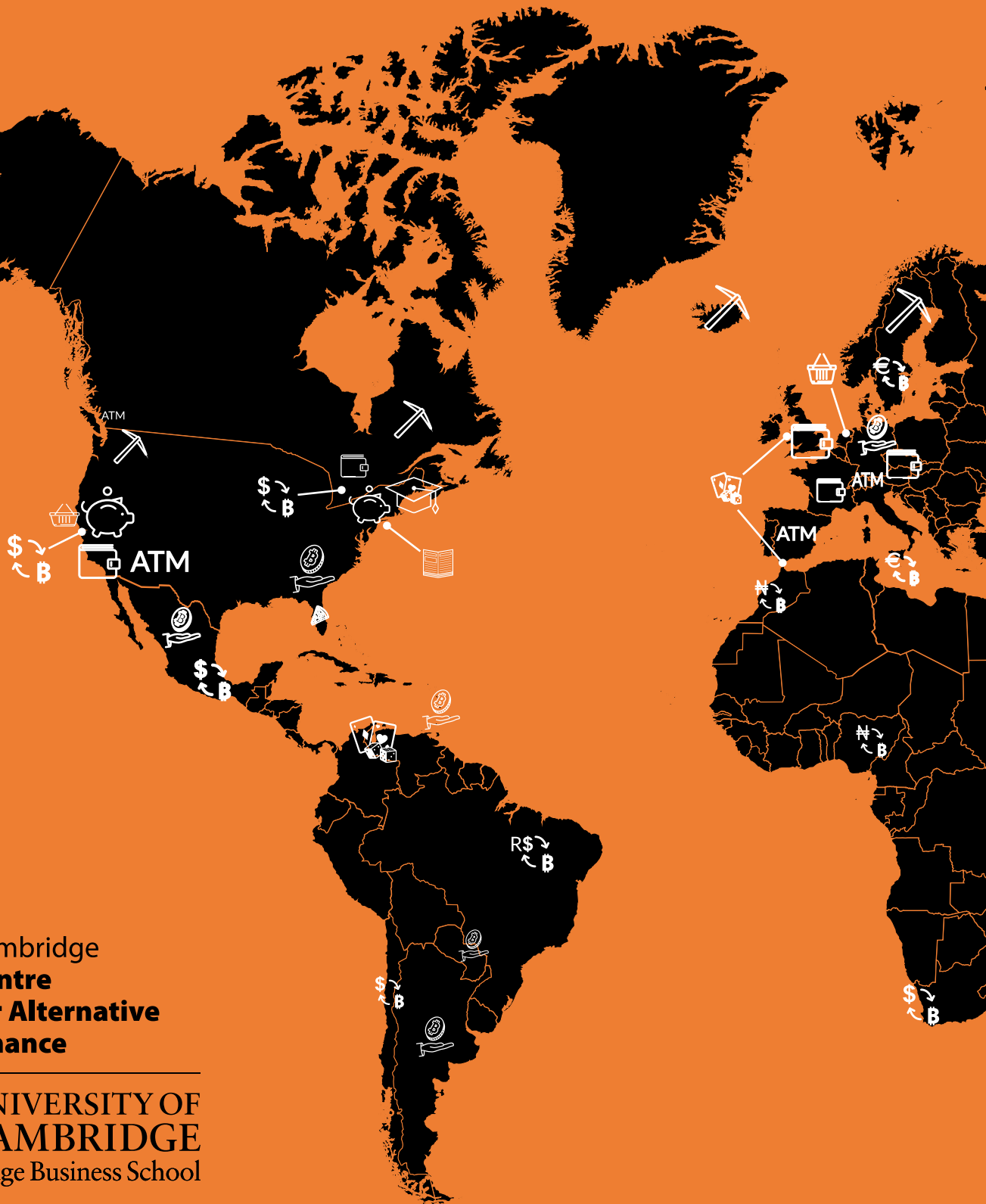


2ND GLOBAL CRYPTOASSET BENCHMARKING STUDY

Michel Rauchs, Apolline Blandin, Kristina Klein,
Gina Pieters, Martino Recanatini, Bryan Zhang

December 2018



Cambridge
Centre
for **Alternative**
Finance



UNIVERSITY OF
CAMBRIDGE
Judge Business School

The Cambridge Centre for Alternative Finance (CCAF) is an international and interdisciplinary research centre based at the University of Cambridge Judge Business School. It is dedicated to the study of innovative instruments, channels, and systems emerging outside of traditional finance. This includes, among others, crowdfunding, marketplace lending, alternative credit and investment analytics, alternative payment systems, cryptoassets, distributed ledger technology (e.g. blockchain) as well as related regulations and regulatory innovations (e.g. sandboxes and RegTech).

TABLE OF CONTENTS

FOREWORD	5
RESEARCH TEAM.....	6
ACKNOWLEDGMENTS	7
EXECUTIVE SUMMARY	10
METHODOLOGY.....	14
SETTING THE SCENE.....	17
The Year in Review.....	17
SECTION 1:	
THE CRYPTOASSET INDUSTRY.....	19
1.1 Segments.....	19
Industry Structure.....	19
Mining Segment.....	20
Storage Segment.....	21
Payments Segment	24
Horizontal Expansion: The Growth of Multi-Segment Firms	25
1.2 Industry Growth.....	26
1.3 Geography	28
A Global Industry	28
Legal Headquarters and Operations.....	28
SECTION 2: GLOBAL USAGE.....	30
2.2 Who Is Using Cryptoassets?.....	31
Total Users	32
User Types.....	34
User Activity	35
User Location.....	35
2.3 Cryptoasset Usage Characteristics.....	37
On-chain Payments.....	37
Off-chain Payments.....	39
Decentralised Applications and Timestamping	40
Speculation and Investment.....	40
SECTION 3: GATEWAYS AND ECONOMIC CONNECTIONS.....	42
On-Ramps and Off-Ramps.....	43
Internal Cryptoasset Ecosystem Flows.....	45
Managing Volatility	47
SECTION 4: STORAGE AND CUSTODY SEGMENT	49
Source Code.....	51
Key Storage Can Take Different Forms	52
Multi-Signature.....	53

SECTION 5: REGULATIONS AND COMPLIANCE.....	54
5.1 The Impact of Regulations.....	54
User Impact of Regulations	54
Cryptoasset Firms Collaborate Directly with Regulators.....	56
5.2 KYC/AML Policies.....	57
Implementation	57
Criteria.....	58
Account Suspensions and Closures.....	59
5.3 Compliance Team.....	60
5.4 Licensing.....	61
SECTION 6: IT SECURITY.....	63
IT Security Team.....	64
Security Audits.....	65
Internal Policies.....	67
SECTION 7: MINING SEGMENT.....	68
Cryptoasset Selection.....	68
Influence on Decision-Making Process	70
Concentration Concerns	71
7.2 Hardware Manufacturing.....	72
Mining Equipment and Algorithms	73
Distribution Channels.....	75
How Concentrated Is Manufacturing?.....	75
7.3 Mining Facilities	77
Meet the Hashers.....	77
Facility Set-up Decision Factors.....	77
Distribution of Mining Facilities.....	78
How Much Energy Does Cryptoasset Mining Consume?	81
How Wasteful Is Cryptoasset Mining?	83
What Do Miners Think?.....	85
7.4 Pool Operators.....	86
Pool Operations.....	86
Pool Concentration.....	87
FUTURE OUTLOOK.....	90
APPENDIX: SENTIMENT QUESTIONS.....	94



FOREWORD

Cambridge
**Centre
for Alternative
Finance**



It is my great pleasure to announce the release of the second Global Cryptoasset Benchmarking Study produced by the Cambridge Centre of Alternative Finance based at the University of Cambridge Judge Business School. It examines significant developments in the global cryptoasset ecosystem that have occurred since the publication of our initial benchmarking study of cryptocurrencies in April 2017. The emphasis on 'global' in the title of this study is critically important given the increasingly fluid, borderless nature of the cryptoasset industry. It also reflects a core competence of our research centre, which is engaging in empirical research investigating global technology-enabled financial innovation emerging outside of the incumbent financial system. For our 2nd cryptoasset report the research team spent several months collecting data from more than 180 entities in 47 different countries, which represents a 25% increase in both the number of participants and countries represented in comparison to our 2017 benchmarking report.

Our series of benchmarking studies analysing emerging forms of alternative finance provides a comparative global snapshot of rapidly developing ecosystems impacting the incumbent financial system. Our goal from the outset was that these periodic reports would become a valuable reference for a wide audience of actors in the financial system, including disruptive product and service innovators, incumbent financial services firms, investors, academics, regulators and policymakers, and the general public. Each of these constituents deserves to be heard in debates about financial innovation, and few finance innovations have been as controversial and attracted as much misinformed opinion as the developments associated with cryptoassets. Our aim is to inform these voices by providing empirically-based evidence of developments to provide common points of reference to build upon. Sometimes this challenges prevailing wisdom. For example, the analysis of excess renewable energy used by a share of mining facilities suggests that the negative environmental externalities – and associated costs – of the energy consumed by proof-of-work consensus systems could be lower than previous estimates. We continue to believe that good research should generate at least as many new questions as it answers, and we hope this report passes that test.

Dr. Robert Wardrop

Director

Cambridge Centre for Alternative Finance



RESEARCH TEAM

Michel Rauchs: Michel is the Lead in Cryptocurrency and Blockchain at the Cambridge Centre for Alternative Finance. He co-authored the inaugural benchmarking studies on the cryptoasset and enterprise blockchain industries, and was the Project Lead of the *Distributed Ledger Technology Systems: A Conceptual Framework* report.

✉ m.rauchs@jbs.cam.ac.uk

🐦 [@mrauchs](https://twitter.com/mrauchs)

Apolline Blandin: Apolline is a Research Manager in Cryptocurrency and Blockchain at the Cambridge Centre for Alternative Finance. Prior to joining CCAF, she graduated from Peking University and the London School of Economics with a dual Master's degree in International Affairs. Her research has mainly focused on mobile finance and financial inclusion in China.

✉ a.blandin@jbs.cam.ac.uk

🐦 [@ApollineBlandin](https://twitter.com/ApollineBlandin)

Kristina Klein: Kristina is a Visiting Student at the Cambridge Centre for Alternative Finance. She is pursuing a Master's degree in Management and Technology at the Technical University of Munich (TUM) and focuses on entrepreneurship and computer science.

✉ k.klein@jbs.cam.ac.uk

🐦 [@kklein93](https://twitter.com/kklein93)

Dr. Gina Pieters: Gina is a Lecturer at the Department of Economics at the University of Chicago and a Research Fellow at the Cambridge Centre for Alternative Finance. Her research examines the economic implications and behaviour of cryptocurrencies across different currencies and monetary systems.

✉ gcpeters@uchicago.edu

🐦 [@ProfPieters](https://twitter.com/ProfPieters)

Martino Recanatini: Martino is a Visiting Student at the Cambridge Centre for Alternative Finance. He is pursuing a Master's degree in Finance and Banking at the Politecnica delle Marche University in Italy. His Master's thesis assesses the potential impact of DLT systems on securities post-trading services.

✉ m.recanatini@jbs.cam.ac.uk

🐦 [@marecanatini](https://twitter.com/marecanatini)

Bryan Zhang: Bryan is the Executive Director and a Co-Founder of the Cambridge Centre for Alternative Finance. He has co-authored more than 20 reports on financial innovation and regulatory innovation.

✉ b.zhang@jbs.cam.ac.uk

🐦 [@BryanZhangZ](https://twitter.com/BryanZhangZ)



ACKNOWLEDGMENTS

We would like to thank Liu Feng and the ChainNews team for providing a Chinese version of the surveys, Miguel Klaggues from the Asociación Bitcoin Chile for translating the surveys into Spanish, as well as Kim Cheol Hwan and Seowon Park from the Korean Blockchain Industry Promotion Association (KBIPA) for the Korean survey version. Nick Chong (Quoine) and Fiorella Velazquez (BitInka) provided helpful comments and undertook significant efforts in helping distribute the surveys.

Special thanks go to Keith Bear (CCAF) and Kathryn Vagneur (CCAF) for providing invaluable feedback in terms of survey design, data analysis, and report structure, Louise Smith for the beautiful design of the report, as well as Derek Snow for his thorough review of an early draft. Our interns Hatim Hussain, Jaya Lalwani, Jinjun Liu, Thomas Eisermann, Ouafaa Hmaddi, and Sabine Damborska deserve special thanks for their tireless work and efforts in helping make this report happen. Finally, we would like to thank the entire CCAF team – and Kate Belger in particular – for their continuous support and assistance.

We would also like to thank the following organisations for helping distribute the surveys to potential respondents in their respective countries and regions:



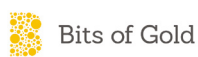
Asociación Bitcoin Chile, Associação Brasileira de Criptoconomia (ABCripto), Association of Cryptocurrency Enterprises and Startups Singapore (ACCESS Singapore), Bitcoin Argentina, Chaintech, Colombia Fintech, Estonian Cryptocurrency Association, Ghana Blockchain Society, Israeli Blockchain Association, the Korean Blockchain Industry Promotion Association (KBIPA), the Bitcoin Foundation, and the Nordic Blockchain Association.



This research study would not have been possible without the generous support and participation from industry actors: we would like to express our gratitude to the following cryptoasset entities for contributing to this research study by completing our surveys. Some survey respondents prefer not to publicly disclose their participation.



B E L E M





cryptobuyer

CryptoMine.by
mining hardware in Belarus



CUMBERLAND
A DRW COMPANY



edge



Genesis Mining

Globitex | GBX



HUT 8

HYDROMINER



Ledger

Leondrino Exchange

LUNO



NetM

niceHASH



PAYMENT 21

QUOINE

SFOX

SHIFT+
CRYPTOSEcurity

SLUSH POOL

SOLIDI

stratum
coinBR

SWISS CRYPTO VAULT
Hyper Secure Storage

TABTRADER

TOKEN
CAPITAL MARKET

tokeny
The Trusted Tokenization Platform

tradebit

trans
crypt



ViaBTC



EXECUTIVE SUMMARY

Since the publication of the first Global Cryptocurrency Benchmarking Study in April 2017, the cryptoasset ecosystem has undergone significant changes: the aggregate market capitalisation of cryptoassets skyrocketed from \$30 billion to more than \$800 billion at its peak in early January 2018, until coming down again to hover at around \$200 billion.

The surge in prices and subsequent fluctuations was accompanied by growing interest and attention from the general public and media, driving in new retail investors, speculators, and institutional investors. The industry was confronted with massive inflows of new users and funds, a situation not all actors had adequately prepared for. Growing interest from the institutional side contributed to the emergence of custom services tailored to meet the needs and requirements of this new type of demand, leading to a deeper interweaving of the industry and the incumbent financial system.

Between May and July 2018, the research team collected survey data from over 180 start-ups, established companies, and individuals from 47 different countries across all major regions. The objective of the study is to provide new insights into the current state of the ecosystem and, in combination with publicly available data sources, capture major trends of the rapid market development. The analysis focuses in particular on the following four key industry segments: mining, exchange, storage, and payments.

The analysis reveals six main findings:

- **Millions of new users have entered the ecosystem, but most remain passive**
Total user accounts at service providers now exceed 139 million with at least 35 million identity-verified users, the latter growing nearly 4X in 2017 and doubling again in the first three quarters of 2018. Only 38% of all users can be considered active, although definitions and criteria of activity levels vary significantly across service providers.
- **Firms are increasingly operating across segments**
The cross-segment expansion observed in 2017 has continued: 57% of cryptoasset service providers are now operating across at least two market segments to provide integrated services for their customers, compared to 31% in early 2017.
- **Multi-coin support is rapidly expanding**
Multi-coin support has nearly doubled from 47% of all service providers in 2017 to 84% in 2018; a trend primarily driven by the emergence of common standards on some cryptoasset platforms (e.g. ERC-20 on Ethereum) that has resulted in a rapid increase in the supply of tokens.
- **The majority of identified mining facilities use some share of renewable energy sources as part of their energy mix**
The study estimates that as of mid-November 2018, the top-6 proof-of-work cryptoassets collectively consume between 52 and 111 TWh of electricity per year. The mid-point of the estimate (82 TWh) is the equivalent of the total energy consumed by the entire country of Belgium – but also constitutes less than 0.01% of the world's global energy production per year. A notable share of the energy consumed by these facilities is supplied by renewable energy sources in regions with excess capacity.
- **Mining is less concentrated than commonly perceived**
Cryptoasset mining appears to be less concentrated geographically, in hashpower ownership, and in manufacturer options than commonly depicted: the mining map exhibits that hashing



facilities and pool operators are distributed globally, with growing operations in the USA and Canada.

- **Self-regulatory efforts reflect growing industry maturity**

Industry actors are pro-actively adopting measures that appear to comply with existing regulation despite not necessarily being explicitly subject to regulations. The increasing number of self-regulatory initiatives, combined with the emergence of sophisticated and professional services, reflect the growing maturity of the industry.

Other notable findings include the following (ordered by section):

The Cryptoasset Industry

- The industry has experienced substantial growth in terms of full-time equivalent (FTE) employees: 2017 year-on-year growth rates reached 164%, driven primarily by the exchange and storage segments.
- Firm size has also increased significantly: the average firm now employs a median number of 20 staff, up from five employees in 2016.
- While 21% of surveyed firms have their legal HQ in a different country than their operational HQ, only 7% have their legal HQ in a different geographic region, suggesting that while organisations may be willing to locate to nearby countries to exploit regulatory arbitrage, many are not willing to move too far afield.

Global Usage

- Individuals constitute the largest share of the user base (primarily served by exchanges and multi-segment firms); payment service providers and storage providers have the highest share of business users among service providers (26% and 32%, respectively).
- Firms predominantly serve customers based in the region where they have their operational HQ.
- Both on-chain and off-chain transaction volumes have significantly increased in 2017; behaviours consistent with speculation and long-term investment still account for the vast majority of cryptoasset usage.
- The share of high-value transactions (i.e. above \$1,000) for cross-border payments processed off-chain rose from 34% in 2016 to 46% in 2017, a trend that is mirrored by on-chain transactions as well.
- While Bitcoin's median on-chain transaction size has consistently grown since 2016, other cryptoasset systems have declining median amounts per transaction.

Gateways and Economic Connections

- The cryptoasset ecosystem is becoming more connected to traditional finance due to the emergence and growth of gateways bridging both systems, as well as growing regulatory clarity. The relatively small size of the industry in the global financial market poses no systemic risk at this time.
- Fiat-to-cryptoasset (and vice-versa) trades are allowed on some exchanges and payment platforms, but not allowed on others. For fiat-supporting exchanges, these fiat-to-cryptoasset trades make up the majority of trading volumes, demonstrating continuous in- and outflows from the cryptoasset ecosystem to the incumbent financial system and the real economy.
- Bank wires dominate supported methods for both deposits and withdrawals; the use of physical cash is more popular in Asia-Pacific than in other world regions.



- Service providers support a greater number of deposit options than withdrawal options, suggesting that entering the ecosystem is generally easier than exiting.
- 69% of surveyed payment service providers have existing relationships with established traditional payment networks, but difficulties of entering and maintaining good banking relationships remain a primary concern, particularly for exchanges.

Storage and Custody Segment

- Custody of cryptoassets is diverse: 62% of large entities retain control over customer funds compared to only 30% of small firms. Similarly, firms operating across multiple segments tend to take user funds into custody more often than companies specialised in one segment.
- Two-thirds of specialised custodial exchanges do not have a refund procedure in the case of customer funds getting lost or stolen.
- The share of funds held in cold storage has slightly decreased over 2017 to enable quick on-demand access, but is still above 80% of all funds.

Regulations and Compliance

- Cryptoasset service providers are fostering their compliance efforts, even when not explicitly subject to regulatory oversight: 37% of cryptoasset-only service providers have an in-house compliance team and more than half perform KYC/AML checks.
- While an average of 14% of KYC/AML checks result in service providers not opening new accounts or closing existing accounts, some firms claim figures between 50% and 80% - well above comparable traditional finance benchmarks.
- The majority of surveyed companies rely on traditional services for third-party support in conducting KYC/AML checks rather than specialised blockchain analytics providers.
- Only 5% of surveyed cryptoasset-only service providers hold an operating license for their jurisdiction, as opposed to 39% of fiat-supporting entities. However, 30% of cryptoasset-only service providers are planning to apply for a license or register with local authorities, which reflects the industry's willingness to proactively engage with compliance.
- There are active efforts at industry self-regulation, with most of entities collaborating with regulators and policymakers to address regulatory issues.
- Changes in the regulatory environment have a measurable impact on operations: 38% of fiat-supporting service providers have closed a location as a result of regulatory actions. However, overall changes in the regulatory environment appear to have a greater impact on encouraging location openings rather than causing closures.

IT Security

- With more than \$1.5 billion stolen from cryptoasset exchanges and storage providers alone to date, IT security has become a crucial operational aspect: specialised storage providers take the highest security precautions of all surveyed firms and dedicate the largest headcount and budget share to IT security of all firms.
- Providing regular training programmes for staff has become a common industry standard as a substantial number of breaches have been caused by employee wrongdoing and/or negligence.
- We observe a lack of transparency on both external and internal security audits: more than 80% of firms do not publicly share information about security audits, indicating a general unwillingness to divulge security-critical information.



Mining Segment

- Miners' concerns about the three main types of mining concentration (control over hashpower, geographic distribution of hashpower, and the geographic distribution of hardware manufacturing) have grown in 2017.
- China remains in the top-3 countries to host mining farms; but the USA and Canada have witnessed a rapid growth of mining farm openings over the past year, often associated with the availability of cheap hydroelectric power.
- Access to high-volume and low-cost electricity as well as stable political and friendly regulatory environments are the major determining factors for hashers to choose an operational location.
- Over half of identified mining facilities, weighted by megawatts of electricity consumed, have some share of renewable energy as part of their total energy mix. An increasing number of hashing facilities are moving to regions with abundant low-cost electricity generated by hydroelectric power.
- Whilst many miners acknowledge the issue of environmental impact of PoW, most would not advocate for switching to a new, less resource-intensive consensus algorithm.
- The total number and geographic distribution of mining pools greatly varies from one cryptoasset to another. While a third of surveyed pools are fully controlled by a single person, past events show that low switching costs keep a check on operator behaviour.
- A small share of pool members provides the majority of total pool hashpower: on average, the top-10% of users contribute 68% of the pool's hashrate (top-1% contributes one third of pool hashpower).
- ASIC mining hardware manufacturing is dominated by a few producers; Ethash, SHA-256 and Equihash are the most supported mining algorithms.

Future Outlook

- The trend towards increased multi-coin support is likely to continue: all single-coin storage providers plan to support more cryptoassets in the near future.
- Innovations in trust-minimised off-chain payment networks ("layer-2 solutions" such as Bitcoin's Lightning Network) are thought to have the largest impact on service providers' business models and operations.
- Storage providers and multi-segment firms see stablecoins as a business-enhancing opportunity, whereas non-fungible tokens (e.g. digital collectibles such as game items) are generally thought to have a limited impact in the coming 12 months.

METHODOLOGY

The Cambridge Centre for Alternative Finance carried out two online surveys between May and July 2018 via secure web-based questionnaires. The *Cryptoasset Service Providers Survey* was directed at organisations operating in one or more segments of the cryptoasset industry as defined by our taxonomy (specifically exchange, storage and payments), whereas the *Cryptoasset Mining Survey* targeted both organisations and individuals involved in mining activities.¹

The research team used various channels to disseminate the surveys globally in order to gather a representative sample of the industry geographic dispersion. Both surveys were available in English, Chinese, Spanish, and Korean. Surveys were distributed directly via email invitations to industry contacts, as well as indirectly by sharing public links on social networks (e.g. Twitter, LinkedIn) and Internet forums (e.g. Reddit, Bitcointalk). The research team also partnered with several national cryptoasset associations to advance survey dissemination locally. The collected data was encrypted and safely stored, accessible only to the authors of this study. All individual company-specific data was anonymised and analysed in aggregate by industry segment, organisation size, supported assets, custody types, and region.

Data was collected from more than 180 entities globally across 47 countries

For cases in which currently active major companies did not contribute to our study, the dataset was supplemented with additional desktop research and web scraping using commonly applied methodologies. Furthermore, publicly available data from a variety of sources was used to complement survey data.

In total, survey data was collected from more than 180 entities across 47 countries and five world regions: 127 firms participated in the *Cryptoasset Service Providers Survey* and 57 entities (22 organisations and 35 individuals) completed the *Cryptoasset Mining Survey*.² Follow-up phone calls or emails were used to clarify survey responses if needed, with further quality assurance provided by comparing results to available public data if feasible.

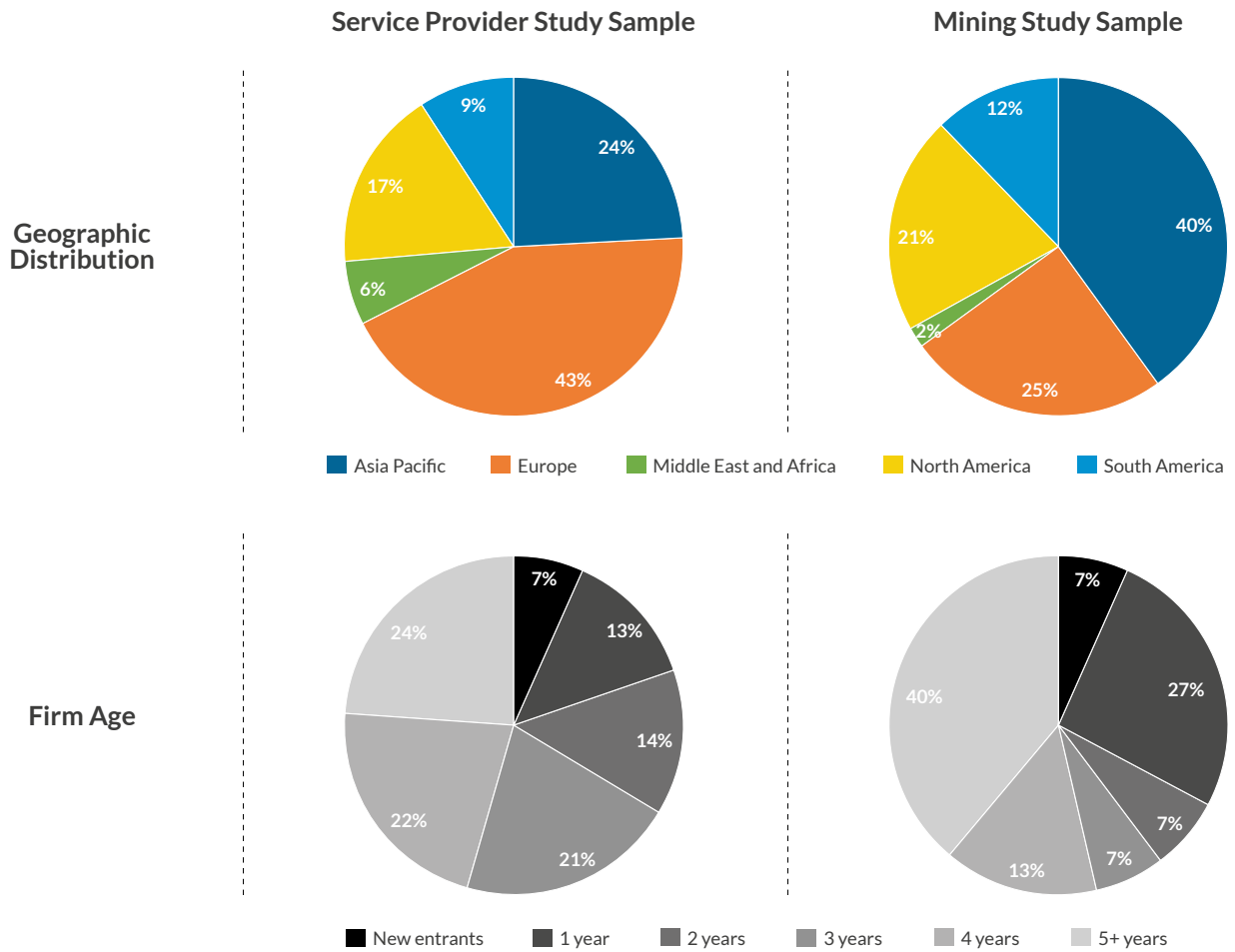
We estimate that our benchmarking study captures more than 75% of the global economic activity in the four cryptoasset industry segments covered in this report

Figure 1 provides a breakdown of survey participants by geographic region and firm age for each dataset. Both samples reflect the global nature of the industry and incorporate a mix of new entrants and incumbent firms. It is worth noting that the Bitcoin white paper was posted online just 10 years ago, with the first large Bitcoin businesses established only 8 years ago: any firm 5 years or older has been in existence for nearly the entirety of the life of the cryptoasset industry.

¹ Other segments of the industry (e.g. Initial Coin Offerings/ICOs) are not covered by this analysis. All data points presented in the following pages will be based on survey data, unless explicitly stated otherwise.

² This represents an increase of 36 firms relative to the 2017 benchmarking survey. While the survey sample represents less than 25% of all identified entities in the four segments, we estimate that the study captures 75% of economic activity in the industry.

Figure 1: The organisations in this study sample represent both industry veterans and new entrants from around the world



Note: individual miners have been removed from the firm age calculation in the mining sample.

European companies dominate the service provider study sample, while individuals and mining organisations based in Asia-Pacific take 40% of the mining study sample. Relative to last year, the survey received more responses from each region, with firms from South America as well as the Middle East and Africa (MEA) representing a small but growing share of respondents in both mining and service providers.³ Some respondents expressed their reluctance to participate in the study because of changes in their immediate regulatory environment.

³ We only provide geographic breakdown of results if it does not compromise survey anonymity.



Classification Terminology:

- **Large firms:** entities with 40 or more full-time equivalent employees.⁴
- **Cryptoasset-only firms:** entities that exclusively handle cryptoassets.
- **Fiat-supporting firms:** entities that handle both cryptoassets and fiat currencies.
- **Multi-segment firms:** entities that operate in multiple industry segments.
- **Custodians:** entities that keep customer funds in custody.
- **Non-custodians:** entities that do not keep control of customer funds.

⁴ An exception has been made for mining organisations, where FTE size is a less important indicator of relative economic influence and position within the segment. Large and small miners are differentiated based on considerations of their hashpower, importance to the ecosystem, or reputational prominence.

SETTING THE SCENE

Focus on the Data Layer

The recently published study *Distributed Ledger Technology Systems: A Conceptual Framework* laid the foundation for a comprehensive framework and terminology for the cryptoasset, blockchain and distributed ledger technology (DLT) fields.⁵ It introduces a conceptual framework that divides a given DLT system into a set of three layers: *protocol*, *network*, and *data*.

The primary focus of this study will be on the intermediaries (service providers and miners) that interact with the *data layer*.⁶ This includes cryptocurrencies that play an essential role in the incentive design of their respective DLT system as well as tokens that grant their holder with the right to access specific functionalities of applications runnings on an existing DLT system.



From Cryptocurrencies to Cryptoassets

The astute reader may have noticed that this year's edition of the study uses the term *cryptoasset* rather than *cryptocurrency* in the title. 2017 has seen a tremendous explosion in the number of tokens that have been issued on top of existing platforms rather than coming with their own, custom distributed ledger. This trend requires expanding the vocabulary to move the discussion from cryptocurrencies to the broader term of cryptoassets, which appears to have become the commonly-accepted umbrella term when referring to the ensemble of (public) blockchain-based tokens, including cryptocurrencies.

The study will provide an empirical analysis of the four key cryptoasset industry segments (mining, exchange, storage, and payments). The report will only sporadically touch on the underlying protocol and network layers.

The Year in Review

During 2017, the total cryptoasset market capitalisation climbed from \$18 billion in January to a staggering \$600 billion in December, raising questions about the cryptoasset market as a whole being a giant bubble.⁷ The desire to be an early investor in “the next Bitcoin” further fueled speculative investment. However, prices across the entire cryptoasset ecosystem started to tumble in January 2018, moving downwards uniformly across all cryptoassets. Despite a few rebounds in early 2018, the price decline has continued throughout the year and resulted in the evaporation of more than \$600 billion of market capitalisation.⁸

- 5 The study, authored by an interdisciplinary team of academics and industry experts, was published in September 2018: Rauchs, M., Glidden, A., Gordon, B., Pieters, G., Recanatini, M., Rostand, F., Vagneur, K., and Zhang, B. (2018) *Distributed Ledger Technology Systems: A Conceptual Framework*. Available at: <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/distributed-ledger-technology-systems/> [Accessed: 02 December 2018].
- 6 The data layer covers the nature and meaning of the final records produced by the DLT system. In the case of open, public, and permissionless systems, these records primarily refer to the creation, transfer, and “destruction” of native cryptoassets.
- 7 The term “market bubble” generally refers to a situation where assets are traded at prices that substantially exceed their fundamental value. In the case of cryptoassets, the definition of a fundamental value is both difficult and controversial to define and determine.
- 8 Market capitalisation as a measure of network value is incomplete and relatively easy to manipulate. It thus bears the question how much of the \$600 billion in lost market capitalisation had been “real” gains in the first place.

The rapid increase in Bitcoin prices spilled over to other cryptoassets and brought both sustained media attention and new speculative investors (retail and institutional). The entry of traditional financial services firms into the cryptoasset market and new offerings such as Bitcoin futures, specialised custody solutions, and dedicated cryptoasset hedge funds further fuelled the expansion of the industry. However, this also brought with it increased regulatory attention.

Tokens became more popular in the ecosystem as well, primarily driven by the wide adoption of the ERC-20 standard on the Ethereum network and the resulting proliferation of Initial Coin Offerings (ICOs). This led to a boom in token-based fundraising and a flurry of ICO activities globally. Blockchain forks⁹ also became more common in 2017, further increasing the number of offerings in the cryptoasset ecosystem by splitting existing coins into separate cryptoassets.¹⁰ The increase in interest – and subsequent usage – brought into the foreground limitations of base layer scaling and led to the launch of so-called “layer-2 solutions”, such as the eagerly-awaited Lightning Network on Bitcoin.¹¹

These developments have left a mark on industry actors: according to data collected from survey participants in both 2017 and 2018, their views on various topics have changed considerably. Particularly operational risks are perceived to have significantly increased: exchange operators consider all listed risk factors more urgent in 2018 than the year before, whereas miners also tend to be faced with increasing challenges (Tables 6 and 9 in Appendix).

9 A hard fork constitutes a controversial change to the protocol rules of a DLT system that causes the network to split into two separate systems, each having their own cryptoasset.

10 Bitcoin alone had at least eleven known hard forks in 2017: Bitcoin Cash, Bitcoin Gold, Bitcoin Diamond, Super Bitcoin, Bitcoin Platinum, Lightning Bitcoin, Bitcoin God, Bitcoin Uranium, Bitcoin Cash Plus, Bitcoin Silver, and Bitcoin Atom. Most of these forks have seen negligible activity and adoption.

11 During the height of the boom, the Bitcoin blockchain experienced significant delays in processing transactions, with average fees rising to levels above \$50. Similarly, the Ethereum blockchain was clogged for a few days because of a single gaming application that suddenly became popular (CryptoKitties). Layer-2 solutions refer to a variety of techniques that aim to materially increase transaction speed and throughput as well as substantially decrease transaction costs by moving payments off-chain in a trust-minimised manner.

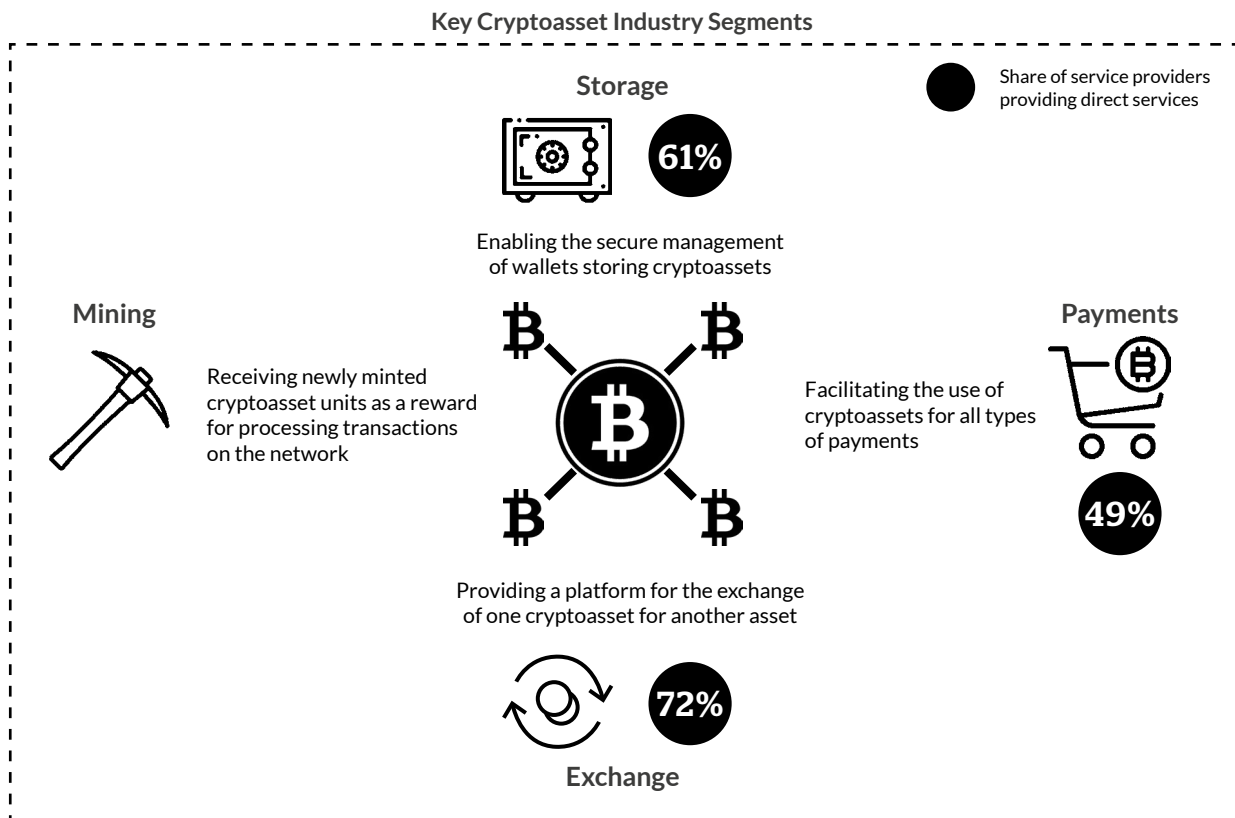
SECTION 1: THE CRYPTOASSET INDUSTRY

1.1 Segments

Industry Structure

In the ten years since the publication of the Bitcoin whitepaper, an entire industry has evolved around cryptoasset systems to build and maintain basic infrastructure as well as to facilitate the use of the platforms and their assets. While there are several smaller segments comprising a great variety of additional services such as blockchain analytics, data, and ICO services, this study will limit its focus to four key industry segments: mining, storage, exchange, and payments (Figure 2).

Figure 2: The cryptoasset industry can be broken down into four key segments



Note: firms can operate in multiple segments.

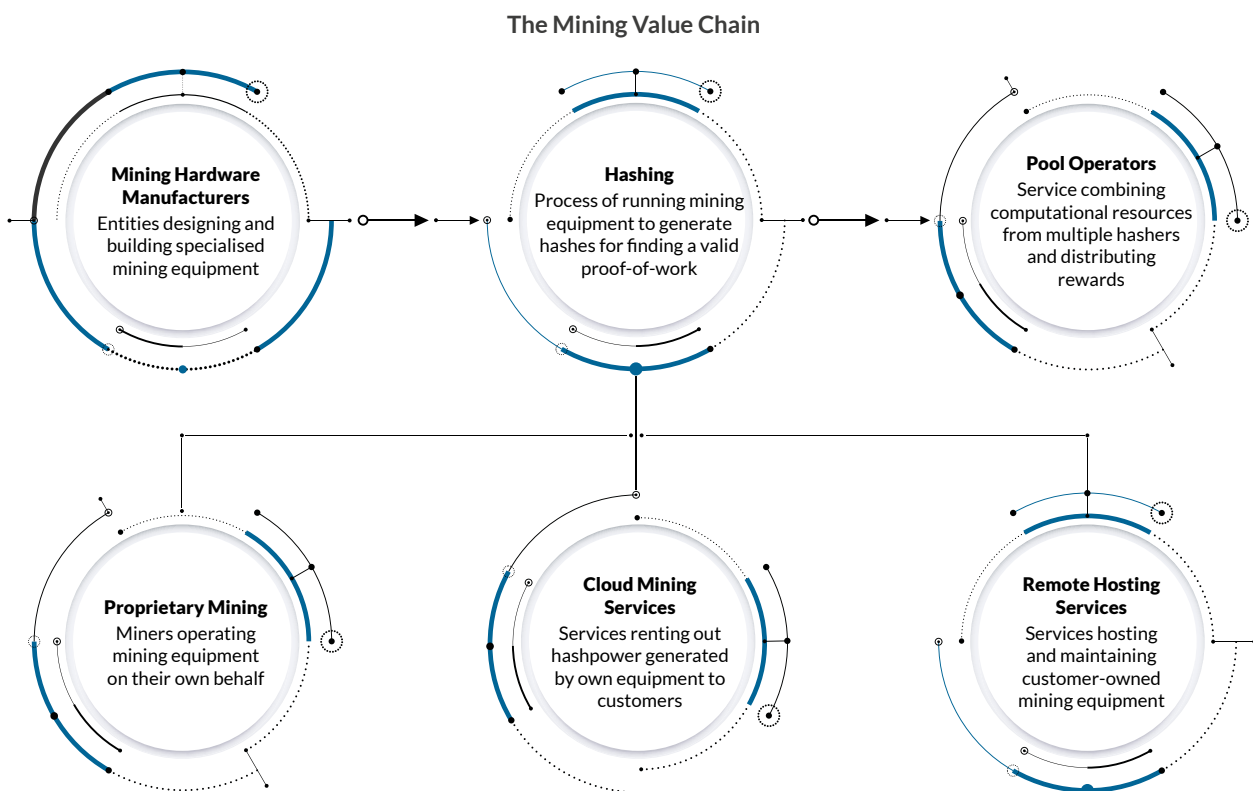
The study further distinguishes between direct and outsourced services. Most entities are providing direct services in the exchange segment (72%), followed by storage (61%) and payments (49%) segment.

In some cases, service providers partner with a third party to outsource specific activities – often those that belong to a different segment. For instance, a storage provider may decide to partner with a third-party exchange to offer in-wallet purchases and sales of cryptoassets. In such instance, the third party is responsible for providing the exchange services – and consequently for abiding by applicable regulations as well. Among respondents, 12% of exchanges, 17% of storage providers, and 23% of payment service providers are contracting out to an external party. The remainder of the report focuses on entities only providing direct services.

Mining Segment

The mining segment comprises agents performing specific operations for the processing of public blockchain transactions (Figure 3). During this process, new units of a specific cryptoasset can be created.

Figure 3: Miners operate across a sophisticated value chain of distinct activities



The majority of mining organisations tend to specialise in a specific activity (46% of small miners and 56% of large miners). In contrast, a small number of large firms have pursued a continuous vertical integration strategy that covers the entire value chain. Large firms tend to be older, whereas the majority of individuals and half of small miners in the sample are new entrants.

Note: Section 7 covers the cryptoasset mining segment in greater detail.

Storage Segment

Cryptoassets can be moved by signing transactions using private keys – these keys are stored using wallet softwares. Initially, wallets were simple software programs handling key management, but they have evolved over time to support a variety of technical and commercial services. Many solutions provide an easy-to-use interface for the end-user that abstracts away the complexity of key management.

Figure 4: Mobile wallets remain the most supported format; web wallet support has significantly increased

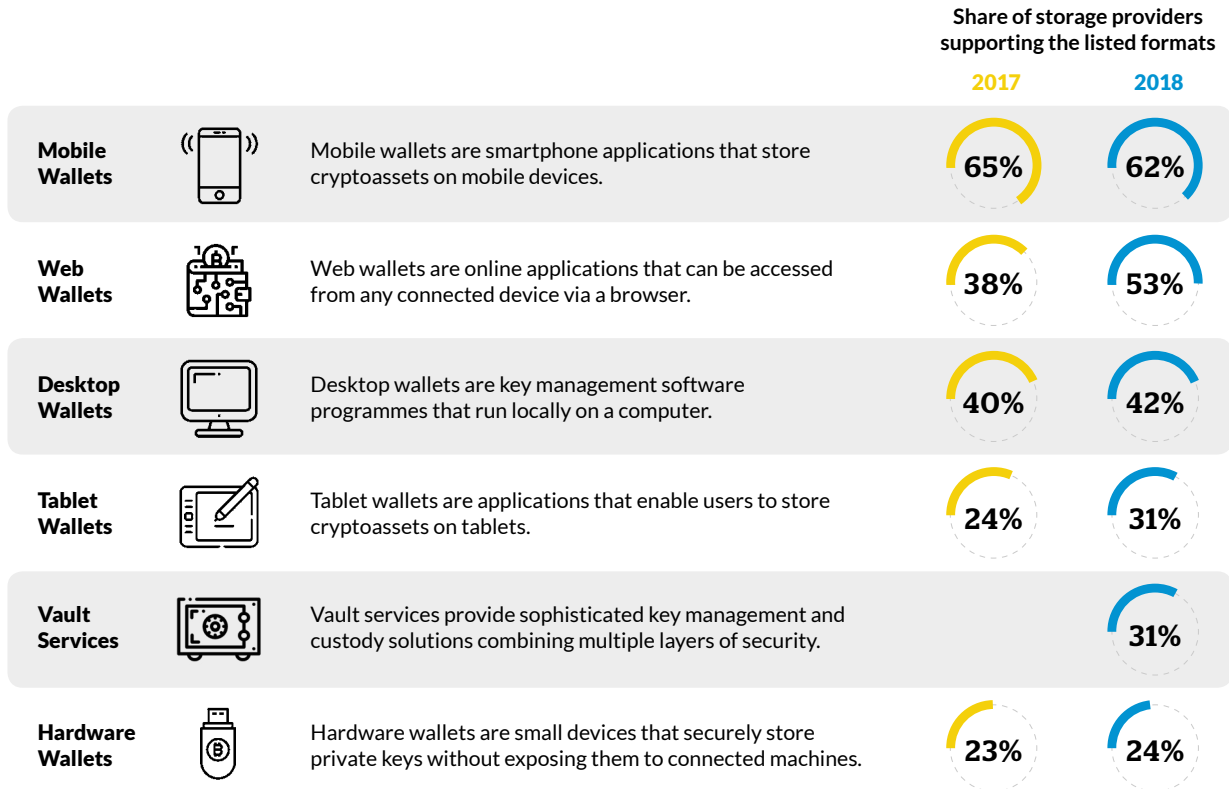


Figure 4 shows the evolution of wallet options between 2017 and the second quarter of 2018. Mobile and web wallets are the most widely offered storage formats, though cold-storage vault services have gained in popularity in late 2017 with the influx of institutional investors, such as hedge funds. No storage format has seen a decrease in support in 2018, indicating that the various forms of storage options are not yet cannibalising each other.

Large storage providers support an average of three of the above types, compared to an average of two types supported by small wallet providers. Storage-only service providers are more likely to specialise in a particular activity, as opposed to multi-segment entities that often support multiple wallet formats.

Note: more detailed information on cryptoasset storage and custody is available in Section 4.

Exchange Segment

Exchanges serve as on-off ramps for users to buy and sell cryptoassets - either in exchange for fiat currency (“fiat-supporting”), another cryptoasset (“cryptoasset-only”), or other assets such as gold. There are a variety of activities in the exchange segment that facilitate trade in different ways.

Figure 5: Brokerage services, order-book exchanges, and over-the-counter (OTC) trading desks are the three major activities performed in the exchange segment.

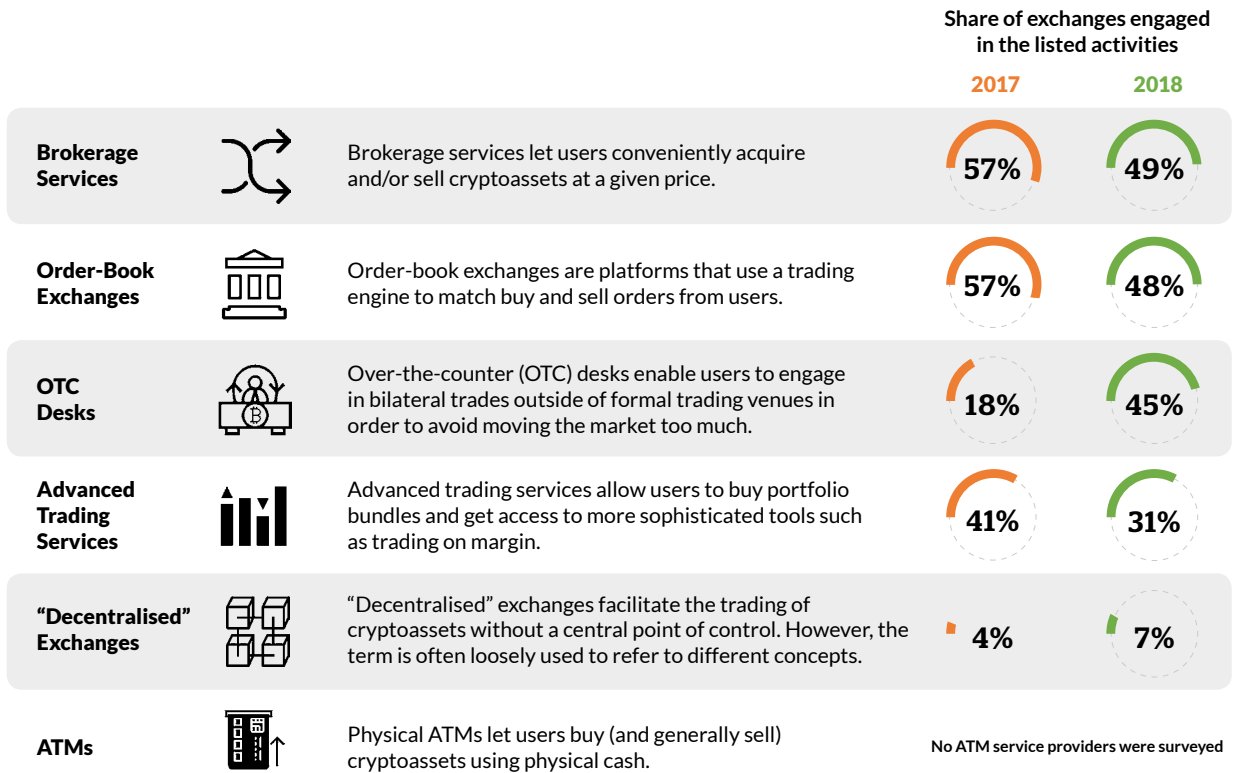


Figure 5 shows that brokerage services, order-book exchanges, and OTC desks are offered by almost half of all exchanges, with OTC desks greatly increasing in popularity since 2017. Exchanges exclusively engaged in a single activity are primarily providing order-book exchange services, brokerage services, or OTC trading desks.

“Decentralised” exchanges continue to be a small, but growing, share of exchanges. While 7% of respondents claimed to be decentralised - or P2P - exchanges, definitions of a decentralised exchange vary widely: it is hence possible that the growth reflects a change in definition, rather than a true increase in decentralised exchanges. Their rise in popularity may explain why surveyed P2P exchanges are a lot more concerned about competition than centralised exchanges.



Decentralised Exchanges (DEX) Rise in Popularity

Most exchanges are centralised businesses with dedicated operators, and therefore more easily subject to regulations unlike direct peer-to-peer, blockchain-based trades. More recently a number of “decentralised exchanges” (or DEXes) have emerged, promising to provide a decentralised and trust-minimised alternative to traditional third-party exchanges.

However, at present nearly all existing exchanges labelling themselves as DEX rely on some degree of centralised control over certain exchange processes (e.g. order matching) which raises questions whether they can claim to be “decentralised”.¹² **Table 1** deconstructs exchange processes into three categories to classify the four exchange types.

Table 1: Decomposing exchange types - from custodial exchanges to DEXes

EXCHANGE TYPE	1. CUSTODY OF FUNDS	2. ORDER MATCHING	3. CLEARING & SETTLEMENT
a. Custodial	Exchange	Exchange	Exchange
b. Non-custodial	Users	Exchange	Exchange
c. P2P	Users/ Exchange	Users/ Blockchain	Exchange
d. DEX	Users	Blockchain	Blockchain

Most self-labelled “DEXes” would be considered *non-custodial exchanges* (users retain full control over their funds, but the exchange handles order matching and/or clearing and settlement centrally) or *P2P exchanges* (primarily provide a flexible user matching platform where users can decide whether to store funds at the exchange and perform the actual trade outside of the platform).

In contrast, a true DEX uses a public blockchain for both order matching as well as clearing and settlement while allowing users to maintain control of their funds for the entirety of the trading process. While a DEX may pose a challenge for regulators, it is worth noting that current implementations are cumbersome, expensive, and inefficient as they require multiple on-chain transactions for a single exchange trade.

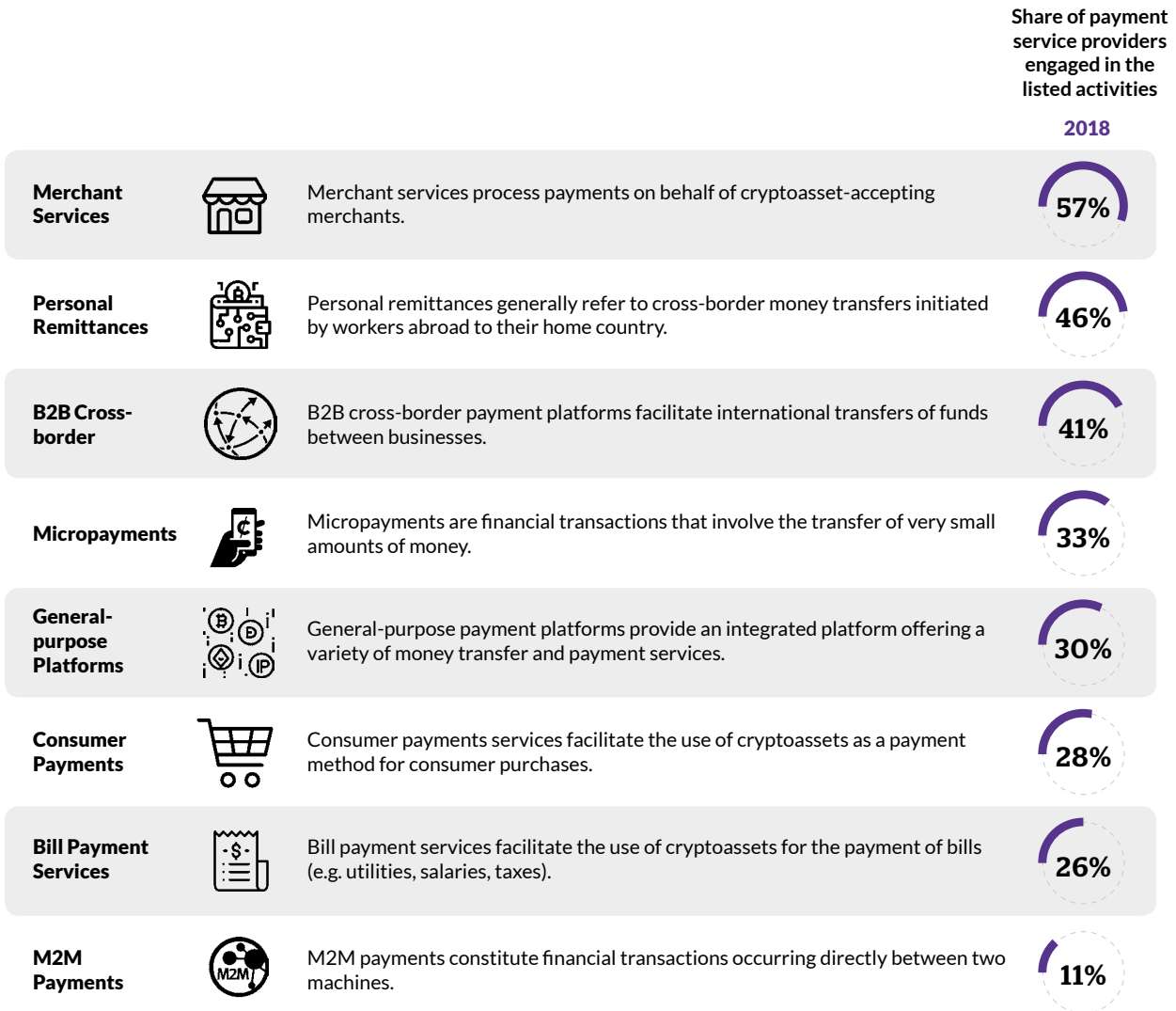
Of the surveyed exchanges, 41% are involved in only a single activity, while 59% are involved in two activities or more. No respondent engages in more than four activities. Large exchanges tend to be engaged in more activities than small exchanges (75% in two activities or more).

¹² For a discussion on the multi-dimensional concept of “decentralisation”, please see p. 44 of the *Distributed Ledger Technology Systems: A Conceptual Framework* report. Available at: <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/distributed-ledger-technology-systems/> [Accessed: 02 December 2018].

Payments Segment

Payment service providers act as gateways to facilitate the use of cryptoassets for payments of all kinds (Figure 6). To this end, the cryptoasset payments segment is composed of a variety of activities that target different payment and user types.

Figure 6: Merchant services remain the most popular activity in the payments sector



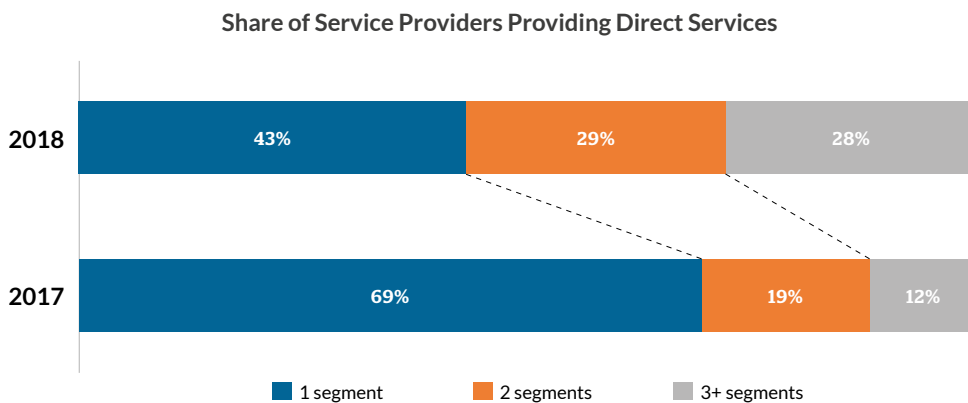
Note: comparison with 2017 data is not possible given changes in activity classifications.

Large payment companies on average engage in three payment activities, while small providers engage in two. Merchant services are the most popular payment activity, increasing slightly from 52% in 2017 to 57% in 2018. Cross-border flows (personal remittances and B2B transfers) are the next two most popular services, with the number of payment providers supporting B2B payments more than doubling from 19% in 2017 to 41% in 2018.

Horizontal Expansion: The Growth of Multi-Segment Firms

The lines between exchange, storage, and payments service segments have become increasingly blurred: in 2017, 69% of surveyed service providers (excluding miners) were active in a single segment, as opposed to 43% of service providers in 2018 (Figure 7). This change has come from firms expanding their offerings across the different segments, and usually not from mergers between two horizontal firms.

Figure 7: The shift towards multi-segment operations continues - more than half of service providers are operating across two or more segments



Note: this chart does not include mining companies, as these - with a few exceptions - generally tend to focus exclusively on the mining segment.

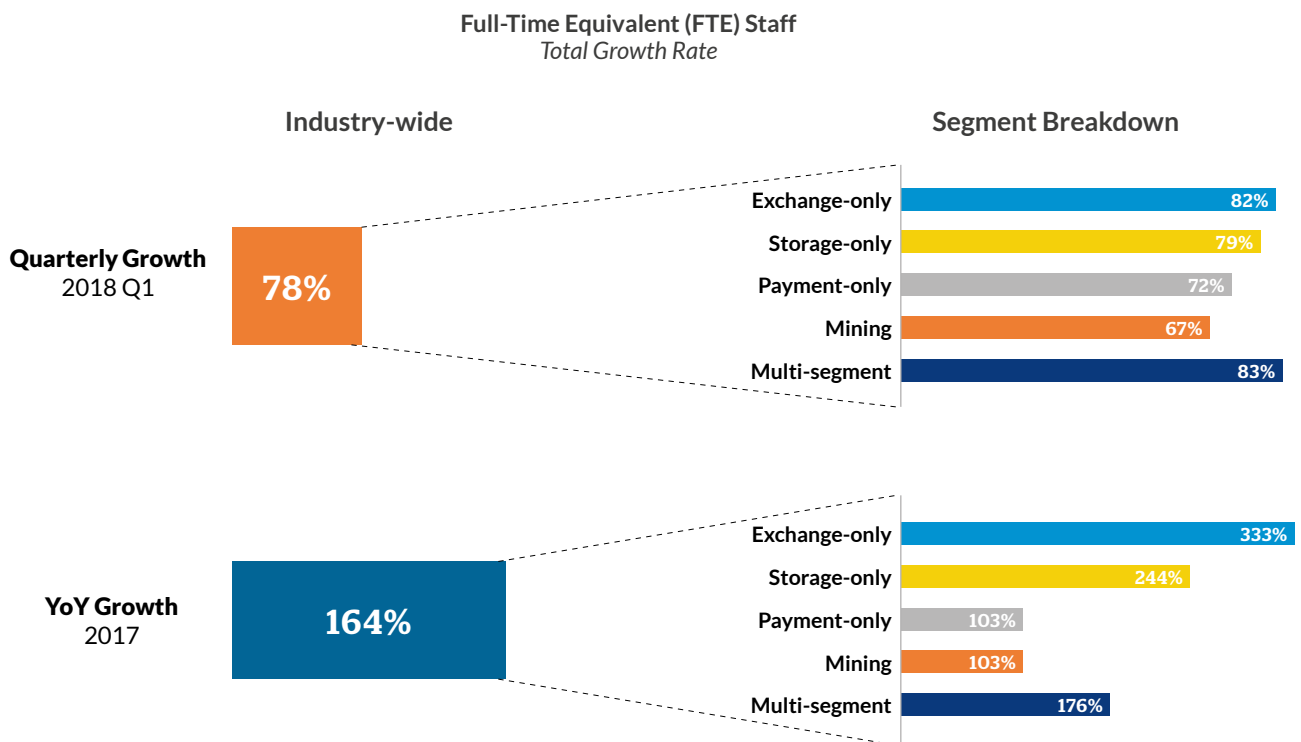
Large firms are more likely to operate across two or more segments, with 69% of large firms reporting they do, compared with approximately half of small firms. The survey has insufficient data to determine whether the firms are large because they are engaging with multiple segments, or whether reaching a certain size grants the firm sufficient resources to operate across different segments and diversify activities. Similarly, it is unclear whether firms are attempting to becoming a “one-stop shop” for cryptoasset users, or whether the expansion is a move to provide more revenue streams to survive frequent industry downturns.

1.2 Industry Growth

The evolution of the total number of full-time equivalent (FTE) employees represents a good proxy for assessing total industry growth. According to [Figure 8](#), total industry headcount has grown by 164% in 2017, an expansion primarily driven by the exchange and storage segments.

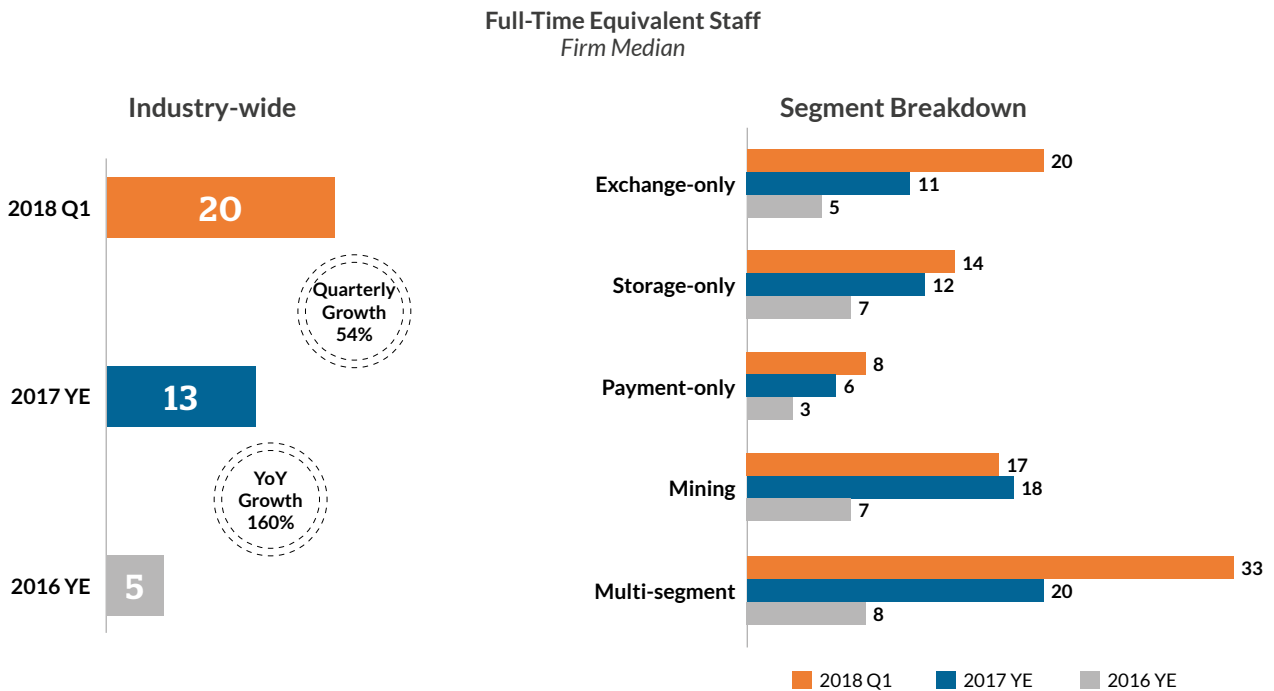
Quarterly FTE staff growth in 2018 Q1 amounted to a staggering 78%: the accumulating backlog of customer onboarding and support requests, the need for compliance staff to navigate the complex landscape, engineers to make the platforms fit for drastic increase in traffic and usage, as well as salespeople to onboard new clients are potential drivers of the segment job growth.

Figure 8: Industry growth in 2017 appears to be primarily driven by the exchange and storage segments



Organisations, including miners, more than doubled in size during the boom year of 2017 (Figure 9). Despite the global market crash at the beginning of the first quarter of 2018, firms in the sample have continued to grow, with the median firm size increasing to 20 employees working exclusively on cryptoassets, up from 13 at the end of 2017 (54% quarterly FTE growth). The job boom resulted in a reported shortage of talent: the majority of surveyed exchanges reported concerns over good access to talent. While the survey results were collected in May -- five months after the price collapse -- it is possible that the sustained nature of the market crash has resulted in layoffs that are only beginning to be realised now.

Figure 9: Organisations have also considerably grown in size - the typical miner has experienced the highest growth in 2017



Increasing prices in the second half of 2017 meant that cryptoasset mining became more profitable for a certain period before the difficulty adjustments kicked in: higher profitability resulted in mining firms growing the most in size over 2017 (157% year-on-year growth), then slowing considerably in 2018 Q1. Instead, firms specialising exclusively in the exchange segment took the lead in the first quarter of 2018, with their median staff number growing by 82%.¹³ Service providers operating in multiple segments have become the largest firms in terms of total employee headcount since 2017 and experienced the second-highest FTE staff growth rates, with 65% year-on-year growth in 2017 and a quarterly growth of 150% in 2018 Q1.

FTE figures widely vary between companies: the number of employees can range from one person to several hundred, with one company employing more than 2,500 staff. No major differences can be observed in terms of FTE growth rates between incumbent firms and newly-entered firms.

Overall, the market appears to be stable to price shocks; indicating that while cryptoassets may be volatile, the economic employment generated by the cryptoasset industry is not. However, it may also be too soon for the effect of the price decline on employment to be reflected in the data.

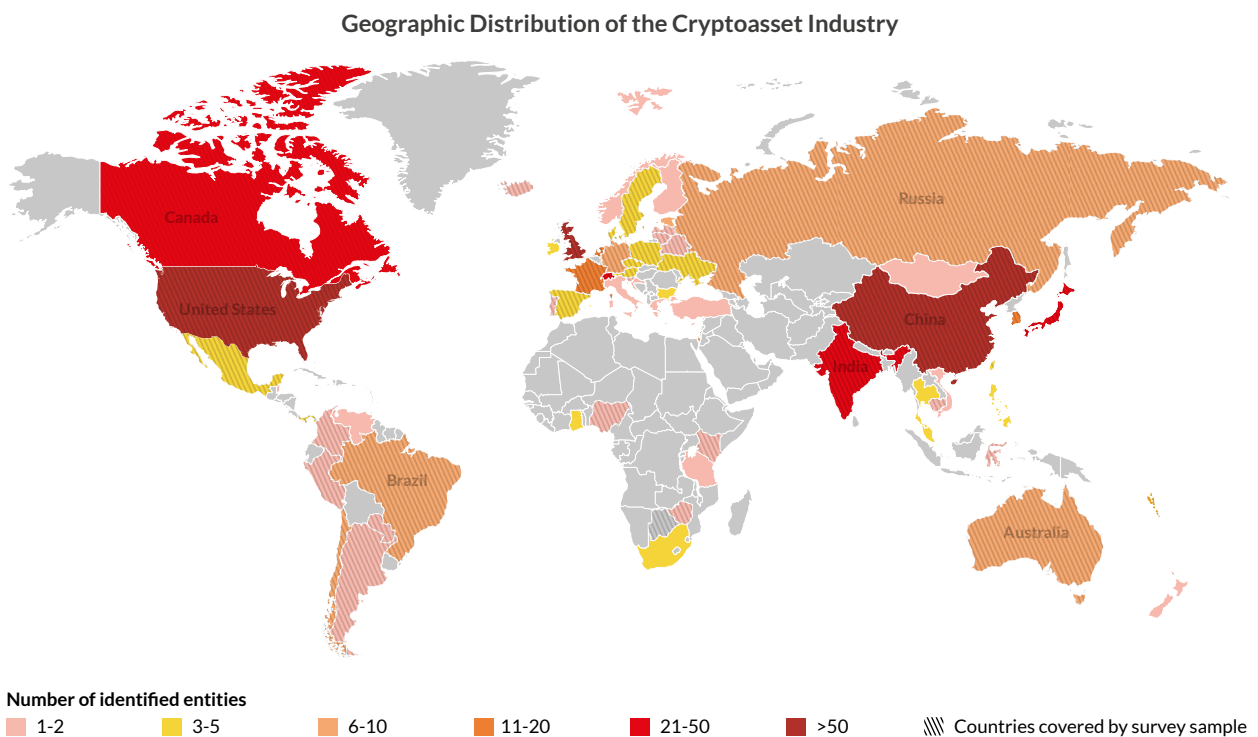
¹³ Figures are significantly lower for other segments, with 17% and 33% FTE staff growth for storage-only and payment-only companies, respectively.

1.3 Geography

A Global Industry

The research team gathered supplementary data on headquarters of 561 companies active in at least one of the four major cryptoasset industry segments. **Figure 10** shows that the distribution of the global cryptoasset industry is geographically uneven with high concentration of headquartered entities in countries such as the USA, China, Japan, India, Canada, and the UK.

Figure 10: While global in nature, the cryptoasset industry is primarily driven by companies based in North America, China, India, and Western Europe



Note: this map is based on operational HQ data from 561 companies active in at least one of the four major cryptoasset industry segments. Colours represent the total number of identified entities from each country; stripes indicate when a country is also covered by our study sample.

Legal Headquarters and Operations

Given the inherent cross-border nature of cryptoasset market activities, it is not uncommon for cryptoasset entities to have operating activities in one country whilst being legally registered in another. The average large entity maintains offices in three countries, compared to an average of two countries for smaller entities. Multi-segment firms own and operate offices and facilities in more countries on average than specialised companies.

The majority of surveyed companies have their operational headquarters and legal headquarters in the same country: across the sample, slightly less than a quarter of firms (21%) have their legal HQ based in a different country to their operating HQ. These results vary across industry segments: 22% of surveyed service providers have their legal HQ in a different country, while only 14% of mining companies have a legal HQ in a different country from their main operations.

Even if companies locate part of their activities in different countries, they may not necessarily move to a new geographic region. Only 12% of service providers have their legal HQ in a different geographic region; a situation that is even less common for surveyed mining companies (9%). Entities registered in Europe appear to be ‘regional’, with facilities and offices being mainly based in Europe. Companies registered in North America are ‘cross-regional’, with offices and facilities often located in multiple regions.

The majority of industry actors have both operational and legal headquarters in the same country

This finding suggests that cryptoasset entities are more ‘grounded’ than previously thought: they are more likely to operate in countries where they are legally registered - perhaps due to greater familiarity with local regulatory structures - instead of looking for the most permissive legal environment. However, focused regulatory attention increased during the latter half of 2017, therefore “regulatory arbitrage” of legal and operational headquarters might be an emerging trend within the industry that would not have been fully captured by the present study.

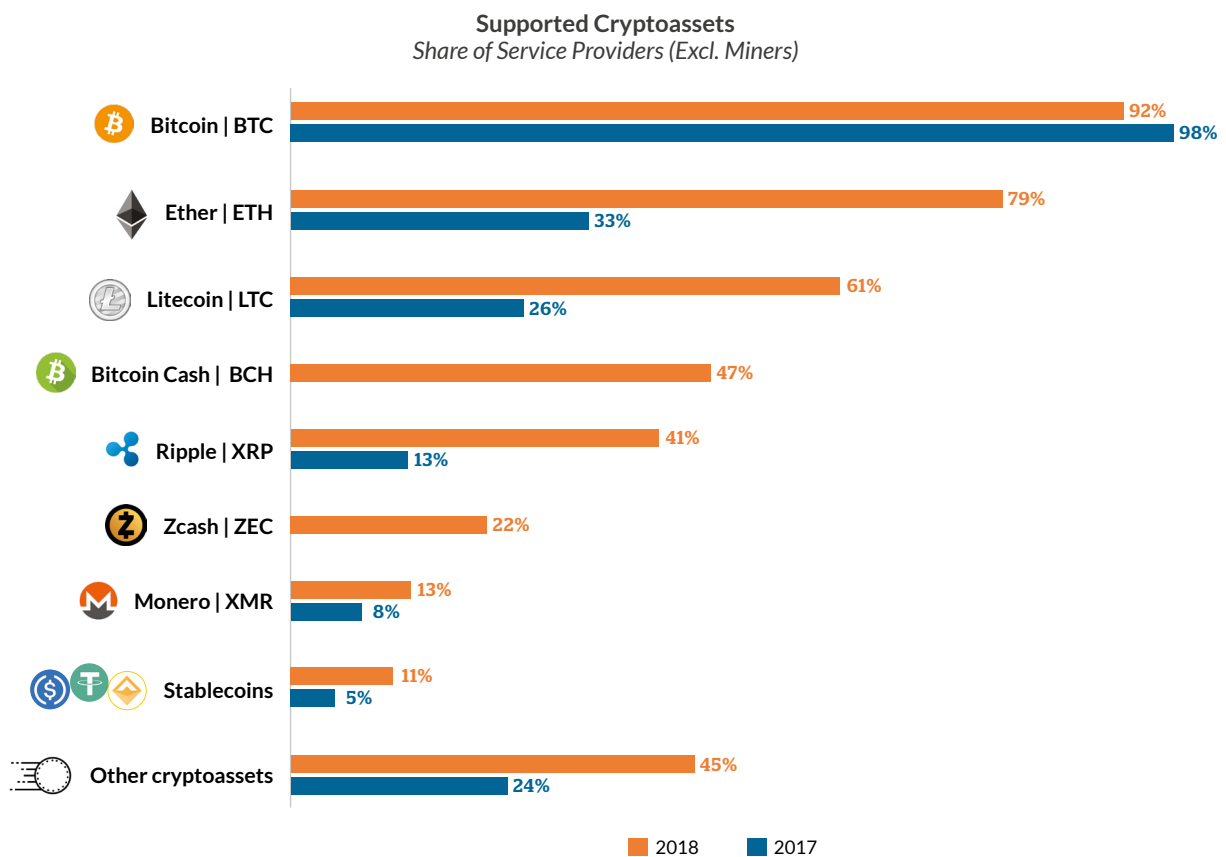
Note: more detailed information on regulation and compliance is available in Section 5.

SECTION 2: GLOBAL USAGE

2.1 Towards a Multi-Coin Universe

2017 saw explosive growth in the total number of cryptoassets. The selected major non-Bitcoin cryptoassets all received increased support among surveyed service providers over 2018 (Figure 11). The slight decline in bitcoin (BTC) support can be explained by the emergence of dedicated services for specific cryptoassets. Privacy-focused coins such as zcash (ZEC) and monero (XMR) have grown in popularity, yet still seem to occupy a niche.

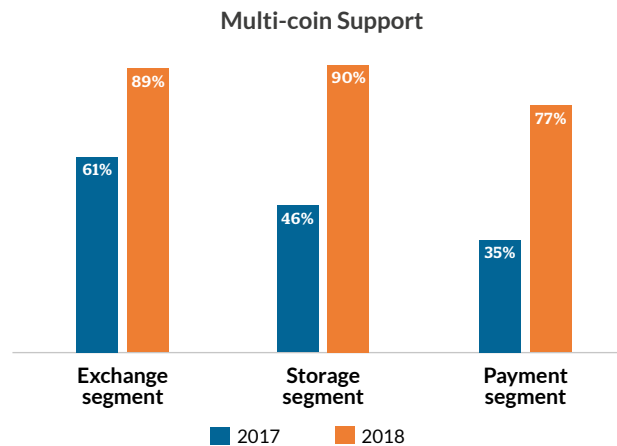
Figure 11: Service provider support for the major cryptoassets has broadened



We observe differences between industry segments: for instance, bitcoin cash (BCH) is supported by 77% of storage-only providers, but only 18% of payment-only companies and 22% of specialised exchanges. This fact highlights that many cryptoassets have not yet been adopted into broader use (e.g. consumer and cross-border payments).

Several interpretations co-exist to explain the increase in number of supported coins: the rise of ERC-20 tokens, fuelled by ICOs and their subsequent listing on exchanges, as well as the growing number of blockchain forks and airdrops are possible supply-side drivers. Meanwhile, tokens catering to niche interests as well as speculation on price appreciation rather than native application usage increase the demand for multiple coins.

Figure 12: Multi-coin support has nearly doubled from 47% in 2017 to 84% in 2018 across the industry



In contrast to 2017, the vast majority of service providers are multi-coin-oriented today (Figure 12). Surveyed storage providers have considerably expanded their cryptoasset coverage since 2017: wallets with multi-coin support surged from 46% in 2017 to 90% in 2018, with 60% of wallets currently supporting more than 3 cryptoassets as opposed to only 10% in 2017. Notably, all storage-only service providers surveyed in 2018 exclusively support cryptoassets (i.e. “cryptoasset-only”).

An interesting observation is that companies specialised in payment services generally support fewer cryptoassets than firms active in other segments: the majority of payment-only service providers merely support one or two cryptoassets. In contrast, specialised exchanges support on average the broadest number of cryptoassets.

2.2 Who Is Using Cryptoassets?

Information on the numbers and characteristics of cryptoasset users is sparse, therefore the results from this survey represent a rare opportunity to gain information at the global level. A few central banks and research institutes have issued surveys trying to determine the number and activity level of cryptoasset users within their area of operation, but information is typically difficult to glean.

Cryptoasset users do not need to establish an account with a service provider in order to access and use the underlying blockchain payment systems, and until recently most entities did not require users to prove identities.¹⁴ Similarly, many users use a variety of different service providers and can thus have multiple accounts. In some cases, users try to obfuscate their location using tools such as VPN servers and the TOR network.

These factors make it difficult to provide precise estimates about the number, nature, origin, and activity levels of cryptoasset users. The following results were constructed as conservative estimates of the global cryptoasset user base, extrapolating from survey responses and publicly available data.

¹⁴ However, a growing number of service providers now require that users undergo Know Your Customer (KYC) and Anti-Money Laundering (AML) checks (see Section 5 for more information), while certain jurisdictions such as South Korea and Japan require the users to open an account at the bank the exchange has partnered with. We will refer to these users as “ID-verified users”.

Total Users

Most attempts to estimate the total number of users are piecemeal. A Bank of Canada survey in July 2018 estimated that the share of the Canadian population owning cryptoassets has nearly doubled from 2.9% in late 2016 to 5% in 2017 – the equivalent of roughly 2 million users.¹⁵ Other studies estimate that between 2% and 8% of US citizens have owned cryptoassets between the fall of 2017 and the first quarter of 2018, which would amount to between 6 and 26 million users.¹⁶

Studies in other regions report similar findings: the Japanese Financial Services Agency (FSA) estimated 3.5 million domestic cryptoasset users (roughly 3% of the population) as of March 2018,¹⁷ whereas an ING study published in June 2018 found that on average 9% of individuals in Europe own cryptoassets, although significant differences between countries exist.¹⁸

Other studies set exclusively in Europe, Canada, Japan, or the USA estimate 2-9% of the population hold cryptoassets

A naive extrapolation would then suggest that between 2% and 9% of the population of developed countries would have owned cryptoassets as of mid-2018, a figure that would amount to between 28 and 126 million unique users.¹⁹ It should be noted that this extrapolation does not include cryptoasset owners and users from developing countries, whose numbers are likely in the millions as well. However, this does not necessarily imply that the actual number of cryptoasset owners worldwide substantially exceeds the 100-million mark.²⁰ Instead, these estimates should merely serve as an indication of the potential number of users.



User Accounts Are Not (Necessarily) Equivalent to Users

The number of *users* and the number of *user accounts* are frequently conflated, even though they represent very different notions. An individual *user* can hold multiple *accounts* at any given service provider. Importantly, if a firm does not collect information on users, it may not be able to link the multiple accounts to the user if a new identity, for example a different email address, is associated with the account. Additionally, users can hold accounts at more than one service provider. It follows that there are more *user accounts* than *users*, more *users* than *ID-verified users*, and more *ID-verified users* than *unique users* who engage in the cryptoasset ecosystem.

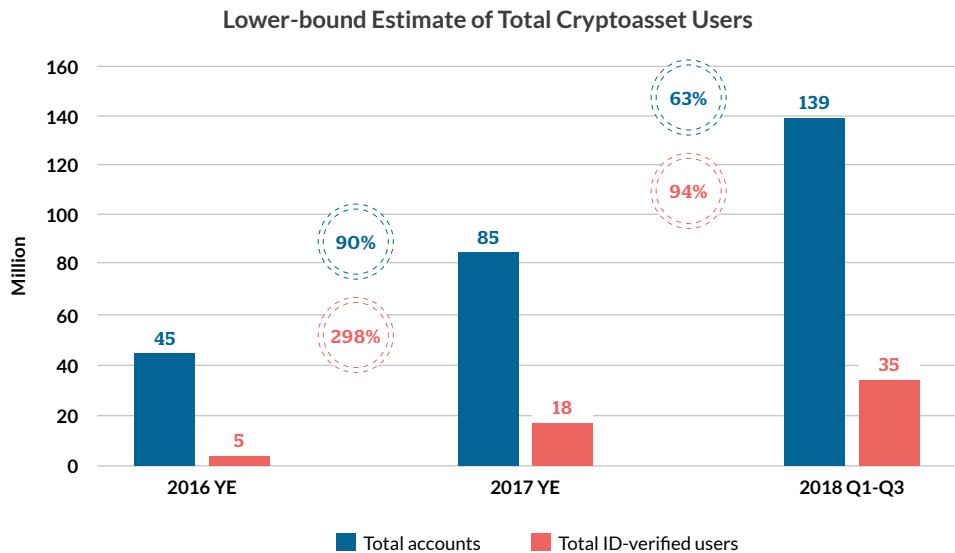
- 15 Bank of Canada (2017) *Bitcoin Awareness and Usage in Canada*. Available at: <https://www.bankofcanada.ca/wp-content/uploads/2017/12/swp2017-56.pdf> [Accessed: 28 November 2018]; and Bank of Canada (2018) *Bitcoin Awareness and Usage in Canada: An Update*. Available at: <https://www.bankofcanada.ca/wp-content/uploads/2018/07/san2018-23.pdf> [Accessed: 28 November 2018].
- 16 Blockchain Capital (2017) *Bitcoin Survey Fall 2017*. Available at: <http://www.survey.blockchain.capital/> [Accessed: 28 November 2018]; and Finder.com (2018) *Why haven't we all bought cryptocurrency yet?* Available at: <https://www.finder.com/why-people-arent-buying-cryptocurrency> [Accessed: 28 November 2018].
- 17 FSA (2018) 仮想通貨取引についての現状報告. Available at: <https://www.fsa.go.jp/news/30/singi/20180410-3.pdf> [Accessed: 28 November 2018].
- 18 ING (2018) *Cracking the Code on Cryptocurrency: Bitcoin buy-in across Europe, the USA and Australia*. Available at: https://think.ing.com/uploads/reports/ING_International_Survey_Mobile_Banking_2018.pdf [Accessed: 28 November 2018].
- 19 For the purpose of this analysis, we consider a country to be developed if it has a very high Human Development Index (HDI) score (i.e. equal to or above 0.8). This currently applies to 59 countries worldwide with an aggregate population of around 1.4 billion people.
- 20 Survey data can suffer from sample bias and be restricted to a certain geography whose context is fundamentally different than another geography, among others. As a result, simple extrapolations should always be met with a healthy dose of scepticism.

While it can be difficult to distinguish user accounts from individual users, survey data indicates that there has been a substantial increase in the proportion of ID-verified users as a share of total user accounts at service providers: while a mere 10% of total accounts could be attributed to ID-verified users in 2016, one in every four accounts has been verified as of 2018 Q1.

There has been a substantial increase in the share of ID-verified accounts: from 10% of user accounts in 2016 to 25% in 2018 Q1

Combining public data and survey findings, we estimate that the total number of user accounts at service providers amounts to at least 139 million in late 2018 (Figure 13).²¹ Using a combination of verified user data and the average share of ID-verified accounts described above, we also estimate there are currently at least 35 million ID-verified users globally.²² While several limitations of the analysis above need to be taken into account, we believe that the figures represent the lower-bound of the global cryptoasset unique user base.²³

Figure 13: Service providers currently serve at least 35 million ID-verified cryptoasset users, and the industry is still undergoing rapid growth



The analysis reveals the continued growth in the number of user accounts at service providers throughout 2017 and 2018. It also shows that KYC'ed user growth has dwarfed total user account growth, which means that new users are more likely to get immediately verified. Growth rates were at their highest in 2017, and the number of new user accounts as well as ID-verified users continued to rapidly grow in 2018 as well.

²¹ The research team collected longitudinal account and user data of both small and larger service providers from publicly available data sources such as press releases, news articles, company websites, social media, and public forums. This dataset was combined with survey data from participating platforms and projects from 47 countries.

²² When available, absolute figures of ID-verified users supplied by survey participants were aggregated for each period. The ratio of ID-verified users as a share of total accounts, calculated using survey data for each period, was then applied to the remaining total account figures. The resulting figures were eventually added together to provide an estimate of the number of ID-verified users in the ecosystem.

²³ The analysis does not capture all accounts at service providers since no data was available for some major platforms (e.g. in China) or individuals who do not use service providers. Together, these would contribute to an underestimation of total users. On the other hand, there are no easy means to identify users with accounts at multiple service providers – a practice that would contribute to an overestimation. Overall, there are reasons to believe that the underestimation factors outweigh the overestimation factors, which suggests that the current figure is a conservative lower-bound estimate.

Table 2 removes the effect of the many new entrants by only analysing the account data of firms that have been operating since 2016. All incumbent firms reported growth in the number of user accounts though there is a consistently wide range of growth reported (from 24% to 2,900%). Given this reported range, it is not surprising that the median growth is considerably lower than the average growth, but it is still very robust.

At least 139 million user accounts have been created at cryptoasset service providers, representing a minimum of 35 million ID-verified users

Consistent with the growth rates of the total accounts, firms saw higher growth rates in 2017 than 2018, and higher growth rates of ID-verified users. This indicates that increased use of KYC and AML methods in the industry also occur among established service providers who already have a substantial user base, rather than just being the result of new entrants.

Table 2: Incumbent firms have experienced massive growth in user accounts and verified users in 2017

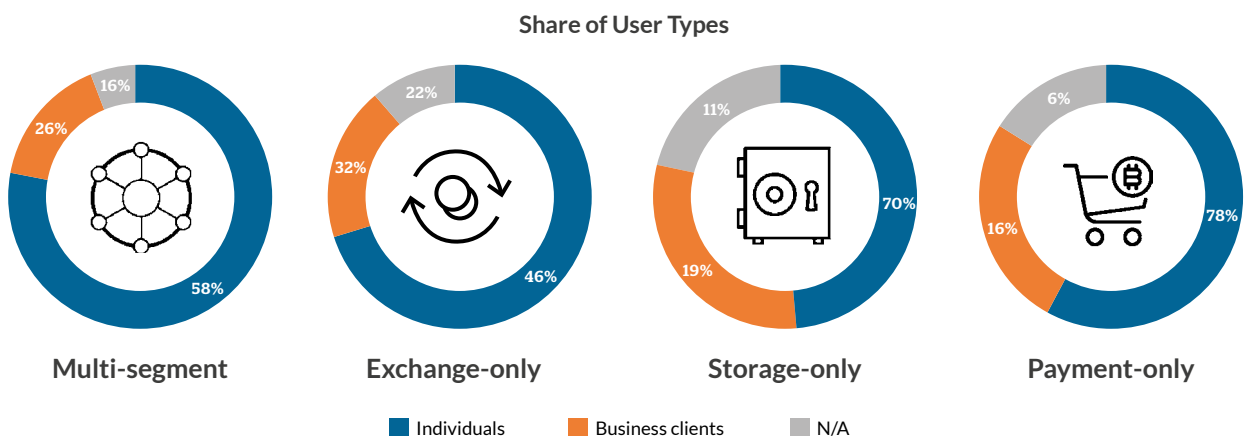
GROWTH RATES: AVERAGE (MEDIAN)		2017 YOY	2018 Q1-Q3
Average firm	Accounts	535% (233%)	161% (50%)
	ID-verified users	977% (446%)	202% (79%)
Observed range	Accounts	24% - 2,900%	4% - 2,400%
	ID-verified users	25% - 6,200%	19% -2,876%

Note: in order to avoid new entrant bias, this analysis only considers firms that have been active for the entire period of 2016-2018. Outliers reporting over 3,000% growth in accounts or more than 7,000% for ID-verified users have been removed.

User Types

Conforming with popular narratives, survey data indicates that the majority of users – both established as well as new entrants – are individuals and not business clients (**Figure 14**). Individuals can be hobbyists, retail investors, consumers, or users seeking a better investment or payment alternative. However, business clients comprise over one quarter of the users for payment-only and storage-only services, suggesting that these two segments in particular represent opportunities to provide specialised services specifically tailored for enterprises.

Figure 14: Individuals still constitute the majority of the user base of most service providers



The majority of business clients are comprised of cryptoasset hedge funds and online merchants

Multi-segment firms provide a fully-integrated suite of services that are especially popular with individuals. Among business clients, 93% of surveyed entities primarily serve hedge funds (on average 60% crypto-focused hedge funds and 40% traditional hedge funds). The second most commonly served category is merchants (86%), of which on average 63% are online merchants and 37% are brick and mortar merchants. A further 35% and 30% of service providers report venture capital firms and other institutional investors as business clients, respectively. Finally, 45% of service providers indicate having miners as business clients, whereas 30% report serving other types of cryptoasset companies.

User Activity

While some use cases (e.g. long-term investment) do not require a user to actively use a service, others such as short-term trading and frequent payments do. However, comparing active users across platforms and services is difficult because the definitions of activity vary widely—even within segments.

Weekly logins are the most popular criteria to determine user activity levels (supported by 28% of service providers), followed by monthly measures related to activities that can involve simple logins, deposits, trading, and withdrawals (26%).

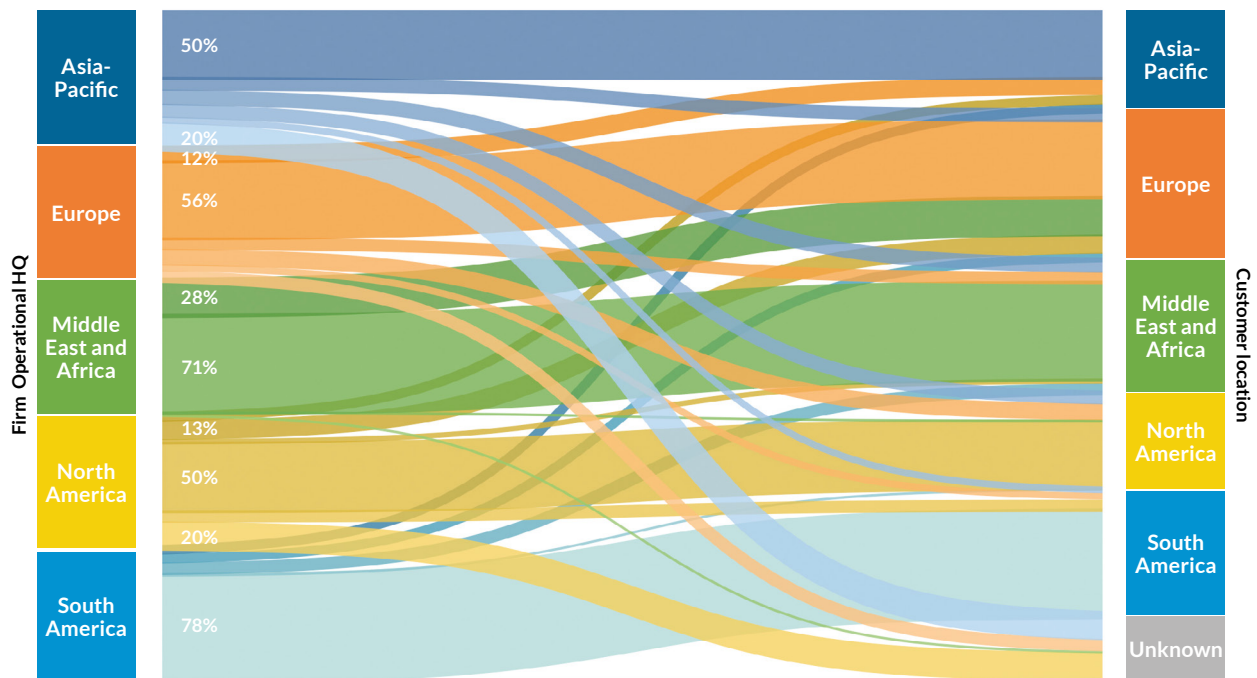
The criteria for determining the level of user activity vary significantly from one service provider to another

Using their own definitions, service providers report an increase in active users: an average of 35% of users were considered active in 2016, 37% of users were active in 2017, and 38% of users in 2018 Q1. However, the median service provider saw a decrease in user activity in 2017: 37% in 2016, falling to 35% in 2017, before rising to 40% in 2018 Q1. This difference reflects the range reported by firms: some report as few as 5% active users, while the upper bound ranges from 85% (2016) to 91% (2017) and 80% (2018 Q1). The extent to which these ranges reflect different definitions instead of different levels of user engagement is something this report cannot answer. Standardising definitions across activities and segments would be a first step towards conducting the analysis described above.

User Location

Cryptoassets directly transacted via a public blockchain can easily move globally, but cryptoasset transactions that move through service providers may be more region-locked. We find that entities predominately serve customers based in the region of their operational headquarters: over half of customers are based within the same region (**Figure 15**). North American and Asian-Pacific firms have the largest share of non-domestic region customers, although on average a fifth of customers have unknown locations. Middle Eastern and African firms have a quarter of their customer base in Europe. European entities serve Asia-Pacific and North America customers in almost equal proportion (12% and 11%, respectively).

Figure 15: Firms predominantly serve regional customers based in the region where they have their operational HQ



This analysis can be complemented with publicly available data sources. For instance, Coinmap shows the geographic distribution of more than 13,000 businesses and merchants worldwide accepting cryptoassets, which is dominated by North America, Europe, as well as some regions in South America, South-East Asia, Southern Africa, and Oceania.²⁴ The geographic distribution of Bitcoin ATMs reveals a similar picture: according to Coin ATM Radar, more than 4,000 ATMs have been set up in over 70 countries, with the USA, Canada, Austria and the UK clearly dominating in absolute numbers.²⁵

A recent analysis on transaction volumes at P2P exchange *LocalBitcoins* conducted by news and research firm *The Block* revealed that when weighted by population size, usage was most popular in developing countries that have lived through severe monetary turmoil (e.g. Russia, Venezuela).²⁶ This may also indicate a lack of reliable local exchange infrastructure in developing countries.

Overall, cryptoasset usage is a global phenomenon that involves users from all around the world. While some regions (e.g. North America, Central and Eastern Europe, South-East Asia, and parts of South America) and specific countries (e.g. USA, Canada, Japan, South Korea, China, UK, India, France) seem to dominate in terms of active usage, other regions are catching up.

²⁴ Data available at <https://coinmap.org/#/world/13.58192090/13.35937500/2> [Accessed: 02 December 2018].

²⁵ Data available at: <https://coinatmradar.com/> [Accessed: 02 December 2018].

²⁶ Cermak, L. (2018) Analysis: Russia and Venezuela dominating LocalBitcoins volumes, an intriguing proxy for bitcoin demand. *The Block*. Available at: <https://www.theblockcrypto.com/2018/10/26/analysis-russia-and-venezuela-dominating-localbitcoins-volumes-an-intriguing-proxy-for-bitcoin-demand/> [Accessed: 02 December 2018].

2.3 Cryptoasset Usage Characteristics

Cryptoasset systems have integrated payment networks that enable the transfer of value between users. The open and transparent nature of these systems allows the analysis and comparison of on-chain transactions of the major cryptoassets, while our survey allows insights into off-chain payments that are processed in internal database systems operated by service providers. However, it is difficult to determine what a given cryptoasset transaction (or payment) is used for given that actual usage is often entirely contextual and depends on a variety of factors (e.g. geographic location, access to alternatives, etc.).



On-chain and off-chain transactions

- **On-chain:** transactions that clear and settle directly on the respective blockchain.
- **Off-chain:**
 - *Trusted:* transactions recorded by, and reliant upon, service providers for internal clearing and settlement.
 - *Trust-minimised:* transactions based on payment channels using the blockchain exclusively for settlement.

On-chain Payments

Figure 16: Bitcoin clearly dominates in terms of monthly on-chain transaction volumes, but loses ground to Ethereum in the number of processed payments

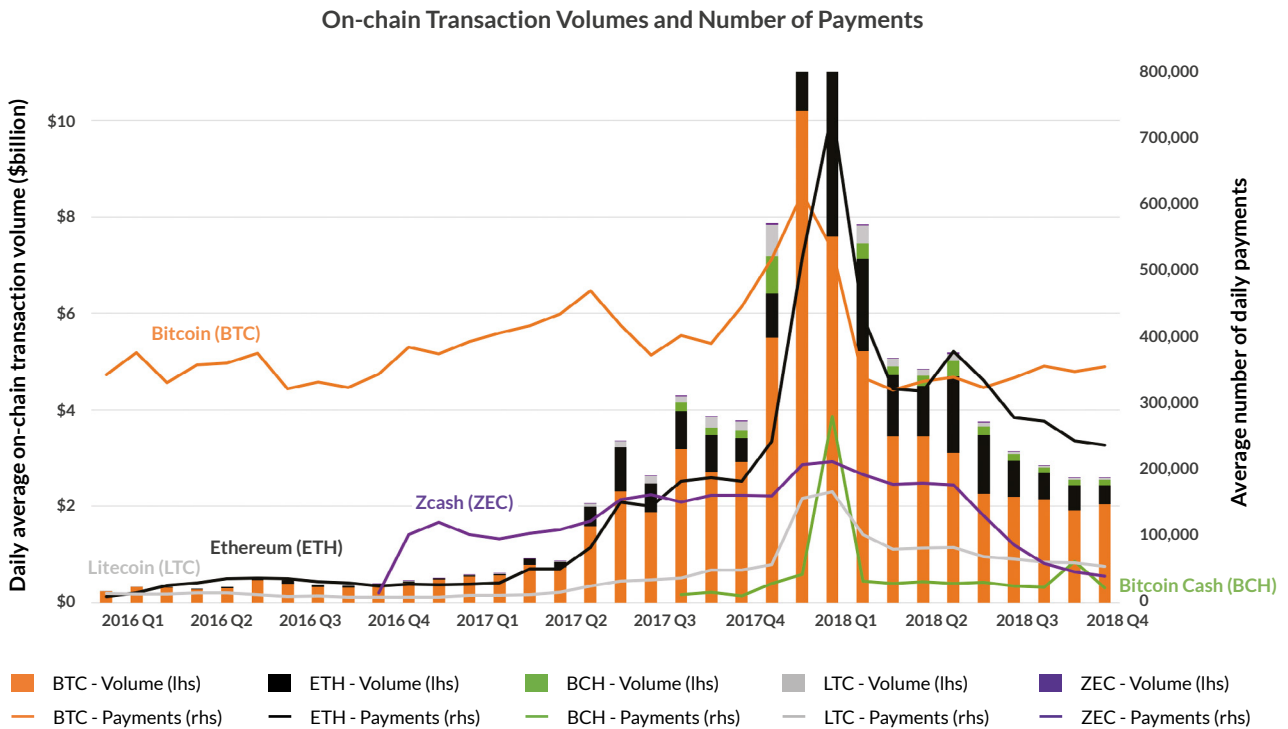


Figure 16 shows the on-chain transaction volume (measured in USD) and the average number of daily payments of five public blockchain systems. Bitcoin (BTC) has the greater transaction volume, followed by Ethereum (ETH). Bitcoin Cash (BCH), Litecoin (LTC) and Zcash (ZEC), which are usually small in comparison. Transaction volume increased during the price boom, but subsequently decreased back to the levels of early 2017. The number of payments for each coin is slightly different: specifically, there was a brief period during which Ethereum surpassed Bitcoin in terms of processing the largest number of payments. This implies that Ethereum payments tend to be of lower value than Bitcoin's.



The Difference Between Transactions and Payments

A general measure of blockchain throughput is the number of transactions that cryptoasset systems can process over a predefined period. However, one *transaction* may contain a bundle of several *payments* – funds moving from different senders to different recipients. This makes it possible for transactions and payments to move differently (e.g. a decreasing number of transactions can support an increasing number of payments), and therefore both must be analysed to obtain a full picture of a blockchain's use as a payment system.

The total value of daily transactions processed by the top-5 cryptoassets has grown nine-fold during 2017 and are still showing positive growth of 44% in 2018 despite the cool-down. However, the median transaction volume and transaction size has evolved differently across cryptoassets (Figure 17).

Figure 17: Bitcoin's on-chain transaction volume and transaction size have been continuously growing since 2016, contrary to other cryptoassets

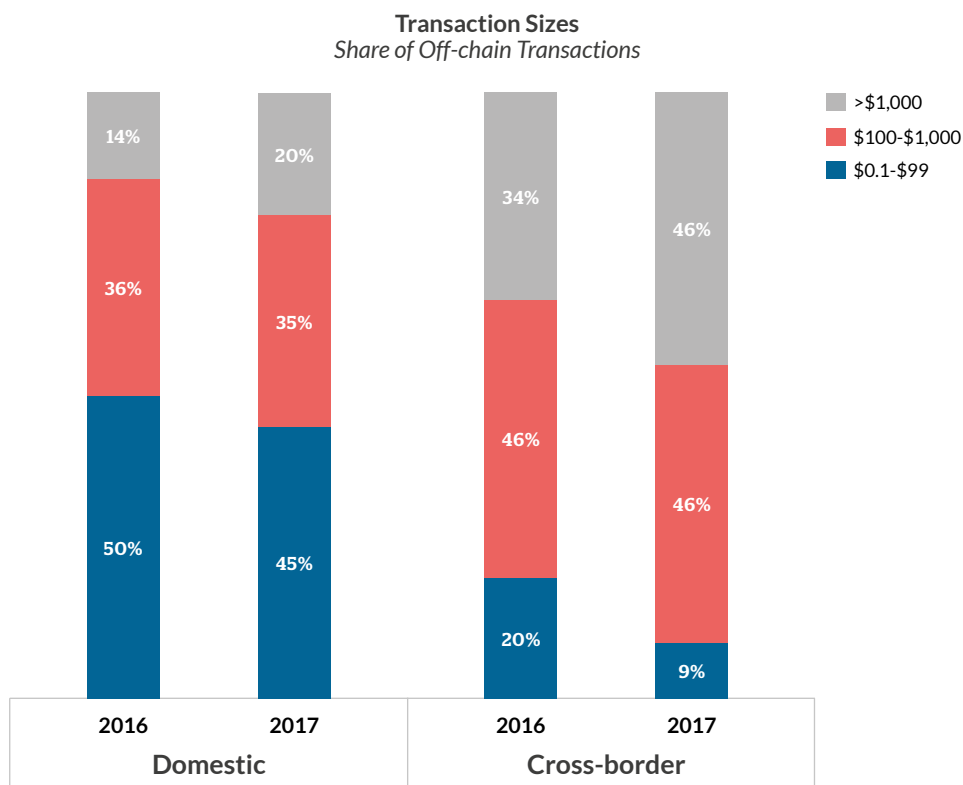


Bitcoin has seen increasing transaction value and transaction size from 2016 to 2017, the only one of the five represented cryptoassets to do so.²⁷ Ethereum has seen growing median transaction volume but constant low transaction size, indicating that it is used mostly for small-value transactions. This is consistent with its status as a major cryptoasset platform for supporting and running applications (“dApps”). While most cryptoasset systems saw a decline in median transaction value during 2018, Bitcoin Cash is unusual in the large decline in transaction value it experienced between 2017 and 2018.

Off-chain Payments

The speed and costs of many cryptoasset systems has resulted in a portion of payments being taken off-chain, often facilitated by custodial service providers rather than trust-minimised second-layer solutions. Payment service providers aggregate all transfers in their internal computer system and only use the blockchain as a settlement layer for netting the outstanding transfers.²⁸ This removes significant burden from the underlying blockchain network by freeing up capacity, at the expense of putting users at the mercy of service providers (e.g. decision to freeze accounts or block payments).

Figure 18: The share of high-value off-chain payments – especially for cross-border transfers – has significantly increased



Survey data gives an indication of the nature of these payments (Figure 18). Transactions that are domestic behave differently than transactions that are cross-border, implying that users employ cryptoassets for different purposes in these two contexts. Domestic transactions are small, with approximately half of all transactions under \$100.

²⁷ The transaction volume is the aggregate dollar-value amount processed by the system during a specific period, whereas transaction size is the median transaction amount processed by the system during the same period.

²⁸ Internal transfers do not actually move cryptoassets but consist in updating balances denominated in cryptoassets held in custody by the service provider.

Cross-border transactions are large, with approximately half of all transactions between \$100 and \$1,000. Both domestic and cross-border transactions have seen a trend toward higher-value payments, with the share of under \$1,000 payments declining from 66% in 2016 to 55% in 2017.²⁹ Whether this is due to the increase in the price of cryptoassets, surge in fees, or greater acceptance of cryptoassets in large transactions is beyond the scope of this report.

Consumer payment volumes remain at low levels

The study also finds that the median size of the average consumer-to-consumer (P2P/C2C) transfer in our survey is \$100, consumer-to-business (C2B) payment is \$14, while the average business-to-business transfer (B2B) is significantly larger (\$50,000). These values imply that cryptoassets are used to transfer funds “within” user types, rather than purchase goods and services. While tens of thousands of merchants worldwide are purported to accept cryptoassets for payment, reported merchant volumes have been relatively low, which suggests that at present cryptoassets have not managed to establish themselves as widely used currencies and general payment method for consumer payments.³⁰

Decentralised Applications and Timestamping

“Decentralised applications” (dApps) – applications that are supposed to run in a decentralised fashion with no central operator – exploded with the release of Ethereum’s ERC-20 standard.³¹ Ethereum currently hosts over 2,000 dApps, with a total average of 50,000 daily active unique addresses.³² Other dApp-focused systems such as EOS and Tezos have experienced substantial growth as well.

While dApps encourage the use of cryptoassets as payments for services or goods, their user and transaction volumes are still very low: they are an emergent phenomenon, not substantial enough to drive cryptoasset use. DEXes are the most popular dApp category, generating most transaction volume and attracting most users.

Timestamping constitutes another, non-monetary application of public blockchains. Large amounts of “off-chain” data can get anchored into networks such as Bitcoin and Ethereum, which can act as global public notaries enabling anyone to independently verify the existence and integrity of the timestamped data. A growing number of transaction outputs using Bitcoin’s OP_RETURN field can be observed since 2015, suggesting that the use of public blockchains for timestamping has become more popular.³³

Speculation and Investment

The volatile nature of cryptoasset markets make them a desirable target for speculators: available data suggests that cryptoassets display behaviour consistent with speculative investment rather than use as currency or payment methods. Reported global exchange volumes frequently amount to US\$12 billion a day, with over-the-counter (OTC) volumes estimated by some to be between two and three times larger.³⁴ Nevertheless, the figures above significantly dwarf observed on-chain transaction volumes, further

²⁹ This seems consistent with on-chain payments analysis (see [Figure 19](#)).

³⁰ Jonkers, N. (2018) What drives bitcoin adoption by retailers? *DNB Working paper 585*. Available at: <https://www.dnb.nl/en/news/dnb-publications/dnb-working-papers-series/dnb-working-papers/Workingpapers2018/dnb373270.jsp> [Accessed: 02 December 2018].

³¹ However, it is unclear whether the majority of currently active dApps can be considered “decentralised” given the presence of centralised developer teams.

³² Data available at: <https://www.stateofthedapps.com/> [Accessed: 02 December 2018]. Readers should recall that a single user may have multiple addresses, meaning that the number of daily active addresses does not necessarily reflect the number of unique users.

³³ Data available at: <https://opreturn.org/> [Accessed: 02 December 2018].

³⁴ TABB Group (2018) *Crypto Trading: Platforms Target Institutional Market*. Available at: <https://research.tabbgroup.com/report/v16-013-crypto-trading-platforms-target-institutional-market/> [Accessed: 02 December 2018].

supporting the view that speculation and long-term investment currently remain the major use case for cryptoassets.

Speculation remains the major cryptoasset use case

On average, the number of available trading pairs has grown from around 6,500 to more than 9,000 in 2018 Q4, with some exchanges providing support for more than a thousand cryptoasset trading pairs.³⁵ According to a recent report from data service provider CryptoCompare, cryptoasset-only exchanges are responsible on average for approximately three quarter of total spot market volumes.³⁶ Bitcoin-to-fiat (and vice-versa) volumes in 2017 Q4 have been dominated by USD trading (roughly responsible for half of volumes), followed by the Japanese Yen (21%) and the Korean Won (16%), with the latter showing significant growth since October 2018. Unfortunately, limited data availability, in conjunction with inconsistency across datasets and data collection methods, hinder conducting further data analysis of this type of usage.³⁷

There is a distinction to be made between investors with different time horizons: some take a short-term perspective and actively trade cryptoassets – often on a daily basis, whereas others adopt a more long-term oriented view. While the former are primarily composed of traders engaging in short-term speculation, the latter are long-term holders that comprise retail investors, high net worth individuals (HNWIs), and institutional investors. These can include both new crypto-focused investment funds and more traditional funds, as well as family offices.

Given high price fluctuations on the cryptoasset trading market, most exchanges are reluctant to offer leverage on trades to their investors. Yet, trading on margin is made available to cryptoasset-investors by some service providers: among surveyed participants, some exchanges provide leverage of 2x whereas others offer up to 100x, with the average amount of leverage being 27x (median 3.3x).

Cryptoasset exchanges offer a median amount of leverage of 3.3x

However as high leverage rates are seen as an unscrupulous business tactic, financial regulators in most countries enforce limits. The Japan Virtual Currency Exchange Association (JVCEA), a self-regulatory organisation of the Japanese cryptocurrency industry, has proposed a cap on the leverage offered by cryptocurrency exchanges (1:4).³⁸

Bitcoin futures have become an integral part of the cryptoasset investment landscape since Chicago-based exchanges CME Group and Cboe started offering cash-settled Bitcoin contracts in December 2017.³⁹ These products allow industry actors, such as miners and payment service providers as well as investors, to hedge the volatility inherent in cryptoasset markets and contribute to the growing maturity of cryptoasset-related services.

³⁵ Data available at: <https://www.blockchaincenter.net/cockpit/stats/> [Accessed: 02 December 2018].

³⁶ CryptoCompare (2018) CCCAGG *Exchange Review*. Available at: https://blog.bitmex.com/wp-content/uploads/2018/11/cryptocompare_exchange_review_october_2018.pdf [Accessed: 02 December 2018].

³⁷ Exchange volumes are frequently reported differently across data service providers, and some exchanges tolerate wash trading to artificially increase volumes.

³⁸ Data available in the Japanese Virtual Currency Exchange Association's (JVCEA) report presentation to the Financial Services Agency (FSA) during the Study Group Meeting on the Virtual Currency Exchanges held in April 2018. A summary is available at: <https://www.coindesk.com/japanese-crypto-exchange-group-gets-legal-status-to-self-regulate-industry/> [Accessed: 02 December 2018].

³⁹ Some cryptoasset exchanges have been offering derivative products a long time before this date.

SECTION 3: GATEWAYS AND ECONOMIC CONNECTIONS

Connecting the Ecosystems

The cryptoasset ecosystem comprises thousands of cryptoassets that each have their own local ecosystem. Cryptoasset gateways provide interfaces for users to seamlessly move between local ecosystems. These entities do not handle fiat currency and provide exclusively cryptoasset services.

In contrast, *fiat gateways* connect the cryptoasset ecosystem with traditional markets: examples include payment service providers that allow cryptoasset holders to purchase items at retail stores, or exchanges that enable users to make deposits or withdrawals into traditional banking or financial systems. An *on-ramp* is a fiat gateway that lets users to convert fiat currency into a cryptoasset, while an *off-ramp* allows user to convert a cryptoasset into fiat currency.

Figure 19: Conceptual mapping of monetary flows between ecosystems

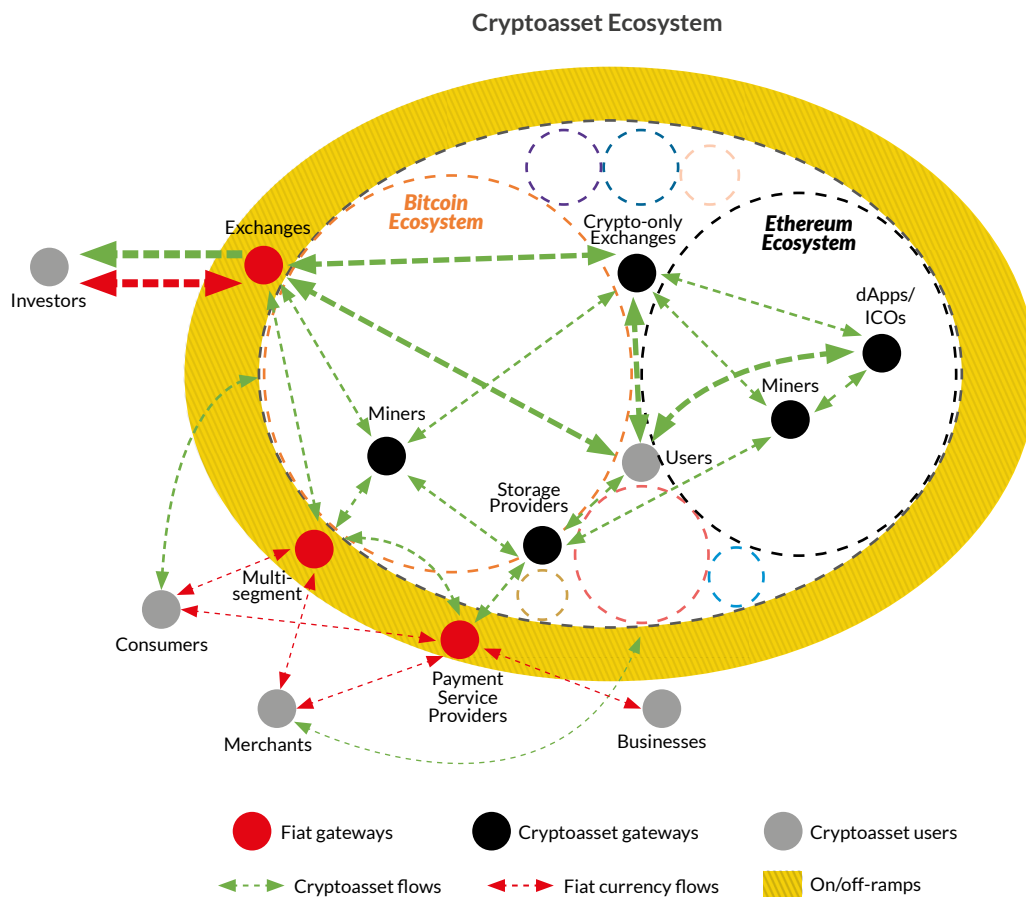


Figure 19 provides an approximation of the major flows of funds between the various ecosystems. Flows can be denominated in cryptoassets or fiat currency, and do originate from various actor types.

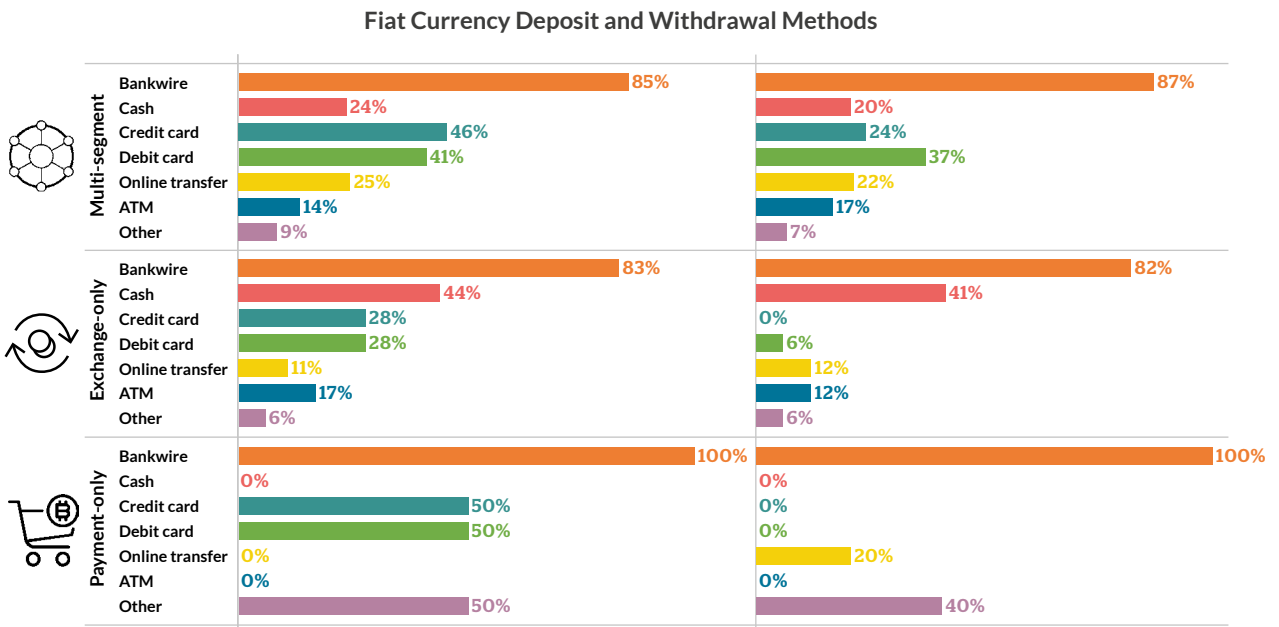
On-Ramps and Off-Ramps

Exchanges are the major on- and off-ramps to the cryptoasset ecosystem, with the majority of exchanges in our sample accepting national fiat currencies for use in cryptoasset trades. Smaller exchanges are more likely to provide cryptoasset-only exchange services than large exchanges.

Only 19% of surveyed small exchanges and 9% of large exchanges support exclusively cryptoasset-to-cryptoasset trading

Figure 20 reports the usage rates of various fiat currency deposit and withdrawals methods for exchanges, payment service providers, and multi-segment firms (in this context companies that blend aspects of exchanges and payment service providers). In all cases, bank wires receive the most support, with cash, debit, and credit cards the second tier of acceptability. While Figure 20 is aggregated data, results are similar when examined across regions.

Figure 20: Bank wires are the most supported payment method for both deposits and withdrawals



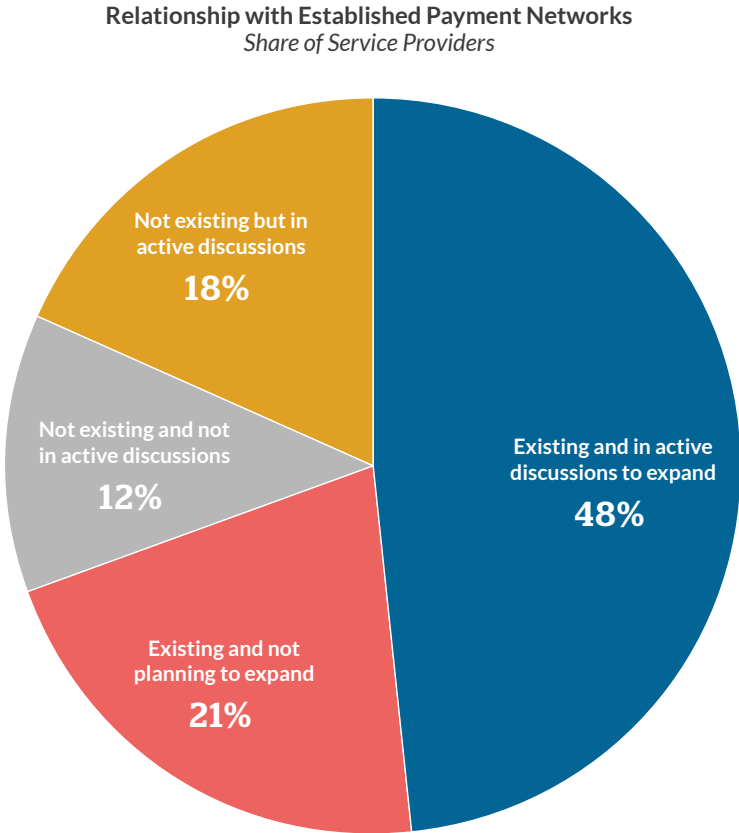
The popularity of multiple means of deposit and withdrawal methods hide the fact that most firms only accept a few. Across survey respondents, 36% reported accepting a single payment method for deposit, while 51% allowed only one payment method for withdrawals. At the other end of the spectrum, one in five firms allow four or more methods to deposit fiat currency, while only 12% allow four or more payment methods for withdrawal. We can observe a pattern of service providers offering fewer withdrawal than deposit methods, with the exception of multi-segment firms. This suggests that it is currently easier for investors, users, and consumers to enter the cryptoasset ecosystem than to leave.

Entering and maintaining good banking relationships remains a major challenge

Establishing and maintaining banking relationships is of great concern to exchanges as bank wires are a popular method of funding and withdrawing funds. Both small and large surveyed exchanges find that the inability to enter a bank relationship poses a risk to their operations -- a concern that has increased considerably since 2017 for large exchanges. For small exchanges, their concern about entering and maintain banking relationships is behind concerns about IT security and regulatory burden, and equivalent to fraud and inability to find talent.⁴⁰

40 See Table 6 in Appendix

Figure 21: Nearly a third of payment service providers have no existing relationships with established payment network



Payment service providers allow cryptoassets to be directly converted into goods and services without requiring conversion into a national fiat currency. **Figure 21** shows that only 12% of surveyed payment service providers do not have any existing relationships with established payment networks (e.g. bank transfers, card networks, point of sale, terminals, ATMs, mobile money, eCommerce platforms), and are currently not in active discussions to build partnerships. The remaining 88% were either actively engaged in discussion to establish a relationship (18%), or already established a relationship (69%). Among those with a relationship (48% of survey respondents) 70% were in an active discussion to expand their relationship.

Internal Cryptoasset Ecosystem Flows

Once actors have entered the cryptoasset ecosystem via on-ramps, they can start transacting with cryptoasset-denominated funds. There are two major ways of transacting within the cryptoasset ecosystem: users can initiate *direct* (on-chain) transactions that will clear and settle on the respective blockchain, or they can do *indirect* (off-chain) transactions using service providers.⁴¹

Figure 22: Small exchanges have a larger relative share of outgoing transactions than large exchanges

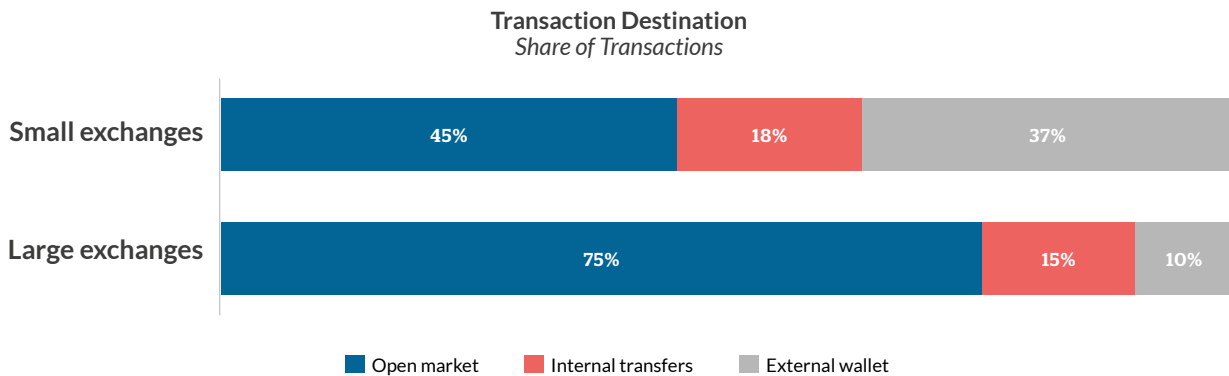


Figure 22 shows that only 10% of transactions initiated from users of large exchanges are directed at external wallets such as service providers, merchants, or user wallets, against 37% for small exchanges. All remaining transactions (63% of small exchanges and 90% of large exchanges) occur off-chain within internal exchange recordkeeping systems.

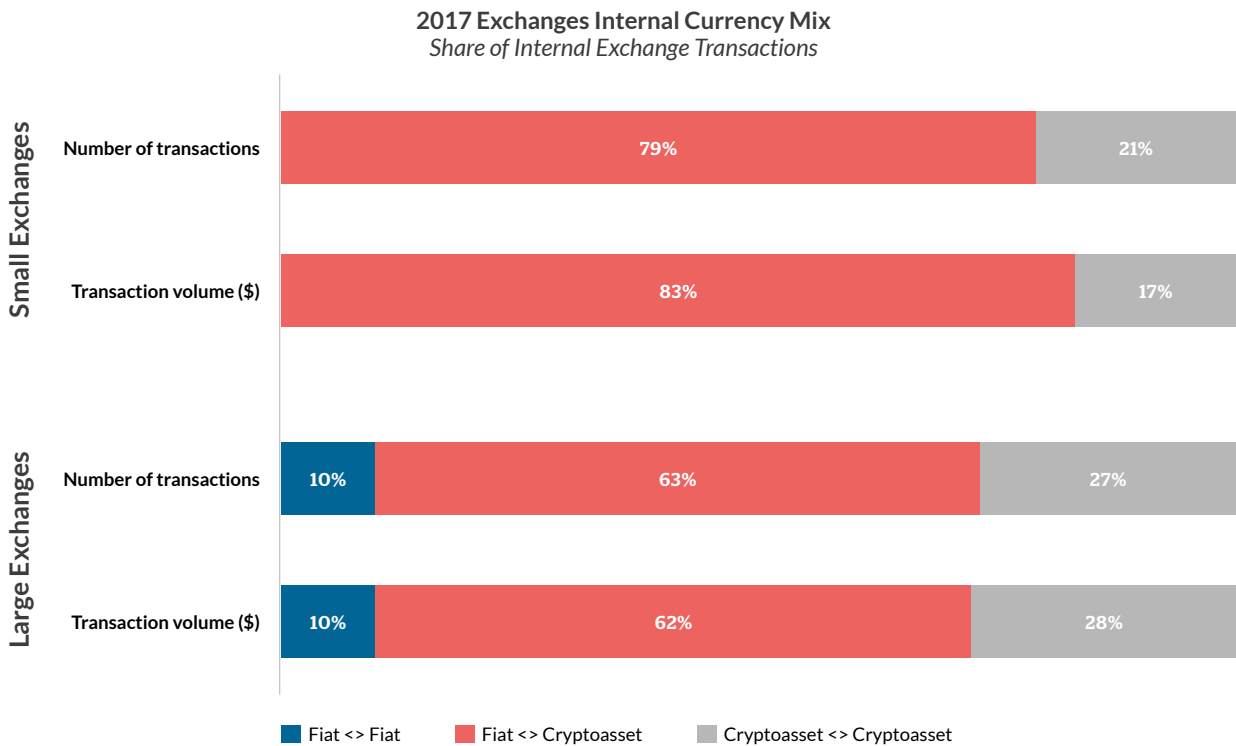
As internal transfers between exchange accounts constitute 15-18% of all transactions for both large and small exchange, the primary difference comes from exchange open-market (e.g. order-book) transactions. For large exchanges, 75% of transactions are directed at the open market within the exchange, while it is only 45% of transactions for smaller exchanges. This could suggest that larger exchanges have a bigger percentage of passive investors who will leave funds at the exchange as opposed to more active traders who tend to use smaller exchanges. On the other hand, it could also reflect that larger exchanges simply have a larger number of transactions on their open market.

Only 18% of transactions from exchanges operating across multiple segments go to an external wallet, compared to 45% for specialised exchanges. This strengthens the theory that multi-segment entities are one-stop shops for storing and managing user funds without having to switch services where most users stay on the platform.

This finding has public policy implications: most fiat-supporting exchanges are regulated or at the very minimum have to comply with existing regulations. As a result, regulators have a certain level of oversight and control over these entities; unlike cryptoasset-only exchanges, which tend to be regulated significantly less frequently (although roughly half are engaged in self-regulation in some form and to some extent – see Section 5 for more information).

⁴¹ Layer-2 solutions such as the Lightning network enable direct off-chain transfer of cryptoassets without going through a service provider (i.e. trust-minimised).

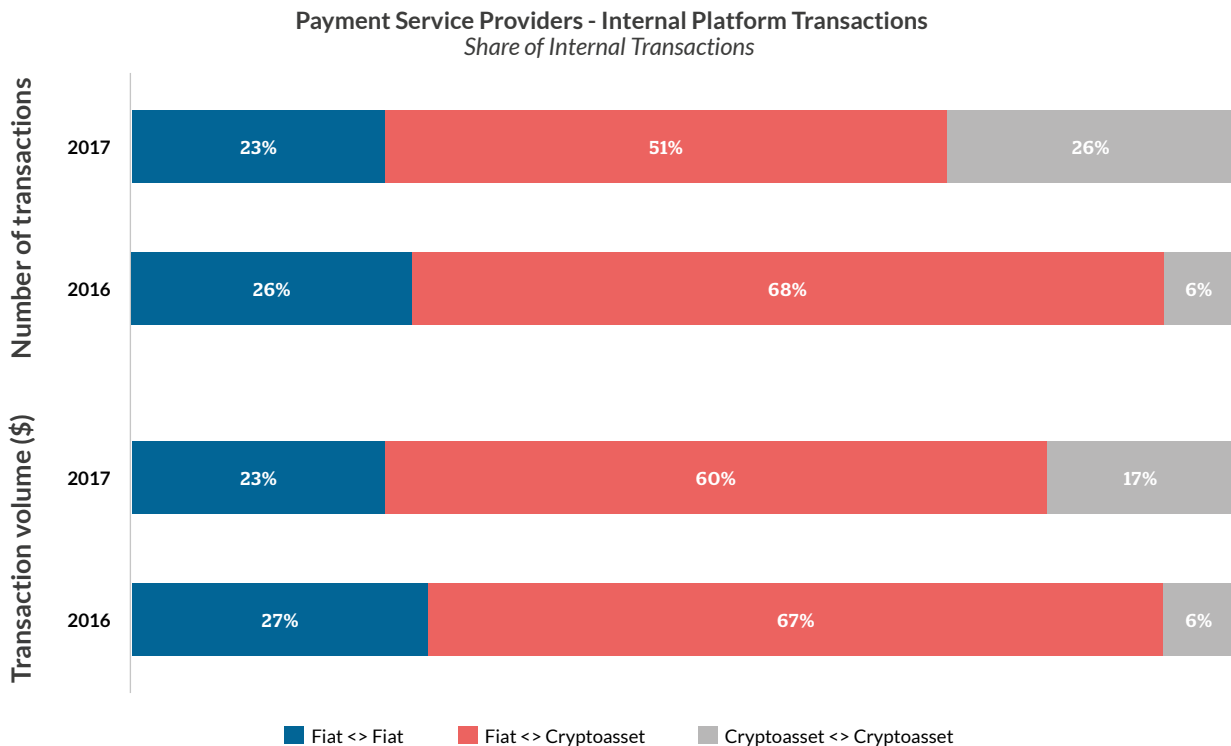
Figure 23: Exchanges report that fiat-to-cryptoasset (and vice-versa) transactions still make up the majority of total exchange trades



Publicly available data on the popularity of fiat-to-cryptoasset trades (and vice-versa) relative to cryptoasset-to-cryptoasset trades is contradictory across sources. Within our survey, [Figure 23](#) shows that both large and small exchanges reported primarily processing fiat-to-cryptoasset trades, with both the number of transactions and their volume reflecting similar shares.

The fiat in- and out-flows of exchanges outnumber internal transaction activity, which may suggest that exchange-based speculation remains the dominant cryptoasset use case: most users are not purchasing cryptoassets and using them as a replacement for means of payment.

Figure 24: Payment service providers use cryptoassets less frequently for fiat-denominated cross-border payments



The dominant use of fiat currency as a primary on- and off-ramp presents an interesting contrast to payment service providers. **Figure 24** shows that payment services reported a decrease in the use of cryptoassets to facilitate fiat-denominated cross-border payments (i.e. using cryptocurrency as a vehicle currency) in 2017 compared to 2016. However, the share of cryptoasset-to-cryptoasset transfers (i.e. directly paying recipients in cryptoassets as opposed to fiat currency) has significantly increased. The payments landscape is still dominated by fiat-to-cryptoasset transfers allowing users to buy and sell cryptoassets with fiat currencies without having to leave the payments platform.

4% of payment service providers are using cryptoassets exclusively as vehicle currencies to facilitate fiat-denominated cross-border transfers

Managing Volatility

Cryptoasset payment service providers may engage in varying activities, but they all share in common that they handle cryptoassets. This can expose companies to significant volatility risk. More than half of payment service providers report reducing volatility risk by simply buying the required cryptoasset on-demand when necessary— a “Just-In-Time” conversion strategy. The use of cryptoasset derivatives for managing volatility risk is very rare: only a quarter of payment services require customers to put up margin. Futures contracts are available in some locations, but primarily focus on Bitcoin.

Payment service providers have different strategies for managing cryptoasset volatility



What are stablecoins?

The current generation of stablecoins are digital tokens that promise stable purchasing power or a fixed conversion rate to a specific asset or commodity. Stablecoin parity can be maintained by promising a redeemable rate using reserves (e.g. fully fiat-collateralised such as Tether, USDC, or the Gemini Dollar), or through algorithmic monetary policy (e.g. MakerDAO) to stabilise price fluctuations. Stablecoins allow cryptoasset users to avoid the high volatility in prices that characterise most existing cryptoassets, while still remaining agile within the cryptoasset space.

There is a growing desire to bring stability to the cryptoasset market through the implementation of stablecoins. These are price-stable tokens, with a market price that is pegged to another familiar and stable asset, like the US dollar or oil. They also help reduce the friction between the cryptoasset and fiat currency financial systems which could potentially increase access to new kinds of assets and opportunities. While the fundamental goal of stablecoins is to reduce the cryptoasset market volatility, they are currently mainly used by traders to arbitrage between exchanges, or by small cryptoasset-only exchanges that have been denied banking relationships and are unable to hold any funds in fiat.

The use of cryptoasset derivatives for managing volatility risk is very rare: only a quarter of payment services require customers to put up margin. Futures contracts are available in some locations, but primarily focus on Bitcoin.

SECTION 4: STORAGE AND CUSTODY SEGMENT

Cryptoasset Custody

Cryptoassets use public key cryptography, where a private key – comparable to an account password – is necessary to authorise (“sign”) a movement of funds stored in an address. The address, which can be thought of as an account number, is derived from the public key that mathematically corresponds to the private key. Software programs, commonly referred to as wallets, handle the management of these key pairs.

If a private key is stolen, the holder of the private key can fraudulently authorise transactions that the owner would not. In the cryptoasset industry, *custody* refers to the business of the secure storage of these private keys -- not storage of the assets themselves.

**Custodial service providers control the users’ private keys of users,
while non-custodial service providers do not**

Storing private keys securely can be a cumbersome task: key management is notoriously difficult and requires a certain level of technical proficiency, which is why it is often outsourced to third-party “custodial” service providers. A custodial service provider is one where the service provider has been granted possession of users’ private keys. In this context, transfers of cryptoassets are generally tracked on the service provider’s balance sheet rather than being verified by the blockchain (see *on-chain vs. off-chain* discussion in Section 2). In contrast, a non-custodial service provider provides wallet infrastructure but does not hold users’ private keys: users remain at all times in full control of their funds and directly transact via the blockchain.

Many exchanges and payment service providers now provide wallets as part of their service, meaning that they can store customer funds and thus potentially act as custodial service providers.

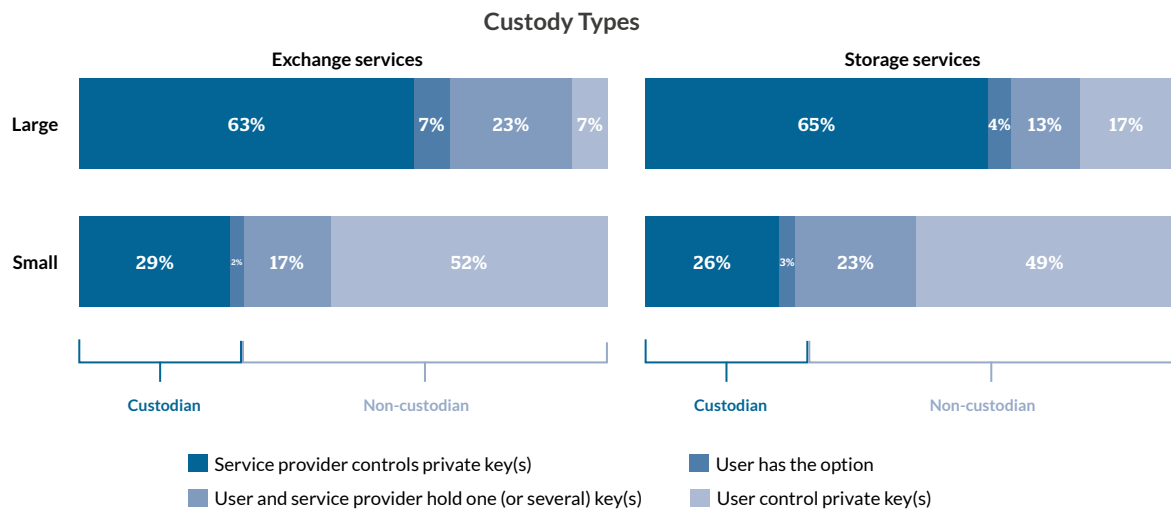


Table 3: We distinguish between four different custody settings

TYPE	“EXTREME” SETTING	“MODERATE” SETTING
Custodial	Service provider controls private keys and has full control over funds.	User has the option and can choose whether to defer custody to a third party or remain in full control over funds.
Non-custodial	User controls private keys and has exclusive control over funds.	Both user and service provider hold one (or several) private keys so that the service provider cannot unilaterally move funds without user approval.

Figure 25 shows that the distribution of custody types is very similar between firms providing exchange services and companies providing storage services. While the majority of small service providers do not keep custody of user funds, approximately two-thirds of large service providers manage custodial wallets for their customers. Firms exclusively providing storage services (69%) and exchange services (48%) more frequently opt for non-custodial methods of storing cryptoassets, regardless of company size.

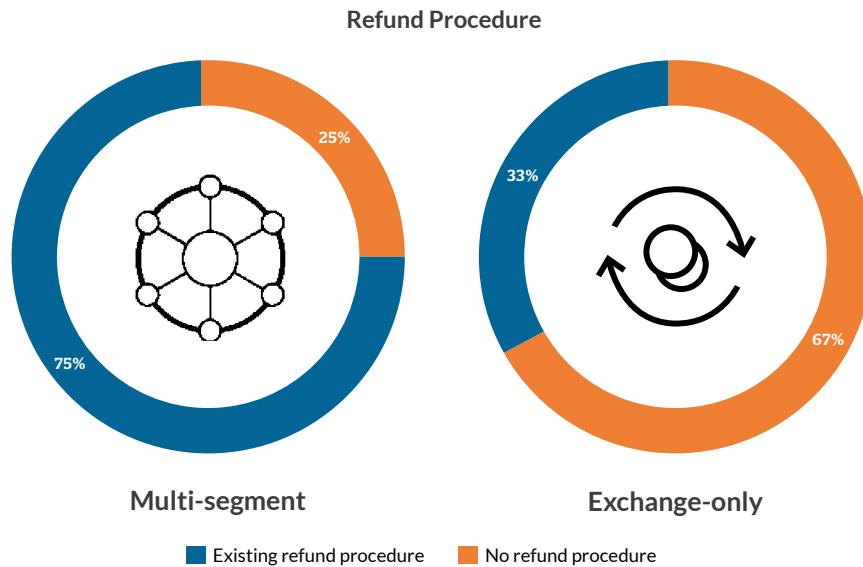
Figure 25: Large companies provide significantly more often custodial services



Despite a significant share of service providers offering self-custody options to their users, the majority of users choose not to use it; instead opting for the convenience and peace-of-mind of custodial solutions. While keeping control of their own funds empowers holders with additional financial independence (e.g. funds cannot be easily seized), it also imposes significant burdens on users when it comes to protecting and accessing their funds.

Custodial service providers take full control over user funds, which can lead to some undesirable outcomes. For instance, internal security breaches can result in the loss or theft of all customer funds, leaving customers often with little to no recourse with regards to recovering their funds. Interestingly, 23% and 13% of small and large companies, respectively, have implemented a system where the company cannot unilaterally move user funds but needs the users' permission first, which somewhat mitigates this danger.

In the event of customer funds being lost or stolen, a growing number of custodial service providers have put a refund procedure in place: 64% of custodians have a written refund procedure, as opposed to 62% in 2017. However, Figure 26 reveals that there are significant differences between specialised exchanges and multi-segment companies: only one third of custodial exchange-only firms have an existing refund procedure, compared to three quarters of multi-segment firms.

Figure 26: Two-thirds of specialised custodial exchanges do not have an existing refund procedure

Note: non-custodial service providers have been removed from the analysis.

Since custodians can move a substantial share of internal volumes off-chain using internal recordkeeping systems, there are concerns that some may run on a fractional-reserve basis. This means that the number of cryptoassets outstanding in their books is larger than the actual amount of cryptoassets held in custody. In such a system, the claims consumers have on the custodian exceed the cryptoassets the custodian has immediately available in their reserves. Unlike direct P2P trades on public blockchains, a lack of transparency resulting from the closed nature of these internal books makes it difficult for users to verify the solvency of the services they use.

Three out of four custodians have an external audit of their cryptoasset reserves

In order to counter the aforementioned allegations, 76% of custodial service providers report conducting an externally-led audit of their cryptoasset reserves in the past 12 months, which stands in stark contrast with the relative minority of non-custodians who did so (35%). In line with previous findings, large service providers (70%) are twice as likely to perform audits than small firms (38%). Interestingly, 71% of cryptoasset-only firms do not conduct audits of their reserves, whereas 58% of fiat-supporting companies do.

Source Code

Storage service providers have the option to release their wallet code under an open-source license or to keep it closed-source (i.e. proprietary). This distinction is important because open-source enhances portability, transparency, and auditability of the software, although it could also make security flaws easier to detect to hostile actors and may decrease the ability of the provider to monetise their service. Conversely to their proprietary counterparts, discontinued software code bases under an open-source license are still available and usable to external parties.

Figure 27: Significant differences in terms of source code openness can be observed between storage providers

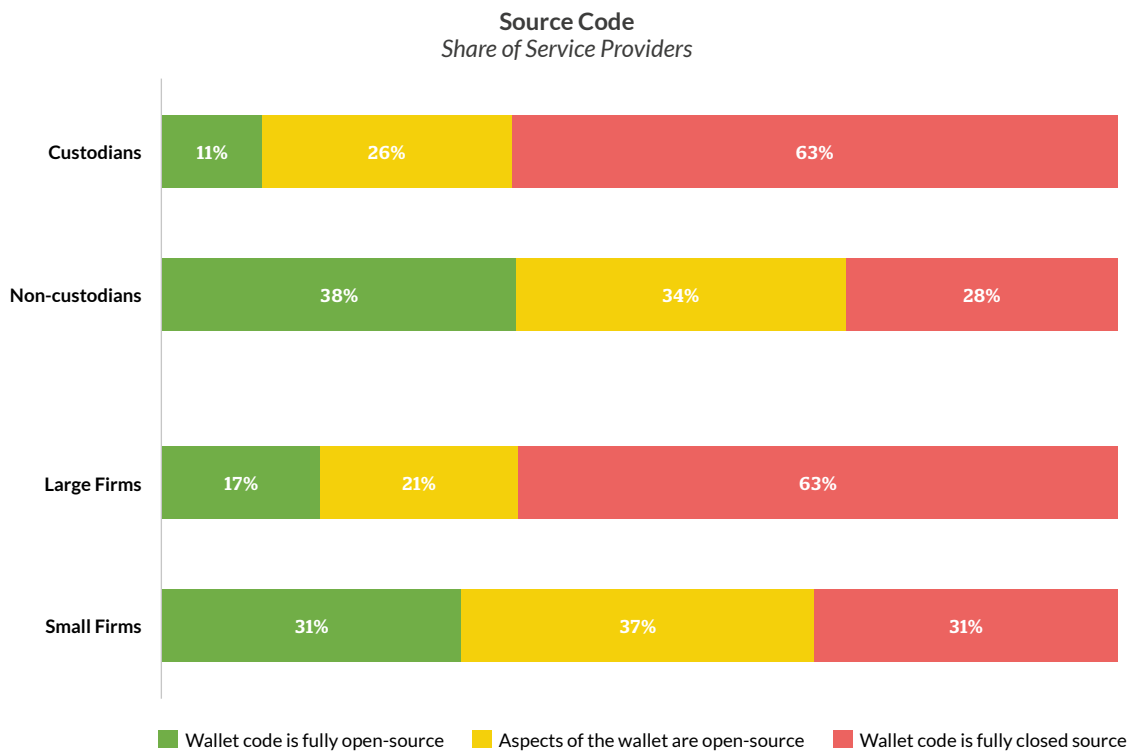


Figure 27 reveals that small storage service providers are more inclined to have partially or fully-open source wallet code than large ones. Similarly, custodians are also more likely to have closed-source wallets (63%) than non-custodial service providers (28%). While two-thirds of storage-only providers have a fully or partially open-source wallet (i.e. elements of the wallet are open-source), more than half of multi-segment entities have closed-source wallet software (mostly in the form of accounts).

Key Storage Can Take Different Forms

Key storage can take two major forms: cold and hot storage. In *cold storage*, the private key is stored offline in a cold wallet that has never been connected to the Internet – and thus should not have been easily compromised. Methods of cold storage include hardware wallets and other air-gapped, disconnected hardware devices. Conversely, *hot storage* refers to keeping private keys on an online device that is connected to some network, i.e. in *hot wallets*. Examples of hot wallets are web-based wallets as well as desktop and mobile wallets running on connected machines.

Cold storage is generally considered a safer form for storing private keys, since cold wallets are less vulnerable to network-based theft and require physical access. However, there are trade-offs involved: cold wallets are generally more cumbersome for users to access, which leads to less flexibility and longer waiting times. Choosing between either form thus comes down to holders' need to access funds, frequency of trading activity, and transaction amounts (hot wallets are deemed fine for storing small amounts, whereas larger amounts should be moved into cold storage).

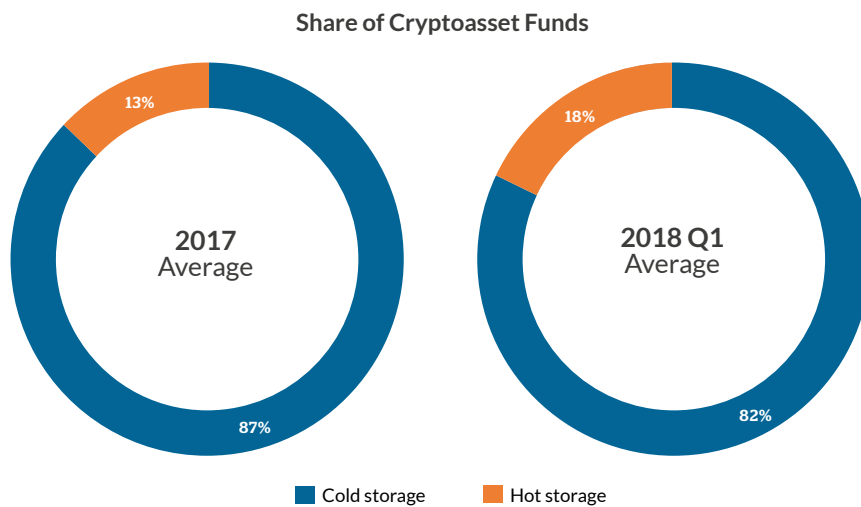
Figure 28: The share of funds held in cold storage has slightly decreased over 2017

Figure 28 shows that the use of funds in cold storage has slightly decreased between 2017 and 2018 Q1. The average share of cryptoasset funds kept in cold storage by multi-segment entities amount to 83%, slightly higher than companies specialised in exchange (79%) or payment services (55%), but smaller than for entities exclusively providing storage services (100%).

From 2017 to 2018 Q1, the figure for exchange-only providers has decreased by 8 percentage points, which is likely a result of intensified trading activities that require exchanges to have immediate access to cryptoasset funds. Interestingly, no significant difference can be observed between custodians and non-custodians, which suggests that trading activities have been equally distributed across both custody types.

Multi-Signature

An additional method for securing private keys is to use multi-signature – often colloquially referred to as *multi-sig*. Under a multi-signature scheme, multiple keys can be combined together so that a specific fixed number of keys is required to sign a transaction and move funds. Holding an individual key is insufficient to enact a transaction.

Multi-signature is a powerful tool that enables new types of ownership and custody. Users can remain in full control of their funds while having peace of mind, because one of several keys required to move funds is stored as a back-up by a service provider who cannot unilaterally access the funds. Similarly, ownership of a given cryptoasset can be distributed among multiple people or entities, requiring a majority of them to reach agreement before being able to enact transactions.

Multi-signature is also often used as a complementary tool for additional security: for instance, 87% of custodians use multi-signature techniques as part of their cold storage system (78% for hot wallets), as opposed to only 69% of non-custodians (68% for hot wallets). The average custodian secures a lower proportion of hot wallets (73%) via multi-sig than the average non-custodian (98%), again likely because they need to have quicker and easier access to wallets for client disbursements.

SECTION 5: REGULATIONS AND COMPLIANCE

The rise and the subsequent plunge in cryptoasset prices triggered a wave of complaints from retail investors who lost money, which in turn has prompted financial watchdogs to further investigate the cryptoasset industry.

The regulatory landscape surrounding cryptoassets is diverse and ever-changing: some jurisdictions have adopted a wait-and-see approach (e.g. UK, Canada) whereas others have taken either a more proactive stance (e.g. Japan, Malta) or an unsupportive position (e.g. China, India). The cryptoasset regulatory landscape will be closely examined in an upcoming report by the CCAF.

5.1 The Impact of Regulations

There is a perception that the cryptoasset industry flaunts regulations and conducts business without regard for any legal directives. This section will show that regulations do impact both the users service providers choose to accept and the countries where service providers choose to do business, indicating that this impression is at least partially incorrect.

User Impact of Regulations

Many respondents report refusing to serve customers located in a particular jurisdiction as a result of changes in the region's regulatory environment. This is particularly high for payment-only (80%), exchange-only (70%), and multi-segment service providers (82%). Small firms (67%) are less likely than large firms (83%) to decline customers from a specific jurisdiction as a result of changes to the regulatory environment with no substantial difference across regions.

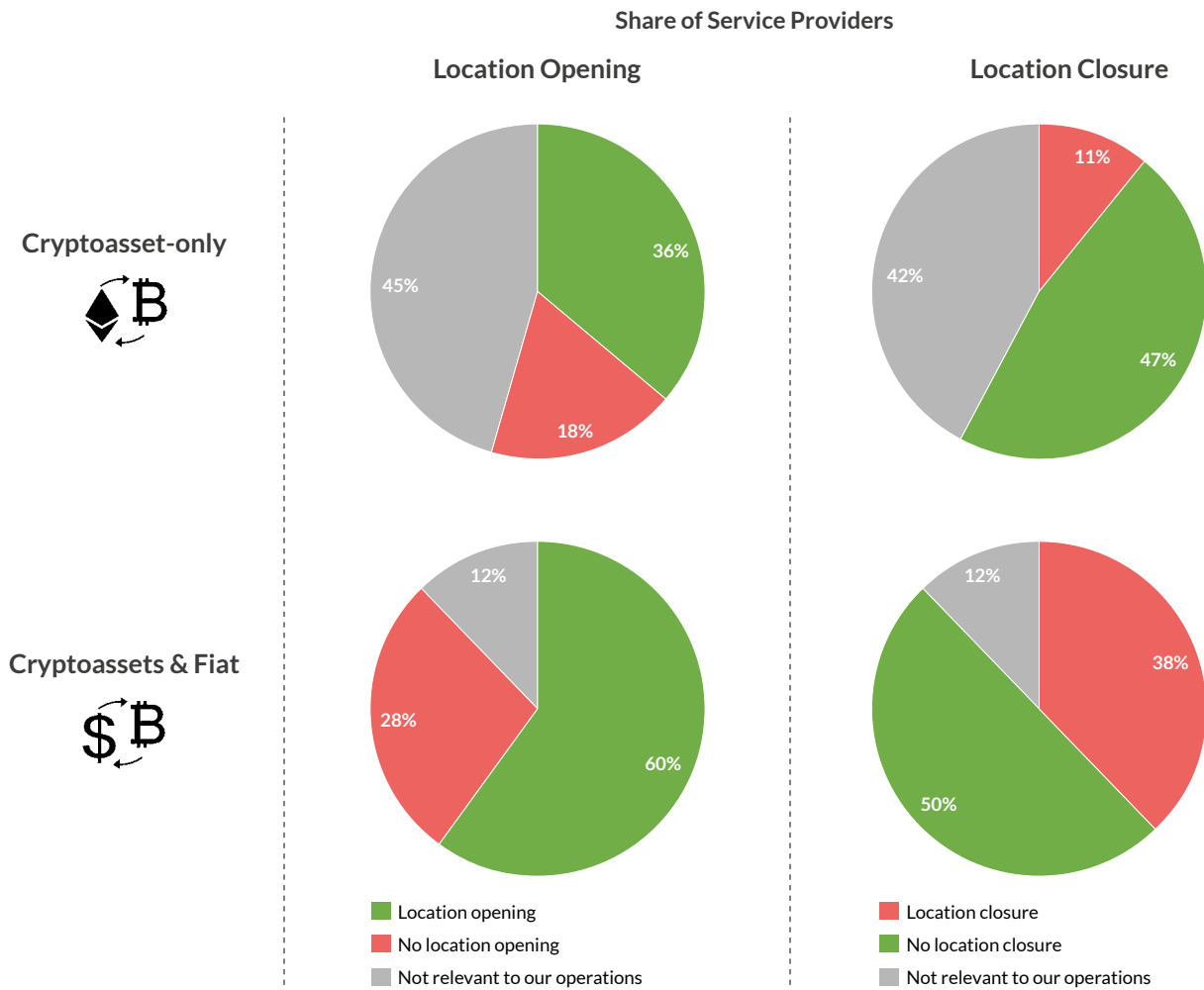
Changes in the regulatory environment have had a significant impact on the decision not to serve customers from a specific jurisdiction

Custodial firms and fiat-supporting service providers most resemble traditional financial entities: 79% and 88%, respectively, refused to serve customers residing in particular jurisdictions. Surprisingly, 68% of non-custodians and 44% of cryptoasset-only firms indicate having had to decline customers from specific jurisdictions after changes in the regulatory environment. These figures are higher than expected given that these firms exist in a regulatory grey zone in many regions due to the particular nature of their services (i.e. no custody of user funds, no handling of fiat currency).

Industry Reactions to Regulations

Survey responses suggest that the regulatory environment, which includes existing regulations, guidelines and planned changes, has a direct influence on cryptoasset businesses' decision to enter or expand to a particular jurisdiction – or alternatively to close operations and leave a given country. In many cases, regulatory changes involve introducing regulatory guidance where none existed or were enforced previously. **Figure 29** illustrates the impact of changes in the regulatory environment on the decision-making process of industry actors.

Figure 29: Regulatory interventions have a significant impact on operations



Note: location can refer to offices, facilities, or similar types of properties.

52% of surveyed exchange-only entities and 67% of multi-segment service providers stated that changes – perceived or actual – in the regulatory environment have led them to open offices or facilities in a new location. For instance, the ban on fiat-to-cryptoasset (and vice-versa) trading imposed on domestic exchanges by the Chinese government in September 2017 spurred the major Chinese companies to open offices in other jurisdictions with “friendlier” regulatory frameworks, such as Singapore or Malta.

However, there are significant differences between small and large firms: 73% of surveyed large entities opened facilities in specific locations following a change in the regulatory environment, compared to only 44% of small entities opting for a similar strategy.

Differences also lie between cryptoasset-only and fiat-supporting entities, where nearly half of cryptoasset-only service providers indicate that the regulatory environment is not a relevant factor in the decision-making process for opening a new location – often because they contend that the regulations do not apply to them. Companies registered in the Middle East and Africa as well as South America have more frequently opened new locations following regulatory changes. Overall, current changes in the regulatory environment are more likely to impact decision-making in encouraging location opening than location closure.

The regulatory environment is also a determining factor for mining organisations when deciding whether to open new facilities or offices in specific locations. About a third of large miners, small miners, and individuals agreed that their immediate regulatory environment is confusing and inconsistent. Half of surveyed large miners perceive regulation as adequate and appropriate, a statement to which only 9% of small mining organisations and individuals agreed. Instead, 23% of small miners believe that no bespoke regulation exists and that none is needed, while 16% think that regulation is non-existent but needed. Interestingly, no clear pattern in terms of regional differences could be observed: it is thus unclear whether there are specific regulations that miners are reacting to in their sentiment responses.

Cryptoasset Firms Collaborate Directly with Regulators

Contrary to popular media narratives, most survey respondents indicate high levels of interaction and collaboration with public-sector stakeholders such as regulators, policymakers, legislators as well as standard-setting bodies with regards to cryptoasset-related regulations. For example, public consultations and other forms of public hearings have been held between cryptoasset entities and respective authorities in the USA, Canada, Bermuda, and Malta, among many others.⁴² Regulatory innovation initiatives such as regulatory sandboxes and innovation offices have facilitated regulators' engagement with industry actors. This type of engagement is a helpful factor for reducing the knowledge gap and addressing regulatory issues from an industry perspective, which might contribute to more regulatory clarity in the future.

High levels of interaction and collaboration are observed between industry and the public sector

The study finds that multi-segment entities and exchange-only firms are most likely to engage with regulators directly, whereas less than half of storage-only companies tend to do so. 91% of surveyed custodians and 85% of fiat-supporting entities collaborate with regulators in some capacity, as opposed to 65% of non-custodians and 50% of cryptoasset-only companies. Similarly, large firms (89%) are more likely to engage with regulators than small firms (67%). Geographically speaking, industry-innovator collaboration appears to be less prevalent in Asia-Pacific than in other regions at the time of the survey.

⁴² There are also efforts to formalise self-regulation across the industry. Examples include the Japanese Virtual Currency Exchange Association (JVCEA), and the Global Digital Finance (GDF) initiative.

5.2 KYC/AML Policies

Enforcement of KYC/AML regulations in the cryptoasset context is a contentious issue amongst some in the industry. Some argue that the original intention of cryptoassets was the freedom to move funds around the globe without involvement or approval from any authority. Others opine that service providers are not a native element of the cryptoasset framework, and that if they facilitate criminal activities they should be prosecuted – just like all other business would be.



What Is KYC/AML?

Know Your Customer (KYC) refers to due diligence activities that financial institutions and other regulated companies must perform to ascertain relevant information from their clients for the purpose of doing business with them. Anti-Money Laundering (AML) refers to laws or regulations designed to stop the practice of generating income through illegal actions. Regulated financial services providers are responsible for the implementation of internal KYC and AML policies.

Figure 30: Half of all cryptoasset-only entities perform KYC/AML checks in some capacity

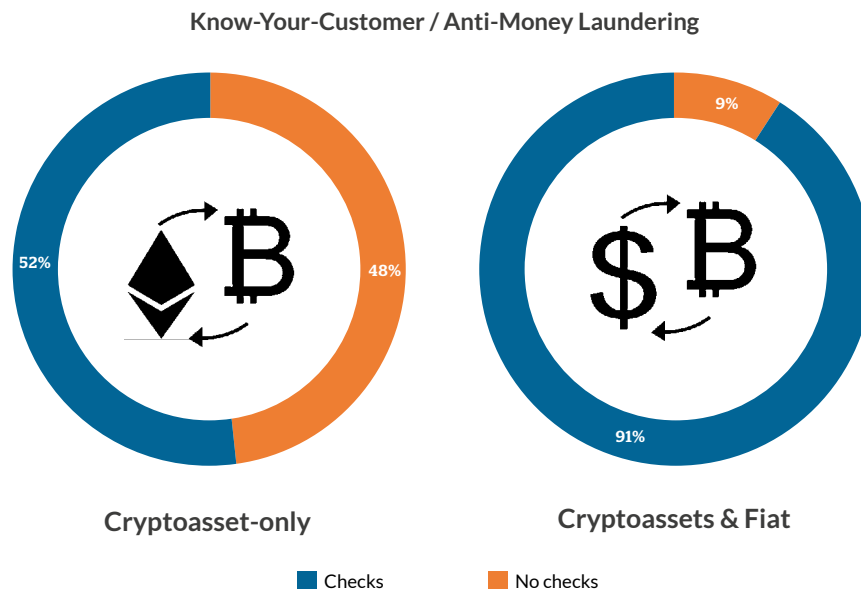
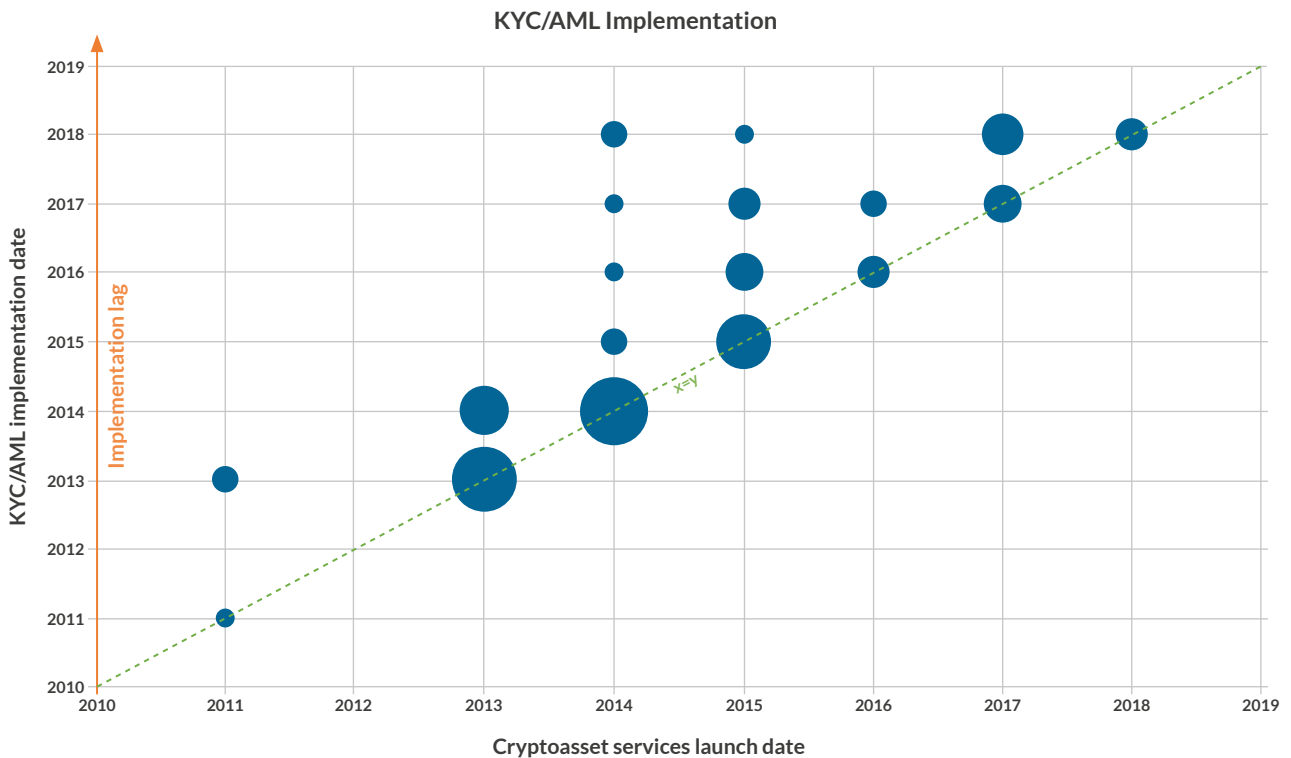


Figure 30 indicates that while nearly all surveyed fiat-supporting companies perform KYC and AML checks (91%), half of cryptoasset-only firms do as well (52%). This is a surprisingly large share considering that, depending on the jurisdiction and the precise type of activity, many were supposedly not bound by KYC/AML regulations at the time of the survey. This may serve as an argument for proactive “good practices” compliance from industry players, despite the absence of regulatory guidance and clarity.

Implementation

Although most entities implemented KYC/AML checks when they started their activities, a few began KYC/AML verification at a later date (**Figure 31**). KYC/AML checks have been implemented by some cryptoasset entities as early as 2011, and the pattern of performing KYC/AML checks continued from 2013 onwards without a clear watershed moment.

Figure 31: The majority of entities immediately implement KYC/AML checks when launching

Note: entities that do not perform KYC/AML checks have been removed from the following analysis.

The majority of entities that support both cryptoasset and fiat currency use third-party support for KYC/AML; thereby relying primarily on traditional service providers (62%) rather than blockchain analytics companies. Overall, only one third of surveyed service providers reported using the services of blockchain analytics companies that provide on-chain forensics of blockchain transactions.

Criteria

The share of service providers conducting KYC/AML verification for all accounts (i.e. both cryptoasset and fiat currency accounts) is relatively consistent throughout industry segments at around 80% on average. 91% of large entities supporting fiat currencies conduct KYC/AML checks on all accounts, as opposed to 74% of small entities. No such difference emerges between small and large entities exclusively supporting cryptoassets.

The vast majority of entities conducting KYC/AML checks inspect every account.

Respondents that do not check all accounts but use “other criteria” to perform KYC/AML verification most frequently use account size or account activity as criteria for triggering additional checks. A slight difference can be observed between fiat currency and cryptoasset accounts: service providers tend to more often use account size as a criterion for the former (63%) than for the latter (56%).

Account size and activity are the two most popular criteria if KYC/AML checks are not applied to all accounts.

Account Suspensions and Closures

In an effort to prevent fraud and financial crimes, service providers may decide to close a customer account (often referred to as “de-risking”) or not to onboard new users after conducting due diligence. An organisation can decide to do so to mitigate risks associated with higher-risk customers or for users conducting suspicious activities plausibly related to money laundering or terrorism financing.

In general, large entities are more likely to discontinue or decide not to initiate customer relationship following KYC/AML checks: all large entities that perform KYC/AML checks have had to close accounts/ refuse to open new accounts, whereas one third of small companies report no account closures.

An average of 14% of KYC checks at multi-segment entities resulted in account closure and/or refusal to open account in the past 12 months

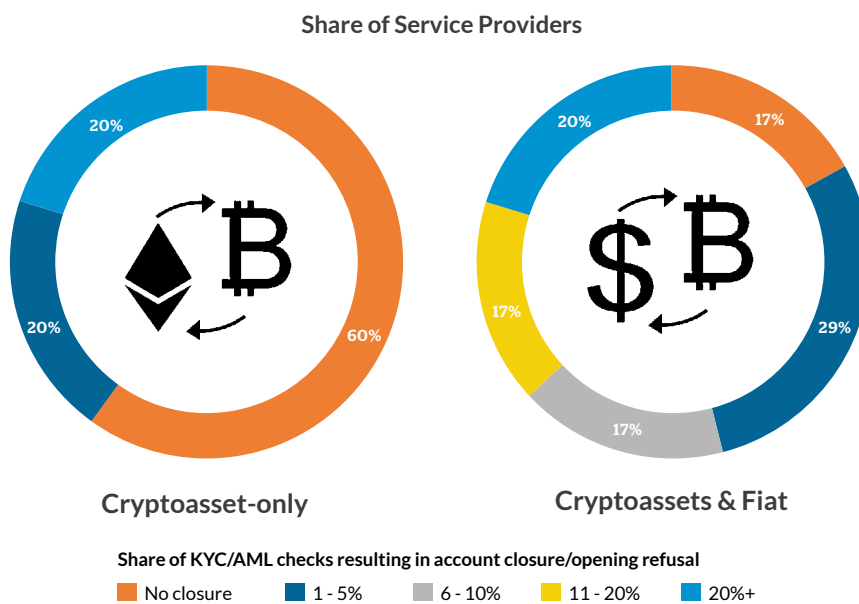
Entities engaged in multiple segments have more frequently decided to close an account or refused to open an account, followed by payment-only service providers. The median percentage of account closure/refusal following customer due diligence is 10% for multi-segment entities and 5% for payment-only companies.

Some fiat-supporting entities have to close up to 85% of accounts (or refuse new account openings) following KYC/AML checks

The median percentage of account closure/refusal that followed KYC/AML checks is higher among large companies (10%) and fiat-supporting entities (9%) than small (3%) and cryptoasset-only (0%) firms, though this range varies significantly from 0% up to 85%. This raises doubts about the quality and nature of implemented KYC/AML programmes, which seem to vary a lot from one provider to another.

Among surveyed entities, four have account closure/refusal rates between 50% and 85%. Interestingly, one in five respondents – both cryptoasset-only and fiat-supporting entities – report having 20% or more of their KYC/AML checks resulting in them not opening a new account or closing an existing one (Figure 32).

Figure 32: 83% of fiat-supporting entities have had to close / refuse to open accounts after KYC/AML checks



Note: entities that do not perform KYC/AML checks have been removed from the analysis.

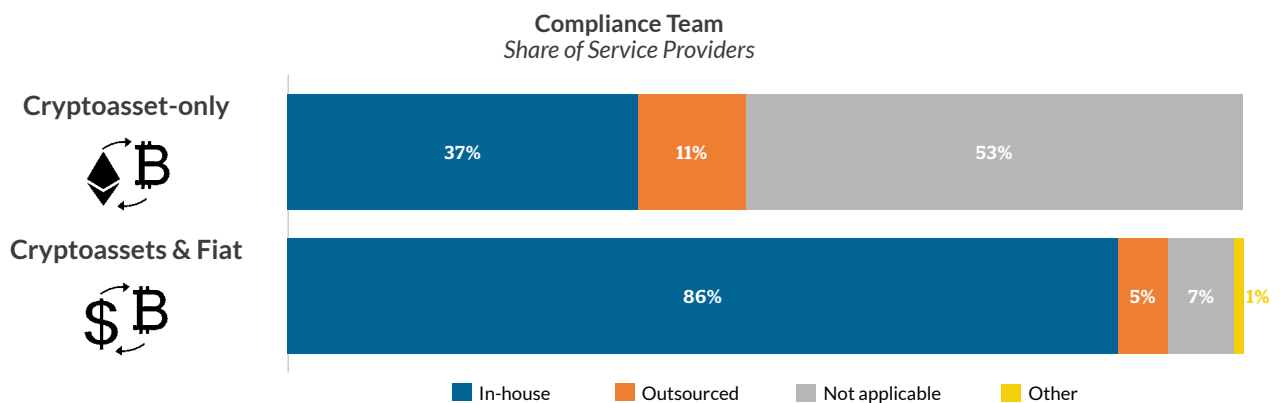
5.3 Compliance Team

KYC and AML obligations have dominated the debate on compliance issues facing cryptoasset companies. However, compliance entails a broader set of rules prescribing standards in relation to, among others, information disclosure to clients, financial statements, cybersecurity, and other prudential aspects. Regulatory requirements vary in respect to different business activities.

While regulators are still studying the cryptoasset industry, many entities involved in the ecosystem have taken a proactive approach to compliance. This often involves building up a dedicated compliance team to monitor the immediate regulatory environment and help executives navigate the complexities of financial regulations.

Figure 33 demonstrates that the use of compliance teams varies with the type of supported assets. As expected, the large majority of entities supporting both fiat currency and cryptoassets have an in-house compliance team, whereas only 5% outsource compliance to a third party. Whilst more than half of cryptoasset-only firms do not have a compliance team – in line with the absence of bespoke regulations in most jurisdictions, a remarkable share (37%) have set up an internal compliance team. This move is primarily intended to better respond to potential newly-introduced regulations specific to cryptoasset businesses or to anticipate future regulatory changes.

Figure 33: Nearly half of cryptoasset-only service providers have a compliance team



With regards to the costs associated with compliance, nearly half of cryptoasset-only firms report allocating a part of their budget to compliance (between 1-10% of total budget) compared to 78% of fiat-supporting entities (with an average of 11-15% of total budget). Noticeably, 4% of fiat-supporting companies indicated having no compliance headcount and cost (the remaining 18% did not provide any figures).

A cross-segment comparison reveals that most service providers have an internal compliance team (71% and 75% of exchange-only and payment-only entities, respectively, as well as 88% of entities involved in more than one industry segment). Although a substantial majority of companies exclusively providing storage services stated not being subject to compliance (79% selected “Not applicable”), 7% of them indicated having an internal team dedicated to compliance.

A growing number of cryptoasset-only firms have positive compliance headcount and cost

Interestingly, some exchanges who responded “Not applicable” were, contrary to their response, subject to existing regulations (primarily KYC and AML laws), which casts doubt upon their regulatory awareness and raises concerns about the quality of compliance checks.

No significant difference was observed between large and small companies in terms of headcount; with both having 6-10% of their employees dealing with compliance. However, compliance costs seem to be of a greater burden for large companies: 11-15% of their budget is allocated to compliance, versus 6-10% of small companies' budget.⁴³

5.4 Licensing

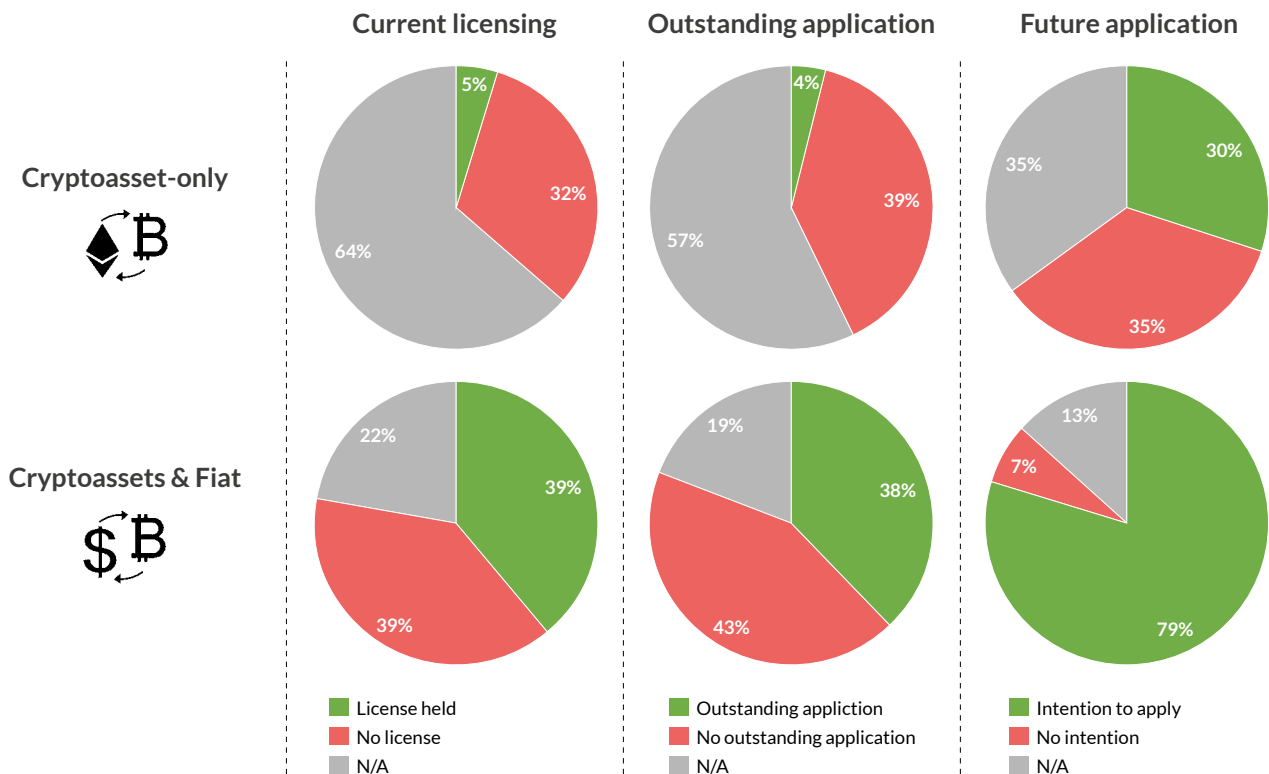
In most jurisdictions, conducting any type of financial activity is conditional upon obtaining an operating license. Licensing landscapes are extremely diverse, and so are the costs and the administrative burden associated with the application process.

A limited number of jurisdictions have created a licensing regime specific to business engaged in cryptoasset activities. For instance, cryptoasset exchanges in Japan are required to apply for the *Virtual Currency Exchange License*, while those registered in Bermuda must obtain a *Digital Asset Business License* from the Bermuda Monetary Authority. A single jurisdiction may require cryptoasset companies to obtain multiple licenses to be fully compliant. The USA, where federal states have different types of licenses (e.g. BitLicense, Money Transmitter License), is a classic example.

5% of surveyed cryptoasset-only service providers hold a license, compared to 39% of fiat-supporting entities

Fiat-supporting entities are most likely than cryptoasset-only firms to currently hold a license, have an outstanding application or have the intention to apply for one in the near future (Figure 34). A small proportion of fiat-supporting entities still consider that no license is needed in the markets they operate in or are expecting regulators to develop a bespoke regulatory framework (i.e. "N/A" respondents).

Figure 34: Most fiat-supporting entities are in the process of applying for a license or intending to apply in the future



43 All numbers presented in this section are median figures.

When further segmenting the data, it appears that none of the cryptoasset-only companies who currently operate without a license have a pending application. Nevertheless, 29% of them have the intention to apply for a license or to register with local authorities in the near future, highlighting their anticipation of changes in the regulation and the current regulatory uncertainty they are facing. In contrast, 27% of fiat-supporting entities that currently not holding a license have an outstanding application and 88% are planning to file a license application in the future.

Licensing-related figures greatly vary across industry segments. Entities active in multiple segments are more likely to hold a license (44%) or to have applied for a license (36%). Noticeably, none of the surveyed storage-only providers currently hold a license, which can be explained by the fact that all surveyed wallet providers are exclusively handling cryptoassets. Nevertheless, one third contemplate filing for a license in the future; which is the case for the majority of exchange-only, payment-only, and multi-segment service providers.

Large firms (45%) are twice as likely as small firms (21%) to currently hold a license, although no major differences can be observed in terms of future applications. Furthermore, 49% of custodians currently operate under a license, 90% of which do not intend to apply for one in the future. This greatly contrasts with the percentage of non-custodial service providers holding a license (17%) or planning to file an application (74%).

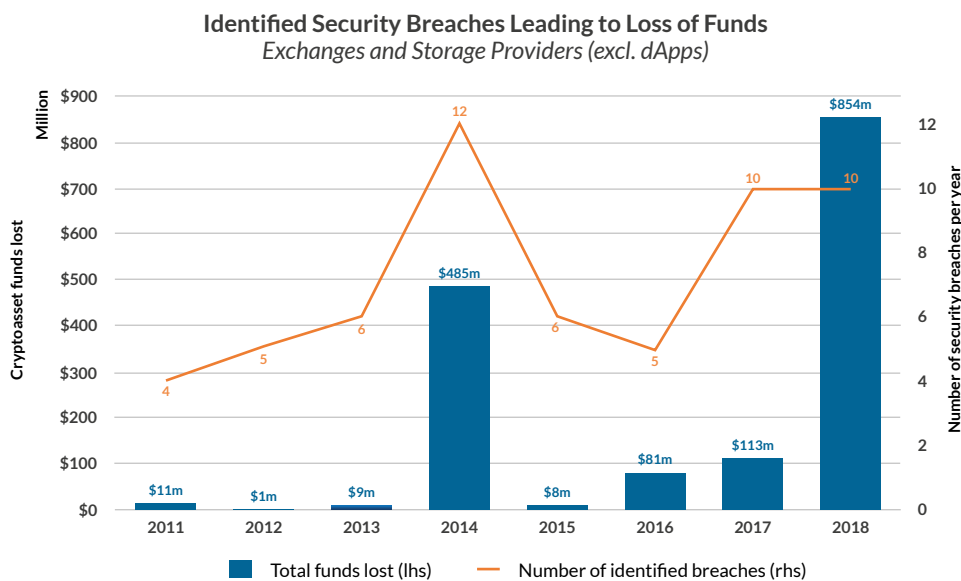
SECTION 6: IT SECURITY

Stolen Funds Remain a Major Issue

IT security remains a major risk factor for all cryptoasset actors. Cryptoasset holders are obvious targets for hackers and criminals as blockchain transactions are generally irreversible once the cryptoasset leaves the intermediary (e.g. exchange or storage provider).

According to **Figure 35**, exchange and storage service providers alone have accounted for the loss of more than \$1.5 billion of cryptoasset funds as a result of 58 identified security breaches. The actual number of hacks and security breaches - and the amount of lost and stolen funds - would be significantly higher if exit scams, the exploit of vulnerabilities in smart contracts, and unreported service provider hacks were to be included.

Figure 35: More than \$1.5 billion worth of cryptoasset funds have been lost as a result of security breaches at exchanges and storage providers



Note: data sourced from a combination of publicly available sources including Rados, CoinTelegraph, and CoinIQ. Exploited vulnerabilities in smart contracts (e.g. The DAO, Bancor) and exit scams have not been included.

Consequently, survey data indicates that concerns over cyber security risks have increased since the beginning of 2017. Large exchanges seem to be disproportionately concerned, presumably because rising prices and increasing amounts of funds in custody have made them lucrative targets for criminals. Challenges for securing internal systems and cryptoasset holdings are not limited to exchanges, though: miners also report growing concern over IT security risks, significantly up from last year.

Security techniques and methodologies are important determinants for traditional third parties such as banks and other financial institutions when deciding whether to enter new – or maintain current – business relationships.⁴⁴ To address IT security concerns, the cryptoasset industry and wider community

⁴⁴ An example constitutes Nonghyup Bank's reported refusal to renew its relationship with local South Korean exchange Bithumb following the exchange's security breach in June 2018. See Young-sil, Y. (2018) Bithumb to Stop Using Real-name Virtual Accounts to Customers from August. *Business Korea*. Available at: <http://www.businesskorea.co.kr/news/articleView.html?idxno=24028> [Accessed: 03 December 2018].

has tackled standardisation of cyber security practices as early as 2014 by issuing Cryptocurrency Security Standards (CSS) to complement existing standards such as ISO 27001.

IT Security Team

On average, large entities have a smaller share (6-10%) of their full-time staff being IT security professionals than small entities (11-20%), which may simply be a result of having a substantially larger workforce in general that distorts relative comparisons. However, the cost structure between large and small firms is very similar, with on average 11-20% of total budget allocated to IT security.

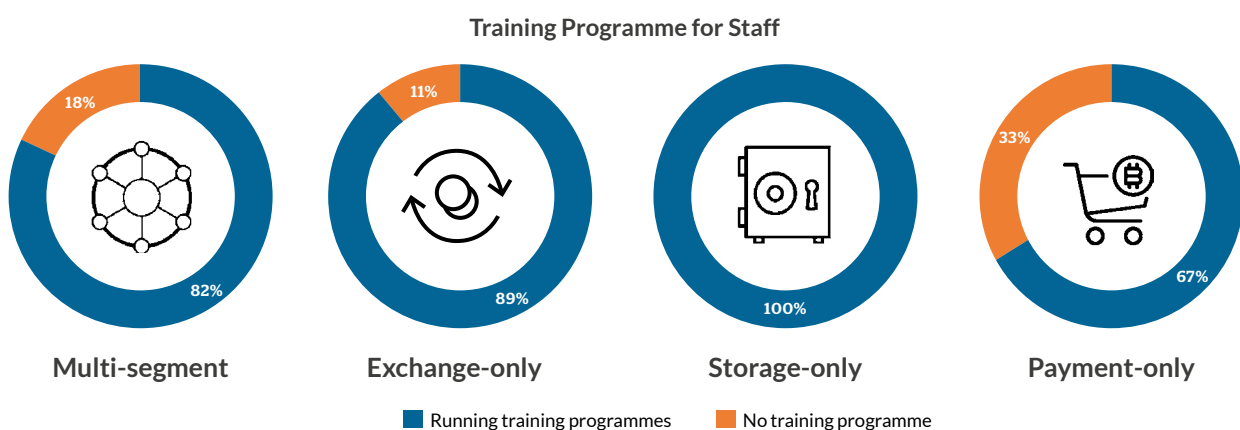
Differences in IT security headcount but similar budget shares are observed between small and large firms

Interestingly, significant differences arise when comparing industry segments: entities exclusively providing exchange and wallet services employ a larger share of IT professionals than payment-only service providers. Similarly, they also spend more on IT security: the majority of exchange-only and storage-only firms allocate more than 11% of their budget to IT security, whereas only 25% of payment-only do so. On average, entities engaged in multiple segments have 11- 20% of their staff working on cyber security; a similar share of their budget is dedicated to IT security.

Entities exclusively providing storage services have the highest headcount and budget share dedicated to IT security

As a preventive measure against potential future security breaches, companies have established dedicated training programmes, i.e. educational programmes for staff to understand major security risks (e.g. social engineering attacks, password security, general security principles) and other attack vectors. These programmes can be part of the employee onboarding process, but are often conducted on a regular basis. As pointed out by one survey participant, training programmes are a mandatory specification of international information security standards (ISO 27001).

Figure 36: Training programmes for staff are a common industry standard



Given that the majority of security breaches can be attributed to employee negligence and/or wrongdoing, it is unsurprising to see that the provision of regular staff training programmes has become a common industry standard across all industry segments (Figure 36). Companies exclusively providing storage services clearly stand out: all surveyed entities indicated running training programmes.

Remarkably, no striking difference can be observed between custodial and non-custodial service providers: around 80% of service providers within both categories have training programmes. As expected, large firms are more likely to run training programmes than small ones, though to a limited extent.

Frequency of training programmes do not only vary from one service provider to another, but also within a given company from one employee to another (e.g. technical and non-technical staff). One surveyed company noted that “basic security training for all non-technical staff happens every 3 months. Advanced training for tech staff is whenever possible.”

Support for staff training programmes has increased from 79% in 2016 to 89% in 2017

Security Audits

Security audits generally cover three dimensions of a company’s activities: people, processes, and technology. After conducting a risk-based assessment, security auditors collect evidence on a wide-range of cyber security aspects, from risk management to human resources security and cryptographic controls.

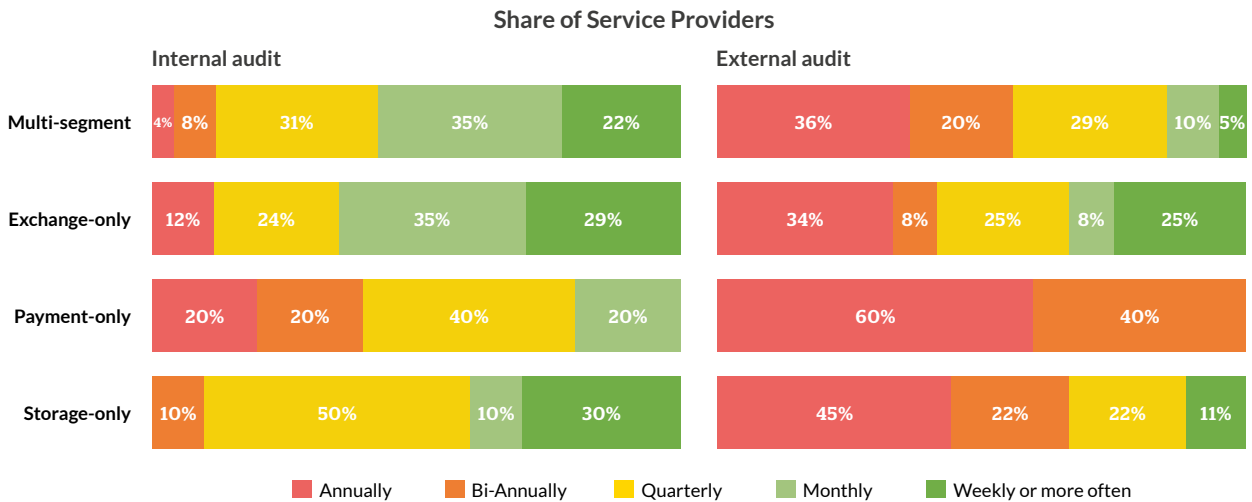
Audits can be either performed internally or externally. External audits are undertaken by an independent third party to identify security loopholes and vulnerabilities that may have been overlooked during internal security audits. In some jurisdictions (e.g. Japan), on-site inspections and security auditing processes by a third party, alongside a more general audit, are mandatory to apply for an operating license.

There is a general reluctance across the industry to talk about security-related issues

A significant number of respondents did not answer the question about the frequency of security audits. With regards to external security audits, more than half of exchange-only and payment-only entities responded “Not applicable” or “Decline to respond”. The figures are somewhat lower for storage-only service providers (35%) and entities engaged in multiple segments (37%). Respondents are fairly more willing to share information about internal security audits, but absence of responses remains considerably high: 44% for exchange-only service providers, 39% for storage-only service providers, 54% for payment-only service providers, and 28% for firms engaged in multiple segments.

This finding either conveys companies’ reluctance to disclose information about their security auditing processes or a lack of awareness about security audits from the surveyed representative. A critical reader would interpret companies’ reluctance as signalling the absence of any formal security verification standards. While disclosure would have shed light on best practices, absence of information reinforces common belief that some entities in the space do not follow security best practices.

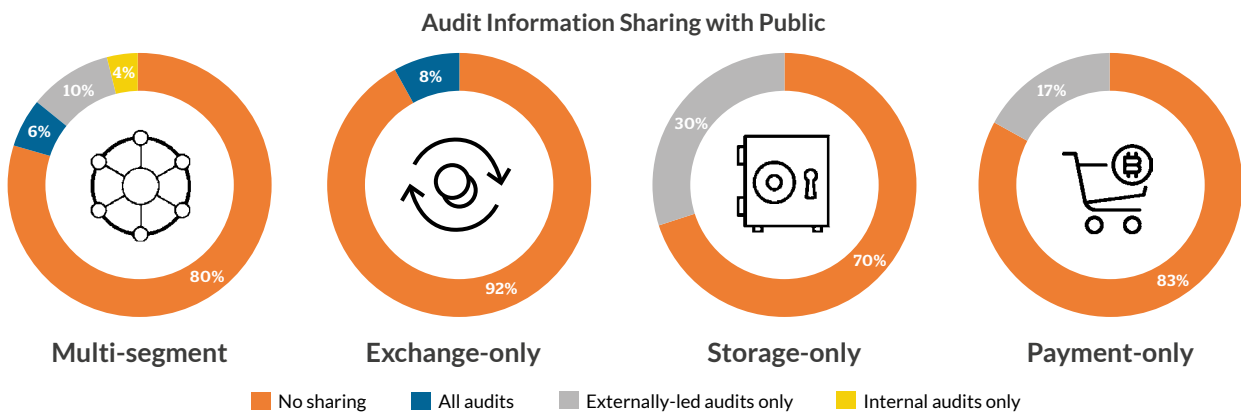
Figure 37: Internal security audits are conducted relatively frequently



Unsurprisingly, internal audits are conducted on a more regular basis than external audits (Figure 37). Multi-segment and exchange-only firms conduct both external and internal security audits on a more regular basis than other firms. However, storage-only entities are closely following when it comes to internal audits, while payment-only firms are lagging behind.

Nearly half of small companies perform an external audit on an annual basis, as opposed to 29% of large firms. However, small firms that conduct external audits several times a year do it more regularly than large firms: 13% of small firms indicate undertaking an external audit on a weekly basis, compared to only 4% of large firms.

Figure 38: The public sharing of information about audits is not common industry practice



As foreshadowed by the low response rate to the security audit question, entities very rarely share information with the public about their security audit results (Figure 38). Entities that do share information publicly are more likely to report on externally-led audits (e.g. announce that an audit has taken place). Protection against potential attackers by disclosing as little information as possible is one possible interpretation.

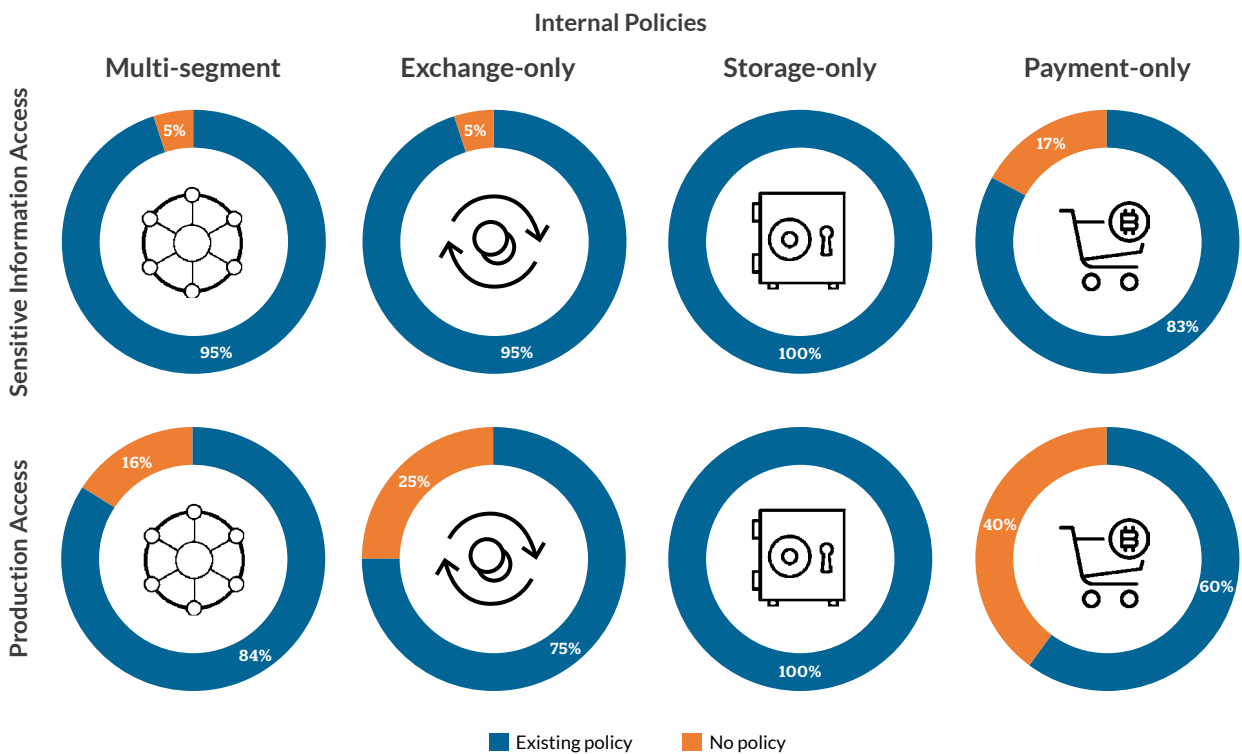
Only a limited number of payment-only and storage-only service providers (17% and 30%, respectively) share information about externally-led audits. Entities specialising in the exchange segment appear to share the least information of all service providers: only 8% publish information on security audits (both internal and external).

The likelihood of information sharing only slightly varies with company size: 25% of large firms indicate disclosing information about security audits, compared to 16% of small firms. A comparison with 2017 survey data suggests that there is a trend to share less information: while one third of large exchanges reported in 2017 to publish data on security audits, none of surveyed large exchanges did so in 2018.

Internal Policies

Figure 39 outlines that a majority of service providers have an internal policy on both access to sensitive customer information (e.g. identification documents, bank details) and access to production environment (e.g. private keys).

Figure 39: Cryptoasset companies are more likely to have written policies regarding access to customer-sensitive information than production access



In line with previous findings, payment-only firms are less likely to have written policies on both sensitive information access and production access than companies operating in other segments. Figures for custodians and non-custodians are mostly similar, as both categories report having a policy for production access in place. Interestingly, 13% of custodial service providers do not have a written policy on sensitive customer information access, while all non-custodians do.

SECTION 7: MINING SEGMENT

7.1 The Power of Miners

Miners are the entities that are involved in the processing of transactions on public blockchains by deciding which transactions will be added – often in a single batch called a “block” – to the global ledger (“blockchain”). This process generally requires attaching a financial cost to each miner’s vote on the next block in order to prevent Sybil attacks.⁴⁵

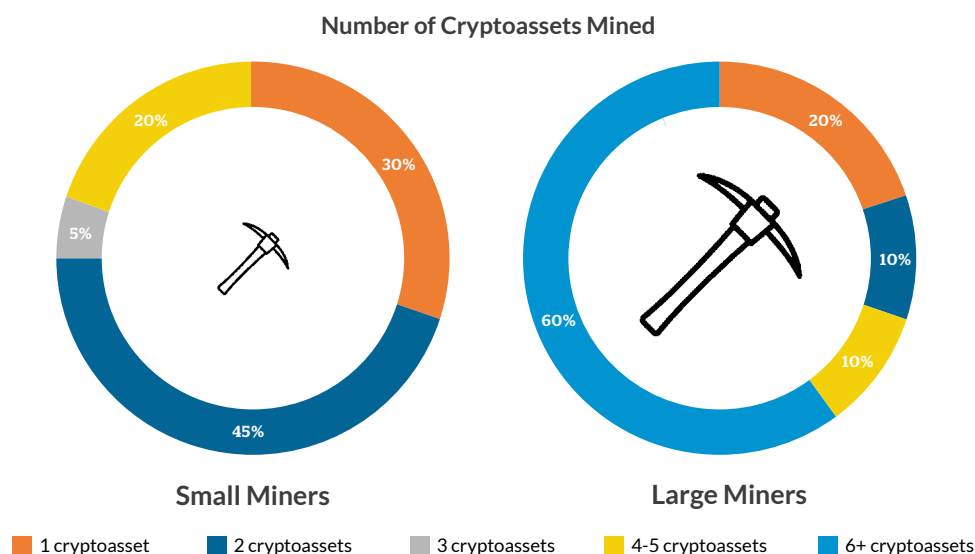
In proof-of-work (PoW), the first and most common Sybil prevention mechanism used by cryptoassets, the costs come in the form of special equipment and electricity required for solving cryptographic puzzles. In proof-of-stake (PoS), an alternative mechanism recently rising to popularity but still mostly experimental, the costs are modelled in the form of a “token deposit” provided by miners that can be destroyed (“slashed”) in case misbehaviour and fraud are detected.

PoW posits that miners have a vote proportional to the computing power (*hashpower*) they provide, whereas PoS gives miners a vote proportional to the “stake” they provide as deposit. At the time of writing, PoW remains the dominant mechanism used by most cryptoassets. The remainder of this section will thus cover primarily PoW miners rather than PoS *stakers*.

Cryptoasset Selection

Access to public blockchains and broader DLT systems is unrestricted and permissionless. This means that miners can decide to enter any cryptoasset system and participate in transaction processing. Survey data shows that the majority of miners are mining more than a single cryptoasset, although significant differences can be observed between small and large miners (Figure 40).

Figure 40: Large miners have a significantly greater diversification than small miners in terms of the number of cryptoassets they mine



⁴⁵ Sybil attacks refer to an entity creating multiple fake identities in order to rig a vote.

Large miners tend to mine a greater number of cryptoassets: 60% of surveyed large companies mine six cryptoassets or more, whereas no small-scale miner is operating across more than five cryptoasset systems. This suggests that scale in the mining segment is an effective factor for reducing barriers to entry to local cryptoasset ecosystems.

When it comes to determining which cryptoassets to mine, both small and large miners indicate that the price is the most important criterion – although large miners also consider market capitalisation, daily reward amount, and cryptoasset price as equally important (Table 4).

Table 4: Large miners consider a larger set of criteria to determine what cryptoassets to mine

	Large Miners	Small Miners
Market capitalisation	88%	38%
Daily reward amount	88%	52%
Price of cryptoasset	88%	76%
Reputation	75%	29%
Energy requirement	63%	24%
Proof system	63%	29%
Low number of other miners/mining pools	25%	19%
Large number of other miners/mining pools	13%	10%
Ideology/personal affection	13%	19%
Friends/colleagues recommendation	13%	5%

Somewhat surprisingly, the energy requirement for mining a particular cryptoasset (and therefore the associated costs) appear to be a less important decision factor – even more so for small miners. Three quarters of large miners also take into account the reputation of a cryptoasset project before engaging in mining. Low levels of competition are preferred to high competition, as these cryptoassets may provide an opportunity for wondrous sudden surges in price (and therefore profitability).

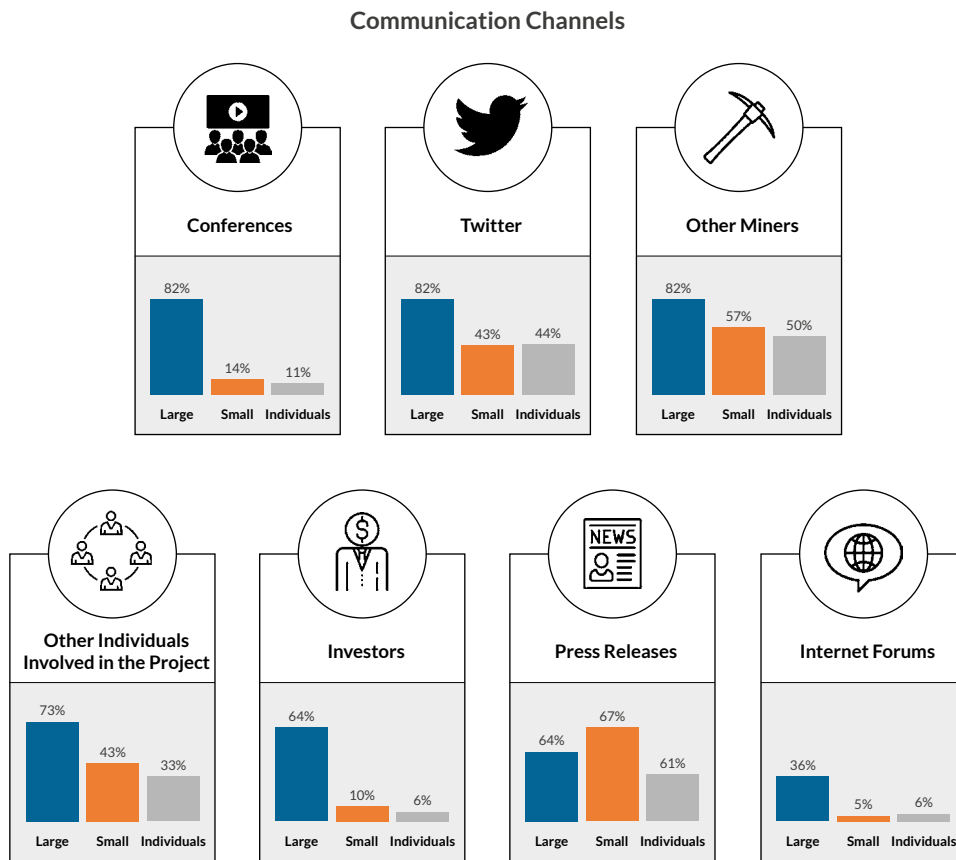
Interestingly, nearly one in five small miners mine coins out of personal affection or because they are ideologically inclined to a coin’s philosophy. This seems to be in line with the finding that miners generally tend to be “loyal” to the cryptoasset(s) they mine: only 13% and 7% of large and small miners, respectively, have discontinued mining a specific cryptoasset since January 2017.⁴⁶ This suggests that most miners are not constantly switching between different coins.

A majority of miners continue mining the same cryptoasset(s) since early 2017

Miners use a variety of communication channels in order to stay up-to-date with the latest developments in the local cryptoasset ecosystems that they support (Figure 41). Large miners use significantly more communication channels than small miners and individuals: while the latter primarily rely on press releases and direct communications among themselves to keep abreast of recent developments, large miners also gather significantly more intelligence from conferences, social media (e.g. Twitter) and investors directly.

⁴⁶ The reasons for stopping mining a particular coin are manifold but can be grouped into the following three categories: rising costs (and/or falling prices) eating away profit margin, change to PoW algorithm, and coin death.

Figure 41: Miners use a variety of off-chain communication channels to stay updated with regards to the latest developments of the cryptoassets they mine



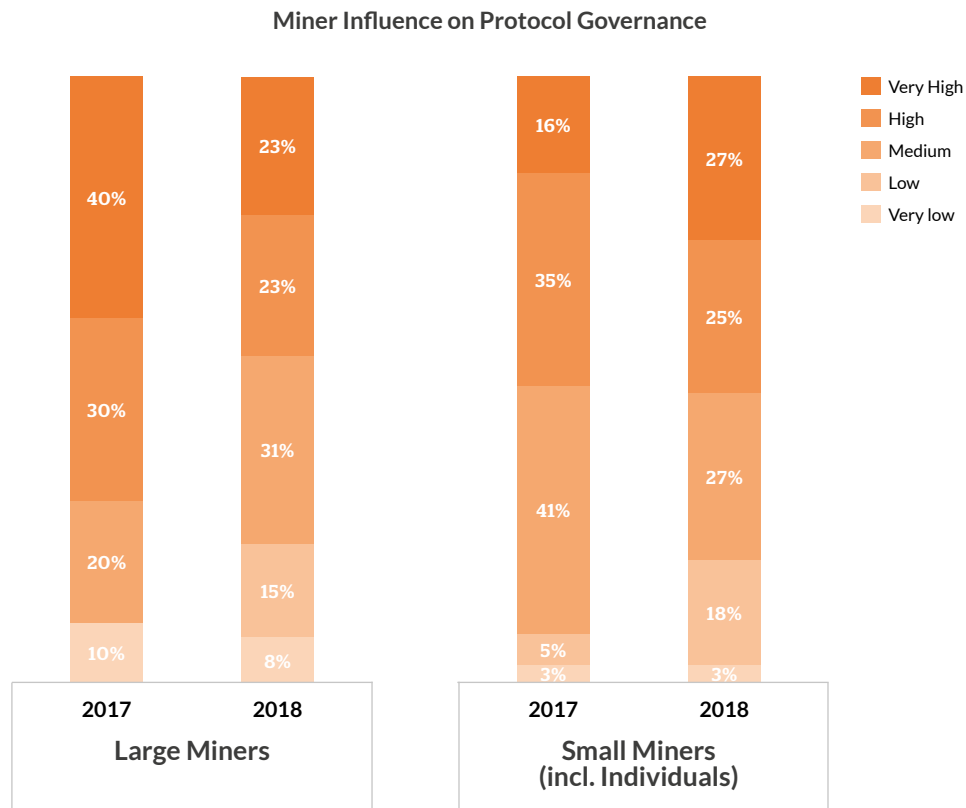
Influence on Decision-Making Process

Concerns have emerged over time in the ecosystem over the role of miners and their relative influence on the decision-making process of the DLT systems they support. These concerns were illustrated in the August 2017 split of Bitcoin Cash (BCH) from the Bitcoin (BTC) network over disagreements on whether users or miners should be in control of protocol governance.⁴⁷

Recent forking episodes have demonstrated the multi-dimensional aspect of public blockchain governance, which involves different groups of entities (e.g. exchanges, wallets, miners, developers, users, merchants) keeping a check on each other. As a result, it appears that miners have become more divided in 2018 with regards to how they perceive their influence on protocol governance (Figure 42).

⁴⁷ In the meantime, Bitcoin Cash itself forked into Bitcoin ABC (BAB) and Bitcoin SV (BSV) in mid-November 2018. At the time of writing, it appears that Bitcoin ABC has won the “hash war” and is recognised as the successor of the original Bitcoin Cash system by receiving the original BCH exchange ticker.

Figure 42: Miners are becoming more divided on their impact on protocol governance



While 70% of large miners believed that their influence on protocol governance was either high or very high in 2017 – before the Bitcoin Cash fork – only 46% of large-scale miners do so in 2018. This change in figures mirrors their growing concern about unexpected changes to the protocols of the cryptoassets they are mining (e.g. a PoW change that would make their equipment worthless), an issue that has become more relevant given the increased frequency of hard forks since mid-2017.

In contrast, the share of small miners believing they have a very high influence on protocol governance has grown since 2017, exceeding that of large miners. Nevertheless, unlike last year's survey no major differences can be observed between small and large miners. Even though the majority of both small and large miners feel that they have at least some influence on protocol governance (i.e. "medium" or above), overall miners appear less confident in their ability to shape protocol governance than they did in 2017.

Concentration Concerns

Another major concern in the ecosystem is the (perceived) growing concentration of mining in the hands of a few entities ([Table 9 in Appendix](#)). The fear of increased mining centralisation goes against the main objective of cryptoasset systems; notably the ability to remain free from third-party control.

While these concerns are certainly justified, they often tend to myopically focus on “miners” as a whole without distinguishing between different activities. Contrary to popular beliefs, miners are not a homogenous group of entities that all perform the same tasks. Instead, miners can engage in a variety of activities across the mining value chain (see [Figure 3](#)); activities that can be substantially different one from another.

Three major types of mining concentration need to be taken into consideration

As a result, it is important to separately analyse each of the activities that are relevant to mining concentration and identify the actors that occupy a dominant position in these respective areas. In essence, concerns about concentration risks in cryptoasset mining can be grouped into three main categories:

1. Hardware manufacturing concentration

The market for the manufacturing of specialised mining hardware equipment that will be used to solve the cryptographic PoW puzzles. The analysis requires considering both the number of competing hardware manufacturers as well as their geographic location.

2. Hashing facility concentration

To determine whether hashing is concentrated, the ownership of hashing facilities (also often referred to as *mining farms*), the entities owning and/or operating these facilities (called *hashers*), and their geographic distribution need to be inspected.⁴⁸

3. Pool concentration

Hashers can contribute hashpower to mining pools.⁴⁹ Pool operators decide which transactions to include (or not to) in a new block before sending the candidate block to connected hashers. Both pool structures and their geographic distribution need to be investigated.

The following subsections will cover each of the three mining concentration types by taking a deeper look into the respective entities engaged in the related activities.

7.2 Hardware Manufacturing

Solving a cryptographic PoW puzzle amounts to finding a hash whose value remains below a specific target value.⁵⁰ This can be compared to a lottery, where there is one winning ticket that gets randomly chosen: the more tickets you have, the more *likely* you are to win the lottery. Similarly, the more hashes you produce, the more likely you are to find a valid solution to the PoW puzzle and receive the block reward.

48 Hashing facilities are akin to data centres specialised for cryptoasset mining: they can host thousands of mining machines that generate hashpower.

49 Hashers connect to mining pools and contribute hashpower in order to smoothen pay-out rates, as pooled mining increases the likelihood of finding a new block and thus receiving the block reward.

50 A hash is a bit string of fixed size that is generated by running a certain input of any size through a cryptographic hashing function. Changing a single bit of the input will result in an entirely different, unpredictable hash (i.e. output). Cryptographic hashing functions are often used to quickly prove data integrity.

Mining Equipment and Algorithms

Hashing is the process of using machines to generate hashes as a potential solution to a PoW puzzle. Hashers are miners who own and operate machines that generate hashes. These machines can range from simple general-purpose computers to application-specific ASICs that are optimised for performing one single task.

General-purpose machines are devices that can perform multiple tasks and can thus be repurposed for other applications. *Application-specific* machines are devices that are specifically designed to perform a single task very well; thus, they cannot be repurposed and used for other applications (e.g. mining other cryptoassets that use a different algorithm).



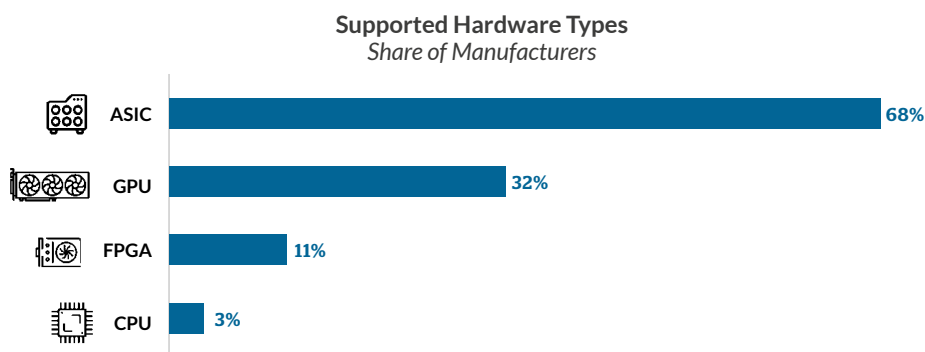
Different Hardware Types

Different types of hardware equipment are being used for cryptoasset mining. They can generally be grouped into the following four categories:

1. **CPU:** The *Central Processing Unit* is a processing device that performs typical control function. Bitcoin mining was first performed using general-purpose CPUs of simple computers.
2. **GPU:** The *Graphic Processing Unit* is the processor that handles display functions and is generally referred to as graphic card. GPU-based Bitcoin mining quickly took over CPU mining in late 2010 because it offered superior efficiency and processing speed.
3. **FPGA:** A *Field Programmable Gate Array* is a particular hardware device whose performance is significantly superior to graphic cards and comes close to performance of customised hardware chips. FPGA-based Bitcoin mining gained significant traction in mid-2011 when the first hashers switched from GPUs to FPGAs.
4. **ASIC:** An *Application-Specific Integrated Circuit* is a customised hardware chip specifically optimised for performing a single task. The emergence of the first Bitcoin ASICs in mid-2012 rapidly displaced FPGA-based mining

Data from an augmented sample of more than 30 cryptoasset mining hardware manufacturers show that nearly 68% of manufacturers produce ASICs – or at least components – that are application-specific machines optimised for a particular mining algorithm (**Figure 43**). GPU-based rigs are manufactured by roughly one third of hardware producers. 71% of surveyed manufacturers indicate that they specialise in the production of one type of equipment.

Figure 43: ASICs and GPU rigs are the most produced mining hardware equipment



Note: the analysis is based on a sample of 30+ manufacturers obtained from a combination of survey data and publicly available data.

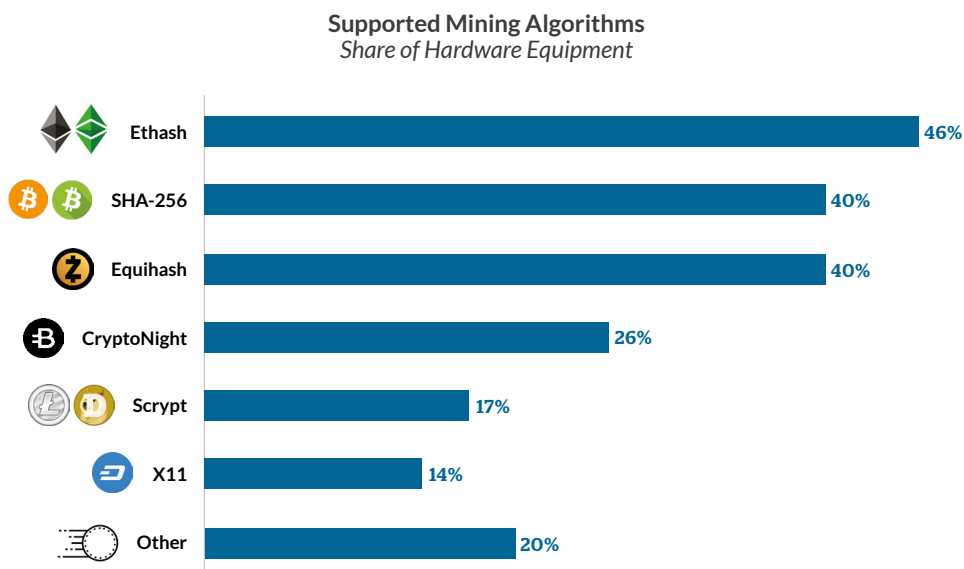
However, the majority of selected manufacturers produce custom mining rigs that are composed of existing hardware machines by other manufacturers. This means that they primarily focus on repurposing existing components to build fully-integrated hardware optimised for cryptoasset mining. Only a small number of surveyed manufacturers produce their own chips.

The majority of manufacturers produce custom mining rigs

Every mineable cryptoasset uses a particular mining algorithm for its PoW: some are using the same algorithm whereas others intentionally choose to use a less common algorithm. Each algorithm has its own peculiarities – and as a result, different types of hardware equipment that are best suited for the task. This means that a machine that is doing well in Bitcoin mining is not necessarily best suited for Ethereum mining, and vice-versa.

Over time, increasing popularity and subsequent price increases of certain cryptoassets have spurred investment into R&D to build application-specific hardware that implements various optimisation techniques designated specifically for the underlying mining algorithms. This has resulted in the emergence of ASICs that are optimised for a given mining algorithm: these machines are considerably more efficient and performant for solving that specific mining algorithm compared to general-purpose hardware. As long as there is a financial incentive (i.e. high profit margins for mining a specific cryptoasset), manufacturers will continue designing new chips optimised for the underlying mining algorithm.

Figure 44: Ethereum’s Ethash is the most often supported algorithm by manufacturers



Note: the analysis is based on a sample of 30+ manufacturers derived from a combination of survey data and publicly available data.

Data suggests that Ethash, a mining algorithm first used by the Ethereum network, is the most often supported algorithm by hardware manufacturers (Figure 44). Ethash is closely followed by SHA-256 (used in Bitcoin and Bitcoin Cash, among others) and Equihash (used in ZCash) in terms of support by selected manufacturers.

Two-thirds of surveyed manufacturers indicate that equipment is primarily produced in a single country, whereas others report to have production facilities in two or three countries. Reported production sites are primarily located in China and Taiwan, but South American countries (e.g. Chile, Paraguay), Western European countries (e.g. France, UK) and Eastern European countries (e.g. Russia, Belarus) were also mentioned.

Distribution Channels

Mining equipment can be primarily purchased via online stores (71% of surveyed manufacturers) that are either directly operated by the manufacturers themselves or via third-party websites. 57% of surveyed manufacturers also conduct direct B2B sales to distribute their equipment directly to customers. Customers can be professional hashing facility operators (e.g. proprietary hashers, cloud mining service providers, remote hosting service providers) as well as individuals.

Major hardware manufacturers have indicated that their customer base has experienced tremendous growth since they launched activities: two manufacturers report growth figures as high as 667% and 2,900%, respectively, for the period running from 2015 to 2017. Interestingly, demand does not seem to have slowed down significantly in the first two quarters of 2018 despite the downturn in cryptoasset prices.

Online stores appear to be the main distribution channel for manufacturers

The two largest Bitcoin ASIC hardware manufacturers alone have sold more than a combined 5 million machines worldwide.⁵¹ The total number of direct customers is estimated to be a lower six-digit figure.⁵² It is worth mentioning that there are millions of users who buy mining contracts at cloud mining service providers in order to “virtually” mine their preferred cryptoassets. However, they cannot be considered “hashers” themselves since they do not operate the machines.

It appears that the majority of customers from hardware manufacturers are based in Asia-Pacific (principally in China), although the share of European and North American customers has been increasing lately. While the two largest Bitcoin ASICs manufacturers indicate that the majority of customers are domestic, efforts towards geographically diversifying their customer base beyond domestic markets can be observed.

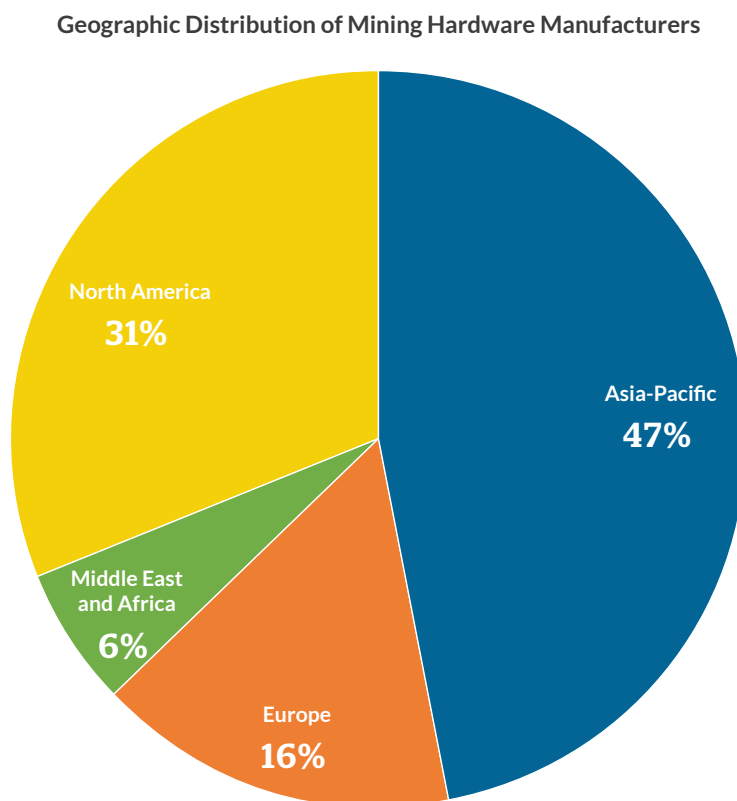
How Concentrated Is Manufacturing?

There are more than 30 identified cryptoasset hardware manufacturers worldwide, although the total number is likely higher. They are present around the world – with the exception of South America – with the largest presence in Asia-Pacific and North America (**Figure 45**).

⁵¹ This data point is based on information included in the Bitmain and Canaan pre-IPO prospectuses, which are publicly available.

⁵² Idem



Figure 45: Mining hardware manufacturers are primarily based in Asia-Pacific and North America

Note: the analysis is based on a sample of 30+ manufacturers derived from a combination of survey data and publicly available data.

When looking at the type of mining hardware devices, it appears that 62% of ASIC producers are based in Asia-Pacific, among which 73% are based in China, whereas 14% and 19% are based in Europe and North America, respectively. In comparison, 50% of GPU producers are based in North America, primarily in the United-States, while the remaining are split across Asia-Pacific (25%), Europe (13%) and MEA (13%).

Mining hardware manufacturing is relatively concentrated

However, as explained above cryptoassets use different mining algorithms which require different machines for the most efficiency. Mining hardware manufacturing concentration varies from one cryptoasset (or rather mining algorithm) to another and is dependent on a variety of factors. Hardware manufacturing for certain algorithms (e.g. Bitcoin's SHA-256) is currently very concentrated (both geographically and from an operator perspective): small miners raise concerns over growing difficulties in accessing state-of-the-art hardware equipment in a timely fashion, an issue that large miners seem to be less concerned by.

Balancing out the current concern about concentration are recent statements from established semiconductor corporations announcing to enter cryptoasset hardware manufacturing.⁵³ This would then lead to a greater diversity in hardware offering and reduce concentration in the market. On the other hand, many cryptoassets can be mined using general-purpose hardware that is easily available and can be repurposed. Some believe that mining hardware will soon become commoditised: the anticipated

⁵³ For an example, see Samsung (2018) Samsung Electronics Announces Fourth Quarter and FY 2017 Results. *Press Release*. Available at: <https://news.samsung.com/global/samsung-electronics-announces-fourth-quarter-and-fy-2017-results> [Accessed: 02 December 2018].

end of significant breakthroughs in chip design combined with the entrance of new players will likely reshuffle market dynamics sufficiently and reduce hardware manufacturing concentration overall.

7.3 Mining Facilities

Meet the Hashers

The process of hashing is permissionless: anyone in the world can – at least in theory – enter cryptoasset mining by downloading and running mining software on a machine. Since the puzzle difficulty of many valuable PoW blockchains has risen substantially over time, hashing now often requires the use of many specialised machines to make operations economically viable. Hashers range from individual hobbyists running a few rigs at home to large companies operating large-scale data centres hosting 100,000 rigs or more.

Hashers can mine for their own account (*proprietary*) or use their data centres to provide services to customers such as *remote hosting* (operating and maintaining customer-owned hardware) and *cloud mining* (renting hashpower). They generally point their hashpower to a mining pool to smoothen pay-outs.

Facility Set-up Decision Factors

Surveyed miners were asked to rank the most important decision factors used for assessing the suitability of a location for a new mining facility ([Table 8 in Appendix](#)). The following five factors stand out:

1. Access to ample and low-cost electricity supply

Running hashing facilities requires substantial amounts of electricity that can be adjusted dynamically in accordance with market conditions. It is not unusual for mining farm operators to make deals with local energy suppliers to guarantee access to sufficient and affordable electricity.⁵⁴

2. Friendly regulatory environment

Local geographies that take a favourable regulatory stance with regards to mining and create incentives (e.g. tax-related, subsidies) will attract hashers.

3. Stable political situation

Ranked third, it highlights the need for a stable and predictable political environment that protects property rights and has a functional justice system. Small miners indicate that the possibility of government seizure or shutdown of their facilities constitutes the biggest risk.

4. Good Internet connectivity

A fast and reliable Internet connection is paramount for hashers in order to quickly receive and broadcast data (e.g. instructions, pool shares proving the “work” performed).

5. Cold climate

Mining machines consume a lot of energy, which requires constant cooling to prevent them from overheating. Facilities located in regions with cold climate offer substantial advantages in terms of cooling cost savings.

Interestingly, the presence of cheap land and skilled labour was ranked much lower, suggesting that these are only secondary factors with minor impact on decision-making. Only South American miners indicated that a low crime rate would be a major decision factor.

⁵⁴ In fact, large surveyed miners ranked sudden increases in electricity prices as the highest operational risk factor ([see Table 8 in Appendix](#)).

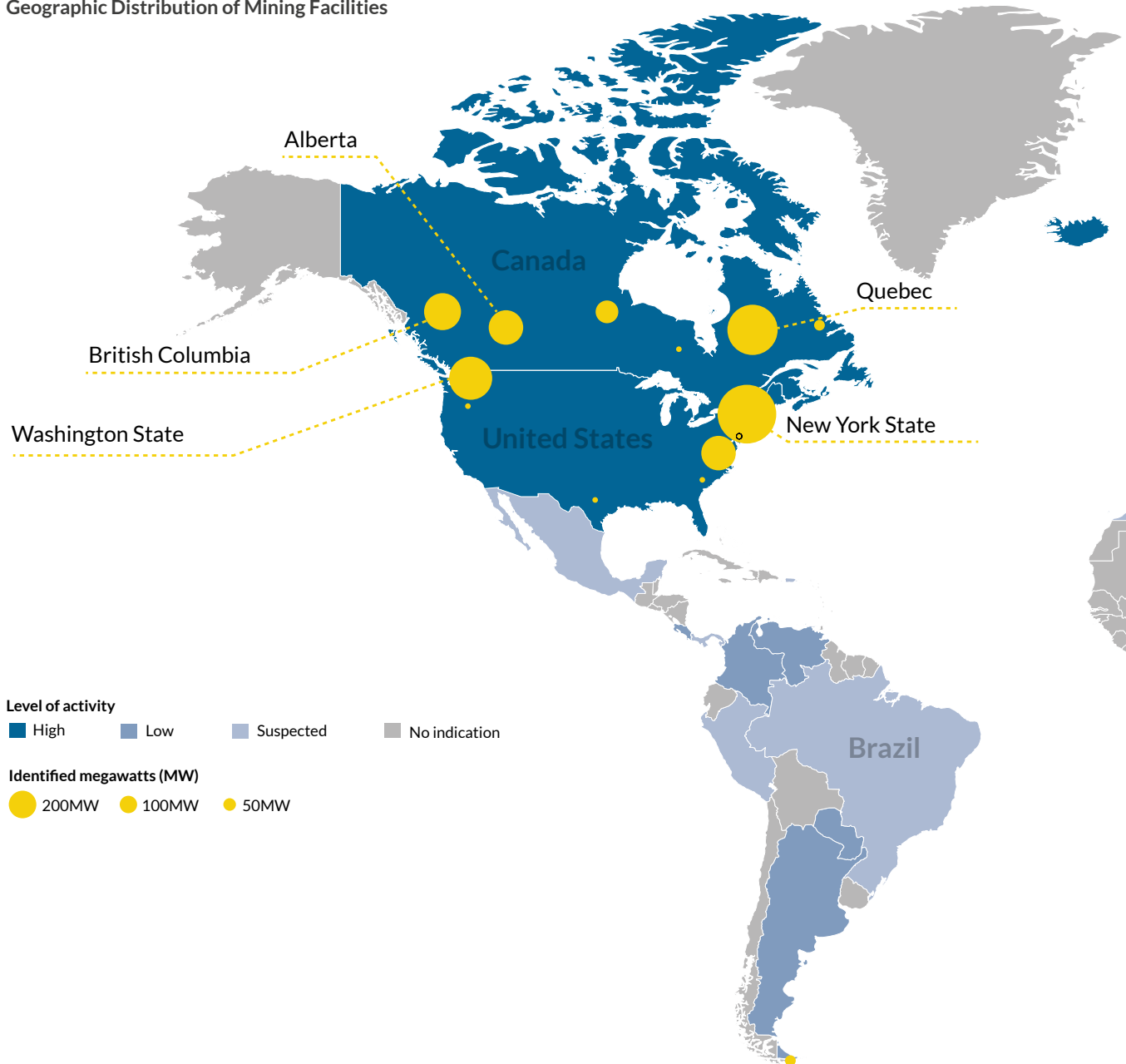


Distribution of Mining Facilities

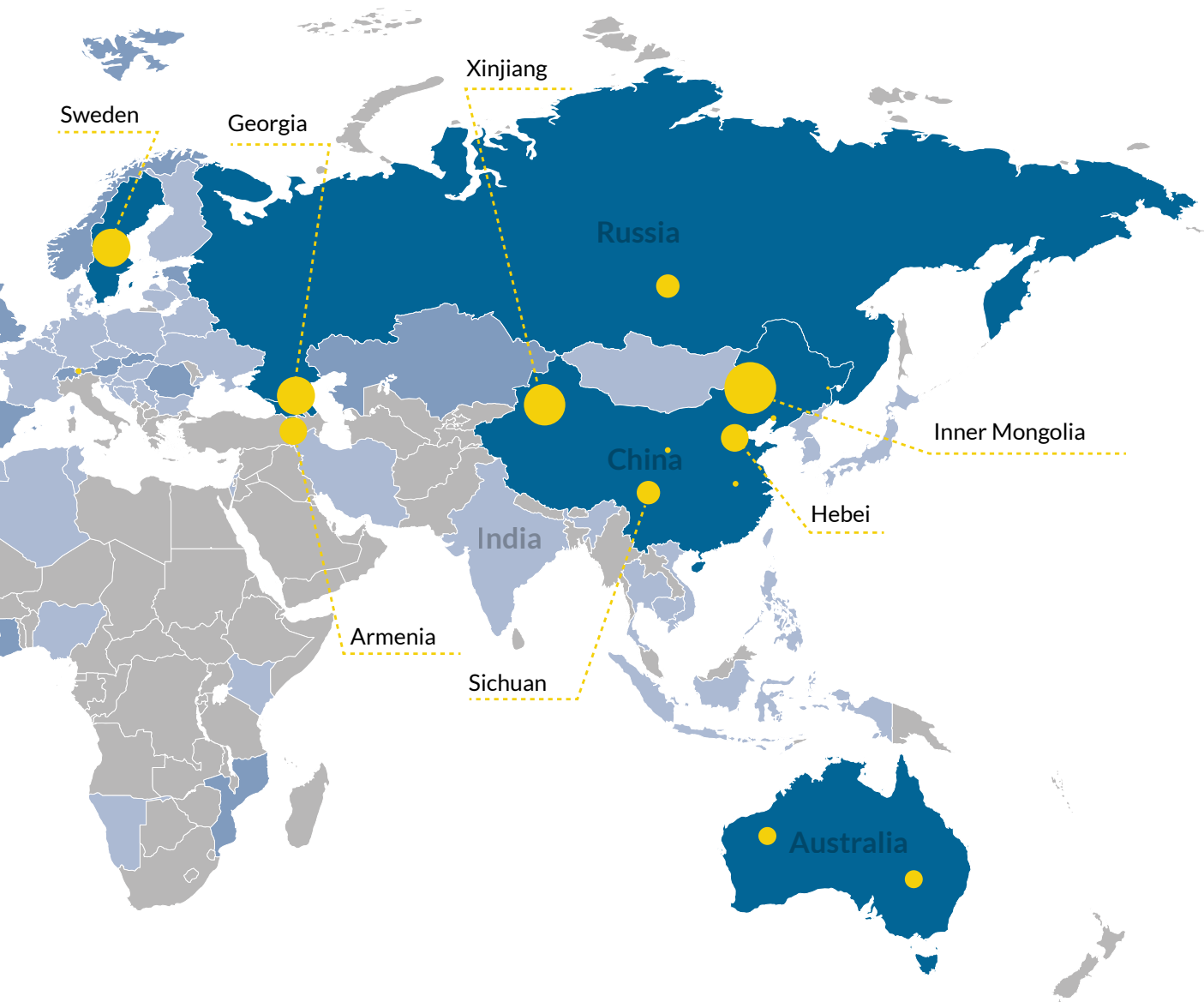
Through a combination of survey data and public sources, the research team built a repository of 128 mining facilities around the globe.⁵⁵ Figure 46 illustrates that hashing activities have scaled globally and are distributed across all world regions, albeit not equally: some continents (e.g. Asia-Pacific, North America) host significantly more mining activity than others (e.g. MEA).

Figure 46: The Global Cryptoasset Mining Map

Geographic Distribution of Mining Facilities



⁵⁵ Data was collected from company websites, press releases, news articles, public forums, social media, and insights from industry experts. When available, the research team aggregated the capacity of regional facilities measured in megawatt (MW) and estimated the level of mining activity in each country. Countries hosting more than 40 MW identified in the above analysis are considered to have a high level of activity. Countries with low activity levels are known to host mining facilities, whereas countries with suspected activities could not be confirmed by multiple sources. In total, 1,745 MW powering mining facilities have been identified.



Note: this map is based on a dataset of 128 mining facilities. A total capacity of 1.7 gigawatts (GW) could be identified for 93 facilities. High-activity countries have 40 megawatts (MW) or more identified capacity; low-activity and suspected activity levels are estimates.

The mining map shows that hashing facilities are primarily located in China, North America (USA and Canada), and North-Eastern Europe (Russia and Georgia). Facilities located in China have been responsible for the majority of mining in the past and the country remains a major hub despite changes in the regulatory environment.

In fact, the government's restrictive measures on mining seem not to have led to a massive exodus of Chinese miners overseas. While some large Chinese miners have opened additional facilities overseas, small domestic miners have been disproportionately affected by falling prices and some were forced to shut down their facilities. The bulk of mining is located in the Northern provinces (e.g. Inner Mongolia, Xinjiang, Hebei, Heilongjiang) and Southwest China (e.g. Sichuan, Yunnan, Guizhou).

Substantial growth of mining activities can be observed in North America, but China remains a major hub

Specific states in the USA (e.g. Washington, New York), Canadian provinces (e.g. Québec, British Columbia, Alberta) and some Scandinavian countries (e.g. Iceland, Norway, Sweden) seem to particularly benefit from these developments, as rapid growth in local mining activities can be observed.⁵⁶

It is no coincidence that these regions satisfy all five criteria laid out in the previous subsection: cheap electricity is provided in ample volumes – often from excess capacity of hydroelectric or geothermal power, the seasonal cold climate drives down cooling costs, and the countries are among the most developed in the world (i.e. having very high human development index scores, good network infrastructure, and functioning institutions).

A growing level of activity can also be observed in some South American countries (e.g. Argentina, Colombia, Venezuela) and Western European countries (e.g. France, UK, Switzerland). It is worth noting that the mining map is incomplete and does only capture a share of global mining activities: some countries may have higher – albeit hidden – activity levels.

Nevertheless, available data suggests that cryptoasset hashing has become more geographically distributed since 2017, particularly with China losing relative “market share” to some North American and Scandinavian regions. Improvements in the geographic distribution will make it more difficult for attackers to seize or shut down hashing facilities, a concern that was ranked first by small miners that took part in the survey. Similarly, it will make global mining less dependent on local events, both economically and politically-driven (e.g. sudden increases in electricity prices, which is the highest-ranked concern of large miners, or the establishment of a tax regime on mining profits particularly worrying small miners and individuals).

A relatively large number of operators cannot hide the fact that a few are dominating

Similarly, hashrate ownership appears to be relatively distributed across many operators: the research team could identify more than 60 different facility and data centre operators, with the majority of identified hashers operating a single facility. However, facility size and capacity do vary significantly from one farm to another. Moreover, hashers can also operate multiple facilities, with some large companies running more than a dozen.

Overall, concern about geographical concentration of hashpower has been overplayed: in reality, hashing appears to be globally distributed. However, when it comes to concentration of hashpower in terms of ownership, the picture is less clear: while there are at least several dozen operators of facilities around the globe, a small number of large hashers seem to occupy a dominant position.

⁵⁶ However, this tendency for clustering in specific locations might be not always be harmonious: In Québec, for instance, the recent surge in mining activities has led to stricter governmental intervention and higher electricity charges for companies in the mining industry in June 2018 (Data available at http://publicsde.regie-energie.qc.ca/projets/457/DocPrj/R-4045-2018-A-0001-Dec-Dec-2018_06_18.pdf [Accessed: 02 December 2018]).

How Much Energy Does Cryptoasset Mining Consume?

The energy-intensive nature of PoW mining and its potential negative implications on the environment have sparked heated debates. Multiple studies estimating the total energy consumption were published using various methodologies which resulted in widely divergent figures.⁵⁷

Estimating the actual energy usage of the major PoW cryptoasset systems requires extensive data on the type of mining equipment used, the nature of energy sources, and the overall energy efficiency of mining data centres. For the lack of reliable data, the research team bases the estimate on a range rather than a precise value.

The top-6 cryptoassets consume between 52 and 111 TWh of energy a year

The lower-bound estimate follows the same methodology as last year's study: it assumes that all hashers are using the most efficient hardware available in the market and run the most efficient data centres.⁵⁸ The upper-bound estimate, based on a methodology developed by Marc Bevand⁵⁹, assumes that all hashers always run the least efficient hardware available in the market as long as the hardware yields a positive return when purely considering electricity costs (i.e. operational expenses).⁶⁰

A separate analysis is conducted for the six major PoW cryptoassets (Bitcoin, Bitcoin Cash, Ethereum, Litecoin, Monero, and ZCash) and outputs are combined to provide an aggregate estimate. **Figure 47** shows that as of mid-November 2018, the top-6 cryptoasset networks are estimated to collectively consume between 52 and 111 terawatt-hours (TWh) of energy a year, up from between 18 and 42 TWh just a year before. Bitcoin alone accounts on average for 75% of the total energy consumption.

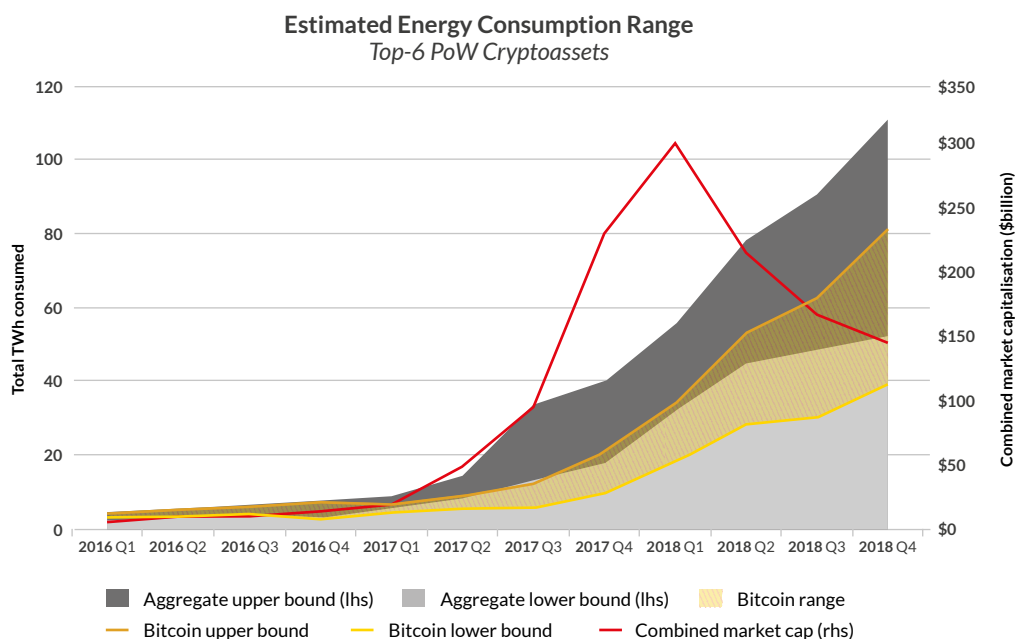
⁵⁷ For a comparison of different estimates and their underlying methodology, see Kolbie, N. (2017) How much energy does Bitcoin mining really use? It's complicated. *Wired*. Available at: <https://www.wired.co.uk/article/how-much-energy-does-bitcoin-mining-really-use> [Accessed: 02 December 2018].

⁵⁸ Using Bitcoin as an example, the following hardware types were used for each respective period as the most efficient equipment: Antminer S7 (Q1 to Q3-2016), Avalon A721 (Q4-2016), Antminer T9 (Q1 and Q2-2017), Antminer S9 (Q3-2017 to Q2-2018), DragonMint 16T (Q3 and Q4-2018). Furthermore, it was assumed that facilities have a power usage effectiveness (PUE) similar to the most efficient data centres in the world (1.03) as well as a low parasitic power consumption of 5%.

⁵⁹ Bevand, M. (March 2017) Electricity consumption of Bitcoin: a market-based and technical analysis. *Personal Blog*. Available at: <http://blog.zorinaq.com/bitcoin-electricity-consumption/> [Accessed: 06 November 2018].

⁶⁰ Using Bitcoin again as an example, the following hardware types were used for each respective period as the least efficient equipment: Avalon A6 (Q1 to Q4-2016), Avalon A721 (Q1 to Q4-2017), Antminer T9 (Q1 and Q2-2018), Avalon A821 (Q3 and Q4-2018). Furthermore, it was assumed that facilities have a PUE of 1.33 and a parasitic power consumption of 15%.

Figure 47: The combined energy consumption of the top-6 PoW coins has consistently grown despite the recent downturn in market capitalisation



Note: 2018 Q4 estimates are based on available hashrate data from October to mid-November 2018. The recent decline in hashpower (and as a result total energy consumption) in late November 2018 is not covered by the chart.

Taking the latest mid-point of the estimated range as a reference (82 TWh), it can be established that the top-6 cryptoasset systems consume approximately as much energy as the entire country of Belgium in 2016.⁶¹ At the same time, this figure amounts to less than 0.01% of the world's total annual energy production⁶², or the equivalent of all electricity generated by biomass and solar energy in Germany alone.⁶³

Energy consumption is a direct function of hashpower. Unless new, more energy-efficient mining hardware is introduced, total consumption will rise in a linear fashion with hashpower.⁶⁴ Skyrocketing market prices in the second quarter of 2017 led to an exponential increase in hashpower, which in return triggered a substantial rise in the amount of energy consumed by mining facilities. Data suggest that hashpower growth is lagging behind market price growth: hashers often cannot immediately increase production when running at full capacity.

Total energy consumption increased more than fivefold between mid-2017 and mid-November 2018

Interestingly, total hashpower – and as a result energy consumption – has continued its steep growth despite the crash of the cryptoasset market that prompted prices to plummet. However, Bitcoin's

⁶¹ CIA World Factbook. Data available at: <https://www.cia.gov/library/publications/resources/the-world-factbook/fields/253rank.html> [Accessed: 25 November 2018].

⁶² IEA Energy Atlas. Data available at: <http://energyatlas.iea.org/#!/tellmap/-1118783123> [Accessed: 25 November 2018].

⁶³ Burger, B. (2018) Power generation in Germany: Assessment of 2017. *Fraunhofer Institute for Solar Energy Systems ISE*. Available at: https://www.ise.fraunhofer.de/content/dam/ise/en/documents/publications/studies/Stromerzeugung_2017_e.pdf, p.8 [Accessed: 25 November 2018].

⁶⁴ New-generation hardware with vastly improved energy efficiency is introduced periodically into the market, which can temporarily lead to a decrease in the total amounts of electricity consumed. However, the increase in margins will incentivise other hashers to expand operations, resulting in a higher hashrate and ultimately PoW difficulty. Over time, the energy efficiency effect is cancelled out by the increase in hashrate, and eventually total energy consumption levels rise again.

hashrate has since come down from 58 Exahashes per second (Ehs) in early November 2018 to 34 Ehs at the time of writing in late November 2018. This decline has resulted in a reduced energy consumption, demonstrating that cryptoasset mining is a dynamic process that is constantly self-adjusting.



Misconceptions About Energy Cost Per Transaction

Many energy consumption estimates include comparisons with traditional payment systems based on transaction throughput. The resulting *energy cost per transaction* is not a meaningful metric in the context of PoW blockchains for the following reasons:

- **Throughput unrelated to energy consumed:** the level of energy required for the networks to function is independent from the number of processed transactions.
- **Hidden semantics:** a single blockchain transaction can include thousands of payments, settle layer-2 network transactions (e.g. open and close channels in the Lightning network), and represent potentially billions of timestamped data points.
- **Different value proposition:** unlike traditional payment systems, PoW blockchains are designed to function as censorship-resistant value transfer systems. This value proposition requires engaging different trade-offs that result in substantial operational costs.

How Wasteful Is Cryptoasset Mining?

Some studies have attempted to estimate the environmental impact of cryptoasset mining on our planet. Krause and Tolaymat (2018) estimate that Bitcoin, Ethereum, Litecoin and Monero have been responsible for 3-15 million tonnes of CO₂ emissions since January 2016,⁶⁵ whereas Mora et al. (2018) project that Bitcoin alone could produce sufficient CO₂ emissions to push global warming above 2°C within less than three decades.⁶⁶

These analyses neglect the mining energy mix – the nature of the energy sources used to operate the hashing facilities. For instance, the energy footprint of one MW of energy generated by a coal-fired power station is not equivalent to the footprint of one MW of energy generated by a hydroelectric power station – particularly if the station produces overcapacities that are unmet by traditional demand.

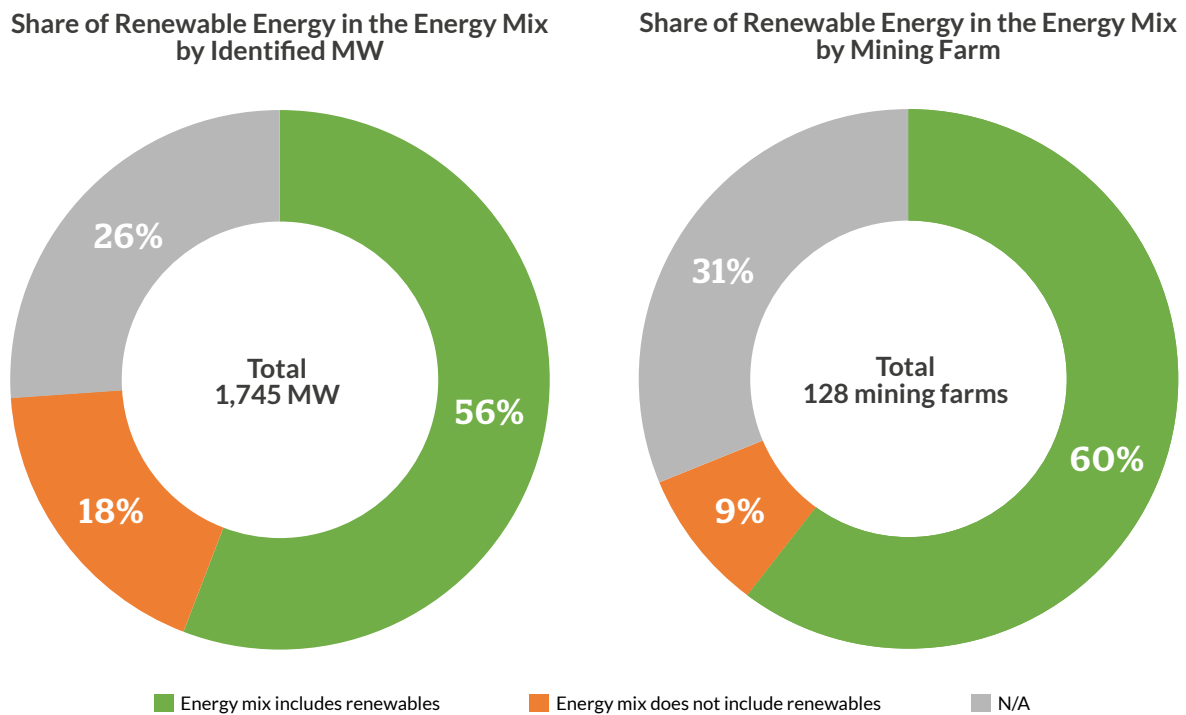
The environmental impact of cryptoasset mining is dependent on the energy mix used

Using the mining facility dataset previously introduced, it is possible to conduct a simple analysis of the average energy mix used by identified hashers. Contrary to popular beliefs, cryptoasset mining does not exclusively rely on fossil fuels: in fact, more than half of hashing facilities run on an energy mix that contains a share of renewables (Figure 48).

⁶⁵ Krause, M. J., and Tolaymat, T (2018) “Quantification of energy and carbon costs for mining cryptocurrencies” *Nature Sustainability*. Available at: <https://www.nature.com/articles/s41893-018-0152-7.pdf>. [Accessed: 30 November 2018].

⁶⁶ Mora, C., Rollins, R.L., Taladay, K., Kantar, M.B., Chock, M.K., Shimada, M., and Franklin, E.C. (2018) “Bitcoin emissions alone could push global warming above 2 degree” *Nature Climate Change*. Available at: <https://www.nature.com/articles/s41558-018-0321-8.pdf>. [Accessed: 30 November 2018].

Figure 48: Identified mining facilities often run on an energy mix that contains a share of renewables



Note: data is based on a dataset of 128 hashing facilities around the globe. Megawatt figures are available for 93 facilities.

Less than a quarter of identified miners do not use any forms of renewable energy sources at all, although the energy mix of one quarter of facilities could not be identified.⁶⁷ Certain regions such as Xinjiang Province in China rely almost entirely on coal. Nevertheless, weighing the farms by identified megawatts results in a similar picture and shows that cryptoasset mining is much less dependent on fossil fuels than anticipated.

Identified facilities draw on average 28% of their energy requirements from renewables

However, the share of renewables varies considerably from one facility to another: while some only use a marginal proportion, others run almost exclusively on renewables. On average, roughly 28% of the total energy supply for both small and large facilities is generated through renewable sources. Among renewables, hydroelectric power is the most frequently used energy source. Nearly half of the identified megawatt capacity featured in the cryptoasset mining map is generated through hydropower. It is worth noting that the mining map identifies 30% of the lower-bound total energy consumption estimate.⁶⁸

An interesting pattern emerges when comparing the energy mix with the location of the respective mining facilities. Regions with substantial green power sources seem to become attractive targets for miners, since these locations tend to overlap with places where there is an abundance of low-cost hydroelectric power that is unused and stranded. Energy in these locations is often cheap because demand cannot compensate the oversupply.

⁶⁷ It should be noted that mining facilities running on renewables may be more incentivised to publicise and advertise their energy mix, whereas facilities running exclusively on fossil fuels have less incentive in sharing information.

⁶⁸ The location of many mining facilities remains unknown; the 1.7 GW figure should thus be considered as a lower-bound estimate. For instance, mining activity in China is expected to be much higher than reported.

Hydroelectric power is the most used renewable energy source among identified facilities

The mining map confirms the pattern and shows that mining activities tend to increasingly cluster and congregate in locations with excess capacities in renewables (in particular hydroelectric power), such as for instance Western and Southwestern China, the North-East and North-West of the USA, as well as South-Eastern Canada and Iceland. While the claims of some proponents suggesting that cryptoasset mining will drive the “green revolution” may be a bit far-fetched, it is fair to say that regions with abundant renewable energy sources progressively attract miners chasing low-cost electricity.

Some renewable energy sources require the use of fossil fuels in their production, whereas others can be very expensive to produce. Moreover, renewables such as hydro (seasonal variances, dry periods), wind (weather-dependent), and solar (available only for a limited number of hours per day) are intermittent: supply is subject to seasonal changes and conditions, and often need to be supplemented by alternative, non-renewable energy sources during certain periods.

However, as such renewable energy sources fluctuate in their production, they can also overproduce relative to local demand. Cryptoasset mining may soak up local overcapacities and prevent the waste of otherwise unused renewable energy – power that cannot be easily stored and transmitted over large distances. However, if such overcapacities are less than the demand of mining operations, this may create an increase in local energy prices and hurt local businesses.

It is important to consider the energy mix used in the hashing process as well as potential alternative uses (or the lack thereof) when assessing the impact of cryptoasset mining on global carbon emissions. The preceding analysis concludes that concerns over Bitcoin – and PoW cryptoassets in general – directly and significantly contributing to climate change are largely overestimated at the time of writing.

What Do Miners Think?

Miners appear to be relatively indifferent with regards to their energy mix and whether it contains renewables. Instead, they prioritise low-cost electricity and a steady, reliable energy supply. As previously seen, it turns out that in some cases, their quest for cheap and ample electricity drives them to locations where excess capacities from renewables have significantly driven electricity prices down. When asked about their views on the environmental impact of PoW mining, surveyed miners provided similar responses to the 2017 survey: while most acknowledge that mining has an environmental impact on the planet to some degree, they urge commentators and critics to put energy consumption into perspective.

While acknowledging the environmental impact of PoW mining, most miners think it needs to be put into perspective

Many comment that other industries, such as physical commodities mining, use substantial amounts of energy as well and are not necessarily known for having a green footprint. Some miners also question the utility of the existing financial system and thus the electricity required to make this system function. Furthermore, both small and large miners strongly believe that the negative environmental externality might be alleviated by switching to more environmentally-friendly power sources. The previous analysis seems to confirm this trend to some extent.

A change in the PoW algorithm or a move from resource-intensive PoW mining to less energy-intensive PoS mining to alleviate the environmental impact do not seem to be acceptable options to most miners. This is not surprising as miners have made considerable investments into specialised equipment and facilities that they need to recover. It will be interesting to see how the planned move by some cryptoassets from PoW to PoS will affect miners, and whether they will grow into a new role as “stakers”.

7.4 Pool Operators

Pool Operations

A mining pool is a structure that “pools” together computational resources provided by connected hashers (*pool contributors*) in order to increase the likelihood and frequency of finding a new block, which results in smoother pay-outs. A pool operator creates a candidate block and sends the template to contributors, who will then perform hashing until a new block is found. Contributors send back pool shares to the pool operator who will distribute mining rewards in proportion to the amount of work performed.

The requirements for running pools are generally low: operators preferably need to run a fully-validating node of the cryptoasset system they are mining, maintain a simple server, and have a fast and stable Internet connection. Pools can range from single-operator projects run by hobbyists to sophisticated service providers with dedicated technical and customer support.

Pools generally do not restrict membership to users from specific jurisdictions

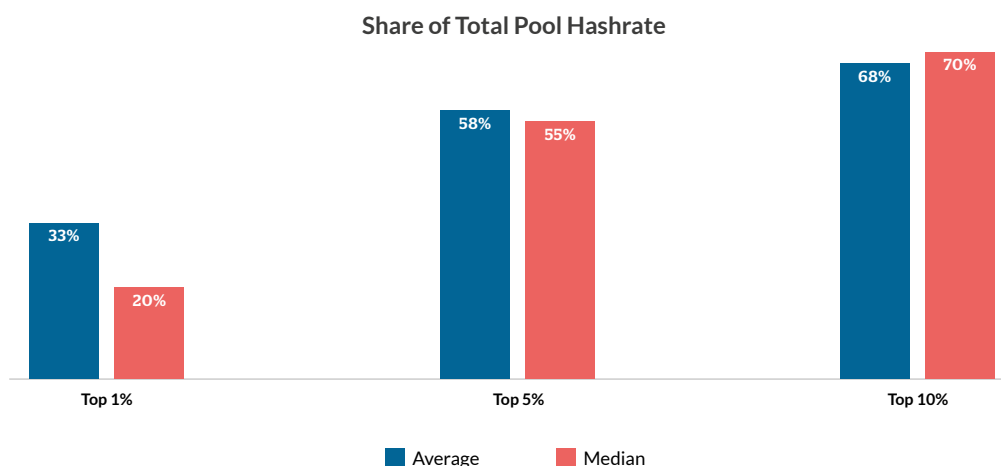
Pools appear to have no restrictions with regards to accepting contributors: only one out of eight surveyed pools mentioned that they are a private pool for investors and do not accept investors from specific regions. However, the majority of pools do implement policies to detect botnet activity and prevent distributed denial-of-service (DDoS) attacks.

On average, more than half of registered pool members actively contribute at least once a week

The number of contributors varies widely from one pool to another, as does the share of active members. Most pools consider hashers to be active when they contribute hashpower at least once a week. According to survey data, the share of active members averages 51%, but can range from a mere 2% up to 100%.

Data suggests that hashpower contribution follows a power law distribution: on average, one third of the pool’s total hashrate is provided by the top-1% of contributors, whereas 10% of active pool members contribute 68% (Figure 49). Nevertheless, figures are widely divergent: some pools indicate that up to 70% of their total hashrate is supplied by the top-1% of their members, whereas others are much more distributed in that only 30% of the total hashrate is provided by 10% of the pool members.

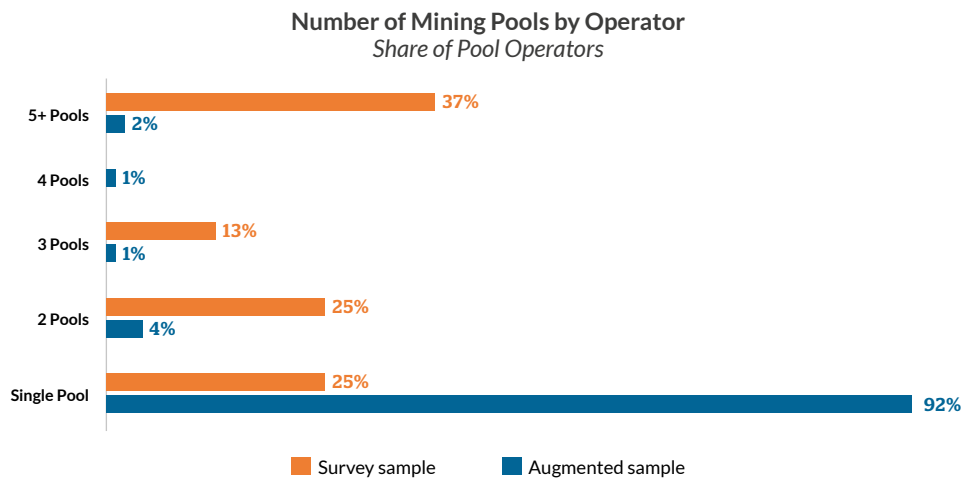
Figure 49: A small share of pool members contribute the majority of total pool hashrate



Pool Concentration

A repository of 147 identified mining pools across the cryptoasset ecosystem was built using a combination of survey data and public sources. Data shows that the vast majority (92%) of identified operators manage only a single pool, which seems to challenge the common view that mining pools are too concentrated (**Figure 50**). Interestingly, however, pool operators who responded to the survey (mostly large miners) are much more likely to operate multiple pools: in fact, more than one third indicates to run five or more pools.

Figure 50: While operators generally tend to manage a single pool, three-quarters of survey participants run two or more pools



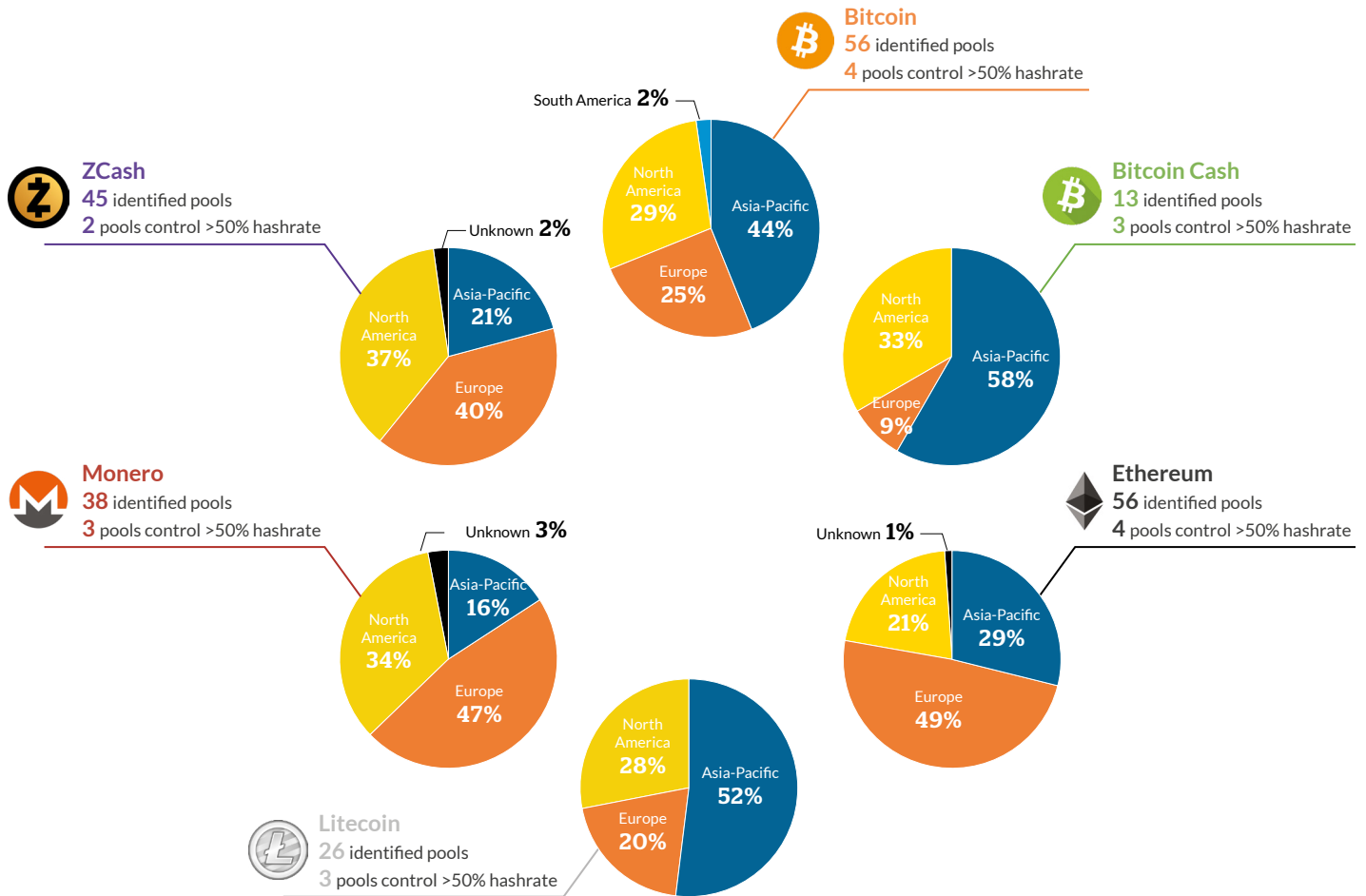
Note: the survey sample is based on data from survey participants. The augmented sample is based on a list of 147 identified mining pools across the cryptoasset ecosystem.

Data suggests that there is no clear pattern with regards to the pool decision-making process, but that pool policy is relatively diverse. Changes to pool policy (e.g. decision to mine a new coin) are equally likely to be made unilaterally by a single individual (38% of surveyed pools) or a group of operators (38%). The remaining 26% of pools take a more user-focused approach: users can participate in a vote-by-CPU (or equivalent) agreement. Other mining pools indicate using a combination of all these factors to instigate modifications of the pool policy.

More than a third of surveyed pools are fully controlled by a single person

The geographic distribution of mining pools varies significantly from one cryptoasset to another. However, they share in common that Asia-Pacific, Europe, and North America are generally dominating, albeit in different constellations (**Figure 51**). As of mid-November 2018, Bitcoin pools seem to be relatively equally distributed between the three aforementioned regions, whereas the Bitcoin Cash pool landscape seems to be dominated by pools located in Asia-Pacific. European pools appear to be dominant in Ethereum and Monero mining.

Figure 51: The mining pool landscape can vary a lot from one cryptoasset to another



Note: in some cases, insufficient information requires the geographic location of operators to be determined by server location. Data as of mid-November 2018.

It is worth noting that determining pool location can be tricky: some operators remain anonymous, whereas others have servers distributed across the world. Renting servers in different countries and regions is relatively simple and means that pool operators can quickly move operations between different locations.

Ethereum has the highest number of identified pools (87), followed by Bitcoin (57) and Zcash (45). However, the total number of pools is not a relevant metric in itself: instead, the relative share of hashpower controlled by each pool needs to be taken into account.⁶⁹ As of mid-November 2018, only four pools combined control more than 50% of Bitcoin's total hashrate. The picture looks even more concentrated for other cryptoassets: it would only take three pools to collude in order to perform a 51%-attack on Bitcoin Cash, Ethereum, Litecoin and the Monero network; whereas two ZCash pools alone control more than half of the network's hashrate.

A minority of pools control the majority of hashrate for the major cryptoassets

⁶⁹ Colluding miners that collectively control more than 50% of a cryptoasset network's hashrate will on average find more blocks than their honest competitors. This enables them to rewrite transaction history and perform double-spends.

While at first sight it appears that the mining pool landscape is significantly concentrated, a second look reveals that pool operators have less influence than anticipated. Hashers generally want to ensure that the pool they contribute to is engaging in a behaviour that is in agreement with their philosophy towards the chosen cryptoasset. In the event of disagreement or unstable reward allocation, miners are free to switch pools. Past events have shown that this also applies when a particular pool becomes too dominant: in 2013, Bitcoin mining pool GHash.io reached more than 50% of the total hashrate for a short period, which prompted hashers to proactively point their hashpower to another pool in order to avoid potential harmful concentration.

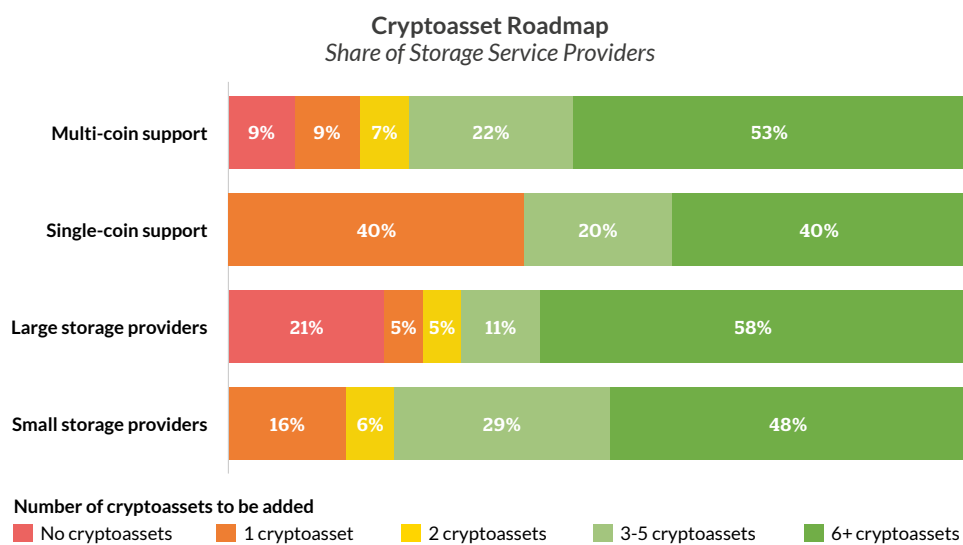
Low switching costs act as a check and balance system on pool operator behaviour

Assuming low switching costs, the ability of hashers to quickly move from one pool to another represents an implicit threat that acts as a check and balance system on mining pool behaviour. This dynamic and self-regulating process has worked relatively well so far, with no major blockchain reorganisation attacks observed for the dominant PoW cryptoassets.

FUTURE OUTLOOK

Sentiment questions from survey data suggest that the trend towards multi-coin support is likely to continue: all small storage service providers envisage to support more cryptoassets when asked about their cryptoasset roadmap. Only less than a quarter of large storage service providers indicated not planning to support more cryptoassets (Figure 52).

Figure 52: All single-coin wallets plan to support more cryptoassets; small wallets more likely to add more cryptoassets than large wallets




Regardless of the scale of their activities, the majority of storage service providers who plan to support more cryptoasset have three or more cryptoassets on their roadmap. This trend has accelerated: while only half of storage service providers surveyed in 2017 mentioned plans to support more cryptoassets, 91% of storage providers have more cryptoassets on their roadmap in 2018. Similarly, it is likely that the trend towards multi-segment services is going to continue.

Non-cryptocurrency cryptoassets (“cryptotokens”) became more popular in the ecosystem, primarily driven by the wide adoption of the ERC-20 standard on the Ethereum network. This led to a boom in token-based fundraising and a flurry of Initial Coin Offering (ICO) activities globally. The ICO market will be examined in detail in a future report. The increase in interest – and subsequent usage of cryptoassets – brought into the foreground limitations of base layer scaling and led to the launch of so-called “layer-2 solutions”, such as the eagerly-awaited Lightning Network on Bitcoin.⁷⁰

Service providers were also asked about their views on new developments in the cryptoasset ecosystem and how these are expected to impact their business models and operations (Table 5). Within a remarkably large ranking range, off-chain “layer-2” payment solutions are perceived to have the greatest impact within the coming 12 months. Payment-only companies in particular support this view.

⁷⁰ During the height of the boom, the Bitcoin blockchain experienced significant delays in processing transactions, with average fees rising to levels above \$50. Similarly, the Ethereum blockchain was clogged for a few days because of one single gaming application that suddenly became popular (CryptoKitties). Layer-2 solutions refer to a variety of techniques that aim to materially increase transaction speed and throughput as well as substantially decrease transaction costs by moving payments off-chain.

Table 5: Innovations in off-chain payment networks (“layer-2”) thought to have the largest impact on service providers’ business model and operations

Respondents scored these categories on a 1-5 scale:
 1: Not important at all 2: Not important 3: Neutral 4: Somewhat important 5: Very important
 Lowest average score  Highest average score

Impact	Payment-only	Exchange-only	Storage-only	Multi-segment
Stablecoins	3.22	2.90	3.73	3.34
CBDC	3.00	2.76	3.18	2.72
Non-fungible tokens	2.40	2.84	2.82	2.69
Security tokens	2.50	3.33	3.36	3.40
Layer 2	4.30	3.65	4.00	3.98
On-chain scaling	3.60	3.11	3.09	3.70
Other	1.00	1.00	3.00	3.40

In contrast, on-chain scaling is perceived to have a lower impact, principally for payment-only and multi-segment companies. It is expected that in vogue technologies like stablecoins will significantly impact operations of storage-only and multi-segment firms. Central bank-issued digital currency (CBDC), however, is not seen as having a large impact in the coming year.

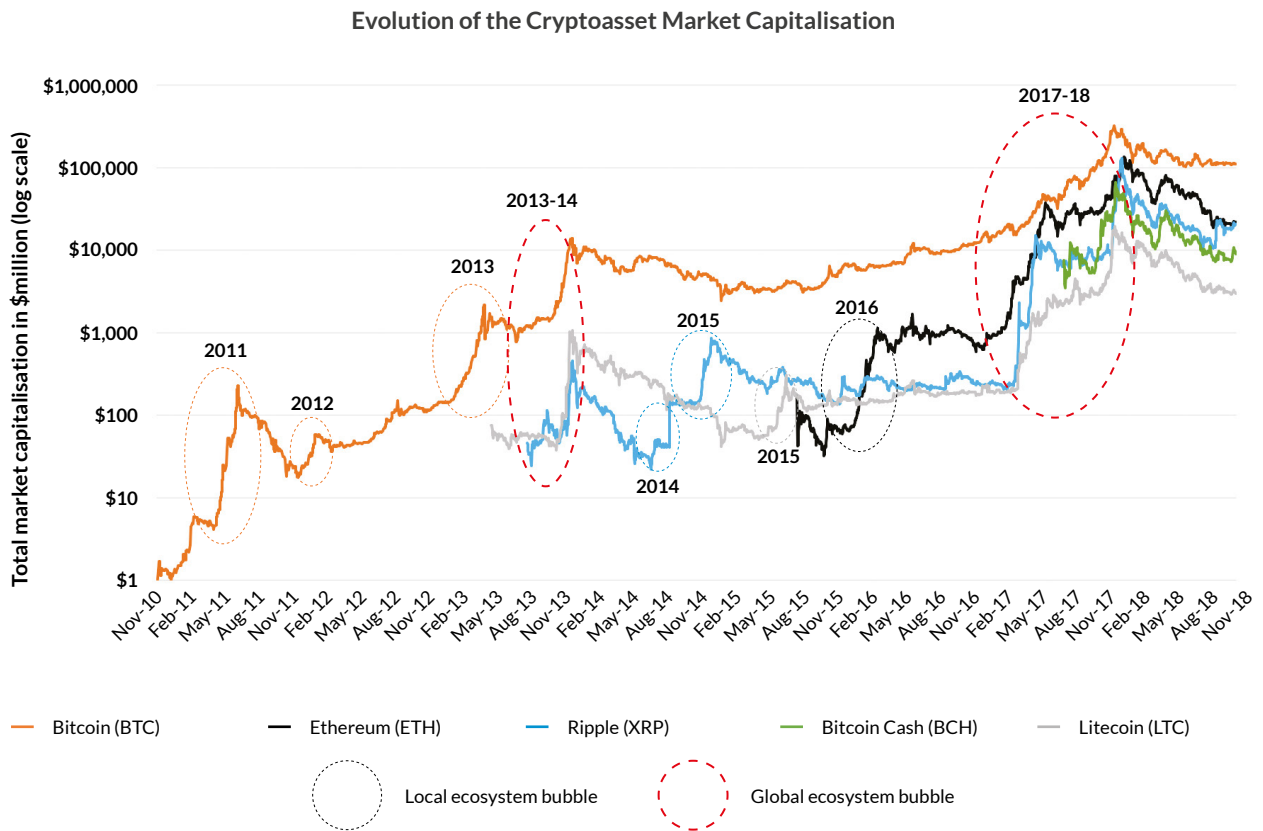
Independent of industry segment, non-fungible tokens (tokens that are cryptographically-unique, for instance implemented by standards such as Ethereum’s ERC-721) currently rank as the least impactful innovation for future evolution. Finally, exchange-only, storage-only, and multi-segment firms expect security tokens – tokens representing a traditional security agreement – to play a more significant role in the future.

Yet, all these future plans were made during or shortly after the 2017 cryptoasset boom and may represent a future that is now beyond the reach of the cryptoasset industry. The following analysis shows that this pattern of rapid-expansion and collapse has characterised the cryptoasset ecosystem since Bitcoin emerged in 2009.

We define a bubble as the market capitalisation of a cryptoasset appreciating by a multiple of 10 or more within a period of 6 months or less, followed by a substantial decline.⁷¹ Figure 53 shows the evolution of the market capitalisation of five leading cryptoassets (bitcoin, ether, ripple, bitcoin cash, and litecoin) and illustrate how a series of speculative bubbles can be observed for each of the selected cryptoassets.

⁷¹ Using price instead of market capitalisation will result in different dates on the bubbles, even when using the same definition. The reason for this discrepancy is rooted in the different supply schedules implemented by each cryptoasset.

Figure 53: Cryptoasset markets have seen a succession of local and global ecosystem bubbles since their inception



Note: data sourced from CoinMarketCap and Coin Dance.

Cryptoasset market bubbles can be categorised into local and global ecosystem bubbles. *Local ecosystem bubbles* only affect a particular cryptoasset and its ecosystem but are largely isolated from the overall development of the global cryptoasset market. In contrast, *global ecosystem bubbles* refer to market frenzies that affect the majority of cryptoassets and the entire ecosystem as a whole.

Before 2013, the cryptoasset ecosystem was dominated by Bitcoin and therefore market bubbles were mostly limited to local Bitcoin bubbles. An example is the “Great Bubble of 2011” that saw the BTC price peak at nearly \$32 in June 2011 before declining again in value by more than 90% over a period of four months.

Local ecosystem bubbles occur on a regular basis: XRP’s price rapidly increased and collapsed in both 2014 and 2015, whereas ETH saw its market capitalisation rise sharply in early 2016 after a successful launch several months before.

Local ecosystem bubbles are much more common than global ecosystem bubbles

The first global ecosystem bubble built up in late 2013 and led to a more than ten-fold increase in the aggregate cryptoasset market capitalisation following the announcement that China would allow cryptoasset trading and the time of Mt. Gox trading bots. It began deflating in early 2014 when China rolled back their announcement and Mt. Gox was hacked.

All previous global bubbles were dwarfed by the market frenzy that began in April 2017. Fueled by intense media coverage, the tempting promise of ‘get-rich-quick’ ICO schemes, and an oversupply of new coins and tokens, many first-time retail and institutional cryptoasset investors rushed in. Aggregate cryptoasset market capitalisation exploded more than 25-fold to peak at nearly \$800 billion, before rapidly declining throughout the year 2018.

The collapse in prices, and subsequent media coverage of the losses borne by speculative investors in 2018, created a media narrative in which Bitcoin, cryptoassets, and ICOs were not only declared bubbles but also declared dead.

Statements proclaiming the death of the cryptoasset industry have been made after every global ecosystem bubble. While it is true that the 2017 bubble was the largest in Bitcoin’s history, the market capitalisation of both Bitcoin and the cryptoasset ecosystem still exceeds its January 2017 levels -- prior to the start of the bubble. This report has shown that the speculation of the death of the market and ecosystem has been greatly exaggerated, and so it seems likely that the future expansion plans of industry participants will, at most, be delayed.

APPENDIX: SENTIMENT QUESTIONS

The survey asked participants several sentiment questions. In general, industry participants are more concerned about operating risk factors in 2018. It is further noted that small and large firms have largely begun to converge in their perceptions and sentiments.

Table 6: Exchanges rank major operational risks

Respondents scored these categories on a 1-5 scale:

1: Completely disagree 2: Disagree 3: Neutral 4: Somewhat agree 5: Completely agree

Lowest average score  Highest average score

		IT Security	Fraud	AML/KYC Enforcement	Regulatory Burden	Risks Competition	Negative Publicity	Bank Relationship	Entering Bank Relationship	Lack of Talent
Large	2018	4.20	3.83	3.40	3.84	3.29	3.52	3.54	3.63	3.83
	2017	3.17	2.08	2.75	3.50	2.58	2.75	2.67	2.67	2.33
Small	2018	3.81	3.48	3.17	3.78	3.21	3.30	3.48	3.69	3.48
	2017	3.93	3.50	2.64	2.89	3.00	2.93	3.79	3.79	2.52

Table 7: Miners rank major concerns over operational risks


Respondents scored these categories on a 1-5 scale:

1: Not concerned at all 2: Not concerned 3: Neutral 4: Somewhat concerned 5: Very concerned

Lowest average score  Highest average score


Operational Risks	Small Miners (incl. Individuals)		Large Miners	
	2017	2018	2017	2018
Sudden increase in energy prices	N/A	3.09	N/A	3.54
Intensive competition among miners of the same cryptoasset	3.17	3.33	3.30	3.23
Cyber attacks (e.g. DDoS)	2.77	3.07	3.00	3.31
Lack of immediate availability of state-of-the-art hardware	2.94	3.35	2.40	2.46
Declining popularity of the cryptoasset you mine	N/A	2.95	N/A	3.00
Unexpected change to protocol	2.52	3.00	1.64	3.38
Increased taxation of mining profits	N/A	3.16	N/A	2.85
Regulations creating barriers to mining	N/A	3.31	N/A	2.92
Government seizure or shutdown of your mining-supporting facilities	N/A	3.55	N/A	2.38

Table 8: Miners rank major decision factors for choosing a location for establishing new hashing facilities

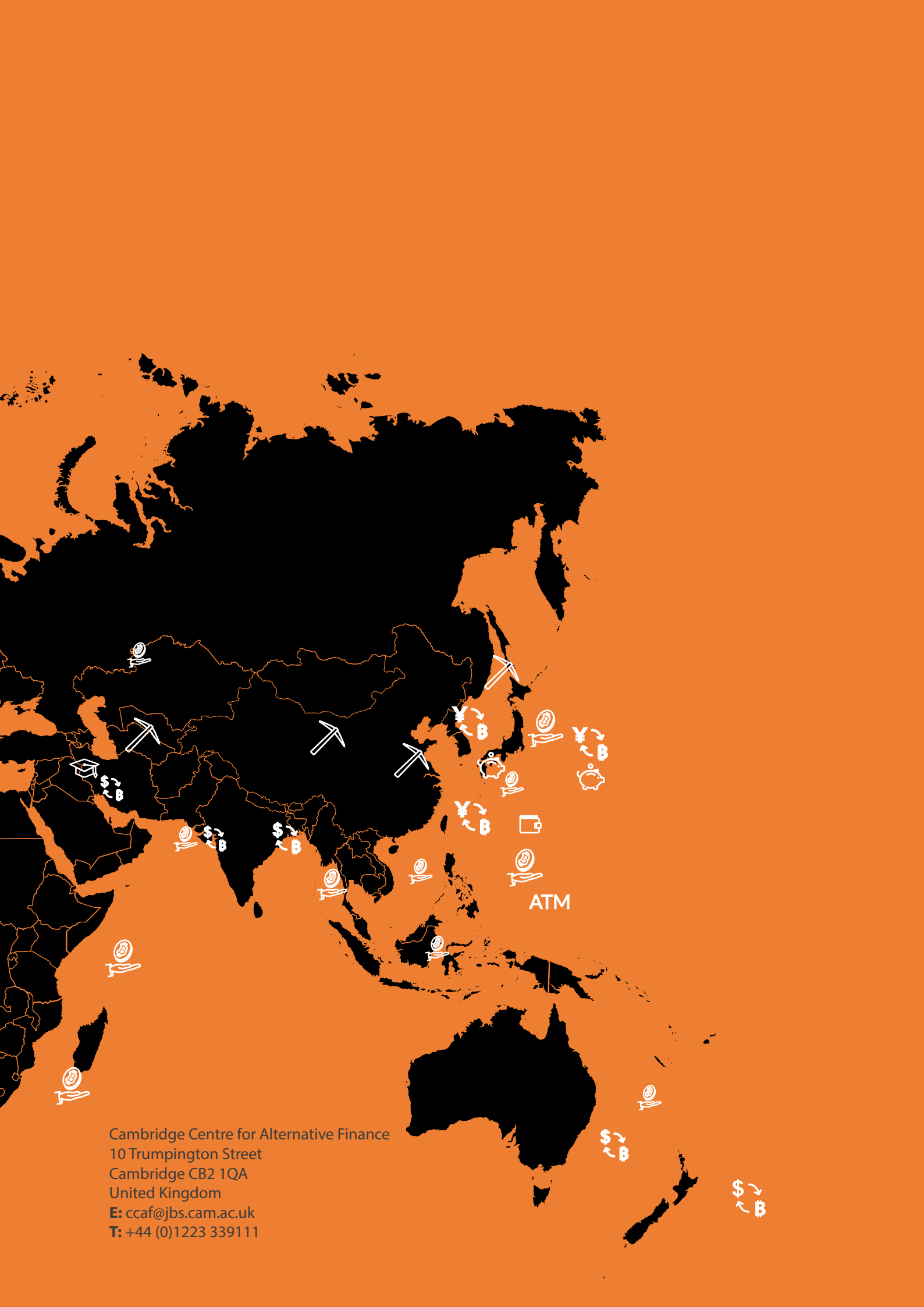
Respondents scored these categories on a 1-5 scale:
 1: Not important at all 2: Not important 3: Neutral 4: Somewhat important 5: Very important
 Lowest average score  Highest average score

Assessment Factors for Setting up a New Mining Facility	Small Miners (incl. Individuals)	Large Miners
Stable political environment	4.37	4.63
Friendly regulatory environment	4.37	4.75
Presence of skilled labour	3.32	3.75
Cold climate	3.11	4.25
Good internet connectivity	4.32	4.38
Easy access to substantial electricity supply	4.37	4.88
Low electricity cost	4.47	4.88
Cheap land	3.58	3.75
Special incentives for mining-related activities	3.95	4.13
Low crime rate	3.63	3.38

Table 9: Miners rank major concerns over additional risks

Respondents scored these categories on a 1-5 scale:
 1: Not concerned at all 2: Not concerned 3: Neutral 4: Somewhat concerned 5: Very concerned
 Lowest average score  Highest average score

Concerns	Small Miners (incl. Individuals)		Large Miners	
	2017	2018	2017	2018
Centralisation of hashpower in a particular geographic area (location)	3.70	3.89	3.11	3.69
Centralisation of hashpower in the hands of a few (control)	3.89	4.41	3.30	4.00
Centralisation of mining equipment production in a particular geographic area	3.35	3.70	2.10	3.50
Risk of state-sponsored attack on a cryptoasset system	N/A	3.37	N/A	2.92
Unfavourable global regulation related to cryptoassets	N/A	3.25	N/A	3.15
Unfavourable global regulation related to cryptoasset mining	N/A	3.33	N/A	3.00
Criminal use of cryptoassets	N/A	3.20	N/A	2.77
Popularity of pre-mined/'mining-less' cryptoassets	N/A	3.07	N/A	2.77
Too many cryptoassets in the market	N/A	3.11	N/A	2.08



Cambridge Centre for Alternative Finance
10 Trumpington Street
Cambridge CB2 1QA
United Kingdom
E: ccaf@jbs.cam.ac.uk
T: +44 (0)1223 339111