approved, the issuer would burn the tokens, triggering the release of the equivalent amount of JPMUSD from the smart contract. Eventually these funds would be returned to the client bank account.

In this scenario, J.P. Morgan would enjoy benefits from the increased use of public blockchain technology while transferring some of the risks and time costs (e.g. AML policies) associated with public blockchains to its corporate clients (stablecoin providers). An extra layer of auditing would also enable the bank to audit the fund origins (thanks to the swap between Quorum’s JPMUSD and Ethereum’s stablecoins) through
public blockchain analysis. However it is yet to be seen whether atomic swaps could be implemented and if compliance costs outweigh the benefits.

*While JPM Coin is still in its early days, Ripple has been developed for several years. It would be instructive and beneficial to discuss the differences and similarities between JPM Coin and its perceived direct competitor, Ripple.*

5. How does JPM Coin Compare to Ripple (XRP)?

Ripple is the company known for creating the XRP token, currently sitting at the No. 3 spot (USD 13.3 billion) amongst all existing crypto assets in terms of circulating market cap 28, behind only Bitcoin and Ethereum. This company has been building a payment and exchange network called *RippleNet*, which relies on a distributed ledger database called the *XRP Ledger*.

This network is an “exchange system for fiat currencies that focuses on global payment solutions for banks and other financial institutions” (Binance Academy).

*The company has three core products: xRapid (relying on XRP and its distributed ledger), xCurrent, and xVia.* 29

<table>
<thead>
<tr>
<th>JPM Coin</th>
<th>Ripple XRP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Blockchain</strong></td>
<td>Quorum **</td>
</tr>
<tr>
<td></td>
<td>Private</td>
</tr>
<tr>
<td></td>
<td>XRP Ledger</td>
</tr>
<tr>
<td><strong>Tradable on exchanges</strong></td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Settlements</strong></td>
<td>Internal clients (current)</td>
</tr>
<tr>
<td></td>
<td>Partner institutions</td>
</tr>
<tr>
<td><strong>Collateralized by an asset</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No</td>
</tr>
<tr>
<td><strong>Smart contracts</strong></td>
<td>Yes (Ethereum fork)</td>
</tr>
<tr>
<td></td>
<td>Not yet (but proposed 30)</td>
</tr>
</tbody>
</table>

**The news release from J.P. Morgan mentions potential use of other blockchains.**

Ripple is building a “frictionless” ecosystem aimed at improving the efficiency in settlement, exchange of currencies, and remittance worldwide. They are attempting to build an entire ecosystem revolving around its products, in which XRP would be a prominent component. On the other hand, J.P. Morgan seems to be inclined in developing an enterprise whitelabel solution relying on its Quorum blockchain to help financial institutions to improve settlements.

---


29 [https://www.binance.vision/economics/what-is-ripple](https://www.binance.vision/economics/what-is-ripple)

30 Codius: [https://codius.org/](https://codius.org/)
However, while JPM Coin does have significant worldwide reach based on J.P. Morgan’s existing client base, the network is currently restricted to these internal clients only. It is highly unlikely that clients of a large competing bank such as Citigroup will be able to settle transactions using JPM Coin, especially if a Citigroup Coin is released in the near future. As such, JPM Coin does not actually improve the speed or efficiency of transactions between the larger traditional banks, which currently rely on SWIFT. To add to this sentiment, it appears that Ripple has already dismissed the idea of a bank issued stablecoin31.

A recent tweet by Ripple’s CEO Brad Garlinghouse32 confirms this view:

“As predicted, banks are changing their tune on crypto. But this JPM project misses the point — introducing a closed network today is like launching AOL after Netscape’s IPO. 2 years later, and bank coins still aren’t the answer.”

Looking back at the Ripple ecosystem and the xRapid infrastructure, XRP works in a similar manner as USD in the traditional financial system: it acts as the mediator currency between both fiat / crypto currencies and any fiduciary product (e.g. commodity, points, miles, etc.). This allows various closed system networks (such as JPM Coin) to interact with each other, with XRP acting as a bridge between these networks.

Overall, the two projects appear to have different focuses and potential applications in the short term. While there is currently no direct overlap on the functionality of the two initiatives, future developments on the reach of JPM Coin outside of its existing closed network will determine to what degree Ripple and JPM Coin will compete.

6. What Implications does JPM Coin have for the Existing Stablecoin Market?

Stablecoins are used by both retail and institutional investors as an initial on-ramp for entering the cryptoasset markets through a fiat-to-crypto exchange. Institutional investors in crypto markets are typically comprised of asset management firms, venture capital funds and proprietary trading firms investing in digital assets who need a way to exchange fiat currencies for cryptoassets, or the other way around.

Large banks and financial institutions such as J.P. Morgan have a distinct set of advantages in issuing fiat-collateralized stablecoins, but these offerings will not displace liquid, publicly traded stablecoins in the near-term given their closed ecosystems built on private blockchains.

While JPM Coin does have the potential to materially impact traditional financial services (particularly in institutional client use cases such as clearing and settlement), it will have minimal impact on public stablecoins used by investors as a gateway to trade and

31 https://www.linkedin.com/pulse/case-against-bankcoin-brad-garlinghouse/
32 https://twitter.com/bgarlinghouse/status/1096118363506434048
interface with cryptoassets. Until JPM Coin’s availability extends to a larger set of commercial institutions beyond J.P. Morgan's own clients and, more importantly, expands the offering to public blockchains and trades on liquid exchanges (which could provide access to retail investors), it will have limited impact on cryptoasset markets.

Nevertheless, over the long term it is possible for JPM Coin (along with similar projects created by other banks) to have a disruptive impact on the entire stablecoin industry as they continue to expand its access and use cases.

7. Stablecoins and Private Blockchains: An Illustration of the Industry Change

Should JPM Coin turn into a successful experiment, corporations might consider private blockchains as a viable and attractive solution for their transactional needs. This could result in a shift of institutional investments from public digital tokens & currencies to technology providers of enterprise whitelabel solutions (such as a Quorum-tailored blockchain for their uses).

It is worth mentioning that today, it is unlikely that companies would rely solely on a public blockchain to manage their sensitive internal data. Hence pitting public and private blockchains head-to-head is somewhat of an artificial matchup that is less relevant than the broader discussion on whether centralized IT systems are to be replaced by private blockchain solutions within companies & industries.

The rise of this third generation of stablecoins may only be an intermediate stepping stone for cryptocurrency mass adoption. Stablecoins running on private blockchains will contribute to increasing awareness of the rest of the blockchain and cryptoasset industry in the long run.

Bitcoin was created to allow “online payments to be sent directly from one party to another without going through a financial institution.” 33 Ten years later, the landscape of the cryptocurrency industry has undoubtedly changed dramatically and financial institutions have become one of the key prominent players in the future of blockchain - be it private or public.

8. Conclusion

It is very unlikely that JPM Coin will disrupt the existing stablecoin industry in the near term owing to its permissioned, private nature. Currently, stablecoins issued by banks are designated to serve a specific purpose and as a result, do not directly compete with the existing stablecoins.

33https://bitcoin.org/bitcoin.pdf
While JPM Coin will be built on a private blockchain and initially restricted to use within the J.P. Morgan network, the initiative could cause other financial institutions to follow suit by creating their own stablecoin running on a proprietary blockchain. However, if banks were to work together to align their interests in the development of interbank settlement solutions, Ripple may suffer from increasing competition as these banks come up with their own syndicated blockchain solutions.

In conclusion, banks already are a main component of the fiat-collateralized stablecoin model as these financial institutions provide custody for the funds of stablecoin issuers. Given their size, scope and strategic network, large banks such as J.P. Morgan could potentially leverage both their large asset bases and partnerships to broaden the influence and impact of their stablecoin offerings.

References
- Binance Academy. https://www.binance.vision/glossary/stablecoin
- Binance Academy. https://www.binance.vision/blockchain/byzantine-fault-tolerance-explained
- Binance Academy. https://www.binance.vision/economics/what-is-ripple
Are Cryptoassets Highly Correlated?

An exploration of relationships between Bitcoin and other large cap digital assets

Binance Research - March 20th 2019

Cryptoasset markets exhibited wild movements in USD prices between 2017 and 2018. Bitcoin moved from a low of $735 to a peak of $19,800 in 2017, before finishing 2018 below $4,000. Ethereum, the second largest cryptoasset by market capitalization, moved from $8 to a peak of $1,440, before closing 2018 at a price below $150. Cryptoassets are generally known to move in similar directions. However, conducting correlation analysis across multiple time periods reveals additional elements that may influence the strength and direction of these correlations.

KEY TAKEAWAYS

- USD returns for the top 30 cryptoassets by market cap were highly correlated over the past 3 months (1 Dec 2018 - 1 Mar 2019). Bitcoin (BTC) exhibited the highest correlation with other assets indicating that it is the bellwether of the industry.
- BTC-denominated returns for large market cap cryptoassets exhibited significantly lower correlations than USD-denominated returns over the same period.
- Correlations of cryptoasset returns in BTC terms in late 2018 were much lower compared to late 2017.
- In contrast, correlation between cryptoasset returns in USD terms actually increased when comparing the same two periods. This has coincided with the rise of stablecoins pair dominance during 2018 and is in line with the overall decline in the contribution of BTC pairs to total industry trade volume.
- Similar to equity markets, idiosyncratic factors influence the correlation of some coins over specific time periods.
- Additional factors beyond project-specific news & catalysts may influence the strength of correlations among cryptoassets:
  - “Binance Effect”: digital assets listed on Binance oftentimes have higher correlations among themselves.
  - Consensus Mechanisms: the type of consensus mechanism could impact the correlation between the returns of cryptoassets (e.g., returns of PoW coins exhibited higher correlations amongst themselves than with non-PoW coins.)
1. Three-month correlations within the cryptoasset market

“Correlation statistically measures the strength of a linear relationship between two relative movements of two variables and ranges from -1 to +1.”

Source: Investopedia

In general, assets with a correlation above 0.5 or below -0.5 are considered to have strong positive/negative correlations. Conversely, a close-to-zero correlation indicates no linear relationship between two variables, and for the purpose of this analysis, the returns of two assets.

If the returns of two assets do exhibit a positive correlation, it implies that the two assets are, to some extent, moving in the same direction, and therefore share similar risks. On the other hand, a negative correlation between the returns of two assets indicates that the two assets are moving in opposite directions, and it is thus possible to use one asset as a hedge against the other.

1.1 Cryptoassets exhibited high correlations in USD terms at the beginning of 2019

To explore correlations between cryptoassets, the top 30 largest cryptoassets by 90-day average market cap were selected and their USD returns were calculated in order to create a correlation matrix as seen below.

Chart 1 - Large-cap asset 3-month daily return correlation matrix (USD) Dec 1 2018 - Mar 1 2019

Based on this analysis, **correlations are highest between altcoins and Bitcoin itself (~average correlation of 0.78), indicating that most of the altcoins move in similar directions as Bitcoin, underscoring Bitcoin’s status as a bellwether for cryptoasset markets.**
While, generally speaking, altcoins are highly correlated with BTC, select cryptoassets exhibit materially weaker correlations both with BTC and among one another, which suggests that additional idiosyncratic factors may affect the prices and returns of these assets.

Examples of assets with the weakest correlations in USD terms include Waves (WAVES), Tron (TRX), Bitcoin Satoshi’s Vision (BSV), Binance Coin (BNB) and Dogecoin (DOGE).

While this report doesn’t intend to provide a direct explanation for specific weaker correlations, some recent news adds additional context that may be informative in understanding possible reasons for these lower correlations.

Possible idiosyncratic factors and events influencing correlations over this period:

- **WAVES**: raised an additional $120 million in December 2018
- **TRX**: BitTorrent ICO on Binance Launchpad, which required TRX or BNB to participate
- **BNB**: Launchpad hosted two token sales successfully and the DEX testnet went live
- **BSV**: Hard-fork (commonly referred to as the “hash power war” from Bitcoin Cash (BCH)

In addition to project specific catalysts, consensus mechanism design and exchange listings also potentially influence correlations among specific assets:

“Binance Effect”

Of the top 30 market cap coins previously highlighted, only three of them are not listed on Binance - Dogecoin (DOGE), Maker (MKR) and Tezos (XTZ). These three cryptoassets exhibit lower than average correlations, which could be a function of less liquidity, resulting in thinner order-books and increased difficulty for investors to buy and sell them with similar frequencies as the other listed assets. Although this is a preliminary observation, these relationships may exist and merit further consideration in future reports.

Consensus Mechanism

Additionally, it appears that consensus mechanism type may play a role in the strength of correlations among coins, as **Proof of Work (PoW) cryptoassets seem to exhibit higher correlations with one another than with non-PoW assets**. Further analysis on correlations among coins with different consensus mechanisms is forthcoming, but of particular interest is the upcoming transition of Ethereum from PoW to PoS and what implications this development may have on its correlation with PoW coins.

---

Broadly speaking, the observation that consensus mechanism may influence correlations among cryptoassets has already been highlighted in previous reports\textsuperscript{37}, but still requires additional investigation as new protocols are built leveraging novel consensus mechanisms.

1.2 BTC returns exhibited lower correlations at the beginning of 2019

In order to analyze correlations of returns across cryptoassets, it is instructive to compare the returns of the same assets (top 30 largest coins by 3-month avg. market cap) in both USD and BTC terms over the same time horizon.

Correlations in BTC returns are important as BTC remains one of the best price indicators of crypto markets for two key reasons:

- **Liquidity**: BTC is tradable against almost all altcoins
- **Dominance**:
  - Market capitalization accounts for nearly half of the total cryptoasset industry
  - Volume represents a significant percentage of the industry

For the purposes of comparing BTC and USD returns of this asset class, it is important to understand the components that comprise BTC returns.

For every cryptoasset, its USD return can be broken down into two components:
- BTC/USD return
- Cryptoasset/BTC return

Therefore, for any cryptoasset (referenced below as “ABC”), its return can be expressed as:

\[
return_{abc\text{USD}} = (1 + return_{btc\text{USD}}) \times (1 + return_{abc\text{BTC}}) - 1
\]

As a result, cryptoasset returns - calculated based on Bitcoin prices - can be viewed as **Bitcoin-adjusted returns**.

The correlation of cryptoasset returns based on BTC prices (i.e., Bitcoin-adjusted returns), highlights significantly lower correlations among cryptoassets relative to correlations among the same coins in USD returns (avg. correlation declines from 0.67 to 0.20).

Although the average correlation among the top 30 coins is significantly lower in BTC returns than in USD returns, the dataset did yield several similarities between correlations when BTC returns were compared to USD returns.

Idiosyncratic factors

The correlations of the same subset of coins (DOGE, WAVES, BSV, TRX, BNB) with other assets are once again relatively lower than the average correlation among the entire basket of cryptoassets. Consequently, it appears that the same baskets of assets, whether calculated in USD or BTC returns, displayed lower correlations than their peers.

“Binance Effect”

Lastly, the existence of a Binance effect also appears in BTC returns correlations. Similar to observations from correlations in USD returns, Dogecoin (DOGE), Maker (MKR) and Tezos (XTZ) exhibit lower correlation than the average correlation among selected cryptoassets for this analysis.

Consensus Mechanism

In addition, PoW coins also exhibited stronger correlations among one another when using Bitcoin-adjusted returns, as was observed in the USD returns dataset.

2. Did stablecoins impact market structure?

Given cryptoassets exhibited lower correlations in BTC returns than in USD returns over the previous 90 days, the same findings were compared to the dataset during a 3-month period both one year before and six months before to understand how the macro environment may have affected correlations.
Comparison of the most recent 3-month correlation matrix with the same period one year prior highlights that USD-denominated returns have stronger correlations now than in the previous time period.

Excluding Dogecoin, the minimum correlation of the dataset was 0.648 (between Litecoin and NEM) between December 1st, 2018 and March 1st, 2019. In contrast, the same assets had an average correlation of 0.51 a year prior during the period between December 1st, 2017 and March 1st, 2018.

The extreme volatility in crypto markets from late 2017-early 2018 may have contributed to the weaker correlation amongst cryptoassets as a whole.
Once again Dogecoin (DOGE) had a lower correlation than the other assets whereas NEM’s average correlation with all assets spiked compared to six months prior.

NEM exhibited the lowest correlation with other coins between December 2017 and March 2018, prior to listing on Binance. A few months after being listed on Binance\(^{38}\) correlations subsequently rose, which underscores a potential “Binance Effect” as previously described. Yet, this single observation is not enough to state a general rule such as “assets not listed on Binance must necessarily exhibit lower correlations” and requires further investigation.

Although correlations among other cryptoassets were higher during this period, ETC’s lower correlation may be partially explained by idiosyncratic factors such as becoming listed on Coinbase in August 2018\(^{39}\).

### 2.2 BTC 3-month Snapshots

**Chart 6 - Dec 1 2018 - Mar 1 2019: Large-cap coins 3-month correlation matrix (BTC)**

Source: Coinmarketcap, Binance Research

---

\(^{38}\) Binance listed NEM in late March 2018.  

Based on BTC returns, correlations from last quarter are much lower than one year prior. On average, the correlation among cryptoassets was 0.24 vs. 0.43 over the same period one year prior.

Correlations during mid-2018 are lower than the previous period (Dec 2017 - Feb 2018), but higher than the most recent period (Dec 2018 - Feb 2019), highlighting a downward trend in overall correlations between cryptoassets.
2.3 Does the Rise of Stablecoins Explain Increased Correlations?

2018 was a bear market year as prices crumbled during the first half of the year and then decreased slowly until a bottom around December.

Chart 9 - 2018: Evolution of the total crypto market cap (USD bn)

![Chart 9 - 2018: Evolution of the total crypto market cap (USD bn)](image)

While the bear market appears to be the most obvious explanation to the increase in cryptoasset correlations (using USD returns), the increased availability of stablecoin trading pairs and listings, as illustrated in our last report\(^{40}\), has led to a material growth in proportion of stablecoin-enabled trading volume versus total cryptoasset trading volume. This could be another factor to consider in evaluating correlations from today’s cryptoasset markets.

Chart 10 - Increasing Volume: Contribution of Stablecoin Volume to Total Industry Volume

![Chart 10 - Increasing Volume: Contribution of Stablecoin Volume to Total Industry Volume](image)

Only one year ago, stablecoin volume represented less than 10% of total cryptoasset trading volume (e.g. Binance had only 5 USDT trading pairs as of February 28th 2018).

Today, stablecoin volume represents more than 30% of the total volume in the cryptoasset industry and Binance has more than 100 stablecoin pairs with different quote currencies (e.g., USDT, USDC, PAX, TUSD, USDS).

During the peak of the bull market (mid-December 2017), speculators used BTC/ETH bought on fiat exchanges to deposit funds onto cryptocurrency exchanges such as Binance or Bittrex to trade immediately into altcoins.

Given these crypto-to-crypto exchanges contributed a large portion of total volume in the industry, most of the cryptoassets used in this correlation analysis were traded solely against BTC, which could explain why their BTC returns had stronger correlations in previous periods than in the most recent period (as many of these large cap assets are now also paired with stablecoins).

Prior to mid-2018, in order to buy/sell coins such as XMR, the highest volume trading pair was XMR/BTC. During large sell-offs or purchases of altcoins, they all exhibited similar price movements in BTC.

Today, cryptoasset trading pairs are no longer BTC-dominated. As of March 2019, most of the largest cryptoassets by market capitalization are now directly traded against stablecoins (USDT as the most popular).

For example, NEO was one of the first coins to be listed on Binance and was extremely popular in 2017.

Chart 11 - NEO trading volume on Binance - Feb 28 2018 vs. Feb 28 2019

---

41 BTCUSDT, ETHUSDT, BNBUSDT, NEOUSDT, LTCUSDT
As of February 28th, 2019, the contribution of the stablecoin pair volume to total Binance volume of NEO increased to 66%, compared to 45% a year ago, taking over the majority of ETH and BTC pair volumes.

NEO is not alone; in fact, most of the assets didn't even have a stablecoin pair on Binance in April 2018. Today, a large majority of the top market capitalization coins do have a “stable counterparty”.

**Table 1 - Existence of stablecoin pairs on Binance**

<table>
<thead>
<tr>
<th>Date</th>
<th>DASH</th>
<th>ETC</th>
<th>XMR</th>
<th>XRP</th>
<th>ETH</th>
<th>ZEC</th>
<th>NEO</th>
<th>DOGE</th>
<th>XLM</th>
<th>NEM</th>
<th>LTC</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 2018</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>-</td>
<td>No</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td>February 2019</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

This trend is not confined to crypto-to-crypto exchanges like Binance - fiat exchanges have also started increasing the number of cryptoasset offerings on their platforms, thereby providing more direct fiat onramps and trading pairs for altcoins. As an example, Coinbase has 17 cryptoassets (and 38 corresponding pairs) as of March 1st, 2019 and continues to explore adding a variety of additional cryptoassets to the platform⁴².

**Conclusion**

In summary, large market-cap cryptoassets exhibited high correlations in USD returns, and these correlations increased over the course of 2018. Conversely, crypto-asset correlations in BTC returns decreased over the same period.

While these changes in correlations coincided with the rise in stablecoin volume and stablecoin trading pair offerings across exchanges, the analysis reveals additional idiosyncratic factors that should be considered when constructing an optimal cryptoasset portfolio.

As this report primarily relied on large market-cap cryptoassets and their performance over a limited time horizon (15 months) that was predominantly a bear market, further analysis across longer time periods, small / medium market-cap assets and additional macro environments can be conducting to augment these findings.

Examining the Implications of Monero's Latest Fork
Discussing the Effects of Forking Out ASIC Miners

Binance Research - March 25th 2019

KEY TAKEAWAYS

- Monero's recent dynamic block-size upgrade will help prevent specific attacks such as the “big bang attack” (i.e. a bloating spam attack to make the blockchain bigger than what the nodes can support).
- However, the change in their PoW algorithm represents the third change over the coin’s existence to provide increased ASIC resistance. Yet, previous Monero forks did not have a long-lasting impact in preventing ASIC miners, as ASIC resistance is essentially a perpetual “cat and mouse game.”
- Following the fork, the subsequent drop in miner participation has led to lower hashrates. As lower difficulty implies lower mining costs, it has resulted in higher profitability for GPU/CPU miners.
- Nevertheless, companies such as Coinhive have halted their Monero mining services, citing a decrease in the price of Monero as a key decision factor. Whereas profitability jumped, the increase in absolute mining revenues remain low.
- Similar to other proof-of-work blockchains, the Monero community faces a tradeoff between centralization and increasing risks associated with lower mining contribution owing to ASIC resistance.

Over its 5-year existence, XMR developers changed the PoW mechanism of Monero software three times in order to achieve “ASIC resistance”. XMR development team typically has scheduled upgrades twice a year for a variety of reasons, such as upgraded security or privacy features. As a result, the protocol has been split into several versions over the years owing to disagreements over these forks.

43 https://threatpost.com/coinhive-monero-shutdown/142290/
44 History of the upgrades: https://github.com/monero-project/monero/tree/release-v0.13#scheduled-software-upgrades
As an example, in April 2018, following disagreements regarding the community’s proposed changes\textsuperscript{45}, Monero (XMR) was forked onto several alternative chains: Monero Original (XMO), Monero Classic (XMC)\textsuperscript{46}, and Monero 0 (XMZ)\textsuperscript{47}. While these projects all claim to represent “the original vision of Monero”, only one of them remains somewhat active, with both development & public interest for XMO and XMZ quickly fading away after release.

**Monero’s XMR Fork in March 2019**

Most recently, Monero (XMR) forked again on March 9th, 2019 but, unlike in April 2018, it was a non-contentious fork that occurred without the creation of any side chain. This time, four justifications were provided for the hard-fork\textsuperscript{48}:

- **an update in the dynamic block size algorithm** designed to prevent a big bang attack\textsuperscript{49} (also referred to as a “spam bloating attack”).
- **a change in the PoW algorithm** (from CryptoNight V8 to CryptoNight-R) in order “to curb the ASICS currently present on the network and further preserve ASIC resistance”.\textsuperscript{50}
- the **addition of a dummy encrypted payment ID to improve transaction homogeneity**. Transaction homogeneity refers to increased fungibility of the cryptoasset, meaning that an individual coin’s history cannot be tainted (like Bitcoin or Litecoin) as addresses are not linked together. In simple terms, Monero is similar to physical bills in the sense that it cannot be traced to the previous owner. As a result, the value of one Monero is always equal to one Monero.
- the **simplification of amount commitments through the shrinkage of “the size of amount encodings”** and the use of “deterministic masks”.

Previous attempts to discourage ASIC miners did not have a long-lasting impact. However, ASIC resistance is somewhat of a “cat and mouse”\textsuperscript{51} game with no permanent solution that completely prevents ASIC mining.

Prior to the March 2019 hard fork, Monero was reportedly dominated by ASIC miners\textsuperscript{52}, with ASICS contributing up to 85% of the network’s cumulative hashrate. Thus, the community decided to push a hard fork update that would force all participants to upgrade to the new protocol.

---

\textsuperscript{45} [https://monero.org/forks/](https://monero.org/forks/)
\textsuperscript{46} [http://monero-classic.org/index_en.html](http://monero-classic.org/index_en.html)
\textsuperscript{47} [https://monero0.org](https://monero0.org)
\textsuperscript{48} [https://www.reddit.com/r/Monero/comments/aw86rx/updated_information_thread_regarding_the/](https://www.reddit.com/r/Monero/comments/aw86rx/updated_information_thread_regarding_the/)
\textsuperscript{49} Please refer to this analysis of the threat of a big bang attack: [https://github.com/noncesense-research-lab/Blockchain_big_bang](https://github.com/noncesense-research-lab/Blockchain_big_bang)
\textsuperscript{50} [https://github.com/monero-project/monero/pull/5126](https://github.com/monero-project/monero/pull/5126) / “ASIC resistance” aims at avoiding the centralization of mining activities due to ASIC miners “kicking out” CPU/GPU miners.
Consequences of Monero’s March 2019 fork

1. Added privacy features and improved security

Newly-included privacy elements such as the addition of dummy information make it harder to determine both the origins and the destinations of every transaction. As several countries (e.g., France) and individual US states (e.g., Texas) are discussing whether or not privacy coins should be banned, this additional privacy feature may lead to higher pressure on countries to create legislature to directly address the status of privacy coins. Regarding the improvement in the countermeasure to prevent a “big bang attack”, the initial issue was that the size of the block could increase exponentially.

- **Constraint on block-size calculation:** Previously, the only constraint on block sizes was that it couldn’t be higher than the median size of the preceding 100 blocks.
- **Initial risk:** Spam attacks were still possible by maximizing the size of each block in order to increase the potential limit of subsequent block sizes. As the total blockchain size is derived from the sum of all existing blocks, a continuous increase of each individual block could lead to an exponential growth of the entire chain, causing nodes with less available disk space to be disconnected from the network. For an in-depth explanation on “big bang attack”, please visit: [GitHub](https://github.com/noncesense-research-lab/Blockchain_big_bang)
- **Solution:** Firstly, XMR development team introduced a long-term (“LT BlockWeight”) median over the previous 100,000 blocks.

**Proposed Code Changes:**

1. \( LT\ BlockWeight = \min(\text{BlockWeight}, 1.4 \times LT\ EffectiveMedianBlockWeight) \)
2. \( \text{EffectiveMedianBlockWeight} = \min(\max(300000, \text{MedianOverPrevious100Blocks}(\text{BlockWeight})), 50 \times LT\ EffectiveMedianBlockWeight) \)
3. \( LT\ EffectiveMedianBlockWeight = \max(300000, \text{MedianOverPrevious100000Blocks}(LT\ BlockWeight)) \)

Going forward, the long-term blocksize can only increase by up to 1.4x after 50,000 blocks.

A second addition is the change in the miner fee as it is now calculated based on a long-term median block weight versus the previous 100-block median weight. Before the fork, clients used a multiplier of the minimum fee during periods of high activities to obtain priority for their transactions and a part of the base block reward would be withheld if the blocksize was higher than the median over the previous 100 blocks. As fees are now set based on the long-term median block weight, fees

---

55. [https://github.com/monero-project/monero/pull/5124/files](https://github.com/monero-project/monero/pull/5124/files)
56. [https://www.reddit.com/r/Monero/comments/av0cn3/is_there_anyone_who_can_explain_the_new_block/ehc1ib3/](https://www.reddit.com/r/Monero/comments/av0cn3/is_there_anyone_who_can_explain_the_new_block/ehc1ib3/)

42
would not decrease when the amount of transactions keep increasing at a lower pace.

2. Knocked out pre-fork ASIC miners

In line with analysis that suggested Monero was mostly mined by ASIC mining equipment, all of these miners were virtually impacted by the fork. Three sub-consequences were directly observable.

1. Sudden drop in hash rate

![Chart 1 - Monero hash rate (in GHash/s) since January 2017](chart1.png)

Between March 8th and March 10th, the hash rate dropped roughly 70%, thereby validating previous pre-fork estimates about the heavy contribution rate of ASICs to Monero’s total network hashrate.

2. Increasing block profitability

![Chart 2 - Mining profitability (USD/day for 1 kH/s) since January 2019](chart2.png)

In the aftermath of the fork, as the difficulty of mining a block decreased, the profitability per block increased sharply by over 200%. On average, the network’s mining difficulty

---

decreased by more than -70%, in line with the slump in the hashrate, meaning that the same CPU or GPU card on average could produce nearly 3 times as many Monero post-fork, on average. The cause of this is two-fold:

- **ASICs are incredibly efficient at mining, so removing their contributions to the network means that the average variable cost of mining on Monero is much higher using general purpose units (GPUs) or alternative hardware used by miners.**
- **Lowering network difficulty also offers a more even playing field for smaller miners using household machines.** After past forks and their corresponding jumps in mining profitability, Moore’s law (chart 3) has been observed, with profitability decaying gradually over time until the next fork was introduced. This time around, it remains to be seen if the same eventual decay in mining profitability will occur once more.

**Chart 3 - Mining profitability (USD/day for 1 kH/s) since January 2017**

3. A brief spike in blocktime

**Chart 4 - Monero average blocktime (in minutes) since January 2017**

Shortly after the upgrade, **the block-time spiked from an average of 2 minutes to more than 10 minutes on March 10th.** Though ASIC miners were excluded from mining activities instantaneously after the fork and the overall network hashrate decreased, **the mining difficulty was mathematically designed to not adjust instantly.**
As a consequence, fewer miners were competing for blocks with pre-fork difficulty levels that assumed higher network aggregate hashrates, leading to longer block times. Interestingly, with longer block times, any adjustments that are implemented at future block height mean that adjustment time is pushed back in terms of real time, further exacerbating the duration of these symptoms. It took roughly 36 hours for the average block-time to return to the normal average of two minutes per block. Unsurprisingly, the fork from April 2018 also led to a similar scenario (as illustrated by the first spike in the chart above to just under 10 minutes per block).

**Conclusion - The Fork’s Outcomes**

**Outcome 1 - Mining remains fairly unprofitable for household miners**

Even though the difficulty has dropped by ~75% since the fork, the profitability increased greatly but the month-on-month increase in absolute USD terms is fairly low.

**Chart 5 - absolute MoM change in mining profitability (USD/day for 1 kH/s)**

![Chart showing MoM change](source: Binance Research, Coinmetrics.io)

As a result, it hints that the project’s efforts to involve more individual users in the network may not be so effective (“fork 2”) with this fork boosting mining profitability by only one-third of the absolute change in the aftermath of the previous fork (“fork 1”). As 20-25% of the size of the pre-fork mining power remains, it suggests that some of the miners still expect a strong price rebound or that they benefit from lower marginal costs for mining than empirically suggested. In comparison, the April 2018 fork (“Fork 1”) had a larger impact in mining profitability, as the price of Monero was more than 3 times higher than XMR price in March 2019, resulting in a much wider magnitude in USD-denominated mining profitability in the aftermath of the two forks.

**Outcome 2 - Lower hashrate = higher probability of 51% attack**

As ASIC miners were forced to “opt out”, the hashrate dropped by more than -70%, resulting in a slightly higher risk of a 51% attack.

In general, ASIC miners may lead to centralization of the mining activities behind any PoW asset, but their absence also exposes a greater tail risk for the network.
Achieving “ASIC resistance” remains a cat and mouse game and there is a trade-off between staving off centralization and boosting mining participation rate. Perhaps an alternative solution would be to encourage competition, transparency, and even collaboration in the ASIC mining industry, such that communities can be in more control in the operations of their networks.

Forks - whether hard, soft, contentious, or non-contentious - are normal events in the crypto-industry and frequent forks may indicate healthy development behind a crypto network. Regardless of the outcomes from this fork, the XMR development team continues future improvement of Monero, with the next fork being already scheduled for October 2019.

**Binance Academy - ASICs**

ASICs are integrated circuits that have been designed to serve a particular use case, in contrast to the general-purpose circuits, such as the CPUs that power our computers and mobile devices. In some circumstances, there are simple computing tasks that don’t require the financial and computational overhead that a general purpose CPU would bring to the table. Instead, an ASIC can be used as a much simpler and efficient alternative (both in terms of cost and energy).

In the world of cryptocurrencies, the term ASIC is widely used to refer to the specialized hardware that are being developed and regularly improved by companies such as Bitmain and Halong Mining. These hardware are designed with the sole intention of mining Bitcoin (or other cryptocurrencies). In short, mining is a process that consists of performing a myriad of hashing functions until a valid hash output is produced. The miner that finds a valid hash uses it as proof for their work, which grants them the right to validate the next block of transactions and collect the block reward.

Although ASICs can be highly efficient, being restricted to a particular use case makes them completely useless for doing anything else. Moreover, the continuous technological advances in the cryptocurrency space bring new ASIC models that quickly render older designs completely unprofitable.

There is also a strong debate in regards to the centralization of mining power caused by ASICs. On the one hand, they provide the much-needed hashpower for securing and verifying blockchains, but they also centralize the power of mining into the hands of a few mining companies who can afford to buy thousands of ASICs to set up and run large mining farms and mining pools.
A look at irregularities discovered on Augur

Design flaws plague Augur’s prediction markets

Binance Research - April 1st 2019

Augur is a decentralized prediction market platform built on top of Ethereum that allows any individual to create a prediction market regarding the outcome of any event, such as a result of a soccer game, the winner of a presidential election, or even the future price of a cryptocurrency. Though the project has stimulated some questions about the legality of some prediction markets and the actions that they may incentivize\(^\text{58}\), the platform itself still has yet to be thoroughly investigated by many.

<table>
<thead>
<tr>
<th>KEY TAKEAWAYS</th>
</tr>
</thead>
</table>
| ● Prediction markets appear to be one of the best use-cases for blockchain as they should be trustless and working without the need of a centralized operator. In theory, a blockchain-based prediction platform can allow for transparency while being out of reach from potential governmental actions and censorship.  
● Yet, Augur - despite being the most popular predictive platform running on a blockchain - faces several issues in its current iteration:  
  ○ Barebones usability functions  
  ○ Low liquidity and participation rates  
  ○ Complex voting, settlement and forking mechanisms  
● Past examples featured scenarios where markets had inherent flaws, leading to controversial outcome reporting and settlements. For active REP token-holders, it illustrates the governance debate between “code is law” and pragmatic approaches.  
● An actively traded market - expiring on April 1st - is currently facing an attack - a “design flaw attack” in which a malicious market creator may design a market with the intention of exploiting a purposeful flaw. Even so, several outcomes can occur during such an attack, without risk. |

Brief description of Augur

Augur is a “trustless, decentralized oracle and platform for prediction markets”. It was founded in 2014 and conducted an ICO in 2015\(^\text{59}\).

\(^{59}\) 80% of the supply was sold through the public initial coin offering. 11,000,000 tokens for 0.58USD. (https://info.binance.com/en/currencies/augur).
Augur markets follow four stages:

- **Creation of a prediction market**: the market creator needs REP to create a market topic, set the event end time, and potentially select a designated reporter that will decide the outcome of the event. However, the community (REP owners) always has the opportunity to dispute and correct any such designated reporter, if there indeed is one.
- **Trading**: trading begins whenever a market is created. Markets are all denominated in Ether (ETH).
- **Reporting**: Reputation (REP) tokens (or designated reporters) are used to determine the outcome of each market.
- **Settlement**: token-holders stake their REP on the actual observed outcome and receive settlement fees from the realized volume in the market, proportional to their stake as determined by the fee set at the time of market creation.

**Existing issues**

Since the official launch of the UI in 2018, there have been some technical issues with the first version of Augur.

1. **General issues**

   In order to access Augur, users must either:
   - download the Augur app (and either utilize (1) an Infura endpoint (2) download the entire Ethereum Blockchain)
   - rely on one of many web UIs

   With a complex base of smart contracts, functions, and features, Augur’s steep learning curve often causes new users to utilize one of two websites - an IPFS-hosted version of a web interface, or the “augur.casino” website. Recently, Veil, Guesser, and several other decentralized apps have been built on Augur to abstract away from some of the usability issues that face an onchain product.

   On these websites, the UI offers several sorting and filtering mechanisms, either by volume, by ending date, or by open interest. This may lead to certain markets receiving more exposure than others via manipulation of its orderbook.

   Decentralized URLs also lead to differences in the warnings, issuances, and features offered on different interfaces. For example, Augur.casino has two sets of warnings for the

---

60 https://www.augur.net/whitepaper.pdf
same prediction market (e.g. “Ethereum Price at end of March 2019?”), one on the market page and one prior to placing an order. Meanwhile, the IPFS version, while nearly identical, lacks such warnings.

**Image 1 - IPFS-hosted version (accessed as of 3/31/2019 at 10am UTC)**

![IPFS-hosted version](image1)

**Image 2 - “Augur.Casino” version displaying a warning (accessed as of 3/31/2019 at 10am UTC)**

![“Augur.Casino” version warning](image2)

**Image 3 - Warning displayed on “Augur.Casino” (accessed as of 3/31/2019 at 10am UTC)**

![Warning displayed](image3)

2. Technical Issues

**Market illiquidity**

With little help in breaking down the complexity of the entire prediction market system, users are usually more likely to participate in markets with low spreads and high volumes, both of which suggest that other users found the market worthy of betting on. However, for the cost of a couple Ethereum transactions’ gas payments, a manipulator could utilize two Ethereum accounts to make fake transactions in order to provide an initial padding of volume that attract potential traders. For the majority of markets, participation rates are incredibly low, conversely leading to a feeding frenzy on the few markets that do have significant reported volume.
Incentive Problems

Currently, the validity bond, or the amount staked by the market creator that is seized if the market created is marked invalid, **does not adjust with size of market**, such that users can repeatedly create bogus markets at a fixed cost. Without trust in the validity of a market, it is difficult for users to participate on any given market, because of increased lockup times due to disputes, and potential swings in value of all outcomes. Consequently, this may exacerbate any existing features that hamper market liquidity.

Voting & Possible Forks

If a market receives a disputé, the settlement of the market will go to a vote, in which the outcomes in question have opportunities to receive stakes denominated in REP from network participants deciding on the outcome they believe in.

The exact proceedings of live disputes may be visualized [here](#).

Stakers that stake with the winning outcome will receive a share of the “wrong stakes” proportional to the amount they contributed to the winning stake. Beginning with an amount as determined by the formula from the whitepaper, each outcome must post 2 times the total amount staked in the entire dispute minus 3 times the stake for the other outcomes in the round. If multiple outcomes pass this threshold continually and one such outcome’s stake reaches 2.5% of Augur’s total supply, the chain will undergo a fork, and all REP users will be able to move their pre-fork REP coins to the chain with the outcome of their choice.

To incentivize users to quickly make a decision, “**all token holders who migrate their REP within 60 days of the start of a fork will receive 5% additional REP in the child universe to which they migrated**”. On top of that, a forking period will end when either:

- 60 days have passed.
- More than 50% of all genesis REP is migrated to a child universe.

This forking situation has some game theoretical situations similar to the Bitcoin - Bitcoin Cash (and subsequently ABC and SV) and the Ethereum - Ethereum Classic forks, in which network participants must judge which network may have a more viable future and a majority of the community’s support.

In the proof-of-work cases, miners must decide which chain has the best utility value, and instantaneously direct their hashrate at their favored chain at the given block height. In this case, **REP holders must decide which result and precedent the result sets is most attractive to keeping and welcoming future volumes from prediction market participants**, such that their governance fees and utility value can be maintained or grow. Users that pick the least popular chains could lose their holdings in the majority’s world, and thus be punished.

It is at this forking juncture that activism of the entire REP body may decide the outcome of
a large market - could a non-active token holder body potentially harm the likelihood success of either outcome? 
With many non-proof-of-work coins, the coins themselves have much power in deciding rewards for participants, and with large amounts of Augur tokens parked on Compound Finance and many centralized exchanges, the number of free tokens that may vote right away may be lower than required to maintain an efficient reporting and settlement for any Augur market.

As a result, with many tokens held in wallet that users does not control or custody themselves, an inactive token holder body may be potentially harmful for the entire Augur ecosystem. Yet it remains unclear whether large token holders, such as exchanges, should - or even can - vote and whether or not the voting ability can be taken away from users who do not hold custody of their own coins.

A Controversial Market
As mentioned before, one of the controversial markets that has just expired is related to the price of Ethereum at the end of March 2019.61
The market posits three outcomes:

1. $1000 or above
2. $100 - $1000
3. $0 - $100

With a volume surpassing 4000 ETH, this market expired on April 1, 2019 1:59 AM (UTC +8). However the additional disclosures section of the market stated that the “General Price of Ethereum Cryptocurrency at end of day March 31st, 2019 UTC.” would be measured. As the contract expires before the end of day UTC time, this contract may end up being marked invalid.

This type of attack can be referred to as a “design flaw attack”.

Here is a summary of the current attack vector as executed on this prediction market:

1. Create a market with multiple outcomes with at least one being quite unrealistic (such as Ethereum being above 1000USD), and one being seemingly very easy to achieve (ETH trading within the range of 100USD to 1000uSD)
2. Simulate market activity by trading between a few wallets to boost volumes (wash trading). As Augur exhibits low volume across a majority of its markets, this specific market becomes the most active and hence, the most visible of all traded markets on Augur.
3. The attacker, on purpose, then sends a limit sell order for the outcome that the “price of Ethereum will be between 100 and 1000USD” at a quote that is above what would be rewarded by an invalid result, but quite below that which an

61https://ipfs.augur.casino/ipfs/QmTbWnep5Cs3eEQMCHRBNyodLReqGF7vLBYCDHKbTJu6F/?ethereum_node_http=https%3a%2f%2feth-mainnet.alchemyapi.io%2fjsonrpc%2f7sE1TzCIRIQA3NJPD5wg7YRIVhxuWAEGa
ugur_node=wss%3a%2f%2faugur-node.augur.casino/#/market?id=0xc9f0006902b67a7a8ef0e94f9140493243bd3019

62 He could alternatively post a limit buy order for any of the other two outcomes if they were priced below 1/3.
unsuspecting participant may consider as a good deal. Thus, the newcomer fills the order, and is now stuck in the potentially invalid market.

4. Once the market expires, the attacker hopes that it will be resolved as “invalid”, such that all shares in the market return an equal amount of ETH for shares of each outcome (“If the market had N possible outcomes (not including the Invalid outcome), and the cost of a complete set of shares was C ETH, then traders will receive C/N ETH for each share settled with the market contract.”)

In this case, each “Yes” outcome in the three-outcome market would be marked to ⅓ value if the market is indeed deemed invalid, and the normal user looking to purchase seemingly undervalued shares for a likely outcome actually ends up purchasing shares that end up getting slashed to ⅓ value.

Outcomes for the settlement of the current case

Outcome 1 - Market resolves as invalid
If the market resolves as invalid, as outlined in the whitepaper, each of the three outcomes would resolve to the price of ⅓, such that all yes outcomes are priced equally, despite the normal participants submitting the majority of the entire pot size for the market reward. According to Predictions.global, the amount invested in the seemingly correct outcome, the $100-1000 range, accounts for a large majority of the market, and based on the market price of this range for the duration of the market, investors buying this outcome, on average, placed nearly twice as much into escrow as the manipulators, so receiving an equal price for all outcomes could cause a loss of over 50% for normal participants, and 100%+ returns for manipulators.

Outcome 2 - Market disputed but doesn’t resolve as invalid
As of March 31st, no rational individual would expect the price of Ethereum to be above 1000USD, so that normal participants would only want to sell this outcome, the only remaining market participants buying the outcome are hoping the market to be resolved as “invalid”.
Yet, if the price of Ethereum is between USD100 and USD1000 at the settlement date (“April 1, 2019 1:59 AM (UTC +8)”) and at the price written in the details section (“General Price of Ethereum Cryptocurrency at end of day March 31st, 2019 UTC.”) and remains between USD100 and USD1000 between both official and implied times on all major exchanges, then pragmatic REP holders may decide to select this outcome as both the intended and correct outcome.

Outcome 3 - Market is not disputed
Though unlikely, the market could potentially be settled as valid and not receive a dispute. In this case, the manipulator, through the use of other addresses, could have also purchased true tokens at a steep discount by creating FUD around the validity of the

---

63 Page 7 of Augur whitepaper.
market. After doing so, he would be able to decide the market and not instigate a decision, fulfilling his own desire to receive funds more quickly. Even so, there’s a chance that the market may be disputed by other market participants who joined with him to push the invalid outcome, leading to risks of defection from any colluding parties.

**Past example of a “design flaw attack”**

In 2018, one of the Augur markets exhibited a total volume of more than USD 2 million on a single market contract: “Which party will control the House after 2018 U.S. mid-term election?”.

One user decided to create a market that would purposely:
- Be generic/vague in the wording of the actual question.
- Specify a settlement date that precedes the actual outcome’s date, yet after the results of the election.

Because the results of the election were public, many “arbitraging participants” decided to bet in favor of the “Democrats controlling the house” outcome, as the Democrats won the election. Yet, the market settlement date was on December 12th, while the change in the US house was effective as of December 13th 2019.

Malicious users decided to provide a market by selling odds that “Democrats would control the house” and then bank on receiving a “Republicans would control the house” dispute settlement that would generate high returns. However this didn’t happen, as the participant eventually settled into “Democrats” being the final outcome. This illustrates the overall debate between pragmatism and “code is law” remains very vivid and difficult to define, making the on-chain governance all the more interesting.

**Potential improvements**

To their credit, the Augur team has already identified several of the considerations mentioned, as well as other potential improvements to consider for the 2nd version of the platform.

However, the improvements were released nearly 6 months ago, yet no official release of upgrades for a version 2 has been announced, while users have been potentially exposed to such concerns this entire duration.

---

64 [https://twitter.com/NTmoney/status/1072536962807066629](https://twitter.com/NTmoney/status/1072536962807066629)
65 [https://predictions.global/augur-markets/which-party-will-control-the-house-after-2018-u-s-midterm-election-0xbbbc0a8baa03535e0a680ee2f057162aaaaafdb570](https://predictions.global/augur-markets/which-party-will-control-the-house-after-2018-u-s-midterm-election-0xbbbc0a8baa03535e0a680ee2f057162aaaaafdb570)
67 [https://medium.com/@AugurProject/augur-v2-details-2547bbfc3c1f](https://medium.com/@AugurProject/augur-v2-details-2547bbfc3c1f)
1. A Price-Based Refunding Mechanism

According to the Augur team, “unfortunately, due to technical limitations, Invalid markets cannot ‘unwind’ trading so that traders receive the exact amount of money they paid for their shares.” However, it would seem to appear that the shares of outcomes for specific markets are in fact fungible, because transactions for outcome “Shares” (held as ERC-20 tokens within one’s wallet) always come with a corresponding transaction for “Cash”, or a value of ETH that was offered by the wallet and escrowed for the purchase of the outcome shares.

Thus, it would be possible, albeit tedious, to track down all the amounts paid for said ERC20s onchain through the smart contract, and that if the user was able to provide all of his or her “shares” ERC-20 in full, they would be able to prove that they were the rightful owner of any shares in question.

In essence, this solution would provide a potential for a “original buyer warranty” - if the market resolves as invalid and the user still holds their full ending position, rather than receiving a mandated 1/N reward for all shares, they could in fact “bring back a receipt of original purchase”, and prove that they indeed sent the corresponding amounts of Ether to the smart contract to receive the shares that they would like to return to the market, less the reporting fees.

Invalidating the market should result in a full return of all funds. The team argues that it cannot reverse funds because the tokens are all ERC20 tokens, meaning that the Augur team has no control over them. Yet, a lock up period is already a huge penalty for users, but it doesn’t properly get attached to the participants who enter the market with their Ethereum.

2. Clear references in the definition of a market

In the current Augur platform, vague sources (in the description of markets) such as “general knowledge” are often used, leading to confusion amongst participants. Further, ambiguous terms referring to time-zones, currencies, denominations, and units may also affect the ability to interpret the true outcome. If the UI were designed to create default times, currencies, and denominations, the chance of accidentally making an invalid market would be much lower.

Additionally, some markets were created long ago, when novice creators didn't fully understand the best practices for specificity, as well as not having the ability to foresee any precedents set after the market’s creation that would deem a market invalid. As far as expiration concerns, market creators could be forced to specify the settlement time a specific period after the event ends, or else be unable to even launch the market in the first place.
3. Market validators with nontrivial stakes prior to the inception of any new market

A potential solution would be to create a new category of participants: **market validators**.

Staking REP tokens, these would verify the integrity of any new market by checking whether the initial terms of the markets to prevent any market resulting in "invalid". For the current controversial market, the designated reporter (ETH address 0xc64e96319366da7d00ef4bc14b42e8b1f3a31f52) **posted a reporter stake of only 0.593 REP, or a little over $5** at time of publishing. That a user could lose such a small amount while potentially reporting maliciously an outcome illustrates the potential for high manipulation due to low validity bonds and stakes for reporters. In fact, the same user has already created an Augur market named “📉Ethereum Price at End of April 📈” designed to exploit the same flaw.

Instead, larger involvement of the REP community prior to the launch of an official market might provide a level of quality control that would encourage users to remain in the ecosystem.

In Veil, a dApp built on top of the Augur protocol, **users have the ability to create user-nominated markets**, in which orders may be placed but the market will not go live until further approval. While this may lead to some elements of centralization, the increased likelihood of validity of markets may inspire greater confidence amongst network participants. The issue of confidence in Augur markets has grown to the point that **metamarkets are being created that discuss the validity of other markets**.

The Augur team **has already admitted that these technical problems** were on their radar 6 months ago, but little action has been taken to protect users. The stance of the team has been that protocol level problems were their main focus and wanted to allow dApps built on top of the protocol to solve some of the user experience shortcomings, but as was seen in the Ethereum fork, sometimes the base protocol needs to react given the issues that may arise at the dApp level. The team and community has already begun to share some additional **materials** and guides to increase the education and awareness of potential users.

A note on Governance Tokens

Governance tokens like Augur may potentially have some perverse incentives - in this case, if there are any disputes or clashes in the market, this is when the token has most value (to settle the dispute), and that stakeholders with opposing views will compete to acquire enough REP tokens to stake in support of their desired outcome. Thus, manipulators may be perversely incentivized to create controversy to spike the price in the voting - fundamentally, the token governing a conflict-riddled platform may see a decline in utility value from declined overall activity and trust the participants, inferring that the long-term value of the project may be hindered by short-term profiteers looking to affect the REP price.
With “reverse network effects” - all participants who are hurt by invalid markets can either:

1. Leave with a loss and warn their friends to not join
2. Trade using their newfound knowledge on the market to trick the next user

While Augur is a strong use-case of blockchain, if some of these issues are not handled properly moving forward, the Augur ecosystem could be left with only its malicious actors and bystanders, as typical normal participants repeatedly losing funds and then leaving the ecosystem.

Binance Academy - Design Flaw Attack

A design flaw attack refers to an attack in which a malicious user purposely creates a smart-contract, decentralized market, or other software with knowledge of certain flaws in order to trick individuals interacting within the permissionless environment. A design flaw attack typically exhibits high apparent incentives for users to lock their funds into a smart contract. A flawed definition in some rules surrounding the contract, or the protocol on which it is built, may lead to unfair settlement or release of funds.

A design flaw attack can also be conducted when a malicious user decides to exploit flaws on a contract that was created by another user without any malevolent intent. In this case, the attack would rely on information asymmetry between the attacker and any potential open network participant.

Examples
Prediction markets on the Augur platform are one target of design flaw attacks. For instance, many of its faulty markets rely on vague and unclear definitions, with the ultimate purpose of tricking users into betting money in a contract whose outcome will be disputed due to conflicting parameters and interpretations.

Other potential design flaw attacks may target oracles or data sources such as price feeds. For example, an attacker could purposely target a market or protocol that relies on a single external price source API that may be deprecated before a contract expiration/settlement date, thus giving the attacker an advantage in being able to manipulate any smart contracts relying on this data source.
Investigating Cryptoasset Cycles

A look at changes in cryptoasset correlations based on market structure

Binance Research - April 11th 2019

KEY TAKEAWAYS

- **Price co-movement** of cryptoassets is quite high; the nascent nature of the cryptoasset market and the weak pricing ability of its participants has likely contributed to this phenomenon.
- **An estimated 7% of the cryptoassets are held by institutional investors**, which is almost one-thirteenth of the institutional holdings proportion for the U.S. stock market.
- Higher turnover rates for cryptoassets (**five times higher** than that of the U.S. stock market) indicate that participants in the crypto asset industry could be more active or reactionary than in traditional markets.
- However, the “UTXO/Realized Cap” metric suggests that **crypto-investors tend to "HODL" as prices drop**, only becoming more active when prices recover.
- Extreme internal correlation among coins is often accompanied by a price “inflection point”.
- Having emerged from a period of the highest internal correlations in crypto history, the data may support the notion that **the cryptomarket has already bottomed out**.

In a previous **report**, we used a cross-sectional method to analyze the internal correlations of the cryptoasset market to observe the cyclical patterns of various assets. We found that low internal correlations between some cryptoassets are often due to three main reasons:

- **Idiosyncratic factors**, such as project-specific news & catalysts, may influence the strength of correlations among cryptoassets.
- **“Binance Effect”**: digital assets listed on Binance often have higher correlations among themselves; conversely, assets not listed on Binance may have lower correlations.
- **Consensus Mechanisms**: a cryptoasset’s consensus mechanism could have an impact on its correlation with the returns of other cryptoassets (i.e., returns of PoW coins exhibited higher correlations amongst themselves than with non-PoW coins.)

However, the overall correlation observed across the cryptoasset market has increased, which may be due to the steady decrease over the course of 2018 in the market’s reliance
on Bitcoin-denominated trading pairs, and the corresponding rise of stablecoin volume in all cryptoasset markets. In this report, we will further discuss the cyclicality of correlations among cryptoassets and the effects of market structure on this cyclicality.

1. Market Turning Points and Cyclical Movements in Correlations

Correlations between the USD price of cryptoassets are constantly fluctuating due to a variety of factors - one of the most important factors is market irrationality, which has an effect similar to a “herding effect” or co-movement phenomenon.

The below chart displays the average correlation, in USD prices, amongst all Altcoins (excluding the top 10 stablecoins). The data shows that whenever correlations between these coins reach a specific positive upper bound of [0.8 to 1.0], the trend of Bitcoin against USD tends to reverse, or at least halts the previous price action.

Chart 1 - Correlation between the smoothed market cap of Bitcoin and Altcoins (excluding stablecoins)

Table 1 below captures the duration and maximum correlation during each period where positive correlations between altcoins and Bitcoin surpassed the 0.8 mark.

---

The cumulative duration of these periods totaled 513 days, or more than one-quarter of the entire sample range from 13 February 2014 to 14 March 2019, indicating that the crypto market is prone to show extreme correlations. This total duration of time above the 0.8 threshold was almost 1.3 times the amount of time during which the metric dipped into negative territory (only 381 days).

Table 1 - Historical crypto-correlation periods over 0.8 (Data from 2013/8/26 to 2019/3/14)

<table>
<thead>
<tr>
<th>Start Date</th>
<th>End Date</th>
<th>Length (Days)</th>
<th>Max Correlation</th>
<th>End of market trend ensues?</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-12-15</td>
<td>-</td>
<td>90</td>
<td>0.991</td>
<td>Y</td>
</tr>
<tr>
<td>2018-09-21</td>
<td>2018-09-30</td>
<td>10</td>
<td>0.830</td>
<td>N</td>
</tr>
<tr>
<td>2018-05-26</td>
<td>2018-07-29</td>
<td>65</td>
<td>0.947</td>
<td>Y</td>
</tr>
<tr>
<td>2018-03-08</td>
<td>2018-04-06</td>
<td>30</td>
<td>0.911</td>
<td>Y</td>
</tr>
<tr>
<td>2017-12-15</td>
<td>2017-12-23</td>
<td>9</td>
<td>0.854</td>
<td>Y</td>
</tr>
<tr>
<td>2017-07-31</td>
<td>2017-09-01</td>
<td>33</td>
<td>0.944</td>
<td>Y</td>
</tr>
<tr>
<td>2017-06-12</td>
<td>2017-06-24</td>
<td>13</td>
<td>0.834</td>
<td>Y</td>
</tr>
<tr>
<td>2016-08-12</td>
<td>2016-10-12</td>
<td>62</td>
<td>0.859</td>
<td>Y</td>
</tr>
<tr>
<td>2016-07-25</td>
<td>2016-07-27</td>
<td>3</td>
<td>0.801</td>
<td>Y</td>
</tr>
<tr>
<td>2015-09-22</td>
<td>2015-10-18</td>
<td>27</td>
<td>0.917</td>
<td>Y</td>
</tr>
<tr>
<td>2015-07-11</td>
<td>2015-08-07</td>
<td>28</td>
<td>0.879</td>
<td>Y</td>
</tr>
<tr>
<td>2014-06-21</td>
<td>2014-09-01</td>
<td>73</td>
<td>0.961</td>
<td>Y</td>
</tr>
<tr>
<td>2014-02-13</td>
<td>2014-04-23</td>
<td>70</td>
<td>0.982</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Average</strong></td>
<td><strong>39</strong></td>
<td><strong>0.901</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

On average, these “0.8+ correlation periods” lasted for durations of about 39 days, with an average maximum correlation of 0.901. The most recent “peak correlation period” lasted 90 days until March 14, the longest such period in crypto-history.

Within this period, the composite altcoin correlation with Bitcoin also hit an all-time high (13 Mar 2018). That coincided with Bitcoin’s fall from the $6,000 range to the $3,000 range. This high correlation suggests that market sentiment has already found a local maximum during that period, and a trend reversal may possibly ensue.

Such a price movement pattern, to some extent, may reflect both the irrational behavior of market participants and some inherent traits of a young market.

---

70 If the trend of the two subsequent weeks after the peak period is different than that of the peak period.
However, given the short history of the crypto market, it may be premature to say that there is a causal relationship between peaks in correlation and market reversals, or if it’s actually a herding effect during the market reversals themselves. We will continue to observe the development of this phenomenon, but believe that it could be a valuable sentiment indicator.

2. Irrational Cognition: Are Crypto Market Correlations Prone To Extremes?

2.1 High proportion of retail investors

The cryptomarket’s frequent periods of extreme correlation are inseparable from the market’s highly retail-driven participation.

From data collected by cryptofundresearch.com, around 700 crypto funds operate in the cryptomarket today, representing a total of just under $10 billion in assets as of January 2019. With a conservative assumption that they all hold solely Bitcoin, this would account for an upper bound of only 14% of the total market value of Bitcoin; If Altcoins are included in the assumption of their holdings, (given that BTC dominance percentage is around 50% as of time of writing according to Coinmarketcap), the “institutional proportion” overall could be less than 7% for the cryptoasset market.

![Investor structure comparison: crypto (estimated) vs. stock markets](chart2.png)

Others include nonprofit holders like central banks or governments.

Meanwhile, crypto’s estimated 7% institutional participation rate represents only one-thirteenth of that for the U.S. stock market.

---

71 [https://cryptofundresearch.com/cryptocurrency-funds-overview-infographic/](https://cryptofundresearch.com/cryptocurrency-funds-overview-infographic/)
Among the main traditional equity markets, only the structure of the Chinese stock market is somewhat similar to the cryptoasset market—in 2017, retail investors accounted for more than 99.8% of the Chinese stock market by number of accounts, more than 40% by market value, and more than 80% by trading volume. In addition to having an unusually high percentage of retail investors, the cryptoasset market and the Chinese stock market both have extremely high turnover rates.

Chart 3 below illustrates the phenomenon that **markets with fewer professional investors tend to have a higher turnover rate** (defined as annual trading volume divided by total outstanding shares).

**Chart 3 - 2018 Annual turnover rate comparison: crypto vs. stock markets**

Annual turnover rate within the cryptoasset market stands at 2150% over 2018, which is 6 times that of the US stock market and 3 times that of the Chinese stock market, indicating that crypto investors are perhaps more easily moved by news and information, holding positions for a shorter time.

---

73 It is based on “adjusted volume” and circulating market capitalization from coinmarketcap.com.
74 An analysis from Obryan (2018) found that consensus was evident across investors as the prices started to rise. In other words, the herding behavior is quite common in cryptomarket.
Generally speaking, non-professional investors are prone to becoming overconfident or overly pessimistic in reacting to market trends, leading to higher potential transaction volume, more volatile prices, as reported in numerous studies.\footnote{Kent and David (2015) provided a summary in Overconfident Investors, Predictable Returns, and Excessive Trading}

However, it is certainly too early to draw the same conclusions about crypto investors. In fact, it may be that crypto investors are more active and attentive to new market developments, and more hands-on with participation in the governance, community development, and general progress of the coins and tokens they invest in. In other words, they have a material impact on the success of the crypto networks they participate in and are incentivized to make their voice heard, even if it is simply through price action.

2.2 HODLing - another feature of the crypto investors

In the face of market downtrends, unlike many momentum-driven institutional investors, most investors in the cryptoasset market may prefer to “HODL” through a prolonged decline in prices, but quickly become active when prices recover to near previous highs.

This behavior can be observed through the metric of “realized cap”, which was introduced by Antoine Le Calvez and Nic Carter\footnote{https://coinmetrics.io/realized-capitalization/} in 2018 and is also referred to as the “UTXO market cap” of a cryptoasset.

This metric is resistant to downward movements in the market capitalization of Bitcoin, as it is a measure based on the summation of the last on-chain movement market price across the Bitcoin network. Thus, rather than marking all of the coin’s available supply to the current spot price, it only marks down coins that are transacted at the spot price from when their most recent transaction occurs.
Chart 4 shows that crypto investors **tended to HODL in bear markets**, leading to only moderate changes in UTXO cap during these periods\(^\text{77}\). If individuals were to transact with Bitcoin at the lower USD value prices at the same pace as pre-bear-market, the decline of **UTXO cap would be steeper**. It is also worth noting that after a significant bear period, the measure does not quickly pick up, at least until the underlying price approaches its previous peak\(^\text{78}\).

For example, from early 2014 to early 2015, the price of Bitcoin fell by 75%, while **UTXO cap actually rose by 15%**; in the most recent bear period from the beginning of 2018 through November 2018, the price of Bitcoin fell nearly 70%, while UTXO cap only fell 5%.

This echoes the findings of Calderón (2018), who utilized the CSAD model\(^\text{79}\) to demonstrate that crypto investors tend to display greater “herding” effects in a bull market, and are more inclined to HODL when overall yields fall in a bearish market.

Additionally, the effects of the price movements of leading coins such as Bitcoin or Ethereum also carry through the rest of the market\(^\text{80}\), as many Altcoins are only available to be traded against other crypto-denominated pairs, leading to the tendency for cryptoassets to form singular, unified trends:

---

\(^{77}\) In some cases, UTXO's market value even rose as the price fell, possibly because investors who entered earlier at a very low price chose to leave, while those who joined later at a high price were reluctant to sell at a loss.

\(^{78}\) As many others, the algorithm isn't perfect, such as when exchanges moving their wallets, can cause a significant amount of market value to be calculated at the new price without any real trading taking place.

\(^{79}\) Identify herding behavior by testing whether the cross-sectional absolute deviations of individual coin returns and the return of a market portfolio keep linear relationship: [https://arxiv.org/pdf/1806.11348](https://arxiv.org/pdf/1806.11348)

\(^{80}\) Also see our report about the impact of the rise of stablecoins on the correlation of the cryptoassets.
Extreme market optimism often drives up the price of all cryptoassets, including the ones with no clear utility or value. This often leads to the formation of a bubble;

Extreme market pessimism often sends the price of all cryptoassets into a tailspin, including the ones with clear utility or value. This often leads to market over-adjustment.

Essentially, high correlation among cryptoassets can be summed up by an “if you can’t beat ‘em, join ‘em” mentality; during a unilateral trend (late bull or early bear phase), excess returns denominated in USD would become harder to capture, so it becomes easier for market participants to just ride the market waves.

However, the effects of “herding behavior” always depend on the specific situation. If the initial information is correct, "herding effects" will cause information to be reflected in the price more quickly. For example, in the 2017 ICO boom, many investors were aware of the potential of cryptoasset financing through the creation ERC-20 tokens, and consequently, investors quickly piled into Ethereum, which illustrates the herding effect that quickly spread through the market and vaulted Ethereum to the second place market cap position behind Bitcoin.  

Whereas the traditional equities market is both mature, with high institutional presence, and sophisticated - with a wide range of derivatives products across many developed countries (e.g. United States, Japan, Germany), the cryptoasset market - which is less than 10 years old - has faced several issues over its young lifetime, such as:

- **Incomplete system and regulations:** The absence of a compulsory information disclosure mechanism adhered to by market participants, a lack of popular market trading instruments (e.g. lack of physically settled futures contracts), and insufficient investor protection measures all reduce enthusiasm of professional investors.

- **Asymmetric information:** The blockchain industry is highly complex, with a relatively high barrier of entry for new participants. This is coupled with the lack of professional, fast and reliable media outlets, resulting in slow information transmission and the rampant spreading of fake news.

- **Limited arbitrage channel:** Inherent limitation of transfer speed/cost of some mainstream coins, regulatory restrictions of many countries, as well as the temporary lack of sufficient derivatives and an in-depth market, there are not enough arbitrageurs, resulted in the asset prices may stay in an unreasonable range for a longer period. However recent reports suggest that cross-exchange arbitrage opportunities decreased over 2018, leading to greater price efficiency.

Due to the above, the effects of a quick-to-react market participant becomes even more pronounced, making accurate pricing of individual cryptoasset even more difficult. Hence,
“irrational behavior” or herding effects should not just be blamed on inexperienced market participants, but should also be attributed to market infrastructure and maturity. However, especially after 2018, we continue to see various traditional research institutions, regulatory bodies, and media outlets paying more attention to the blockchain industry, in addition to a wave of crypto-native coverage and research being built and grown each and every day.

The quickly maturing industry has already attracted new funds and support from governmental and traditional capital sources, and looks to continue to do so with each additional step of regulatory clarity, improved data and news reliability, and reduced usability friction, leading to more efficient price discovery in the market as a whole.

Please see tables 2 and 3 below for a recap of the progress of the space over the last few quarters. With the rollout of many mature financial products covering the industry and a clearer regulatory framework worldwide, the crypto market may be maturing faster than ever.
Table 2 - Recent cryptoasset products by traditional institutions and regulatory progress

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018.5.9</td>
<td>Bloomberg launched its first cryptocurrency benchmark index</td>
</tr>
<tr>
<td>2018.6.28</td>
<td>South Korea reveals new crypto regulatory framework and guidelines pertaining to AML and KYC requirements for crypto exchanges</td>
</tr>
<tr>
<td>2018.7.31</td>
<td>CryptoCompare provide order book and trade data on 50 cryptocurrencies for Thomson Reuters’ financial desktop platform Eikon</td>
</tr>
<tr>
<td>2018.9.10</td>
<td>First bitcoin mutual fund launches in Canada</td>
</tr>
<tr>
<td>2018.11.1</td>
<td>Hong Kong issues new rules to regulate cryptocurrency funds and exchanges</td>
</tr>
<tr>
<td>2018.11.16</td>
<td>Switzerland’s principal stock exchange SIX lists World’s first multi-crypto ETP amidst market collapse</td>
</tr>
<tr>
<td>2019.2.12</td>
<td>First U.S. pension funds invest in crypto venture capital (Morgan Creek)</td>
</tr>
<tr>
<td>2019.2.25</td>
<td>Samsung include a cryptocurrency wallet in its latest flagship Galaxy S10 phones</td>
</tr>
<tr>
<td>2018.2.27</td>
<td>Russian president Putin orders the government to adopt regulations for the digital assets industry by July 2019</td>
</tr>
<tr>
<td>2019.2.26</td>
<td>SIX (Swiss stock exchange) lists its first physically backed Bitcoin ETP (Ethereum ETP was announced a week after)</td>
</tr>
<tr>
<td>2019.3.20</td>
<td>Two CoinMarketCap crypto indices launch on Nasdaq, Bloomberg, Reuters</td>
</tr>
<tr>
<td>2019.4.4</td>
<td>Highest volume ever on CME Bitcoin Futures (USD546m in one day)</td>
</tr>
</tbody>
</table>
### Table 3 - The status of cryptoasset regulations around the world

<table>
<thead>
<tr>
<th>Country</th>
<th>Are crypto exchanges banned, regulated or do they operate in a gray area?</th>
<th>Are ICOs banned, regulated or do they operate in a gray area?</th>
<th>Are crypto payments banned?</th>
<th>Are conversions from virtual currencies to fiat currencies banned?</th>
<th>Is there any planned legislation to increase crypto regulation?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Japan</td>
<td>Regulated</td>
<td>Gray</td>
<td>×</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>Gray</td>
<td>Gray</td>
<td>×</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td>Singapore</td>
<td>Gray</td>
<td>Gray</td>
<td>×</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td>Philippines</td>
<td>Regulated</td>
<td>Gray</td>
<td>×</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td>Thailand</td>
<td>Regulated</td>
<td>Gray</td>
<td>×</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td>India</td>
<td>Gray</td>
<td>Gray</td>
<td>×</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td>S. Korea</td>
<td>Gray</td>
<td>Banned</td>
<td>×</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td>Indonesia</td>
<td>Gray</td>
<td>Gray</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>China</td>
<td>Banned</td>
<td>Banned</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Australia</td>
<td>Gray</td>
<td>Gray</td>
<td>×</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td>U.S.</td>
<td>Gray</td>
<td>Regulated</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Canada</td>
<td>Gray</td>
<td>Regulated</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Brazil</td>
<td>Gray</td>
<td>Gray</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>U.K.</td>
<td>Gray</td>
<td>Gray</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>France</td>
<td>Gray</td>
<td>Gray</td>
<td>×</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td>Germany</td>
<td>Gray</td>
<td>Gray</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Switzerland</td>
<td>Regulated</td>
<td>Regulated</td>
<td>×</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td>Russia</td>
<td>Gray</td>
<td>Gray</td>
<td>×</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td>Nigeria</td>
<td>Gray</td>
<td>Gray</td>
<td>×</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td>South Africa</td>
<td>Gray</td>
<td>Gray</td>
<td>×</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td>Zimbabwe</td>
<td>Gray</td>
<td>Gray</td>
<td>√</td>
<td>×</td>
<td>×</td>
</tr>
</tbody>
</table>

---

82 Data compiled by Bloomberg, released in March 26, 2019, updated by Binance Research on March 29th 2019.
Litecoin’s 2019 Halving Scenarios

What are the implications for Litecoin’s (and Bitcoin’s) future decrease in block rewards?

Binance Research - April 16th 2019

KEY TAKEAWAYS

- Litecoin (LTC), one of the earliest Bitcoin’s spinoffs, will see its **mining reward halved from 25 to 12.5 coins** per block on August 6th, 2019.
- The **block profitability will be cut in half** - all things being equal - in the span of 5 minutes.
- Litecoin’s previous halving was preceded by a large price rally with an increase by more than 200% (and spiking by over 500% over the 3-month period before).
- Bitcoin’s previous two halvings ultimately led to lower mining profitability, providing useful, but limited insights on the general impact of halving events.
- For Litecoin’s upcoming halving, several non-mutually exclusive scenarios are possible:
  - **Price rally that pushes mining profitability** (measured in fiat terms) to levels approaching its pre-halving long-term average.
  - **Increasing hashrate** in the months prior to the halving
  - **Self-adjustment mechanism** where price doesn’t rally, leading to miners exiting the market, resulting in lower block difficulty, which ultimately leads to higher (recovered) profitability.
  - **Permanent drop** in the mining profitability of Litecoin.

Litecoin was created in 2011 by Charlie Lee, who built the new chain by forking most of Bitcoin’s code from its Github repository. Some of the key differences between Litecoin and Bitcoin are its hash function, Scrypt (instead of SHA-256), and reduced block times of 2.5 minutes (versus 10 minutes), allowing a higher theoretical ceiling on maximum transactions per day given a similar blocksize.

In a similar fashion to Bitcoin, the block reward for Litecoin is scheduled to decrease over time, with the decaying rate of issuance leading to an eventual finite supply for the cryptocurrency.

Litecoin’s block reward is **halved** every 840,000 blocks (roughly every 4 years). This time around, what will be the implications for Litecoin’s upcoming block reward halving? Will the Litecoin’s halving be a precursor to Bitcoin’s block reward halving in 2020?

---

83 While most of the code is the same, Litecoin’s blockchain is not a fork of Bitcoin and its blockchain is completely independent from it.

84 Not to forget both Bitcoin Cash and Bitcoin SV.
1. Why are halvings important?

While Litecoin doesn’t have a whitepaper, it is well-publicized that the chain’s block rewards for mining are perpetually reduced by one half every 840,000 blocks\(^85\). With a current average block generation time of ~2.5 minutes, approximately 576 blocks are generated per day. As a result, **block reward halving events occur every 4 years for Litecoin**.

Litecoin’s current block reward is set at 25 litecoin per block and will subsequently decrease to 12.5 litecoin per block around August 6th (at exactly block 1,680,000).

Halving has many important implications for any POW cryptocurrency, but the following are the main general aspects to consider when any chain’s block rewards are halved:

- **Mining profitability is cut by half.** As block rewards are halved, the profitability will be subsequently reduced by 50% as difficulty doesn’t adjust immediately.

\[
\text{Mining profitability (per day)} = \frac{\text{mining rewards per day}}{\text{difficulty}}
\]

- **Potential decrease in miners** may lead to higher risk of a 51% attack if the hashrate decreases, as the cost to rent hashpower would decrease as well. An additional issue is related to potential concentration of the miners in a few pools, typically using ASIC mining equipment.

Halving events are, to some extent, similar to a **predefined change in digital central banking policy**, as they ultimately impact the inflation rate of a cryptocurrency for an extended period of time through the reduction in future supply increase.

A traditional central bank’s policy is determined through periodic meetings by committee members who determine what should be the appropriate policies, approaches, and rates (e.g. marginal lending facility rate, deposit rate) to be set for the economy. The only certainty in central banking policy is the frequency of the meetings (usually every six weeks for the United States Federal Reserve).

Alternatively, the inflation rate for PoW cryptocurrencies such as Litecoin or Bitcoin is pre-determined and set in stone (code), **immutable** and bound to occur at specific block times.

For instance, here are the predicted inflation rates on Litecoin.

---

\(^{85}\) [https://litecoin.org/](https://litecoin.org/)
The current inflation in the Litecoin supply is around 8.4% per year. However, after the halving, the network’s inflation rate is expected to drop to ~4%.

This reduction should not be analyzed in isolation, however there are also some particular aspects of Litecoin that must be considered when discussing its halvings:

- **Lack of hedging markets:** Litecoin doesn’t have any major, liquid markets\(^{87}\) allowing miners to hedge their exposure (e.g. futures markets). As a result, profitability is highly dependent on prices.

- **Revenues from transaction fees are insignificant compared to block rewards:**
  Relative to Bitcoin, Litecoin has much lower on-chain number of transactions, so that a greater proportion of fees collected by miners come from the block rewards as opposed to transaction fees. In addition, the growing popularity of Lightning Network\(^{88}\) may further jeopardize the contribution of transaction fees to total miner revenues. Furthermore, the growing popularity of the Lightning Network - currently being tested on Litecoin - may further shrink the size of transaction fees, thus further constricting miner revenues to just the block rewards themselves. Based on the chart below, Litecoin transaction fees currently represent less than 0.12% of the mining block reward from Litecoin and historically have never represented more than 6% of the mining block reward. In comparison, Bitcoin transaction fees currently represent 4-8% of the mining block rewards and more than 30-40% of the block rewards during December 2017.

---

\(^{86}\) 2019 refers to the period between August 6th 2019 to August 5th 2020.

\(^{87}\) Bitmex only has a single futures contract traded for Litecoin and its volume is insignificant compared to other Bitmex contracts or even to the spot volume of Litecoin markets.

\(^{88}\) Lightning Network layer was enabled on Litecoin before it was activated on Bitcoin.
2. A look at past halving events

Across its 8-year history, Litecoin has had only a single halving of its block rewards, where the block reward dropped from 50 LTC to 25 LTC. This halving occurred at a block height of 840,000 (on August 26th 2015). What were the main key takeaways from this previous halving?

2.1 Litecoin’s August 2015 halving

2.1.1 Price rallied before the event

Litecoin’s price increased from around 1.5 USD (3 months before halving) to over 3 USD post-halving, with a peak of 7 USD in mid-July 2015. The overall volatility of the cryptoasset also correspondingly increased in the months prior to the halving event.

---

89 https://www.coindesk.com/litecoin-first-mining-reward-decline/
90 https://live.blockcypher.com/ltc/block/e2acdf2dd19a702e5d12a925f1e984b01e47a933562ca893656d4af8b44e83/
2.1.2 Hashrate barely dropped

One of the potential consequences from the halving of Litecoin was a potential drop in miner participation. As seen in the chart above, however, Litecoin miners didn’t “opt out” after the reduction in mining rewards per block. The hashrate dropped by roughly 15% around the event, before quickly rebounding in the two weeks following the halving.

2.1.3 Permanent drop in mining profitability

The drop in mining profitability was compensated by the price rally that occurred a few months before block 840,000.

Specifically, this price increase led to a spike in profitability prior to the event. Eventually the halving pushed down the mining profitability back to its long-run equilibrium point, mitigating the effects of the short-term price movement, which led to a skyrocketing profitability prior to the halving.

As a result, post-halving mining profitability was only inferior by a few percent to the long-term median profitability (around 38 USD/day per GH/sec).

In general, price fluctuations remain the largest determinant of the mining profitability as discussed in the report about Monero’s March 2019 fork.

2.2 Bitcoin’s previous halvings

Since the genesis block was created, Bitcoin has had two halvings in block rewards:
- November 28th 2012 (from 50BTC to 25BTC per block)
- July 9th 2016 (from 25BTC to 12.5BTC per block)

Bitcoin’s third halving is expected to occur in May 2020\(^1\).

**Table 1 - Bitcoin’s historical halving figures**

<table>
<thead>
<tr>
<th>Halving date</th>
<th>Preceding 90-day price change</th>
<th>Post 90-day price change</th>
<th>Day-to-day change in mining profitability</th>
<th>Preceding 90-day change in block profitability</th>
<th>Post 90-day change in block profitability</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-08-28</td>
<td>+18%</td>
<td>+141%</td>
<td>-44%</td>
<td>-53%</td>
<td>+139%</td>
</tr>
<tr>
<td>2016-07-09</td>
<td>+54%</td>
<td>-4%</td>
<td>-41%</td>
<td>-37%</td>
<td>-13%</td>
</tr>
</tbody>
</table>

In the case of Bitcoin’s first halving, the post-halving rally in Bitcoin price helped partially offset the nominal decrease in mining profitability.

However, the second halving in Bitcoin led to a general decrease in block profitability (given a constant amount of hashpower). The initial price rally did not compensate for the loss in block profitability. Over the long run, alternative factors such as greater competition in the mining industry, measured by growing difficulty to mine blocks\(^2\), could explain these findings.

As the main results to previous halvings for both Bitcoin and Litecoin have been investigated, what could be the different scenarios for Litecoin’s upcoming halving?

### 3. Halving scenarios

**Outcome 1 - price rallies before stabilizing at a new high**

The price of Litecoin has already started rallying since the beginning of the year, exhibiting a 200% year-to-date return, while the broader market is up by 40% YTD (as represented by Bletchley 10 Index).


\(^2\) [https://bitinfocharts.com/comparison/bitcoin-difficulty.html](https://bitinfocharts.com/comparison/bitcoin-difficulty.html)
Outcome 2 - hashrate increases before the halving

As the rewards will be halved, more miners may decide to start mining Litecoin (instead of other currencies) as they want to mine as much litecoins as possible short-term in anticipation of the future decrease in mining rewards. As a result, the hashrate (and subsequently the mining difficulty) may rise in the months preceding the halving. The hashrate has more than doubled since the beginning of the year and is now at its highest historical level, surpassing 350 THash/sec as of the current time of writing (April 14th).

Outcome 3 - mining profitability adjust as miners exit the market

If some miners were to leave the market and/or switch over to mining other, more profitable coins\(^3\), the hashrate would decrease. As a result, this reduced competition would help compensate for the loss of profitability due to the absolute block reward reduction. On the other hand, loss of hashrate and network participants would increase the centralization of Litecoin, with fewer miners, pools, and participants, which ultimately leads to a greater risk of a 51% attack.

An alternative explanation could be centered around the supply-side mining narrative. Fewer LTCs will be mined after the halving, lessening the selling pressure from miners, as the smaller block rewards act as a smaller relative dilution to the total supply. As a result, fewer litecoins being released per day may result in new market environment which may lead to the stabilization of the price at overall higher price than before the decrease in mining rewards.

Outcome 4 - permanent drop in mining profitability
If Litecoin's post 90-day price post-halving would be near its historical long-term median, all other things being equal, it would result in lower profitability for all Litecoin miners. Ceteris paribus, assuming that manufacturers of mining chips do not innovate and create more efficient equipment instantaneously, LTC prices failing to stabilize at a much higher point than pre-halving prices may lead to a permanent reduction in equilibrium levels of mining profitability for Litecoin miners.

Since this did not occur after last fork, it is impossible to predict how miners would react this time if this outcome were to occur.

Conclusion
If Litecoin price increased further (in USD terms) but remained flat relative to other cryptocurrencies (e.g. BTC, ETH), the mining profitability would still increase, as mining costs, such as electricity and hardware equipments, are denominated in fiat. However, rational miners would still consider the marginal profitability and opportunity costs of mining each PoW cryptocurrency over the same time periods to decide whether or not it is more profitable to mine Litecoin or other cryptocurrencies.

Only an exogenous rally in Litecoin's price (i.e., outperforming all other PoW cryptocurrencies) or increasing usage of the chain itself - resulting in higher total transaction fees collected by miners per block - could compensate for this future decrease in mining block rewards.

Unlike the US Federal Reserve providing guidance that projects roughly 3 future rate hikes for the rest of the year, these halving events are written in the stone of code and are — to some extent — similar to a predefined central banking change in policy for any POW cryptocurrency. Whereas these events are important for miners and other market participants, the scarcity of historical cases lead to uncertainty about what could be the potential outcomes from future halvings, regardless if it is Litecoin, Bitcoin, or even Bitcoin Cash.
In the context of cryptocurrencies, consensus algorithms are a crucial element of every blockchain network as they are responsible for maintaining the integrity and security of these distributed systems. The first cryptocurrency consensus algorithm to be created was the **Proof of Work** (PoW), which was designed by Satoshi Nakamoto and implemented on **Bitcoin** as a way to overcome the **Byzantine faults**.

### Consensus Algorithm

**Definition**

A consensus algorithm may be defined as the mechanism through which a blockchain network reach consensus. Public (decentralized) blockchains are built as distributed systems and, since they do not rely on a central authority, the distributed **nodes** need to agree on the validity of transactions. This is where consensus algorithms come into play. They assure that the protocol rules are being followed and guarantee that all transactions occur in a trustless way, so the coins are only able to be spent once.

### Consensus Algorithm vs Protocol

The term algorithm and protocol are often used interchangeably, but they are not the same thing. In simple terms, we may define a protocol as the primary rules of a blockchain and the algorithm as the mechanism through which these rules will be followed.

Besides being extensively used on financial systems, the blockchain technology can be applied to a wide variety of businesses and may be suitable for different use cases. But regardless of the context, a blockchain network will be built on top of a protocol that will define how the system is supposed to work, so all the different parts of the system and all participants of the network will need to follow the rules of the underlying protocol.

While the protocol determines what the rules are, the algorithm tells the system what steps to take in order to comply with these rules and produce the desired results. For instance, the consensus algorithm of a blockchain is what determines the validity of transactions and blocks. In a nutshell, Bitcoin and Ethereum are protocols while the Proof of Work and Proof of Stake are their consensus algorithms.

To further illustrate, consider that the **Bitcoin protocol** defines how the nodes should interact, how the data should be transmitted between them, and what are the requirements
for a successful block validation. On the other hand, the consensus algorithm is responsible for verifying the balances and signatures, confirming transactions, and for actually executing the validation of blocks - and all this is dependent on network consensus.

Different Types of Consensus Algorithms

There are several types of consensus algorithms. The most common implementations are Proof of Work (PoW) and Proof of Stake (PoS) but other algorithms exist such as hybrid mechanisms or complete alternative methods (e.g. Proof of Authority).

Proof of Work (PoW)

PoW was the first consensus algorithm to be created. It is employed by Bitcoin and other cryptocurrencies. The Proof of Work algorithm is an essential part of the mining process. The PoW mining involves numerous hashing attempts, so more computational power means more trials per second. In other words, miners with a high hash rate have better chances to find a valid solution for the next block (aka. block hash). The PoW consensus algorithm makes sure that miners are only able to validate a new block of transactions and add it to the blockchain if the distributed nodes of the network reach consensus and agree that the block hash provided by the miner is a valid proof of work.

Proof of Stake (PoS)

The PoS consensus algorithm was developed in 2011 as an alternative to PoW. Although PoS and PoW share similar goals, they present some fundamental differences and particularities, especially during the validation of new blocks.

In a few words, the Proof of Stake consensus algorithm replaces the PoW mining with a mechanism where blocks are validated according to the stake of the participants. The validator of each block (also called forger or minter) is determined by an investment of the cryptocurrency itself and not by the amount of computational power allocated. Each PoS system may implement the algorithm in different ways, but in general, the blockchain is secured by a pseudo-random election process that considers the node’s wealth and the coins age (how long the coins are being locked or staked) - along with a randomization factor.

The Ethereum blockchain is currently based on a PoW algorithm, but the Casper protocol will eventually be released to switch the network from PoW to PoS in an attempt to increase the network’s scalability.

Delegated Proof of Stake (DPoS)

The Delegated Proof of Stake (DPoS) consensus algorithm was developed by Daniel Larimer, in 2014. Bitshares, Steem, Ark, and Lisk are some of the cryptocurrency projects that make use of DPoS consensus algorithm.
A DPoS-based blockchain counts with a voting system where stakeholders outsource their work to a third-party. In other words, they are able to vote for a few delegates that will secure the network on their behalf. The delegates may also be referred to as witnesses and they are responsible for achieving consensus during the generation and validation of new blocks. The voting power is proportional to the number of coins each user holds. The voting system varies from project to project, but in general, each delegate presents an individual proposal when asking for votes. Usually, the rewards collected by the delegates are proportionally shared with their respective electors.

Therefore, the DPoS algorithm creates a voting system that is directly dependent on the delegates’ reputation. If an elected node misbehaves or does not work efficiently, it will be quickly expelled and replaced by another one.

In regards to performance, DPoS blockchains are more scalable, being able to process more transactions per second (TPS), when compared to PoW and PoS.

Delayed Proof of Work (dPoW)

Delayed Proof of Work (dPoW) is a security mechanism designed by the Komodo project. It is basically a modified version of the Proof of Work (PoW) consensus algorithm that makes use of Bitcoin blockchain’s hash-power as a way to enhance network security. By using dPoW, Komodo developers are able to secure not only their own network but also any third-party chain that ends up joining the Komodo ecosystem in the future. In fact, dPoW can be implemented for any project that develops an independent blockchain using a UTXO model.

Taking Komodo as one example, the dPoW security mechanism was developed and implemented into the Zcash code base, allowing zero-knowledge privacy and increasing network security by leveraging Bitcoin’s hash rate. At intervals of ten minutes, the Komodo system takes a snapshot of its own blockchain. Then, the snapshot is written into a block on the Bitcoin network in a process called notarization. Basically, this process creates a backup of the entire Komodo system, which is saved within the Bitcoin blockchain.

Technically speaking, Komodo’s community-elected notary nodes write a block hash from every dPoW-protected blockchain onto the Komodo ledger, by executing a transaction on the Komodo chain. Using the OP_RETURN command, the notary nodes store a single block hash onto the Komodo chain.

The reason why the notary nodes select a block hash that is about ten minutes old is to ensure that the entire network agrees the block is valid. Each blockchain’s network still comes to consensus for each block. The notary nodes simply record a block hash from a previously-mined block. Then, the notary nodes write a block hash from the Komodo chain onto the Bitcoin ledger. This process is also completed by executing a BTC transaction and using OP_RETURN to write the data into a block on the Bitcoin chain.
Once this notarization to Bitcoin occurs, Komodo’s notary nodes write that block data from the BTC chain back onto the chain of every other protected chain. At this point, the network will not accept any re-organizations that attempt to change a notarized block (or any blocks that were created prior to the most recently-notarized block).

Currently, dPoW is being used with Bitcoin, but it has the potential to be used as a tool for leveraging both the security and the features of any other blockchain that uses a UTXO model.

Proof of Burn (PoB)

There is more than one version of PoB, but the concept of Proof of Burn idealized by Iain Stewart is probably the most acknowledged within the cryptocurrency space. It was proposed as a more sustainable alternative to the PoW consensus algorithm.

Essentially, **Proof of Burn looks like a Proof of Work algorithm but with reduced rates of energy consumption.** The block validation process of PoB-based networks does not require the use of powerful computational resources and does not depend on powerful mining hardware (like ASICs). Instead, cryptocurrencies are intentionally burned as a way to “invest” resources in the blockchain, so the candidate miners are not required to invest physical resources. In PoB systems, miners invest in virtual mining rigs (or virtual mining power).

In other words, **by performing coin burns, users are able to demonstrate their commitment to the network, gaining the right to “mine” and validate transactions.** Since the process of burning coins represents virtual mining power the more coins a user burns in favor of the system, the more mining power he/she has and, thus, the higher the chances to be chosen as the next block validator.

The process of burning coins consists of sending these to a public verifiably address where they become inaccessible and useless. Typically, these addresses (aka. eater addresses) are randomly generated without having any private key associated with them. Naturally, the process of burning coins reduces the market availability and creates an economic scarcity, causing a potential increase in its value. But more than that, coin burning is another way of investing in the security of the network.

One of the reasons Proof of Work blockchains are secure is the fact that miners need to invest lots of resources in order to finally be profitable. This means that a PoW miner will have all the incentives to act honestly and help the network in order to prevent the initial investments from being wasted. The idea is similar for PoB algorithms but, instead of investing electricity, labor work, and computational power, **Proof of Burn blockchains are supposed to be secured by the investment made through coin burns** and nothing else.
Similarly to PoW blockchains, PoB systems will provide block rewards to miners and within a certain period of time, the rewards are expected to cover the initial investment of the burned coins.

As previously stated, there are different ways of implementing the Proof of Burn consensus algorithm. While some projects perform their PoB mining through the burning of Bitcoins, others achieve consensus by burning their own native coin.

Proof of Authority (PoA)

Proof of Authority (PoA) is a reputation-based consensus algorithm that introduces a practical and efficient solution for blockchain networks (especially the private ones).

The term was proposed in 2017 by Ethereum co-founder and former CTO Gavin Wood. The PoA consensus algorithm leverages the value of identities, which means that block validators are not staking coins but their own reputation instead. Therefore, PoA blockchains are secured by the validating nodes that are arbitrarily selected as trustworthy entities.

The PoA consensus algorithm may be applied in a variety of scenarios and they are deemed a high-value option for logistical applications. When it comes to supply chains, for example, PoA consensus is considered an effective and reasonable solution.

The Proof of Authority model enables companies to maintain their privacy while availing the benefits of blockchain technology. Microsoft Azure is another example where the PoA is being implemented. In a few words, the Azure platform provides solutions for private networks, with a system that does not require a native currency like the ether ‘gas’, since there is no need for mining.

Although the conditions may vary from system to system, the PoA consensus algorithm is usually reliant upon:

- **valid and trustworthy identities**: validators need to confirm their real identities.
- **difficulty to become a validator**: a candidate must be willing to invest money and put his reputation at stake. A tough process reduces the risks of selecting questionable validators and incentivize a long-term commitment.
- **a standard for validator approval**: the method for selecting validators must be equal to all candidates.

The essence behind the reputation mechanism is the certainty behind a validator’s identity. This cannot be an easy process nor one that would be readily given up. It must be capable.
of weeding out bad players. Finally, ensuring that all validators go through the same procedure guarantees the system’s integrity and reliability.

Why Consensus Algorithms Matter to Cryptocurrencies

As previously mentioned, the consensus algorithms are crucial for maintaining the integrity and security of a cryptocurrency network. They provide a means of distributed nodes reaching consensus on which version of the blockchain is the real one. Agreeing upon the current blockchain state is essential for a digital economic system to work properly.

The Proof of Work consensus algorithm is considered one of the best solutions to the Byzantine Generals’ Problem, which allowed the creation of Bitcoin as a Byzantine Fault Tolerant system. This means that the Bitcoin blockchain is highly resistant to attacks, such as the 51% attack (or majority attack). Not only because the network is decentralized but also because of the PoW algorithm. The high costs involved in the process of mining makes it very difficult and unlikely that miners will invest their resources to disrupt the network.

About Binance Academy

Binance Academy is a nonprofit blockchain education portal that offers quality, easy-to-understand content for cryptocurrency users and enthusiasts worldwide.

The above content was selected and retrieved from Binance Academy website. All of this content is publicly and freely accessible in 13 languages.

If you want to learn more about cryptocurrencies and blockchain technology, check out the Binance Academy.
Categorizing Cryptoassets: A Return-Driven Cluster Analysis

What does cluster analysis reveal about Bitcoin, Ripple and other large digital assets?

Binance Research - April 26th 2019

KEY TAKEAWAYS

- Using a correlation matrix along with hierarchical clustering, digital assets can be grouped into several sub-segments.
- Based on weekly returns, large cryptoassets such as Bitcoin and Ethereum exhibit the highest correlations, but Ripple displays a lower correlation than in our previous report and is an exception as the best diversifier amongst digital assets with a market cap above $3 billion.
- Bitcoin forks (Gold and Cash), Ethereum Classic and Litecoin form a single cluster whereas other potential groups around the following effects:
  - “Binance effect”: Tezos and Dogecoin, two assets not listed on Binance, each form a single child cluster.
  - Potential geographical effects such as a dichotomy between American and Asian cryptoassets.
  - “Coinbase listing effect”: some assets that were reported to be listed or investigated by Coinbase seemed to belong to similar clusters.
  - Some privacy coins (Dash and Monero) form a single cluster.
- On the other hand, performing K-Means clustering on risk-return profiles of each cryptoasset did not return any meaningful results. One potential explanation is that return & volatility profiles are not related to underlying price co-movements over the study period.

In a previous report, we used a cross-sectional method to analyze the internal correlations of the cryptoasset market to observe the cyclical patterns of various assets. We found that low internal correlations between cryptoassets are often due to idiosyncratic factors, in addition to a coin’s consensus mechanism and a potential “Binance Effect”. However, the overall correlation observed across the cryptoasset market has increased, which may be due to the rise of stablecoin volume, and corresponding increase in pair offerings, in all cryptoasset markets. In this report, cluster analysis over the twelve previous trading months (March 2018 to March 2019) was conducted to distinguish whether cryptoasset clusters, constructed using an unsupervised learning approach, can be created and more importantly, interpreted.
1. Methodology

“Cluster analysis is a technique used to group sets of objects that share similar characteristics. It is common in statistics, but investors will use the approach to build a diversified portfolio. Stocks that exhibit high correlations in returns fall into one basket, those slightly less correlated in another, and so on, until each stock is placed into a category.”

Source: Investopedia

1.1 Dataset

For the top 30 cryptoassets by market capitalization, USD-equivalent prices were retrieved as reported by CoinMarketCap. Stablecoins are excluded from the analysis along with any cryptoasset that is backed by other assets, whether they are digital or physical. Specifically, 30-day rolling average market capitalizations were computed and the 30 “non-backed” largest cryptoassets (as of March 31st 2019) were selected. The data collection period covers a full year between March 31st, 2018 and March 31st, 2019.

1.2 Algorithm selection

Cluster algorithms are one of the sub-segments of unsupervised learning algorithms. The table below highlights key differences between two of the most common cluster algorithms, k-means clustering and hierarchical clustering.

---

94 Indices, stablecoins or cryptoassets claiming to be backed by collateral (e.g. gold) are excluded from this analysis.

95 http://www.cs.utah.edu/~piyush/teaching/4-10-print.pdf
Table 1 - Comparison between K-Means and Hierarchical clustering methods

<table>
<thead>
<tr>
<th></th>
<th>K-MEANS CLUSTERING</th>
<th>HIERARCHICAL CLUSTERING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size of the dataset?</td>
<td>Large datasets</td>
<td>Small datasets</td>
</tr>
<tr>
<td>Selection of amount of clusters?</td>
<td>Predefined manually</td>
<td>Automatic</td>
</tr>
<tr>
<td>Partitionings?</td>
<td>Single</td>
<td>Multiple</td>
</tr>
<tr>
<td>Approach?</td>
<td>Heuristic</td>
<td>Bottom-up (Agglomerative) Top-down (Divisive)</td>
</tr>
</tbody>
</table>

1.2.1 Hierarchical clustering methodology

1. Data is pre-processed using a correlation matrix based on 1-year weekly returns, thus representing 52 observations. This correlation matrix captures variable interactions in a normalized way. As a result, it **simplifies calculations by inherently eliminating a lot of irrelevant information**.

2. A dendrogram illustrates the composition of each cluster by drawing a U-shaped link between a non-singleton cluster and its children. The height of the top of the U-link represents the distance between his groups of children but also the cophenetic distance between the original observations in the two groups of children.

3. Euclidean distance (i.e. \(L^2\) distance) is used and the linkage method relies on the “Ward” method which **minimizes within-cluster variance**.

1.2.2 K-means clustering methodology

1. Weekly returns are calculated for the largest 30 assets by market capitalization.

2. From these weekly returns, the annualized volatility is computed along with the annualized average return.

   \[
   \text{annualized return} = (1 + \text{average weekly return})^{52} - 1
   \]

   \[
   \text{annualized volatility} = \text{standard deviation of weekly returns} \times \sqrt{52}
   \]

3. Data is pre-processed, using a feature scaling, such that each single value is normalized based on the variance(\(s\)) and mean(\(\mu\)):

   \[
   Z = (X - \mu) / s
   \]

4. Eventually, the analysis relies on a three-process methodology:
   a. **Initialization**: \(k\)-initial centroids are generated randomly.
   b. **Assignment**: \(k\)-clusters are created by matching each observation with the nearest centroid.
   c. **Update**: the centroid of the clusters becomes the new mean.
The second and third steps above are repeated until they converge to a solution that minimizes the sum of squared errors between points and their respective centroids.

5. The k-optimal amount of clusters is selected based on the “elbow curve” methodology that selects an optimal value that minimizes the distance to the centroid for each center while minimizing the amount of clusters.

2. Results

2.1 Selection of assets

The eligible assets based on the methodology described in 1.1 results in the following digital assets being selected are the following:

**Top 10 cryptoassets selected:**
Bitcoin (BTC), Ethereum (ETH), Ripple (XRP), Litecoin (LTC), EOS, Bitcoin Cash (BCHABC), Binance Coin (BNB), Stellar (XLM), Tron (TRX), Cardano (ADA).

**Top 11-20 cryptoassets selected:**
Monero (XMR), IOTA, DASH, Maker (MKR), NEO, Ethereum Classic (ETC), Ontology (ONT), NEM, Tezos (XTZ), ZCash (ZEC).

**Top 21-30 cryptoassets selected:**
Waves (WAVES), Basic Attention Token (BAT), Dogecoin (DOGE), Bitcoin Gold (BTG), Qtum (QTUM), OmiseGo (OMG), Decred (DCR), Lisk (LSK), ChainLink (LINK), 0x (ZRX).

**Chart 1 - 30-day 10 largest average market capitalizations (USDbn) as of March 31st 2019**

Bitcoin, Ethereum and Ripple account for most of the industry total market capitalization.
As explained in the first section, the top 30 digital assets, based on the 30-day mean market capitalization as of March 31st 2019, were considered for this analysis.

As highlighted in our previous reports:
- Correlations are extremely high among large-cap digital assets.
- Ether and Bitcoin also exhibited an extremely high correlation (0.872) between each other.
- **POW assets exhibited higher correlations** with each other than with non-POW assets.
- **Observation of a potential “Binance effect”:** Tezos and Dogecoin, the only two assets not listed on Binance, exhibited lower correlations with other cryptoassets. However, a few additional observations were noted:

- **Dogecoin (DOGE), Tezos (XTZ), Ripple (XRP) exhibited the lowest correlations with other digital assets** across this one-year period. Notably, Ripple is less correlated in the long-term than what our previous analysis suggested across several 3-month time-periods, using daily returns.
- **Ripple is highly correlated with Stellar (0.73).** While Stellar was initially built on the Ripple protocol, its code was forked quickly forked and revamped. As of today, Stellar and Ripple code does not rely on the same common core. Yet these two digital assets still share several similarities as they both aim to "reshape the global remittance industry."

2.3 Hierarchical clustering results

**Figure 2 - Dendrogram based on correlation matrix (based on squared euclidean distances)**

Based on the above dendrogram, some clusters seem to share similar characteristics such as:
- **Geographical affinities**: the popularity of the coins in specific countries and the team’s own location could affect the clusters. For instance, Qtum (QTUM), Cardano (ADA), NEO and OmiseGo (OMG) are projects based in Asia, and most of their coin-holders are located in this region. Similarly, Ripple (XRP), Basic Attention Token (BAT) or Dogecoin (DOGE) are digital assets where most of the teams and investors are located in America.

- **Privacy coins belong to the same sub-cluster** such as DASH and Monero (XMR).

- Stellar (XLM) and NEM are payment systems and they ultimately form a single cluster.

- **“Coinbase listing effect”**: Ripple (XRP) and Basic Attention Token (BAT) are two digital assets that got listed on Coinbase over the study period. Furthermore, Zcoin (ZEC) was listed on Coinbase in November 2018, and followed by Stellar (XLM) and Maker (MKR) a few months after. These three digital assets reside in a common sub-group as well, supporting the notion that depending on the timing of listings on the same exchanges, coins may exhibit similar trends in the same market conditions.

- **Hard forks and “code forks”**: Litecoin (LTC), Ethereum Classic (ETC), Bitcoin Cash (BCHABC), Bitcoin Gold (BTG) all share a common history, whether it is on the chain or not, with the top 2 largest digital assets: Ethereum (ETH) and Bitcoin (BTC).
  - While Litecoin is not a fork of Bitcoin, its code was initially forked with very little changes, from the Bitcoin Github repository. On the other hand, Bitcoin Cash and Bitcoin Gold were forked from Bitcoin.
  - Conversely, Ethereum Classic and Ethereum shares the same genesis block. Whereas Ethereum Classic may be the original chain, Ethereum has become, by far, the most used and active of the two.
  - Here, Bitcoin Cash is in the same child cluster with Bitcoin Gold whereas Litecoin is grouped with Ethereum Classic.

- **Binance Coin represents its own child group and first-degree parent group** but is in a 2nd degree parent group with EOS, Tron (TRX), Lisk (LSK) and Decred (DCR).

- **Potential “Binance effect”**: Dogecoin (DOGE) and Tezos (XTZ), the only two digital assets not listed on Binance, are each their only component in their child group.

- **“Largest market capitalization”**: Bitcoin (BTC) and Ethereum (ETH), the two largest digital assets, belong to the same sub-cluster.

However there are clear limitations to any of the interpretation above:

- **The timing of the listings on Coinbase does not match**. For example, Ripple(XRP) and Basic Attention Token(BAT) were listed more than five months apart.

- **Matches of Misfits**. Waves (WAVES), Ontology (ONT) and Tezos (XTZ) fundamentally, share little in common. By default, they were grouped together as they all exhibited lower correlations with other assets.

- IOTA is grouped with Bitcoin (BTC) and Ethereum (ETH), but its market capitalization is not close to any of them. However it is arguable that:

---

96 For instance, Cardano’s ICO was aimed at Japanese investors who bought up to 95% of the total issue. Furthermore, Emergo is based in Tokyo, Japan. [https://www.worldcryptoidex.com/cardano/](https://www.worldcryptoidex.com/cardano/) [https://emurgo.io/#/ja](https://emurgo.io/#/ja)

97 [https://blog.coinbase.com/stellar-lumens-xlm-now-available-on-coinbase-37bc730ec79a](https://blog.coinbase.com/stellar-lumens-xlm-now-available-on-coinbase-37bc730ec79a)
- Bitcoin: the first Blockchain 1.0 for digital money
- Ethereum: the first Blockchain 2.0 with the introduction of smart contracts
- IOTA could be seen as the first Blockchain 3.0 for the Internet of Things
- If EOS, Tron (TRX) and Lisk (LSK) are all on a similar market same segment ("blockchains with smart contracts"), they don’t have much in common with Decred (DCR) that defines itself as an “autonomous digital currency”.

2.4 K-means analysis

**Figure 3 - Elbow curve - Selecting the optimal amount of clusters**

![Elbow curve](image)

Based on the above figure, the optimal amount of clusters appears to be around 6, as the marginal improvement in the total within-cluster sum of squared distances becomes very small beyond 6 clusters.

As a result, six clusters are selected.

**Table 2. Risk-return profiles for first cluster (A)**

<table>
<thead>
<tr>
<th></th>
<th>BNB</th>
<th>BAT</th>
<th>MKR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Return (%)</td>
<td>134</td>
<td>242</td>
<td>186</td>
</tr>
<tr>
<td>Volatility (%)</td>
<td>91</td>
<td>132</td>
<td>116</td>
</tr>
<tr>
<td>Cluster</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
</tbody>
</table>
Table 3. Risk-return profiles for second cluster (B)

<table>
<thead>
<tr>
<th></th>
<th>BTC</th>
<th>LSK</th>
<th>DCR</th>
<th>OMG</th>
<th>QTUM</th>
<th>BTG</th>
<th>ZEC</th>
<th>NEM</th>
<th>ETC</th>
<th>NEO</th>
<th>XLM</th>
<th>ETH</th>
<th>XMR</th>
<th>LTC</th>
<th>DASH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annualized volatility (%)</td>
<td>65</td>
<td>102</td>
<td>97</td>
<td>116</td>
<td>117</td>
<td>106</td>
<td>98</td>
<td>100</td>
<td>94</td>
<td>110</td>
<td>106</td>
<td>96</td>
<td>94</td>
<td>104</td>
<td></td>
</tr>
</tbody>
</table>

Cluster B is constituted by digital asset with high volatility but negative average returns over the period.

Table 4 - Risk-return profiles for the 4 other clusters (C-F)

<table>
<thead>
<tr>
<th></th>
<th>XRP</th>
<th>EOS</th>
<th>DOGE</th>
<th>IOTA</th>
<th>TRX</th>
<th>XTZ</th>
<th>ADA</th>
<th>WAVE</th>
<th>ZRX</th>
<th>BCHABC</th>
<th>LINK</th>
<th>ONT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annualized average return (%)</td>
<td>29</td>
<td>95</td>
<td>70</td>
<td>-33</td>
<td>55</td>
<td>-8</td>
<td>1</td>
<td>63</td>
<td>29</td>
<td>420</td>
<td>214</td>
<td></td>
</tr>
<tr>
<td>Annualized volatility (%)</td>
<td>136</td>
<td>152</td>
<td>150</td>
<td>130</td>
<td>132</td>
<td>129</td>
<td>128</td>
<td>126</td>
<td>119</td>
<td>192</td>
<td>143</td>
<td>208</td>
</tr>
</tbody>
</table>

Based on a traditional risk-return attributes of cryptoassets, many assets share the same risk-return profiles (clusters B and C). Cluster C is consistuded assets with extremely high volatility but annualized returns either positive or slightly negative (the exception being IOTA).

Clusters C, D and E are made of one single digital asset such as:
- Cluster is constituted by Bitcoin Cash (BCHABC): the second highest-volatility asset in the group but with an extremely small positive return. This risk-profile is explained by the Bitcoin Cash fork (in November 2018) that led to the creation of Bitcoin SV (BSV/BCHSV), creating a common event in the coins’ mutual histories.
- Clusters E and F are each made of a single asset that exhibit extremely high returns:
  - ChainLink (LINK) forms cluster E.
  - Ontology (ONT) forms cluster F.98

In general, the drawback of this method is that two assets might belong to the same cluster without having any correlation. Precisely, two assets may display a negative correlation.

98 As Ontology weekly returns are not normally distributed (with large extreme positive values), the annualized average return is strongly biased upward.
while simultaneously sharing an exact same risk-return profile within the market, resulting in them being part of the same cluster.

In the future, our approach must be extended to include additional characteristics such as: market capitalization, volume and turnover ratio.

Native blockchain metrics such as hashrate, active addresses, on-chain transactions or amount of active nodes could also be used as inputs in cluster analysis to analyze what are the underlying dynamics among cryptoassets.

3. Conclusion

Cluster analysis is an unsupervised learning technique that provides flexibility in classification of objects in groups without introducing human bias. For digital assets, cluster analysis has not been extensively studied in research and this report represents one of the first attempts at classifying cryptoassets from an unsupervised approach.

Hierarchical cluster analysis revealed potential groups of cryptoassets such based on characteristics such as asset function (e.g. privacy tokens), chain history (e.g. Bitcoin forks) or a potential dichotomy between Asian and US-based cryptoassets. Eventually the potential existence of a “Binance effect” strikes again along with a newer potential effect related to Coinbase-related news (e.g. Ripple, Basic Attention Token).

Whereas some of the results appear to be consistent with industry-defined fundamental approaches, the difficulty of finding trustworthy data may hold investors back from completing a thorough analysis on this topic. In comparison, traditional equity markets offer plenty of metrics (e.g. P/E ratio, turnover, ROE) that are routinely used in research reports.

Additional cluster analysis of the digital asset industry could be performed from different perspectives, and further research on different crypto market cap segments (e.g. mid and small caps) with alternative inputs such as hashrate or on-chain transactions may help paint a more complete picture for the cryptoasset market as a whole.
The Evolution of Stablecoins

How are fiat-backed stablecoins adapting their strategies to remain competitive?

—

Binance Research - May 15th 2019

KEY TAKEAWAYS

- As USD-backed stablecoins continue to see increased adoption and trading pair usage, their **volume dominance** over BTC-denominated pairs is **higher** than ever. However, from a trading environment perspective, there are few differentiations amongst the mid-cap stablecoins (i.e. PAX, TUSD and USDC).

- The first four months of 2019 led to **net inflows** for most stablecoins; January saw the largest inflows, but the subsequent three months had more redemptions than deposits. Bucking this trend, PAX and USDC exhibited strong inflows of **over USD 40 million respectively** towards the end of April, potentially owing to the recent Tether turmoil.

- Irrespective of its recent breaking of its dollar peg, Tether (USDT)’s use is continuing to shift from the Omni blockchain to other public chains like Ethereum and Tron. Meanwhile, Paxos (PAX) will soon be rolled out on the Ontology blockchain.

- Furthermore, the expansion of non-USD stablecoins, illustrated by Trust Token’s new offerings (HKD, AUD, CAD, GBP, EUR), may lead to several key developments:
  - **Additional channels for global remittance**
  - **Easier to hedge against fiat currency risk**
  - **Greater price efficiency for non-USD cryptocurrency exchanges**
  - **The development of blockchain FX exchanges, either on or off-chain**

- Eventually, stablecoin initiatives from various non-financial companies, i.e. **Facebook and Samsung**, might further the **growth of the digital asset industry by introducing cryptocurrencies and blockchain technology to their large existing user bases**.

The large majority of collateralized stablecoins are USD-pegged. However, many stablecoin-related projects are now rolling out additional products and services that may expand the use cases and reach of these coins beyond USD barriers. In this report, we examine the current state of stablecoin popularity, and what might be next on the stablecoin horizon.
1. Ever-increasing popularity in USD-collateralized stablecoins

1.1 Year-On-Year Volume Breakdown comparison on Binance

Chart 1 - Comparison of 24h Quote Asset volume between May 1st 2018 and May 1st 2019 on Binance

As discussed in our previous report about crypto-correlations, stablecoins are continually growing in popularity. Quote asset volumes driven by stablecoins on Binance (denoted as USD(S) in the figure above) have grown from just over one-third of all volume (35.78%) one year ago to over three-fifths (60.55% as of May 1st, 2019), eating into the market share of both BTC-denominated and ETH-denominated pairs. Interestingly, the share of volume in BNB pairs also doubled during the same time period.

1.2 Stablecoin pair additions on Binance over first 4 months of 2019

Part of the increase in volume from stablecoins can be attributed to the introduction of several stablecoin pairs with new quote assets and base assets.

Table 1 - Addition of new stablecoin pairs on Binance for existing assets over the first four months of 2019 *

<table>
<thead>
<tr>
<th>Quote Asset</th>
<th>USDT*</th>
<th>PAX</th>
<th>TUSD</th>
<th>USDC</th>
<th>USDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Base Asset</td>
<td>WAVES, HOT, ZIL, ZRX, BAT, XMR, ZEC, IOST, DASH, OMG, THETA, ENJ, MITH, USD</td>
<td>WAVES, BCHABC, LTC, NEO, BTT, ZEC, ADA, USDS</td>
<td>WAVES, BCHABC, LTC, BTT, ZEC, ADA, USD</td>
<td>WAVES, BCHABC, NEO, LTC, BTT, ZEC, ADA, USDS</td>
<td>BTC, BNB</td>
</tr>
</tbody>
</table>

* excluding new base asset listings (e.g. initial pairs offered for BTT or FET)

Large cryptoassets such as NEO, Litecoin (LTC), Cardano (ADA) or Bitcoin Cash (BCHABC) received additional trading pairs against PAX, TUSD and USDC, complementing the previous
addition of USDT pairs. On top of this, a dozen of large assets were listed against USDT which is expected to further reduce the percentage of the cryptoasset total trading activity from BTC pairs to stablecoin pairs.

1.3 Net inflows: more deposits than redemptions over the first four months of 2019

Table 2 - 2019 first 4-month redemptions & deposits for main USD-backed stablecoins

<table>
<thead>
<tr>
<th></th>
<th>USDT⁹⁹</th>
<th>PAX</th>
<th>TUSD</th>
<th>USDC</th>
<th>USDS</th>
<th>GUSD</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Redemptions</strong></td>
<td>-</td>
<td>(155,469,012)</td>
<td>(67,750,435)</td>
<td>(395,289,454)</td>
<td>(3,014,519)</td>
<td>(97,462,832)</td>
</tr>
<tr>
<td><strong>Deposits</strong></td>
<td>-</td>
<td>173,879,681</td>
<td>70,800,456</td>
<td>437,262,481</td>
<td>7,215,884</td>
<td>54,299,444</td>
</tr>
<tr>
<td><strong>Net inflows</strong></td>
<td>975,370,119</td>
<td>18,410,669</td>
<td>3,050,021</td>
<td>41,973,026</td>
<td>4,201,365</td>
<td>(43,163,389)</td>
</tr>
<tr>
<td><strong>Market Cap</strong></td>
<td>2,888,440,781</td>
<td>160,737,039</td>
<td>208,021,789</td>
<td>293,184,174</td>
<td>5,635,840</td>
<td>47,831,688</td>
</tr>
<tr>
<td><strong>% Relative</strong></td>
<td>+51.0%</td>
<td>+12.9%</td>
<td>+1.5%</td>
<td>+16.7%</td>
<td>+292.9%</td>
<td>-47.4%</td>
</tr>
</tbody>
</table>

Once again, USD Tether (USDT) saw the largest net inflow, with a total increase slightly below $1bn USD. Though Tether’s market cap is much bigger than the cumulative market capitalization of all five other stablecoins discussed in the table above, these inflows still represent an increase of around 50% of Tether’s total supply, particularly notable in a period of turmoil for the company.

Chart 2 - Evolution of total monthly net inflows (USD million) in non-USDT stablecoins in 2019

![Chart 2](image)

Amongst the non-USDT stablecoins, USDC was the biggest gainer in circulating supply, seeing an inflow of nearly **60 million USD** in January. While USDC saw the largest monthly

---

⁹⁹ Based on changes from the total assets displayed on the current balances from [Tether’s website](https://tether.to). Historical snapshot are saved [here](https://tether.to/assets).
net redemption amount in February, it rebounded with a slightly positive inflow in March. In April, both USDC and PAX saw minting of over 40 million tokens. Notably, GUSD was the only stablecoin not to have an inflow in any of the four months, *displaying a continual net redemption trend.* As a result, owing to its small market cap, Gemini Dollar lost nearly half of its market capitalization in the first four months of 2019.

2. Trading environment overview

2.1 Untethered stablecoins have small differences

We selected BTC, being the largest digital asset in the world by market capitalization, to act as the base currency for comparing the liquidity of each stablecoin on Binance: Tether (USDT), Paxos (PAX), TrueUSD (TUSD), USD Coin (USDC), and StableUSD (USDS).

<table>
<thead>
<tr>
<th>Stablecoin Pair</th>
<th>Average Spread (%)</th>
<th>Median Spread (%)</th>
<th>95-pctile Spread (%)</th>
<th>5-pctile Spread (%)</th>
<th>Average time between 2 fills</th>
</tr>
</thead>
<tbody>
<tr>
<td>BTCUSDT</td>
<td>0.02</td>
<td>0.02</td>
<td>0.05</td>
<td>Inferior to 0.01</td>
<td>00:00.3</td>
</tr>
<tr>
<td>BTCUSDC</td>
<td>0.09</td>
<td>0.08</td>
<td>0.19</td>
<td>0.03</td>
<td>00:07.3</td>
</tr>
<tr>
<td>BTCUSDS</td>
<td>0.26</td>
<td>0.23</td>
<td>0.47</td>
<td>0.13</td>
<td>02:33.1</td>
</tr>
</tbody>
</table>

Unsurprisingly, the BTC/USDT pair exhibits the lowest median and average spreads over April 2019. With USDT listed on so many other exchanges, one would expect a tight spread given the potential for cross-exchange arbitrage strategies. On top of this, the frequency of filled trades (measured by the distance in time between two consecutive trades) is extremely high for this pair, occurring at an average frequency of under 0.3 seconds.

What does this data reveal about the “untethered” trading landscape?

- Paxos (PAX) and USD Coin (USDC) exhibit the lowest BTC median and average spreads, with both figures being below 0.09%. A close third is TUSD, with an average BTC spread of around 0.11% and a median spread around 0.10%. This slight gap between TUSD and PAX / USDC could be linked to the recent change of pair naming logic from “TUSD/BTC” to “BTC/TUSD” may have thrown off automated traders who failed to update the ticker accordingly.
- StableUSD (USDS) lags behind the first three stablecoins, as the average time (on BTC/USDS) between two consecutives fills is above 2 minutes. The main explanation is that the supply is extremely small in comparison to the other stablecoins (around 5 million) and concentrated on a single exchange. As a result, cross-venue arbitrage opportunities are limited, ultimately resulting in lower volumes and higher spreads.
- The average time between two fills is under 10 seconds for all stablecoins against BTC with the exception of StableUSD (USDS).

2.2 Tether volatility: low but recent spike in late April

Chart 3 - Kraken USDT/USD daily OHLC from January 1st 2019 to April 30th 2019

Over the past trading four months, there were three major phases & events in the price of Tether:
1. The price fluctuated around dollar parity (0.99-1.01) for the first three months of 2019.
2. Bitcoin rebounded on April 1st and USDT jumped to stabilize around 1.01.
3. Recent news from NY AG\textsuperscript{100} led to a large price drop in Tether with a brief bottom of 0.95 on April 26th. Since then, the price has rebounded to a median price bouncing between 0.98 and 0.99.

Recent developments\textsuperscript{101} about Tether may lead to greater price volatility in the coming months. What are other expected developments in the stablecoin industry and their potential implications for the digital asset industry?

\textsuperscript{100} https://www.bloomberg.com/news/articles/2019-04-26/cryptocurrencies-lose-10-billion-on-tether-cover-up-allegations
3. Axes of differentiation

3.1 Addition of new blockchains

3.1.1 Tether: OMNI is not the end-all-be-all

While Tether is “blockchain agnostic” and features an ERC-20 token, most of its supply runs on the OMNI layer, which is built on top of the Bitcoin blockchain. Recently, a partnership between Tether and Tron has made the news, leading to potential expansion on yet another chain.

Regardless of the specific chain, the trend of Tether lessening its OMNI reliance marches on. As of April 30th, 400 million for Ethereum-based and 137 million for Tron-based tokens existed. In comparison, USD Tether running on the OMNI blockchain represents roughly 2.82 billion, or 80% of all the USDT in existence today.

**Chart 4 - Breakdown of all USD Tether issued across blockchains as of April 30th 2019**

This is expected to change, however, as large exchanges are now increasingly supporting deposits and withdrawals of Tether on alternative (i.e. non-OMNI) blockchains as illustrated below.

---

102 [https://tether.to/usdt-introduced-to-tron-blockchain/](https://tether.to/usdt-introduced-to-tron-blockchain/)
103 All authorized Tethers were included. [https://wallet.tether.to/transparency](https://wallet.tether.to/transparency)
Table 4 - Exchanges supporting non-OMNI versions of USD Tether

<table>
<thead>
<tr>
<th>Exchange</th>
<th>Binance</th>
<th>Bitfinex</th>
<th>Huobi</th>
<th>OKEX</th>
<th>Gate.io</th>
<th>Poloniex</th>
<th>Kraken</th>
<th>Kucoin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethereum</td>
<td>no*</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Tron</td>
<td>no*</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>

* Binance has both an ERC20 USDT and a TRC10 USDT wallet.

In contrast with USDT, EURT (EUR Tether) runs solely on the Ethereum blockchain, with a total slightly above EUR50 million.

Over time, the proportion of USDTs minted on Ethereum/Tron relative to total supply has grown to be much higher than before, as illustrated by the chart below from the end of 2018, when ERC-20 USDT marked just a small, small sliver of the entire USDT supply.

Chart 5 - Breakdown of all USD Tether issued across chains as of December 31st 2018

3.1.2 Ontology’s support of the PAX stablecoin

Ontology recently announced that it will partner with Paxos to issue a collateralized stablecoin based on Ontology’s OEP-4 token standard while keeping its existing ticker “PAX”. For Ontology, this would allow greater participation of individuals and institutions into the Ontology decentralized ecosystem. Eventually the team would “enable atomic swaps between the Ontology-based main blockchain and other blockchains” in order to make it easier to transact stable units with its technology.

For Paxos, it would enable the company to further differentiate from other stablecoin issuers such as Circle or TrustToken, and potentially to obtain a “stablecoin monopoly” for decentralized applications running on Ontology. This may be a recurring trend for many stablecoin issuers and chain pairs, leading to future pairing of specific blockchains with stablecoin issuers marking the end of blockchain agnosticism for these issuing companies.

USD 100 million worth of PAX tokens are reportedly going to be issued on the Ontology blockchain in May-June 2019. It remains to be seen which exchanges will also start...
accepting deposits and withdrawals of this token. However, the main goal of this partnership appeared to be aimed at in-dApp usage, rather than trading.

Chart 6 - To-be-issued Ontology-based PAX compared to existing Ethereum-based PAX (as of April 30th 2019)

3.2 Additional support of new collaterals: Trust Token’s expansion to a wide range of fiat currencies

TrustToken, the company behind TUSD, which launched in March 2018, announced consecutively in April 2019 that TrueGBP\textsuperscript{104} and TrueAUD\textsuperscript{105} tokens, along with future support of a wider range of fiat currencies, namely CAD & HKD (2019 Q2) and EUR (2019 Q3) in the roadmap.

What are the potential implications of the ever-increasing range of fiat collateralized stablecoin that are non-USD denominated?

- **Additional channels for global remittance**: from a speed and cost perspective, these new stablecoins are likely to help transferring money worldwide, and users will continually demand a greater range of currencies beyond USD. For end users whose primary currency is not the US dollar, the currency risk will be mitigated.

- **Ability to hedge against fiat currency risk**: fund managers or retail investors/traders, whose profit currency is not the US dollar, will be able to calculate their PnL in their local currency with the added ability to recognize their profits in a different currency with greater ease.

- **Greater price efficiency for non-USD fiat exchanges**: new stablecoins can lead to broader opportunities for cross-exchange arbitrage, particularly between non-USD fiat exchanges. Exchanges where the primary quote currency is different from the US dollar (e.g. EUR: Kraken, Binance Jersey) could be more efficiently arbitraged with the introduction of these new stablecoins.

- **Creation of FX markets on the blockchain**: if stablecoin providers such as TrustToken continue to develop new stablecoins that receive large subsequent inflows, it is possible that this added liquidity may ultimately result in added opportunities for more advanced exchange-related products. In particular, FX blockchain-based exchanges may be developed, where users could trade

\textsuperscript{104} [https://www.coindesk.com/a16z-backed-trusttoken-launches-stablecoin-pegged-to-uk-pound](https://www.coindesk.com/a16z-backed-trusttoken-launches-stablecoin-pegged-to-uk-pound)

\textsuperscript{105} [https://www.coindesk.com/trusttoken-launches-aud-backed-stablecoin-with-3-more-to-follow](https://www.coindesk.com/trusttoken-launches-aud-backed-stablecoin-with-3-more-to-follow)
popular FX pairs such as EUR/USD or JPY/USD in a blockchain environment. These exchanges could be either:
- **centralized** allowing the use of **high leverage and margin trading**.
- **decentralized** such as an **Ethereum-based DEX for stablecoins**, addressing the counterparty risk problem.

3.3 Increasing participation of non-financial institutions: could Facebook Coin and Samsung Coin become future game changers?

3.3.1 Facebook Coin

Facebook is reportedly working on its own blockchain solution for a future stablecoin tentatively named “Facebook Coin” (also referred to as “Project Libra”). This digital currency is expected to be integrated into Whatsapp, the popular messaging service previously acquired by Facebook, to allow users to transfer money to each other. More technical details on Project Libra are still unknown, including whether this digital currency would run on an existing blockchain or a new one built from scratch, and whether its blockchain would be public or private (such as an implementation of **Quorum with the JPM Coin**).

Regardless, Facebook has an entire ecosystem across its Facebook, Messenger, Whatsapp, and Instagram products that could integrate this future digital currency. With a user base in the billions, end use-cases could span from international remittances to payment for premium content (e.g. games) for individual users and services such as advertising campaigns, etc. for businesses. The project is led by David Marcus (ex-Paypal president) and, as noted by Barclays analyst Ross Sandler, has the potential to generate new income-generating sources for Facebook.

Four core scenarios can be drawn for this chain/coin, based on two independent variables: whether the chain is public or private, and whether there is a central authority, a la Ripple, or not:

1. **Private with a central authority**: the blockchain would not be immutable by design (e.g. Facebook controlling the majority of the nodes) and would solely be used as an accounting system to avoid double payment issues.
2. **Private with no central authority**: the blockchain would be immutable but an insurance mechanism or a litigation system would exist to prevent fraud.

---

3. **Public with a central authority:** the blockchain would not be immutable but all transactions would be public.

4. **Public with no central authority:** the blockchain would be immutable with all transactions being public.

While it is difficult to predict what this project will ultimately result in, this blockchain is likely to be private (or partially private) with some degree of authority from Facebook itself. In a similar fashion to the JPM Coin, this project could constitute a stepping stone in mass-adopt of cryptocurrency and other digital assets while contributing to the “unbanking” of the payment industry.

### 3.3.2 Samsung Coin

On April 24th, Samsung was reportedly building its own blockchain on top of Ethereum. This announcement follows the hype about the Samsung Galaxy S10, the company’s flagship phone, which features an integrated Ethereum wallet, and also echoes the company’s focus on blockchain given its recent investments from the Korean company into several prominent blockchain-based companies such as Ledger.

While “Samsung Coin” may not be a pegged currency (very few details have been provided at this stage), it remains a strong possibility that it will be a price-stable currency, as the stability would allow for easier integration across the entire ecosystem of Samsung services and devices.

Initial reports indicate that this blockchain could be a hybrid in structure, with potential private elements such as a private-public state option (similar to that to JP Morgan’s Quorum). However, the exact consensus mechanism and nature of the blockchain, i.e. “whether it would be a permissioned or permissionless network?”, remains unknown.

---


Conclusion

Unsurprisingly, collateralized stablecoins are continuing to gain popularity but major differences in stablecoins exist from a trading perspective. BTC markets are dominated by Tether with greater liquidity represented by lower spreads and higher volumes than other stablecoins. Excluding StableUSD (USDS), all other stablecoins exhibit similar liquidity profiles but USD Coin (USDC) and Paxos (PAX) exhibited slightly lower spreads than TrueUSD (TUSD) in April 2019. Most of the stablecoins also received more deposits than withdrawals during the first four months of 2019, with recent large inflows in April for Paxos and USD Coin.

Competing for market share, these stablecoin providers are becoming increasingly innovative in their product offering:

- **Tether** is seeing increased adoption of its Ethereum-based and Tron-based tokens.
- **TrustToken** is planning to roll out several new stablecoins in 2019 in a wide variety of fiat currencies such as AUD, GBP, HKD and EUR.
- **Paxos has partnered with Ontology** to expand its offerings on different blockchains, in a similar manner as Tether.

These may lead to long-term benefits such as additional channels for global remittance, greater price efficiency for non-USD cryptocurrency exchanges or the development of blockchain FX exchanges, either off or on-chain.

The digital asset industry is seeing wider interest from non-financial institutions and its future may be fueled by these large institutional players creating tradable assets running on public blockchains, hence championing the use of blockchain as the key technology for all digital wallets.

These non-financial companies (e.g. Facebook or Samsung) are likely to be less risk-averse than traditional financial companies, and have greater incentive to disrupt the payments industry, with the added ability to execute at a faster, scalable pace. As a result, these companies may help defining future key growth drivers for both the global payment and the digital asset industry.
Quick insights

@BinanceResearch

Are things starting to look up for Bitcoin?

2 April 2019, the 12th highest single day gain in history at 17.4%

Sources: Binance Research, Blockchain.com

Will KRW traders return to boost the crypto market?

KRW traders were one of the most important forces to dominate the crypto world

Sources: Binance Research, Bitoinity.org
New French law may open up a channel from insurance funds to cryptoassets

Currently, the proportion of alternative assets held by French life insurers is at least 4.2% (Others). Based on this, we estimate that at least 1% of the funds may be allocated to cryptoassets in the future.

AUM of French life and composite insurers: €2.3 trillion


Moving Billions of USD Via Mainnet Swaps

With BNB's mainnet swap coming up on April 23rd, how does BNB weigh up amongst the largest mainnet swaps in history?

Sources: Binance Research, CoinMarketCap

* Yet to complete mainnet swap, value as of April 19th 2019 14:00UTC
May is Historically the 3rd Best Month for Alts

Monthly Change of Total Altcoin Market Cap (excluding stablecoins) Denominated in BTC

<table>
<thead>
<tr>
<th>Year</th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Apr</th>
<th>May</th>
<th>Jun</th>
<th>Jul</th>
<th>Aug</th>
<th>Sep</th>
<th>Oct</th>
<th>Nov</th>
<th>Dec</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019</td>
<td>-6.0%</td>
<td>2.8%</td>
<td>7.1%</td>
<td>-18.8%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2018</td>
<td>27.3%</td>
<td>-17.3%</td>
<td>-25.3%</td>
<td>47.7%</td>
<td>-12.9%</td>
<td>-20.0%</td>
<td>-7.1%</td>
<td>-25.3%</td>
<td>11.1%</td>
<td>-9.5%</td>
<td>6.6%</td>
<td>6.4%</td>
</tr>
<tr>
<td>2017</td>
<td>16.1%</td>
<td>-4.9%</td>
<td>195.3%</td>
<td>34.8%</td>
<td>76.2%</td>
<td>39.6%</td>
<td>-39.2%</td>
<td>25.5%</td>
<td>-12.8%</td>
<td>-30.0%</td>
<td>25.3%</td>
<td>72.3%</td>
</tr>
<tr>
<td>2016</td>
<td>50.6%</td>
<td>31.9%</td>
<td>48.1%</td>
<td>-27.9%</td>
<td>25.0%</td>
<td>-15.5%</td>
<td>22.0%</td>
<td>2.6%</td>
<td>3.6%</td>
<td>-22.5%</td>
<td>-18.3%</td>
<td>-12.2%</td>
</tr>
<tr>
<td>2015</td>
<td>-15.4%</td>
<td>-15.8%</td>
<td>-23.2%</td>
<td>-8.9%</td>
<td>22.8%</td>
<td>23.5%</td>
<td>-14.9%</td>
<td>14.9%</td>
<td>-17.3%</td>
<td>-16.9%</td>
<td>-28.3%</td>
<td>2.3%</td>
</tr>
<tr>
<td>2014</td>
<td>-21.6%</td>
<td>29.6%</td>
<td>-5.4%</td>
<td>-15.9%</td>
<td>-17.8%</td>
<td>-13.3%</td>
<td>-3.8%</td>
<td>27.3%</td>
<td>24.9%</td>
<td>-1.9%</td>
<td>52.5%</td>
<td>79.0%</td>
</tr>
</tbody>
</table>

Average: 8.5%  4.4%  32.7%  1.8%  18.7%  2.8%  -8.6%  9.0%  1.9%  -16.1%  7.5%  29.6%

Positive Months*  50%  50%  50%  33%  60%  40%  20%  80%  60%  0%  60%  80%

*Number of months with positive change / total sample months

Source: Binance Research, Coinmarketcap.com

Is the Market Ready for Institutional Players?
Aggregate Market Depth is Increasing

USD equivalent amount of total trading depth within a ±1% bid and ask price range.

Sources: Binance Research, Investing.com
Another Bullish Divergence?
Total Altcoin market cap in BTC terms has fallen as much as 34% since the beginning of April. But over the past 5 years, this type of divergence has occurred more in bull markets (246 of 300 days).

Sources: Binance Research, Coinmarketcap

It’s Not All About Yields
Despite its perceived riskiness, Bitcoin has a far higher risk-return ratio than most of the traditional assets

Ranking of 2-year returns of multiple asset classes

All returns are calculated in USD terms
Apr 2017 to Apr 2019

Sources: Binance Research, BISB.com
Binance Research provides in-depth analysis and data-driven insights of digital assets and the overall crypto market by generating unbiased, institutional-grade research reports for investors in the crypto space.

—

How to trade with Binance?

- https://binance.com/
- tradesdesk1@binance.com
- @BinanceTrading

—

Don’t miss the latest research!

- https://research.binance.com/
- @BinanceResearch
- @BinanceResearch