



The State of the Token Market

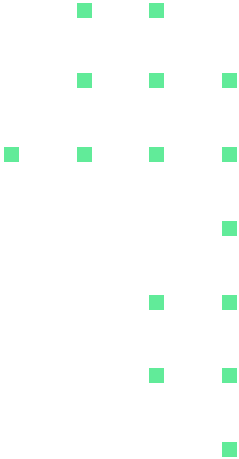


A Year in
Review & an
Outlook for
2018

A joint production by

FabricVentures × **TokenData**





This page is intentionally left blank

Fabric Ventures

Fabric Ventures, a new VC fund backed by OpenOcean and Firestartr, is adapting the traditional long-term venture approach to investing in scalable decentralised networks. It is building on OpenOcean's peerless open source pedigree and Firestartr's background in seed investing & blockchain focus, and is backing the boldest projects forming the foundation of the 'Fourth Age of Open Source'. Fabric has already backed projects including Orchid, Status.im, Polkadot, Ocean Protocol, and Blockstack Signature Fund, among others.



Ani Banerjee



Anastasiya Belyaeva



Christina Frankopan



Max Mersch



Richard Muirhead

www.fabric.vc

[@fabric_vc](https://twitter.com/fabric_vc)



TokenData is a free platform tracking all publicly available data (qualitative & quantitative) on token sales (1600+). TokenData is unaffiliated to mainstream media, crypto currency news outlets or token sales. They distribute a bi-weekly newsletter that is read by a wide spectrum of people interested in the blockchain space, ranging from cryptocurrency hobbyists to prominent VCs and national regulators.

www.tokendata.io

Contents

Foreword

Part 1: 2017 in Numbers

- 03 Are Token Sales Taking Over?
- 04 Token Sale Capital Breakdown
- 05 Capital Raised by Sector
- 06 - 07 Token Returns and Model Portfolio
- 08-10 Geographic Diversity of Token Sales

Part 2: Outlook for 2018

- 11 - 14 The Future of Open Source Funding
- 15 - 18 Upgradability of Smart Contracts and the Emergence of New Standards
- 19 - 25 Scalability of Blockchains
- 26-29 The Importance of Stablecoins

Foreword

2017 was definitely a year that operated on token time. Decentralised projects collectively raised \$5.6b, with hundreds of worthy projects laying the groundwork for a new client-to-client computing architecture powered by a multitude of token economies. However, at Fabric Ventures we believe that this has been in the making for many decades. In fact, the history of a formally implemented 'token economy' actually pre-dates Satoshi and Vitalik quite a bit. It dates back to the early part of last century and was focused on non-monetary rewards or dis-incentives for toddlers, prisoners and, perhaps notably, the psychologically unstable.

For several decades entrepreneurs and developers have been building software companies, deeply rooted in open source. Among them are successes like MySQL, built and coded by one of our team members Monty Widenius, and which remains the world's most popular database to date. What we see as the power of decentralised ledger technology, or more particularly the trustless digital networks it enables, is the new age of open source software development that can fund and build a whole new generation of censor-resistant projects that will ultimately overtake the impact of MySQL or even Internet itself.

We have rarely been more excited about what the upcoming year promises to deliver: numerous projects intending to go live on main-net, decentralised exchanges gaining traction, industry grade services including custody and accounting, identity networks and data ownership models enabling the blooming of the sovereign individual and many more. In this report, we are reviewing the state of the token market in 2017, and exploring the importance of some of the most critical developments we expect to take place in the year ahead.

Richard Muirhead,

Founder & Partner, Fabric Ventures



FabricVentures × TokenData



Part 1

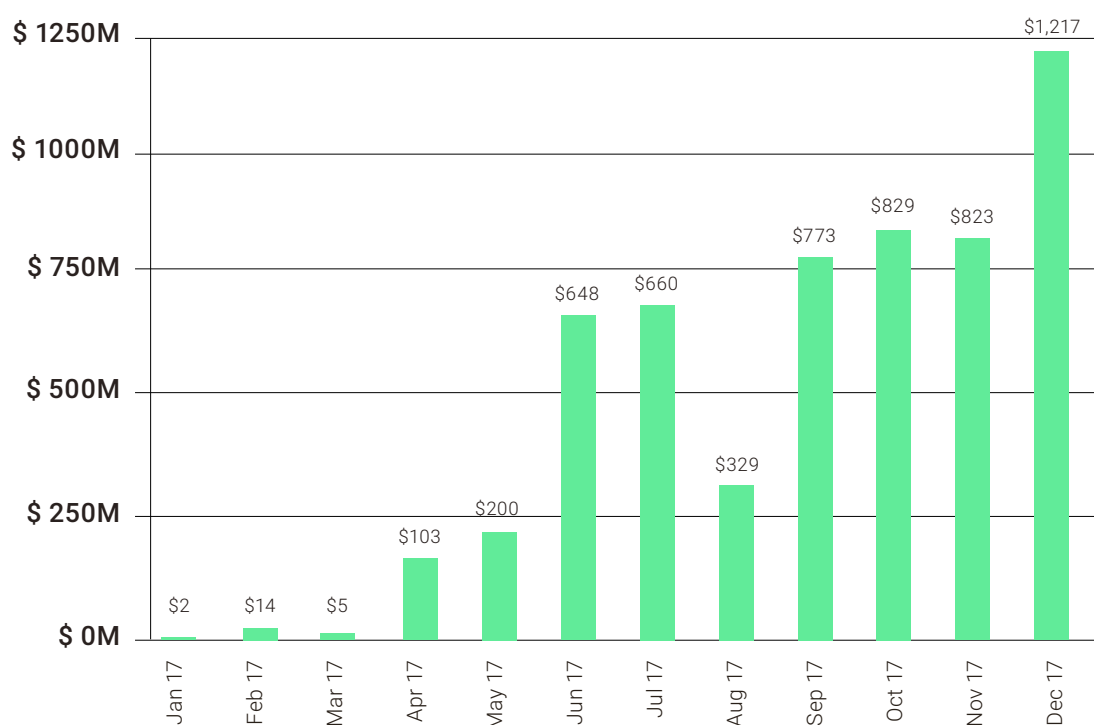
2017 in numbers



Are Token Sales Taking Over?

2017 will go down as the year that token sales (also known as ICOs) dominated a large part of the daily conversations in the worlds of cryptocurrencies, decentralized web/ Web 3.0 economics and venture capital. More than **5.6 billion dollars** of capital was raised in 2017 according to the metrics¹ used by the TokenData team. This compares to 1 billion dollars of 'traditional' venture investing in blockchain startups in the same timeframe and a 'mere' **240 million dollars** raised by token sales in 2016.

USD Raised by ICOs in 2017 - Monthly Totals



Using publicly available information, we have distilled a number of key insights about the projects behind the token sales, capital structure and financial returns of the distributed tokens.

¹Requirements: a) Token sale must have ended, b) token sale must have announced the end result of the sale OR at least 2 independent sources confirm the capital raised, c) if capital is denominated in cryptocurrency the closing price as cited on coinmarketcap.com is utilized to convert to dollars

Token Sale Capital Breakdown

We start our insights with a breakdown of the capital raised numbers:

Only 48% of all Token Sales (ICOs) were successful

Token Sale Descriptive Statistics:

- **USD Raised:** \$5,596 Million
- **Nr of Token Sales:** 913
- **Nr of "completed" Token Sales:** 435
- **Average Capital Raised:** \$12.7M
- **Median Capital Raised:** \$4.5M

435 token sales raised **\$5.6B** in **2017**

However, more than 900 token sales were planned and/or active at one point in time during the year. The gap between the two numbers is due to failures/refunds

- 1 Failures/Refunds:** 131 projects reported that they failed to meet their minimum threshold
- 2 Unreported:** 347 sales did not report the end result of their token sales, TokenData was unable to gather the information from at least 2 independent sources or token sale websites have simply disappeared.

The 10 largest token sales raised 25% of all capital

Looking more closely at the distribution of raise amounts the average raise is almost 3 times larger than the median raise, indicating that the capital raised is skewed towards the larger token sales. This is supported by a closer look of the top 10 completed token sales of 2017. Collectively, the 10 largest sales raised close to \$1.4B and roughly 25% of the total capital raised in 2017.

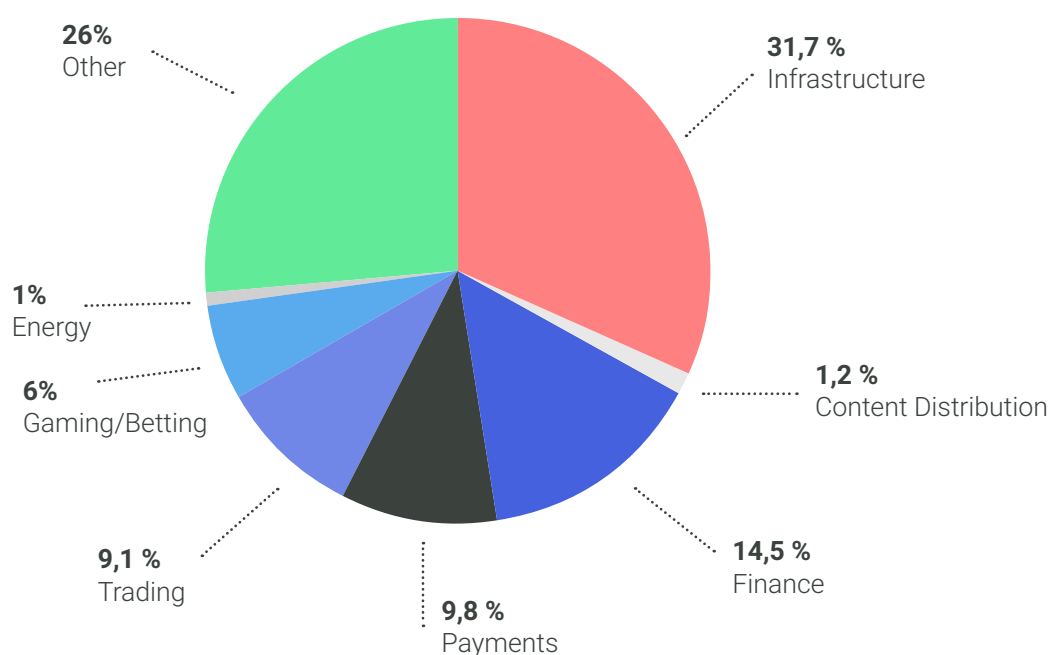


²Token Sales with publicly available information about capital raised

Capital Raised by Sector

Project	Sector	Raise
Tezos	Blockchain Infrastructure	\$230,498,884
Filecoin	Blockchain Infrastructure	\$200,000,000
Sirin Labs	Other	\$157,885,825
The Bancor Protocol	Blockchain Infrastructure	\$153,000,000
Polkadot	Blockchain Infrastructure	\$144,347,146
QASH	Trading & Exchange	\$108,174,500
Status	Blockchain Infrastructure	\$107,664,904
Kin	Payments	\$98,500,326
COMSA	Finance	\$95,614,242
TenX	Finance	\$83,110,818
Total		\$1,378,796,646

One pattern that stands out from the 10 largest token sales is that Blockchain Infrastructure projects³ raised a significant amount of capital in 2017 - a pattern consistent with a larger picture, when looking at all token sale projects.

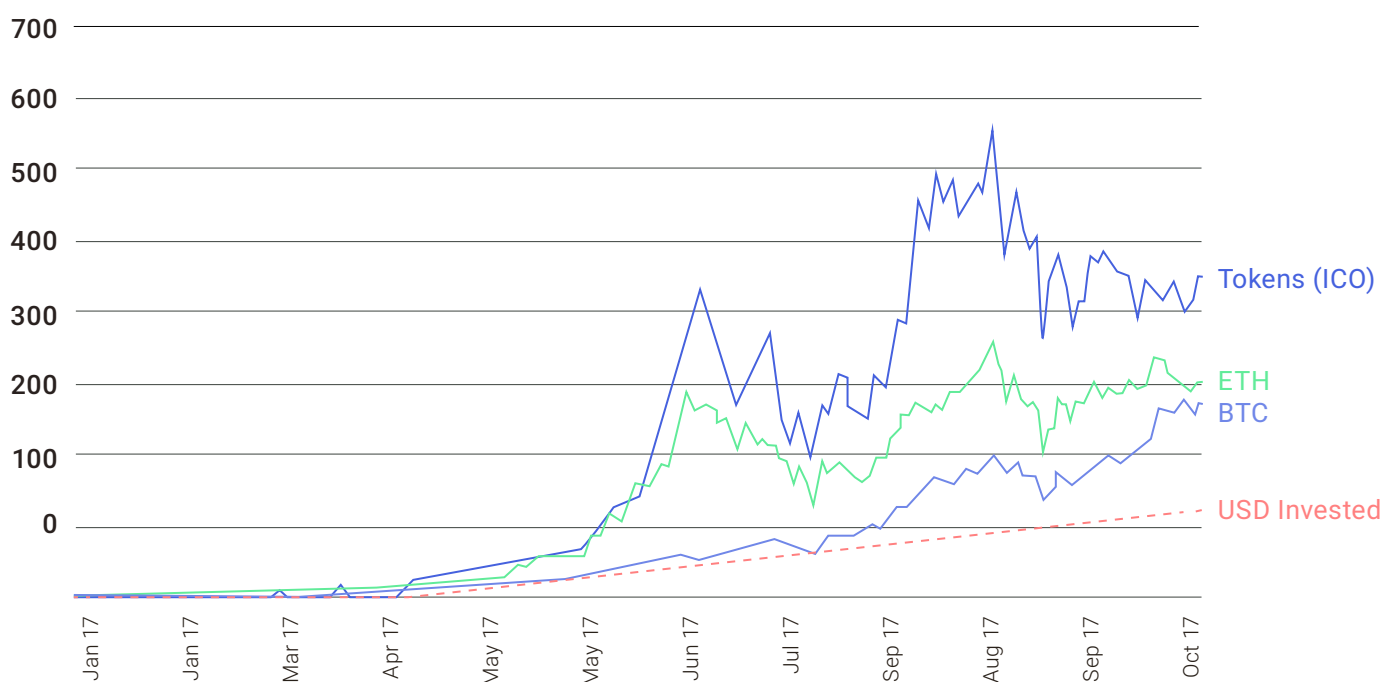


³ This includes core blockchain protocols as well as projects that focus on second layer protocols such as decentralized file storage, computing

Token Returns and Model Portfolio

One of the main catalysts for the capital flows into token sales has been the search for financial returns and outperformance of the two base cryptocurrencies Bitcoin (BTC) and Ethereum (ETH). The below graph illustrates this trend, mapping all listed ICO tokens with enough historical data against investments in ETH and BTC.

Historical Values for Token Portfolios



* Dataset consists of traded ICO tokens on www.tokendata.io that had enough historical data

** Returns are calculated assuming that someone invested 1 USD in every ICO and put 1 USD in ETH and BTC at the same time in separate portfolios. There is no rebalancing or weighting.

However, a closer look at the number of “ICO Issued” tokens which outperform both BTC and ETH in dollar terms show that only 25% of the tokens issued in 2017 yielded better buy-and-hold returns since their issuance than BTC and ETH.

Token Returns and Model Portfolio

To further explore the token vs. BTC/ ETH portfolio returns, we've constructed hypothetical equally weighted portfolios of more than 175 tokens that were issued in 2017 and compared the returns with portfolios of either BTC or ETH in which the investments are made at exactly the same time as the issuance of a token.

This analysis shows that on average tokens have returned 12.8x the initial investment in dollar terms versus 7.7x for ETH and 4.9x for BTC during 2017. A closer look shows that returns are skewed towards a handful of tokens issued in the first quarter of 2017 - when the ICO hype had not fully erupted, and that average token returns have been trending down since. Additionally, a breakdown of median returns still shows outperformance by tokens, but paints a much more nuanced picture.

ICO Date	Average Returns			Median Returns		
	Token	ETH	BTC	Token	ETH	BTC
Q1 2017	44.6x	64.6x	13.1x	48.2x	67.5x	12.9x
Q2 2017	17.0x	7.1x	6.9x	6.1x	3.8x	5.4x
Q3 2017	9.3x	3.4x	4.0x	3.1x	3.2x	3.7x
Q4 2017	6.5x	2.4x	1.9x	4.8x	2.3x	1.9x
2017	12.8x	7.7x	4.9x	4.9x	3.0x	4.3x

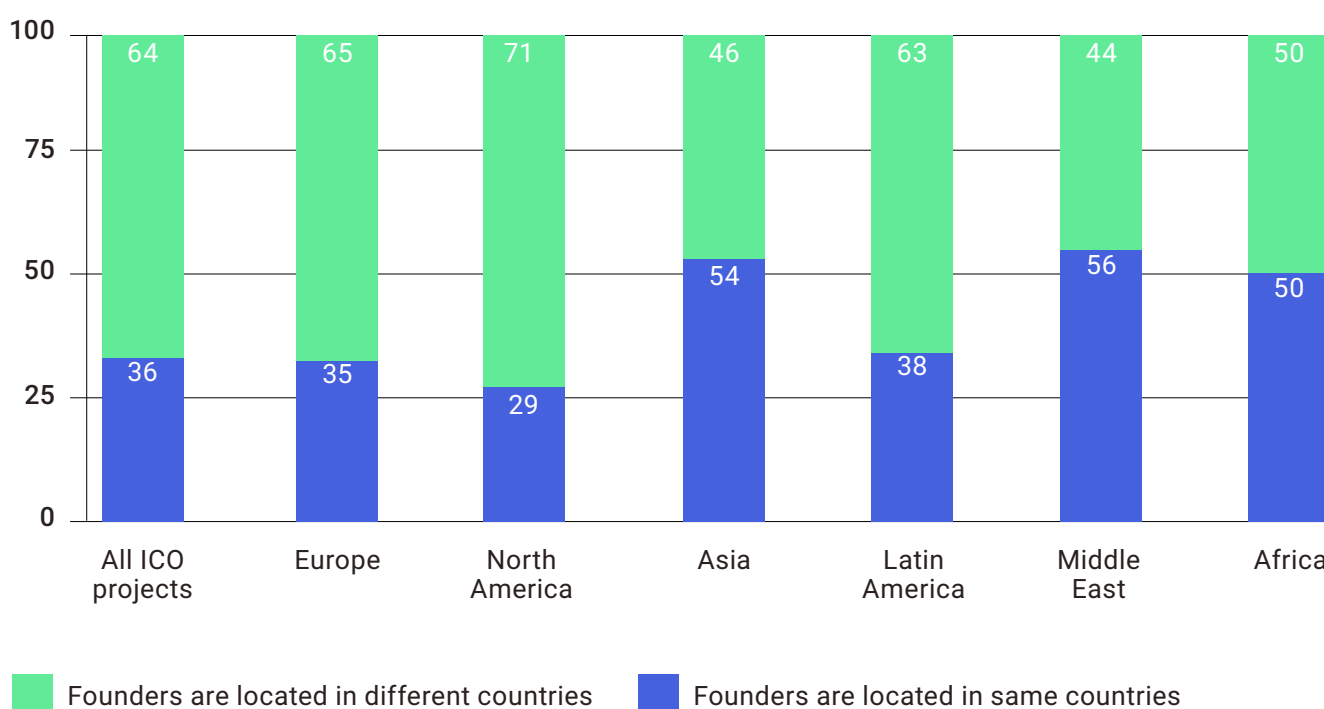
* Dataset consists of all traded ICO tokens on www.tokendata.io and prices on December 31st 2017

** Returns are calculated assuming that someone invested 1 USD in every ICO and put 1 USD in ETH and BTC at the same time in separate portfolios. There is no rebalancing or weighting.

Geographic Diversity of Token Sales

Token Sales & their Founding Teams are Geographically Decentralized...

An often overlooked but interesting part of token sales and blockchain startups is the geographical location of the teams behind them. We counted more than fifty (56) different countries in which the legal entities behind token sales are located. Furthermore, looking at the location of the principal founders of the token sales, we counted 62 different countries. Both metrics for geographic diversity are lower bounds, because close to 20% of all token sales in 2017 did not report any geographic location. Therefore, from the geographic distribution of token sales, we can conclude that the cryptocurrency community behind token sales is a geographically diverse one. This statement is further underlined by an analysis of the composition of the token sale teams. A breakdown of the domicile for the key founders of a project (CEO, CTO and COO) shows that two thirds of all token sale projects have teams located in different countries⁴.

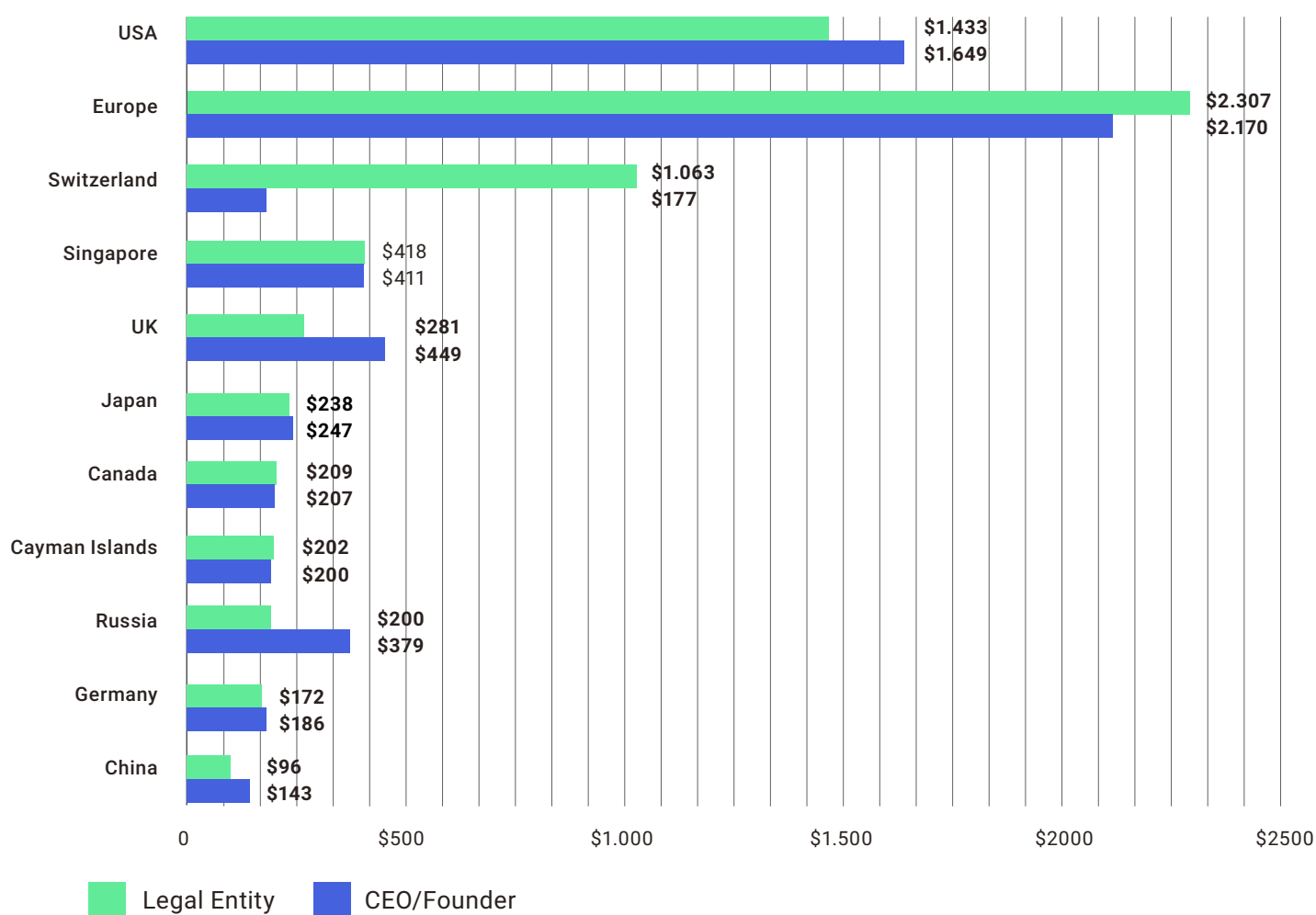


⁴We combined publicly available information supplied by token sales with social media profiles (LinkedIn & Facebook) to map geographic location of founders

...but Capital is Geographically Concentrated

Looking at the geographic location of the legal entities as reported by token sales, we conclude that projects located in the top 10 countries have raised more than 75% (\$4.3B) of all capital in 2017. While the U.S. is leading the way as a single country - home for blockchain projects, with \$1.4B (25%) capital from a legal domicile perspective, and \$1.6B (29%) from the founder location perspective, Europe as a whole outraces it with \$2.3B and \$2.1B of capital respectively - an exciting benchmark for the European tech community.

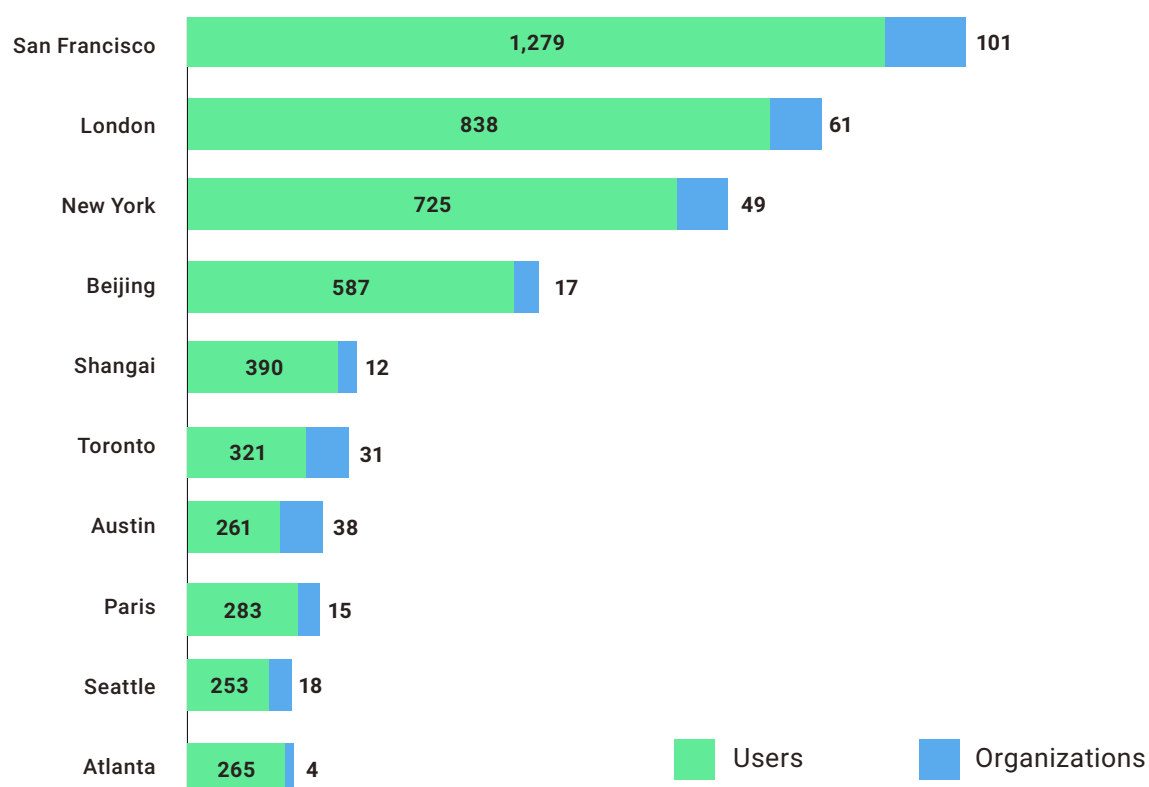
Top 10 countries by capital raised (\$M) via ICOs based on country of legal entity location and country of CEO/Founder location



A detailed look at European countries reveals a significant contrast for Switzerland. With Switzerland's regulatory openness to cryptocurrencies, the emergence of "Crypto Valley" and Zug as the city in which many ICOs are legally based, Switzerland has attracted more than \$1B of capital and transformed to a leading home for token sales from a legal perspective - but not (yet) from a founder's perspective.

From the blockchain development perspective, the largest concentration of developer talent (based on GitHub project ownership) is in San Francisco - with London and New York following in popularity.

Top 10 cities for blockchain development



Source: Deloitte analysis of GH Torrent data and GitHub API data, as of October 12, 2017



FabricVentures × TokenData



Part 2

Outlook for 2018



The Future of Open Source Funding

When looking at the history of free & open source software, one can retrace to an idealistic period of development in the 60's and 70's - in which developers, primarily motivated by political and privacy reasons, collaborated with governmental efforts that could not be commercialised. Eleftherios Diakomichalis (founder of oscoin) elegantly describes it as *"the free software movement - the ethical and even romantic age of software development"* - there was a common agreement that the infrastructure that underpins society needs to be in the open domain.

This was followed by the 2nd and 3rd ages of open source software, which were much more pragmatic and efficient. Developers started realising that it was a clearly superior way of developing projects with a community of enthusiastic contributors & evangelists. Today, the early artisanal, passionate movement has been transformed comprehensively and optimised by cultural movements like DevOps; processes like Agile, Scrum, Kanban and tools from the likes of Atlassian and GitHub. We do, however, fundamentally believe that, as Allan Mertner (Engineering Director at Facebook) points out: *"Developers are, like most people who work in a knowledge field, mainly motivated by doing interesting work. As Dan Pink says: Autonomy, Mastery and Purpose is what matters above all; in other words, doing something that matters, and doing it well."*

Companies also quickly realised that there were creative ways to monetise on top of open source software and moved forward aggressively. We're now living in a reality where large corporates have built trillions of dollars of market capitalisation with software they don't own and with data that is ours.

As our entire society is hooked on open source software that has been created and is being maintained by a few enthusiastic but un-incentivised contributors, developers are starting to realise the influence that lies in their creation. So far there had been extremely small rewards for these creators & maintainers, compared to the outsized value creation they have originated. The efficiency and effectiveness of development and the far-reaching distribution of open source software had been demonstrated - the final missing piece remained the incentives layer.

Over the past few years, following the innovative integration of native tokens, we've seen an explosive funneling of money aimed at open source projects. \$5.6b has been invested in new projects in 2017 and projects now have decades of runway to operate from. However, in our view, the current token model is still very far from solving the open source funding problem. The majority of investors are more interested in the speculative nature of cryptocurrencies than in the efficiency of open source development. A lot of these projects have raised massive amounts of money upfront before receiving any market validation, creating problems for long term incentivisation of the team. All the work that still needs to be done, is thrown in the spotlight by Mike Hearn's (Lead engineer at R3 and early Bitcoin contributor) general observations: in most projects there is a misapprehension that *"the hard part of writing decentralised apps is the cryptography part"* rather than figuring out *"workflow...UI, P2P network issues... the challenge of decentralised software updates"*.

Many projects have resorted to raising the funds in a Swiss Foundation in order to separate the project's funds from the potentially temporary developer team (e.g. while Satoshi Nakamoto launched Bitcoin, active maintenance has been taken over by new developers). This foundation model is not without faults, as we've seen with the recent disputes between the Tezos development team and the Tezos Foundation. We've seen numerous other sensible and self-regulating initiatives spring up, such as founder vesting contracts, capped initial sales and even full transparency reports on use of funds. As an example, Aragon has been leading the way with a [live dashboard of their funds](#), clear quarterly [transparency reports](#) and [public community meetings](#).

We're extremely excited to see a wealth of new token distribution mechanisms being used over the coming year. Starting from the earliest stages, we believe many projects will opt to raise small equity rounds from strategic investors first, giving the team of developers time to test, verify and iterate their protocol before launch. It's even more important than in the traditional start-up world, where most companies pivot on multiple occasions before finding product market fit, as these protocols have very little room for pivoting once deployed. This additional early runway will avoid locking in half-tested ideas at network launch, and more importantly, will allow projects to have a working protocol by the time they release a token.

Once network-market fit has been found and the protocol is launched, we're expecting to see multiple iterations of token distribution mechanisms including DAICOs, Continuous Token Models and Interactive Coin offerings. While adopting these more restrictive models might currently seem unlikely, we strongly believe that self-regulation

and community governance will have to prevail for the healthy growth of the ecosystem.

We expect a Darwinistic process to kick-in, in which projects with better governance will raise funds more successfully and operate more efficiently (we can already see that over 52% of projects do not achieve their target raises). Without surprise, we found the same problems when discussing Mike Hearn's synthesis of his recommendation to Gavin Andresen and Satoshi Nakamoto from his time in the trenches in the Bitcoin governance battles:

"[Getting] the community used to doing votes through the blockchain, developing "proof of stake" type voting mechanisms (but not for consensus), getting the community used to hard forks, and explicit rejection of the following ideas - all of which are bogus: Rule of maths; Digital gold; Immutable cryptocurrency."

DAICOs combine the best parts of Decentralised Autonomous Organisations (DAO) and Initial Coin Offerings (ICO) - a hybrid model that enables projects to raise large amounts of funds, but gives the token holding community control over the 'tap' that controls these funds. This improved governance mechanism enforces a milestone based approach for the development of a project and puts the interest of the network itself at the highest importance.

Continuous Token Models as described by Simon de la Rouviere explore *"the idea that instead of pre-selling tokens during a launch phase, the tokens are minted as needed through various means. The tokens are then dispensed for services rendered in the network"*. Such continuous token models could enable small issuer specific bounty networks as well as an ongoing generation of non-fungible assets (e.g. Decentraland Mana inflation or Generation 0 Cryptokitties sales).

Interactive Coin Offerings was presented by Jason Teutsch (Truebit) and Vitalik Buterin (Ethereum) as a solution that strives to ensure both certainty of valuation and certainty of participation: a conundrum that Vitalik had previously outlined as *"the first token sale dilemma"*. Through a dynamic and interactive mechanism, each participant specifies a desired purchase quantity at each valuation, which results in a final price that should satisfy both goals.

Taking a different perspective from these large scale token distribution mechanisms, on a much more granular level of individual incentivisation, Eleftherios envisioned a

future where developers find two primary methods of funding open source software: monetising at the code level with native tokens, or more interestingly, monetising at the governance level. By exchanging value for governance input on projects, companies, and DAOs, developers will be able to monetise their influence and reputation (which was until now purely symbolic). In an economy that's overarchingly built on open source software, a significant amount of power lies within the ability to influence its development. As Mike Goldin pointed out, *"what blockchains give us, fundamentally, is programmable money. When you can program money, you can program incentives. When you can program incentives, you can kind of program people's behavior."*

***"When you can program incentives,
you can kind of program people's
behavior."***

"
— Mike Golden

Upgradability of Smart Contracts and the Emergence of New Standards

// *Overall, the rate of innovation in building decentralized applications is limited by the manual and duplicative efforts projects must make to ensure basic usability and security.*

— Demian Brener //

As a direct product of the permissionless innovation enabled by The Rise of the Token Sale, we've seen numerous token model iterations cement into place. We initially started with store of value & medium of exchange tokens and more recently, a lot of projects started focusing on token curated registries & staking tokens. As a natural process of innovation, these iterations have spawned networks governed by token models that could be proven to be inefficient and friction-inducing.

In time, we believe we'll find that numerous projects used token models mainly as a fundraising mechanism, and are left with tokens that induce friction into the network. Medium of exchange tokens, that could easily be replaced by more widely distributed ETH or stablecoins, add an arbitrary fee to users that have to exchange into the native currency and don't necessarily increase incentives for stakeholders to keep using the network. Some projects might initially build in velocity sinks (mechanisms that discourages token holders to sell) or token burn mechanisms, but they might also realise that while such inflationary policies were a useful bootstrapping mechanism to attract investors, they're not in the best long term interest of the users of the networks. While these innovative models are a great way to push funding for projects that were not necessarily fundable before, these token models are often locked into protocols and become difficult to change & upgrade over time. The lack of upgradability and standardisation also leads to vulnerabilities and hacks: The DAO

hacker drained \$70m of Ether, while the Parity multisig code flaw froze \$160m of Ether.

Creating future proof smart contracts will require the ability to easily upgrade for vulnerabilities but also for price optimisations in deployment and compute cycle consumption on the Ethereum Virtual Machine (EVM). This will allow projects to solve for problems that were not foreseeable during initial deployment, or iterate & pivot their incentives structures to get closer to network-market fit. Or it could quite simply be required to add new features upon the community's request.

Demian Brener (founder of zeppelin_os) points out:

"tools developers are using to build the Blockchain economy are very rudimentary. Once a contract is deployed, there's no way to upgrade it, even for security reasons, which means applications can't easily upgrade with new features and fixes; instead of calling standard libraries, application developers are copy/pasting code with each deployed contract, increasing deployment costs and margin for error; and, last but not least, debugging a contract's failing function calls is hell with current tools."

The upgradability of smart contracts contains a set of problems that span from governance to security and efficiency/usability of developer tools. We've eagerly been following the teams at zeppelin_os and Aragon, who've been collaborating on solutions for future proof smart contract deployment. Whether through upgradeable solidity libraries, or delegate proxy solutions that can delegate the main deployed contract logic to an upgradable proxy contract (e.g. upgrading the logic without risking erroneous changes on the live contract), the conclusion seems to be: keep it simple! Both the zeppelin_os kernel and the AragonOS kernel are providing the central structure and developer tools for upgrading smart contracts, while keeping all the business logic on the edge.

Diving into the theory behind upgradable governance with Luis Cuende (co-founder at Aragon):

"Upgradable governance means that the method used to drive the correct functioning of a network, protocol, or in general any system, can be upgraded to achieve a better functioning system over time. This is very similar to the concept of natural evolution. Given changes in the environment, living organisms have to adapt in order to better use the resources they have available. I think decentralized networks are a new kind of living

organisms. They align incentives for other entities to nurture and grow them (usually humans), but they are still subject to the rules of evolution. Therefore, they need upgradeability."

Coming back to more practical examples, Luis mentions:

"upgradeability is necessary for decentralized networks, because they provide a way to signal voice, instead of executing exit. This means that if two different parties want the network to be two different things, they can voice their concerns and let the governance decide. This is opposed to exiting, which would be the case of forks, which greatly reduce network effects.

Also, in this very experimental phase, creating decentralized networks that don't have any upgradeability built in is a huge mistake because of the security implications of it. If there's a critical bug inside the protocol (or even the governance mechanism itself!), then the governance process for fixing it should be fast, because stakeholders are incentivized not to lose their stake.

Finally, in 2017 we have seen hundreds of ICOs. Unfortunately, the teams are the ones raising the funds in a very centralized manner. This feels weird because of the raised capital should belong and be governed by the network. Upgradeability here means that the governance process for managing those funds can be improved, and the funds kept secure, while including the community in its governance."

In our opinion, the upgradability of smart contracts will be a paramount piece of the puzzle that still needs to come together for scalable applications to be built and maintained for the Web3 vision to come true. This will enable the creation of standards and frameworks that the developer community can adopt and collaborate on with the expectation to scale along new feature requests and security measures. As Demian Brener explains:

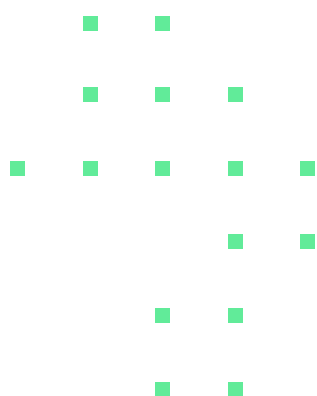
"Overall, the rate of innovation in building decentralized applications is limited by the manual and duplicative efforts projects must make to ensure basic usability and security. Much like in the early days of computing, where operating systems enabled the development of feature-rich applications, the same is needed for the development of complex smart contract applications."

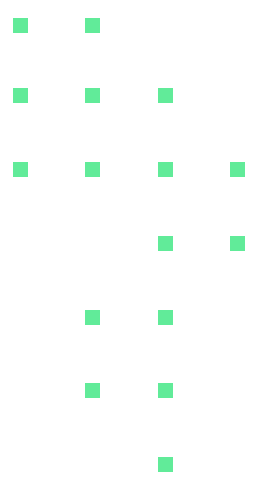
After all, Software Change and Configuration Management is a multi billion dollar industry today...

In 2017 we've seen the emergence of [ERC20](#) as the preferred token standard adopted by the large majority of projects (with 2018 bringing along an improved [ERC777](#)) and OpenZeppelin's smart contract framework as the premier & most secure framework. More recently CryptoKitties and Decentraland collaborated on creating [ERC721](#) - the non-fungible token standard - aimed at assigning ownership over scarce digital goods, which unlocks a wealth of applications for unique tokens with individually differing properties. One of the standards that has gotten the most excitement out of our team has been [ERC725](#) which Fabian Vogelsteller is working on and presented at Devcon3: A standard set of functions for a unique identity for humans, groups, objects and machines, which can sign actions, are attested by 3rd parties and can proxy functions for the given identity.

The Aragon team on the other hand is working on the [aragonOS](#) standard, enabling developers to *"expose their smart contracts' functions to other apps, provide fine-grained permissions over each of them and leverage any compatible governance method, effectively leveraging easy upgradeability"* (Luis Cuende).

We're looking forward to a wealth of new upgradable, modular and flexible standards emerging in 2018 with the hopes that these will create frameworks for identity, data & value exchange, ownership of non-fungible assets, bounty programs, vesting & incentivisation mechanisms etc... These will consolidate the required tools & frameworks for developers to properly unleash the power of an interoperable decentralised application ecosystem and will bring the first large wave of usable dApps to the masses.





Scalability of Blockchains

// Scalability is probably problem number one [...] There's a graveyard of systems that claim to solve the scalability problem but don't. It's a very significant and hard challenge. These are just known facts. //

— Vitalik Buterin “A Modest Proposal” at DevCon3, Nov 2017

The oft-repeated trilemma of blockchain systems is that they can have at most two of the three properties: decentralised, scalable and/or consensus (the “DCS triangle”). Arguably, existing blockchains (e.g., Bitcoin, Ethereum) have successfully delivered on the objectives of robust security and decentralisation, but at the cost of scalability.

This can be seen as a blockchain variant of classic engineering trilemmas such as “fast, cheap, good: choose two” (RAID), or “consistency, availability, partition tolerance: choose two” (CAP theorem). Trilemmas of this kind can at times seem artificial, but in the case of blockchain systems it is a fundamental problem with no easy balanced solution.

What are the obstacles to scaling blockchain systems?

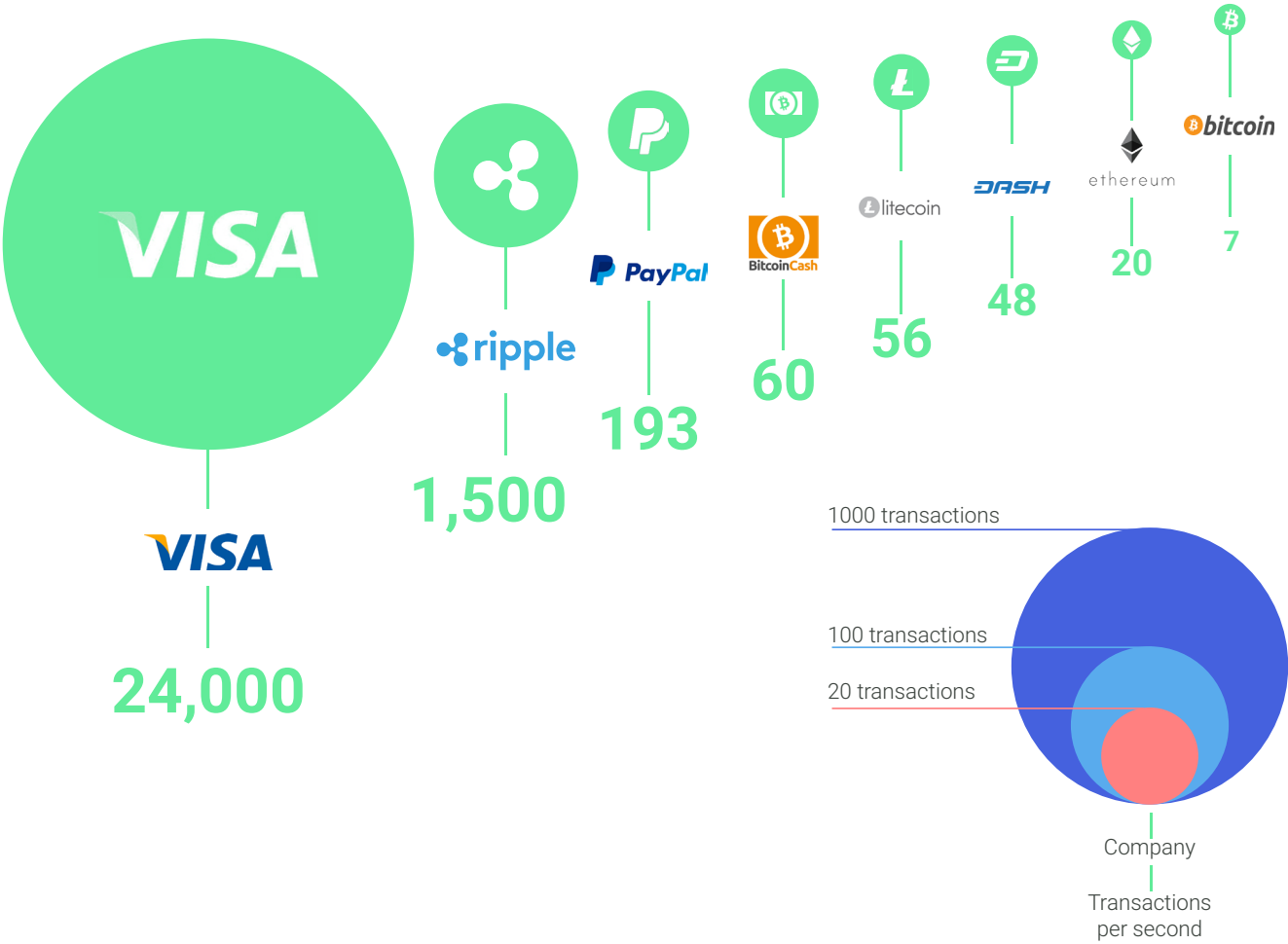
In blockchain systems, every node in the network processes and synchronises a copy of the entire state or transaction history. Typical blockchain design requires every node in the network to process every transaction, which limits the transaction processing capacity of the entire system to the capacity of a single node.

Inter-node latency grows logarithmically with each node added to the network which increases the risk of centralisation. Consortium chains such as Ripple can in principle improve on scaling issues by ensuring high capacity node availability, but only at the cost of centralisation.

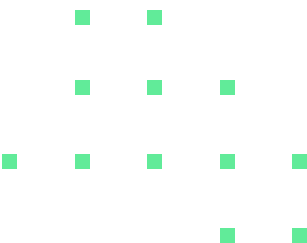
To put the scaling problem in context, the bitcoin network typically processes on

average 3.5 transactions per second (tx/s) up to a maximum of 7 tx/s, while ethereum processes around 15-20 tx/s. By contrast, Paypal processes around 190 tx/s and Visa around 24,000 tx/s.

Cryptocurrencies Transaction Speeds Compared to Visa & Paypal



<https://howmuch.net/sources/crypto-transaction-speeds-compared>



The scaling issue has manifested in very concrete terms through increased transaction fees and at times severe network congestion (often unintended or unanticipated) from transaction demand for a large ICO, or from a sudden craze for cryptokitties.

There are additional problems to resolve including data availability whereby a node might go offline, for reasons including malicious attack and power loss. This is in fact a much broader problem which gets worse as we start to shard the state. Basically, nodes know that they should accept something as canonical, but have no way of accessing it, thus halting any further progress.

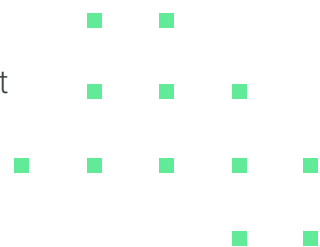
Why does scaling matter?

One of the consequences of this issue to date; has been that interesting use cases and applications (in particular micro-transactions) could not be economically processed on the main chains. More broadly, at Fabric Ventures we find that many blockchain projects with which we work see scaling as a major limiting factor on their development plans in the immediate 12 months. Notwithstanding this “block” (pun intended), we see this a strong imperative for progress and it is a testament to the open source culture of the space to see continued cross-community collaborations between platforms and technologists (e.g. Plasma, lightning cross-chain swaps).

What solutions are available or in progress?

Work on scaling solutions can be broadly segregated into base layer scaling solutions and “Layer 2” solutions. We see both sets of solutions as probably necessary and indeed complementary, depending on use cases. Much of the groundwork for progress in Layer 2 was laid in 2017 by the Segwit soft-fork in Bitcoin and the Byzantium hard fork in Ethereum, by making it lighter, faster to run, more secure smart contracts and preparing for native support of cryptographic privacy technologies such as zk-snarks, as pioneered by Zcash.

We are excited to see 2018 kicking off with some accelerated signs of progress, particularly in Layer 2 solutions such as a network of payment channels (e.g. Lightning, Raiden). These approaches have the potential to deliver millions or even billions of transactions per second, with particular applicability to payment



systems for IoT, M2M, adtech and live streaming to name but a few. However, general state channels are still under research and existing solutions are only able to handle a limited set of transaction types.

There are many interconnecting elements to the solution space for scaling blockchain systems and we will just outline some of the initiatives in this area:

On the bitcoin chain, segregated witness was activated last August and allows for 2mb blocks or greater. The industry is still working toward greater adoption of this opt-in solution. Segwit in fact shifts the focus from block size to “block weight” which adjusts based on witness data, and technically enables effective block sizes of up to 4mb, with 2mb already having been experienced. There has been continued debate on blockweight (to increase it 2x or more) which would allow for more transactions on-chain, but again, at the risk of centralisation (as fewer nodes could run at larger block sizes). One of the interesting debates in the bitcoin community continues to centre on governance and how and when block weight changes will be implemented. There has also been some interest in sidechains which allow one to receive and spend bitcoins using a two-way peg (2WP). An open question however remains how one might find sufficient node capacity to deliver such solutions.

One direction for the ethereum community meanwhile is sharding. The concept of sharding is to split the blockchain state into a number of “universes”, where each client will process only a small portion of transactions. This has potentially enormous benefits. Yet we will still have some time to wait (up to 3 years) before sharding is implemented on the main ethereum chain. Also, the transition from proof-of-work to proof-of-stake (Casper) is a prerequisite for any implementation of sharding, so we are watching, waiting and hoping for successful implementation of that transition in 2018.

We also believe that it is likely that the future Web 3.0 stack houses a multitude of blockchains, public and private, some general purpose, some special purpose, each with their own “features”. This is potentially an important part of longer-term scaling solutions where a hyper-modularized system of features can be combined depending on application requirements - we may start to see more industry chains for example. In this vision, interoperability at both the transactional level, but also the more generalised data level between blockchains, (including cross-shard communication) will be a central element of that future stack. We see “blockchain of blockchain” projects such as Polkadot which will allow general trust-free transactions between chains and Cosmos which will allow token transfers as critical

infrastructure projects.

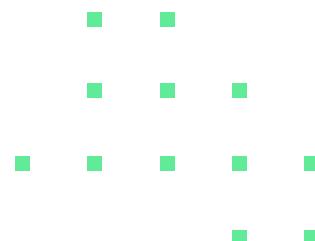
In this vision, interoperability at both the transactional level, but also the more generalised data level between blockchains, (including cross-shard communication) will be a central element of that future stack. We see “blockchain of blockchain” projects such as [Polkadot](#) which will allow general trust-free transactions between chains and [Cosmos](#) which will allow token transfers as critical infrastructure projects.

There is some potential for immediate gains of [Proof of Authority](#) - based approaches which are addressing scaling issues through open, public, permissioned networks based on Ethereum protocol with PoA consensus, reached by independent pre-selected validators. This potentially enables a swarm of blockchains with PoA consensus, connected by interledger protocols. PoA networks are actually ready now, but are waiting for solutions such as sharding and polkadot to solve the issue of dispersed security.

There is also interesting work in progress on probabilistic [micropayments](#) which may be more efficient than payment channels “whenever the service provided is continuous and granular enough for the probabilistic variance to become negligible”. Use cases include video streaming, electricity/energy markets and bandwidth sharing.

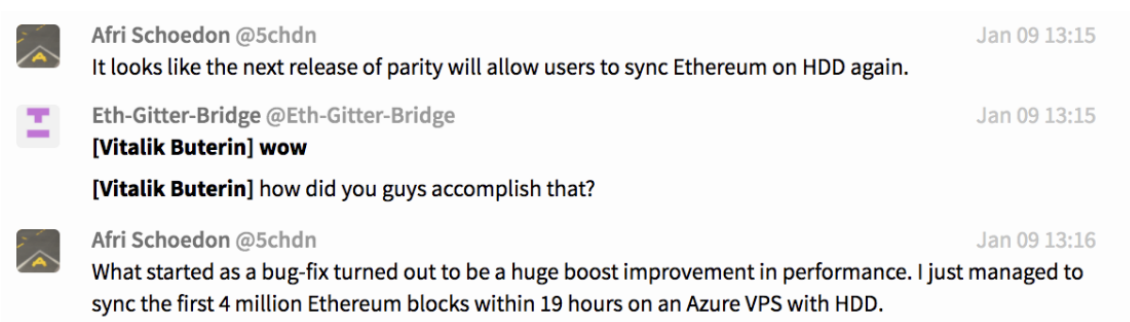
Post-segwit, the Lightning Network is now evolving at a pace. In [December 2017](#), a phone payment provider Bitrefill used the Lightning Network to execute a virtually free and instant transaction on the bitcoin mainnet. Several companies are working on compatible implementations, including Lightning Labs, Acinq, and Blockstream, who performed a successful [interoperable mainnet test](#) in December. Thousands of developers have tested Lightning on the bitcoin test network, and have already built [dozens of apps](#) on top of Lightning Labs’ implementation. Blockstream recently released a micropayment processing system “[Lightning Charge](#)” designed as a simple system for developers to build payment applications. Lightning also recently performed the first ever lightning [cross-chain](#) atomic [swap](#) (instant and high volume) between bitcoin and litecoin.

The Raiden team revealed [μRaiden](#) at a compelling presentation at [DevCon3](#) which has now been implemented on the ethereum mainnet. This also enables virtually instant and free many-to-one micro-transactions. The main [Raiden](#) state channel network could launch as early as this year, enabling powerful applications for (micro)payments,



peer-2-peer cash and instant atomic token swaps. This opens entire new possibilities for decentralised crypto exchanges.

The two most popular ethereum clients – Geth and Parity – have recently released updates that attempt to improve storage performance. The Parity [release](#) reduced storage requirements by eliminating unnecessary, temporary files. By vastly minimizing the storage requirements, users then experience faster synchronization times. Parity's ethereum software could now be run on a hard drive (again) instead of a solid state drive. This is the type of advance innovation that would have gone unnoticed to many crypto-enthusiasts but which demonstrates continued technical progress in the space.



A screenshot of a Gitter chat interface showing a conversation about the Parity Ethereum client. The chat is set in a room named 'AllCoreDevs'. The first message is from Afri Schoedon (@5chdn) at 13:15, stating that the next release of Parity will allow users to sync Ethereum on HDD again. The second message is from Eth-Gitter-Bridge (@Eth-Gitter-Bridge) at 13:15, quoting Vitalik Buterin saying 'wow' and asking how they accomplished that. The third message is from Afri Schoedon (@5chdn) at 13:16, explaining that what started as a bug-fix turned out to be a huge performance boost, allowing them to sync the first 4 million Ethereum blocks within 19 hours on an Azure VPS with HDD.

Afri Schoedon @5chdn Jan 09 13:15
It looks like the next release of parity will allow users to sync Ethereum on HDD again.

Eth-Gitter-Bridge @Eth-Gitter-Bridge Jan 09 13:15
[Vitalik Buterin] wow
[Vitalik Buterin] how did you guys accomplish that?

Afri Schoedon @5chdn Jan 09 13:16
What started as a bug-fix turned out to be a huge boost improvement in performance. I just managed to sync the first 4 million Ethereum blocks within 19 hours on an Azure VPS with HDD.

<https://gitter.im/ethereum/AllCoreDevs?at=5a513d1e232e79134dd468a7>

There is also exciting work being done on “speculative optimisation” for the Geth client ([turbo-geth](#)) which aims to reduce the time for blocks to propagate by optimising how ethereum clients process the overall state.

Some conclusions for the short, medium and long-term

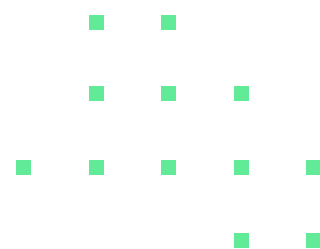
There is no easy panacea for scalability objectives in blockchain systems, yet it is critical that the community finds solutions. The Ethereum Foundation has recently recognised the importance of collaborative scaling research through the announcement of a series of [incentives](#) to accelerate progress: an entire subsidy program for work on the sharding client and on Layer 2 scalability solutions.

We believe it is likely that we will see a range of complementary solutions which will probably be implemented in phases. In all cases, optimisation will probably require refined sense of use cases and choice of solutions which matches real-world

applicability. There probably is no one-size-fits-all solution. We believe it is essential to ask exactly why we need scaling? What are the specific use cases we are trying to solve for? Some applications will require general state transitions for example, while others will only require token transfers. Equally, while some scaling solutions will apply to fungible tokens, they might not work for non-fungible tokens...

The DCS trilemma presents an enormous challenge to resolve scalability for decentralised technologists, but such challenges can at times be overcome. For example, Zooko's triangle, which in 2001 set out the challenge of "secure, decentralized, and human-readable names: choose two" has arguably been squared (with input from Aaron Swartz (RIP) among others) through the eventual implementation of blockchain naming systems such as Namecoin, Blockstack, ENS.

Equally, we are optimistic that we will see an initial range of practical, fit-for-purpose and complementary on and off-chain scaling solutions over the next 12-24 months. Longer term, within the next 3-5 years we hope to see further base layer solutions and are excited about the possibilities this entails for massively scalable use cases of blockchain technology at the application level.



The Importance of Stablecoins

“...in many ways, virtual currencies might just give existing currencies and monetary policy a run for their money.”

— Christine Lagarde

A Stablecoin is a cryptocurrency whose value is pegged to that of another asset, such as the US Dollar or gold. Like any other cryptocurrency, stablecoins are fungible, divisible, and free from any restrictions. In the world of cryptocurrencies, extreme volatility shocks no-one. A stable coin can be seen as a “cryptocurrency with price stability” for short and mid-term use as “unit of account”.

When a currency is used as a medium of exchange, it becomes very difficult for other people to stop valuing it. The currency stops being a purely speculative asset, backed by nothing, and transitions into an equilibrium where it is backed, effectively, by the immense pain people would incur from having to switch away from it. Students of game theory will understand this as a Nash Equilibrium, where if everyone else believes a currency is valuable, the optimal strategy is for one to treat it as valuable as well. Once the USD established its medium of exchange monopoly on the world, and succeeded in getting other countries to use it for trade, it could safely transition away from tangible backing without fear of losing its abstract value. It could rely on a collective action problem, where it became impractical and/or inefficient for everyone to switch to a new currency at the same time, thereby maintaining its position as the dominant medium of exchange.

After World War II, the world economy adopted the Bretton Woods system. The Bretton Woods system specified that the U.S. would back its currency with gold and that every other country would keep USD as its reserve. As long as the U.S. maintained its backing to gold, every other country would also be implicitly backed by gold. This worked well until the 1970’s when the U.S. decided to officially end

the gold standard, a decision partially caused by bad discretionary monetary policy. Since that point, the U.S. money supply, and implicitly the global money supply, has not been backed by tangible assets. One cannot go to the U.S. government and ask for a fixed amount of gold for a dollar - the only thing that gives the dollar value is the circular promise that other people will continue to value it. While it is true that the U.S. government can use coercion to force its citizens to continue using dollars, nothing else stops the rest of the world from moving to, say, a crypto backed stablecoin other than a very, very strong network effect based on trade between nations. This same network effect can keep a currency in a stable equilibrium in the absence of tangible backing.

Christine Lagarde recently dove into the IMF's interest in virtual currencies: *"Because it may one day be easier and safer than obtaining paper bills, especially in remote regions. And because virtual currencies could actually become more stable. For instance, they could be issued one-for-one for dollars, or a stable basket of currencies. Issuance could be fully transparent, governed by a credible, predefined rule, an algorithm that can be monitored...or even a "smart rule" that might reflect changing macroeconomic circumstances. So in many ways, virtual currencies might just give existing currencies and monetary policy a run for their money. The best response by central bankers is to continue running effective monetary policy, while being open to fresh ideas and new demands, as economies evolve".*

It is important for a stablecoin to create an ecosystem of incentives that keep the currency in an equilibrium, powered by network effects, where its purchasing power is constant. The stronger the network effects powering this equilibrium, the more stable the coin will be. What this implies at a high level is that if such a stablecoin is successful in getting a foothold initially as a medium of exchange, it can leverage that network effect to keep its value stable even in the complete absence of physical backing. That initial foothold can start with integrations into dApps, but if one can dream for a moment, one might end up "dollarizing" such a stablecoin. For example in countries such as Zimbabwe or Egypt, where one's savings are disappearing at the rate of currency depreciation adjusted inflation, a stablecoin that acts as a dominant medium of exchange is much needed. The team at Intangible Labs (Basecoin) rightly points out that *"a cryptocurrency solution, by which millions of dollars could be transported on one's phone, seems like a vastly superior alternative to paper dollars in all dollarization scenarios"*.

When looking at the various models employed to create stablecoins, we've found

Myles Snider's (Multicoin Capital) framework to be particularly simple & efficient: Centralised IOU Issuance, Collateral Backed and Seigniorage Shares.

So far, the major stablecoin in circulation has been Tether. Tether works on a centralised IOU Issuance principle, and requires the user to trust the issuing party. To trust that they actually own the assets being represented and that they are willing to honor the IOUs it creates when needed. The Tether model imposes counterparty risk on holders of the token and there have in fact been recent concerns over the solvency of the central issuer.

Collateral backed stablecoins have so far been the major attempt at creating a fully decentralised stablecoin: MakerDAO has recently gone live with their DAI stablecoin and has held its peg remarkably well during recent volatile market movements. Arguably, one of the concerns with this model is that, in order to make this a fully decentralised solution that doesn't require the user to trust a 3rd party, the collateral asset ends up being a cryptoasset such as Bitcoin or Ethereum. Given the volatile nature of the collateral asset, the stablecoin could very quickly become under-collateralised and suffer from the problems of traditional asset liability mismatch risk. As a result, collateral backed stablecoins could end up requiring over-collateralisation and require extremely strong dynamic risk management infrastructure to manage the collateral risk.

One of the more recent approaches we've come across, is trying to replicate a central bank through a decentralised algorithmic approach. This approach, also called the Seigniorage Shares model, expands and contracts the economy by issuing additional stablecoins to the network when the demand increases beyond the supply, and issuing discounted bonds to contract the economy when the demand falls back down. The team at Basecoin has been working on implementing this model in a fully decentralised and self-governing structure, and we're looking forward to their live launch in the hopefully not too distant future.

There has been some vocal criticism and/or scepticism about the rationale of stablecoin models, both economic and technical. The starting point for us is recognising the valid use-case of stablecoins, which we believe is a given. We also believe that time will tell which solutions are most effective and that a range of stablecoins solutions will emerge over time, each of which may have different features depending on appropriate use case. We continue to watch the space with great interest.

References

The Future of Open Source Funding

Against on-chain governance, Vlad Zamfir, December 2017. See also: https://medium.com/@Vlad_Zamfir/against-on-chain-governance-a4ceacd040ca

Analyzing Token Sale Models, Vitalik Buterin, June 2017. See also: <http://vitalik.ca/general/2017/06/09/sales.html>

Anyone Using Lighthouse for Crowdfunding? Reddit discussion. See also: https://www.reddit.com/r/Bitcoin/comments/4k1gu3/is_anyone_using_lighthouse_for_crowdfunding/

A Path Towards Better Token Sales, Damian Brener, November 2017. See also: <https://blog.zeppelin.solutions/a-path-toward-better-token-sales-91a07efa0d5e>

Crypto Currency Incentives, Elad Gil, October 2017. See also: <http://blog.eladgil.com/2017/10/cryptocurrency-incentives-and-corporate.html>

Explanation of DAICOs, Vitalik Buterin, January 2018. See also: <https://ethresear.ch/t/explanation-of-daicos/465>

Exploring Continuous Token Models: Towards a Million Networks of Value, Simon de la Rouviere, February 2017. See also: <https://media.consensys.net/exploring-continuous-token-models-towards-a-million-networks-of-value-fff153175776>

Fabric Ventures Interview with Mike Hearn, January, 2018.

Fabric Ventures Interview with Allan Mertner, January, 2018.

Fabric Ventures Interview with Eleftherios Diakomichalis, January, 2018.

Funding the Evolution of Blockchains, Fred Ehrsam, August 2017. See also: <https://medium.com/@FEhrsam/funding-the-evolution-of-blockchains-87d160988481>

Github for Lighthouse, Mike Hearn. See also: <https://github.com/vinumeris/lighthouse>

Interactive Coin Offerings, Jason Teutsch, Vitalik Buterin, and Christopher Brown, December, 2017. See also: <https://people.cs.uchicago.edu/~teutsch/papers/ico.pdf>

Lighthouse Objectives and Lessons, Mike Hearn, February 2015. See also: <https://www.youtube.com/watch?v=i4iZKISMZS8>

Upgradability of Smart Contracts and the Emergence of New Standards

On Medium-of-Exchange Token Valuations, Vitalik Buterin, October 2017. See also: <http://vitalik.ca/general/2017/10/17/moe.html>

Parity Team Publishes Postmortem on \$160 Million Ether Freeze, Rachel O'Leary, November 2017. See also: <https://www.coindesk.com/parity-team-publishes-postmortem-160-million-ether-freeze/>

The Rise of the Token Sale, Max Mersch, May 2017. See also: <https://blog.openocean.vc/the-rise-of-the-token-sale-28f2d07651c9>

Thoughts On Governance and Network Effects, Luke Duncan, December 2017. See also: <https://blog.aragon.one/thoughts-on-governance-and-network-effects-f40fda3e3f98>

Token-Curated Registries 1.0, Mike Goldin, September 2017. See also: <https://medium.com/@ilovebagels/token-curated-registries-1-0-61a232f8dac7>

Understanding The DAO Attack, David Siegel, June 2016. See also: <https://www.coindesk.com/understanding-dao-hack-journalists/>

Scalability of Blockchains

AP Twelve Years Later: How the "Rules" Have Changed, Eric Brewer, May 2012. See also: <https://www.infoq.com/articles/cap-twelve-years-later-how-the-rules-have-changed>

Enabling Blockchain Innovations with Pegged Sidechains, Adam Back et al, October 2014. See also: <https://www.blockstream.com/sidechains.pdf>

Ethereum scalability research and development subsidy programs, Vitalik Buterin, January 2018. See also: <https://blog.ethereum.org/2018/01/02/ethereum-scalability-research-development-subsidy-programs/>

Names: Distributed, Secure, Human-Readable: Choose Two, Zooko, October 2001. See also: <https://web.archive.org/web/20011020191610/http://zooko.com/distnames.html>

On sharding blockchains, Alexei Zamiatin, December 2017. See also: <https://github.com/ethereum/wiki/wiki/Sharding-FAQ>

Proof of Stake FAQ, Vitalik Buterin. See also: <https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ>

Rootstock: Smart Contracts on a Bitcoin Sidechain, Elements Project. See also: <https://elementsproject.org/sidechains/rootstock/>

Squaring the Triangle: Secure, Decentralized, Human-Readable Names, Aaron Swartz, January 2011. See also: <http://www.aaronsw.com/weblog/squarezooko>

The DCS Theorem, Greg Slepak and Anya Petrova, October 2017. See also: <https://arxiv.org/ftp/arxiv/papers/1801/1801.04335.pdf>

The Ethereum network is getting jammed up because people are rushing to buy cartoon cats on its blockchain, Joon Ian Wong, December 2017. See also: <https://qz.com/1145833/cryptokitties-is-causing-ethereum-network-congestion/>

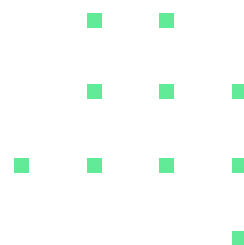
The Importance of Stablecoins

An Overview Of Stablecoins, Myles Snider, January 2018. See also: <https://multicoin.capital/2018/01/17/an-overview-of-stablecoins/>

Basecoin: A Price-Stable Cryptocurrency with an Algorithmic Central Bank, Nadel Al-Naji, Josh Chen, and Lawrence Diao, January 2018. See also: http://www.getbasecoin.com/basecoin_whitepaper_0_99.pdf

Central Banking and Fintech—A Brave New World?, Christine Lagarde, September 2017. See also: <https://www.imf.org/en/News/Articles/2017/09/28/sp092917-central-banking-and-fintech-a-brave-new-world>

Stablecoins are doomed to fail, Preston Byrne, December 2017. See also: <https://prestonbyrne.com/2017/12/10/stablecoins-are-doomed-to-fail/>



Contributors

We would like to thank these people for giving us inspiration, engaging in helpful discussions, sharing their opinions, and commenting on early drafts. All errors and omissions are ours.

Contributors

Carl Bennetts, Status.im
Julien Bouteloup, IDbox & Doshup
Demian Brener, Zeppelin OS
Luis Cuende, Aragon
Alexander Cullum, Brainbot
Peter Czaban, Web 3 Foundation
Eleftherios Diakomichalis, oscoin
Mike Hearn, R3
Allan Mertner, Facebook
Trent McConaghy, Ocean Protocol
Nabil Naghdy, Status.im
Yessin Schiegg, Status.im
Elizabeth Stark, Lightning Network
Jutta Steiner, Parity
Steve Waterhouse, Orchid

Sponsors





FabricVentures × TokenData

Thank You



www.fabric.vc/report
[@fabric_vc](https://twitter.com/fabric_vc)

If you would like to be on the mailing list for the Q2 report, please email tokenreport@fabric.vc

If you notice any errors or omissions, please let us know!

