The fuel of the blockchain

April 2018

GP Bullhound
Dealmakers in Technology

Important disclosures appear at the back of this report
GP Bullhound LLP is authorised and regulated by the Financial Conduct Authority
GP Bullhound Inc is a member of FINRA

Subscribe to receive GP Bullhound Research and News on www.gpbullhound.com/subscribe/
EXECUTIVE SUMMARY

CRYPTOGRAPHICALLY ENABLED VIRTUAL CURRENCIES – EQUIVALENT TO PIECES OF CODE: CAN THEY CARRY ANY VALUE AT ALL? ARE THEY SECURE? WHILE THESE QUESTIONS ARE CONTROVERSially debated for major cryptocurrencies ("cryptos") like Bitcoin or Ethereum, it becomes a totally unsolvable task when looking at the plethora of altcoins ("cryptos") like Bitcoin or Ethereum, it becomes a totally unsolvable task when looking at the plethora of altcoins.

THE VIEW

From GP Bullhound

Sebastian N. Markowsky

Director

Cryptographically enabled virtual currencies equivalent to pieces of code: Can they carry any value at all? Are they secure? While these questions are controversially debated for major cryptocurrencies ("cryptos") like Bitcoin or Ethereum, it becomes a totally unsolvable task when looking at the plethora of altcoins.

We expect the crypto market to materially mature and the token phenomenon to undergo major changes over the coming months to come, not least driven by regulation. Regardless of the immaturity of the current activities, the ongoing buzz will likely give way to a quantum leap of technological achievements in the distributed ledger technology space.

What began among an evangelist group of academic computer scientists and developers has now captured the attention of media, political, and economic agendas. From these origins, few would have expected blockchain's long-term potential of distributed ledger technologies. From these origins, few would have expected blockchain's long-term potential of distributed ledger technologies.

This has left many strategic and institutional investors wary of the technology. In contrast, the broader strategic applications of blockchain are succeeding. From 2013, as a 19-year-old cryptocurrency researcher and programmer, Buterin created his version of a blockchain-based protocol, which today is one of the largest, most influential distributed ledger technologies.

The first revolutionary use case of the Ethereum protocol, particularly its approach to smart contracts, was the initial coin offering (ICO). The ICO is an entirely new form of fundraising that has transformed the way start-ups can access capital. Being an automated form of crowd funding through blockchain technology, ICOs became an overnight phenomenon, with around USD 4bn raised in 2017 alone.

This momentum appears to be continuing into 2018. Telegram, the Russia-founded instant messaging service, plans to raise USD 1bn through its own ICO this year. As a result of these larger funding rounds, the average ICO is rising every day and investors are becoming more sophisticated on a broader scale, we expect fundraising volumes to rise substantially.

Overall, the market is still immature, and the largest rounds raised by blockchain-focused companies are still far behind of what we see in more mature sectors; even ICO funding cannot compete with the megatrends we see in the biotech, e-commerce, or FinTech sectors. However, the broader technology is still focused on building next generation blockchain protocols, infrastructure projects, and developer tools. Distributed apps appear to be an early area yet to engage.

THE VIEW

From GP Bullhound

From GP Bullhound, we have worked side-by-side with a generation of leading entrepreneurs that have transformed the digital economy worldwide. We are prepared to harness the new technology and financial expertise to enable the scale of a new generation of technology pioneers.
EVOLUTION OF BITCOIN & ALTCOINS
A retrospective of cryptos

Cryptocurrency market capitalisation development and major milestones

- December 2005: Nick Szabo lays out the foundation for Bitcoin by releasing a paper titled ‘Bit Gold’. It outlines some of the concepts that would later be implemented in distributed ledger technology.
- October 2009: Bitcoin whitepaper is published by an unknown author under a pseudonym Satoshi Nakamoto.
- November 2013: Ethereum whitepaper is released. The following year the project commences and in 2015 raises funds through one of the first ICOs ever.
- March 2016: Cabinet of Japan approves a bill recognising virtual currencies as payment method. The country becomes the first major economy to do so.
- Mid-2017 & ongoing: During an unprecedented ‘ICO wave’, blockchain start-ups raise funds in the scale of USD billions. This relatively new form of financing catches the eye of regulators.
- February 2018: After weeks of speculation, China blocks internet access to foreign crypto exchanges, citing ‘financial risks’ associated with crypto trading.
- Ongoing: Regulator scrutiny of ICOs and exchanges regarding KYC and AML compliance continues to grow; the role of non-profit foundations in certain cases remains unclear; types of token and connected rights continue to multiply.

Source: GP Bullhound analysis based on Coinmarketcap and publicly available data as of March 5, 2018.

Current share of total market capitalisation

- Bitcoin: 41%
- Ethereum: 18%
- Ripple: 8%
- Bitcoin Cash: 5%
- Other: 27%
# Blockchain Technology Universe

Overview of selected base protocols and dApps

<table>
<thead>
<tr>
<th>Application Category</th>
<th>Base Layer Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction &amp; payment services</td>
<td>Ethereum</td>
</tr>
<tr>
<td>Ecosystem</td>
<td>WAVES</td>
</tr>
<tr>
<td>Cryptocurrency exchanges &amp; trading platforms</td>
<td>Bitcoin</td>
</tr>
<tr>
<td>Social, games &amp; gambling</td>
<td>NEO</td>
</tr>
<tr>
<td>Identity, authentication &amp; security</td>
<td>Own base protocols</td>
</tr>
<tr>
<td>Enterprise blockchain solutions</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
</tr>
</tbody>
</table>

1. These companies use directed acyclic graphs which is a blockless distributed ledger technology.
2. Not exclusive to Ethereum, based on publicly available information.
3. Scalability layer that can be ported to other blockchains (e.g., Iota.com).
MVPs IN THE BLOCKCHAIN SECTOR
The people behind Bitcoin, Ethereum, etc.
Leading blockchain investors are almost exclusively based in the US. These investors are largely general technology venture capitalists that have shifted their focus towards blockchain technologies.

European blockchain funding is currently experiencing strong momentum due to a large base of top blockchain talent, particularly in Berlin and Zug (Switzerland). Still, most investments into European blockchain companies originate from the US. While there is a vibrant scene of angels and seed investors that have shifted towards crypto investments, only a few funds of meaningful size currently focus on the space.

Asia is also picking up pace quite fast with a number of leading entrepreneurs in the region having realised the potential of blockchain. These investors and supporters often focus on local blockchain projects.

Venture capital funding into blockchain companies, by region

<table>
<thead>
<tr>
<th>Region</th>
<th>Venture Capital Funding (USDm)</th>
<th>CAGR (2015-2017)</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>247</td>
<td>35%</td>
</tr>
<tr>
<td>Europe</td>
<td>152</td>
<td>75%</td>
</tr>
<tr>
<td>Asia</td>
<td>111</td>
<td>57%</td>
</tr>
</tbody>
</table>

Source: Pitchbook and publicly available data.
VENTURE CAPITAL BLOCKCHAIN TARGETS

Venture capital activity remains early stage

- The 10 best funded blockchain companies combined only accumulated USD 1.3bn of venture capital funding between 2014 and 2017


<table>
<thead>
<tr>
<th>Cumulative venture capital funding (USDm)</th>
<th>Selected investors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coindesk</td>
<td>251</td>
</tr>
<tr>
<td>Circle</td>
<td>136</td>
</tr>
<tr>
<td>Kik</td>
<td>121</td>
</tr>
<tr>
<td>Earn</td>
<td>116</td>
</tr>
<tr>
<td>R3</td>
<td>107</td>
</tr>
<tr>
<td>Hyperledger</td>
<td>100</td>
</tr>
<tr>
<td>Ripple</td>
<td>94</td>
</tr>
<tr>
<td>Nxt</td>
<td>90</td>
</tr>
<tr>
<td>Blockman</td>
<td>77</td>
</tr>
</tbody>
</table>

Source: Pitchbook and publicly available data.

MOST ACTIVE INVESTORS

Regional concentration is high

- 9 out of the 10 blockchain investors are based in the US
- Top 10 investors made 13.3% of total investments from 2015-2017

Investors by number of blockchain companies in which they have invested

<table>
<thead>
<tr>
<th>Investors</th>
<th>Number of blockchain companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>45</td>
</tr>
<tr>
<td>Asia</td>
<td>27</td>
</tr>
</tbody>
</table>

Investors with holdings in 6-8 blockchain companies

- Naval Ravikant, Founder of AngelList
- Ben Davenport, Founder of BitGo
- Peter Thiel
- Naval Ravikant
- Peter Thiel
- Naval Ravikant
- Peter Thiel
- Naval Ravikant
- Peter Thiel
- Naval Ravikant

Source: Pitchbook and publicly available data. Note: Includes both past and current investments.
1) Including investments by CEO Barry Silbert. 2) Companies linked to Adam and Timothy Draper (who are father and son).
3) Including investments by Founder & Managing Director Timothy Draper.
ICO FUNDING BOOM

Funding explosion in 2017

For blockchain companies ICO funding outperforms venture capital funding by a factor of 5, while 1 USD of venture capital funding usually translates into over 4 USD of ICO volume when looking at the top 10 ICO rounds.

Total venture capital funding vs. ICO funding (USDm)

ICO vs. venture capital funding volume across categories (2015-2017)

INVESTOR FOCUS

Venture capital vs. ICO preferences

Due to the surge in 2017, ICOs now constitute around ¾ of all funding in blockchain start-ups in 2015-2017.

Projects with the potential to generate traction near term prefer ICO funding. Longer term ecosystem projects are less suited for coin offerings.

Source: Pitchbook, Cryptocompare, Coinmarketcap, ICO Bench, ICO Bazaar, ICO Drops and publicly available data.
Note: Includes disclosed venture capital rounds. Includes ICOs with >1 USDm funds raised and ICO end date between 2015 and 2017.
1) We did not start as blockchain project but raised significant ICO funding. This resulted in a distortion of the data presented.
With the rapid rise of the ICO funding market, the period from venture capital funding to the ICO has shortened significantly. This is partly driven by the fact that venture capital funding typically available for a couple of years of development was completely overtaken by ICOs as a relatively young exit route promising more or less similar exit times.

As shown in the graph, many younger companies pursuing an ICO have completely ignored venture capital funding and started raising money through a private pre-ICO round, followed up by a public ICO. However with the predicted cooldown of the ICO market, we expect to see venture capital funding picking up versus ICOs and periods of venture capital funding before ICOs increasing. Venture capital with a strong understanding and hands-on mentality that can add value to a proposal and its execution will clearly win over crowd investor money.

Equity funding into blockchain is here to stay

With the rapid rise of the ICO funding market, the period from venture capital funding to the ICO has shortened significantly. This is partly driven by the fact that venture capital funding typically available for a couple of years of development was completely overtaken by ICOs as a relatively young exit route promising more or less similar exit times.

As shown in the graph, many younger companies pursuing an ICO have completely ignored venture capital funding and started raising money through a private pre-ICO round, followed up by a public ICO. However with the predicted cooldown of the ICO market, we expect to see venture capital funding picking up versus ICOs and periods of venture capital funding before ICOs increasing. Venture capital with a strong understanding and hands-on mentality that can add value to a proposal and its execution will clearly win over crowd investor money.

**Return of Venture Capital**

Equity funding into blockchain is here to stay

With the rapid rise of the ICO funding market, the period from venture capital funding to the ICO has shortened significantly. This is partly driven by the fact that venture capital funding typically available for a couple of years of development was completely overtaken by ICOs as a relatively young exit route promising more or less similar exit times.

As shown in the graph, many younger companies pursuing an ICO have completely ignored venture capital funding and started raising money through a private pre-ICO round, followed up by a public ICO. However with the predicted cooldown of the ICO market, we expect to see venture capital funding picking up versus ICOs and periods of venture capital funding before ICOs increasing. Venture capital with a strong understanding and hands-on mentality that can add value to a proposal and its execution will clearly win over crowd investor money.

**Investor Influence**

ICO performance is driven by reputation

> Investments by major blockchain investors and post-ICO trading performance are positively correlated

> Engagement of a reputable investor in a project appears to be a key determinant for success. It remains to be seen if contributions of reputable investors improve projects or merely serve as a key orientation for ICO investors

> Long-term post ICO performance will likely reveal more details on the question whether reputable investors increase the probability of long-term success

**Number of years of venture capital funding prior to ICO vs. year founded**

- Horizontal axis denotes founding year
- Vertical axis denotes time period between year founded and the ICO financing round
- Bubble size denotes number of companies/projects for a given founding year and time period

Source: Pitchbook, Cryptocompare, Coinmarketcap, ICO Benchmark, ICO Bazaar, ICO Drops and publicly available data.

Note: Includes disclosed venture capital rounds. Includes ICOs with >1 USDm funds raised and ICO end date between 2015 and 2017.

**Investor Influence**

ICO performance is driven by reputation

> Investments by major blockchain investors and post-ICO trading performance are positively correlated

> Engagement of a reputable investor in a project appears to be a key determinant for success. It remains to be seen if contributions of reputable investors improve projects or merely serve as a key orientation for ICO investors

> Long-term post ICO performance will likely reveal more details on the question whether reputable investors increase the probability of long-term success

**Number of years of venture capital funding prior to ICO vs. year founded**

- Horizontal axis denotes founding year
- Vertical axis denotes time period between year founded and the ICO financing round
- Bubble size denotes number of companies/projects for a given founding year and time period

Source: Pitchbook, Cryptocompare, Coinmarketcap, ICO Benchmark, ICO Bazaar, ICO Drops and publicly available data.

Note: Includes disclosed venture capital rounds. Includes ICOs with >1 USDm funds raised and ICO end date between 2015 and 2017.

**Investor Influence**

ICO performance is driven by reputation

> Investments by major blockchain investors and post-ICO trading performance are positively correlated

> Engagement of a reputable investor in a project appears to be a key determinant for success. It remains to be seen if contributions of reputable investors improve projects or merely serve as a key orientation for ICO investors

> Long-term post ICO performance will likely reveal more details on the question whether reputable investors increase the probability of long-term success

**Number of years of venture capital funding prior to ICO vs. year founded**

- Horizontal axis denotes founding year
- Vertical axis denotes time period between year founded and the ICO financing round
- Bubble size denotes number of companies/projects for a given founding year and time period

Source: Pitchbook, Cryptocompare, Coinmarketcap, ICO Benchmark, ICO Bazaar, ICO Drops and publicly available data.

Note: Includes disclosed venture capital rounds. Includes ICOs with >1 USDm funds raised and ICO end date between 2015 and 2017.

**Investor Influence**

ICO performance is driven by reputation

> Investments by major blockchain investors and post-ICO trading performance are positively correlated

> Engagement of a reputable investor in a project appears to be a key determinant for success. It remains to be seen if contributions of reputable investors improve projects or merely serve as a key orientation for ICO investors

> Long-term post ICO performance will likely reveal more details on the question whether reputable investors increase the probability of long-term success

**Number of years of venture capital funding prior to ICO vs. year founded**

- Horizontal axis denotes founding year
- Vertical axis denotes time period between year founded and the ICO financing round
- Bubble size denotes number of companies/projects for a given founding year and time period

Source: Pitchbook, Cryptocompare, Coinmarketcap, ICO Benchmark, ICO Bazaar, ICO Drops and publicly available data.

Note: Includes disclosed venture capital rounds. Includes ICOs with >1 USDm funds raised and ICO end date between 2015 and 2017.

**Investor Influence**

ICO performance is driven by reputation

> Investments by major blockchain investors and post-ICO trading performance are positively correlated

> Engagement of a reputable investor in a project appears to be a key determinant for success. It remains to be seen if contributions of reputable investors improve projects or merely serve as a key orientation for ICO investors

> Long-term post ICO performance will likely reveal more details on the question whether reputable investors increase the probability of long-term success

**Number of years of venture capital funding prior to ICO vs. year founded**

- Horizontal axis denotes founding year
- Vertical axis denotes time period between year founded and the ICO financing round
- Bubble size denotes number of companies/projects for a given founding year and time period

Source: Pitchbook, Cryptocompare, Coinmarketcap, ICO Benchmark, ICO Bazaar, ICO Drops and publicly available data.

Note: Includes disclosed venture capital rounds. Includes ICOs with >1 USDm funds raised and ICO end date between 2015 and 2017.

**Investor Influence**

ICO performance is driven by reputation

> Investments by major blockchain investors and post-ICO trading performance are positively correlated

> Engagement of a reputable investor in a project appears to be a key determinant for success. It remains to be seen if contributions of reputable investors improve projects or merely serve as a key orientation for ICO investors

> Long-term post ICO performance will likely reveal more details on the question whether reputable investors increase the probability of long-term success

**Number of years of venture capital funding prior to ICO vs. year founded**

- Horizontal axis denotes founding year
- Vertical axis denotes time period between year founded and the ICO financing round
- Bubble size denotes number of companies/projects for a given founding year and time period

Source: Pitchbook, Cryptocompare, Coinmarketcap, ICO Benchmark, ICO Bazaar, ICO Drops and publicly available data.

Note: Includes disclosed venture capital rounds. Includes ICOs with >1 USDm funds raised and ICO end date between 2015 and 2017.

**Investor Influence**

ICO performance is driven by reputation

> Investments by major blockchain investors and post-ICO trading performance are positively correlated

> Engagement of a reputable investor in a project appears to be a key determinant for success. It remains to be seen if contributions of reputable investors improve projects or merely serve as a key orientation for ICO investors

> Long-term post ICO performance will likely reveal more details on the question whether reputable investors increase the probability of long-term success

**Number of years of venture capital funding prior to ICO vs. year founded**

- Horizontal axis denotes founding year
- Vertical axis denotes time period between year founded and the ICO financing round
- Bubble size denotes number of companies/projects for a given founding year and time period

Source: Pitchbook, Cryptocompare, Coinmarketcap, ICO Benchmark, ICO Bazaar, ICO Drops and publicly available data.

Note: Includes disclosed venture capital rounds. Includes ICOs with >1 USDm funds raised and ICO end date between 2015 and 2017.
After peaking in October 2017, the ICO market has cooled down.

In Q3 & Q4 2017 there was a large number of smaller, less successful ICOs.

Many projects conducting an ICO specify soft and hard caps in their whitepaper. The former indicates the minimum amount of funds required to pursue the project. Should this threshold not be reached, all funds invested in the project are returned. The latter represents the upper boundary of funds required for the project. Funds in excess of this figure are returned.

The chart below examines trading performance in relation to funds raised as a fraction of communicated hard cap. The bar to the right shows the performance of projects that reached or exceeded their funding goals. It should be noted that not all ICOs specify funding caps, essentially “taking all they can get”. The largest ICO in 2017, Tezos, collected USD 232m without specifying the amount of funds the project would require.

Reaching (or in some cases exceeding) the funding cap is positively linked to trading performance. Projects that reached less than 50% of their funding goal underperformed on average. In contrast, projects that exceeded their pre-specified fund requirements were able to more than double the quote of their token 60 days after their ICO.

Average 60-day performance by % of funding cap reached:

- 0-49%: 75 ICOs, average multiple: 0.7x
- 50-99%: 41 ICOs, average multiple: 1.8x
- >100%: 48 ICOs, average multiple: 2.3x

Source: Cryptocompare, Coinmarketcap, ICO Bench, ICO Bazaar, ICO Drops and publicly available data. Note: Includes ICOs with specified hard cap, >1 USDm funds raised and ICO end date between 2015 and 2017. 1) All-day multiple of ICO price (adjusted for ETH price development, ICO volume weighted). Performance multiples only include ICOs with available 60-day trading data. Data as of March 5, 2018.
# LEADING PROTOCOLS & blockchain ecosystems

---

## KEY BASE PROTOCOLS

Who dominates the market?

<table>
<thead>
<tr>
<th>Protocol</th>
<th># of ICOs to date</th>
<th>ICO volume (USD)</th>
<th>Maternity of platform (year of release)</th>
<th>Market cap ratio</th>
<th>Market cap share</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethereum</td>
<td>201</td>
<td>3,213m</td>
<td>3 (2015)</td>
<td>21.2%</td>
<td>18.1%</td>
</tr>
<tr>
<td>Waves</td>
<td>14</td>
<td>63m</td>
<td>2 (2016)</td>
<td>17.2%</td>
<td>&lt;0.1%</td>
</tr>
<tr>
<td>Bitcoin</td>
<td>4</td>
<td>27m</td>
<td>9 (2009)</td>
<td>1.0%</td>
<td>41.4%</td>
</tr>
<tr>
<td>NEO</td>
<td>3</td>
<td>38m</td>
<td>3 (2015)</td>
<td>1.8%</td>
<td>0.02%</td>
</tr>
</tbody>
</table>

Source: GP Bullhound analysis based on Pitchbook, Cryptocompare, Coinmarketcap, ICO Bench, ICO Bazaar, ICO Drops and publicly available data.

Note: Includes ICOs with >1 USD$m funds raised and ICO end date between 2015 and 2017. 1) Defined as (market cap of ICO companies on base protocol) / (market capitalisation of base protocol). Data as of 5 March 2018. 2) Market share as of total market capitalisation.
CHAPTER 3

Chapter 3

SETTLING THE PACE for blockchain developers

Joseph Lubin
Co-founder Ethereum & Founder ConsenSys

We have reached a turning point. Technology has significantly advanced our civilization; and yet, over the last few decades, certain institutions have lost the trust of vast swathes of the population. As a result, there is a lot of people who believe in the philosophy of trust and decentralization – this is the fundamental principle behind the blockchain.

ConsenSys is a global organization that specializes in developing blockchain software – primarily within the Ethereum ecosystem – for institutions, corporations, and governments. It also dedicates a lot of time towards building the infrastructure of the public Ethereum ecosystem, ensuring that it can process around 10,000 requests per day.

Ethereum has set itself apart from other blockchain platforms as far more expressive and accessible. If you can build a web or mobile application then you can build applications on top of Ethereum instead of needing to build and maintain their own blockchain.

This growth has, of course, created some challenges. Ethereum was built primarily as an elegant solution to creating a blockchain protocol that reflected fundamental principles of trust, privacy and confidentiality. While most developers have spent the last three decades attempting to build a global infrastructure, we instead focused on harnessing cryptographic techniques that protected our basic ethos but did not operate at scale.

One of our key objectives over the coming months will therefore be building scalability back into our infrastructure. There are solutions already being developed – sharing, for one, provides a potential solution to the problem of scalability. Similarly, I believe that 2018 will see substantial strides made in the development of an internet that operates between different blockchain systems – this will also enable the Ethereum protocol to scale.

One analyst estimated that the number of developers working on the Ethereum protocol is 30 times larger than its closest competitor, the IBM-backed Hyperledger fabric. We have strived to retain Ethereum’s founding principles of friendliness and cooperation as it has grown. This focus has ensured that we have maintained the diversity of people operating on Ethereum, meaning governance and leadership in this community do not rely on one single person, but thrive on the collective input of different classes of actors.

As a result, the only metric I truly pay attention to is the number of developers operating in the Ethereum ecosystem. Certainly, ConsenSys has expanded substantially over the past couple of years and we now have around 700 employees spanning 28 countries around the world. Likewise, the rise in monetary value of Ether – the cryptocurrency closely associated with the Ethereum protocol – has added value to the ecosystem and drawn the attention of developers, entrepreneurs, and investors, all of which are vital to our future success.

WHY ETHEREUM?

Explanations for its dominance

1. Relative ease-of-use

Ethereum offers the easy-to-use scripting language Solidity and, amongst others, the ERC20 token standard which allows developers to build decentralized applications on top of Ethereum instead of needing to build and maintain their own blockchain.

2. Strong community

Ethereum enjoys broad acceptance in the community and can arguably be described as the standard protocol for decentralized applications. Strong supporters like ConsenSys or the Enterprise Ethereum Alliance further drive the momentum.

3. Better performance metrics

Ethereum offers some of the best block time/speed ratios in the market (currently below 15 seconds) and is the first offering these advancements in performance.

4. Addressed scams

The aim of Ethereum is 50,000 transactions per second with no loss of decentralization.

5. Clear vision, leadership and credibility

While founders and key developers of Ethereum might deny the leadership aspect of their position, they’ve managed to act coherently and consistently over time offering a promise of long-term security through multiple independent development teams and preference of algorithmic governance.
KEY CHALLENGES TO BE SOLVED

Addressing these topics will help enable mass adoption

- BLOCKCHAIN SCALABILITY
- DECENTRALISATION OF EXCHANGES
- STAYING PRIVATE
- EFFECTIVE GOVERNANCE
- CONSENSUS EFFICIENCY
CHAPTER 4

1) Scalability initiatives by the Ethereum foundation.
Source: GP Bullhound analysis based on Etherscan and proprietary data.

Different aspects are tied to the scalability issue. Improvements in one area negatively affect others.

**MAJOR SCALING CONCEPTS**

**Multi-chain scaling**
The shared database is split into several parts, lowering the amount of data each single node has to store.

**Off-chain scaling**
Transactions are regularly done off-chain. The blockchain is only used to settle disputes, significantly lowering the load.

**THE ETH ECO SYSTEM – AN OVERVIEW**

The ecosystem that we have today began with the development of public blockchain technologies and the production of cryptocurrencies. Public blockchains face challenges, but fundamentally have far more potential than private blockchain networks.

The public blockchain ecosystem has been forced to address significant technological challenges. First is the problem of scale: on-chain scaling – the process of increasing the capacity of a network through amendments to the blockchain itself - a technically complex issue for developers. Off-chain transactions offer a simpler solution to create capacity, through harnessing something other than the blockchain to scale, such as virtual payments. Yet, this undermines the basic premise of using blockchain for trust and decentralization.

My research group is at the forefront of both on-chain and off-chain scaling. I think on-chain scaling is critical to the future of blockchain – anybody who attempts to bypass it is not operating with the correct principles. If you see this playing out with Bitcoin, Amy Tom, Dick or Harry will tell you about the lightning network, a payment protocol that operates on top of Bitcoin. While Tom, Dick, and Harry may be telling us to engage in the network and create payments channels, I have never seen a mathematical proof for its vision and my gut feeling is that this is nothing more than a pipe dream.

A greater risk still is the existence of unsecured, potentially fraudulent protocols. As we speak, the Tether cryptocurrency is going through an investigation by the US commodity futures trading commission. If Tether goes down, it will take down multiple exchanges and the price of Bitcoin will plummet. Likewise, there are many, many pitfalls in the distributed systems that we have been building. History is littered with badly designed systems, and while we continue to develop with gut feelings, we will face fundamental system failures.

The ambition to create an entirely secure ecosystem has similarly created challenges for the public blockchain community. We can rely upon the ecosystem itself to be secure, but the endpoints of the network - the interface for everyday users - can remain insecure. We may spend decades waiting for these to become secure, so developers have created coins that have an in-built system to protect users.

Private institutions have attempted to bypass these technical difficulties through creating closed networks and using ‘permissioned launching’. Permissioned launching started with the notion of an industry approaching the field and saying: "Looking at blockchain, there are several features of the technology that we would like to cherry pick, so long as we can disregard the difficult parts."

As a result, these industries are breaking the technology and harnessing private networks of ‘validation’ – machines that are tasked with keeping track of the blockchain. This is not how the technology should work. While it may appear to remove the need for a single central authority, the fact that the data is smeared across five or ten or twenty people does not make me sleep any easier at night.

Yet, there are countless businesses now creating deployments of permissioned launching. I do not expect them to be used for mission-critical applications, but there will be plenty of applications that are far from mission-critical. The Whoppercoin that Burger King developed for example - essentially a vehicle for customer loyalty points. This is a perfect example of blockchain without purpose: it simply does not matter what happens to the data, so why is it on the blockchain?

More promising progress is being made developing hybrid architectures that combine a public and private blockchain infrastructure. In these hybrid systems, you create a chain that is subject to the public blockchain, then move onto a private blockchain before reverting back to the public blockchain. For instance, a government may want to record votes on a public blockchain, tally these votes on a private blockchain before reverting back to the public blockchain. It will take a very diverse and broad range of operators to successfully deploy blockchain at scale. This is why we have established the Initiative for Cryptocurrency and Smart Contracts – we are harnessing the diverse approaches of around fifteen professors and about forty to sixty PhD students, to carry out groundbreaking research and build blockchain technology that lasts.
Chapter 4

Decentralisation of Exchanges

Solving the issues in cryptotrading

Centralised structures undermine the ground principles of blockchain

» Future changes to protocol
» Tech flaws
» STATUS QUO
» CHALLENGES TO BE SOLVED
» CENTRALISED
» HYBRID
» DECENTRALISED

Blockchain relevance

Number of crypto coins and tokens
As of March 5, 2018
1,522 different tokens

.STATUS QUO.

As of March 5, 2018
1,522 different tokens
USD 470.5bn

Total market cap

<table>
<thead>
<tr>
<th>Year</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>66</td>
<td>506</td>
<td>562</td>
<td>644</td>
<td>1,335</td>
</tr>
</tbody>
</table>

1,335

Solving the issues in cryptotrading

Challenges to be solved

- Liquidity
- Key storage
- Cross-chain transactions
- KYC / AML / CFT
- Fiat limitations

Unclear trading

 Miner front-running
 Off-chain order manipulation

Other

Blockchain in today's financial world is facing several hurdles. While it has demonstrated an exceptional theoretical potential, it has yet to break into mainstream adoption. This is largely due to the fact that the technology is struggling to develop at a scale with simple user cases.

The magnitude of development of viable user cases is inversely proportional to how difficult it is for developers to build projects on blockchain protocols. When working on blockchain becomes easier, more projects are conceived, more entrepreneurs enter the field and more likely it will get for feasible relevant user cases to evolve. However, a lot of projects in the space right now are focusing not on end users, but rather on the protocol itself. These are teams, often with academic backgrounds, that have raised funds with what they are using for research, concept development and other pre-alpha activities. Many of these teams have a very loose approach to the practical aspects of their projects and will certainly fail to break into the mainstream.

On the other hand, it is yet difficult to build blockchain-based applications comparable with their traditional counterparts for several reasons mostly related to the underlying basic protocols limited throughput, transaction costs and so on. Also currently, individual protocols operate in isolation and while they could offer a lot of exciting functionality, they do not interoperate with one another. This leads to applications built on siloed protocols becoming too expensive to use compared to "traditional" entangled solutions available.

This is the issue Polkadot – being one of the Web3 Foundation’s most prominent projects – tackles. Started about a year ago, Polkadot is a protocol that is guided by a mission to enable faster interactions throughout the blockchain ecosystem and make use cases easier to bring into life. Polkadot seeks to create a network of interoperable blockchains, where a single project or application could benefit from advantages of different protocols. It does this through a relay chain, which communicates and continues consensus across the entire network, individual parachains – public or private blockchains that make up the constituent parts of the overall network – and bridges that link to blockchains with their own consensus, such as Ethereum.

All this eventually plays a part of a greater, more complex challenge that the blockchain technology is facing: scalability. The market has yet to solve the problem of limited blockchain throughput (comparatively low number of transactions processed). The industry needs to have concrete roadmaps to address the topic efficiently. While there are several teams working on the issue right now -

Polkadot enabling a network of blockchains, Ethereum sharding, off-chain solutions, etc. - what we’ll eventually need is a combination of all these approaches. Currently, it looks like splitting the blockchain validation between the nodes is the way to go forward. However, do you guarantee that the validation is accurate?

The problem of blockchain scaling goes hand-in-hand with a trade-off between transaction complexity and transaction security. The complexity might naturally vary from one protocol to another. The Ethereum protocol is an rigorous contract-based system, while other blockchains are simpler value transfers. The security is a burden, closely tied with usability: how long am I, as a user ready to wait to ensure that the transaction was executed smoothly AND in a secure manner?

Today, each blockchain requires a separate security community. For instance, Bitcoin and Ethereum have a community of miners that provide computational power to verify transactions and ensure the security of the ecosystem. However, these communities are self-serving. If I want to establish a new blockchain, whether public or private, I need to persuade enough people to join the ecosystem, maintain it and verify transactions.

Relay chains of Polkadot create a network of pooled security through tying different blockchain ecosystems into one. This makes it possible to deploy a new blockchain which is secured not only by my own small community of maintainers, but the entire Polkadot network. This radically transforms the challenge of scalability through guaranteeing security throughout a global network of distinct blockchains.

There is every likelihood that the Polkadot network could become the fabric that interconnects all the pieces of the ecosystem, while providing the needed security. And we do believe that connected decentralised systems are the future of the Internet.

This is why the Web3 Foundation aims at helping young initiatives in the decentralised software space by educating and nurturing them towards a clear future development. We need widespread education both within the industry to move it forward, as well as outside of it – to make it more lucrative for the traditional developers to join the booming market.

We strongly believe that through the combination of educational and tech projects, we will be able to unlock blockchain’s full potential – and bring us to the future where trustless, serverless and fully decentralised web is a reality.

Interoperability

Polkadot contributor & CEO Web3 Foundation
A blockchain is a public database of transactions and therefore not private by definition, since validators on the blockchain need to be able to verify these transactions. At the same time, the connection between a blockchain address and the person or organisation behind it is often missing. General Data Protection Regulation ("GDPR") becoming effective in May 2018 will pose some key challenges to the entire blockchain space.

**PRIVACY SOLUTIONS**

**Encryption will be key**

MacLane Wilkison
Founder NuCypher

Blockchain has a privacy problem. On the one hand, the concept of creating a private network with hidden data or transactions conflicts with the technology's founding principles of openness, trust, and decentralisation. On the other hand, we believe privacy will prove critical to the ability of blockchain technologies to achieve widespread adoption and scale.

We founded NuCypher to begin addressing this problem. We have focused primarily on the issue of data privacy. By default, the data that is created on distributed ledgers is public, particularly when using the Ethereum protocol. However, many of the projects harnessing these protocols have developed decentralised applications that are working with sensitive data that needs to remain private.

For instance, a healthcare provider might be looking to create a decentralised method of storing patient records. The provider will be seeking to benefit from the security and efficiency of a distributed ledger. Yet, the records that it is storing must be private, confidential, and encrypted. NuCypher provides a platform for harnessing the public blockchain with privacy.

The issue of privacy of transactions in a blockchain ecosystem has recently given rise to a number of cryptocurrencies focused on providing anonymity and inscrutability. These "privacy coins", such as Monero, Dash, and Zcash, offer a vehicle to keep the personal information of users hidden during transactions. However, there is an obvious concern that this anonymity will simply be used to obscure criminal activity and it is certainly the case that a lot of their current usage is for transactions on the black market.

As a result of this concern, there has been some discussion of building back-doors into the currencies to allow certain parties, such as a regulator or auditor, to not be in the loop. These kind of services are offered by some players as standalone services or additional layers to existing protocols.

Privacy coins provide a strong offering for concealing transactions. However, extending these privacy tools to other data stored on the blockchain and being able to securely share it with other entities in the network, such as regulators or auditors, is not in their scope. These kind of services are offered by some players as standalone services or additional layers to existing protocols.

If there was to be some regulation of privacy coins, it would be a non-technical solution as attempting to adapt the protocol is more or less impossible. In order to maintain the mathematical or cryptogrophic integrity of transactions, you could introduce “know your customer” checks, and traditional financial services. These checks are used to ensure that banks know and verify the identity of their consumers. In blockchain, this would mean that vendors or exchanges would have a duty to know their customers.

In the future, NuCypher could plug into this process to create a central order book for vendors and exchanges that is encrypted to the public but accessible by an approved list of users. While this is a potential use case, we do not currently have anyone using our solution in this way. For now, we are largely focused on providing our users with a way to store private data on public blockchain protocols.

We have been fortunate to work with supportive, insightful, and influential investors, from specialist funds like Polychain Capital and FBG Capital to traditional groups such as Base Ventures and Y Combinator. As with any tech company, these investors support our growth strategy, refer potential hires, and help us with our legal frameworks. One area that has required more specialist support, however, is our upcoming token sale.

The majority of token sales currently taking place are simply vehicles to raise capital quickly. If you are seriously trying to build a sustainable protocol with a sustainable network, you need to think carefully about how you actually want to distribute those tokens – who should have them, how many should each person have – the foundations of crypto-economic’s. These are technical hurdles that have required more specialist support, however, it is our upcoming token sale.

Our token sale is a serious commitment to creating blockchain technologies with genuine strategic value for our users. The future success of the blockchain will rest on its ability to deliver a trusted solution, whether private or public, to developers and enterprises around the world.
There are many types of coins and tokens in the market which differ in rights granted to token holders. Within the respective groups, differences in entity structure and jurisdiction must be taken into account.

**CURRENT LACK OF COMMON STANDARDS IMPEDES TRANSPARENCY**

Information in whitepapers is usually insufficient for proper assessments.

**STAGE-EXPLAINED COMMUNICATION STANDARDS**

The current lack of common standards impedes transparency — information in whitepapers is usually insufficient for proper assessments.

**PARTICIPATION IN DECISION-MAKING**

Token holders currently have no rights to participate in corporate decisions.

**MANAGEMENT SUPERVISION**

No influence on personnel set-up of entities by token holders.

**GOVERNANCE TECHNOLOGY**

Aragon

Bordroom

Dfinity

Decred

Kleros

**GOVERNANCE FOCUSED PROTOCOLS**

Aragon

Bordroom

Dfinity

Decred

Kleros

Source: GP Bullhound analysis based on proprietary data.

**NAVIGATING TOKEN TYPES**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Analogy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currency Tokens</td>
<td>Currency serving as medium of exchange and/or store of value</td>
<td>Fiat currencies</td>
</tr>
<tr>
<td>Asset Tokens</td>
<td>Tokenised shares, debt or other investment contracts on the blockchain, allowing issuers to forego regulated financial markets</td>
<td>Financial instruments</td>
</tr>
<tr>
<td>Utility Tokens</td>
<td>Exchange medium within the crypto-economy of specific projects</td>
<td>Prepaid software/service fees</td>
</tr>
</tbody>
</table>

**FORESEEABLE TOPICS**

- Governance is the lifeblood of blockchain. This is not simply a technology, but a movement founded upon the principle of creating the means to decentralise power and give it back to the people through technology.
- At Aragon, we seek to provide the tools to empower people across the world to easily and securely manage the structure of communities and organisations. We have begun to see progress made towards creating these decentralised structures. In Malta, the government has begun to enable people to run legal cryptocurrency projects and exchanges, while, in Switzerland, lawmakers are integrating decentralised systems into existing practices. As a result, there is evidence that decentralised structures, representative of the same legal structure that a body, corporation, or government already had, can be implemented. This evidence suggests that we are moving to a future where there are simply decentralised digital structures, but we are not there yet.

**GOVERNANCE FOCUSED PROTOCOLS**

- Santiment’s Project Transparency has begun to build a system for its community to safely and securely trade cryptocurrencies, while MakerDAO has been setting an excellent example of creating a stable, transparent digital currency.
- Through the Aragon community, we have also sought to build a transparent network from the ground up. From the outset, we focused on our own community governance model, laying out the ways in which we would incorporate the community in the decision-making.

**SOURCE**

- Tatu Kärki
  Communications Lead, Aragon

**BLOCK CHAIN GOVERNANCE**

**DAO and more**

Governance is the lifeblood of blockchain. This is not simply a technology, but a movement founded upon the principle of creating the means to decentralise power and give it back to the people through technology.

At Aragon, we seek to provide the tools to empower people across the world to easily and securely manage the structure of communities and organisations. We have begun to see progress made towards creating these decentralised structures. In Malta, the government has begun to enable people to run legal cryptocurrency projects and exchanges, while, in Switzerland, lawmakers are integrating decentralised systems into existing practices. As a result, there is evidence that decentralised structures, representative of the same legal structure that a body, corporation, or government already had, can be implemented. This evidence suggests that we are moving to a future where there are simply decentralised digital structures, but we are not there yet.

I believe that a critical barrier to the widespread adoption of blockchain technology is solving the issue of the potential for volatility and instability. In our own community of governance, the memory of the hacking of the DAO has meant that the word DAO has become a taboo. Meanwhile, everyday users have a persistent and real fear of losing their money in cryptocurrencies. Visa’s choice to end its relationship with WaveCrest, a card provider associated with crypto-wallets, left thousands of people out of pocket.

To remedy this volatility, we must begin to instil greater transparency into the blockchain ecosystem. The failure of the DAO came as a result of someone developing a token sale where the code left an entry point that obscured a backdoor allowed to extract funds. Only experts with substantial technical knowledge might have had any chance of spotting this backdoor. People simply did not have the time or ability to fully evaluate the nuances of the network, which led to someone being able to take the money and run.

There are, however, projects that are doing a lot of good work to create fully transparent blockchain technologies. Settlement’s Project Transparency has begun to build a system for its community to safely and securely trade cryptocurrencies, while MakerDAO has been setting an excellent example of creating a stable, transparent digital currency.

This begins with setting out the code base on a public open source and continues through monthly meetings on online forums and live streams. We also produce quarterly reports that outline how we have used our funds. Underpinning this all, we have our transparency framework – a transparency code that allows anyone to view transactions that have been taking place in our network.

Providing the community with this information helps them to make better decisions and moves us towards a system where the network has the power. Ultimately, we will move to a point where we cannot control the actions of users on the network. However, we will have sustained the true lifeblood of the blockchain — governance.
CONSENSUS EFFICIENCY
Overdue transition to Proof of Stake

STATUS QUO

<table>
<thead>
<tr>
<th>Proof of Work</th>
<th>Proof of Stake</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description &amp; functionality</strong></td>
<td>Major protocols, including the Bitcoin blockchain, operate under PoW. Switching public protocols from PoW to PoS is complex due to the major changes in code required.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>If a single party provides the majority of all mining power it can effectively &quot;take control&quot; of the entire blockchain in what is called a 51% attack. This becomes a relevant threat in the presence of centralised mining pools.</td>
</tr>
<tr>
<td><strong>Transaction cost</strong></td>
<td>HIGH</td>
</tr>
<tr>
<td><strong>Validation speed</strong></td>
<td>LOW</td>
</tr>
</tbody>
</table>

OUTLOOK

Final remarks

KEY TOPICS

- PoS is a central component in many efforts to improve scalability.
- Major protocol changes on running blockchains, such as transitioning to a new consensus mechanism, are difficult to implement and bear risks.
- Final implementation of PoW to PoS on large scale protocol is still outstanding. Ethereum is currently testing Casper (PoS mechanism) in some shards of its blockchain.
- Miners in PoW-based ecosystems are likely to oppose transitions to PoS. For Ethereum, this might lead to further hard forks.

Source: GP Bullhound analysis based on proprietary data.
THE YEAR IN BLOCKCHAIN

GP Bullhound Outlook

1. ICO funding is here to stay but it will mature significantly and rapidly

No longer will companies be able to launch an ICO off the back of a whitepaper. Exceptions confirm the rule where the stage of the company or product will be largely meaningless versus the size of the ICO itself. We expect to see several giant ICOs far beyond Telegram’s USD 2bn round by April 2019. Key for success will be execution track record, transparency and credibility of founders. Elon Musk would qualify for such a raise.

2. No next-generation beast protocol in sight

People will become more cautious towards second generation protocols. Aspirational upstarts such as Dfinity, RChain, Cardano and Tezos will have to do much more than simply technically outperform to win market share. They will, however, keep the pressure on Ethereum to implement long overdue changes. Ethereum will keep its position as the clear leader and become the most valuable cryptocurrency by market cap.

3. 2018 will see a number of important hard forks and first attempts at M&A activity

The mechanisms around forking will mature significantly including activities that resemble “hostile takeovers” and “activist hedge funds”. In the wake of early M&A deals in the 1980s, protocol ecosystems will likely develop by means of hard forks together with friendly investor support, raising stakeholder awareness, leveraging developer talent and smart airdrop strategies. Since the code is public, potential counter measures within the code are entirely transparent.

4. The next killer app

After the ICO as the first killer app in 2017, 2018 will be defined by asset tokens or tokenization of assets (“TOA”) offerings, also strongly driving the adoption of Ethereum for financial applications. This will cause the cryptocurrency market to spike up sharply and peak at a total market cap far beyond USD 1 trillion and the volume of tokenized assets will exceed ICO volumes of 2018. At the same time, non-fungible tokens will conquer the blockchain and create the first use cases capable of driving mass consumer adoption.

5. 2018 will see airdrops become new normal for token distribution

2018 will see widespread usage of token airdrops. Since token issuing should be seen as the means to create network effects, a sale of tokens with no utility value seems unsustainable. An airdrop may be a preferable option to include current and future stakeholders and maximize network effects. 2018 efforts will aim to ensure the best possible distribution and allocation, since early airdrop models show an ability to create immediate impact and exceptional growth stories.

6. 2018 will see the first corporate ICO

We define corporate ICO as the transition of a formerly private and permissioned chain onto a public blockchain. This ICO will also likely be the first ICO based upon a consortium chain which will see several corporates join forces in a private, permissioned blockchain before setting the protocol free for the wider universe of early adopters. The automotive, raw materials or luxury goods sector might be the most likely industries driving such a project.

7. Smart money will keep dominating blockchain

Venture capital is not going anywhere. However, we believe that there needs to be a paradigm shift: the industry must aspire to a more inclusive and idealistic form of VC investing that supports founders with the knowledge and expertise to execute successful distributed ledger technologies. Average equity funding pre-ICO will rise to over USD 20m for successful ICOs in 2018.

8. Mass market wipe out

Finally, cryptocurrencies will experience a heavy correction of up to 90 per cent in the next 12 months and very few companies will survive this correction. While this correction will be decisive in cutting through the hype, its lack of impact on financial institutions will create new phenomena that we have never seen in any previous bubble burst. Nonetheless, once this “crypto-winter” passes, the growth dynamics for the precious few survivors will be unprecedented.
## Creating the Internet of Value

### Applications for blockchain

### Evolution of Functionalities of the Internet

<table>
<thead>
<tr>
<th>Internet of Information</th>
<th>Internet of Things</th>
<th>Internet of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange of information (based on Internet protocol)</td>
<td>Connectivity of devices (based on specific protocols)</td>
<td>Creation of digital assets (based on blockchain protocols)</td>
</tr>
</tbody>
</table>

**Key issues where distributed ledger technologies add value**

- Need for decentralisation
- Need for transparency
- Need for immutability
- Need for viable smart contract functionality

### Selected Near-Term Use Cases & Comparable Market

<table>
<thead>
<tr>
<th><strong>Fungible Token Use Cases</strong></th>
<th><strong>Non-Fungible Token Use Cases</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fundraising</strong>&lt;br&gt;Token distribution through ICOs as an independent means of raising funds</td>
<td><strong>Collectibles</strong>&lt;br&gt;Unique digital assets with intrinsic value properties (e.g. sports cards, cryptokitties, etc.)&lt;br&gt;&lt;br&gt;<strong>Ownership record</strong>&lt;br&gt;Tokens as ownership record for specific assets (e.g. real estate, luxury goods, cars)&lt;br&gt;&lt;br&gt;<strong>Identity record</strong>&lt;br&gt;Personal records and identifying data, verifiable through unique tokens</td>
</tr>
<tr>
<td><strong>Tokenisation of assets</strong>&lt;br&gt;Tokens backed by real assets (debt, real estate, commodities, art, etc.)&lt;br&gt;&lt;br&gt;<strong>Exchanges</strong>&lt;br&gt;Decentralised trading and settlement of tokens and tokenised assets</td>
<td><strong>USD 868bn</strong>&lt;br&gt;Global venture capital funding (2017)&lt;br&gt;&lt;br&gt;<strong>USD 200bn</strong>&lt;br&gt;Annual spend on collectibles (2016, global)&lt;br&gt;&lt;br&gt;<strong>USD 800bn</strong>&lt;br&gt;Global structured products issuance (2017 est.)&lt;br&gt;&lt;br&gt;<strong>USD 660bn</strong>&lt;br&gt;Real estate transactions (2016, global)</td>
</tr>
<tr>
<td><strong>Exchanges</strong>&lt;br&gt;Global stock trading volume (2016)</td>
<td><strong>USD 75bn</strong>&lt;br&gt;Global stock trading volume (2016)</td>
</tr>
<tr>
<td><strong>USD 16bn</strong>&lt;br&gt;Identity theft damages (2016, US only)</td>
<td></td>
</tr>
</tbody>
</table>

While the majority of the market has clearly focused on fungible token applications so far, we have seen first use cases being created via non-fungible tokens. Non-fungible tokens have mostly emerged in the collectibles space in form of e.g. Cryptokitties. We expect the non-fungible phenomenon to spread outside of the collectibles space and find use in further blockchain applications. Blockchain applications for ownership and identity solutions will only be fully enabled by non-fungible token models.

### Surge in Blockchain Popularity

Over the past year, the world has become obsessed with blockchain technology. While the tech itself is not new, experts admit that its mass adoption could be compared to the rise of the internet in the 1990s.

Blockchain technology bears a potential that is hard to evaluate in its amplitude. It offers to change our everyday lives in a multitude of ways, from the way we buy and sell to the way we participate in politics and state governance.

Promising to erase intermediaries and borders, the technology suggests a new definition of trust and transparency, that will impact both our online and offline lives.

---

*Sebastian N. Markowsky<br>G P Bullhound*
We took an in-depth look at the state of blockchain technology to date. Areas of focus were funding of blockchain projects, both from venture capital investors and through ICOs, and key issues that will determine the success and adaptation of the technology going forward. Our goal is to provide an overview of relevant characteristics and key trends in the blockchain sector and offer insights into what is currently happening with regards to base protocol developments and show promising distributed ledger concepts and people that will likely shape the future development of the technology.

OUR METHODOLOGY AND SOURCES

WE HAVE INCLUDED:

Companies developing proprietary blockchain technology and related services comprising smart contract functionality and where the public and decentralized nature of the planned blockchain project will benefit from a token distribution event.

We have not looked at permissioned blockchain companies, protocol technologies or projects. Our analysis of venture capital funding is mainly based on publicly available data and Pitchbook. Data on ICO rounds was sourced from various online databases as well as the relevant whitepapers. We focused on funding rounds between 2015 and 2017. ICO performance analyses exclude companies with less than USD 1m funds raised.

CAVATAS: Our sources only include public data (e.g. press articles, public databases and websites). The accuracy of the data sets underlying our analysis is therefore limited to the disclosed data.

WE HAVE EXCLUDED:

We have not looked at permissioned blockchain companies, protocol technologies or projects. Our analysis of venture capital funding is mainly based on publicly available data and Pitchbook. Data on ICO rounds was sourced from various online databases as well as the relevant whitepapers. We focused on funding rounds between 2015 and 2017. ICO performance analyses exclude companies with less than USD 1m funds raised.

CAVATAS: Our sources only include public data (e.g. press articles, public databases and websites). The accuracy of the data sets underlying our analysis is therefore limited to the disclosed data.

WE HAVE INCLUDED:

Companies developing proprietary blockchain technology and related services comprising smart contract functionality and where the public and decentralized nature of the planned blockchain project will benefit from a token distribution event.

We have not looked at permissioned blockchain companies, protocol technologies or projects. Our analysis of venture capital funding is mainly based on publicly available data and Pitchbook. Data on ICO rounds was sourced from various online databases as well as the relevant whitepapers. We focused on funding rounds between 2015 and 2017. ICO performance analyses exclude companies with less than USD 1m funds raised.

CAVATAS: Our sources only include public data (e.g. press articles, public databases and websites). The accuracy of the data sets underlying our analysis is therefore limited to the disclosed data.

WE HAVE EXCLUDED:

We have not looked at permissioned blockchain companies, protocol technologies or projects. Our analysis of venture capital funding is mainly based on publicly available data and Pitchbook. Data on ICO rounds was sourced from various online databases as well as the relevant whitepapers. We focused on funding rounds between 2015 and 2017. ICO performance analyses exclude companies with less than USD 1m funds raised.

CAVATAS: Our sources only include public data (e.g. press articles, public databases and websites). The accuracy of the data sets underlying our analysis is therefore limited to the disclosed data.

AUTHORS

SEBASTIAN MARKOWSKY
Director

SIMON MIREMADI
Associate

ELENA BOCHAROVA
Analyst

HANNES FELSBERG
Analyst

BULAT MARDANOV
Analyst

FELIX LUTJEN
Intern

ACKNOWLEDGEMENT

Special thanks to Joe Lubin and the ConsenSys-Team, Prof. Emin Gün Sirer, Peter Czaban, MacLane Wilkison and Tatu Kärki, our interview partners featured in this report.

Big thank you also to the further contributors to the report that have provided great insights themselves or been instrumental in providing access to the knowledge centers in the space: Jan Kamath, Hugo Anselm, Bermio Lind, Konstantinos “Dino” Milhofopoulou, Stefan George, Gero Decker, Fabio Federici, Philipp Moehring, Mikko Alasarela, Fabian Vogelsteller, Alex Felix, John Quinn, Mal Marziali, Stefano Bernardi, Lorenzo Sanna, Robert Henker, Adrian Fako, Gavin McDermott, Kaan Narin, Kai Chan, Barren Jeter, Eli Turlington, James Knight. Thanks a million and looking forward to exciting times ahead with all of you.
No information set out or referred to in this research report shall form the basis of any contract. The issue of this research report shall not be deemed to be or form any offer or solicitation to purchase or sell, nor the content, in any way, a prediction or a definitive statement of fact or probability. Actual events and circumstances may be subject to change at any time without notice. GP Bullhound LLP is under no obligation to update the information contained in this research report or to other companies who might be said to be competitors of the company or companies referenced in this research report or to other entities that might be said to be competitors of any of the companies referenced in this research report. Accordingly, information may be available to GP Bullhound LLP and/or its associated undertakings may from time-to-time add or dispose of such interests. The information contained in this research report or to any part thereof, be redistributed or disclosed to anyone without the prior consent of GP Bullhound LLP. Hence, no party shall have any claim for prejudice to the generality of the foregoing, no party shall have any claim for damages. The information contained in this research report is not intended to be a complete and independent verification of all the assumptions, criteria, estimates, scenarios, data or other information set out or referred to herein. No representations or warranty, express or implied, is made or accepted by GP Bullhound LLP, its member, directors, officers, employees, agents or associated undertakings relating to the accuracy, completeness or reliability of the information in this research report or to other companies who might be said to be competitors of any of the companies referred to in this research report and may from time to time add or dispose of such interests. GP Bullhound LLP is a limited liability partnership registered in England and Wales, registered number OC314854, and is authorised and regulated by the Financial Conduct Authority. Any reference to a partner is in relation to GP Bullhound LLP as a member of GP Bullhound Ltd. GP Bullhound Ltd is an employee with equivalent standing and qualifications. A list of the members of GP Bullhound LLP is available on request at its registered office, 12 Jersey Street, London SW1Y 6LX.

For US Persons: This research report is distributed to US persons by GP Bullhound Inc., a broker-dealer registered with the SEC and a member of the FINRA, GP Bullhound Inc. as an affiliate of GP Bullhound LLP. This research report does not provide personalized advice or recommendations of any kind. All investments bear certain material risks that should be considered in consultation with one’s financial advisors and/or tax advisors. GP Bullhound Inc. engages in private placements and mergers and acquisitions advisory activities with clients and counterparties in the Technology and CleanTech sectors. Certain members of the research team and GP Bullhound are long certain positions as an indication of their belief that such investments may fall as well as rise. For US Persons: This research report is distributed to US persons by GP Bullhound Inc., a broker-dealer registered with the SEC and a member of the FINRA, GP Bullhound Inc. as an affiliate of GP Bullhound LLP. This research report does not provide personalized advice or recommendations of any kind. All investments bear certain material risks that should be considered in consultation with one’s financial advisors and/or tax advisors. GP Bullhound Inc. engages in private placements and mergers and acquisitions advisory activities with clients and counterparties in the Technology and CleanTech sectors. Certain members of the research team and GP Bullhound are long certain positions as an indication of their belief that such investments may fall as well as rise.
OUR MISSION

To advise the most passionate technology entrepreneurs

GP. Bullhound