# GLOBAL CRYPTOCURRENCY BENCHMARKING STUDY

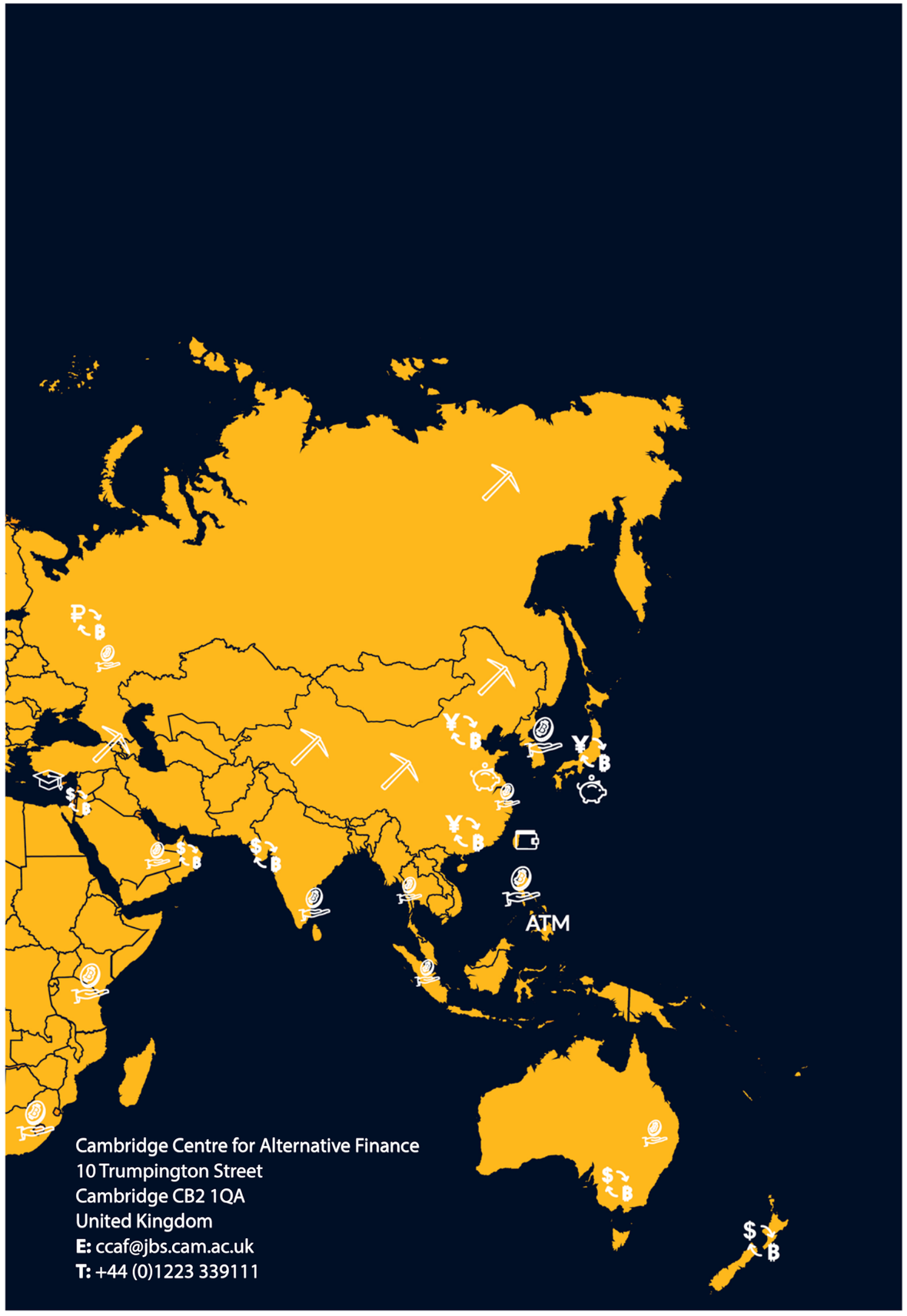
Dr Garrick Hileman & Michel Rauchs
2017


Cambridge
**Centre**
**for Alternative**
**Finance**

UNIVERSITY OF CAMBRIDGE
Judge Business School

With the support of:

VISA




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

# CONTENTS

# FOREWORDS

Cambridge **Centre for Alternative Finance**

UNIVERSITY OF CAMBRIDGE
Judge Business School

The world of money and finance is transforming before our eyes. Digitised assets and innovative financial channels, instruments and systems are creating new paradigms for financial transaction and forging alternative conduits of capital. The Cambridge Centre for Alternative Finance, since its founding in 2015, has been at the forefront of documenting, analysing and indeed critically challenging that digital financial transformation.

This Global Cryptocurrency Benchmarking Study is our inaugural research focused on alternative payment systems and digital assets. Led by Dr Garrick Hileman, it is the first study of its kind to holistically examine the burgeoning global cryptocurrency industry and its key constituents, which include exchanges, wallets, payments and mining.

The findings are both striking and thought-provoking. First, the user adoption of various cryptocurrencies has really taken off, with billions in market cap and millions of wallets estimated to have been 'active' in 2016. Second, the cryptocurrency industry is both globalised and localised, with borderless exchange operations, as well as geographically clustered mining activities. Third, the industry is becoming more fluid, as the lines between exchanges and wallets are increasingly 'blurred' and a multitude of cryptocurrencies, not just bitcoin, are now supported by a growing ecosystem, fulfilling an array of functions. Fourth, issues of security and regulatory compliance are likely to remain prevalent for years to come.

I hope this study will provide value to academics, practitioners, policymakers and regulators alike. We thank Visa very much for its generous support of independent academic research in this important area.

**Bryan Zhang**
Co-founder and Executive Director (Interim)

VISA

Blockchain has received a significant amount of analyst and press attention over the last few years as this emerging technology holds significant potential. Use cases are many and varied: ranging from programmable cryptocurrencies to property deeds management to provenance tracking to voting records.

Cryptocurrencies were the first application of this technology, and in doing so introduced an entirely new set of businesses, jobs and vocabulary to the world of payments. Visa has been exploring the impact of these technologies to determine how this new ecosystem will continue to grow and evolve.

Amongst all the excitement and enthusiasm in the press there has also been some hyperbole, and any efforts to provide a realistic snapshot of the industry should be welcomed. Visa welcomes opportunity to sponsor research from a respected organisation, the Judge Business School at Cambridge University, which we trust, the reader will find objective, informative and insightful.

**Jonathan Vaux**
VP, Innovation & Strategic Partnerships




Electronic copy available at: http

Cambridge
**Centre**
**for Alternative**
**Finance**

UNIVERSITY OF CAMBRIDGE
Judge Business School

It is my great pleasure to present the first global cryptocurrency benchmarking study. The findings from our study are based on the collection of non-public data from nearly 150 companies and individuals, and this report offers new insights on an innovative and rapidly evolving sector of the economy.

Cryptocurrencies such as bitcoin have been seen by some as merely a passing fad or insignificant, but that view is increasingly at odds with the data we are observing. As of April 2017, the combined market value of all cryptocurrencies is $27 billion, which represents a level of value creation on the order of Silicon Valley success stories like AirBnB. The advent of cryptocurrency has also sparked many new business platforms with sizable valuations of their own, along with new forms of peer-to-peer economic activity.

Next year will mark the ten-year anniversary of the publication of Satoshi Nakamoto's paper describing how a new digital financial instrument could be created and operated securely with a blockchain. The growing usage and range of capabilities we document in this study indicate that cryptocurrencies are taking on an ever more important role in the lives of a growing number of people (and machines) around the world. As we show in this study, the number of people using cryptocurrency today has seen significant growth and rivals the population of small countries.

By our count, over 300 academic articles have been published on various aspects of bitcoin and other cryptocurrencies over the past several years. However, these works tend to take a narrow focus. To our knowledge this is the first global cryptocurrency study based on non-public 'off-chain' data. We designed the study to present an empirical picture of the current state of this still maturing industry, and to explore how cryptocurrencies are being used today. The findings from this study will be useful to industry, academics, policymakers, media, and anyone seeking to better understand the cryptocurrency landscape.

This study would not have been possible without the support and participation from nearly 150 cryptocurrency companies and individuals that contributed data, many of which have elected to have their logos displayed in this report. This study also greatly benefitted from suggestions and support we received from many individuals and firms we recognise in the Acknowledgements. We are grateful for the trust placed by study participants in the University of Cambridge research team.

We are looking forward to continuing and expanding our cryptocurrency and blockchain research program. In a few weeks, we will also be publishing the results of a separate study focused on the use of distributed ledger technology (DLT), which examines the use of DLT by more established industry players as well as at public sector institutions such as central banks.

Thank you for your interest in this study. We will be conducting these benchmarking studies on an annual basis, and I welcome your comments and feedback.

**Garrick Hileman**
g.hileman@jbs.cam.ac.uk

# RESEARCH TEAM

**DR GARRICK HILEMAN**

Dr Garrick Hileman is a Senior Research Associate at the Cambridge Centre for Alternative Finance and a Researcher at the Centre for Macroeconomics. He was recently ranked as one of the 100 most influential economists in the UK and Ireland and he is regularly asked to share his research and perspective with the FT, BBC, CNBC, WSJ, Sky News, and other media. Garrick has been invited to present his research on monetary and distributed systems innovation to government organisations, including central banks and war colleges, as well as private firms such as Visa, Black Rock, and UBS. Garrick has 20 years' private sector experience with both startups and established companies such as Visa, Lloyd's of London, Bank of America, The Home Depot, and Allianz. Garrick's technology experience includes co-founding a San Francisco-based new venture incubator, IT strategy consulting for multinationals, and founding MacroDigest, which employs a proprietary algorithm to cluster trending economic analysis and perspective.

**MICHEL RAUCHS**

Michel Rauchs is a Research Assistant at the Cambridge Centre for Alternative Finance. Cryptocurrencies and distributed ledger technologies have been the topic of his academic studies for the last two years, and his Master's thesis visualised the evolution of the Bitcoin business ecosystem from 2010-2015 using a unique longitudinal dataset of 514 companies and projects. He holds a Bachelor in Economics from HEC Lausanne and recently graduated from Grenoble Ecole de Management with a Master's degree in International Business.

# ACKNOWLEDGMENTS

We would like to thank the Asia Blockchain Foundation, 8btc.com, Coin Center, CoinDesk, The Coinspondent and the r/bitcoin forum on Reddit for helping to build awareness and supporting the study.

We would also like to specifically thank Jelena Strelnikova (Asia Blockchain Foundation), Neil Woodfine (Remitsy), Dave Hudson (PeerNova), Philip Martin and David Farmer (Coinbase), Peter Smith (Blockchain), Jez San, Jon Matonis (Globitex/ Bitcoin Foundation), Roger Ver (Bitcoin.com), Jill Carlson (Chain), Christopher Harborne, Sveinn Vallfels (Flux), Cathy Lige, Jonathan Levin and Michael Gronager (Chainalysis), George Giaglis (Athens University of Economics and Business), George Papageorgiou (University of Nicosia), Vitalii Demianets (Norbloc) and CoinATMRadar for their generous help and assistance throughout the research process.

Special thanks go also to Alexis Lui, Alex Wong and Hritu Patel (Judge Business School) for the design of this study.

Finally, we would like to express our gratitude to Kate Belger, Hungyi Chen, Raghavendra Rau, Nia Robinson, Robert Wardrop, Bryan Zhang and Tania Ziegler of the CCAF for their continued support and help in producing this report. Special thanks also go to Jack Kleeman.

We would like to thank the following cryptocurrency organisations for participating and contributing to this research study:[1]

# EXECUTIVE SUMMARY

This is the first study to systematically investigate key cryptocurrency industry sectors by collecting empirical, non-public data. The study gathered survey data from nearly 150 cryptocurrency companies and individuals, and it covers 38 countries from five world regions. The study details the key industry sectors that have emerged and the different entities that inhabit them.

### KEY HIGHLIGHTS OF THE STUDY

- The current number of unique active users of cryptocurrency wallets is estimated to be between 2.9 million and 5.8 million.
- The lines between the different cryptocurrency industry sectors are increasingly blurred: 31% of cryptocurrency companies surveyed are operating across two cryptocurrency industry sectors or more, giving rise to an increasing number of universal cryptocurrency companies.
- At least 1,876 people are working full-time in the cryptocurrency industry, and the actual total figure is likely well above two thousand when large mining organisations and other organisations that did not provide headcount figures are added.
- Average security headcount and costs for payment companies and exchanges as a percentage of total headcount/operating expenses are similar, but significantly higher for wallets.

### EXCHANGES

- The exchanges sector has the highest number of operating entities and employs more people than any other industry sector covered in this study; a significant geographical dispersion of exchanges is observed.
- 52% of small exchanges hold a formal government license compared to only 35% of large exchanges.
- On average, security headcount corresponds to 13% of total employees and 17% of budget is spent on security.

### WALLETS

- Between 5.8 million and 11.5 million wallets are estimated to be currently ‘active’.
- The lines between wallets and exchanges are increasingly blurred: 52% of wallets surveyed provide an integrated currency exchange feature, of which 80% offer a national-to-cryptocurrency exchange service. In contrast with exchanges, the majority of wallets do not control access to user keys.

### PAYMENTS

- While 79% of payment companies have existing relationships with banking institutions and payment networks, the difficulty of obtaining and maintaining these relationships is cited as this sector's biggest challenge.
- On average, national-to-cryptocurrency payments constitute two-thirds of total payment company transaction volume, whereas national-to-national currency transfers and cryptocurrency-to-cryptocurrency payments account for 27% and 6%, respectively.

### MINING

- 70% of large miners rate their influence on protocol development as high or very high, compared to 51% of small miners.
- The cryptocurrency mining map shows that publicly known mining facilities are geographically dispersed, but a significant concentration can be observed in certain Chinese provinces.

# METHODOLOGY AND STUDY STRUCTURE

### METHODOLOGY

The Cambridge Centre for Alternative Finance carried out four online surveys from September 2016 to January 2017 via secure web-based questionnaires. Each survey was directed at organizations and individuals operating in a specific sector of the cryptocurrency industry as defined by our taxonomy (specifically exchanges, wallets, payment service providers, and miners). All surveys were written and distributed in English, and the exchanges survey as well as the mining survey were translated and distributed in Chinese with the generous help of 8btc.com.

The research team collected data from cryptocurrency companies and organisations across 38 countries and five world regions. Over one hundred cryptocurrency companies and organisations as well as 30 individual miners participated in one or more of the four surveys. During the survey process, the research team communicated directly with individual organisations, explaining the study's objectives. For cases in which currently active major companies did not contribute to our study, the dataset was supplemented with additional research and web scraping using commonly applied methodologies.

## 144 cryptocurrency organisations and individual miners are included in the research study sample

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 sector, type of activity, organisation size, region and country. We estimate that our benchmarking study captured more than 75% of the four cryptocurrency industry sectors covered in this report.

### REPORT STRUCTURE

The remainder of this report is structured as follows:

- **Setting the Scene** provides a global overview of cryptocurrencies, introduces the industry and its key constituents, and discusses cryptocurrency usage and activity.
- **The Exchanges section** presents an overview of the cryptocurrency exchange sector and the different types of exchange activities, with a particular focus on security.
- **The Wallets section** explores the different types and formats of wallets, as well as widely offered features including currency exchange services.
- **The Payments section** features a taxonomy of the four major payment activity types, and compares national and cross-border payment channels and transaction sizes.
- **The Mining section** describes the mining value chain and features a map with publicly known mining facilities across the world; miners' views on policy issues and operational challenges are also presented.
- **Appendix A: Brief introduction to cryptocurrencies** highlights the general concept of cryptocurrencies and presents their key properties and value propositions.
- **Appendix B: The cryptocurrency industry** offers a more detailed introduction to the emergence of the cryptocurrency industry.
- **Appendix C: The geographical dispersion of cryptocurrency users** discusses the geographical dispersion of cryptocurrency users and activity.
- **References and Endnotes** provide information on where outside information was gathered and further explanation of how some figures were calculated (e.g., employee figures by sector).

# GLOSSARY

**GEOGRAPHY**

- **Asia-Pacific:** region that comprises East Asia, South Asia, South-East Asia and Oceania
- **Africa and Middle East:** region that comprises the African continent as well as the Middle East
- **Europe:** region that comprises Western Europe, Southern Europe and Eastern Europe including Russia
- **Latin America:** region that comprises South America and Central America including Mexico
- **North America:** region composed of Canada and the United States

**EXCHANGES**

- **Order-book exchange:** platform that uses a trading engine to match buy and sell orders from users
- **Brokerage service:** service that lets users conveniently acquire and/or sell cryptocurrencies at a given price
- **Trading platform:** platform that provides a single interface for connecting to several other exchanges and/or offers leveraged trading and cryptocurrency derivatives
- **Large exchange:** exchange with more than 20 full-time employees and/or a non-negligible market share
- **Custodial exchange/custodian:** exchange that takes custody of users' cryptocurrency funds

**WALLETS**

- **Incorporated wallet:** registered corporation that provides software and/or hardware wallets.
- **Custodial wallet/custodian:** wallet provider that takes custody of users' cryptocurrency holdings by controlling the private key(s).
- **Self-hosted wallet:** wallet that lets users control private key(s), meaning that the wallet service does not have access to users' cryptocurrency funds
- **Large wallet:** incorporated wallet that has more than 10 full-time employees
- **Wallets with integrated currency exchange:** wallets that provide currency exchange services within the wallet interface using one of three exchange models:
  - *Centralised exchange/brokerage service model:* wallet provider acts as central counterparty
  - *Integrated third-party exchange model:* wallet provider partners with a third-party exchange to provide exchange services
  - *P2P exchange/marketplace model:* wallet provider offers a built-in P2P exchange that lets users exchange currencies between themselves

**PAYMENTS**

- **National currency-focused:** services that use cryptocurrency primarily as a 'payment rail' for fast and cost-efficient payments, which are generally denominated in national currencies
    - *B2B payment services:* platforms that provide payments for businesses, often times across borders
    - *Money transfer services:* services that provide primarily international money transfers for individuals (e.g., traditional remittances, bill payment services)
- **Cryptocurrency-focused:** services that facilitate the use of cryptocurrencies; generally payments are denominated in cryptocurrency, but can also be exchanged to national currencies
    - *Merchant services:* services that process payments for cryptocurrency-accepting merchants, and provide additional merchant services (e.g., shopping cart integrations, point-of-sale terminals)
    - *General-purpose cryptocurrency platform:* platforms that perform a variety of cryptocurrency transfer services (e.g., instant payments to other users of the same platform using cryptocurrency and/or national currencies, payroll, bill payment services)

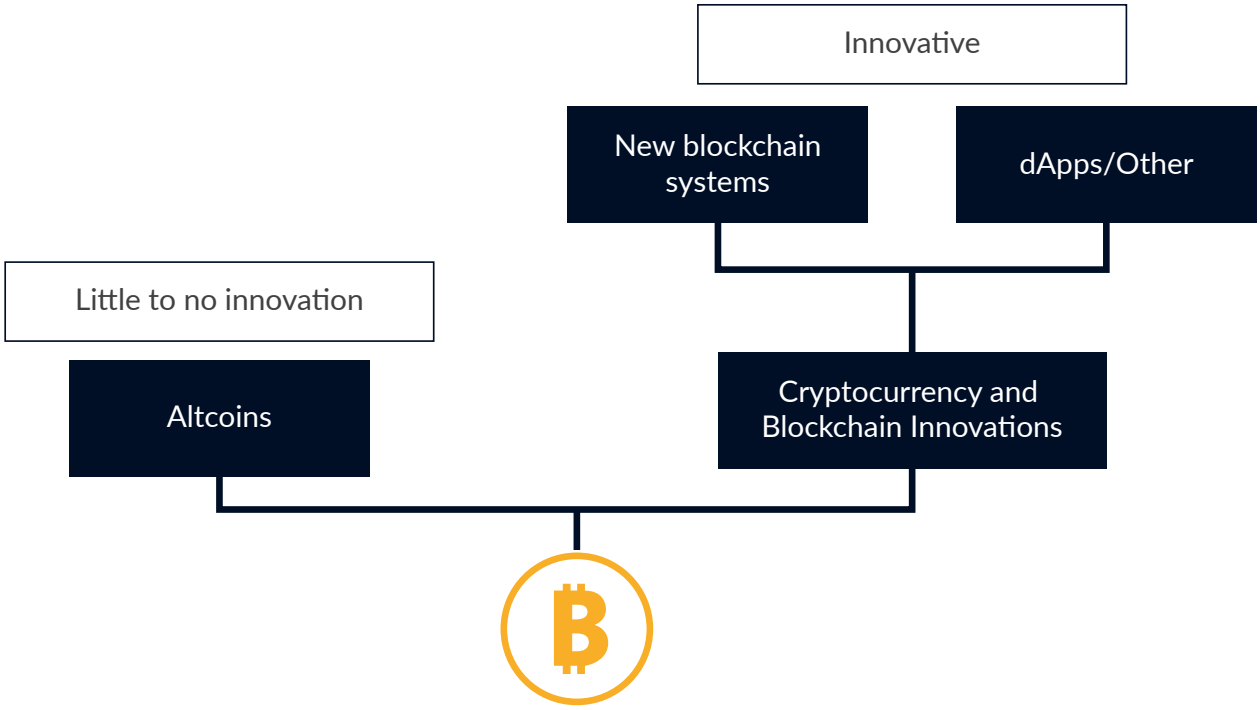
**MINING**

- **Mining value chain:** the cryptocurrency mining sector is composed of the following principal activities:
    - *Mining hardware manufacturing:* design and building of specialised mining equipment
    - *Self-mining:* miners running their own equipment to find valid blocks
    - *Cloud mining services:* services that rent out hashing power to customers
    - *Remote hosting services:* services that host and maintain customer-owned mining equipment
    - *Mining pool:* structure that combines computational resources from multiple miners to increase the frequency and likelihood of finding a valid block; rewards are shared among participants
- **Small miners:** registered companies active in the mining industry, but operating with limited scale; individual miners operating as sole proprietors
- **Large miners:** mining organisations that engage in medium-to-large scale mining operations and occupy a significant position in the industry

**TECHNICAL**

- **Blockchain:** record of all validated transactions grouped into blocks, each cryptographically linked to predecessor transactions down to the genesis block, thereby creating a 'chain of blocks'
- **Keys:** term used to describe a pair of cryptographic keys that consists of a private (secret) key and a corresponding public key: the private key can be compared to a password needed to 'unlock' cryptocurrency funds while the public key (if converted to an address) can be compared to a public email address or bank account number
- **Multi-signature:** mechanism to split control over an address among multiple private keys such that a specific threshold of keys are needed to unlock funds stored in that particular address

Figure 1: Bitcoin's genealogical tree




# CRYPTOCURRENCY OVERVIEW

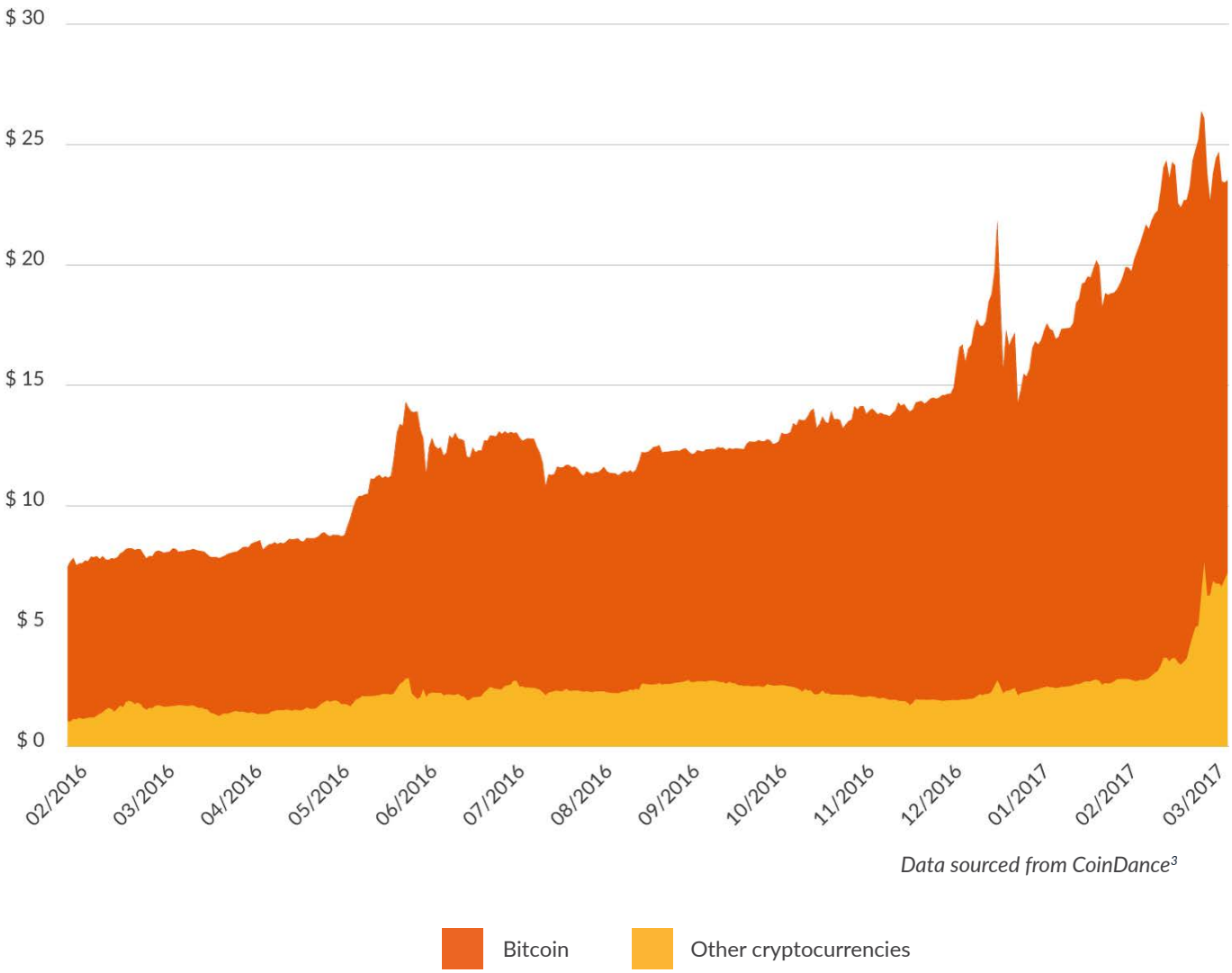
**BITCOIN, ALTCOINS, AND INNOVATION**

Bitcoin began operating in January 2009 and is the first decentralised cryptocurrency, with the second cryptocurrency, Namecoin, not emerging until more than two years later in April 2011. Today, there are hundreds of cryptocurrencies with market value that are being traded, and thousands of cryptocurrencies that have existed at some point.[1]

The common element of these different cryptocurrency systems is the public ledger ('blockchain') that is shared between network participants and the use of native tokens as a way to incentivise participants for running the network in the absence of a central authority. However, there are significant differences between some cryptocurrencies with regards to the level of innovation displayed (Figure 1).

The majority of cryptocurrencies are largely clones of bitcoin or other cryptocurrencies and simply feature different parameter values (e.g., different block time, currency supply, and issuance scheme). These cryptocurrencies show little to no innovation and can be referred to as 'altcoins'.[2]

Figure 2: The total cryptocurrency market capitalisation has increased more than 3x since early 2016, reaching nearly $25 billion in March 2017




*Data sourced from CoinDance*[3]

In contrast, a number of cryptocurrencies have emerged that, while borrowing some concepts from Bitcoin, provide novel and innovative features that offer substantive differences. These can include the introduction of new consensus mechanisms (e.g., proof-of-stake) as well as decentralised computing platforms with 'smart contract' capabilities that provide substantially different functionality and enable non-monetary use cases. It can be useful to distinguish between altcoins lacking any significant innovation and what we refer to as 'cryptocurrency and blockchain innovations', which can be grouped into two categories: *new (public) blockchain systems* that feature their own blockchain (e.g., Ethereum, Peercoin, Zcash), and *dApps/Other* that exist on additional layers built on top of existing blockchain systems (e.g., Counterparty, Augur).[4]

It should be noted that Figure 1 only captures cryptocurrencies built on public and permissionless blockchains. It does not include private or permissioned blockchain systems that restrict the number of network participants, and do not require a native asset for running the network.

The combined market capitalisation (i.e., market price multiplied by the number of existing currency units) of all cryptocurrencies has increased more than threefold since early 2016 and has reached $27 billion in April 2017 (Figure 2). A relatively low, but not insignificant share of value is allocated to duplication (i.e., 'altcoins'), while a growing share has been apportioned to innovative cryptocurrencies ('cryptocurrency and blockchain innovations').

As of April 2017, the following cryptocurrencies are the largest after bitcoin in terms of market capitalisation:

**ETHEREUM (ETH)**
Decentralised computing platform which features its own Turing-complete programming language. The blockchain records scripts or contracts that are run and executed by every participating node, and are activated through payments with the native cryptocurrency 'ether'. Officially launched in 2015, Ethereum has attracted significant interest from many developers and institutional actors.

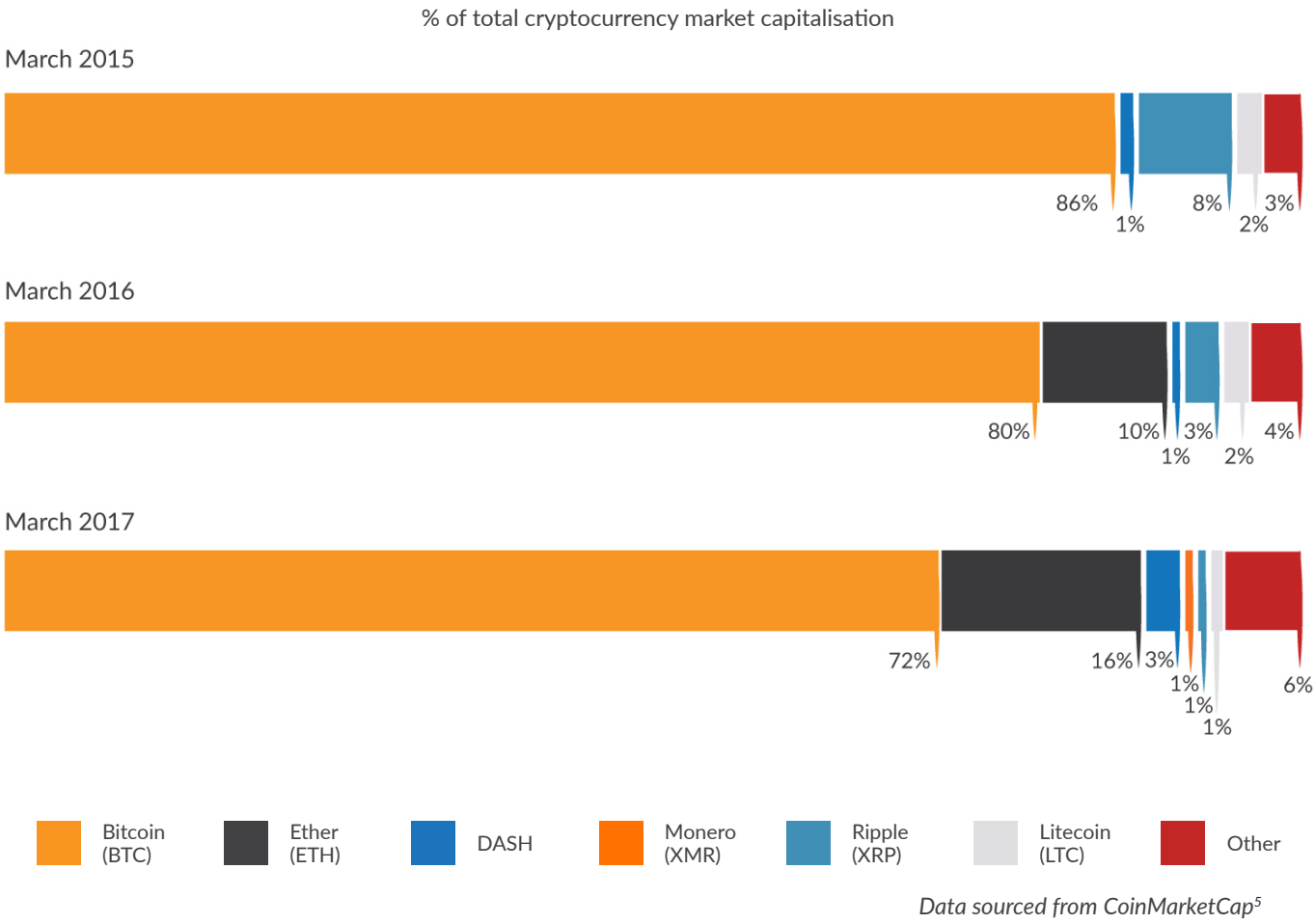
**DASH**
Privacy-focused cryptocurrency launched in early 2014 that has recently experienced a significant increase in market value since the beginning of 2017. In contrast to most other cryptocurrencies, block rewards are being equally shared between miners and 'masternodes', with 10% of revenues going to the 'treasury' to fund development, community projects and marketing.

**MONERO (XMR)**
Cryptocurrency system that aims to provide anonymous digital cash using ring signatures, confidential transactions and stealth addresses to obfuscate the origin, transaction amount and destination of transacted coins. Launched in 2014, it saw a substantial increase in market value in 2016.

**RIPPLE (XRP)**
Only cryptocurrency in this list that does not have a blockchain but instead uses a 'global consensus ledger'. The Ripple protocol is used by institutional actors such as large banks and money service businesses. A function of the native token XRP is to serve as a bridge currency between national currency pairs that are rarely traded, and to prevent spam attacks.

**LITECOIN (LTC)**
Litecoin was launched in 2011 and is considered to be the 'silver' to bitcoin's 'gold' due to its more plentiful total supply of 84 million LTC. It borrows the main concepts from bitcoin but has altered some key parameters (e.g., the mining algorithm is based on Scrypt instead of bitcoin's SHA-265).

Figure 3: Bitcoin (BTC) has ceded significant 'market cap share' to other cryptocurrencies, most notably ether (ETH)



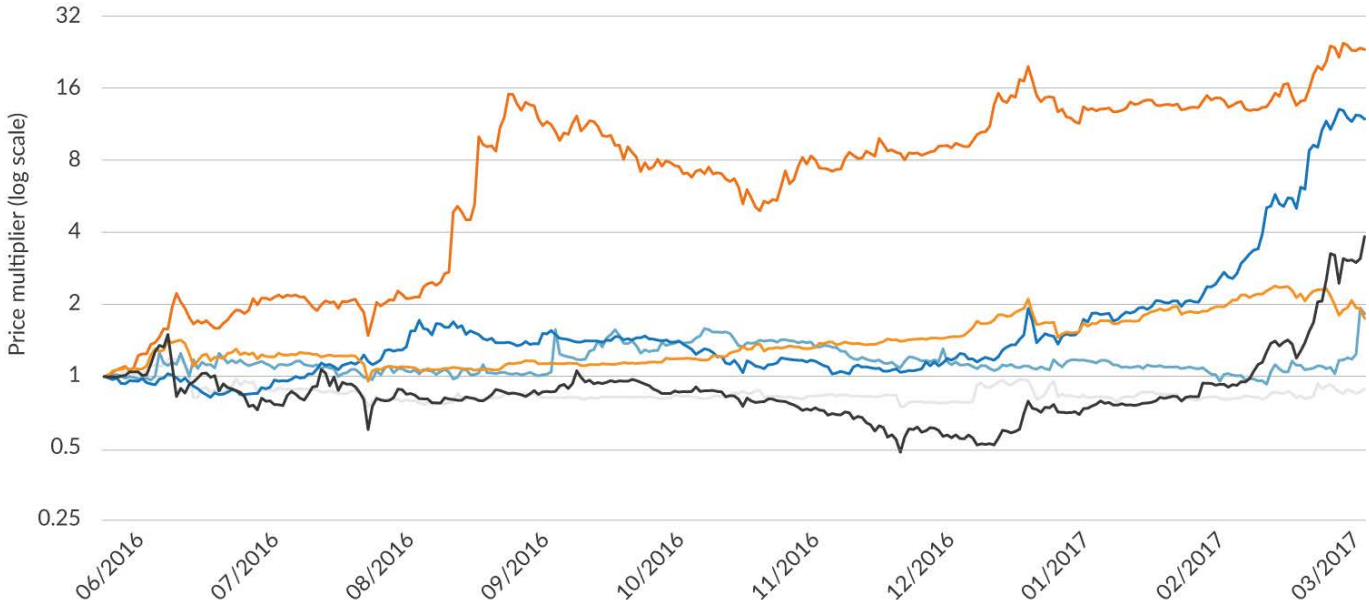

*Data sourced from CoinMarketCap*[5]

Although bitcoin remains the dominant cryptocurrency in terms of market capitalisation, other cryptocurrencies are increasingly cutting into bitcoin's historically dominant market cap share: while bitcoin's market capitalisation accounted for 86% of the total cryptocurrency market in March 2015, it has dropped to 72% as of March 2017 (Figure 3). Ether (ETH), the native cryptocurrency of the Ethereum network, has established itself as the second-largest cryptocurrency. The combined 'other cryptocurrency' category has doubled its share of the total market capitalisation from 3% in 2015 to 6% in 2017.

Privacy-focused cryptocurrencies DASH and monero (XMR) have become increasingly popular and currently constitute a combined 4% of the total cryptocurrency market capitalisation.

Figure 4 shows that both DASH and monero have experienced the most significant growth in terms of price in recent months. While monero's price already began skyrocketing in the summer of 2016, the price of DASH has increased exponentially since December 2016. The price of ether has also recovered since a series of attacks on the Ethereum ecosystem, starting with the DAO hack in June 2016, and increased 8x since its 2016 low of less than $7 in December. All listed cryptocurrencies have increased their market value in this time window.

Figure 4: Market prices of DASH, monero (XMR) and ether (ETH) have experienced the most significant growth since June 2016

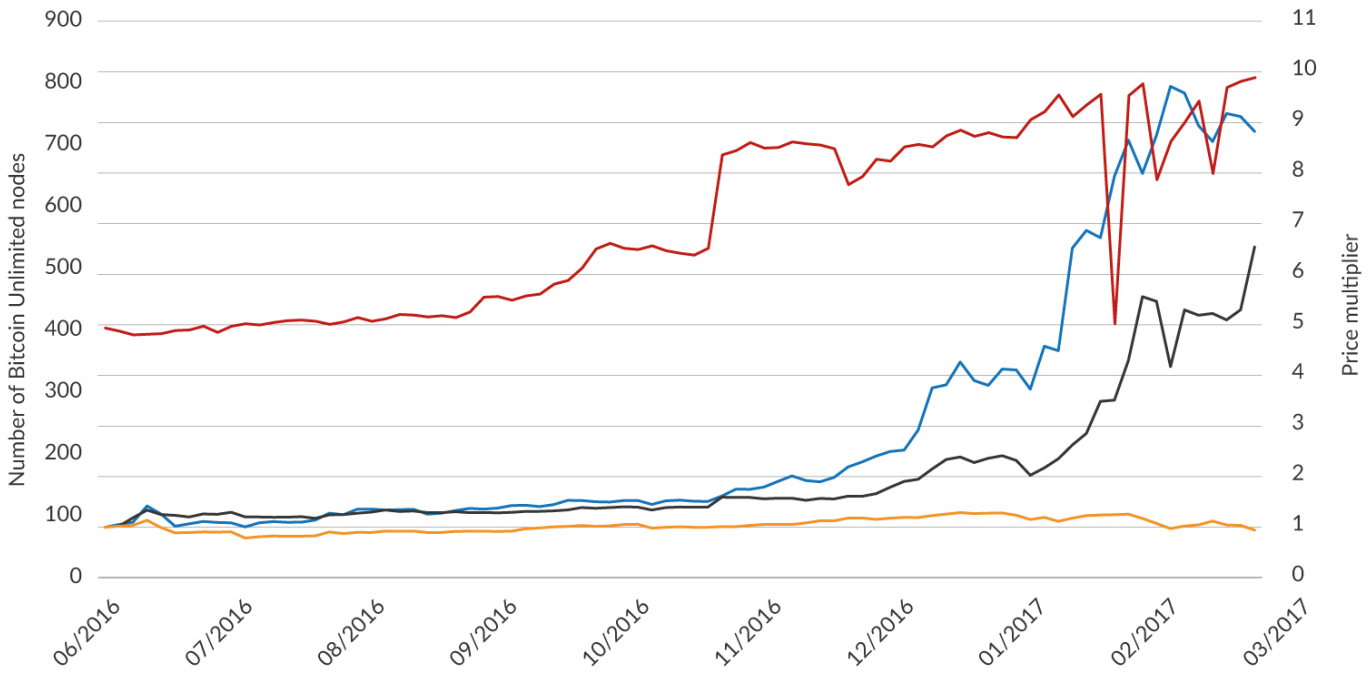



*Data sourced from CryptoCompare[6]*

*Note: the price multiplier variable shows the price evolution of each cryptocurrency since the beginning of June 2016. A value above 1 means that the price has increased by this factor, whereas a value below 1 indicates that the price has decreased during the specified time window.*

Bitcoin (BTC) | Ether (ETH) | DASH | Monero (XMR) | Ripple (XRP) | Litecoin (LTC)

Figure 5: Are ETH and DASH becoming the preferred 'safe haven' assets as Bitcoin's scaling debate heats up or is their price rise a sign of growing interest in other cryptocurrencies?




*Data sourced from CoinDance[7] and CryptoCompare*

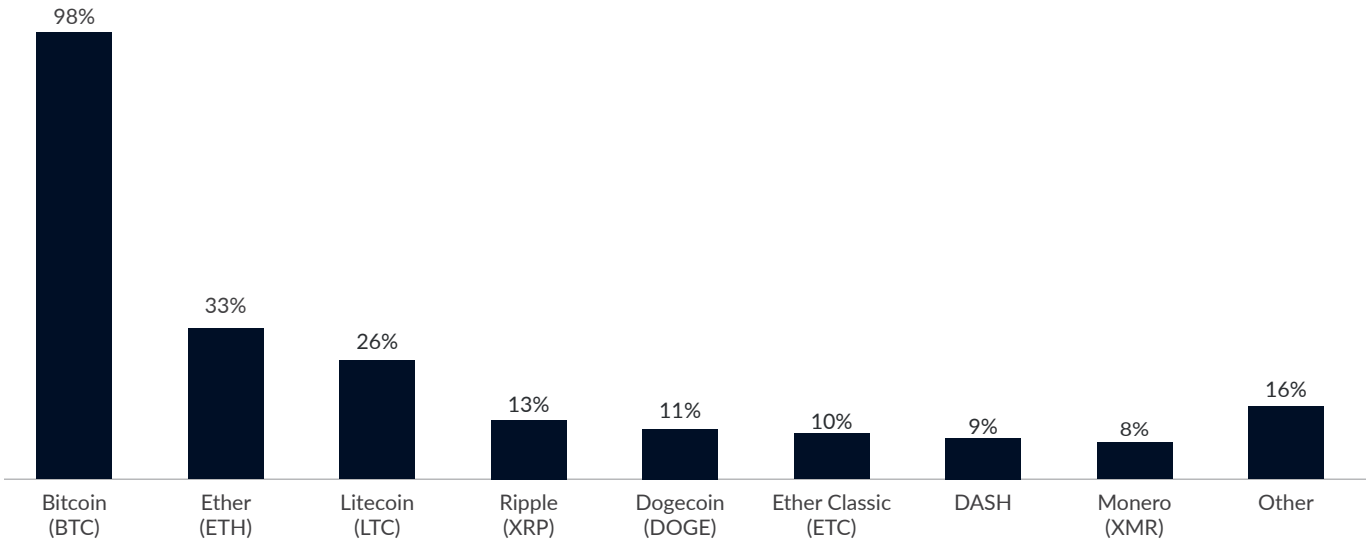
Number of Bitcoin Unlimited Nodes (left axis) | DASH (right axis) | Ether (right axis) | Bitcoin (right axis)

Table 1: Average daily number of transactions for largest cryptocurrencies

| | Bitcoin | Ethereum | DASH | Ripple | Monero | Litecoin |
|---|---|---|---|---|---|---|
| Q1 2016 | 201,595 | 20,242 | 1,582 | N/A | 579 | 4,453 |
| Q2 2016 | 221,018 | 40,895 | 1,184 | N/A | 435 | 5,520 |
| Q3 2016 | 219,624 | 45,109 | 1,549 | N/A | 1,045 | 3,432 |
| Q4 2016 | 261,710 | 42,908 | 1,238 | N/A | 1,598 | 3,455 |
| January - February 2017 | 286,419 | 47,792 | 1,800 | N/A | 2,611 | 3,244 |

*Data sourced from multiple block explorers*[8]

Figure 6: Bitcoin is the most widely supported cryptocurrency among participating exchanges, wallets and payment companies




When comparing the average number of daily transactions performed on each cryptocurrency's payment network, Bitcoin is by far the most widely used, followed by considerably distant second-place Ethereum (Table 1). All other cryptocurrencies have rather low transaction volumes in comparison. However, a general trend towards rising transaction volumes can be observed for all analysed cryptocurrencies since Q4 2016 (except Litecoin, whose volumes are stagnant). Monero and DASH transaction volumes are growing the fastest.

If significant price movements and on-chain transaction volumes reflect the popularity of a cryptocurrency system, it can be established that DASH, Monero and Ethereum have seen the greatest increase in popularity in recent months.

Nevertheless, Bitcoin remains the clear leader both in terms of market capitalisation and usage despite the rising interest in other cryptocurrencies. Bitcoin is also the cryptocurrency that is supported and used by the overwhelming majority of wallets, exchanges and payment service providers that participated in this study (Figure 6). As a result, the report will be mainly focused on bitcoin although we attempt to consider other cryptocurrencies whenever it is relevant to do so and sufficient data exists.

Table 2: The four key cryptocurrency industry sectors and their primary function

| Industry sectors | Primary function |
|---|---|
| Exchanges | Purchase, sale and trading of cryptocurrency |
| Wallets | Storage of cryptocurrency |
| Payments | Facilitating payments using cryptocurrency |
| Mining | Securing the global ledger ('blockchain') generally by computing large amounts of hashes to find a valid block that gets added to the blockchain |

# THE CRYPTOCURRENCY INDUSTRY

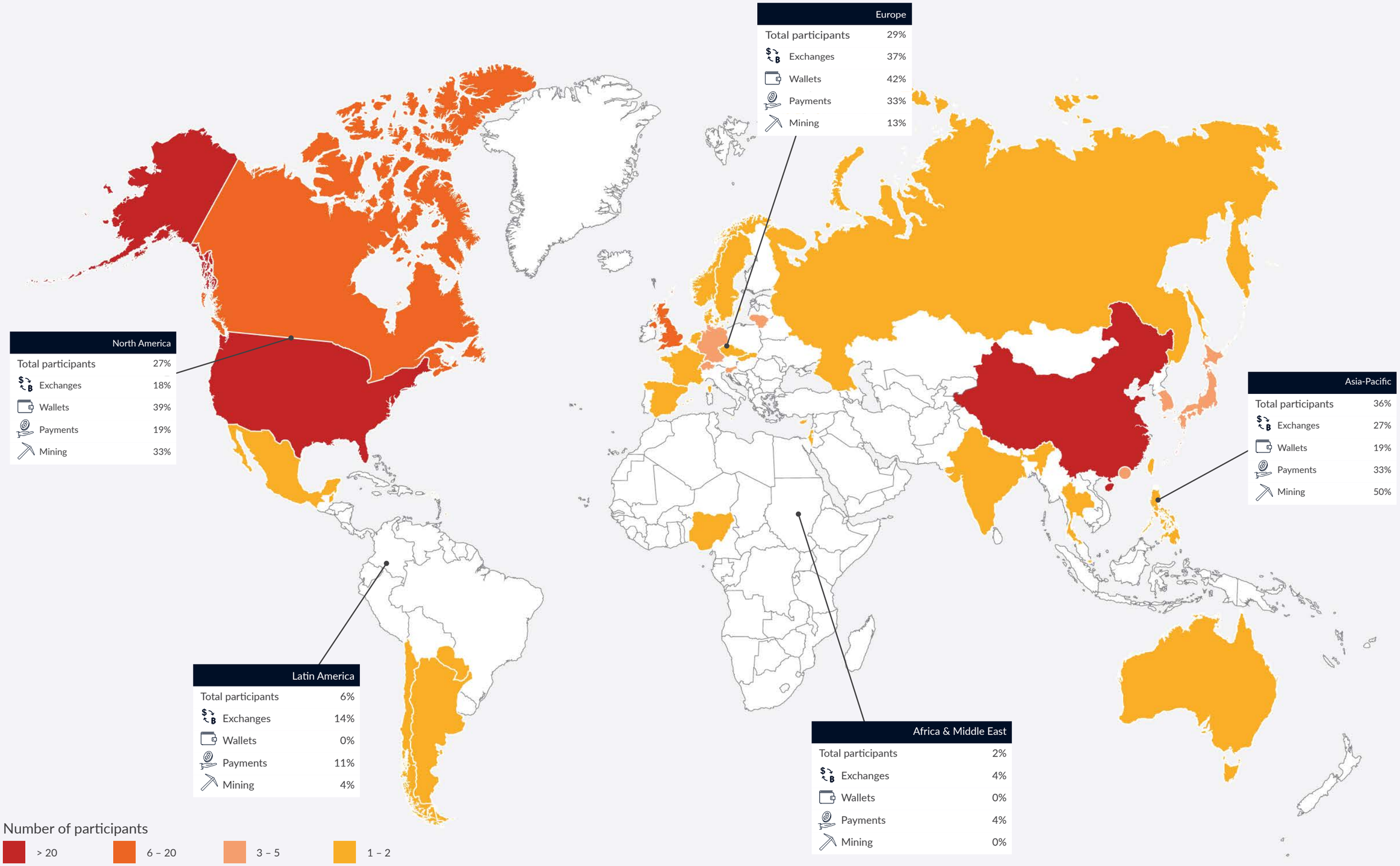
### EMERGENCE OF A BUSINESS ECOSYSTEM

A multitude of projects and companies have emerged to provide products and services that facilitate the use of cryptocurrency for mainstream users and build the infrastructure for applications running on top of public blockchains. A cryptocurrency ecosystem, composed of a diverse set of actors, builds interfaces between public blockchains, traditional finance and various economic sectors. The existence of these services adds significant value to cryptocurrencies as they provide the means for public blockchains and their native currencies to be used beyond in the broader economy.

### CRYPTOCURRENCY INDUSTRY SECTORS

While the cryptocurrency industry is composed of many important actors and groups, this study limits the analysis to what we believe are the four key cryptocurrency industry sectors today: exchanges, wallets, payments companies, and mining (Table 2).[9]

Figure 7: The geographical distribution of study participants



*Exchanges* can be used to buy, sell and trade cryptocurrencies for other cryptocurrencies and/or national currencies, thereby offering liquidity and setting a reference price. *Wallets* provide a means to securely store cryptocurrencies by handling key management. The *payments* sector is composed of companies that provide a wide range of services to facilitate cryptocurrency payments. Finally, the *mining* sector is responsible for confirming transactions and securing the global record of all transactions (the 'blockchain').

> The lines between the different cryptocurrency industry sectors are increasingly blurred and a growing number of cryptocurrency companies can be characterised as 'universal' platforms

Each of these sectors has its own working taxonomy that subdivides actors and activities into more refined categories to account for the diversity of services within each industry sector. These taxonomies are presented at the beginning of each of the report sections.

While we have organised this report in a way that suggests distinct industry sectors, it should be noted that the lines between sectors are increasingly blurred. Some companies provide a platform featuring products and services across multiple industry sectors, whereas others are operating in multiple industry segments using different brands. In fact, 19% of cryptocurrency companies that participated in the study provide services that span two industry sectors, 11% are active in three industry sectors, and some entities operate across all four industry sectors. A growing number of companies in the industry can thus be considered *universal* cryptocurrency platforms given the diverse range of products and services they offer to their customers.

It can be observed that wallets are progressively integrating exchange services within the wallet interface as a means to load the wallet, while exchanges often also provide a means to securely store newly acquired cryptocurrency within their platform. Similarly, payment companies increasingly offer fully-fledged money transfer platforms that enable the storage and transfer of cryptocurrencies, and often include an integrated currency exchange service. As a result, putting cryptocurrency companies into fixed categories can represent a challenging task in some cases.

**THE GEOGRAPHY OF THE CRYPTOCURRENCY INDUSTRY**

Our sample covers cryptocurrency companies, organisations and individuals across 38 countries. The United States leads with 32 study participants, closely followed by China where 29 participants are based (Figure 7). After a significant gap, the United Kingdom comes third with 16 participants, followed by Canada where 7 participants are based.

In terms of regional distribution, most study participants come from the Asia-Pacific region (36%). Europe and North America follow with 29% and 27%, respectively. Only a small proportion of study participants are based in Latin America (6%) as well as Africa and the Middle East (2%).

Figure 8: Cryptocurrency companies based in Asia-Pacific and North America have the highest number of employees

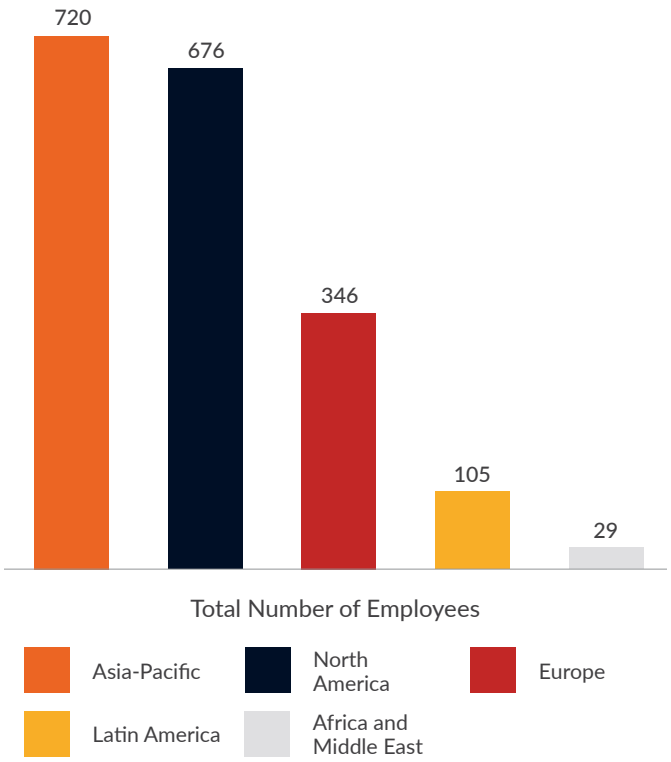
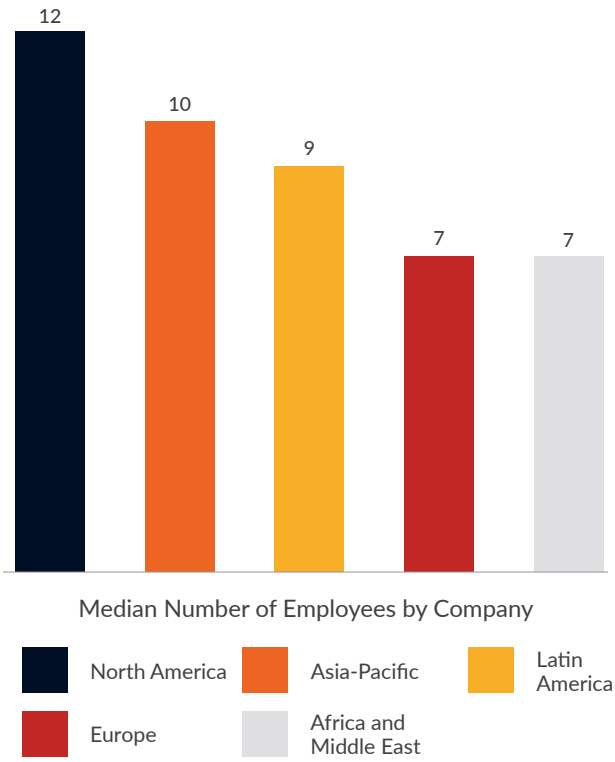



Figure 9: North American cryptocurrency companies have the highest median number of employees




# EMPLOYEES

## At least 1,876 people work full-time in the cryptocurrency industry

Combining the participating entities of all industry sectors reviewed in this report (with the exception of miners, for which no employee data was collected), the lower bound of the total number of people employed in the cryptocurrency industry can be established at 1,876 employees.

Significant differences between regions can be observed (Figure 8). Most full-time employees of the cryptocurrency industry are employed by companies based in Asia-Pacific, followed closely by North America (and more specifically the US). With a considerable gap follows Europe, while the total number of people working for cryptocurrency firms based in Latin America and especially Africa and the Middle East are comparatively low. However, it should be noted that many companies have offices in several regions and not all employees work in the region where the employer is based.

Companies surveyed have 21 full-time employees on average, but the existence of several large companies with considerable headcount makes it useful to also examine the median number of employees, which is nine. Figure 9 shows that study participants based in North America have the highest median number of employees (12), whereas participants from Africa and the Middle East as well as from Europe have the lowest (seven).

# USE CASES AND ACTIVITY


**USE CASES**

As discussed in more detail in appendix A, the use cases for cryptocurrencies can be grouped into four major categories:

* Speculative digital asset/investment
* Medium of exchange
* Payment rail
* Non-monetary use cases

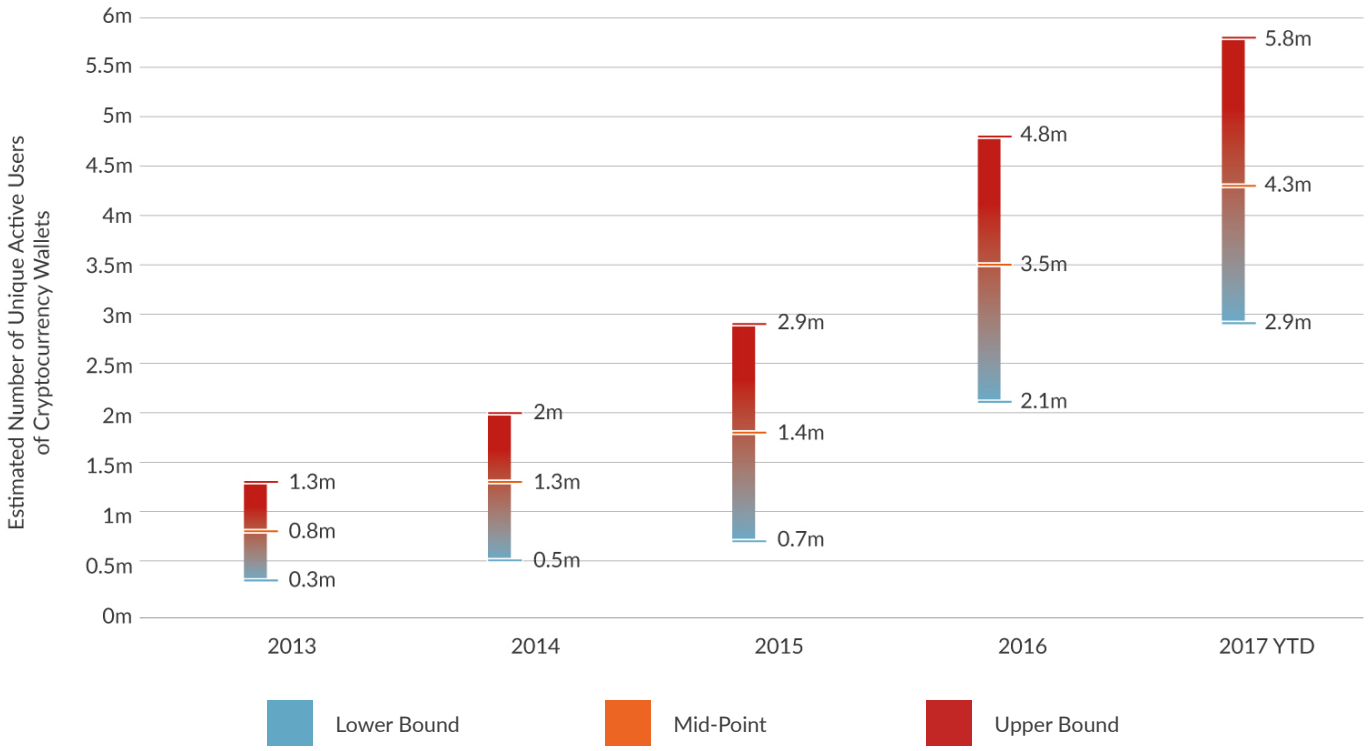
Some evidence exists that as of today the main use case for cryptocurrencies is speculation. A 2016 joint report from Coinbase and ARK Invest estimates that 54% of Coinbase users use bitcoin strictly as an investment.[10] Global bitcoin trading volumes have been significantly higher than network transaction volumes, a figure that is even higher for most other cryptocurrencies. However, it must also be noted that a rising number of cryptocurrency transactions are not performed '*on-chain*' (i.e., directly on the blockchain network), but '*off-chain*' via internal accounting systems operated by centralised exchanges, wallets and payment companies. These off-chain transactions do not appear on a public ledger.

Estimates of the use of cryptocurrency for payments has varied significantly across different sources. For example, a 2016 report from the Boston Federal Reserve has estimated that 75% of US consumer who own cryptocurrencies have used them for payments within a 12 month period, while the Coinbase/ARK Invest report indicates that 46% of Coinbase users use bitcoin as a 'transactional medium' (defined as making at least one payment per year).[11] While a growing number of merchants worldwide are accepting cryptocurrency as a payment method, it appears that cryptocurrencies are not primarily being used as a medium of exchange for daily purchases.[12] This is due to several factors, including price volatility and the lack of a 'closed loop' cryptocurrency economy, in which people or businesses would get paid in cryptocurrency and then use cryptocurrency as a primary payment method for everyday expenses.

As will be discussed in more detail in the Payments section, a considerable number of companies have emerged that use cryptocurrency networks primarily as a 'payment rail' to make fast and cheap cross-border payments. However, following the recent surge in bitcoin transaction fees, some are reconsidering this strategy and shifting transactions towards private blockchain-based solutions. Ripple's payment network is being used by large financial institutions, with 15 of the world's largest banks working with Ripple's global consensus ledger.

Finally, Ethereum has established itself as a major blockchain system for non-monetary applications, with nearly 400

Figure 10: The estimated number of unique active users of cryptocurrency wallets has grown significantly since 2013 to between 2.9 million and 5.8 million today




projects building on its decentralised computing platform.[13] Ethereum is also increasingly being used as a platform for launching new cryptocurrencies that are powering applications built on Ethereum (*dApp tokens*). Non-monetary use of Bitcoin has also increased. For example, the use of the OP_RETURN feature in the bitcoin scripting language (frequently used for embedding metadata in bitcoin transactions, for enabling e.g., time-stamping services and overlay networks) has increased roughly 100x since January 2015.[14]

**USERS**

Estimating both the number of cryptocurrency holders and users is a difficult endeavour as individuals can use multiple wallets from several providers at the same time. Moreover, one single user can have multiple wallets and exchange accounts for different cryptocurrencies and thus be counted multiple times. In addition, many individuals are using centralised wallet, exchange or payment platforms that pool funds together into a limited number of large wallets or addresses, which further complicates the picture.

> It is impossible to know *precisely* how many people use cryptocurrency

According to the earlier referenced 2016 report from the Boston Federal Reserve, 0.87% of US consumers are estimated to have owned cryptocurrency in 2015, which amounts to around 2.8 million people in the US alone. Based on calculations using their own user data, Coinbase and ARK Research estimate that in 2016 around 10 million people around the world have owned bitcoin.

Using data obtained from study participants and assuming that an individual holds on average two wallets, we estimate that currently there are between 2.9 million and 5.8 million unique users *actively* using a cryptocurrency wallet.[15] This figure has significantly increased since 2013 (Figure 10). It is important to note that our estimate of the total number of active wallets does not include users whose exchange accounts serve as their de facto wallet to store cryptocurrency, nor users from payment service providers or other platforms that enable the storage of cryptocurrency. In other words, the total number of active cryptocurrency users is likely considerably higher than our estimate of unique active wallet users.

For a variety of reasons, determining the geographical distribution of cryptocurrency users is challenging. Appendix C contains a discussion of the geographical dispersion of users based on data we collected and public data sources.

# EXCHANGES

Exchanges provide on-off ramps for users wishing to buy or sell cryptocurrency. The exchange sector is the first to have emerged in the cryptocurrency industry and remains the largest sector both in terms of the number of companies and employees.

# KEY FINDINGS

**Services/Operations**

- Of all industry sectors covered in this study, the exchange sector has the highest number of operating entities and employs the most people
- 52% of small exchanges hold a formal government license compared to only 35% of large exchanges
- 73% of small exchanges have one or two cryptocurrencies listed, while 72% of large exchanges provide trading support for two or more cryptocurrencies: bitcoin is supported by all exchanges, followed by ether (43%) and litecoin (35%)
- A handful of large exchanges and four national currencies (USD, EUR, JPY and CNY) dominate global cryptocurrency trading volumes
- Study participants reported cryptocurrency trading in 42 different national currencies
- 53% of exchanges support national currencies other than the five global reserve currencies (USD, CNY, EUR, GBP, JPY)
- Exchange services/activities fall into three categories - order-book exchanges, brokerage services and trading platforms: 72% of small exchanges specialise in one type of exchange activity (brokerage services being the most widely offered), while the same percentage of large exchanges are providing multiple exchange activities
- 73% of exchanges take custody of user funds, 23% let users control keys

**Security**

- On average, security headcount corresponds to 13% of total employees, and 17% of budget is spent on security; small exchanges have slightly higher figures than large exchanges
- 80% of large exchanges and 69% of small exchanges use external security providers; large exchanges use a larger number of external security providers than small exchanges
- Optional two-factor authentication (2FA) is offered for customers by a majority of exchanges and required for employees for most operations; small exchanges tend to use 2FA less than large exchanges
- Exchanges use a variety of internal security measures; differences in approaches are observed between small and large exchanges
- Only 53% of small custodial exchanges have a written policy outlining what happens to customer funds in the event of a security breach resulting in the loss of customer funds, compared to 78% of large custodial exchanges
- 79% of exchanges provide regular security training programs to their staff
- 92% of exchanges use cold-storage systems; on average 87% of funds are kept in cold storage
- Multi-signature architecture is supported by 86% of large exchanges and 76% of small exchanges
- Frequency of formal security audits varies considerably between exchanges; large exchanges tend to perform them on a more regular basis
- 60% of large exchanges have external parties performing their formal security audits, while 65% of small exchanges perform them internally.
- 33% of custodial exchanges have a proof-of-reserve component as part of their formal security audit

Table 3: Taxonomy of exchange services

| Type of activity | Description |
|---|---|
| Order-book exchange | Platform that uses a trading engine to match buy and sell orders from users |
| Brokerage service | Service that lets users conveniently acquire and/or sell cryptocurrencies at a given price |
| Trading platform | Platform that provides a single interface for connecting to several other exchanges and/or offers leveraged trading and cryptocurrency derivatives |

# INTRODUCTION AND LANDSCAPE

### INTRODUCTION

Exchanges provide services to buy and sell cryptocurrencies and other digital assets for national currencies and other cryptocurrencies. Exchanges play an essential role in the cryptocurrency economy by offering a marketplace for trading, liquidity, and price discovery.

Throughout this section, we define a cryptocurrency exchange as any entity that allows customers to exchange (buy/sell) cryptocurrencies for other forms of money or assets. We use the taxonomy in Table 3 for categorising the three main types of activities provided by cryptocurrency exchanges.

### LANDSCAPE

Exchanges were one of the first services to emerge in the cryptocurrency industry: the first exchange was founded in early 2010 as a project to enable early users to trade bitcoin and thereby establish a market price. The exchange sector remains the most populated in terms of the number of active entities. One data services website alone lists daily trading volumes for 138 different cryptocurrency exchanges, which suggests that the total number of operating exchanges is likely considerably higher.[1]

We collected data from 51 exchanges based in 27 countries and representing all five world regions (Figure 11). Our sample contains more exchanges from Europe than any other region, followed by Asia-Pacific. With regards to individual countries, the United Kingdom and the United States are leading with 18% and 12%, respectively, of all cryptocurrency exchanges.

However, the market share in terms of bitcoin trading volume is substantially different: although there are a hundreds of companies providing cryptocurrency exchange services, fewer than a dozen order-book exchanges dominate bitcoin trading (Figure 12).[2]

Figure 11: Europe has the most number of exchanges in our study sample, followed by Asia-Pacific

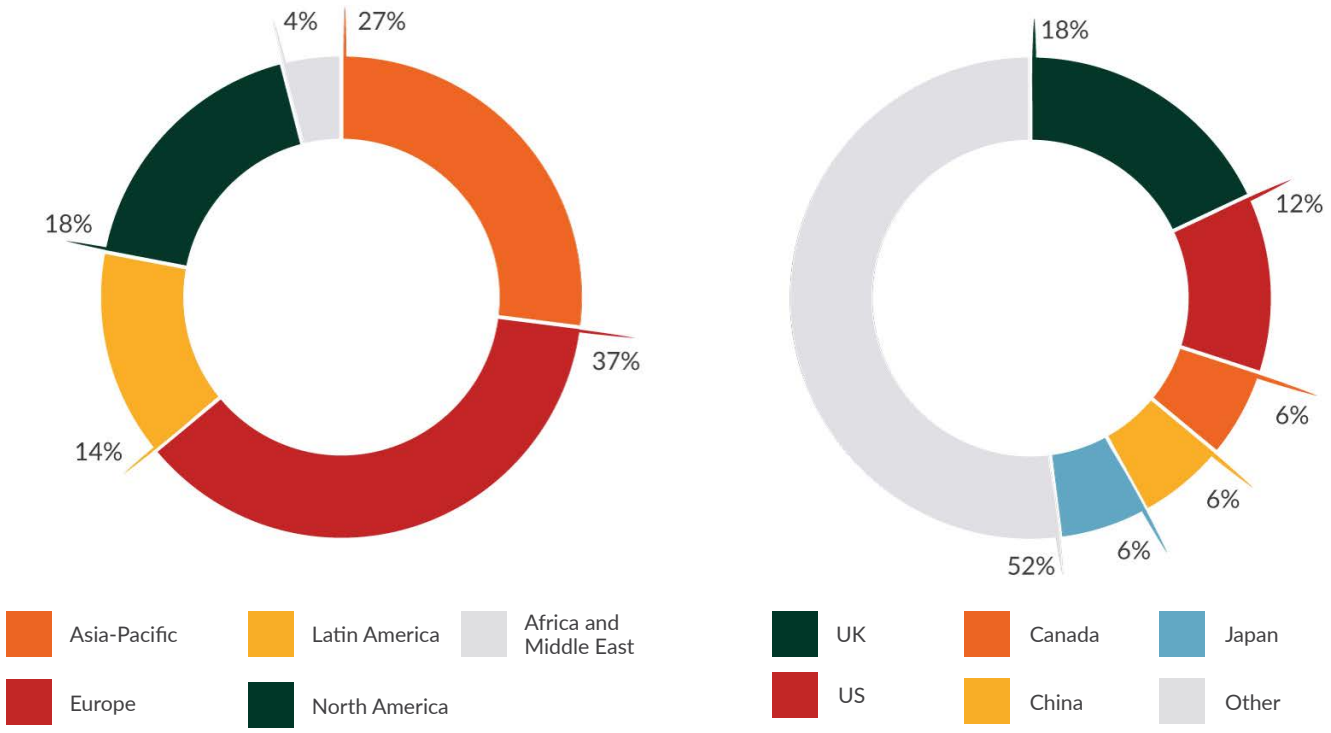
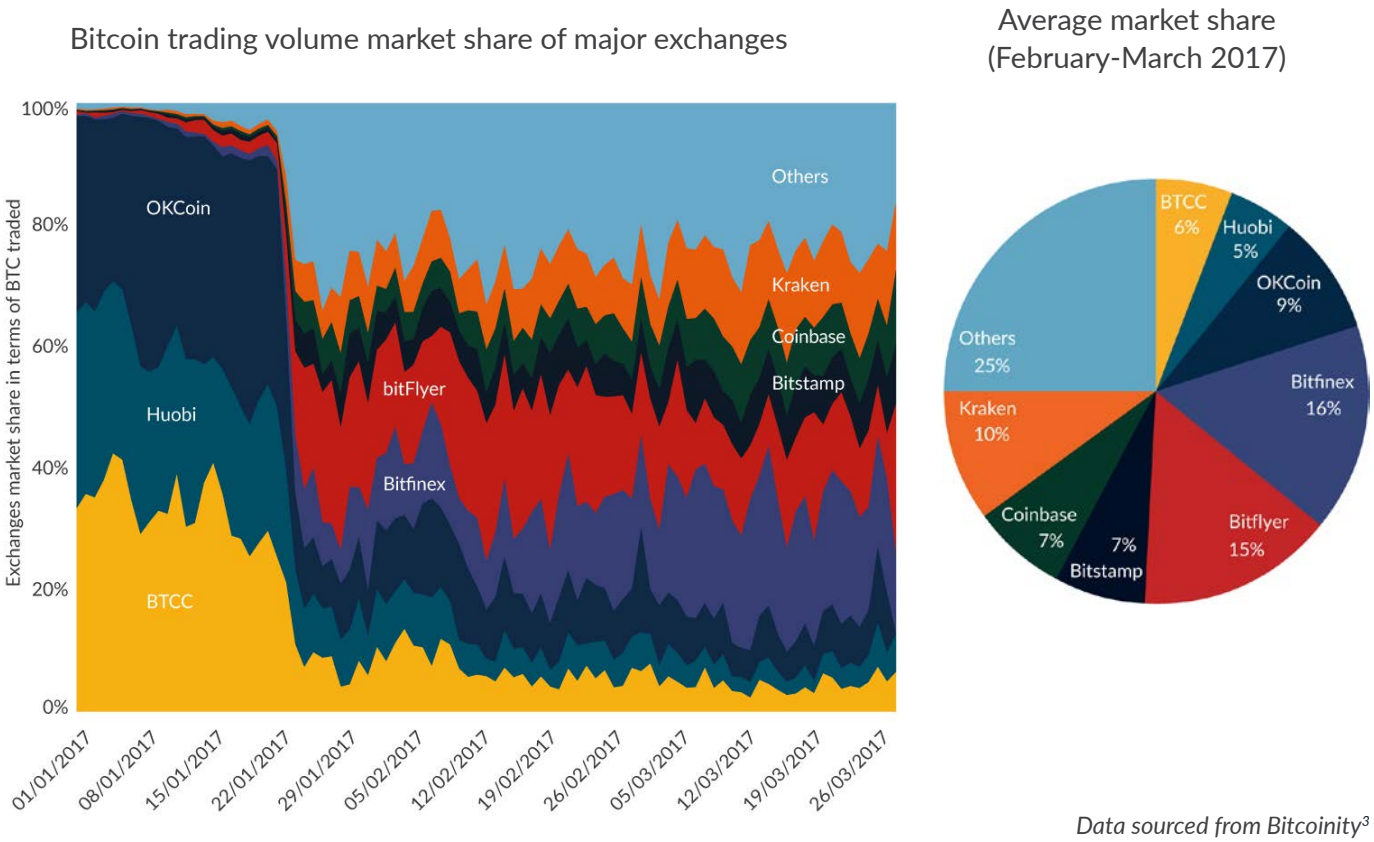
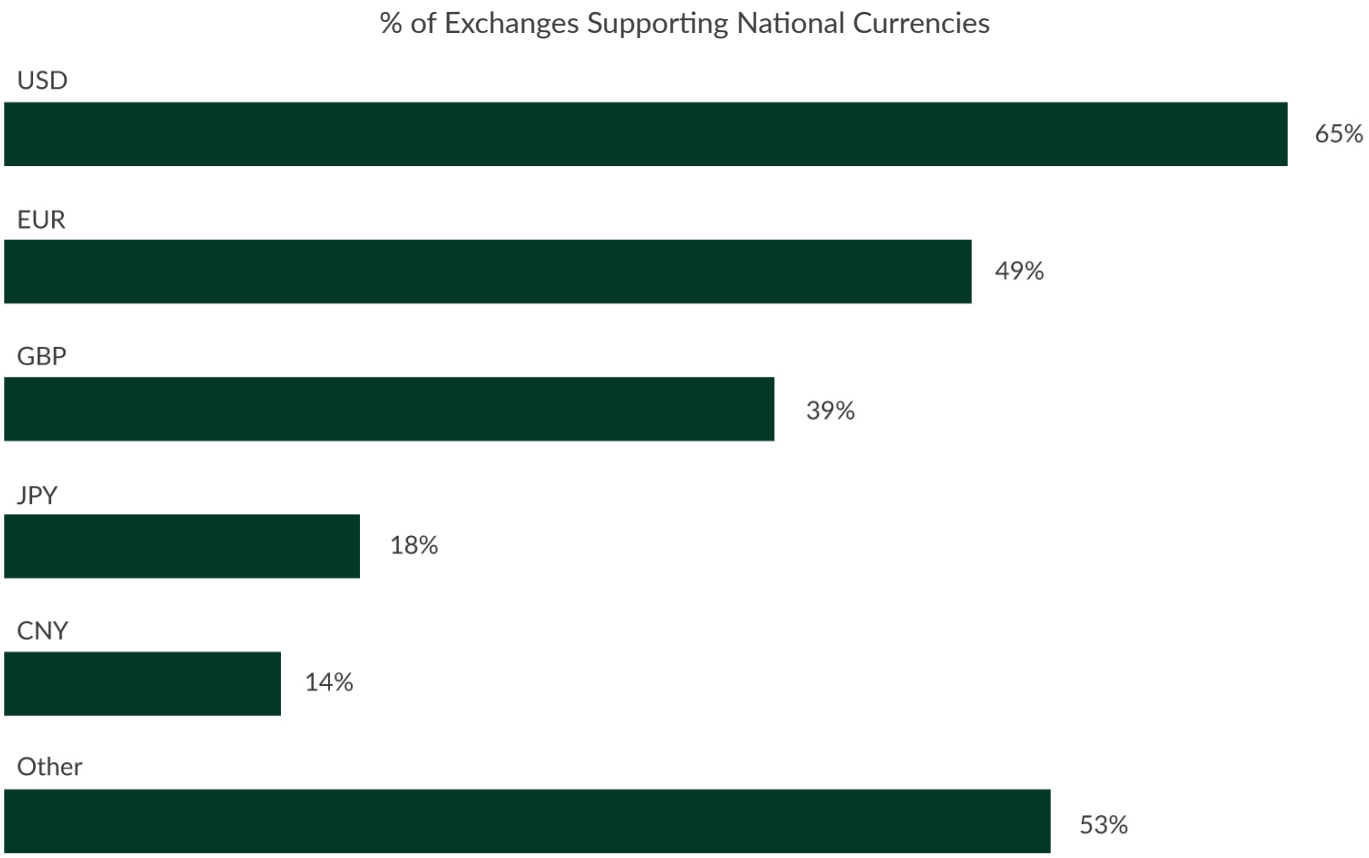



Figure 12: Trading volumes across the top exchanges are more evenly distributed following increased regulation of Chinese exchanges in early 2017




*Data sourced from Bitcoinity*[3]

Figure 13: USD is the most widely supported national currency on exchanges; many specialise in local currencies




In terms of trading volumes by national currencies, there are major differences as well between the top-traded currencies and the most widely supported currencies. The US dollar (USD) is the most widely supported national currency, followed by the Euro (EUR) and the British Pound (GBP) (Figure 13). While reported trading in the Chinese Renminbi (CNY) appeared to represent an often significant majority of global bitcoin trading volumes from 2014 to 2016 (ranging from 50% to 90%)[4], bitcoin trading denominated in CNY has plummeted in early 2017 after the tightening of regulation by the People's Bank of China (Figure 14).

> While global cryptocurrency trading volume is dominated by four reserve currencies, trading in at least 40 other national currencies is supported

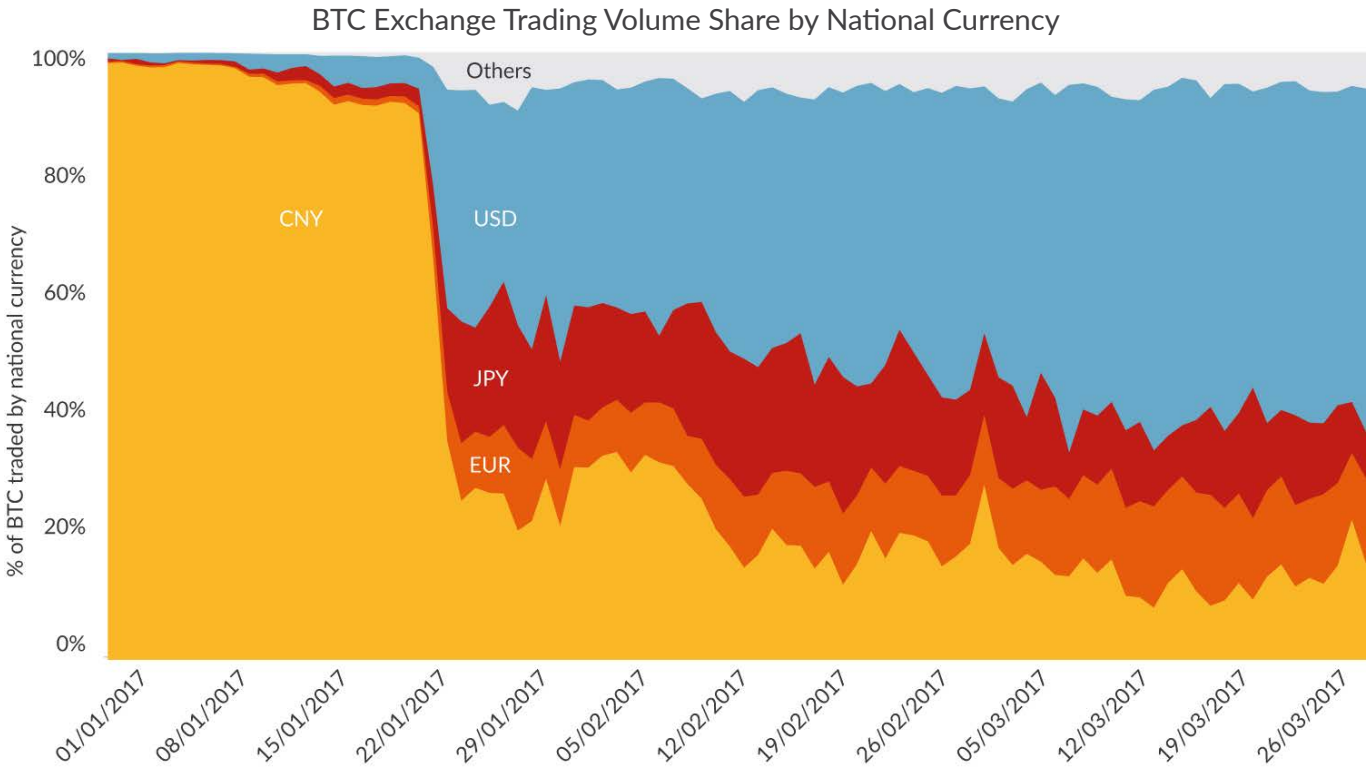
The data demonstrate that the exchange market is dominated by a handful of exchanges that are responsible for the majority of global bitcoin trading volumes, of which the lion share is denominated in a small number of international currencies. In contrast, the majority of exchanges (mostly small) specialise in local markets by supporting local currencies: 53% of all exchanges support national currencies other than the five reserve currencies. Trading volumes at most small exchanges are insignificant compared to the market leaders, but these exchanges service local markets and make cryptocurrencies more available in many countries.

### TYPES

Using the taxonomy of the three types of exchange activities introduced above, findings show that there are major differences between the services that small and large exchanges provide.[5] While 72% of small exchanges specialise in one type of activity, the same percentage of large exchanges are providing multiple types of exchange activities (Figure 15). The most popular combination of two activities are order-book exchanges that also offer a trading platform.

22% of large exchanges and only 4% of small exchanges offer a platform that includes an order-book exchange, trading

Figure 14: Trading in renminbi has plummeted since Chinese authorities tightened regulation




*Data sourced from Bitcoinity*

Figure 15: The majority of small exchanges specialise in a single type of exchange activity while large exchanges are generally engaged in more than one activity

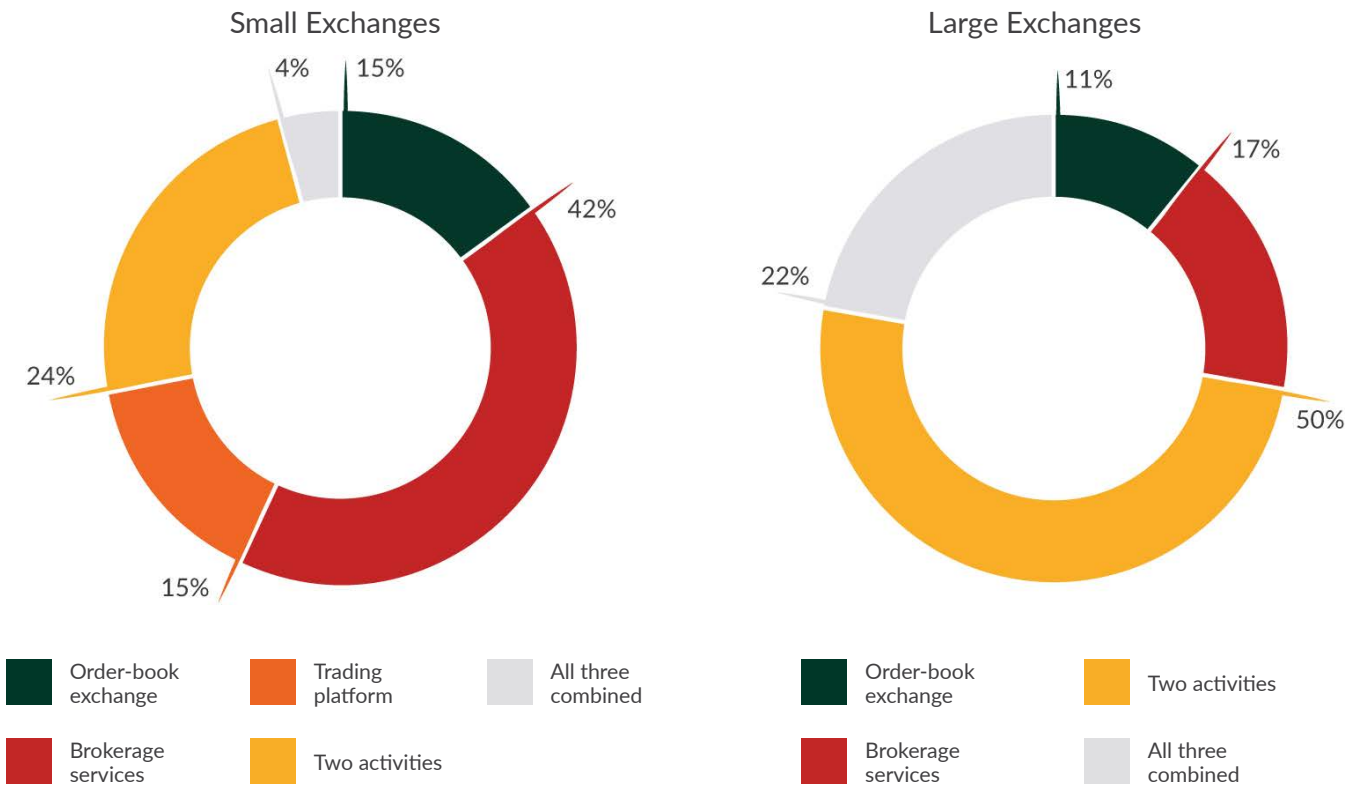
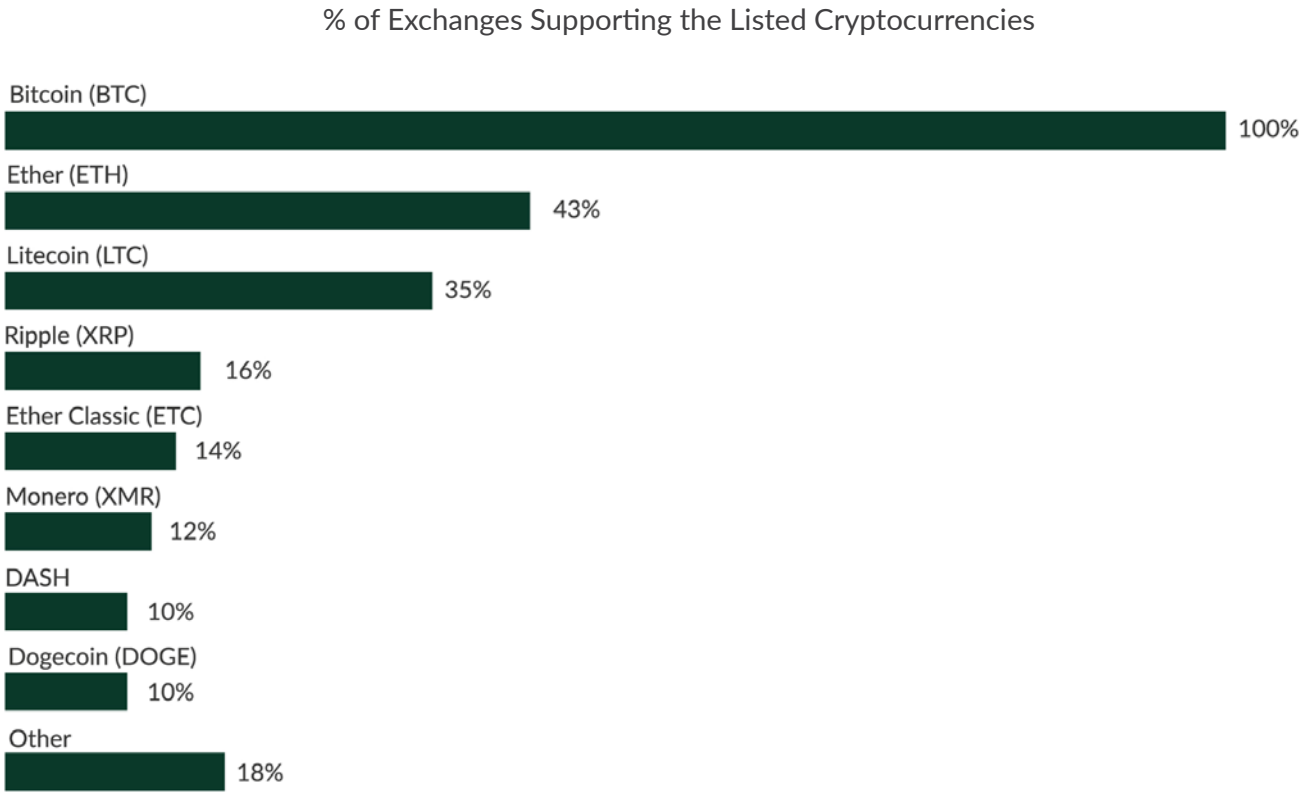


Figure 16: Bitcoin is listed on all surveyed exchanges; ether and litecoin are also widely supported




platform and brokerage services. Over 40% of small exchanges specialise in the provision of brokerage services, compared to only 17% of large exchanges. 15% of small exchanges provide a stand-alone trading platform, while large exchanges generally combine this activity with an order-book exchange.

Despite many cases of internal fraud and bankruptcies of centralised exchanges, P2P exchanges have yet to gain more popularity: of the 51 exchanges represented in this study, only 2 provide a decentralised marketplace for exchanging cryptocurrencies.

### SUPPORTED CRYPTOCURRENCIES

All exchanges support bitcoin, while ether and litecoin are listed on 43% and 35% of exchanges, respectively (Figure 16). Only a minority of exchanges make markets for the exchange of cryptocurrencies other than the above three.

While 39% of exchanges solely support bitcoin, 25% have two listed cryptocurrencies, and 36% of all entities enable trading three or more cryptocurrencies. We observe that 72% of large exchanges provide trading support for two or more cryptocurrencies, while 73% of small exchanges have only one or two cryptocurrencies listed. 6% of survey participants also provide cryptocurrency-based derivatives, and 16% are offering margin trading.

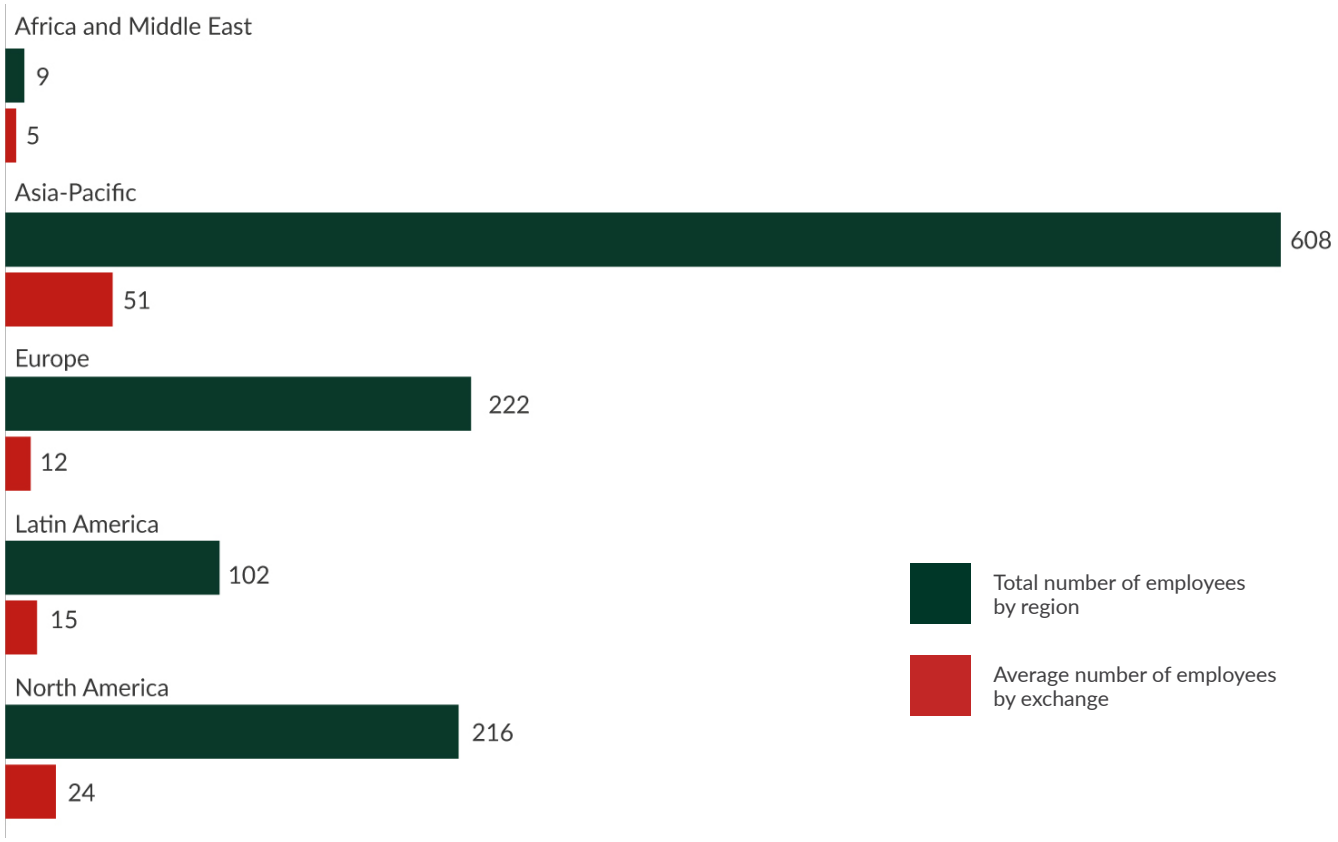
### EMPLOYEES

There are 1,157 total employees at participating exchanges, making exchanges the largest employer in the cryptocurrency industry.[6] Even though 37% of all exchanges are based in Europe, the total number of employees at European exchanges is considerably less than the total headcount at companies based in Asia-Pacific, where almost 60% of large exchanges are based (Figure 17).

> The exchange industry sector employs more people than any other cryptocurrency sector

On average, cryptocurrency exchanges employ 24 people. However, the distribution reveals that nearly half of exchanges have less than 11 employees (Figure 18), indicating that the majority of exchanges are small companies. Indeed, 20% of all exchanges have less than 5 employees. However, 9% of exchanges have more than 50 employees, with the largest employing around 150 people.

Figure 17: Asian-Pacific exchanges have the highest number of employees




*Note: these figures include employees from universal cryptocurrency companies that are also active in industry sectors other than exchanges.*

Figure 18: Nearly half of exchanges have less than 11 employees

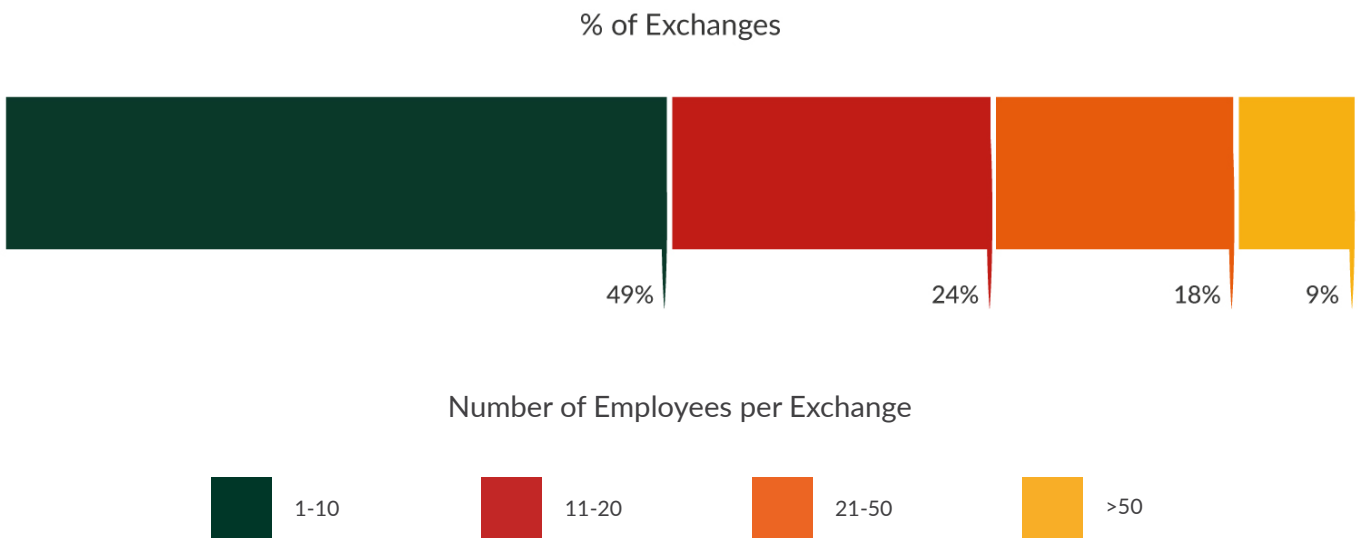
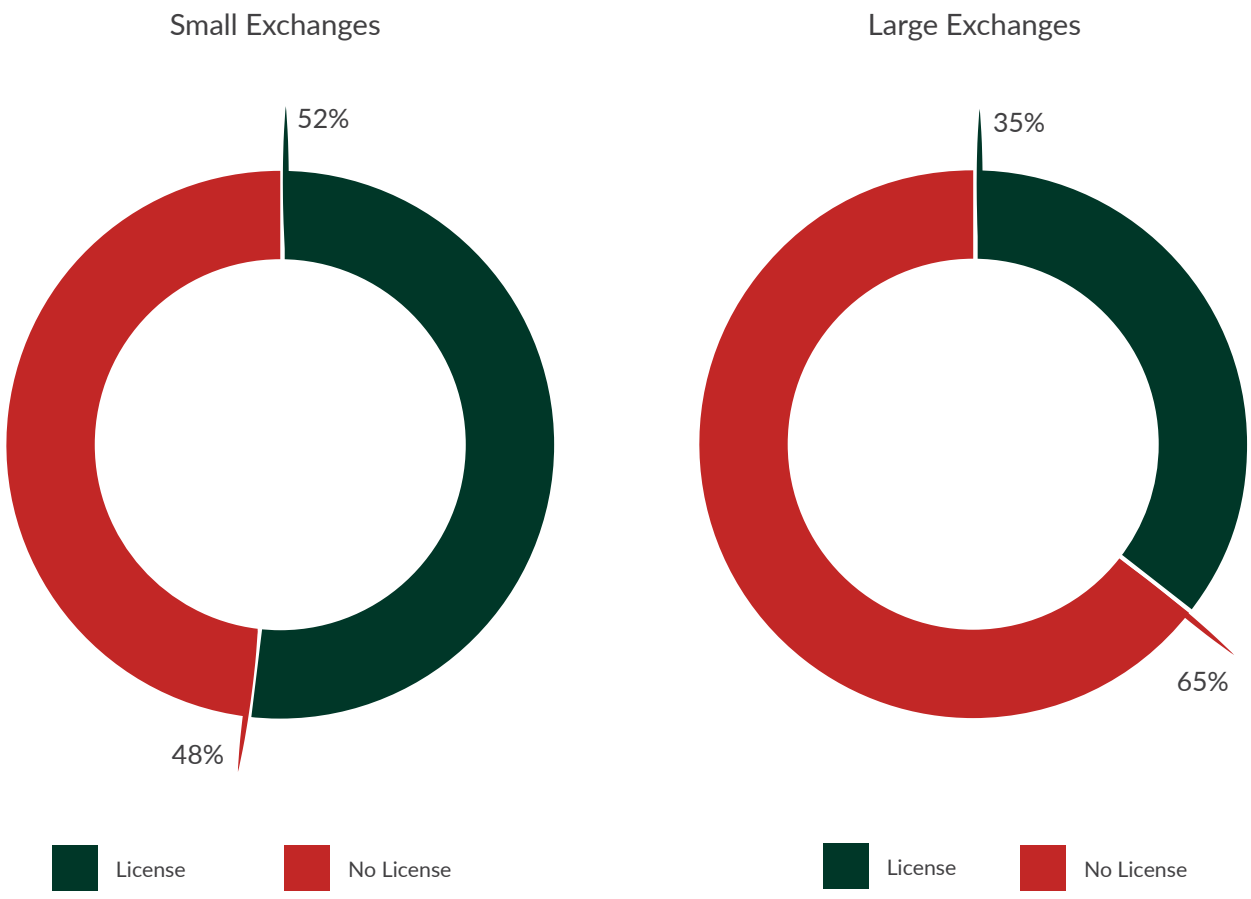


Figure 19: More than half of small exchanges hold a government license compared to only 35% of large exchanges




## LICENSE

One notable observation is the difference between the share of small and large exchanges that hold a government license of some kind: 52% of small exchanges have a formal government license or authorisation compared to only 35% of large exchanges (Figure 19).

85% of all exchanges based in Asia-Pacific do not have a license, whereas 78% of North American-based exchanges hold a formal government license or authorisation. 47% and 43% of European and Latin American-based exchanges, respectively, hold a license as well. However, not having a formal license does not necessarily mean that the exchanges are not regulated, as appears to be the case now with many of the China-based exchanges.

## OPERATIONAL CHALLENGES AND RISK FACTORS

We presented a list of operational challenges to participating exchanges and asked them to rate these factors according to the level of risk that they currently pose to operations. Findings show that while small and large exchanges rate certain factors approximately similarly, there are substantial differences with regards to other factors (Table 4). Generally, small exchanges have a tendency to rate risks higher than large exchanges.

The highest risk factor for small exchanges and second highest risk factor for large exchanges are security breaches that could result in a loss of funds.

One finding that stands out is that large exchanges rate challenges posed by regulation in general as posing the highest risk to their operations – a factor that is rated lower by small exchanges.

## Table 4: Operational risk factors rated by exchanges

Respondents Scored these Categories on a 1 - 5 Scale

1: Very low risk | 2: Low risk | 3: Medium risk | 4: High risk | 5: Very high risk

Lowest average score — Highest average score

| | Weighted average | Small exchanges | Large exchanges |
|---|---|---|---|
| IT security/hacking | **3.70** | 3.93 | 3.17 |
| Deteriorating banking relationships | **3.45** | 3.79 | 2.67 |
| Fraud | **3.08** | 3.50 | 2.08 |
| Regulation (in general) | **3.08** | 2.89 | 3.50 |
| Competitors/business model risk | **2.88** | 3.00 | 2.58 |
| Reputation risk | **2.88** | 2.93 | 2.75 |
| AML/KYC enforcement | **2.68** | 2.64 | 2.75 |
| Insufficient demand for services | **2.58** | 2.82 | 2.00 |
| Lack of talent | **2.46** | 2.52 | 2.33 |

Small exchanges seem to have considerable difficulties with either obtaining or maintaining banking relationships, while large exchanges appear to have this risk factor under control. Small exchanges are also substantially more concerned about fraud than large exchanges, which suggests that they are either targeted more often than large exchanges or simply that fraud has more a more severe financial impact due to the limited scale of their operations and budget.

Figure 20: 73% of exchanges take custody of users' cryptocurrency funds by controlling the private keys

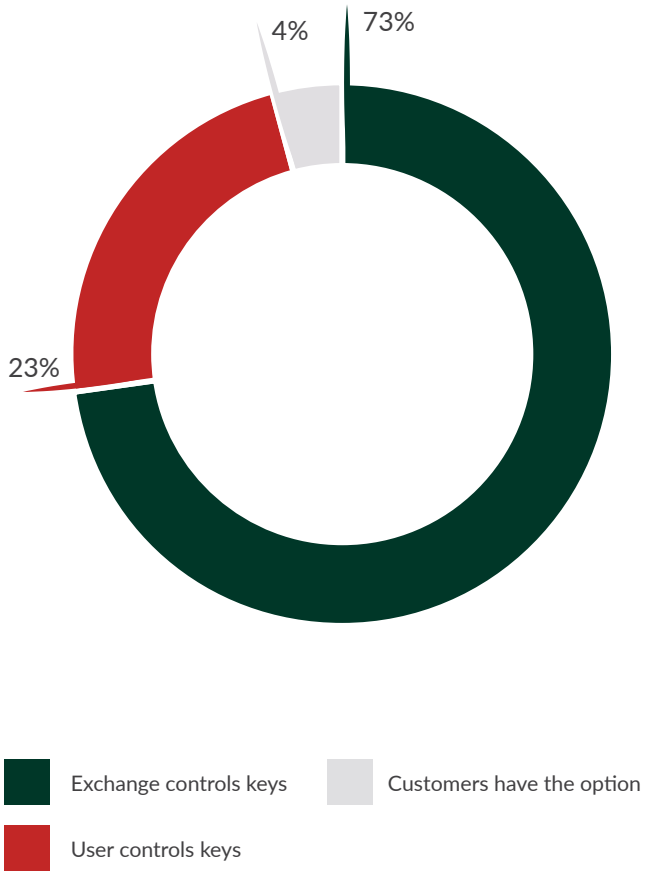
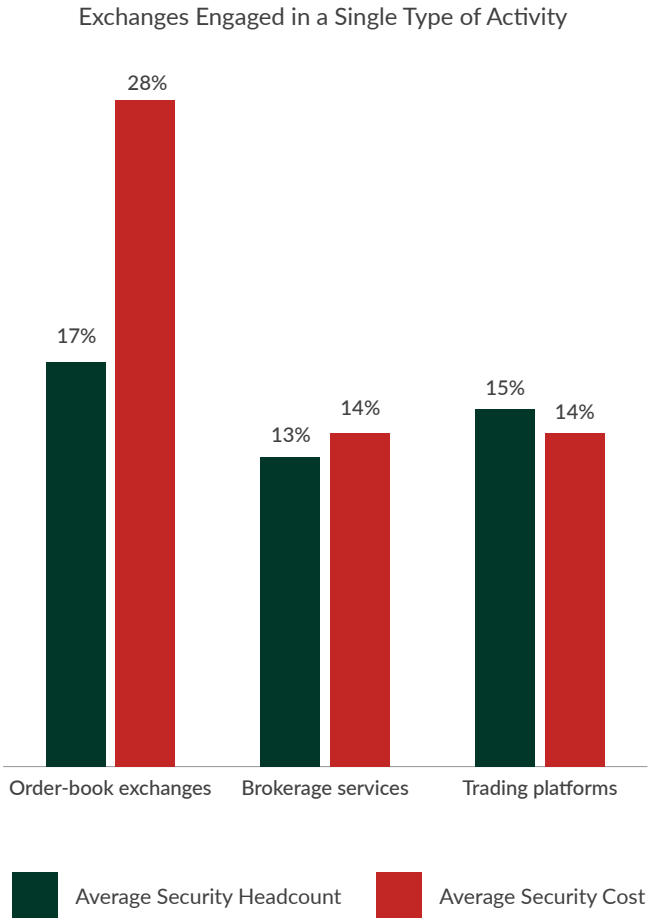



Figure 21: Order-book-only exchanges spend 2x more on security as a share of total budget than 'pure' brokerage services and trading platforms




# SECURITY

## EXCHANGES CONTINUE TO BE POPULAR TARGETS FOR CRIMINALS

Cryptocurrencies are digital bearer assets that once transferred cannot easily be recovered (i.e., the payment cannot be reversed unless the recipient decides to do so). The surge in market prices of cryptocurrencies in recent years has made exchanges a popular target for criminals as they handle and store large amounts of cryptocurrencies. Numerous events have led to the loss of exchange customer funds, and a wide variety of schemes have been employed ranging from outside server breaches to insider theft. In many cases, exchanges where losses occurred were forced to close and customer funds were never recovered. One 2013 study analysing the survival rate of 40 bitcoin exchanges found that over 22% of exchanges had experienced security breaches, forcing 56% of affected exchanges to go out of business.[7]

Figure 22: Small exchanges have a higher percentage of employees working full-time on security than large exchanges

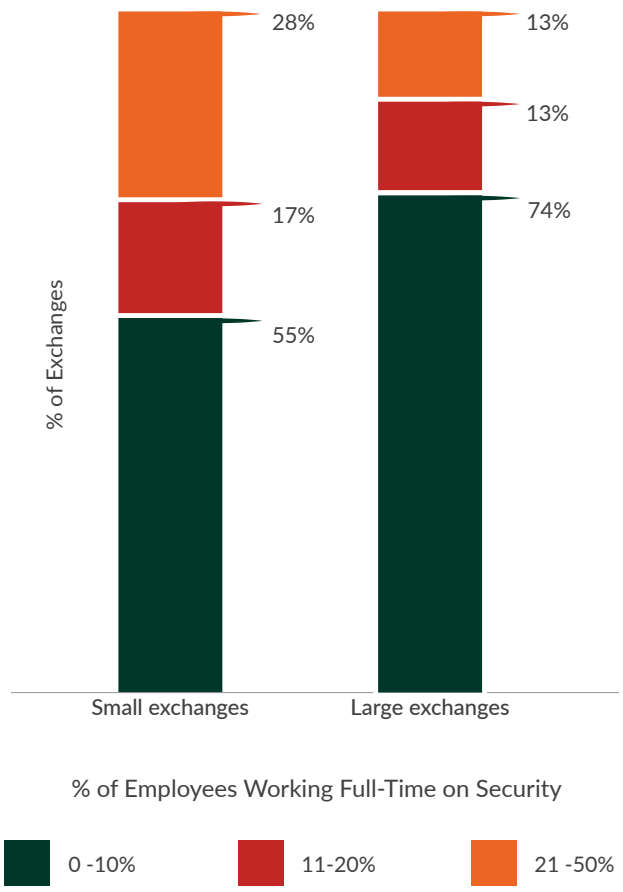
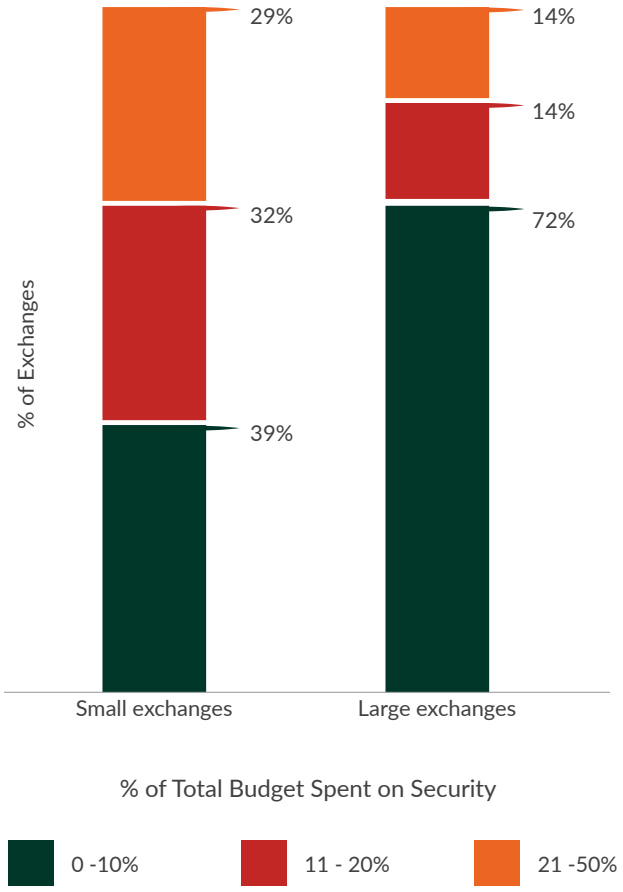



Figure 23: Large exchanges are realising economies of scale as they spend less of their total budget on security than small exchanges




73% of exchanges control customers' private keys, making them a potentially attractive 'honeypot' for hackers as these exchanges have possession of user funds denominated in cryptocurrency (Figure 20). 23% of exchanges do not control customers' private keys, thereby preventing exchanges from accessing customer holdings or not being able to return funds to users in the event the exchange ceases to function.[8] Large exchanges act more often as custodians than small exchanges: only 11% of large exchanges let users control keys compared to 30% of small exchanges.

### SECURITY HEADCOUNT AND COST

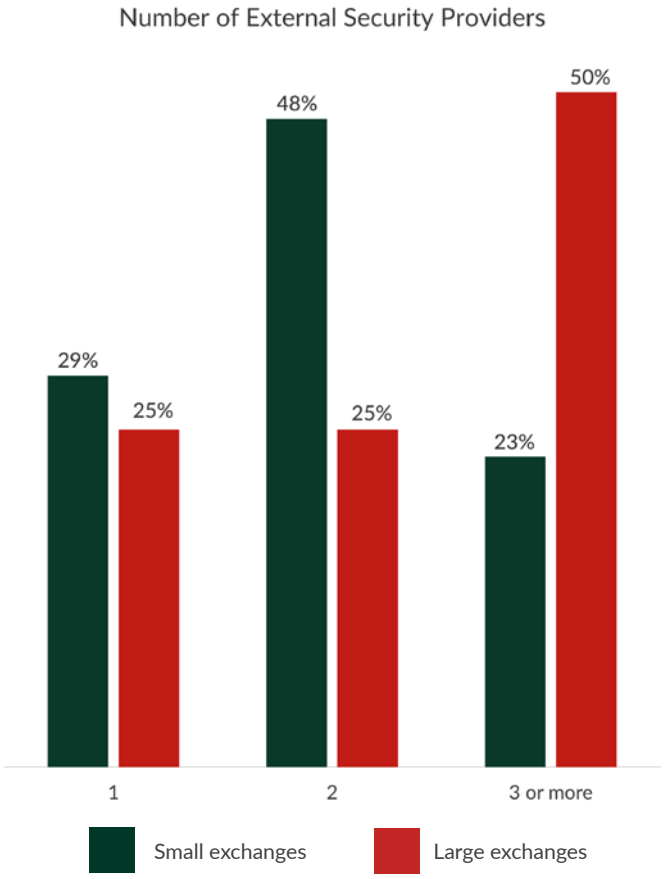
On average, exchanges have 13% of their employees working full-time on security and spend 17% of their total budget on security. Order-book-only exchanges (i.e., entities not engaged in brokerage services and trading platforms) spend two times more of their budget on security than companies providing solely brokerage services or pure trading platforms (Figure 21).

Findings show that on average, small exchanges have slightly higher headcount (+5%) associated with security than large exchanges. The distribution indicates that the security headcount ranges for both small and large exchanges from 0% to 50% of their total employees (Figure 22). 55% of small exchanges and 74% of large exchanges have between 0% and 10% of employees working full-time on security. In fact, more than half of large exchanges have less than 6% of headcount associated with security.

Similar to security headcount, we observe that small exchanges have on average a slightly higher cost (+7%) as a percentage of their budget associated with security than large exchanges. 72% of large exchanges spend less than 11%, while 61% of small exchanges spend more than 10% (Figure 23). The upper limit that both small and large exchanges spend on security cost is 50% of their total budget.

Percentage of Exchanges That Use External Security Providers


Figure 24: Large exchanges use a greater number of external security providers than small exchanges




## EXTERNAL SECURITY PROVIDERS

Over 70% of exchanges secure their systems with the help of external security providers, including external code reviewers, multi-signature wallet service providers and two-factor authentication (2FA) service providers. However, there are differences between small and large exchanges: 80% of large exchanges use external security providers as opposed to 69% of small exchanges.

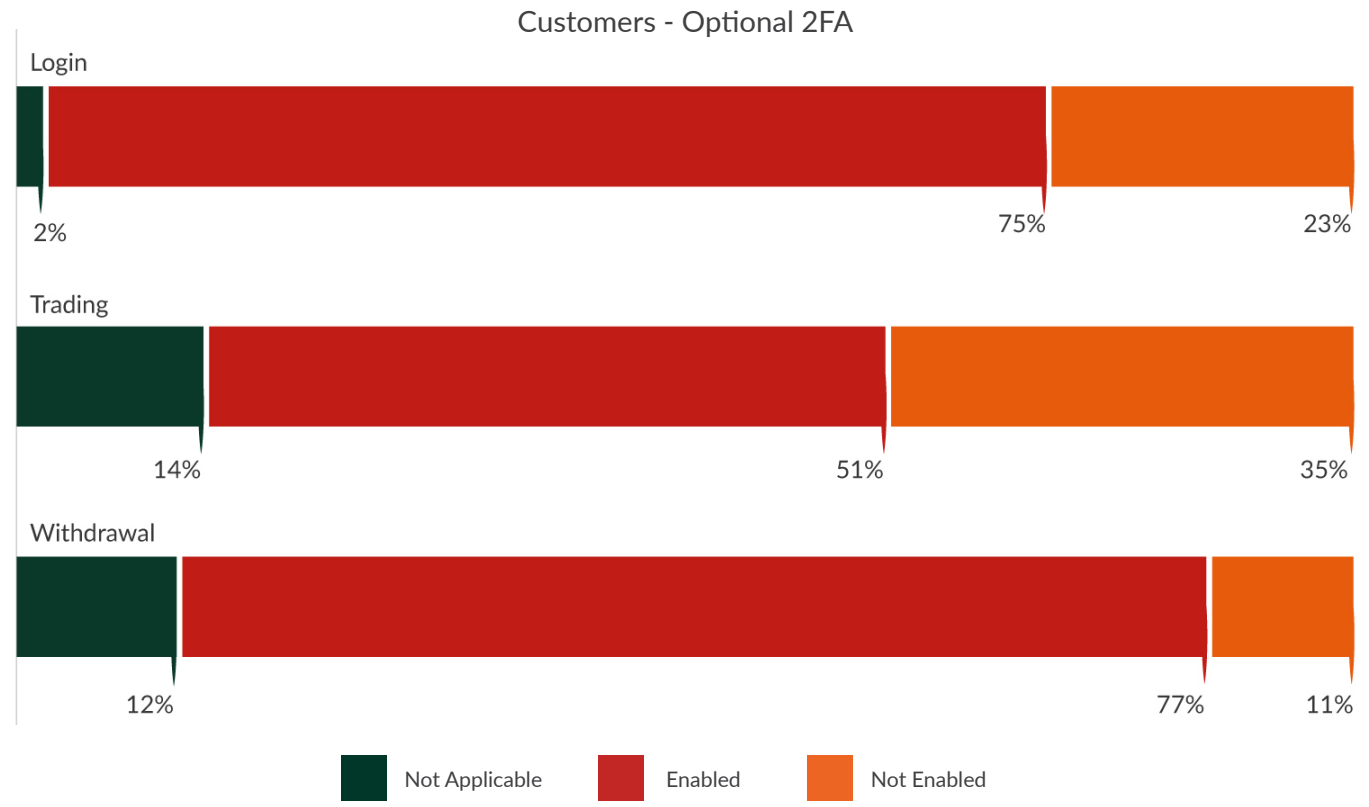
While the majority of small exchanges that use external security providers place trust in one to two providers, half of large exchanges make use of three or more external security providers (Figure 24). More than half of exchanges indicate that they have not come to rely more on external security providers over time.

## USE OF TWO-FACTOR AUTHENTICATION (2FA)

Multi-factor authentication is an access control method that grants access to a computer system only if the requester can supply multiple 'factors' (e.g., password and a unique one-time generated token).[9] The most widely used form in everyday life is two-factor authentication (2FA) which requires the user to provide two factors in order to identify himself. 75% of exchanges offer customers the option to enable 2FA for logging into their exchange account, and 77% offer users 2FA for withdrawing funds (Figure 25). Only 51% of exchanges provide optional 2FA for trading.

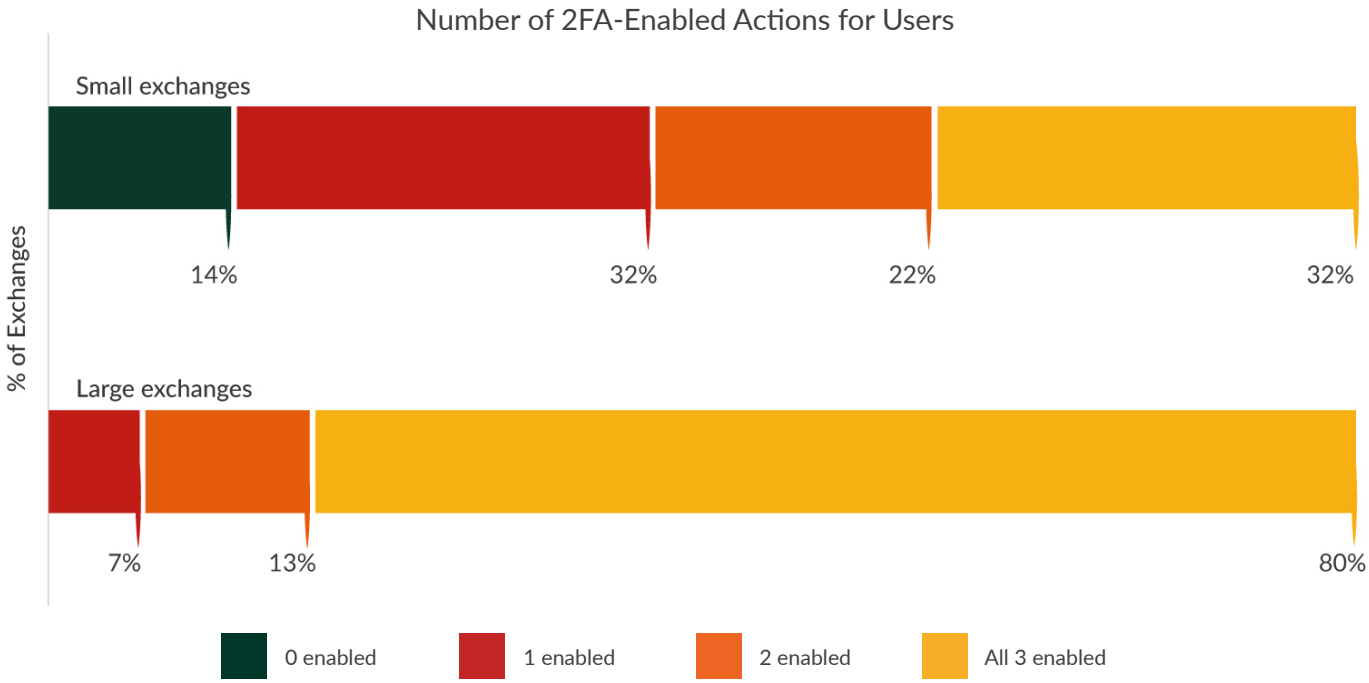
40% of exchanges that control users' private keys do not offer 2FA for trading, as they suppose enabling 2FA for login is enough to prevent an unauthorised person from gaining access to the exchange account features. It is important to note that 2FA is an optional security feature that most exchanges offer to their customers and encourage use, but that users are not required to activate 2FA. 48% of exchanges enable 2FA for all listed actions, but there are notable differences between small and large exchanges: 80% of large exchanges have 2FA enabled for all listed actions compared to 32% of small exchanges (Figure 26).

Figure 25: Majority of exchanges enable optional 2FA for customers for logging in and withdrawing funds




*Note: the 'not applicable' option has been chosen for a variety of reasons, that include exchanges that do not offer accounts and do not hold customer funds*

Figure 26: Large exchanges enable optional 2FA for nearly all customer actions




*Note: these refer to the customer actions listed in Figure 25*

## Figure 27: The majority of exchanges require employees to use 2FA for sensitive operations


*Note: some exchanges have chosen the 'not applicable' option for various reasons, including security for employees being classified, and private keys not being accessible to staff*

While the use of 2FA is mostly an optional feature offered to security-conscious customers, it is often required by exchanges for internal operations (Figure 27). In fact, 85% of exchanges have mandatory 2FA for at least one internal operation action: 80% require 2FA for administrator login, and 74% have mandatory use of 2FA for production access. 73% require 2FA for accessing private keys, which roughly matches the percentage of exchanges that do hold customer keys.

Some exchanges also indicate that they are using three-factor authentication (3FA) internally for access to all systems and require hardware devices such as YubiKeys or even hardware wallets as one factor. 82% of large exchanges and over 60% of small exchanges require the use of 2FA for all of the listed operational actions (Figure 28).

### SECURITY MEASURES

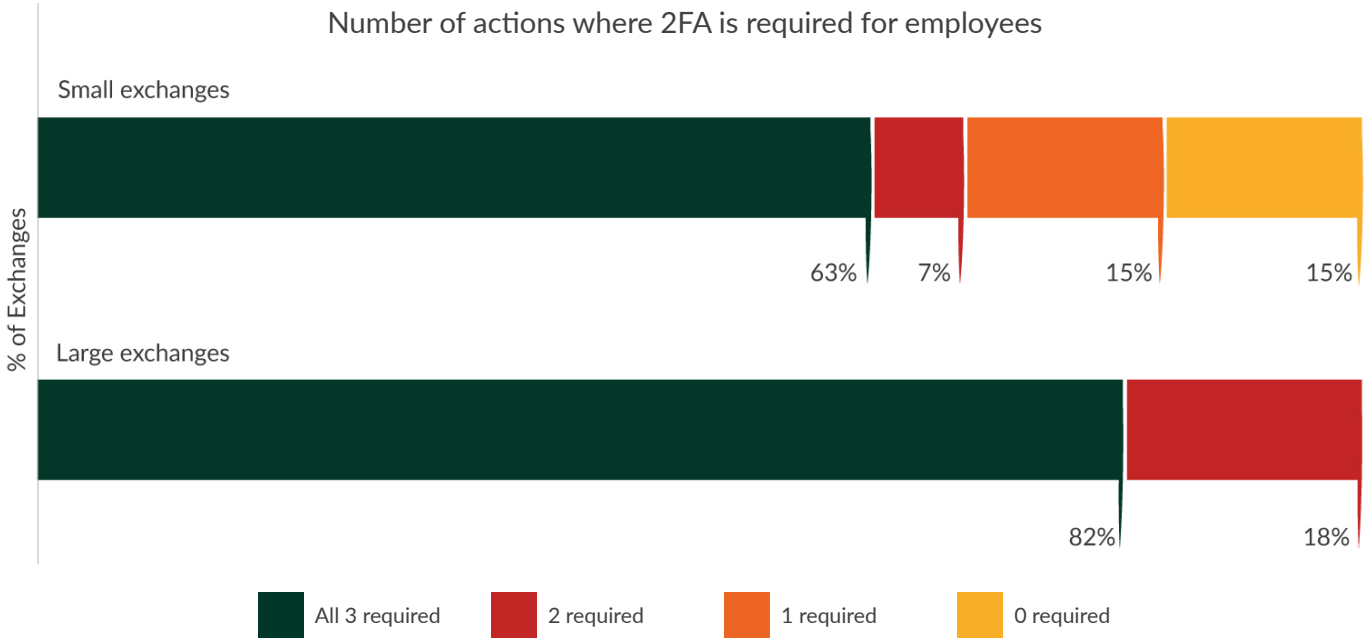
Exchanges use a variety of internal security measures to monitor production access and restrict access to sensitive information. However, large exchanges use them considerably more often than small exchanges (Figure 29).

91% of large exchanges and 83% of small exchanges use software to create a complete record of all internal processes and actions which allows them to quickly discover potential inconsistencies. The largest difference between small and large exchanges is observed regarding the use of special hardware dedicated to a single purpose (e.g., air-gapped device for cold storage of cryptocurrency funds), which are used by 91% of large exchanges compared to only 59% of small exchanges.

82% of large exchanges and 62% of small exchanges also use physical site location security systems or devices to monitor access to facilities. 73% of large exchanges use various types of 'consensus mechanisms' that require several employees to authorise a specific action (e.g., access to customer funds), as opposed to 55% of small exchanges. 64% of large exchanges and 38% of small exchanges use all four security measures.

85% of exchanges require that employees must be over a certain threshold of seniority within the company to get access to the production environment (Figure 30). Fingerprinting is only used by 15% of exchanges. Some exchanges also

Figure 28: 82% of large exchanges require 2FA for employees for all listed actions; differences between small exchanges can be observed




*Note: these refer to the employee actions listed in Figure 27*

Figure 29: Large exchanges use more internal security measures than small exchanges

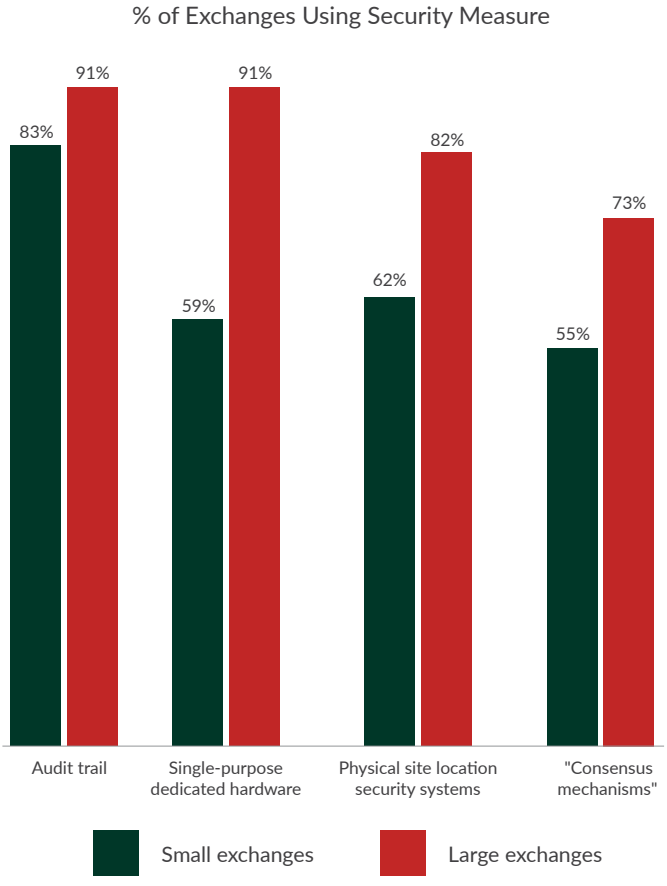



Figure 30: Measures used by exchanges to vet staff for production access

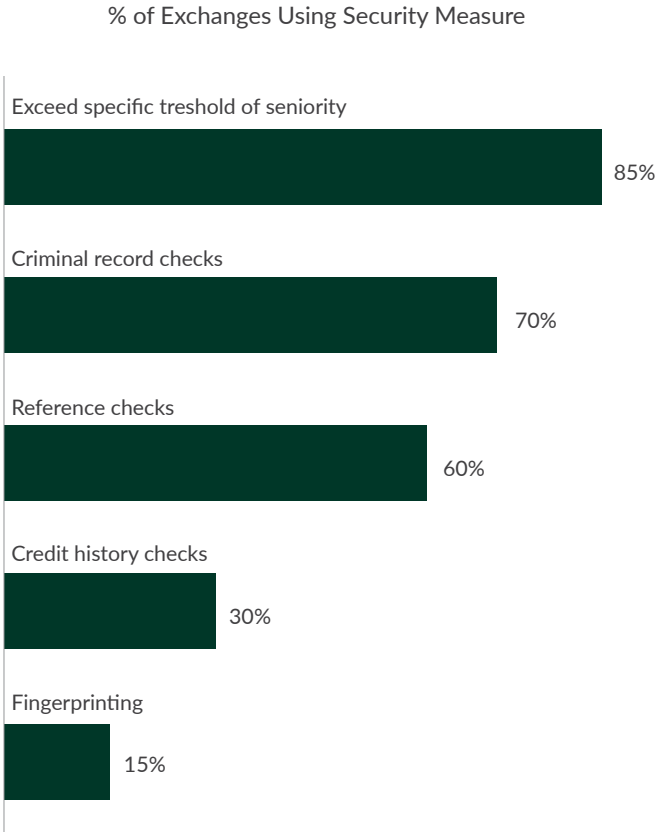
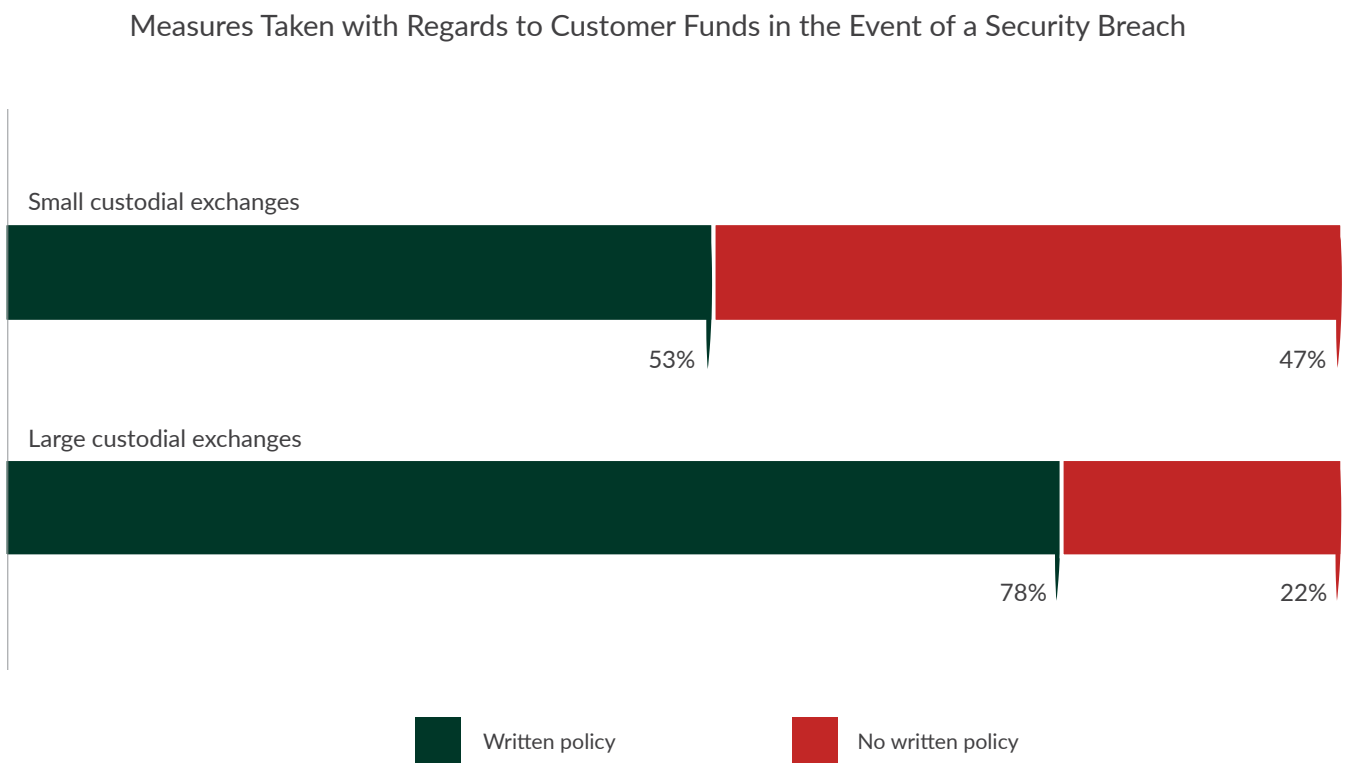


Figure 31: Nearly half of small exchanges acting as custodians do not have a written policy that outlines what happens to customer funds in the event of a security breach




commented that full credit history checks might constitute a breach of employee privacy and be difficult to defend before a tribunal, and also questioned whether such checks are e a good measure for deciding whether employees should be trusted with production access. Other exchanges indicated that personal relationships would play an important role as well. As for the internal security measures discussed above, large exchanges do make considerably more use of the referenced actions than small exchanges: 73% of large exchanges use three or more compared to 48% of small exchanges.

Only 53% of small exchanges that act as a custodian by controlling customer keys have a written policy that outlines what happens to customer funds in the event of a security breach that could lead to the loss of customer funds (Figure 31). In contrast, 78% of large custodial exchanges have such a written policy.

82% of large exchanges and 64% of small exchanges have a written policy on which employees and parties have access to sensitive information, such as private keys and user data (Figure 32). A major difference between small and large exchanges can be observed with regards to production access: only 63% of small exchanges have a written policy on who has access to the production environment compared to 92% of large exchanges.

Having the most sophisticated security measures in place does not necessarily prevent malicious actors from successfully breaking into the exchange, as the human element is often the weakest link in any security system. It is essential that staff are well trained and familiar with popular social engineering attacks. 79% of exchanges do provide security training programs to their staff to educate them on security issues (Figure 33). Some exchanges provide ongoing education and training (e.g., daily or weekly case studies about possible attack vectors) while others offer periodic training sessions and best security practices reminders. We do not observe a substantial difference between small and large exchanges with regards to staff training programs.

### KEY STORAGE

This section refers to the key management systems that exchanges use to secure both customer and exchange keys.

Figure 32: Do you have a written policy on the following actions?

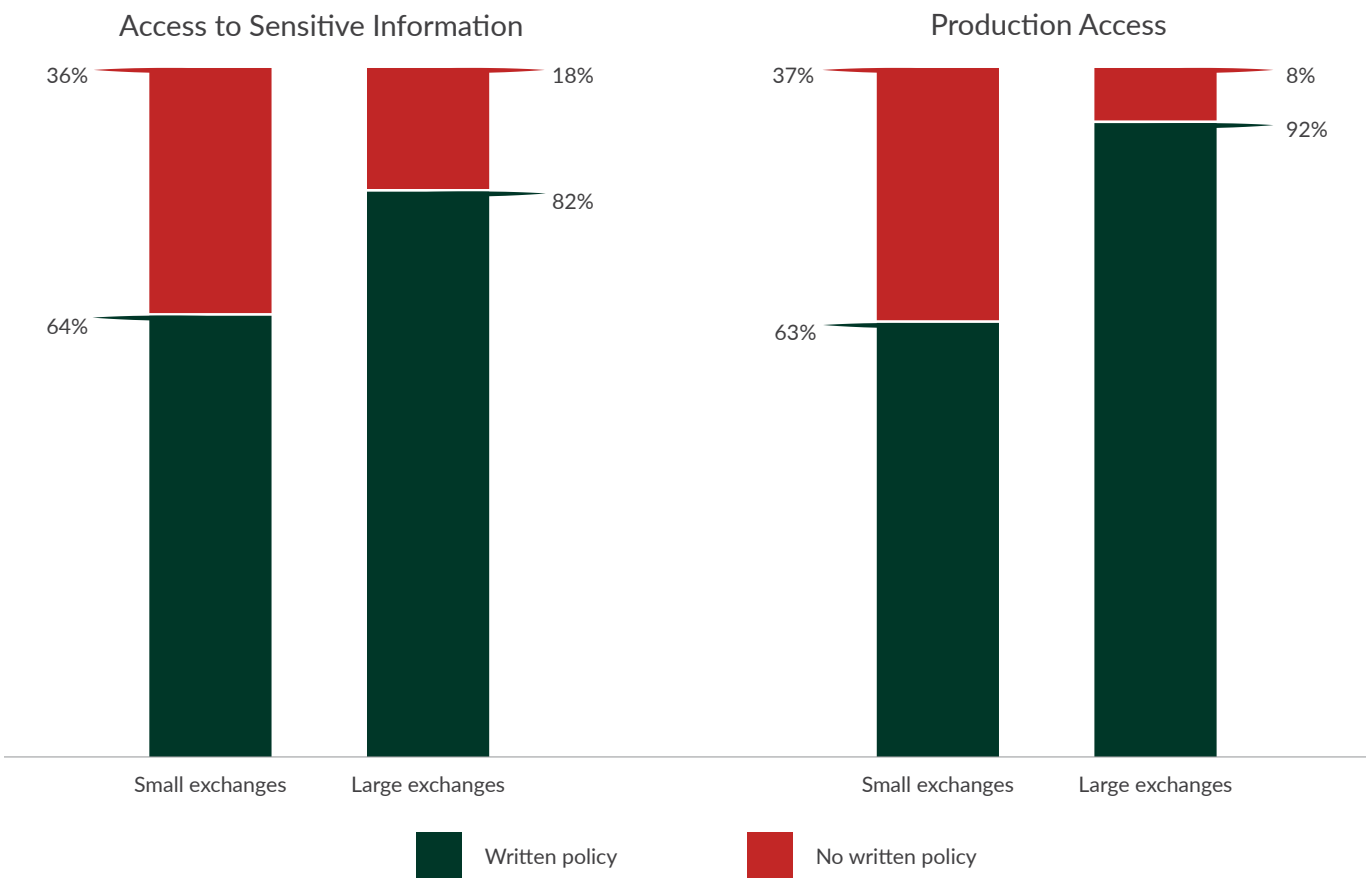
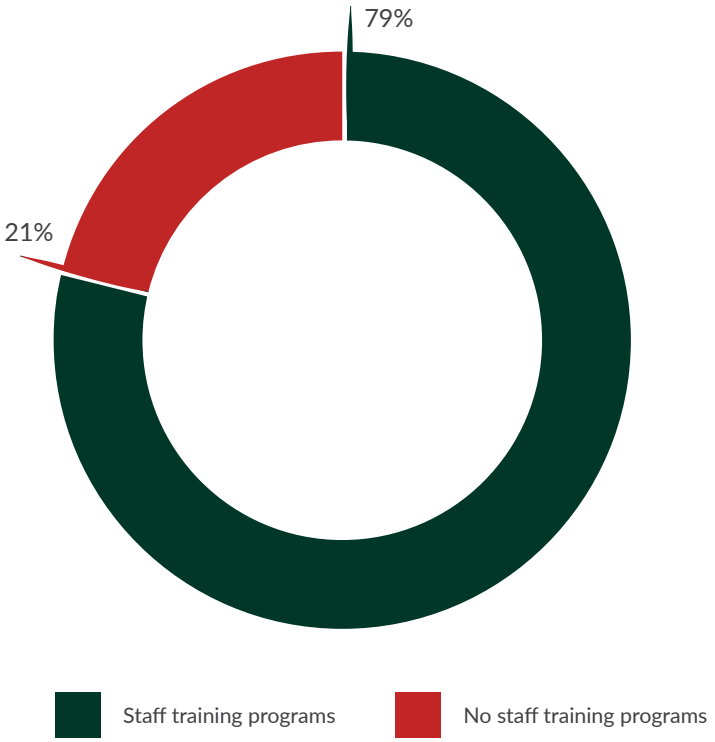
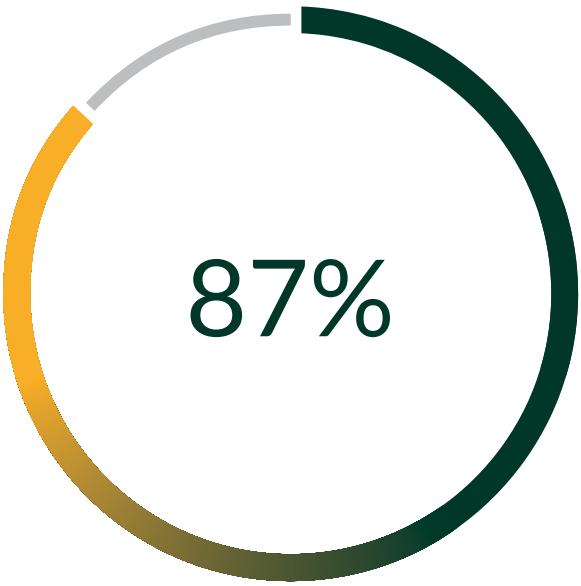


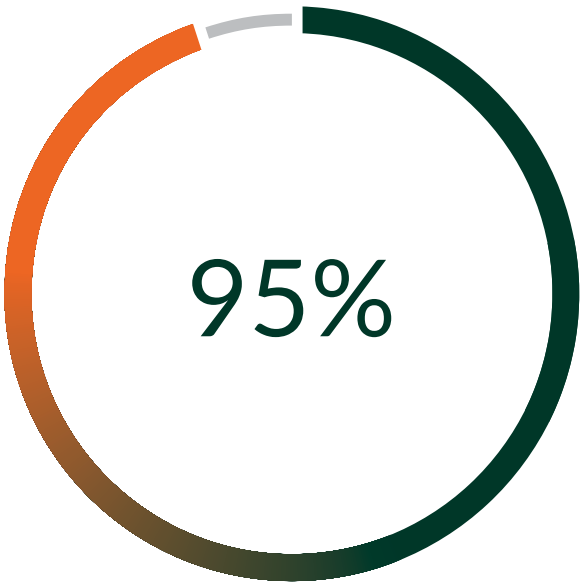

Figure 33: 21% of exchanges do not provide security training programs to their staff



Average % of Funds Held in Cold Storage




Median % of Funds Held in Cold Storage




**COLD STORAGE**

92% of exchanges indicate that they are using some type of cold storage system (i.e., generating and keeping keys offline) to secure a portion of both customer and their own funds. Only 8% are not using any type of cold storage system and instead keep funds in hot wallets that are online. These figures are approximately the same for both small and large exchanges.

## 92% of exchanges use some type of cold storage system

On average, exchanges keep 87% of total funds in cold storage (median corresponds to 95% of total funds). There is no significant difference between small and large exchanges with regards to the proportion of funds held in cold storage.

All large exchanges and 95% of small exchanges that use a cold storage system have their cold storage funds 'air-gapped', meaning that they reside on storage devices that are physically isolated from a network connection. All large exchanges have multiple cold storage locations, as opposed to 68% of small exchanges. 78% of large exchanges also use external parties as part of their cold storage system, compared to only 53% of small exchanges.

**MULTI-SIGNATURE AND PRIVATE KEY STORAGE**

Multi-signature is supported by 86% of production systems from large exchanges, but only by 76% of small exchanges. All exchanges that do not use cold storage systems have multi-signature support. 85% of large exchanges and 75% of small exchanges that have cold storage systems in place also have multi-signature support. Large exchanges that support multi-signature architectures also more often use external third-party multi-signature platforms than small exchanges (60% compared to 44%). While all large exchanges distribute keys of multi-signature wallets among multiple holders, 19% of small exchanges do not.

All large exchanges encrypt private keys when they are not in use, but 9% of small exchanges do not. 100% of large

Figure 34: Large exchanges appear to perform more frequent formal security audits than small exchanges

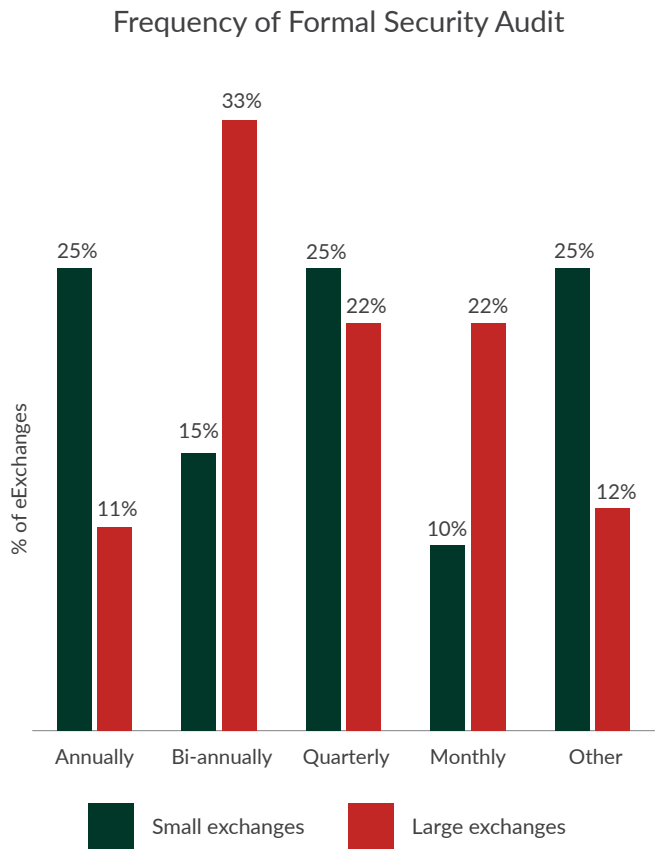
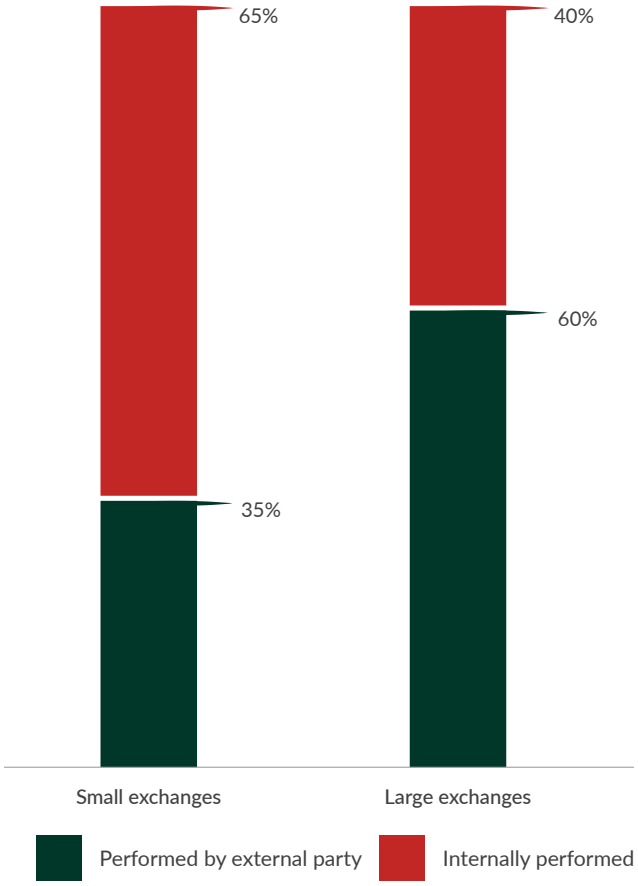



Figure 35: Large exchanges have more often external parties perform their formal security audits




exchanges and 91% of small exchanges store key back-ups in distinct geographical locations.

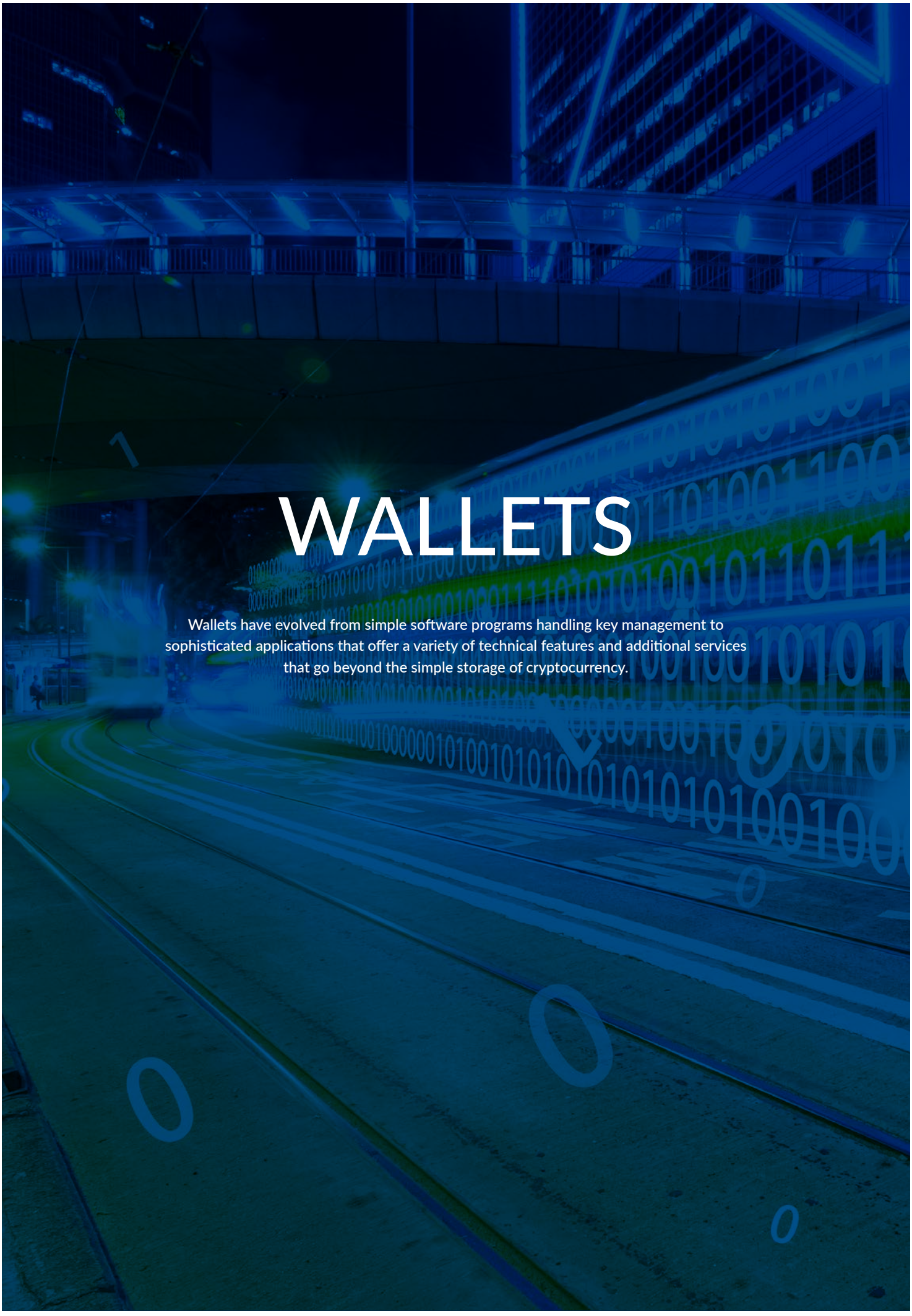
**FORMAL SECURITY AUDITS AND PROOF OF RESERVES**

We observe that the frequency of formal security audits conducted at exchanges surveyed varies considerably for both small and large exchanges (Figure 34). It appears that large exchanges perform formal security audits on a more regular basis than small exchanges. However, it is not always clear what exchanges define as 'formal' security audits, as many exchanges also reported that they would perform standard security checks and audits on an ongoing basis.

60% of large exchanges have their formal security audit performed by external parties, while 65% of small exchanges perform the audit internally (Figure 35). Findings also show that custodial exchanges are more likely to use external parties for their formal security audit. Two-thirds of large exchanges and over 90% of small exchanges do not publicly share information about their formal security audits (e.g., public announcement that it took place).

One third of custodial exchanges indicate that the formal security audit also encompasses a proof-of-reserve (mechanism to prove whether the exchange has sufficient funds; usually auditable by customers). Some exchanges commented that they would regularly have their reserves reviewed and certified by auditing firms, but that there would not be enough customer request for a formal proof-of-reserve to justify the costs and complexities of implementing such a system. Non-custodial exchanges do not perform a proof-of-reserve audit as they do not control customer funds.

All large exchanges that perform a proof-of-reserve audit indicate that an independent third-party was used, while only 17% of small exchanges use a third-party. However, many of the exchanges that do not use a third party for proof-of-reserves instead rely on providing cryptographic proof of reserves through various means that can be independently verified by the customer.



# WALLETS

Wallets have evolved from simple software programs handling key management to sophisticated applications that offer a variety of technical features and additional services that go beyond the simple storage of cryptocurrency.

# KEY FINDINGS

**Use and Features**

- The percentage of active wallets ranges across different providers from a low of 7.5% to a high of 30.9% of total wallets, but wallet providers define 'active' differently
- Between 5.8 million and 11.5 million wallets are estimated to be active today
- The lines between wallets and exchanges are increasingly blurred: 52% of wallets surveyed provide an integrated currency exchange feature, of which 80% offer national-to-cryptocurrency exchange services using one of three existing exchange models
- 81% of wallet providers are based in North America and Europe, but only 61% of wallet users are based in these two regions
- 73% of wallets do not control private keys (meaning they do not have access to user funds); 12% of wallets let the user decide whether to have sole control over private keys
- 32% of wallets are closed source; all custodial wallets (wallet provider holds private keys) are as well
- Mobile wallet apps are the most widely offered format, followed by desktop and web
- 39% of wallets already offer multi-cryptocurrency support, and nearly one third of those currently without multi-cryptocurrency support have this feature on their roadmap
- Only 42% of small wallet providers offer multi-signature support compared to 86% of large wallet providers

**Compliance and Operations**

- 24% of incorporated wallets hold a formal government license; all of them are wallets that offer national-to-cryptocurrency exchange services
- 75% of wallets providing national-to-cryptocurrency exchange services using the centralised exchange model hold a formal government license
- Large wallets providing centralised national-to-cryptocurrency exchange services spend over 4x more on compliance than small wallet providers and have more than 4x the headcount associated with compliance
- All wallets providing centralised national-to-cryptocurrency exchange services perform KYC/AML checks; the preferred method is internal checks
- Average IT security headcount for wallet providers amounts to 37% of total employees, and average IT security cost constitute 35% of total budget, both of which represent highest percentage spent on security of any sector in this study; considerable differences on these measures are observed between wallets providing national-to-cryptocurrency exchange services and those that do not, as well as between custodial and non-custodial wallets

Figure 36: 81% of wallet providers are based in North America and Europe

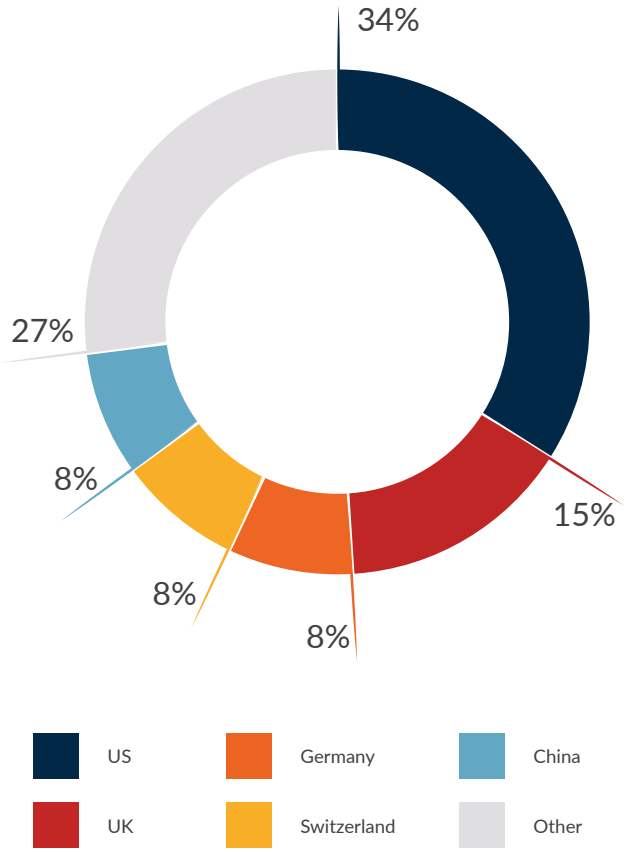
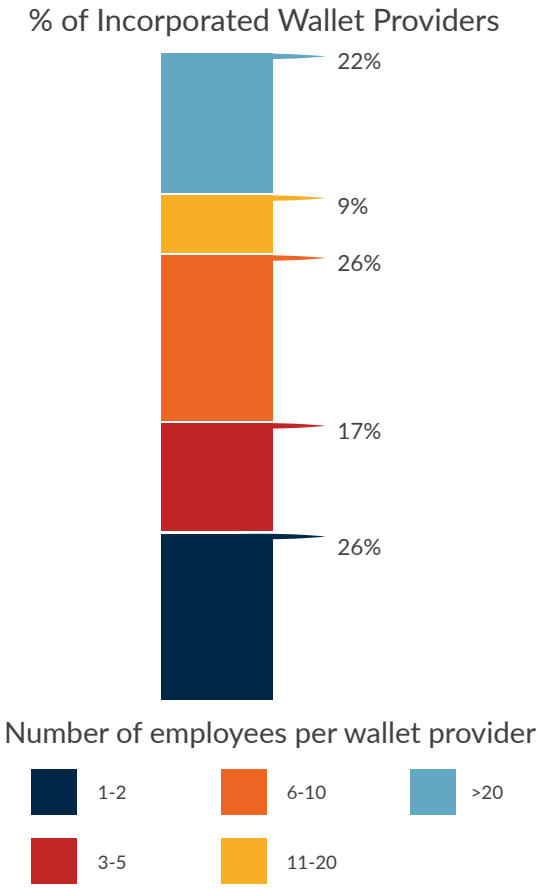



Figure 37: 69% of incorporated wallet providers have less than 11 employees




# INTRODUCTION AND LANDSCAPE

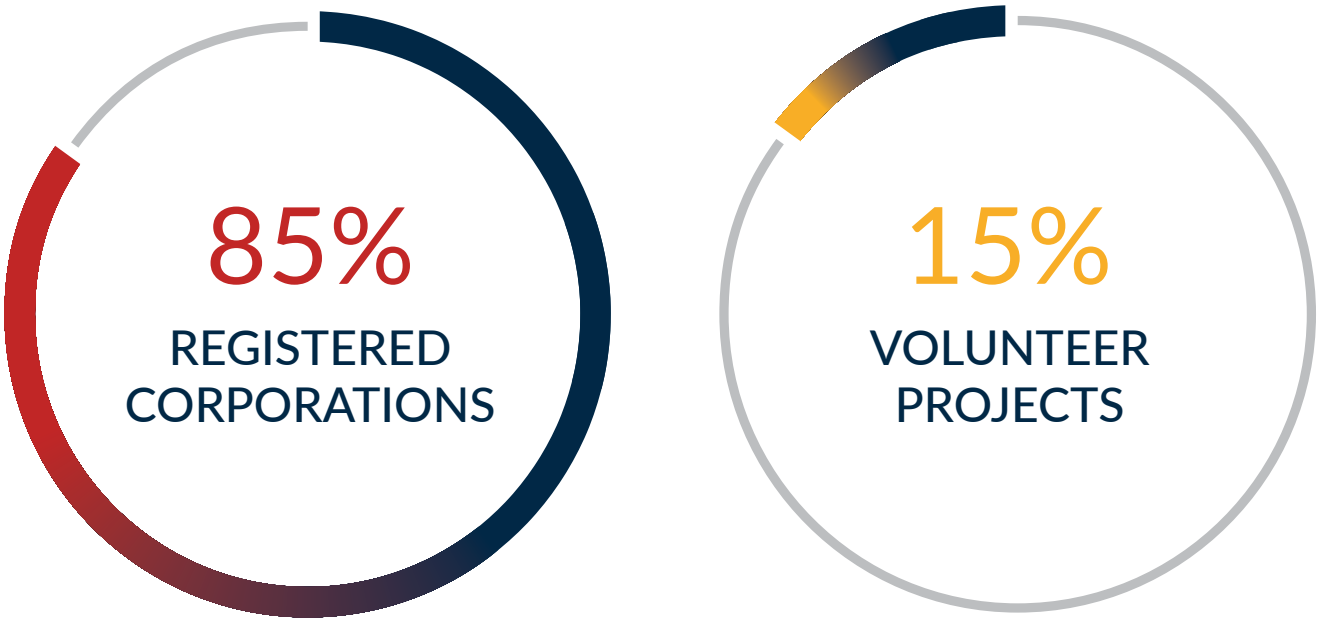
**DEFINITION**

A wallet generally is a software program that is used to securely store, send and receive cryptocurrencies through the management of private and public cryptographic keys.[1] Wallets also provide a user interface to track the balance of cryptocurrency holdings and automate certain functions, such as estimating what fee to pay to achieve a desired transaction confirmation time.

**LANDSCAPE**

Each cryptocurrency has a reference implementation that includes basic wallet functionality (e.g., Bitcoin Core for Bitcoin, Mist browser for Ethereum). However, for a variety of reasons the reference implementation wallet is simply not practical for many users.[2] As a result, a multitude of wallet providers have emerged in recent years to facilitate the storage of cryptocurrencies and make wallets easier to use. These wallets range from open-source projects run by volunteer developers to ones created by venture capital-backed registered corporations.

## Majority of Wallets are Provided by Registered Corporations




The following figures are based on a dataset of 26 wallets that participated in our wallet survey. We define a wallet provider as any volunteer project or company that provides a stand-alone wallet that anyone can use. The wallet functionality is clearly separated from other commercial offerings and explicitly branded as such. Based on the total number of wallet providers meeting this definition, we estimate that the sample in this study represents over 90% of the total cryptocurrency wallet sector.

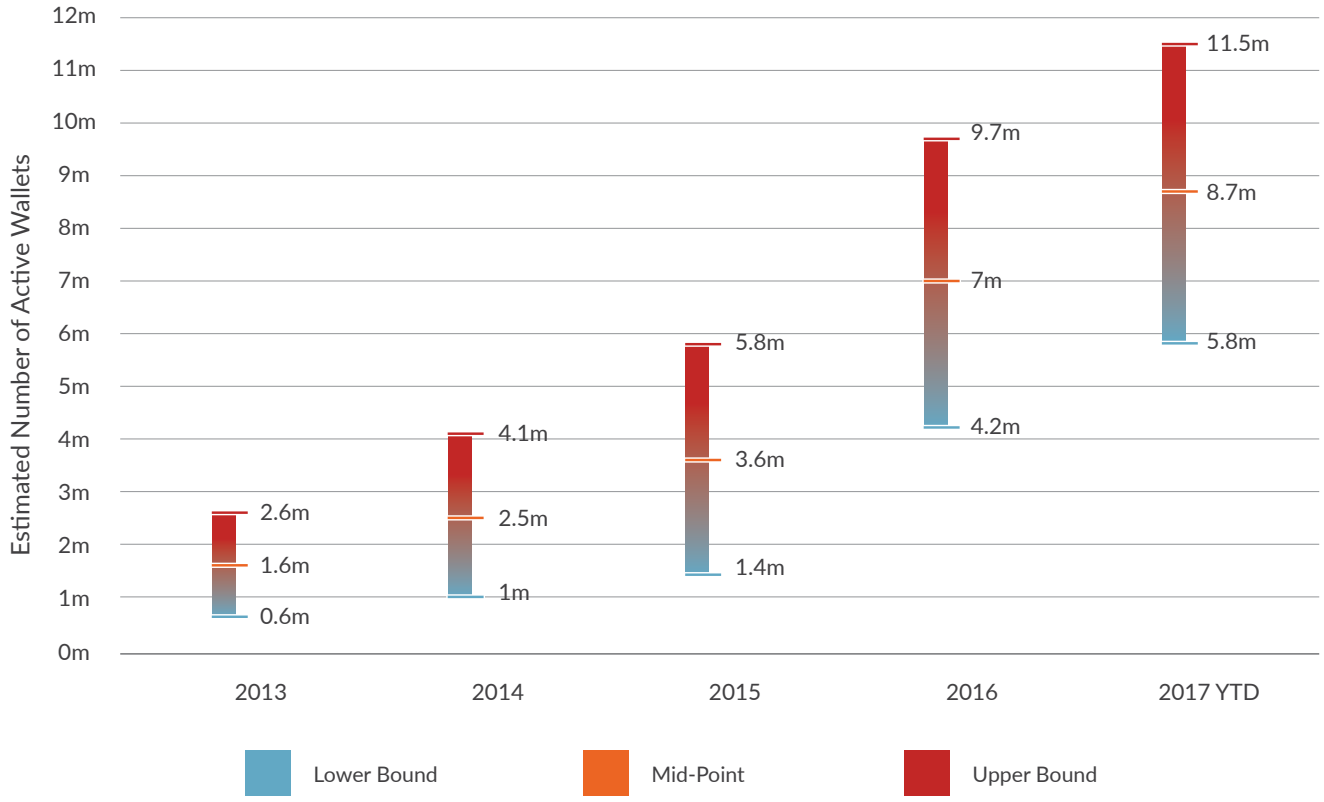
Almost half of all wallet providers are located in the United States and the United Kingdom (Figure 36). If we break down origin by world region, Europe is leading with 42% of wallet providers, followed by North America with 39% and Asia-Pacific with 19%.

Registered corporations with limited liability represent 85% of wallet providers, and 15% are open-source/volunteer projects. For the rest of this section, we will refer to wallets provided by registered corporations as 'incorporated wallets'.

There are a total 418 full-time employees working at incorporated wallets, with an average of 19 employees per wallet provider.[3] However, more than a quarter of incorporated wallet providers have less than three employees, and 69% have less than 11 full-time employees, which suggests that the average wallet provider is a relatively small company (Figure 37). Only 22% of surveyed wallets have more than 20 full-time employees. It should be noted that some wallet providers are also active in other cryptocurrency industry sectors and that the exact number of employees working full-time on the wallet service cannot be established.

> Incorporated wallets employ 418 people, with an average of 19 employees per wallet provider

Figure 38: The current number of estimated active wallets ranges between 5.8 million and 11.5 million




*Note: no wallet data available for some wallet providers prior to 2016*

# USERS

Data obtained from study participants suggests that the number of active wallets ranges from 7.5% to 30.9% of the total number of wallets

### NUMBER OF WALLETS

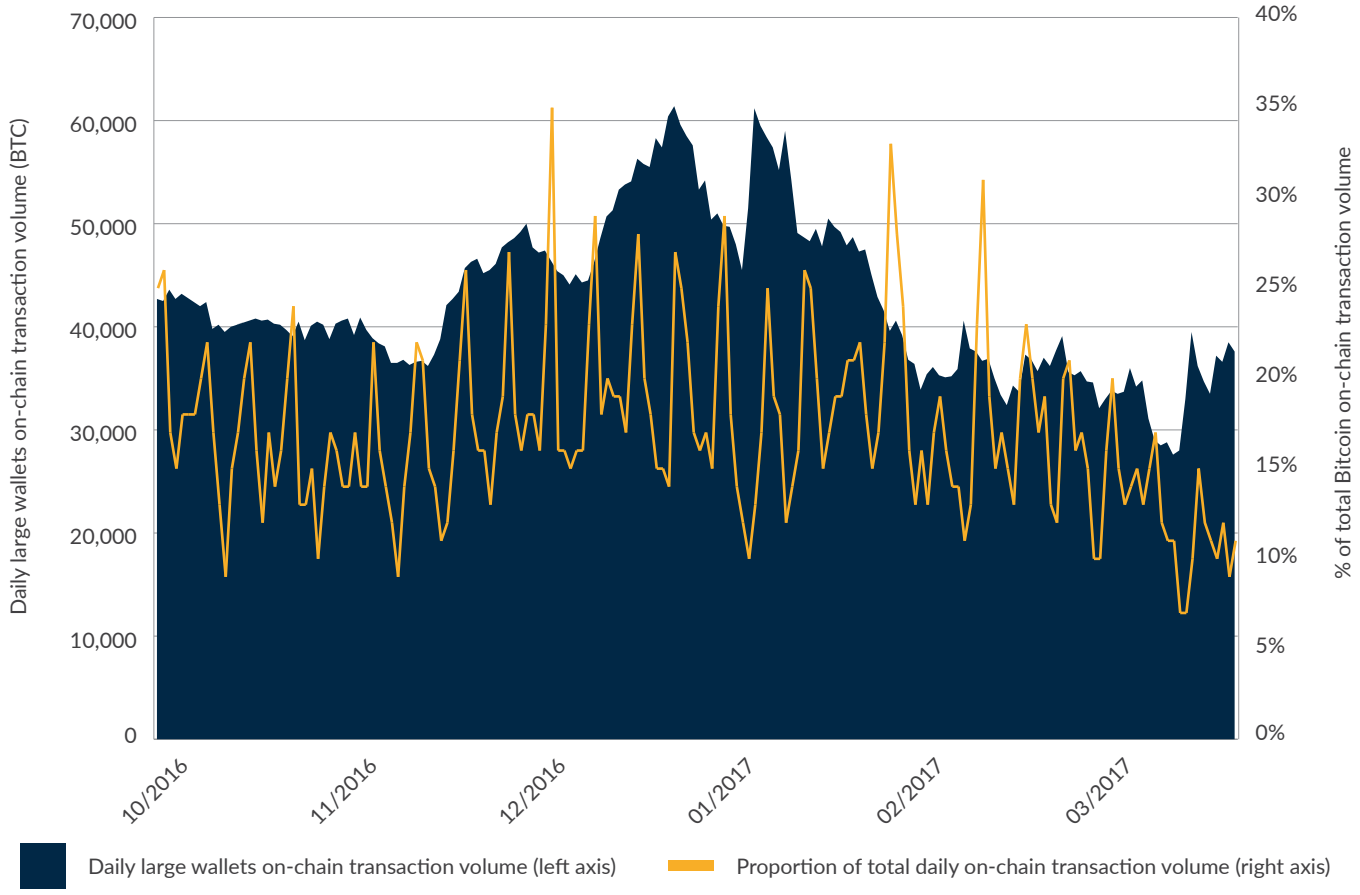
The total number of wallets can be estimated using data collected from study participants as well as including the number of software downloads of major wallet providers and Bitcoin's reference implementation. It is estimated that the total number of wallets has increased more than 4x from 8.2 million in 2013 to nearly 35 million in 2016.

We used the conservative assumption that one software download is the equivalent of one wallet created, although in theory a potentially infinite number of wallets could be created from a single software download. No data is available for download figures for some open-source wallets, and so these figures can be viewed as a 'lower bound'. As some of the wallets also offer multi-cryptocurrency support, these figures do also include users storing cryptocurrencies other than bitcoin.

### NUMBER OF ACTIVE WALLETS

Publicly reported cumulative wallet figures generally do not reflect whether these wallets are *active* or not. Data obtained from study participants suggests that the number of active wallets ranges from 7.5% to 30.9% of the total number of wallets.

Figure 39: Daily on-chain transactions performed by users of large wallets generally range between 10% and 25% of total bitcoin on-chain transaction volume, but are trending down slightly of late




However, the term 'active' is ambiguous as wallet providers use different definitions for determining active wallets: some consider active wallets to be wallets owned by users that *login* in at least once a week or less frequently, while others define active wallets as wallets that *transact* at least once a week or less frequently. Based on these definitions, long-term holders who do not frequently transact are thus usually considered 'inactive', although many consider long-term inactive holders of cryptocurrency as still playing an important role in the cryptocurrency ecosystem.

## Wallet providers use different methods for reporting total number of wallets and determining 'active' wallets

A rough estimate of the total number of active wallets can be provided by applying the observed range (7.5%-30.9%) to the estimated number of total wallets. The number of active wallets is thus estimated to have increased from between 0.6 million and 2.6 million in 2013 to currently between 5.8 million and 11.5 million in 2017 (Figure 38).[4]

It is important to recall that these figures do not necessarily reflect the total number of active wallet *users*. Estimating the total number of unique individuals using a cryptocurrency wallet poses significant challenges as there is no limit on the number of wallets any one individual can create, and the number of additional wallets held by an individual is unknown to any particular wallet provider. For these reasons, the actual number of cryptocurrency wallet users (active and long-term holders) is likely significantly below the total number of wallets in existence.

### ON-CHAIN WALLET TRANSACTION VOLUMES

The daily transaction volume performed by users of large incorporated wallets on the bitcoin network has increased from an average 17% of total network volume in October 2016 to an average of 20% in December 2016 (Figure 39).[5] Wallet share of transaction volume has recently decreased again and currently amounts to approximately 12%-15% of total transaction volume. It can be observed that the wallet share of total daily on-chain transactions increases during the weekends, when total transaction volumes are generally lower.

Figure 40: Greatest number of wallet users are based in North America and Europe

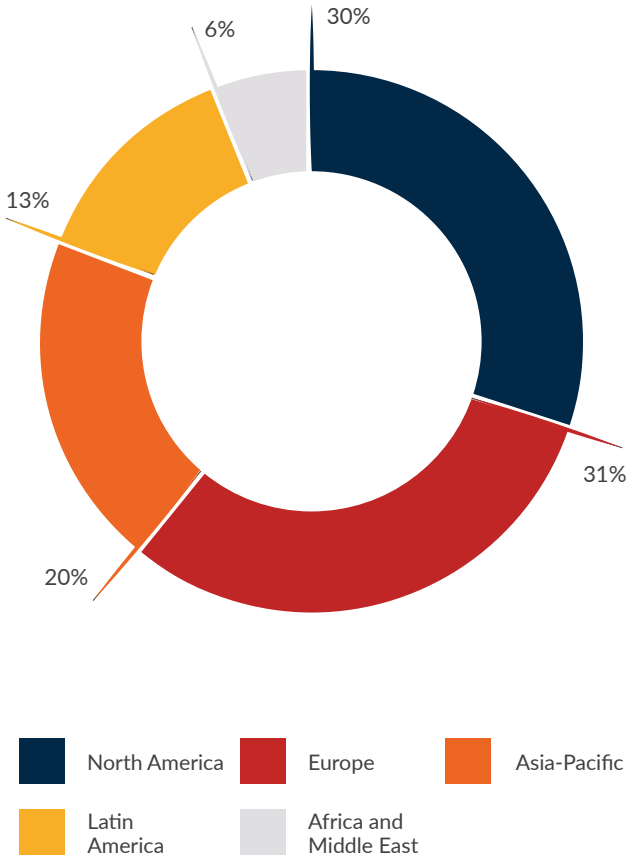
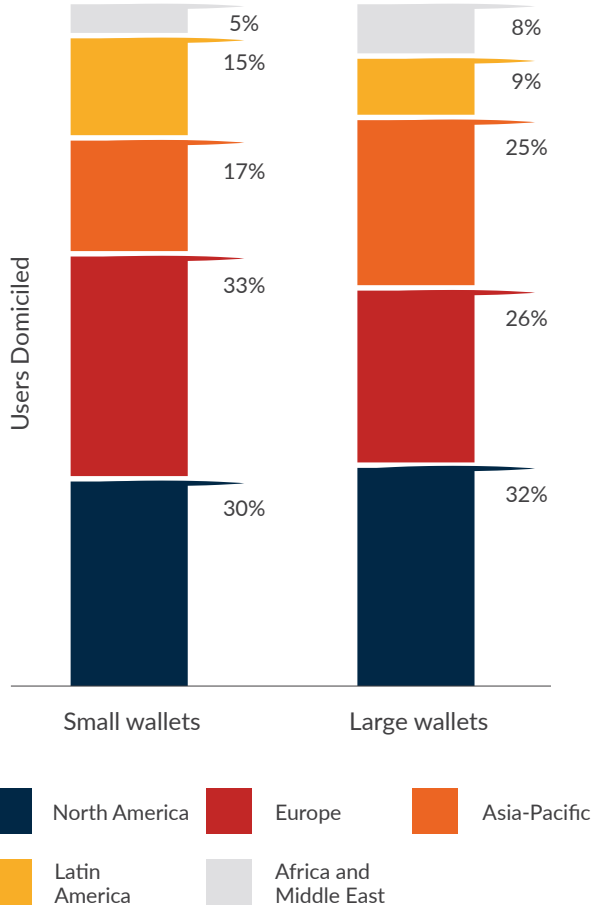



Figure 41: Small differences in user share by region can be observed between small and large wallet providers




**GEOGRAPHY**

Based on user data obtained from incorporated wallets, we can make a rough estimate of the origins of wallet users by segmenting the data by world region. 61% of wallet users are domiciled in North America and Europe, while 20% of users come from Asia-Pacific (Figure 40). Latin America is the next largest region, followed by Africa and the Middle East which lag behind. The relatively small proportion of wallet users for some regions may stem from the fact that there are still a considerable number of people in certain countries (e.g., China) that use exchange accounts as their *de facto* wallet to store cryptocurrency.

> 81% of wallet providers are based in North America and Europe, but only 61% of wallet users are based in these two regions

We observe some minor differences when segmenting between small and large wallets.[6] Users from Asia-Pacific as well as Africa and the Middle East tend to use large wallet providers, whereas Latin American and European users seem to prefer small wallet providers (Figure 41). The user share of North American wallet users is approximately equal for both small and large wallets.

Similarly, we can also analyse if there are divergences between the location of wallet providers and their users. In general, the customer base of incorporated wallet providers is diversified and includes users from all world regions. However, it appears that in some markets, there is a relationship between the location of wallet providers and their customer base (Figure 42). European and North American users seem to prefer using local wallets, as they constitute the largest share of users from wallet providers located in these regions. Somewhat surprisingly, Latin American users appear to prefer European and Asian-Pacific wallets over North American wallets.

Figure 42: European and North American wallet users seem to prefer using local wallets

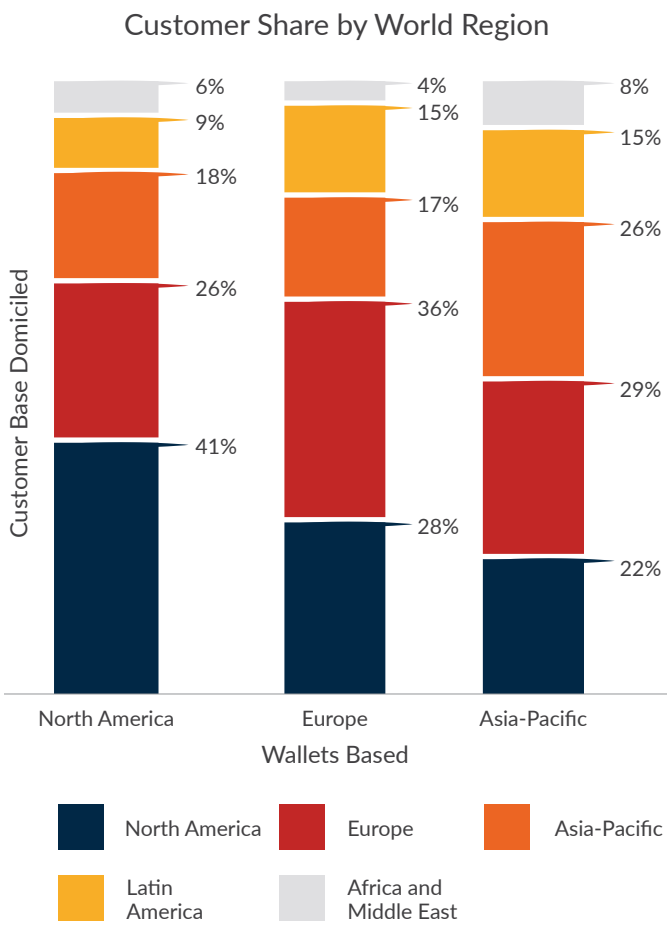
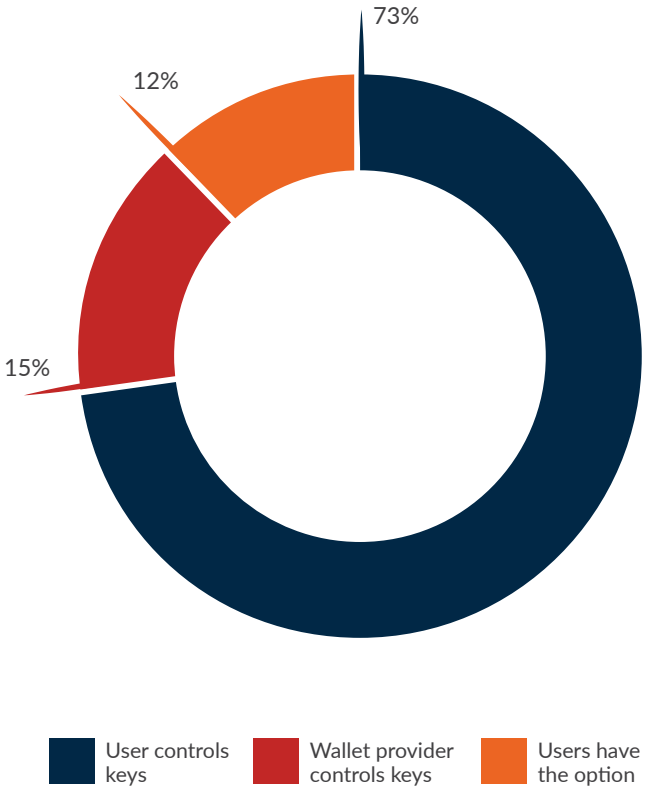



Figure 43: Over 70% of wallet providers do not control user funds




# WALLET TYPES

In contrast with exchanges, the majority of wallets do not control access to user keys: 73% of surveyed wallets do not take custody of user funds but let the user control private keys (Figure 43). Moreover, 12% of wallets offer users the possibility to choose whether they want to control their private keys themselves – at the risk of losing them and not being able to recover their funds – or to let the wallet service provider handle key management. Only 15% of wallets take full custody of user funds. We do not observe major differences between small and large wallet providers.

## All custodial wallets surveyed are closed source

32% of surveyed wallets are 'closed source', which means the wallet source code is not freely available for outside developers to inspect for vulnerabilities. All custodial wallets (services that control private keys and have access to user funds) are closed source. An interesting observation is that 11% of self-hosted wallets (individual controls private keys, wallet provider does not have access to user funds) are closed source as well. These figures are approximately the same for small and large wallet providers.

Over 30% of Wallets are Closed Source

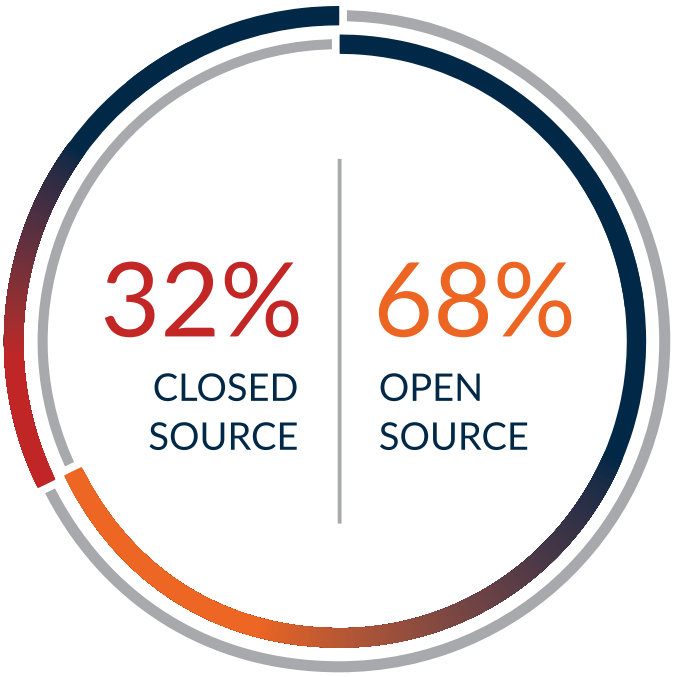
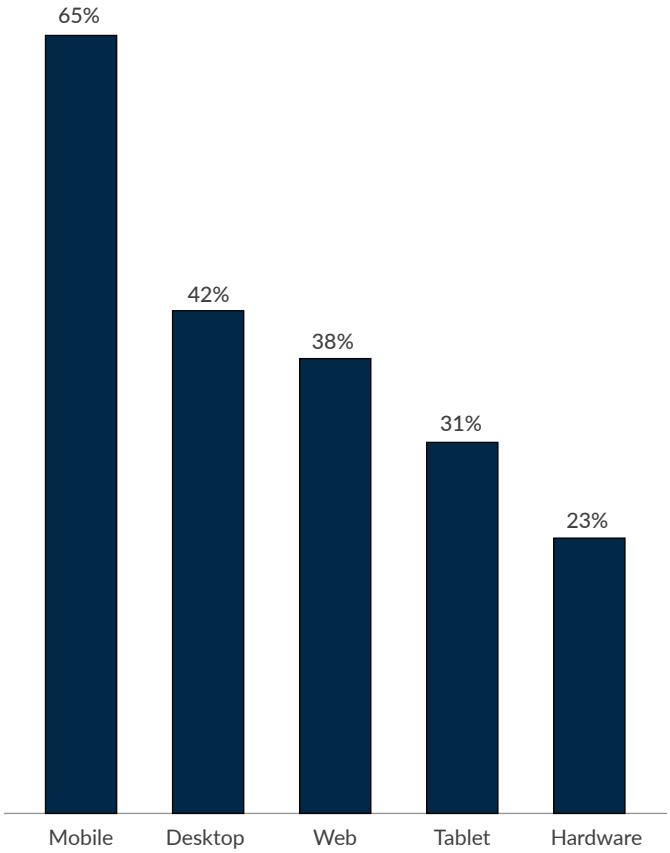



Figure 44: Mobile wallet app is the most widely offered wallet format

% of wallet providers supporting the listed formats




Most wallet services support multiple formats (e.g., web, mobile, hardware) and allow users to easily switch between different devices, and most wallets support different operating systems. The most common wallet format offered is a smartphone wallet application (Figure 44). Many find smartphone wallet apps to be one of the most convenient ways to use cryptocurrencies on a daily basis as the wallet is readily available and easily transportable.

An increasing number of companies specialise in the development of hardware wallets, which store private keys in a secure hardware device. This development coincides with the observed increase in the value of cryptocurrencies and the greater incentives for criminals to target cryptocurrency holders.

**SUPPORTED CRYPTOCURRENCIES**

39% of wallets providers offer the ability for users to store more than one cryptocurrency in the same wallet, and 19% allow users to store more than three cryptocurrencies. The vast majority of wallets support bitcoin (Figure 45). Litecoin, ether and dogecoin are the next three most commonly supported cryptocurrencies.

Wallets continue to support more and more different cryptocurrencies: 31% of wallets that currently only support storing a single cryptocurrency indicate that their current roadmap includes offering support for more cryptocurrencies. 78% of multi-cryptocurrency wallets plan to also add more cryptocurrencies to their current offering.

> 39% of wallets already offer multi-cryptocurrency support, and 31% of wallets that currently do not offer multi-cryptocurrency support have this feature on their roadmap

Figure 45: Litecoin, ether and dogecoin are the most widely supported cryptocurrencies after bitcoin

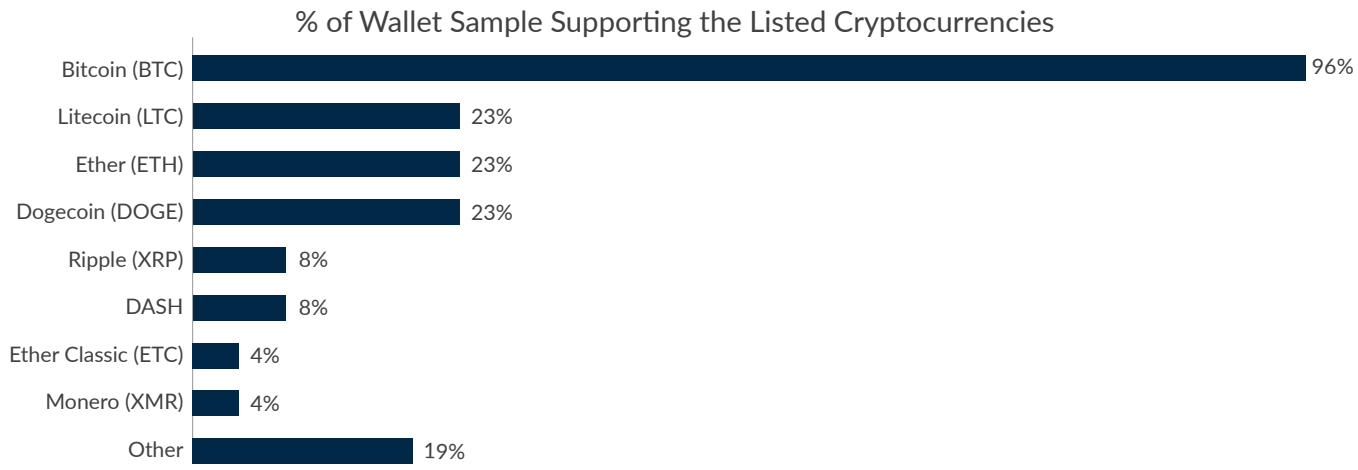
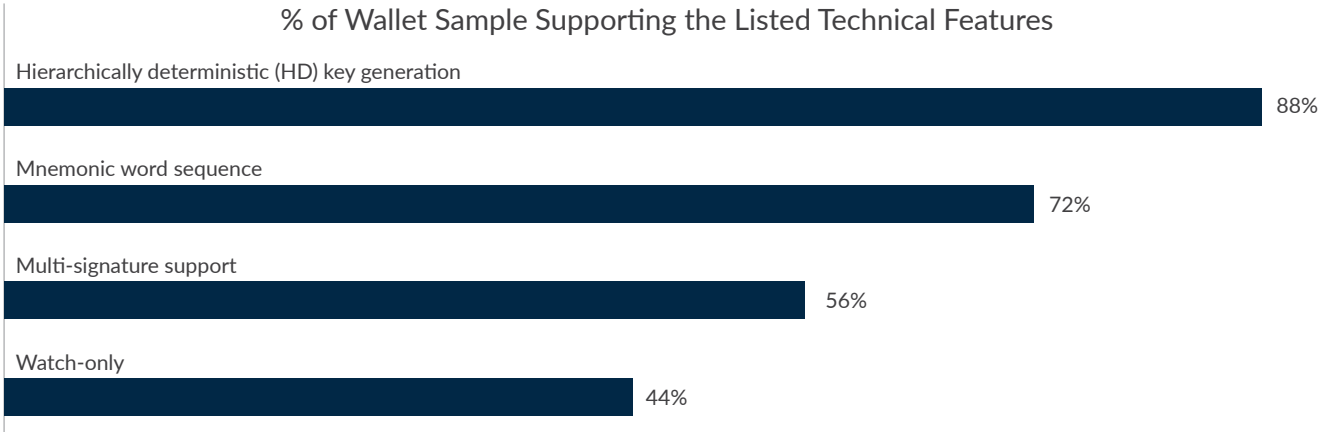



Figure 46: Majority of wallets support mechanisms to easily back up and migrate keys



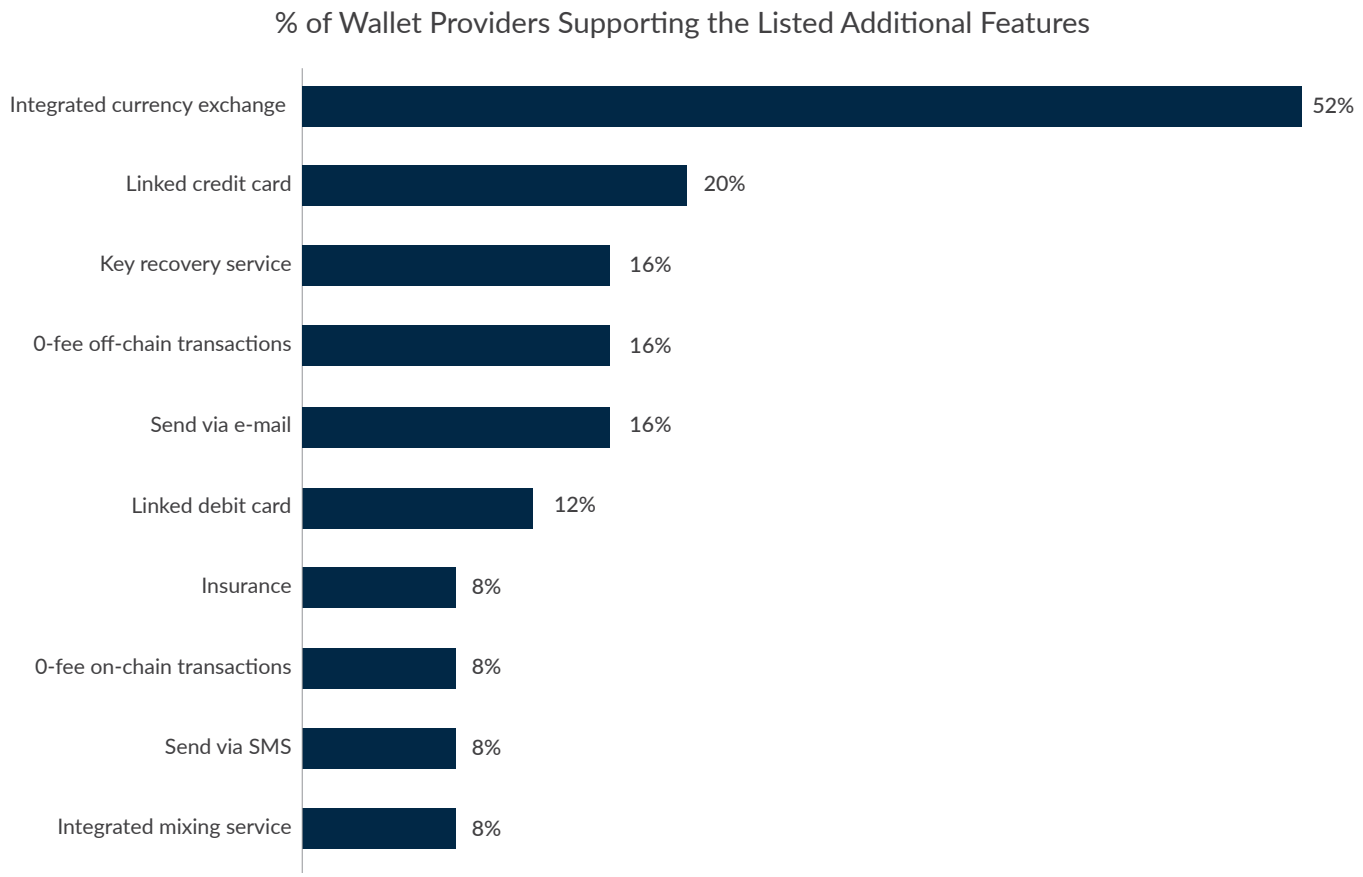

# WALLET FEATURES

### TECHNICAL FEATURES

Wallets have evolved from simple software programs handling key management to sophisticated applications that offer a variety of features. Significant innovation at both the protocol level and amongst wallet providers has led to the emergence of several technical standards that are considered state-of-the-art, such as multi-signature.[7] While 56% of wallets offer multi-signature support (Figure 46), there are notable differences between small and large wallets: only 42% of small wallet providers offer multi-signature support compared to 86% of large wallet providers.

While 79% of smaller wallets and all large wallets support hierarchically deterministic (HD) key generation, only 57% of large incorporated wallets have implemented mnemonic word sequences to date.[8] This may be due to custodial wallet services that store user keys on their servers and do not therefore offer a passphrase for backup.

Figure 47: More than half of surveyed wallet providers offer integrated currency exchange services




**ADDITIONAL FEATURES**

56% of all wallet providers offer additional features and services that go beyond the basic storage of cryptocurrencies. All of the wallets offering additional features are incorporated wallets.

> 56% of wallets offer additional features and services that go beyond the basic storage of cryptocurrencies

The most popular additional feature is an integrated currency exchange service that lets users and customers conveniently exchange cryptocurrencies from the same wallet interface. 52% of all wallets provide an integrated currency exchange service, supporting our observation that the distinction between wallets and exchanges are increasingly blurred (Figure 47). 55% of wallet providers have also stated that they have plans to expand their services and add more features in the near future.

It can be observed that already very few wallets (8%) offer 0-fee on-chain transactions to their users, and if the recent spike observed in transaction fees persists we expect that number to decline even more.

Again, we observe differences between the features offered by small and large companies: 86% of large wallets provide integrated currency exchange services compared to only 39% of small wallets. Similarly, additional financial services, such as linking a debit and a credit card to the wallet account, are more often provided by large companies.

**INTEGRATED CURRENCY EXCHANGE SERVICES**

In general, there are three different models used by wallets to provide currency exchange services (Table 5).

23% of all incorporated wallets offering currency exchange services provide a built-in P2P exchange/marketplace, while 31% use the centralised currency exchange model (Figure 48). 46% have integrated a third-party exchange within the wallet interface to provide currency exchange services to users.

## Table 5: Taxonomy of currency exchange models used by wallet providers

| Exchange Model | Description |
|---|---|
| Centralised exchange/ brokerage service | Traditional model that implies a central exchange operator taking deposits and offering a price for the purchase and sale of currencies. The central party, in this case the wallet provider, directly handles currency exchange by acting as the counterparty to users wishing to acquire and/or sell cryptocurrencies. |
| Integrated third-party exchange | Model that sees the wallet provider integrating the services of an independent exchange within the wallet interface so that users can purchase and sell cryptocurrencies through a partnership with a third-party exchange. |
| P2P exchange/ marketplace | Emerging model that enables users to make currency exchanges between themselves without having to use a centralised exchange operator. The wallet interface acts as a secure environment for a decentralised marketplace that connects buyers to sellers. The wallet provider does not act as a central counterparty, but only provides the infrastructure for the P2P exchange. Some wallets offer to hold funds in escrow during the trade, while others offer a built-in trustless escrow function based on the multi-signature feature. This means that in the former case, the 'P2P' element refers only to the marketplace aspect (users trading with each other), while the latter constitutes a truly decentralised exchange that lets users in control of their funds during the entire trade process. |

## Figure 48: Nearly half of wallets providing currency exchange services integrate a third-party exchange

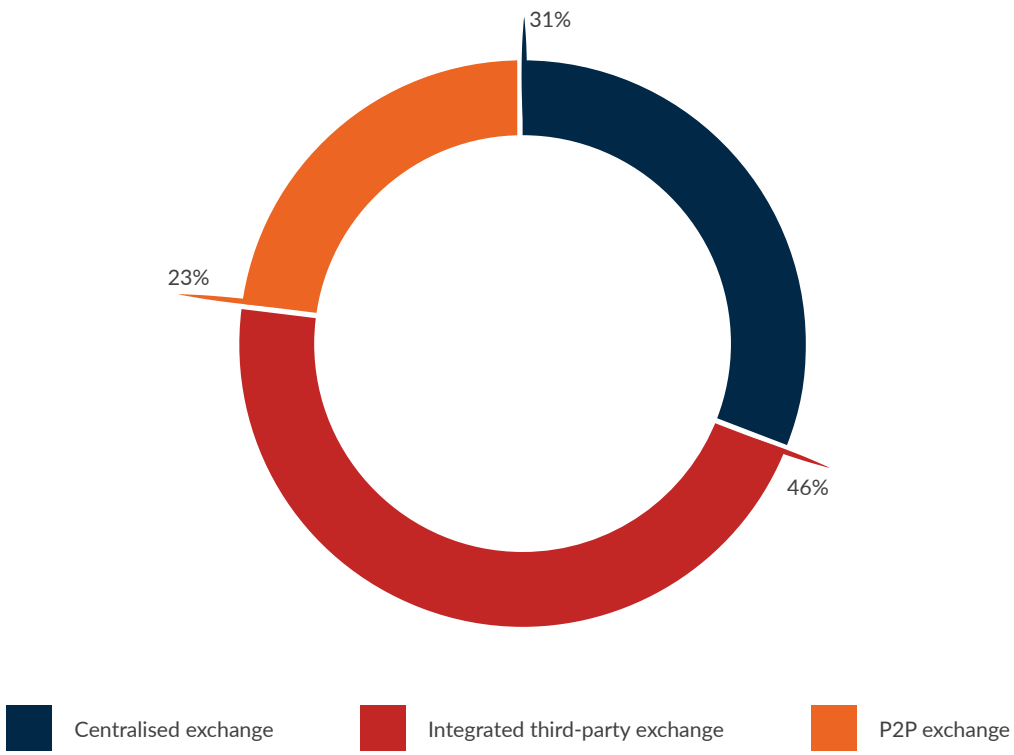
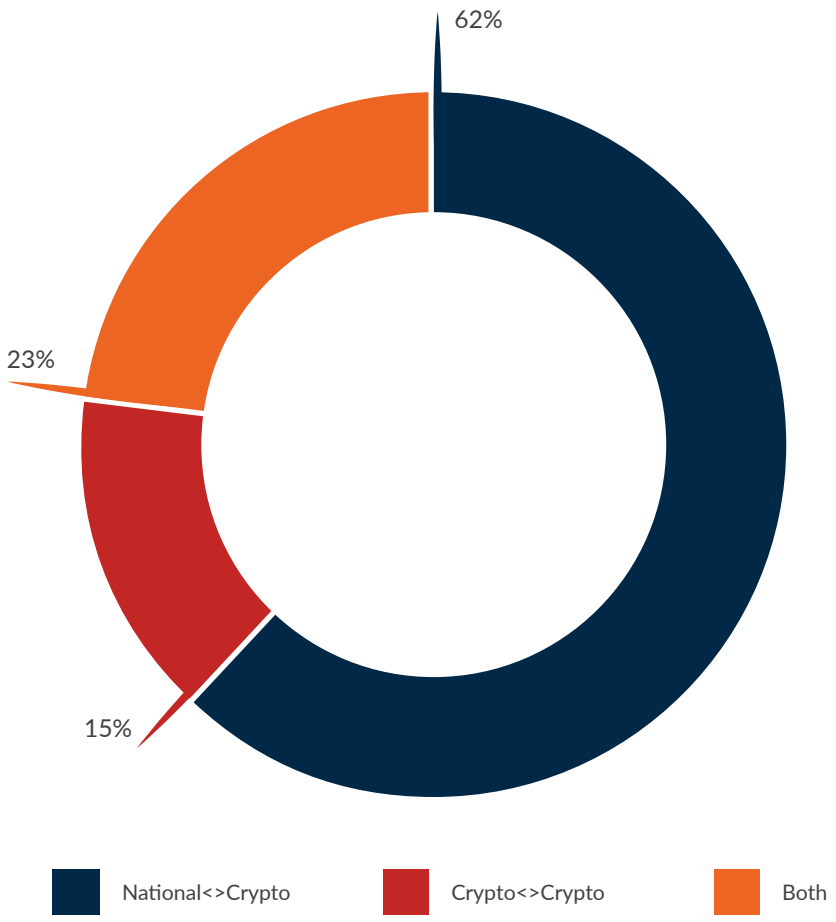


Figure 49: 85% of wallets providing currency exchange services enable the exchange of national currency




85% of all wallets providing currency exchange services enable the purchase and sale of national currencies (Figure 49). 15% provide only cryptocurrency-to-cryptocurrency exchange services, and 23% provide both national-to-cryptocurrency as well as cryptocurrency-to-cryptocurrency exchange services.

All surveyed wallets providing cryptocurrency-only exchange services have integrated a third-party exchange which is responsible for providing the exchange services. Wallet providers offering national-to-cryptocurrency exchange services use different models: 28% are providing the infrastructure via their wallet environment for a P2P exchange/marketplace between users, while 36% are operating a centralised exchange/brokerage service themselves and another 36% have integrated a third-party exchange (Figure 50).

It turns out that only 27% of wallets offering national currency exchange services take custody of users' cryptocurrency funds. 18% let users choose whether to hold private keys, and over half do not control private keys (Figure 51).[9] No wallet offering cryptocurrency-only exchange services has access to customer funds.

> Half of all incorporated wallets surveyed provide currency exchange services that involve the use of national currency.

Figure 50: 28% of wallets offering national-to-cryptocurrency exchange services are using the P2P exchange model

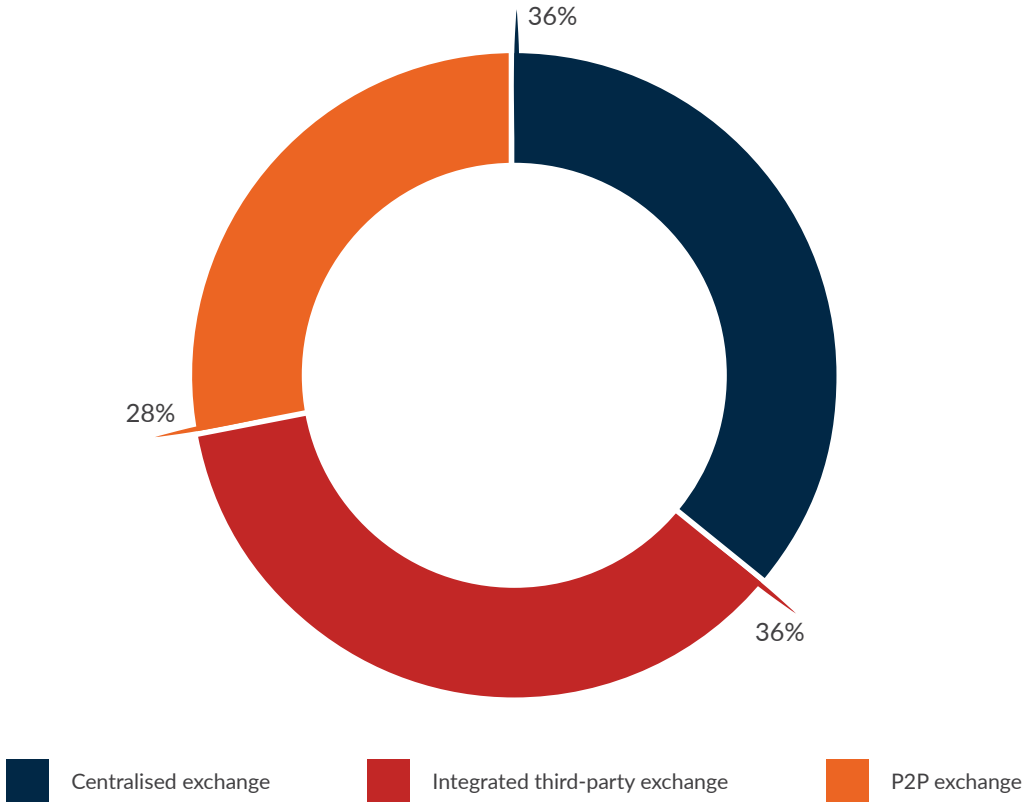



Figure 51: Only 27% of wallets providing national currency exchange services take full custody of users' cryptocurrency funds

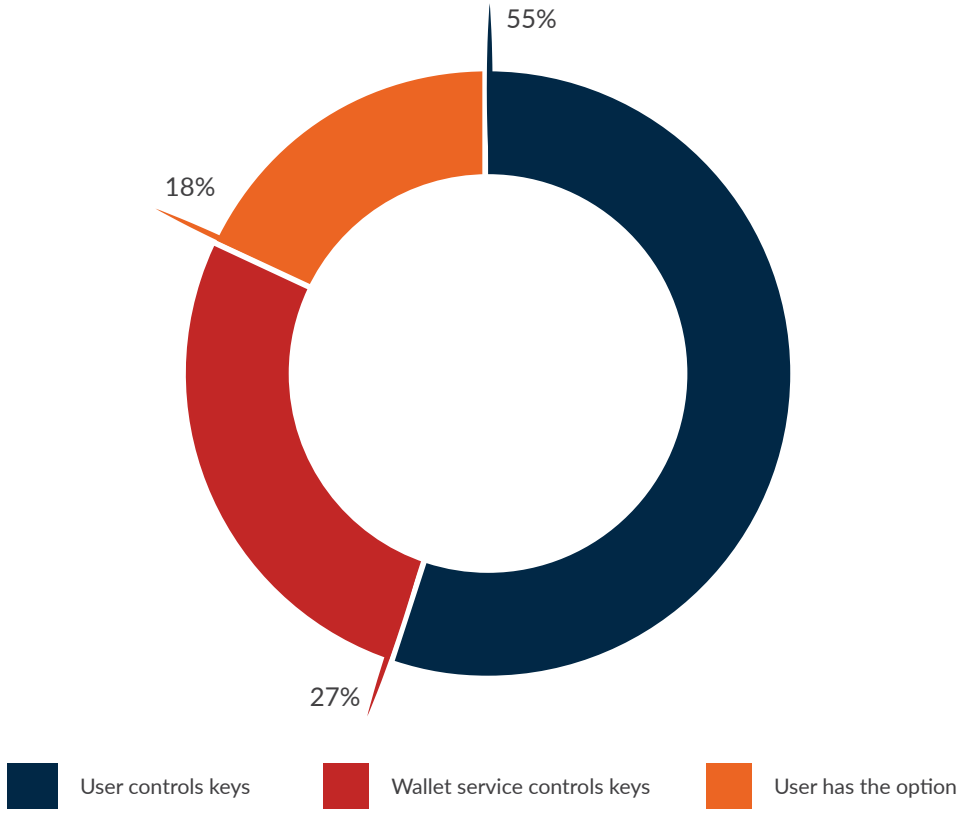


Figure 52: 76% of incorporated wallet providers do not have a license

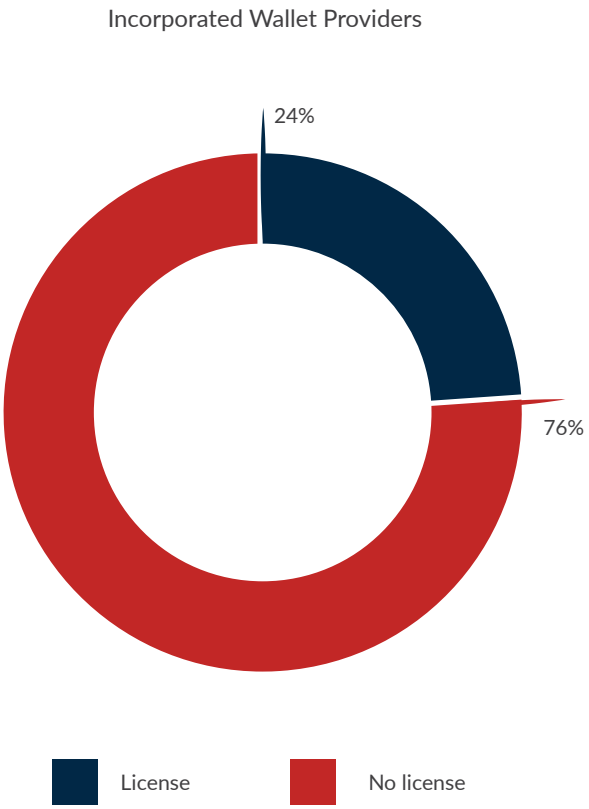
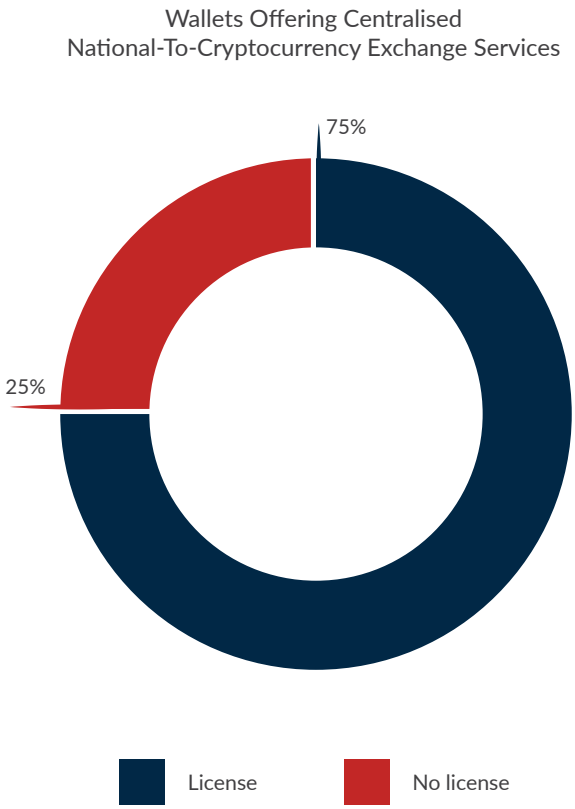



Figure 53: 75% of wallets providing centralised national-to-cryptocurrency exchange services have a license




# REGULATION AND COMPLIANCE

In contrast with exchanges and firms designated as money transfer operators, the compliance requirements for the cryptocurrency storage function performed by wallets are less clear. The fact that wallet providers are often operating globally, which again contrasts with exchanges and money transfer operators which tend to limit services to particular jurisdictions, further muddies the wallet compliance waters. For example, if cryptocurrencies are legally considered to be 'money', does that require companies providing basic cryptocurrency storage services to be compliant with existing banking regulation, or does this only apply to wallet providers that take custody of user funds and/or provide integrated currency exchange services?

**LICENSE**

24% of incorporated wallets have a formal license from a regulatory authority, and all of them are wallet providers that offer national-to-cryptocurrency exchange services (Figure 52). 25% of wallets providing centralised national-to-cryptocurrency exchange services do not have a government license (Figure 53).[10]

Figure 54: Large wallets providing centralised national-to-cryptocurrency exchange services have more than 4x higher compliance headcount and cost than small wallets

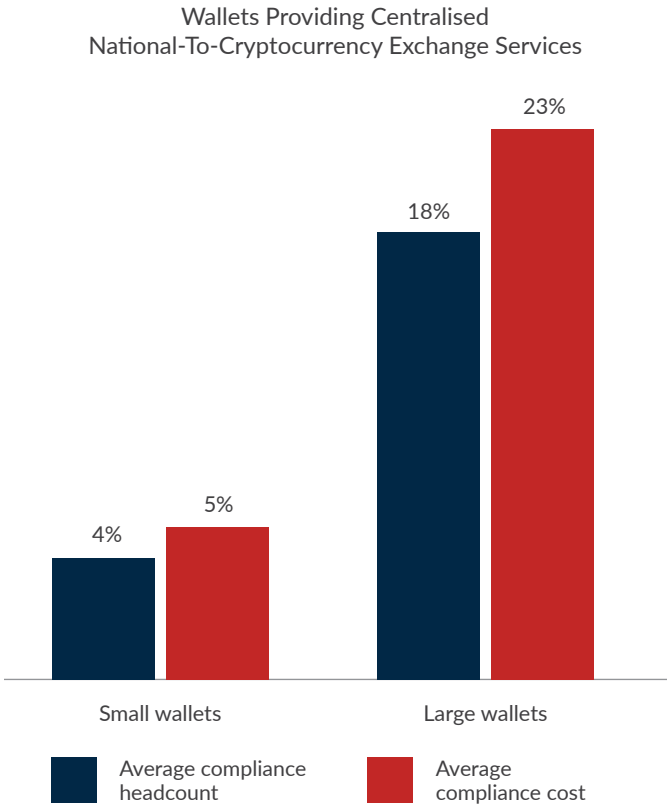
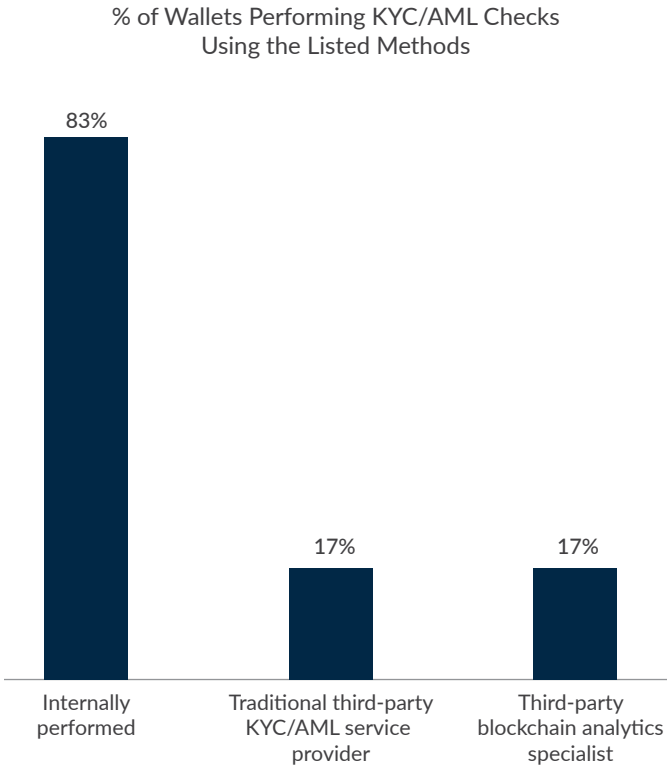



Figure 55: KYC/AML checks are predominantly performed internally by wallet providers




**COMPLIANCE PROGRAMS**

78% of incorporated storage-only wallets do not perform any user compliance, but 80% of wallets providing currency exchange services do. However, it is important to make a distinction between the compliance requirements (or lack thereof) for the three types of currency exchange models used by wallet providers as discussed above.

> Compliance programs are observed at all wallets offering centralised national-to-cryptocurrency exchange services, and less often at wallets with P2P or third-party exchange services

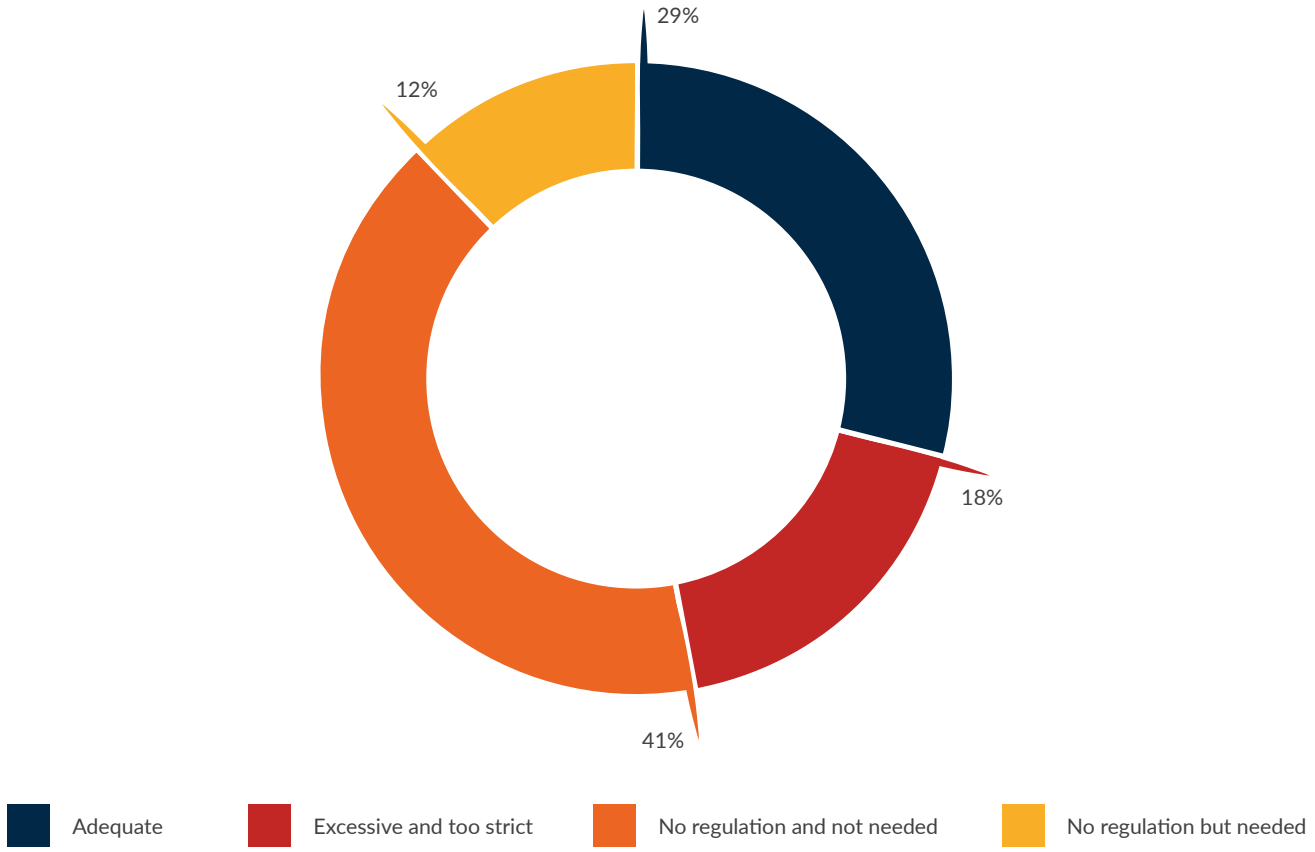
All wallets that provide centralised national-to-cryptocurrency exchange services (i.e., directly executing currency exchange) have a compliance program. In the case of wallets that integrate a third-party exchange, the third-party exchange may be responsible for user verification and compliance requirements, while there is no clear legal framework that applies to wallets with built-in P2P exchange services as trades are happening directly between users. As a result, these wallets generally have less compliance programs than wallets providing centralised exchange services.

**COMPLIANCE HEADCOUNT AND COST**

There are differences with regards to the compliance programs of small and large wallets providing centralised national-to-cryptocurrency exchange services. Large wallet providers have more than four times the headcount and cost associated with compliance than small wallets (Figure 54).

All wallets providing centralised national-to-cryptocurrency exchange services perform KYC and AML checks.[11] The preferred KYC and AML method are internal checks, which are in some cases complemented with traditional third-party KYC/AML service providers (Figure 55). Third-party blockchain analytics specialists are only used by 17% of wallets performing KYC/AML checks. All small wallets performing KYC/AML checks only do so internally.

Figure 56: Wallet providers' perception of the current regulatory environment is mixed, and no clear trend is observed for both small and large wallets




**CURRENT REGULATORY ENVIRONMENT**

In terms of the perception of existing regulations, over 40% of wallet providers indicate they perceive no existing regulations specific to their activities and that they are not needed, while only 12% of all wallets see the lack of specific regulations as problematic and believe they are needed (Figure 56). Almost 30% of wallets deem the existing regulatory environment to be adequate and appropriate.

When breaking down the views of wallet service providers on regulation by wallet activity, it turns out that half of wallets that provide national currency exchange services believe that regulation is adequate, while the perception of the other half is divided between 'excessive' and 'not needed'. An interesting observation is that 50% of large wallets deem the current regulatory environment excessive and too strict, while 46% of small wallets perceive no specific existing regulations and state that they are not needed. No wallet provider selected the options "Cryptocurrencies are illegal in my country" and "Regulation is too relaxed".

Not a single North American wallet provider thinks that existing regulations are adequate and appropriate, but 57% of European wallet services and 20% of Asian-Pacific wallets appear to be satisfied with the current level of regulation (Figure 57). On the opposite end of the spectrum, 40% of North American wallet services perceive existing regulations to be excessive and too strict, a sentiment that is only shared by 14% of European providers (Figure 28).

However, also 40% of North American wallets perceive no existing regulations that specifically apply to them (and indicate that they are not needed) – as do 60% of wallets from Asia-Pacific (Figure 59). No European wallets perceive a lack of existing regulations and advocate for more regulatory clarity, but 20% of both Asian-Pacific and North American wallet providers do (Figure 60).

Overall, responses suggest that the majority of wallet providers based in Europe and Asia-Pacific are satisfied with the existing regulatory environment (or the lack thereof), but that North American wallet providers are divided in how they perceive existing regulations.

Figure 57: Regulation is adequate and appropriate

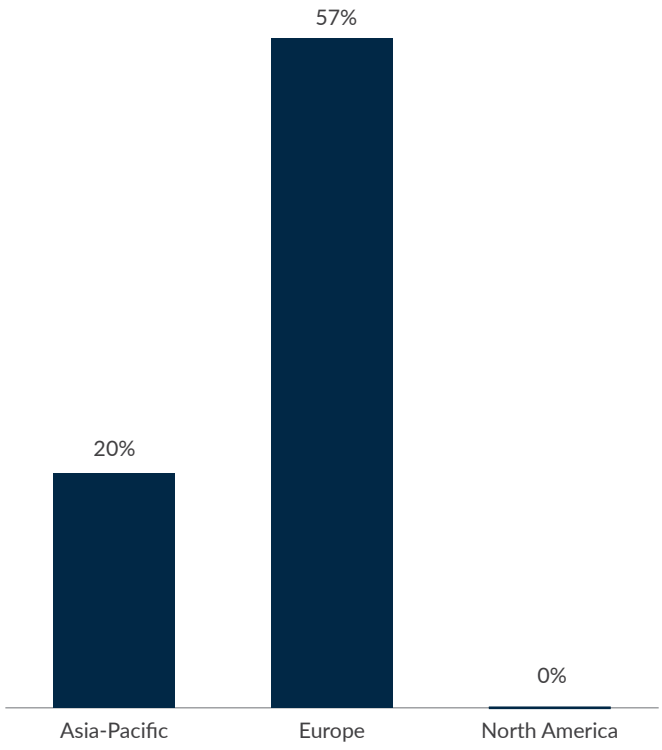



Figure 58: Regulation is excessive and too strict

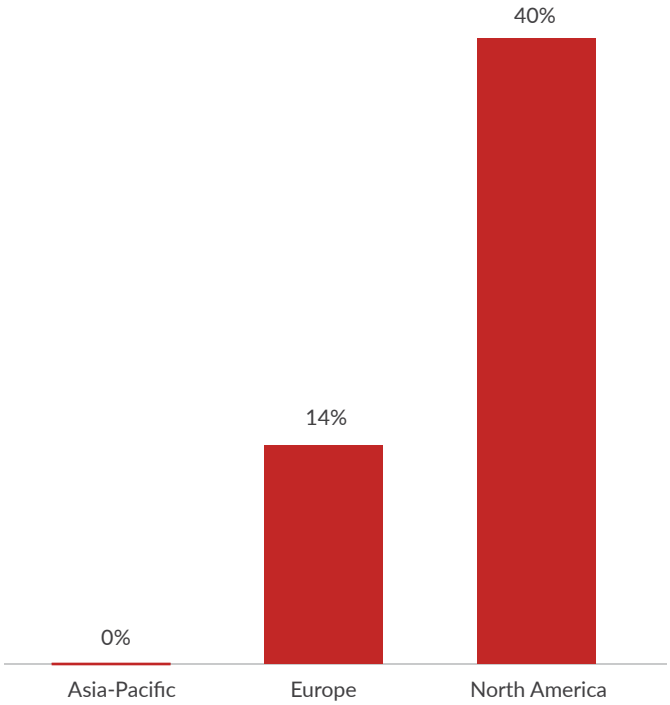



Figure 59: No specific regulation and not needed

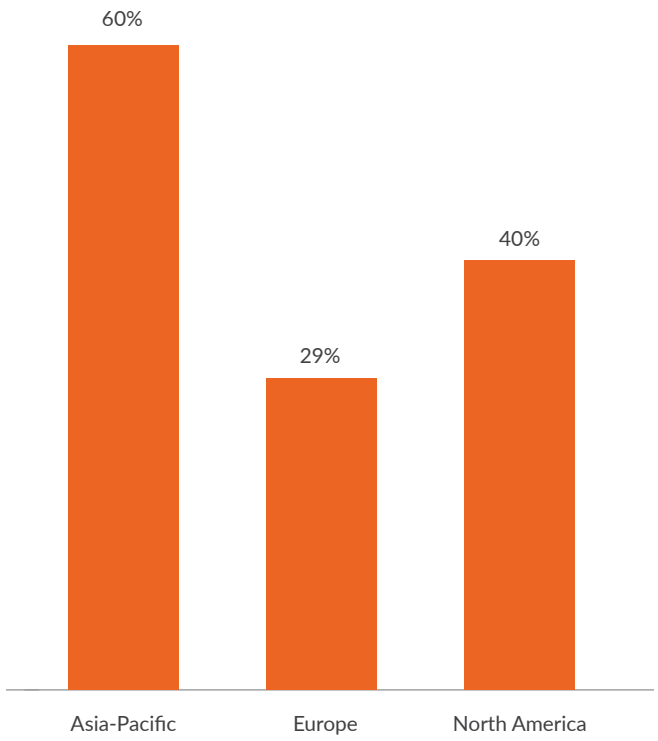



Figure 60: No specific regulation but needed

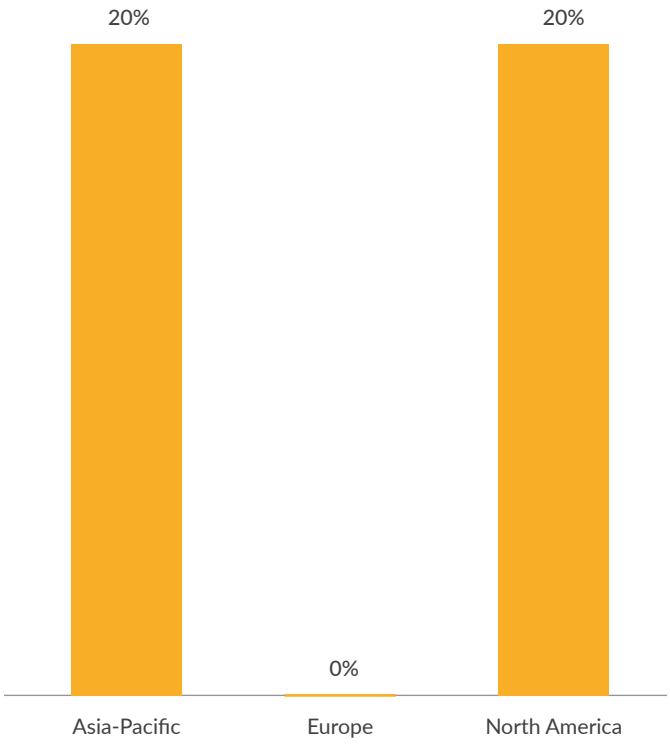


Figure 61: Security headcount varies considerably between small and large wallets

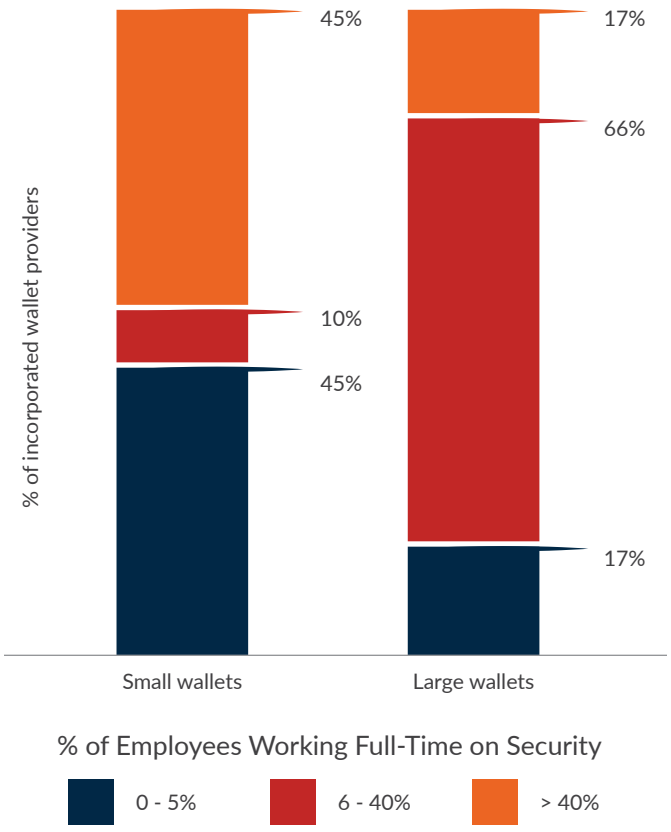
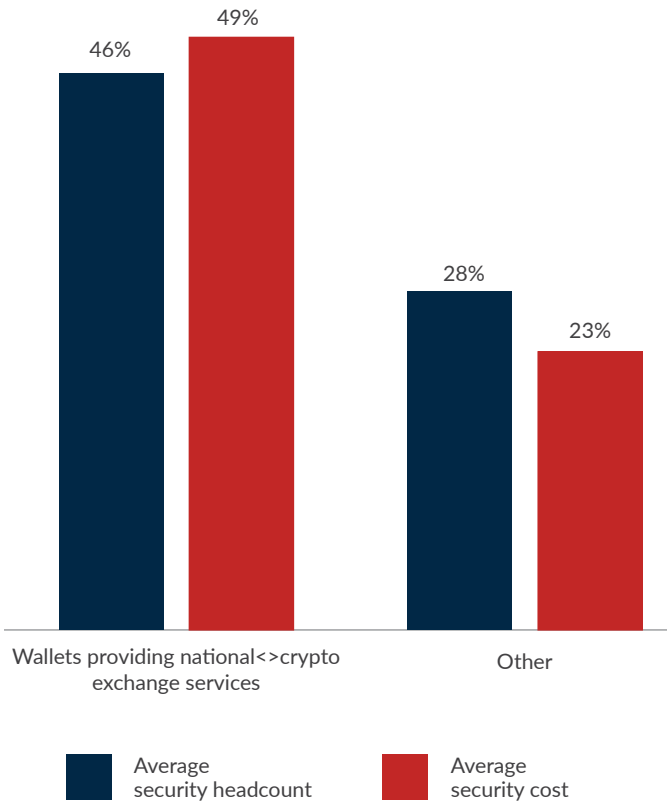



Figure 62: Wallets providing national-to-cryptocurrency exchange services have on average considerably higher security headcount and cost than those that do not




# SECURITY

### SECURITY HEADCOUNT AND COST

Average headcount dedicated to security as a share of total employee headcount is 37%, and security costs as a percentage of total budget are approximately the same at 35%. Both of these figures are significantly higher than those for exchanges and payments companies.

Small wallet companies have on average slightly more security headcount in percentage of total employees than large companies (+9%), but there is no significant difference between large and small wallets in terms of average security costs as a percentage of total budget.

A look at the distribution reveals that there are also considerable differences between wallet providers within the small/large categories: 45% of small wallet providers have only between 0% and 5% headcount working full-time on security, suggesting that employees of these companies perform multiple roles at the same time and are thus not strictly assigned to security (Figure 61). Another 45% of small wallet providers have more than 40% of employees working full-time on security, which indicates that these companies employ at least one full-time security professional. In contrast, two-thirds

Percentage of Wallet Providers That Use External Security Providers


Average Number of External Security Providers


of large wallets have between 6% and 40% of employees working full-time on security.

In terms of security costs, the picture looks slightly different: all incorporated wallet providers spend at least 10% of their budget on security. 45% of small wallets spend between 21% and 40% on security, and 18% allocate over 40% of their budget to security. The disparities between small wallets are substantial as the proportions of the budget associated with security range from 10% to 100%. For large wallets, there are also considerable discrepancies with budgets allocated to security ranging from 20% to 80%.

> Security costs at large wallets range from 20% to 80% of the overall budget

Custodial wallets spend on average 51% of their total budget on security, which is 20% more than non-custodial wallets.[12] We do not observe a significant increase in security headcount at wallet providers that control user keys.

> Custodial wallets spend 20% more of their budget on security than non-custodial wallets

However, the most striking difference becomes apparent when comparing wallet providers offering national-to-cryptocurrency exchange services to those that do not: the former spend more than twice as much of their budget on keeping their wallet secure (Figure 62). On average, wallets that provide national-to-cryptocurrency exchange services also have 18% more headcount working full-time on security. We do observe that wallets providing P2P national-to-cryptocurrency exchange services have the highest security headcount as a percentage of total employees and spend the most on security as a percentage of total budget.

> Wallets with built-in P2P national-to-cryptocurrency marketplaces have the highest headcount and cost associated with security of all wallets

**EXTERNAL SECURITY PROVIDERS**

Of all surveyed wallets, 53% use external security providers. 80% of large wallets use external security providers compared to only 42% of small wallets. 75% of wallet providers offering national-to-cryptocurrency exchanges make use of external security providers, and even 83% of wallets operating centralised national-to cryptocurrency exchanges use the services of at least one external security provider.

On average, wallets use 3 different security providers. Of all wallets using external security providers, 89% state that they have not come to rely more on them over time.

# KEY FINDINGS

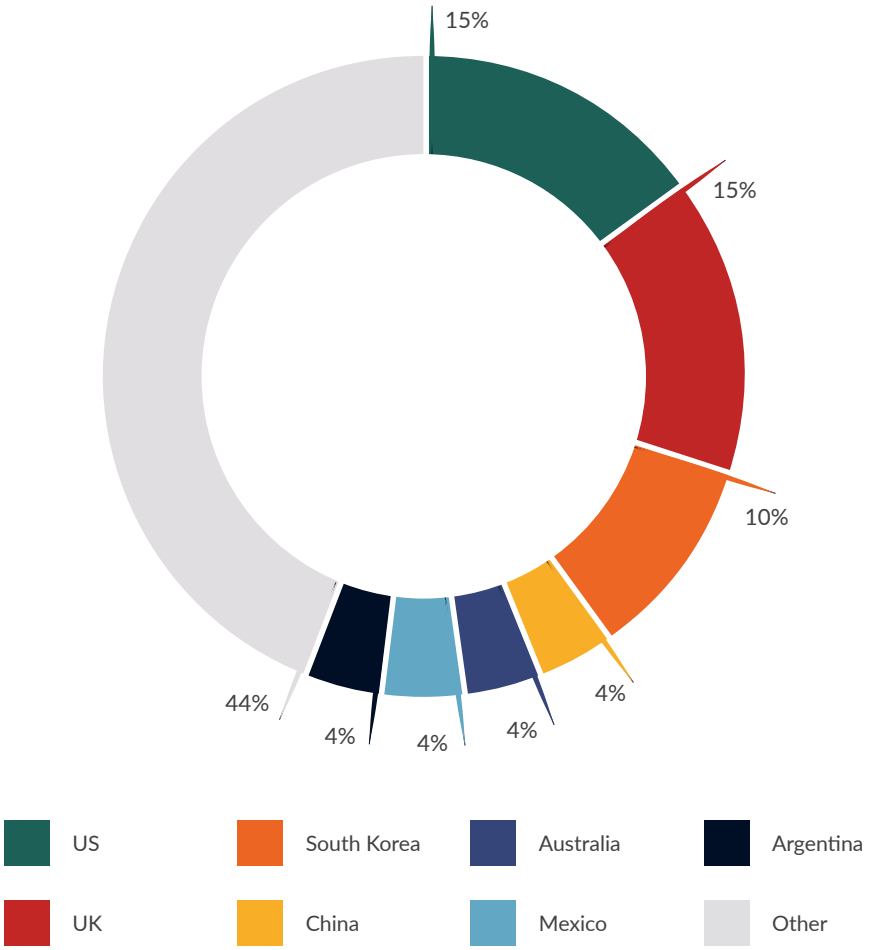
**Activities and Operations**

- While 79% of payment companies have existing relationships with banking institutions and payment networks, the difficulty of obtaining and maintaining these relationships is cited as the sector's biggest challenge
- A significant geographic dispersion of cryptocurrency payment companies can be observed, in-line with the dispersion observed with exchanges
- Asian-Pacific and Latin American payment companies focus primarily on local users, whereas European and North American payment companies have a significant user share in non-local regions
- Nearly two-thirds of payment companies are specialising in a single payment activity (e.g., B2B payments); 8% are engaged in three activities or more
- Merchant services, which mainly consist of processing payments for merchants that accept cryptocurrencies, is the most widely offered payment service (52% of survey respondents)
- 56% of all payment companies surveyed are also operating a stand-alone cryptocurrency exchange themselves in addition to their payment services
- Payment service providers employ a total of 1,057 people, with an average of 22 full-time employees per company
- 54% of payment companies have a formal government license; of all payment type activities, platforms providing B2B payment services are most likely to have a license (83%)
- The average compliance headcount of payment companies is 8% of total headcount, and an average of 12% of the total budget is spent on compliance
- 86% of payment companies perform KYC/AML checks; internally performed checks are the preferred method

**Payments**

- Cross-border payments generally have a higher transactional value than intra-country payments: 46% have a transaction size between $100 and $1,000, and 34% have a transaction size that exceeds $1000
- The average business (B2B) payment has a transaction size of $1,878, whereas P2P transfers ($351) have higher average transaction sizes than consumer (C2B) payments ($210)
- On average, national-to-cryptocurrency payments constitute two-thirds of total payment company transaction volume, whereas national-to-national currency transfers and cryptocurrency-to-cryptocurrency payments account for 27% and 6%, respectively
- 21% of payment companies exclusively process national-to-national currency payments, whereas half of payment companies do not process any national-to-national payments at all
- The bitcoin network is used by 86% of surveyed payment companies as main payment rail for cross-border transactions

Figure 63: Geographic dispersion of payment companies in the study sample




# LANDSCAPE

## INTRODUCTION

All cryptocurrency systems have an integrated payment network to process transactions denominated in the native token. While the promise of these systems is that users can independently transact on these networks, there are a variety of reasons why users prefer using services provided by third-party payment service providers.[1]

## GEOGRAPHY

We collected data from a sample of 48 companies from 27 countries that are providing payment services that involve the use of cryptocurrencies (Figure 63). All five world regions are represented, with one third of participants based in the Asia-Pacific region and another third based in Europe. In terms of countries, the US and the UK are leading with each country serving as home to 15% of payment service providers, followed by South Korea (10%).

## Table 6: Taxonomy of main cryptocurrency payment platform types

| Use case | Payment activity | Description |
|---|---|---|
| Payment rail ('national currency-focused') | Money transfer services | Services that primarily provide international money transfers for individuals denominated in national currencies. These include among others traditional remittances and bill payment services. |
| | B2B payments | Platforms that provide payments for businesses, denominated in national currencies, often times across borders. |
| Cryptocurrency payments ('cryptocurrency-focused') | Merchant services | Services that process payments for cryptocurrency-accepting merchants. May provide additional merchant services such as shopping cart integrations and point-of-sale terminals. |
| | General-purpose cryptocurrency platform | Platforms that perform a variety of cryptocurrency transfer services including instant payments to other users on the same platform using cryptocurrency and/or national currencies, payroll, and other services. In general, payments are denominated in cryptocurrency but can be easily exchanged to national currencies. |

### TAXONOMY

The use of cryptocurrencies by payment service providers can be grouped into two broad categories:

a) *Payment rail*: use of cryptocurrencies as a channel for fast and cost-effective transfer of national currencies (mainly cross-border/international payments, but also intra-country payments)

b) *Cryptocurrency payments*: provide services to facilitate the use of cryptocurrencies

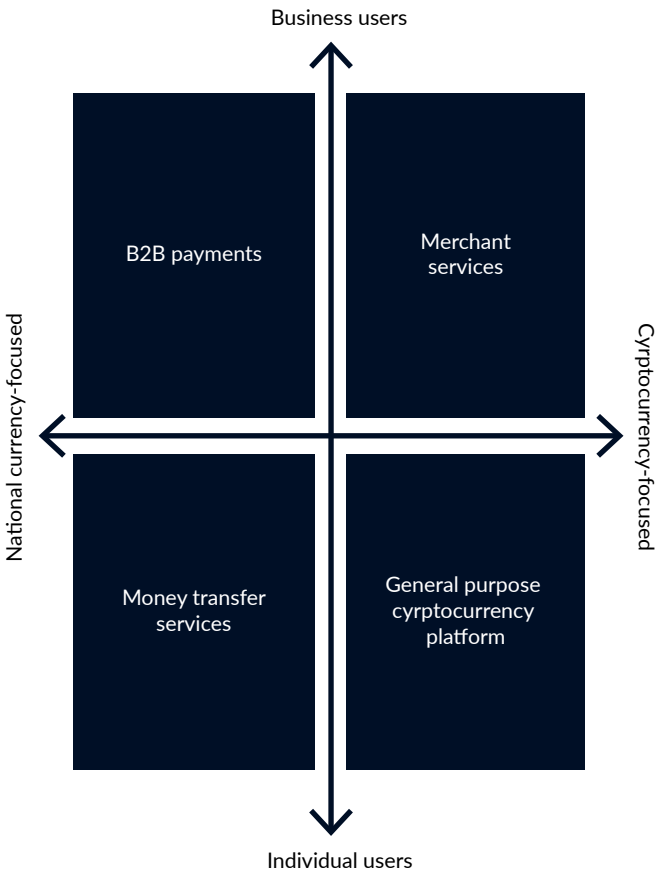
For service providers from category a), cryptocurrency is not the primary focus of the transaction but rather a means to an end: transfers are generally denominated in national currencies and users do not necessarily know that a cryptocurrency system is used on the back-end ('national currency-focused'). This is what is meant when bitcoin and other cryptocurrencies are described as a 'payment rail'.

In contrast, companies from category b) provide a platform to facilitate the use of cryptocurrencies for users and generally brand or market their services as 'cryptocurrency-focused'. While transfers are usually denominated in cryptocurrencies, they can also be denominated in national currencies.

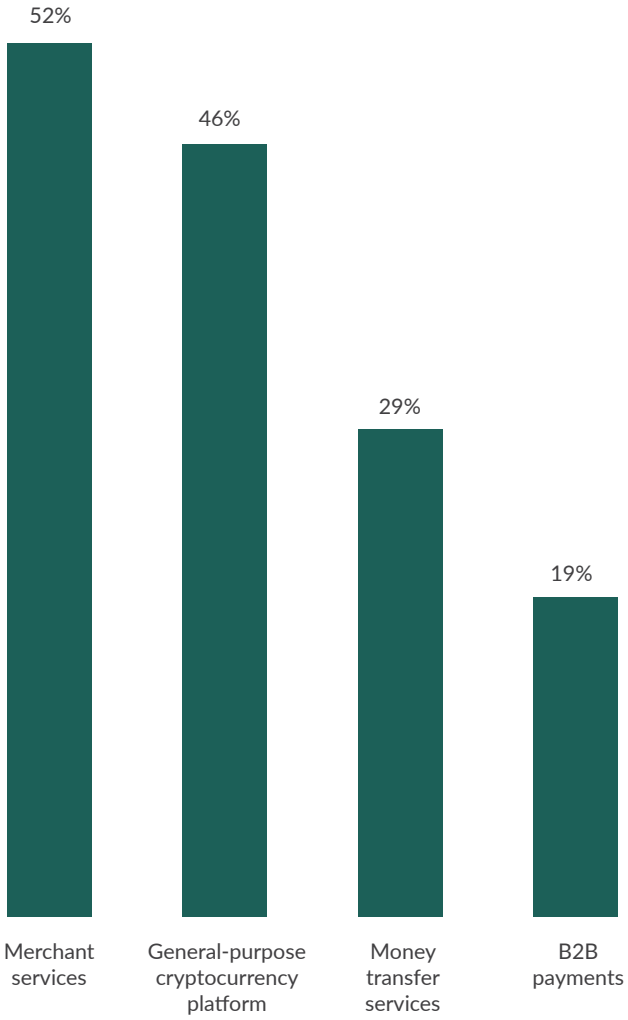
> The payments sector can be broadly split into two categories – 'cryptocurrency-focused' and 'national currency-focused'

Based on these categories, we can establish a simple taxonomy of the four main types of activity in the cryptocurrency payments segment (Table 6).

## Figure 64: The cryptocurrency payment sector




## Figure 65: More than half of payment companies provide merchant services




It should be noted that in some cases, the lines between these categories are blurred as some general-purpose cryptocurrency platforms also enable all payments being denominated in national currencies, and some B2B payment service providers also enable payments being denominated in cryptocurrencies. Nonetheless, this working taxonomy provides a basic framework to categorise the different types of payment activities as depicted in Figure 64.

### ACTIVITIES

52% of study participants provide merchant services (as defined above), making it the most widely offered cryptocurrency payment activity (Figure 65). Processing payments for merchants that accept cryptocurrencies as a payment method constitutes the most frequently offered merchant services. 46% of payment service providers feature a fuller-featured platform that lets users buy, store and transfer cryptocurrency, often providing additional services such as insured accounts and bill payment services. 29% of companies are operating a platform for personal remittances and money transfers, while 19 % of payment service providers offer a platform for B2B payments targeting business customers.

Nearly two-thirds of payment service providers are specialising in a single type of payment activity, whereas 27% of payments companies are providing two payment activity types and 8% are performing three or more (Figure 66). Companies that specialise in a single payment activity are most often providing merchant services (35%).

It is worth noting, however, that 56% of all payment companies surveyed are also operating a stand-alone cryptocurrency exchange themselves in addition to their payment services.[2] In

Figure 66: Nearly two-thirds of payment companies specialise in a single payment activity, of which merchant services are the most frequent

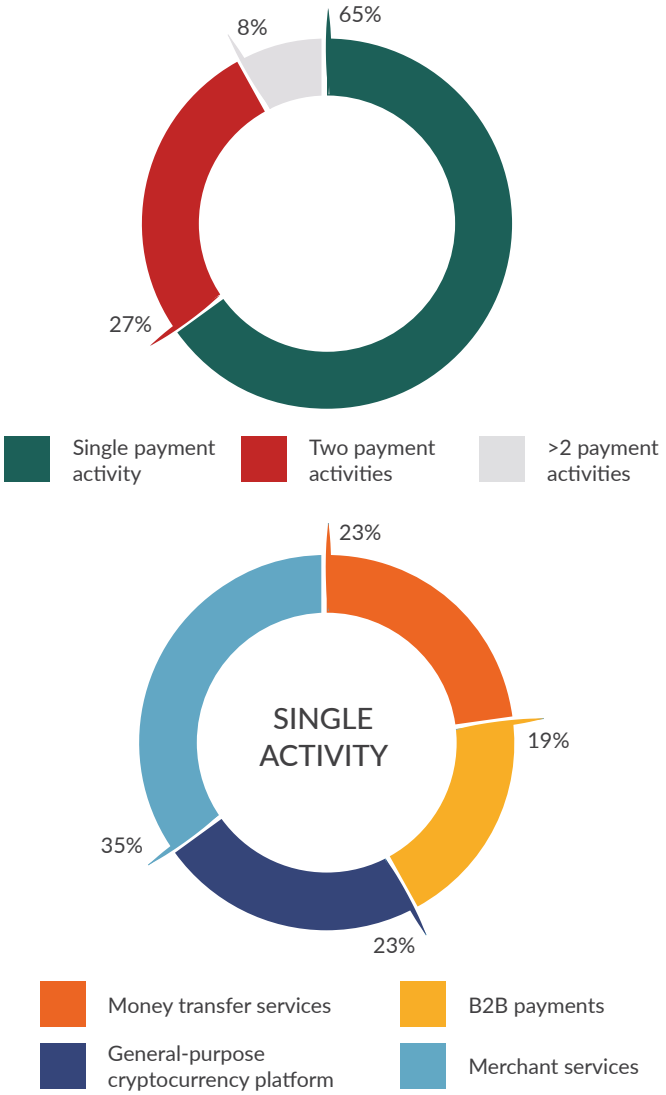
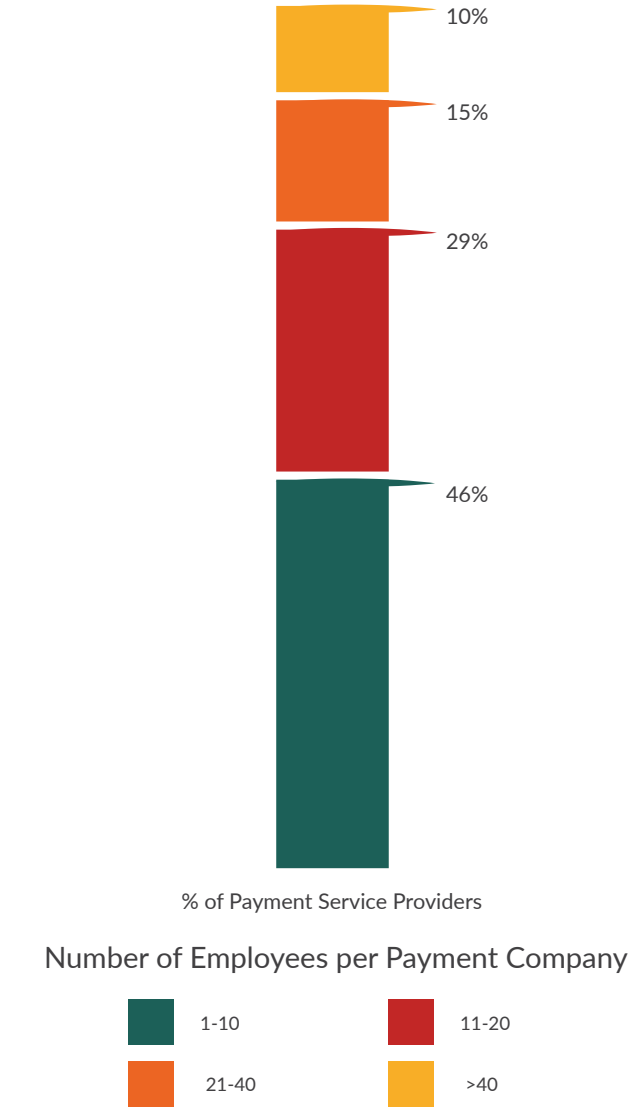



Figure 67: Over half of payment service providers have more than 10 full-time employees



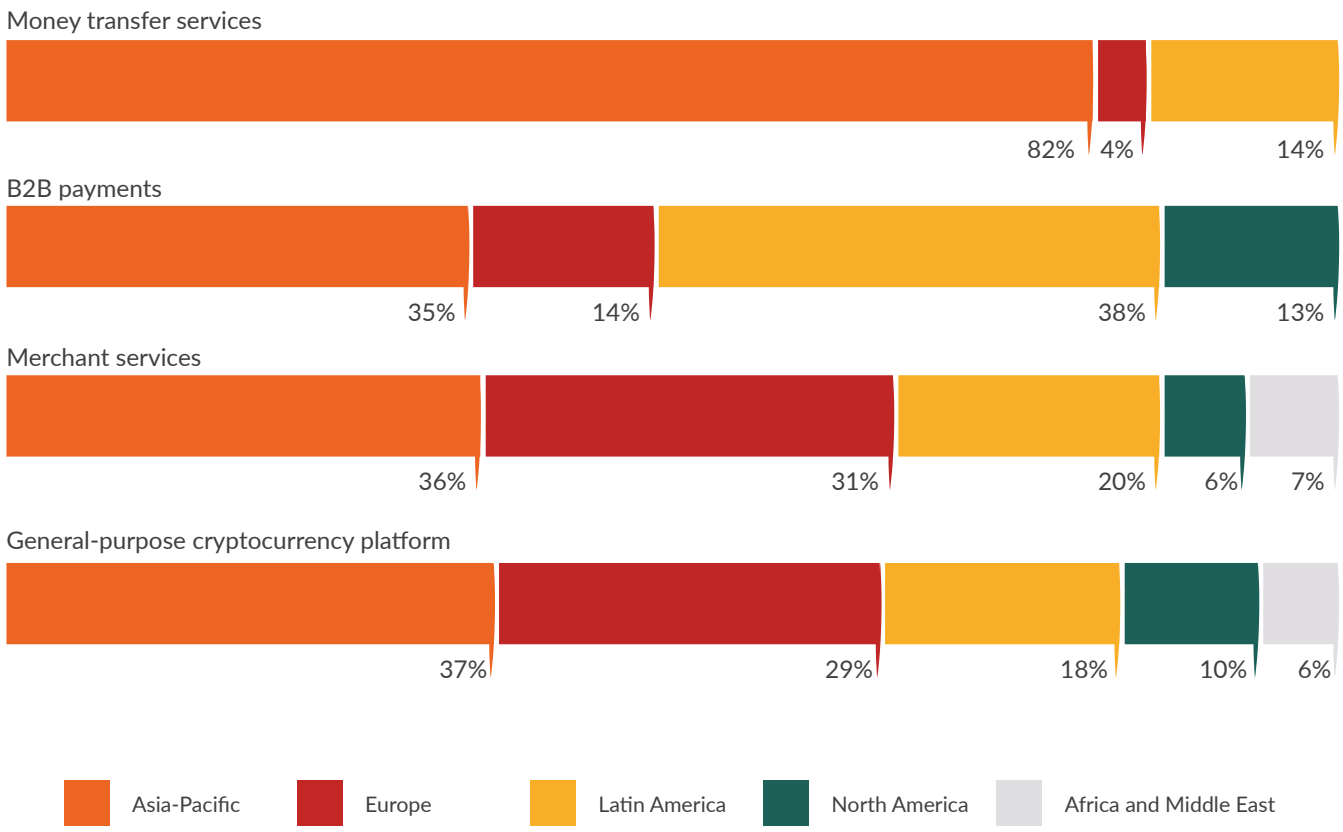

fact, 84% of companies providing merchant services also operate a cryptocurrency exchange, as do 76% of companies offering a general-purpose cryptocurrency platform. This shows that many cryptocurrency exchanges have expanded their product line to provide additional services to merchants as well as consumers.

### EMPLOYEES

The total number of people employed by payment service providers active in the cryptocurrency industry amount to 1,057.[3] Payment companies have on average 22 full-time employees, which is more than wallet providers (19 on average) but less than exchanges (24 on average).

A look at the distribution shows, however, that 46% of payment service providers have only between 1 and 10 employees (Figure 67). In fact, 21% have less than five employees. Nonetheless, over half of payment service providers surveyed have more than ten full-time employees, and 10% employ even more than 40. In most cases, these companies are also active in other cryptocurrency sectors and it cannot be clearly established how many employees are working full-time on the payment services.

Figure 68: Origin of customers segmented by payment activity types




# USERS

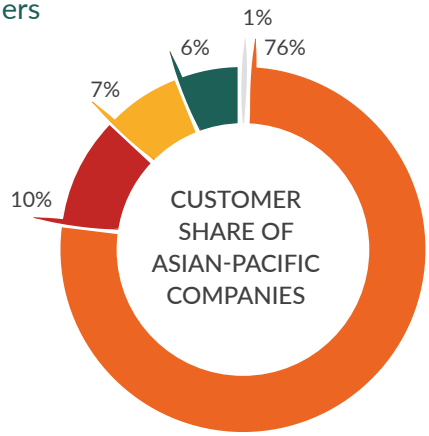
## GEOGRAPHY

We have segmented users to explore whether differences exist between companies performing different types of payment activities, as well as any differences between companies located in different regions.

Segmenting by type of payment activities, findings show that money transfer services are most popular in Asia-Pacific, and that B2B payment platforms are mostly used by customers based in Asia-Pacific and Latin America (Figure 68). Findings also suggest that companies engaged in 'cryptocurrency-focused' activities have a more international customer base. The customer share proportions by world region are approximately equal for both general-purpose cryptocurrency platforms and merchant service providers. In contrast, companies providing 'national currency-focused' payment services appear to have a less broadly distributed customer base in geographical terms and focus more on local markets – this applies especially to money transfer services.

A significant relationship between the location of payment service providers and their customers can be observed for Asian-Pacific and Latin American payment companies (Figure 69).

Figure 69: Payment companies based in Asia-Pacific and Latin America serve primarily local customers



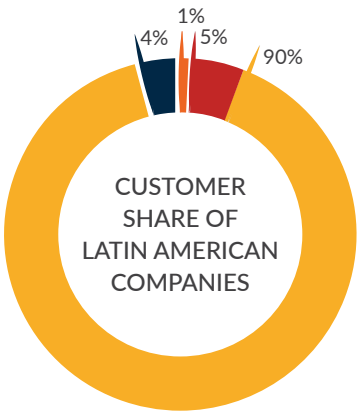
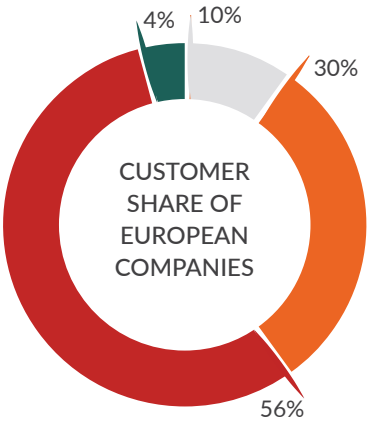
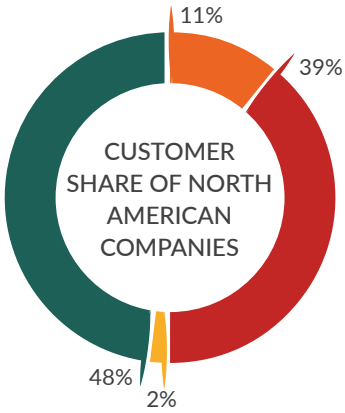




Figure 70: Payment companies based in Europe and North America have a significant share of customers that are based in other regions





76% and 90% of customers from companies based in Asia-Pacific and Latin America, respectively, are based in the same region as the payment service provider. This indicates that payment companies based in these regions primarily serve local markets.

In contrast, payment companies based in Europe and North America appear to be serving more diverse markets since a significant share of their customers are based in other, non-local regions (Figure 70). 44% of customers from European payment companies and over half of customers from payment service providers based in North America are not domiciled in the same region. Surprisingly, only 2% of customers from North American companies are based in Latin America.

Significant differences with regards to the customer share by region are observed between payment companies based in different regions

There is not enough data available from companies based in Africa and the Middle East to make a more detailed breakdown. It appears that users from this region are mainly served by European payment companies when excluding local payment companies.

It is not surprising that the majority of customers from payment companies are based in the same region. In contrast to most wallet providers whose users are often widely distributed around the world, payment companies generally provide services that involve the use of locally-used national currencies. This is further evidenced by Figure 71, which shows that surveyed payment companies support over 30 different national currencies.

While the major global reserve currencies (US dollar, euro, Chinese renminbi, Japanese yen, and British pound sterling) are not surprisingly the most widely supported currencies, many regionally used national currencies are supported as well. We can presume that the fact these national currencies are supported means that there is local demand in these countries for the services provided by payment companies.

## Figure 71: National currencies supported by surveyed cryptocurrency payment companies

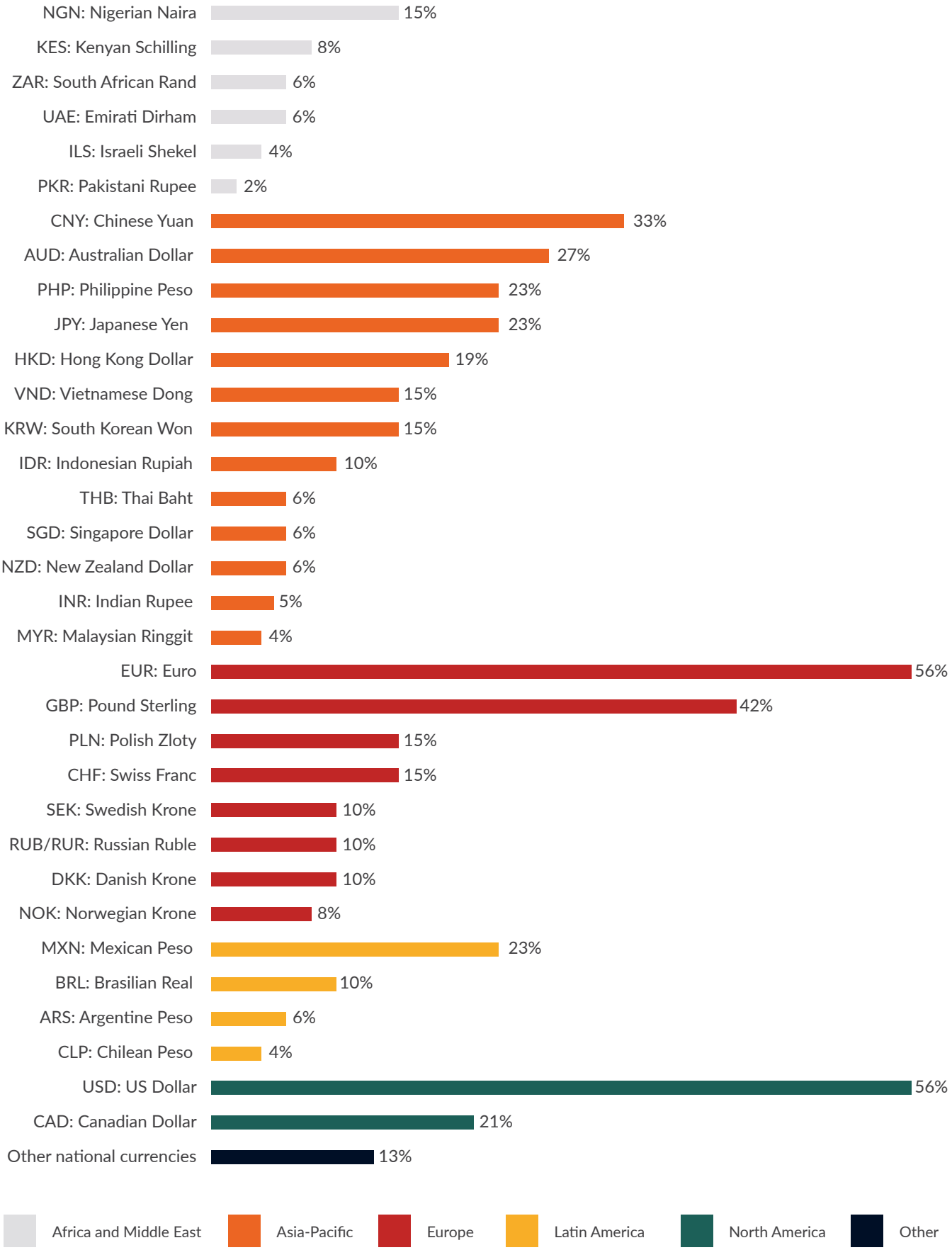
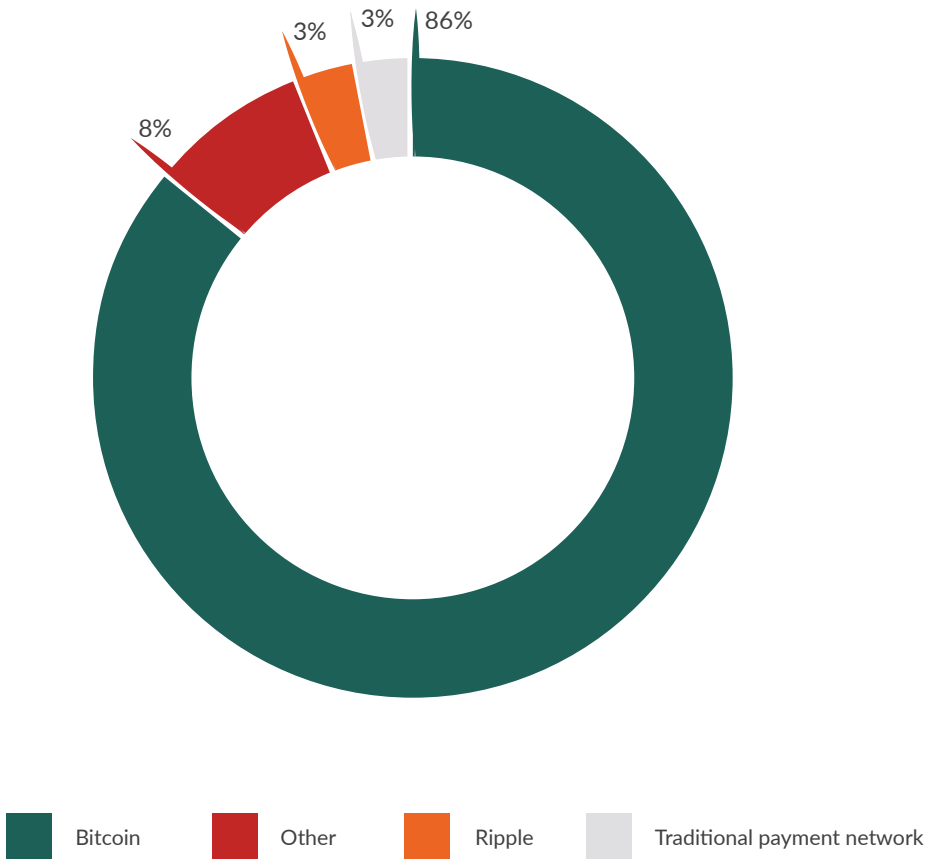


Figure 72: The Bitcoin network is the most widely used payment rail for cross-border transactions




# OPERATIONS

### PAYMENT RAIL

86% of participating payment companies indicate that they use bitcoin as their primary payment rail for cross-border transactions (Figure 72). Ripple as well as traditional payment networks are only used by 3% of payment service providers as the main payment rail. 8% of payment companies indicate that they use other payment rails, including combinations of various payment networks as well as the use of Ethereum contracts.

### CURRENCY MIX

There are three options in which transfers can be denominated:

- National-to-national currency (using cryptocurrency strictly as a payment rail)[4]
- National-to-cryptocurrency (or vice-versa)
- Cryptocurrency-to-cryptocurrency

Figure 73: Majority of transactions are national-to-cryptocurrency (and vice-versa)


21% of payment service providers state that all their transactions are national-to-national transfers. By contrast, half of payment service providers do not process direct national-to-national currency transfers. 43% of payment companies indicate that all their transactions are national-to-cryptocurrency (or vice-versa) payments.

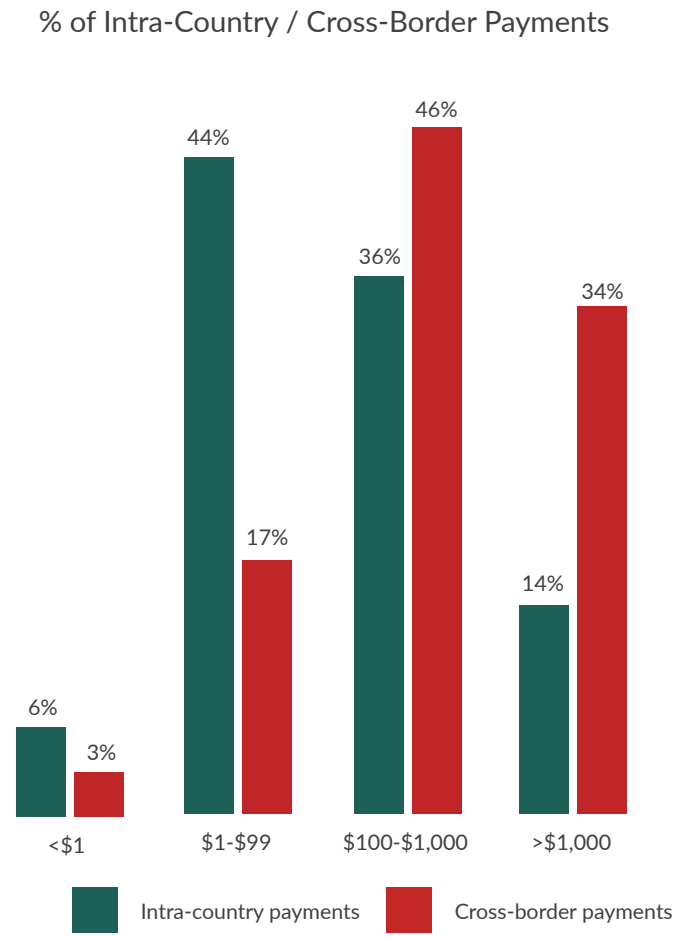
> 21% of payment companies exclusively process national-to-national currency payments, whereas half of payment companies do not process any national-to-national payments at all

National-to-cryptocurrency (or vice-versa) payments constitute on average 99% of all transactions processed by payment companies that do not provide direct national-to-national currency payments. Cryptocurrency-to-cryptocurrency payments only account for roughly 1% of total transaction volumes (both in terms of USD-value and by the number of transactions).

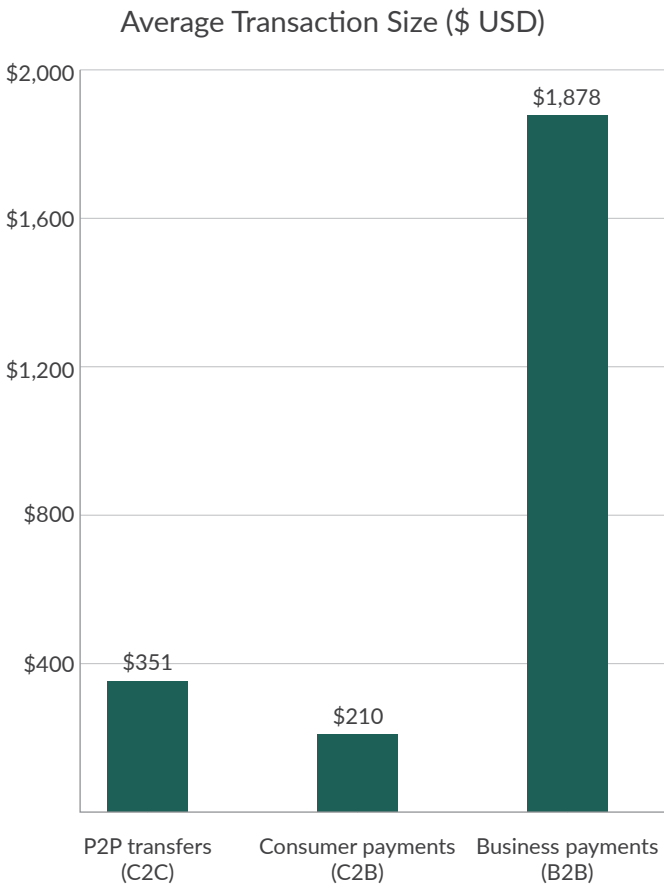
> 99% of transaction volumes from payment companies that do not process national-to-national payments are constituted of national-to-cryptocurrency payments

When analysing the currency mix of payment companies that provide all three options, findings show that on average, two-thirds of transactions are national-to-cryptocurrency (or vice-versa) payments (Figure 73). In terms of transaction volumes in USD-value, national-to-national currency payments account for 27% of all transactions, while cryptocurrency-to-cryptocurrency payments only amount to 6% of both transaction volume in USD-value and transaction volume measured by the number of transactions.

## Figure 74: Cross-border transactions are generally higher-value transactions




## Figure 75: Average transaction sizes by payment channel




The proportion of national-to-cryptocurrency transactions in terms of the number of transactions is slightly higher than the proportion in terms of USD-value, although the difference observed is minuscule. This might suggest that the average national-to-cryptocurrency transaction size is slightly smaller than the average national-to-national transaction. For cryptocurrency-to-cryptocurrency transactions, no differences can be observed.

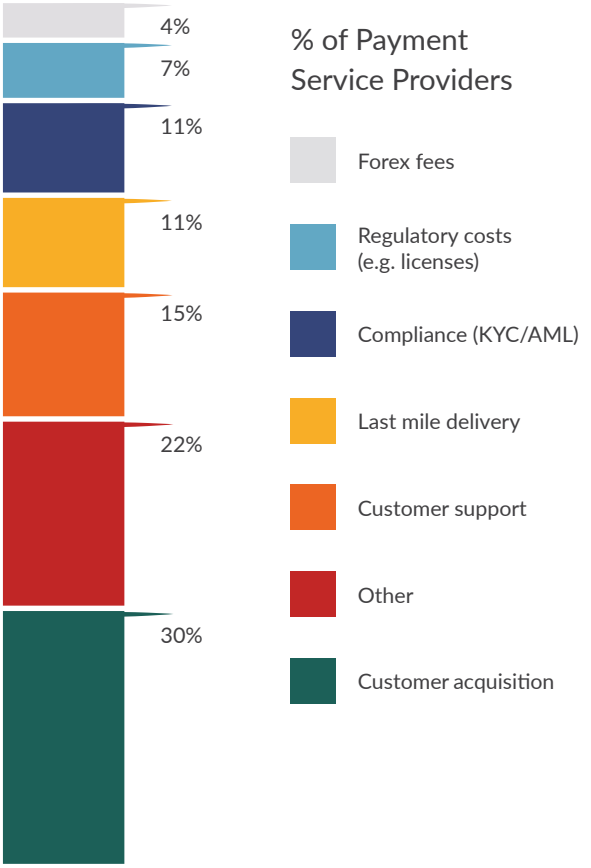
### TRANSACTION SIZE

Findings show that the average cross-border payment is generally a higher-value transaction as 35% of cross-border payments have a transactional value exceeding $1,000, and 46% of transactions have an average size of between $100 and $1,000 (Figure 74). In contrast, national (i.e., 'intra-country') payments facilitated by payment service providers tend to be rather lower-value transactions, since 44% of all national payments have a transactional value of between $1 and $99.

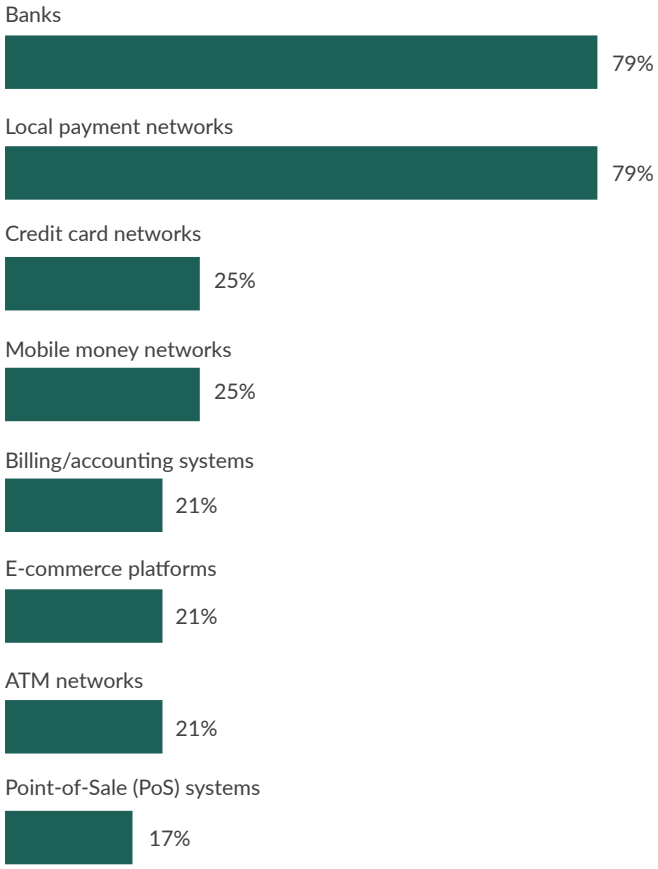
Interestingly, 6% of national payments and 3% of cross-border payments have a transaction size that is less than one USD, indicating that a not-insignificant number of micropayments facilitated by cryptocurrency payments companies are taking place today.

Findings also show that the average transaction size of P2P transfers (i.e., payments between individuals) amounts to $351 (Figure 75). Consumer payments (i.e., consumers buying goods and services from merchants and paying bills) have an average transaction size of $210, whereas business payments between corporations have an average transactional value of nearly $1,900.

## Figure 76: 'Customer acquisition' is cited most often by payment companies as highest operational cost factor




## Figure 77: Nearly 80% of payment companies have existing relationships with banks and local payment networks




### COST FACTORS

Findings show that customer acquisition constitutes the major operational cost factor for payment companies (Figure 76). Costs associated with the development of the IT infrastructure underlying the payment platform were most often cited by payment companies in the 'Other' category.

Expenses related to customer support as well as compliance and regulatory costs are most often cited as second- or third-highest operational expenses. Operational cost factors ranked highest represent on average 25% to 60% of total operational expenses, whereas the expenses ranked second range between 8% and 28% of total operational expenses.

Costs associated with security constitute on average 14% of the total budget, but security costs range considerably from one payment service provider to another: while 58% spend between 0% and 10% of their budget on security, 29% of payment companies have security costs that range between 20% and 50% of their total budget. It can be observed that payment companies operating cryptocurrency exchanges themselves tend to have higher costs as a percentage of total budget associated with security.

### EXISTING PARTNERSHIPS

Payment companies generally act as gateways between businesses, traditional financial services, and cryptocurrency systems. They thus need to interact at some point with other payment systems and networks to bridge national currencies and cryptocurrencies. Findings show that 79% of payment companies have existing partnerships with banks and local payment networks (Figure 77). The latter include among others pawnshop networks and local remittances networks in Asia as well as traditional banking infrastructure such as the Single Euro Payments Area (SEPA).

A quarter of companies have partnerships with credit card and mobile money networks (e.g., MPesa), while a smaller percentage of companies are partnering with services providers that specialise in merchant solutions to enhance the utility of their products and services, such as for example integrating online shopping cart systems.

41% of payment companies have partnerships with one or two of the listed systems and networks in Figure 77, whereas 59% have integrated three or more. 9% of payment companies even have partnerships with seven of the eight listed networks.

## Table 7: Challenges currently faced by cryptocurrency payment companies

Respondents Scored these Categories on a 1 - 7 Scale

1: Strongly disagree 2: Disagree 3: Somewhat disagree 4: Indifferent 5: Somewhat agree 6: Agree 7: Strongly agree

Lowest average score — Highest average score

| Risk factors | Weighted average | Money transfer services | B2B payments | Merchant services | General-purpose cryptocurrency platform |
|---|---|---|---|---|---|
| Difficulty of obtaining banking/ money transfer operator (MTO) relationships | **5.85** | 5.29 | 5.83 | 5.92 | 5.91 |
| High cost of regulatory compliance | **5.11** | 5.43 | 4.5 | 4.36 | 5.42 |
| Low liquidity in local currency markets | **4.56** | 4.63 | 4.33 | 4.27 | 5.08 |
| Customer acquisition costs | **3.96** | 3.71 | 5.33 | 3,45 | 4.00 |
| Profitability | **3.82** | 3.63 | 3.83 | 3.42 | 3.92 |
| Exchange rate risk | **3.80** | 4.71 | 4.75 | 3.60 | 3.08 |
| Last mile costs | **3.76** | 3.71 | 4.00 | 3.67 | 3.82 |
| Competition from FinTech firms | **3.20** | 3.14 | 4.33 | 2.70 | 2.67 |
| Competition from traditional MTOs (e.g., Western Union) | **3.00** | 4.00 | 4.17 | 2.10 | 2.33 |

This suggests that for cryptocurrencies to be useful to users they cannot live in a closed vacuum, but require interfaces and bridges to the broader economy.

### CHALLENGES

Participating payment service providers were asked to rate the challenges presented in Table 7 according to the level of 'urgency' that they currently pose to their operations.

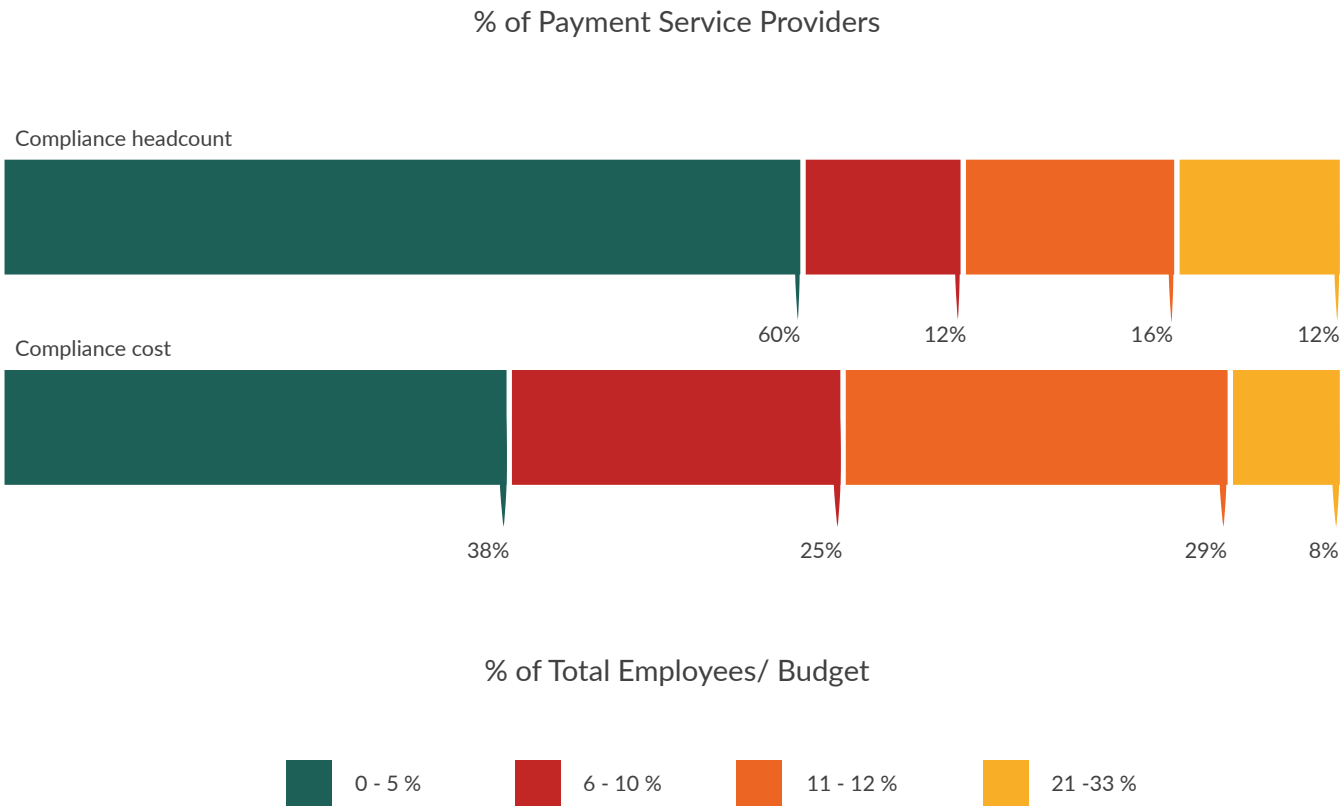
The biggest challenge for nearly all cryptocurrency payment service providers constitutes the difficulty of obtaining and maintaining relationships with banking institutions and money transfer operators (MTOs). Only companies that provide money transfer services (as defined by the taxonomy introduced before) indicate that the high cost of regulatory compliance poses the biggest challenge to their operations.

An interesting observation is that 'national currency-focused' money transfer services and B2B payment platforms are more concerned by exchange rate risk than 'cryptocurrency-focused' merchant services and general-purpose cryptocurrency platforms. An explanation could be that the latter often also operate a cryptocurrency exchange in addition to their payment activities that can be used to help manage exchange rate risk.

Of all payment categories, companies providing B2B payments are most concerned with competition from both FinTech firms and traditional MTOs, whereas entities providing merchant services and general-purpose cryptocurrency platforms show no particular concern with regards to these factors. Companies providing money transfer services seem to be slightly concerned by the competition from traditional MTOs.

Another interesting observation from a geographical perspective is that low liquidity in local currency markets is cited as the main challenge by Latin American payment service providers, whereas payment companies from all other regions are only moderately concerned about this factor. This could pose a significant challenge to companies using cryptocurrency systems as payment rails as they face difficulties converting cryptocurrencies back to national currencies.

Figure 78: Proportion of budget spent on compliance is higher than the proportion of employees working full-time on compliance

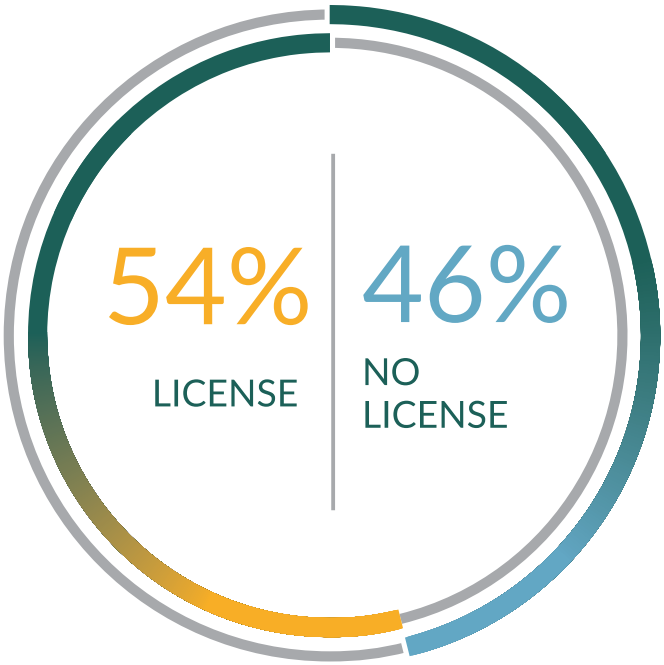



# REGULATION AND COMPLIANCE

**LICENSE**

54% of payment service providers surveyed have a formal government license or authorisation. While 86% of payment services providers based in North America and all payment companies from Africa and the Middle East hold a license, only 40% of Latin American payment companies have a license. The proportion of companies based in Asia-Pacific and Europe that have a license is approximately similar at 42% and 46%, respectively.

> Less than half of payment companies based in Asia-Pacific, Europe and Latin America hold a formal government license





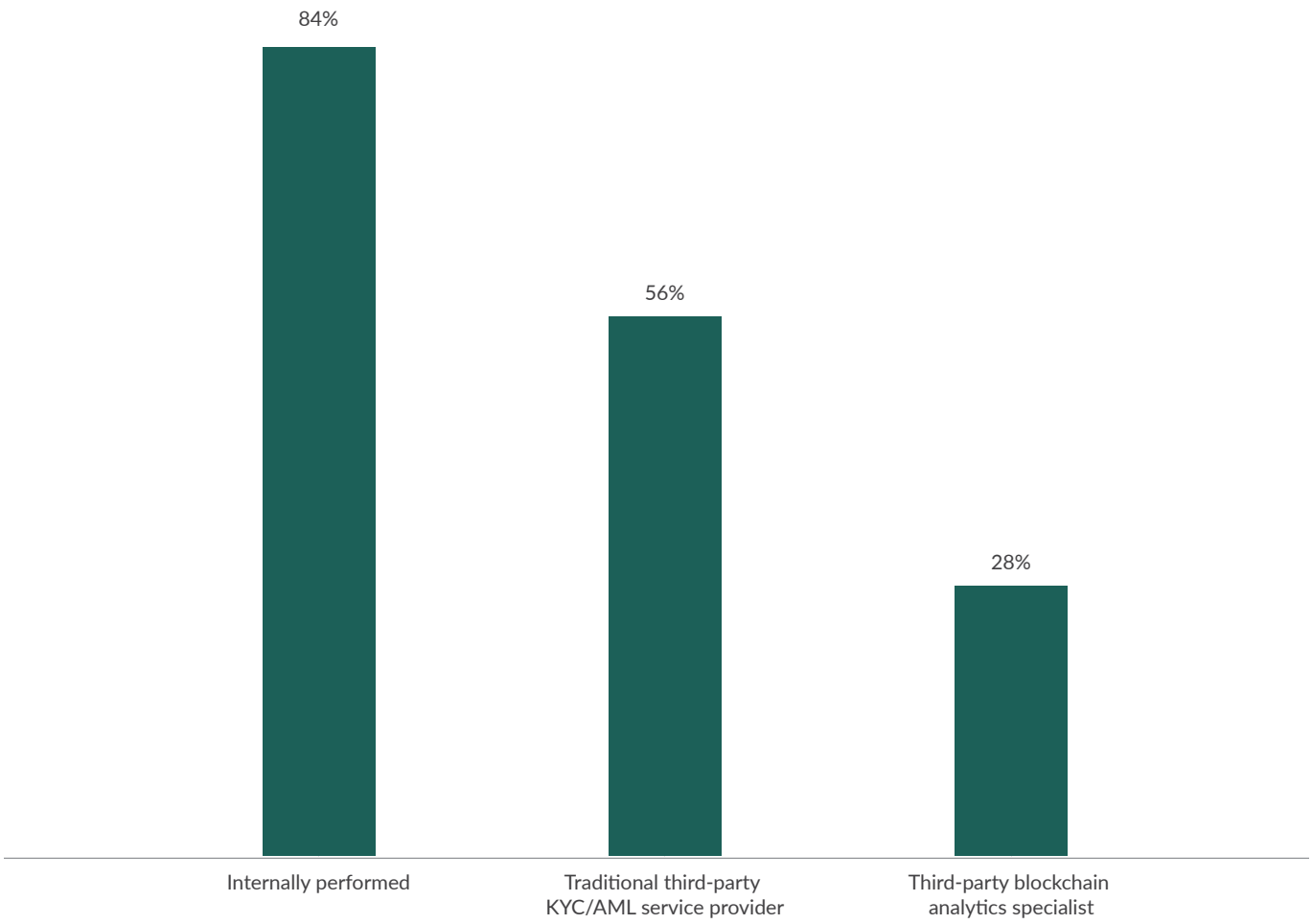
Findings show that companies providing B2B payment services are most likely to have a government license (83%), whereas companies providing merchant services are least likely to hold a license (52%).

### COMPLIANCE HEADCOUNT AND COST

Payment service providers have on average 8% of their total employees working full-time on compliance, and spend 12% of their total budget on compliance. Compliance headcount figures range from 0% to an upper limit of 33% of total employees, and compliance cost figures range from 0% to 30% of total budget.

60% of payment companies have between 0% and 5% of their headcount working full-time on compliance, but only 38% of payment service providers spend between 0% and 5% of their total budget on compliance (Figure 78). This suggests that a considerable number of payment service providers do not have employees working full-time on compliance, but spend a part of their budget on compliance.

Figure 79: Internal checks are the preferred KYC/AML method of payment service providers




### KYC/AML CHECKS

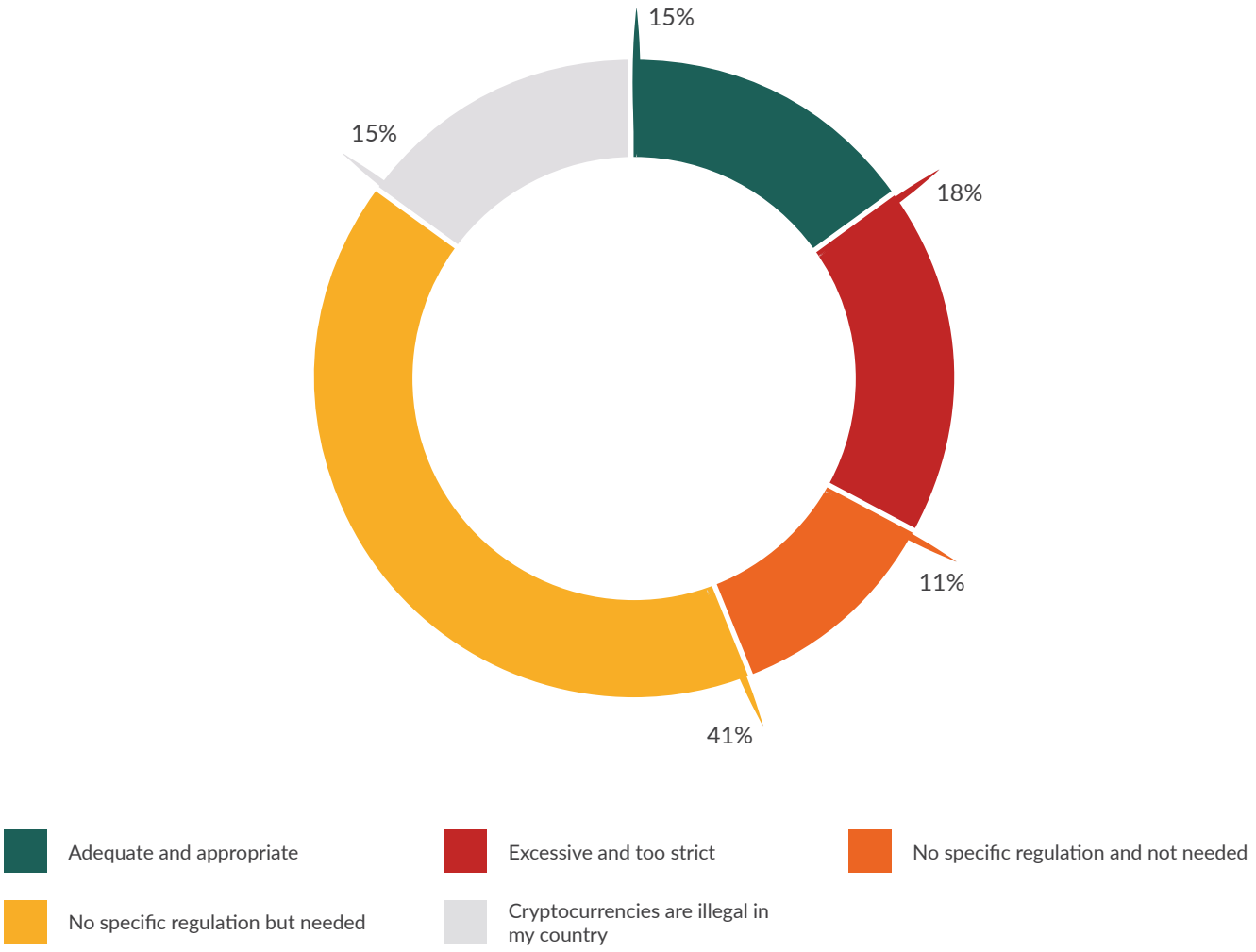
86% of payment service providers surveyed indicate that they are performing KYC and AML checks. Those that do not perform KYC/AML checks cited a variety of reasons for not doing so, which include some B2B payment platforms outsourcing KYC/AML requirements to business customers, and some cryptocurrency platforms not directly holding customer funds.

84% of payment service providers that perform KYC/AML checks do so internally, while 56% use the services of a traditional third-party provider (Figure 79). 28% of companies surveyed also use third-party blockchain analytics specialists who screen the blockchain to identify suspicious transactions. While 52% of payment companies use one of the listed methods, 28% use two methods and 20% use a combination of all three.

### CURRENT REGULATORY ENVIRONMENT

With regards to the current regulatory environment, a noteworthy observation is that over 40% of payment service providers perceive no existing regulations that specifically apply to cryptocurrencies and their activities, but would like to have more regulatory clarity (Figure 80). While 11% of payment companies state that they are satisfied with what they perceive as a lack of specific regulations, 15% deem

Figure 80: Payment service providers' perception of the current regulatory environment




existing regulations adequate and appropriate. However, 18% of payment service providers believe that the current regulatory environment is too strict, whereas 15% perceive cryptocurrencies to be illegal in their countries (mainly companies based in Asia-Pacific and Latin America).

From a geographical perspective, we observe that Latin American and Asian-Pacific companies are most concerned about the current regulatory environment (67% and 45%, respectively, would like to have more regulatory clarity with regards to their operations). 18% of both European and Asian-Pacific payment service providers deem existing regulations excessive and too strict. However, also 18% of payment companies based in these two regions are satisfied with the current regulatory environment. There is not enough data available for making a more detailed breakdown for Africa and the Middle East as well as for North America.

# KEY FINDINGS

**Governance and Operations**

- 70% of large miners rate their influence on protocol development as high or very high, compared to 51% of small miners
- Scaling cryptocurrency transaction capacity is cited by small and large miners alike as a significant concern
- 82% of large miners perform multiple mining value chain activities (e.g., pool operator, hardware manufacturing, etc.)
- 27% of large miners engage in three or more value chain activities, while all small miners specialise in a single activity
- Nearly three-quarters of all major mining pools are based in just two countries: 58% of mining pools with greater than 1% of the total bitcoin hash rate are based in China, followed by the US with 16%
- Mining pools are seeking to attract international users: all mining pools with greater than 1% of the total bitcoin hash rate offer an English language version of their website, and 63% have two or more language versions available

**Regulation/Policy**

- Only a small minority of miners believe that the negative environmental externalities from proof-of-work (PoW) mining are not an important issue; large miners in particular are aware of the environmental impact of their activities
- Overall, miners are not particularly concerned at present about legal and regulatory risk factors
- Regional differences can be observed with regards to how miners perceive the current regulatory environment: more than half of miners based in Asia-Pacific do not report any significant impact from regulation but would like to have more regulatory clarity, while the majority of North American and European miners seem to be satisfied with existing regulations (or the lack thereof)
- Tighter regulation to create barriers to mining and/or cryptocurrency adoption as well as increased taxation of mining profits are considered the highest regulatory risks by both small and large miners
- Small and large miners prefer cryptocurrency to be treated as commodity over currency for tax purposes, although a considerable proportion of miners are indifferent
- The vast majority of both small and large miners believe cryptocurrencies should be exempt from VAT

**Risk Management and Challenges**

- Small and individual miners are concerned that mining fees will not be able to compensate for decreasing block rewards in the long run; data shows that the proportion of transaction fees as a percentage of total bitcoin mining revenues have significantly increased in 2016, and are projected to reach 10% at the end of 2017
- Small miners are generally more concerned about operational risk factors than large miners
- The biggest concern for large miners is the fierce competition amongst miners of the same cryptocurrency, while small miners are most concerned by sudden large cryptocurrency price drops
- Total bitcoin mining revenues in 2016 have increased compared to 2015 despite the July 2016 bitcoin block reward halving
- Miners are worried about the centralisation of hashing power, as well as the centralisation of hashing power in a particular geographical area
- Centralisation of mining hardware manufacturing in particular geographical areas is not a major concern

Table 8: Taxonomy of mining industry actors and their activities

| Type of activities/actors | Description |
|---|---|
| Mining | Individuals and organisations using their own mining equipment to process transactions and earn the mining reward and transaction fees |
| Mining pool | Combines computational resources from multiple miners to increase the likelihood and frequency of finding a new block, and then distributes mining rewards among participating miners based on the proportion of contributed computational resources |
| Mining hardware manufacturing | Organisations designing and building specialised mining equipment |
| Cloud mining services | Organisations renting out hashing power to customers |
| Remote hosting services | Organisations hosting and maintaining customer-owned mining equipment |

# INTRODUCTION AND LANDSCAPE

### INTRODUCTION

Miners play a crucial role in any cryptocurrency system as they are responsible for grouping unconfirmed transactions into new blocks and adding them to the global ledger (the 'blockchain'). They provide the necessary computing power to secure a blockchain by computing vast numbers of hashes to find a valid block. Each valid block added by a miner to the blockchain generates a reward for the miner and makes it more difficult for an attacker to reorganise the ledger and double-spend already confirmed transactions.

### ACTIVITIES

Mining has grown from a simple hobby performed by early adopters on ordinary PCs into a capital-intensive industry that uses custom hardware equipment and features a specialised value chain, which can be summarised into five categories (Table 8).

Figure 81: The mining industry value chain

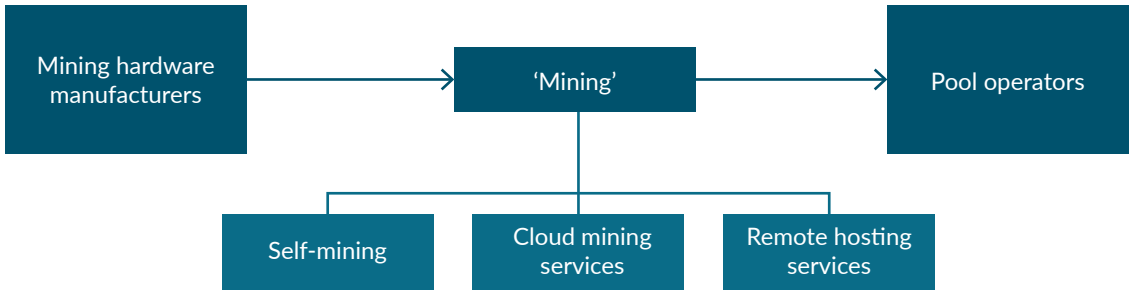
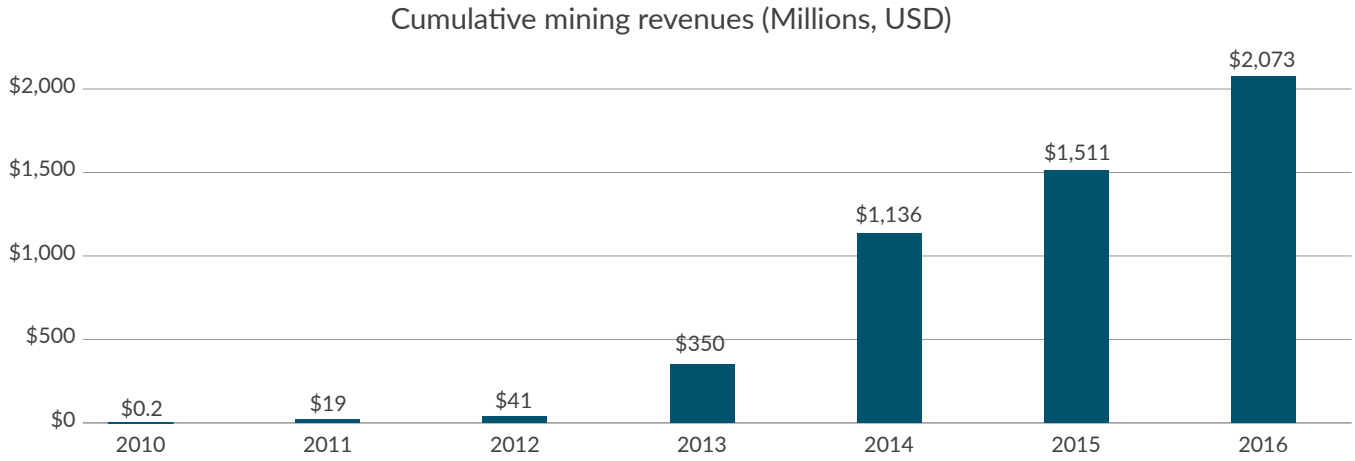



Figure 82: Cumulative bitcoin mining revenues (block rewards & transaction fees) if immediately converted to USD




*Data sourced from Blockchain.info*

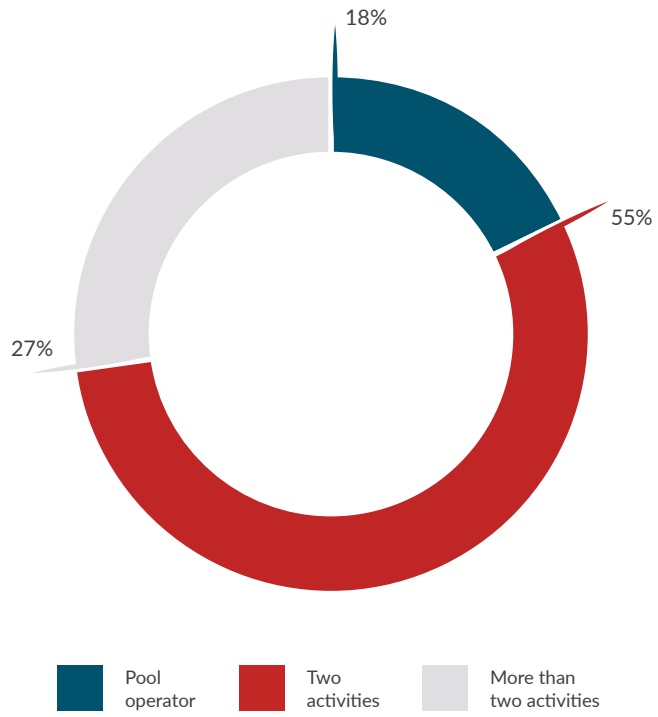
A BRIEF HISTORY OF CRYPTOCURRENCY MINING

As more computing power is added by miners, the difficulty of solving the 'puzzle' that allows miners to earn a reward increases. This led to the emergence of the first bitcoin mining pools in 2010, which apportion rewards across pool participants based on the share of computing power contributed to the pool by each miner. Coupled with the price increase and surge in general interest in cryptocurrencies, early adopters and engineers were incentivised to develop increasingly efficient mining hardware that vastly outperformed previous generations of mining equipment.[1] This led to further increases in the difficulty of solving the puzzle and accelerated an arms race amongst miners to use the cheapest energy sources and the most efficient equipment to keep operations profitable. Today, mining has become a competitive and resource-intensive industry that features its own value chain.

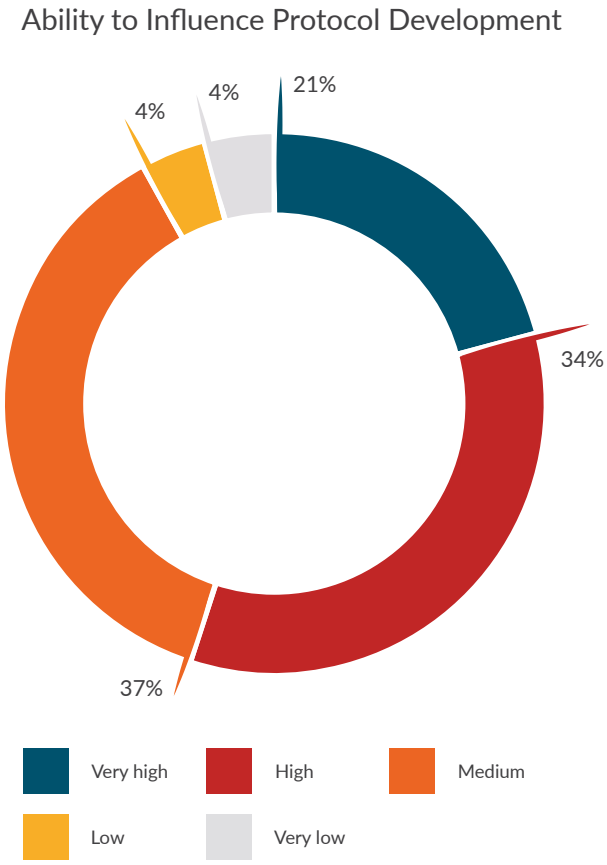
The mining value chain is depicted in Figure 81. A small number of large mining hardware manufacturers supply the industry with the newest and most efficient equipment. Remote hosting and cloud mining services have emerged to offer customers the possibility to participate in the mining process without having to run equipment themselves. Large mining organisations build and maintain vast mining facilities and data centres all over the world. Individual and corporate miners alike point their hashing power towards the mining pools of their choice to increase the likelihood and frequency of finding new blocks and 'smooth earnings'. Mining pools have become increasingly professionalised, with some offering customer support phone numbers and additional services to their customers.

Figure 82 shows that bitcoin miners alone have earned over $2 billion to date.[2] This further evidences the evolution of cryptocurrency mining from a hobby activity in the early days to a professional industry where large amounts of capital are at stake. It is worth noting that these figures do not include revenues generated from the sale of mining hardware

### Figure 83: Over 80% of large miners are performing multiple mining value chain activities




### Figure 84: Over half of miners consider their ability to influence protocol development to be high or very high



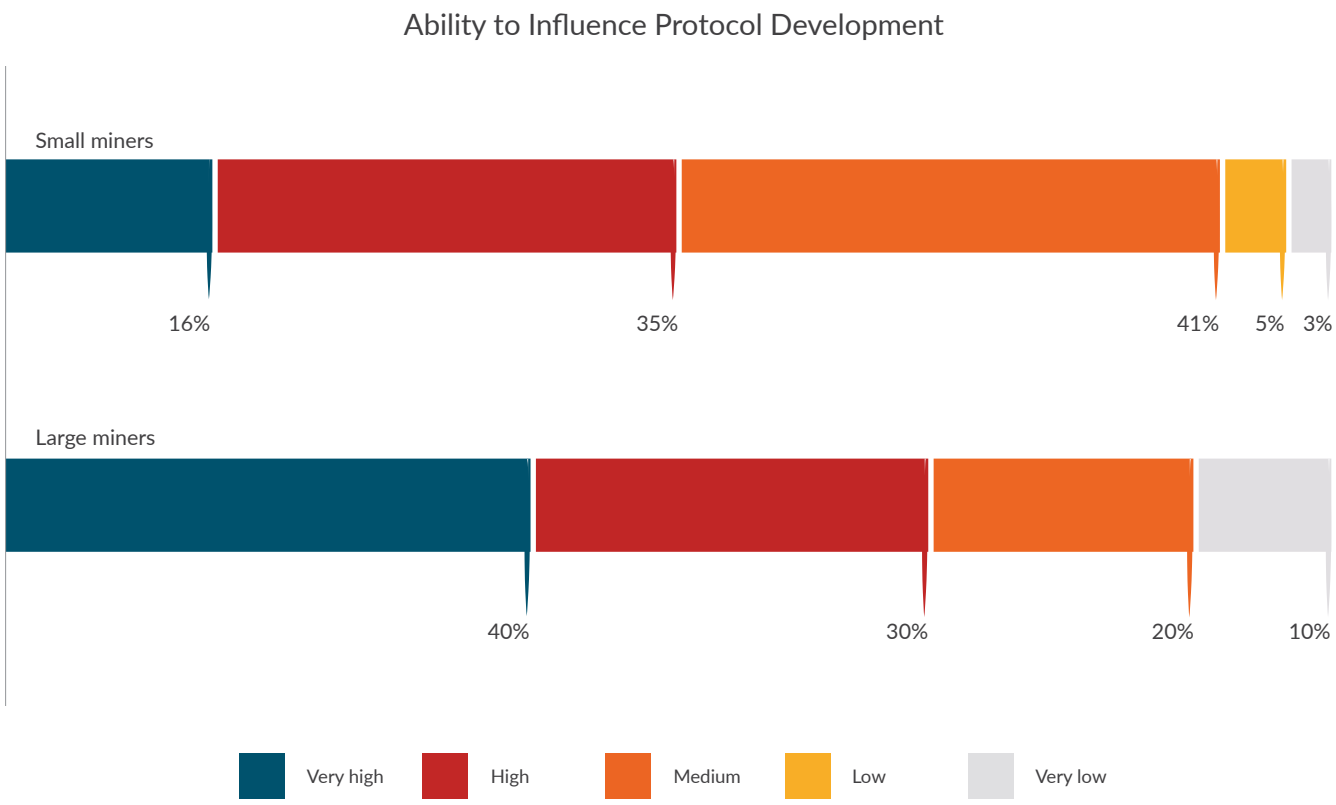

equipment, nor fee revenues generated from the provision of cloud mining and remote hosting services, or gains realized from bitcoin's price appreciation. As a result, the total revenues generated by all actors of the cryptocurrency mining industry are likely significantly higher.

The following figures are based on a sample of 48 miners that participated in our study. Of the 48 participants, 18 are mining organisations (38% of sample) and 30 are individual miners (62% of sample). For the purpose of this analysis, 11 participating organisations have been designated as 'large' mining organisations.[3] We estimate that the large mining organisations in this study cover over 50% of the total professional mining sector in terms of global hash rate as well as the scale of mining hardware manufacturing and cloud mining operations.

For the rest of this section, we will refer to small mining organisations as 'small miners' and large mining organisations as 'large miners'. The small miner category includes both small mining organisations which have a registered legal personality and individual miners operating as sole proprietors. While all small miners specialise in a single section of the mining value chain (running small mining facilities being the most common), large miners have a much more diversified range of activities and often perform multiple value chain activities: 82% of large miners surveyed are performing more than a single mining activity, and 27% are engaged in more than two activities (Figure 83).

Some large miners even cover the entire mining value chain by producing their own hardware, running their own pool and mining facilities, and providing additional services to individual customers. The 18% of large miners that are performing a single mining activity are all specialising in running mining pools.

Figure 85: Large miners believe they have a much greater ability to influence protocol development than small miners




THE POLITICS OF MINING

Over time, more and more miners have connected to mining pools, meaning that pool operators largely decide which transactions to include in a new block. Mining pool operators also hold considerable power in terms of which protocol rules they want to support by running preferred client implementations. However, full nodes (and especially 'economically relevant' full nodes run by major cryptocurrency businesses) ensure that only valid blocks as defined by the protocol implementation they are running are added to the blockchain. This means that if a miner runs a protocol implementation that enforces different rules than the majority of full nodes, the latter may reject the blocks produced by such miners. This may result in a scenario of two incompatible networks in which there is one chain backed by a considerable amount of computing power but not accepted by the 'economic majority', and a second chain that is considered valid by the 'economic majority' but not backed by as much computing power as before the chain 'fork'.[4]

## INFLUENCE ON PROTOCOL DEVELOPMENT

We asked survey participants about how they perceive their ability to influence protocol development (Figure 84). Although more than half believe that their decision power is high or very high, nearly 40% of miners indicate that they think they only have medium influence on protocol development.

We can observe differences in perceptions between small and large miners, with large miners not surprisingly rating their influence higher than small miners: 40% of large miners rate their influence over protocol development as very high, compared to only 16% of small miners (Figure 85). In contrast, 41% of small miners consider themselves to only have medium influence on protocol development.

## Table 9: Mining pool market share - evolution of average hash rate distribution of major mining pools in 2016

| Mining pools | Q1 2016 | Q2 2016 | Q3 2016 | Q4 2016 |
|---|---|---|---|---|
| AntPool | 26% | 26% | 21% | 23% |
| F2Pool | 25% | 26% | 23% | 20% |
| BTCC Pool | 15% | 14% | 15% | 13% |
| BitFury | 14% | 10% | 11% | 10% |
| BW.com | 7% | 11% | 16% | 13% |
| Slush Pool | 4% | 5% | 7% | 8% |
| KnCMiner | 4% | 4% | 2% | Closed |
| BitClub Network | 3% | 3% | 4% | 4% |
| GHash.io | 1% | <1% | <1% | Closed |
| Eligius | 1% | <1% | <1% | <1% |
| Telco 214 | <1% | 1% | 1% | <1% |
| ViaBTC | - | - | Launched | 3% |
| HaoBTC/Bixin | - | - | Launched | 3% |
| BTC.com | - | - | Launched | 3% |

*Data sourced from BitcoinChain*[5]

### MINING POOLS

Mining is a very competitive industry characterised by the frequent entry of new mining pools and the exit of previously successful pools. The 'market share' of mining pools is generally calculated as the number of blocks mined divided by total number of blocks found during a specific period.[6] There are a number of organisations that have established themselves as leading pools that occupy a dominant position in the industry, although it appears that mining has become more distributed in 2016 with the entry of new pools that have taken some of the large players' market share (Table 9).

Looking at the geographic distribution of the major mining pools, nearly three-quarters of all major mining pools are based in just two countries, China and the US. 58% of mining pools are based in China, followed by the US with 16% (Figure 86).

The location of the mining pool operator does not necessarily coincide with the location of miners contributing computing power to the pool: individual miners and organisations can easily switch between different mining pools, making pool location largely unimportant. In fact, all major mining pool websites have an English version and 74% have a Chinese version (Figure 87). Moreover, 63% of mining pools have two or more languages available on their website, which suggests that their customer base is international and not limited to domestic miners.

Figure 86: More than half of the major mining pools are based in China

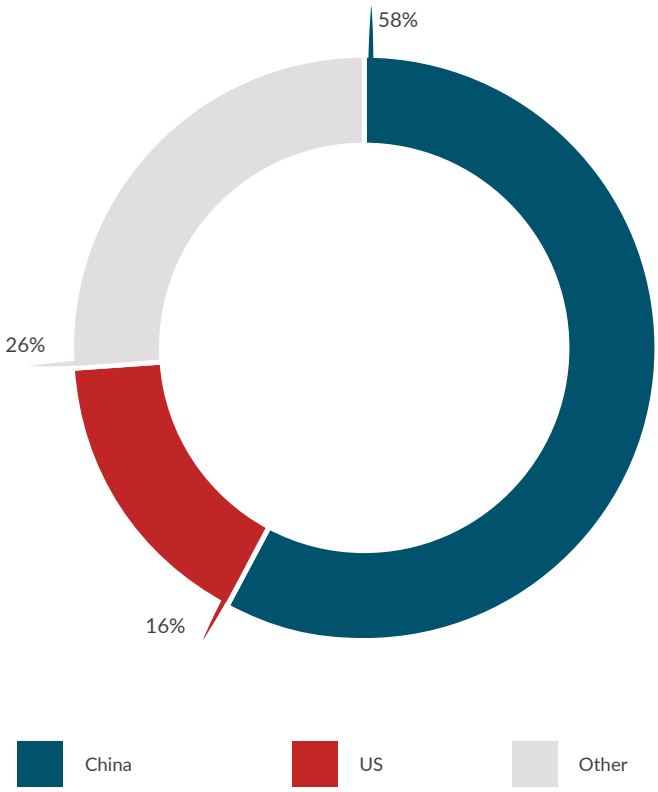
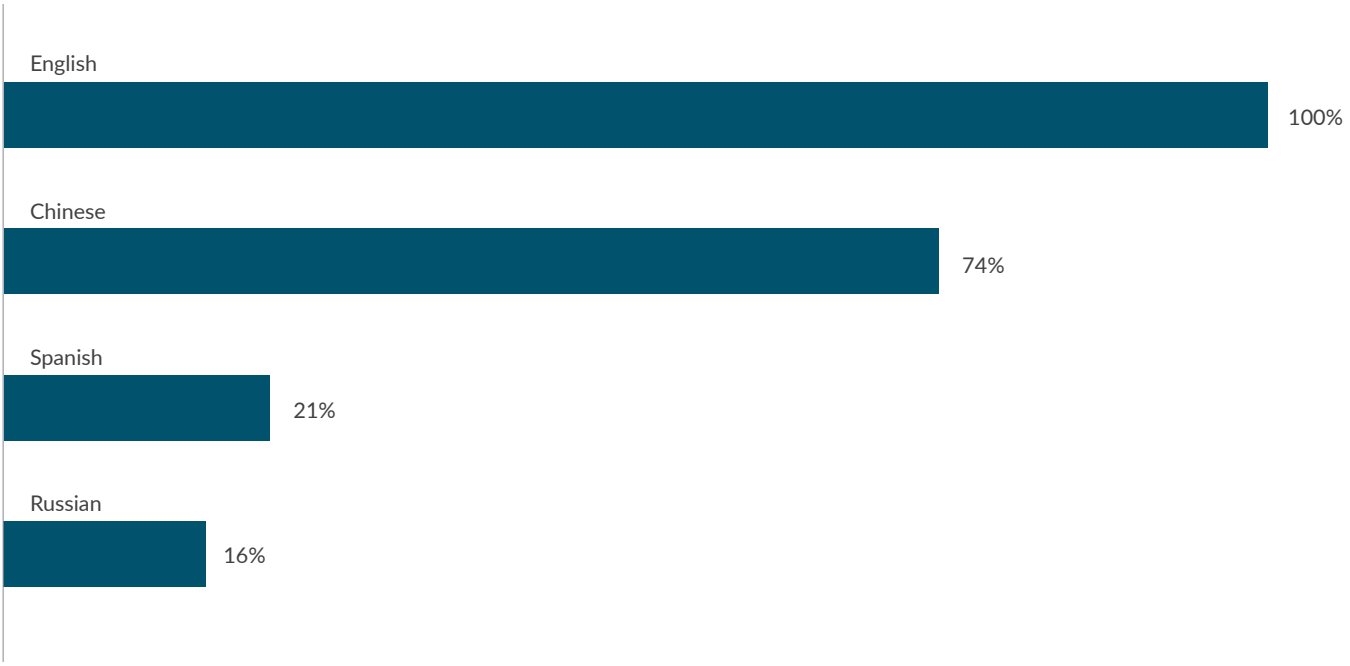



Figure 87: Most commonly available languages on major mining pool websites



## MINING FACILITIES

Determining where to set up a cryptocurrency mining facility is generally based on three key factors: miners need to have access to low-cost electricity to run their operations profitably, they need to have a sufficiently fast internet connection to quickly receive and broadcast data with other nodes on the network, and mining equipment must be kept from overheating to function optimally, which is why locations that have low temperature zones offer substantial advantages as cooling costs can be kept low.

The cryptocurrency mining map in Figure 88 shows that mining facilities are mainly concentrated in locations where most of the key drivers discussed above are satisfied.[7] Mining facilities are primarily located in North America, Northern and Eastern Europe as well as in China. In fact, China is the country that hosts most mining facilities and uses the highest power consumption of all countries for cryptocurrency mining. A zoom into China shows that mining facilities are concentrated in remote areas where both electricity and land are very cheap. A significant concentration can be observed in the Sichuan province, where miners have struck deals with local hydroelectric power stations to access cheap electricity.

The cryptocurrency mining map shows an estimate of the location of medium-to-large scale mining operations around the globe.[8] We were able to map mining facilities consuming a total of 288 megawatts (MW) to power cryptocurrency (mainly bitcoin) mining.

However, as a substantial fraction of the cryptocurrency mining capacity is not reported and the location of many mining facilities across the globe are kept secret, the 288MW figure should be considered as a lower-bound. Using a bottom-up approach that takes into account the current network hash rate (close to 4,000 Petahashes/second) and assuming that all miners are using the most efficient hardware in the most efficient setting, it can be estimated that at least 462MW are consistently being consumed to secure Bitcoin's blockchain alone.[9] This would mean that Figure 88 captures the origin of more than half of the entire bitcoin hash rate.[10]

Figure 88: Global Cryptocurrency Mining Map

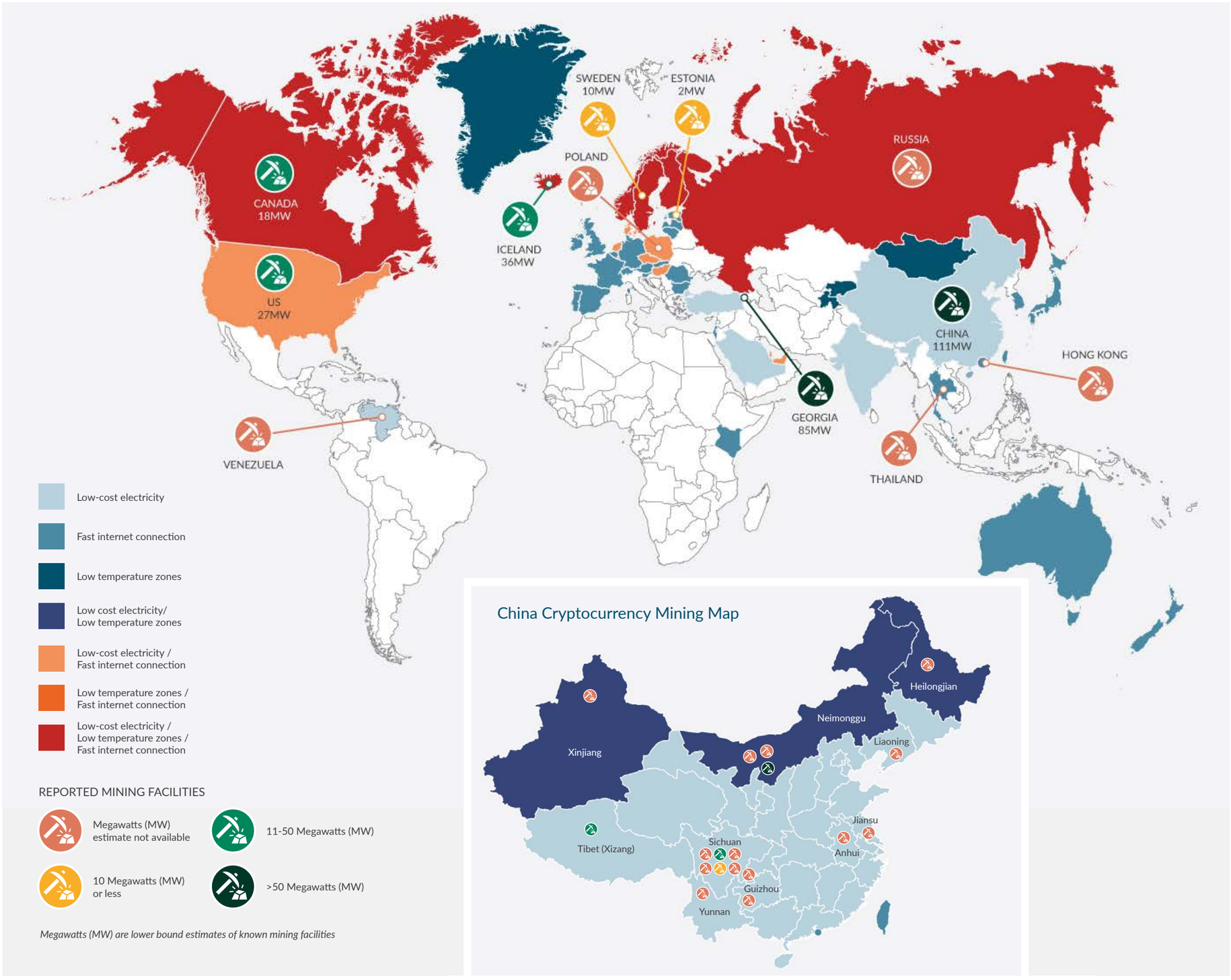
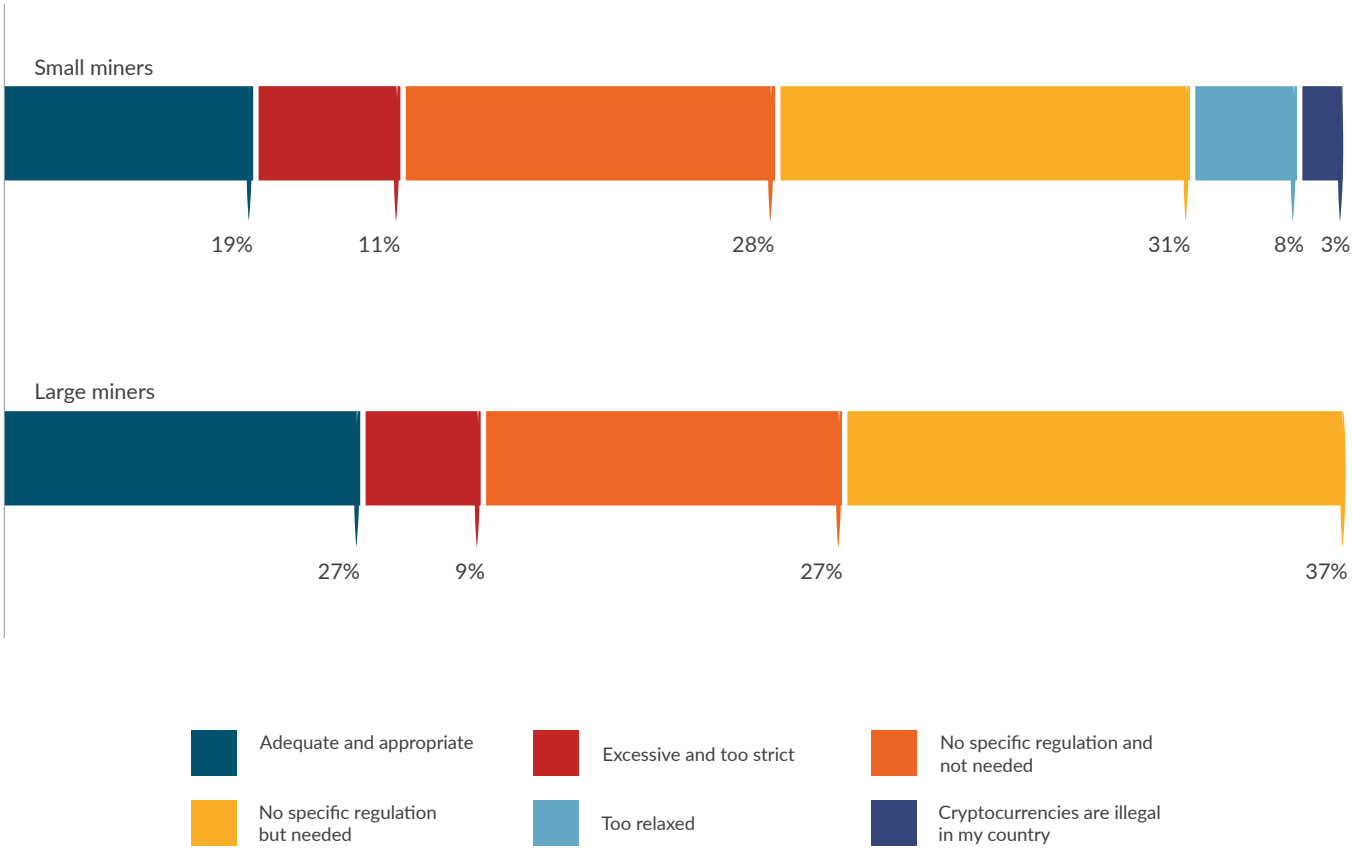


Figure 89: No significant differences can be observed between small and large miners with regards to how they perceive the current regulatory environment




# REGULATION AND POLICY

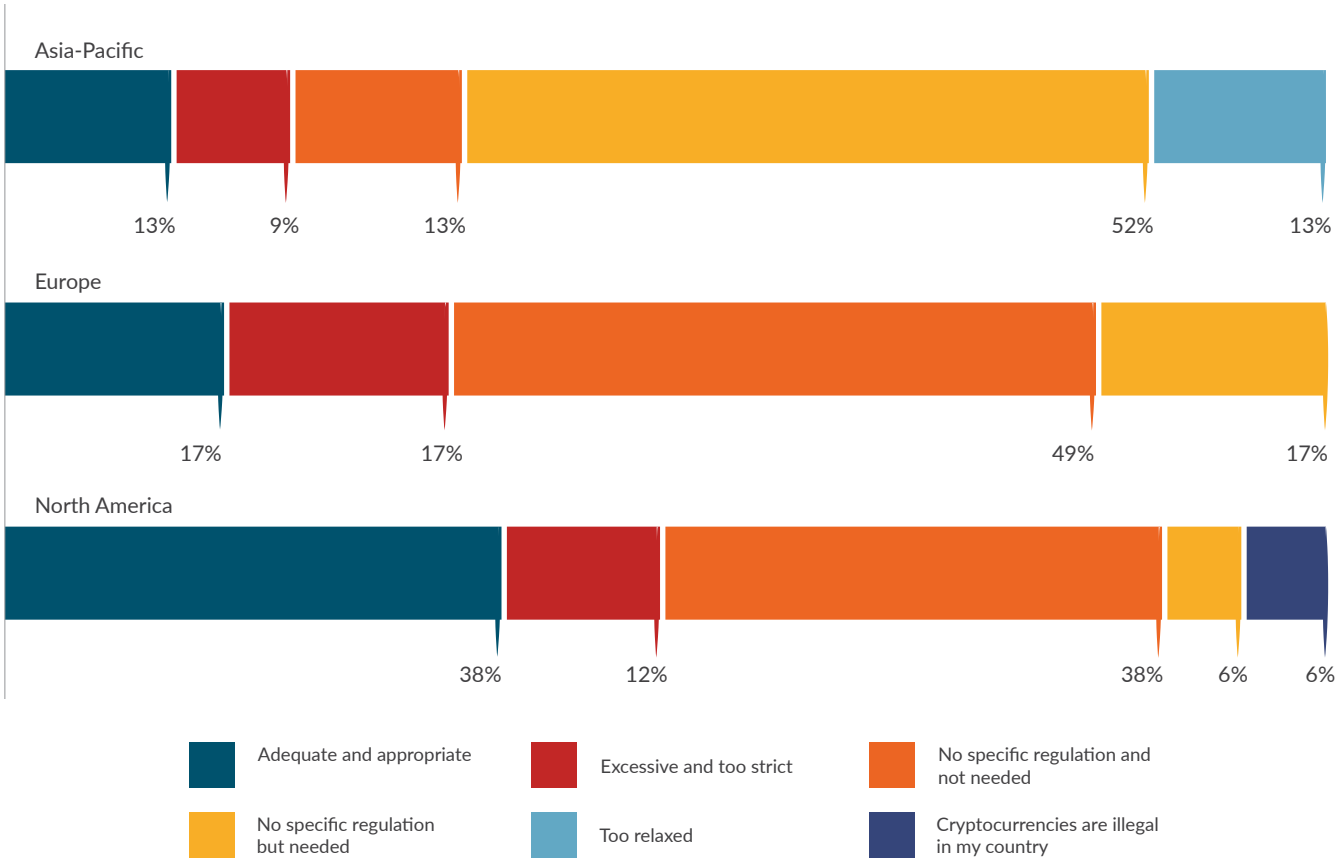
### TAX TREATMENT

87% of small miners and 90% of large miners state that cryptocurrencies should be exempt from value-added tax (VAT). While nearly all miners (both small/individual and large) based in Europe, North and Latin America indicate that no VAT should be applied to cryptocurrencies, 21% of small/individual miners and 17% of large miners based in Asia-Pacific believe it should.

> The vast majority of both individual and corporate miners believe cryptocurrencies should be exempt from VAT

We asked miners whether cryptocurrencies should be treated as currencies or as commodities for tax purposes, and responses varied between individuals, small miners and large miners, and across different world regions. One observation that stands out is that nearly 60% of Asian-Pacific individual miners are indifferent. In contrast, a slight majority of individual miners from other regions indicate they would like to see cryptocurrencies being treated as currencies for tax purposes. Asian-Pacific individual miners that are not indifferent would

Figure 90: Majority of European and North American miners are satisfied with existing regulations or the lack thereof




prefer cryptocurrencies to be treated as commodities for tax purposes.

For mining organisations, the picture looks different: 29% of large miners and one third of small miners are indifferent. Those who are not indifferent, however, favour the commodity tax treatment over the currency tax treatment, and no significant differences between world regions can be observed.

Overall, findings show that a considerable number of miners seem to be indifferent as to how cryptocurrencies should treated for tax purposes, but that individual miners who are not indifferent would like to see cryptocurrencies being treated as currencies for tax purposes (except Asian-Pacific individuals who prefer the commodity option), as opposed to both small and large miners who prefer the commodity tax treatment.

> Both small and large miners prefer cryptocurrencies to be treated as commodity over currency for tax purposes; a significant number of miners are indifferent

### CURRENT REGULATORY ENVIRONMENT

Miners are divided with regards to how they perceive the current regulatory environment (Figure 99). There are no substantial differences between small and large miners, except that 27% of large miners deem current regulations adequate and appropriate compared to only 19% of small miners.

However, significant regional differences can be observed when combining all miners together.[11] In Asia-Pacific (and China specifically), more than half of miners are concerned about what they perceive as a lack of specific cryptocurrency-related regulations, and would like to see more regulatory clarity (Figure 90). In contrast, the majority of European and North American miners seem to be satisfied either with existing regulations or the lack thereof.

## Table 10: Legal/regulatory risk factors rated by miners

Respondents Scored these Categories on a 1 - 5 Scale

1: Very low risk | 2: Low risk | 3: Medium risk | 4: High risk | 5: Very high risk

Lowest average score — Highest average score

| | Weighted average | Small miners | Large miners |
|---|---|---|---|
| Tighter regulation to create barriers to mining and/or cryptocurrency adoption | **3.00** | 3.09 | 2.73 |
| Increased taxation of mining profits | **2.98** | 3.03 | 2.82 |
| Government ban of cryptocurrencies | **2.55** | 2.81 | 1.73 |
| Energy price hikes targeted at miners | **2.57** | 2.67 | 2.27 |
| Seizure of mining facilities | **2.48** | 2.60 | 2.09 |
| Mining becoming money transmission service | **2.40** | 2.50 | 2.09 |

38% of North American miners perceive existing regulations to be adequate compared to only 17% of European miners, whereas nearly half of European miners perceive no existing regulations and believe that they are not needed, as opposed to 38% of North American miners. Only a minor proportion of miners deem existing regulations excessive and too strict, a sentiment that is most prominent in Europe. 13% of miners based in Asia-Pacific indicate that they perceive existing regulations as too relaxed, while 6% of miners based in North America perceive cryptocurrencies to be illegal (all being small miners).

### LEGAL/REGULATORY RISKS AND CHALLENGES

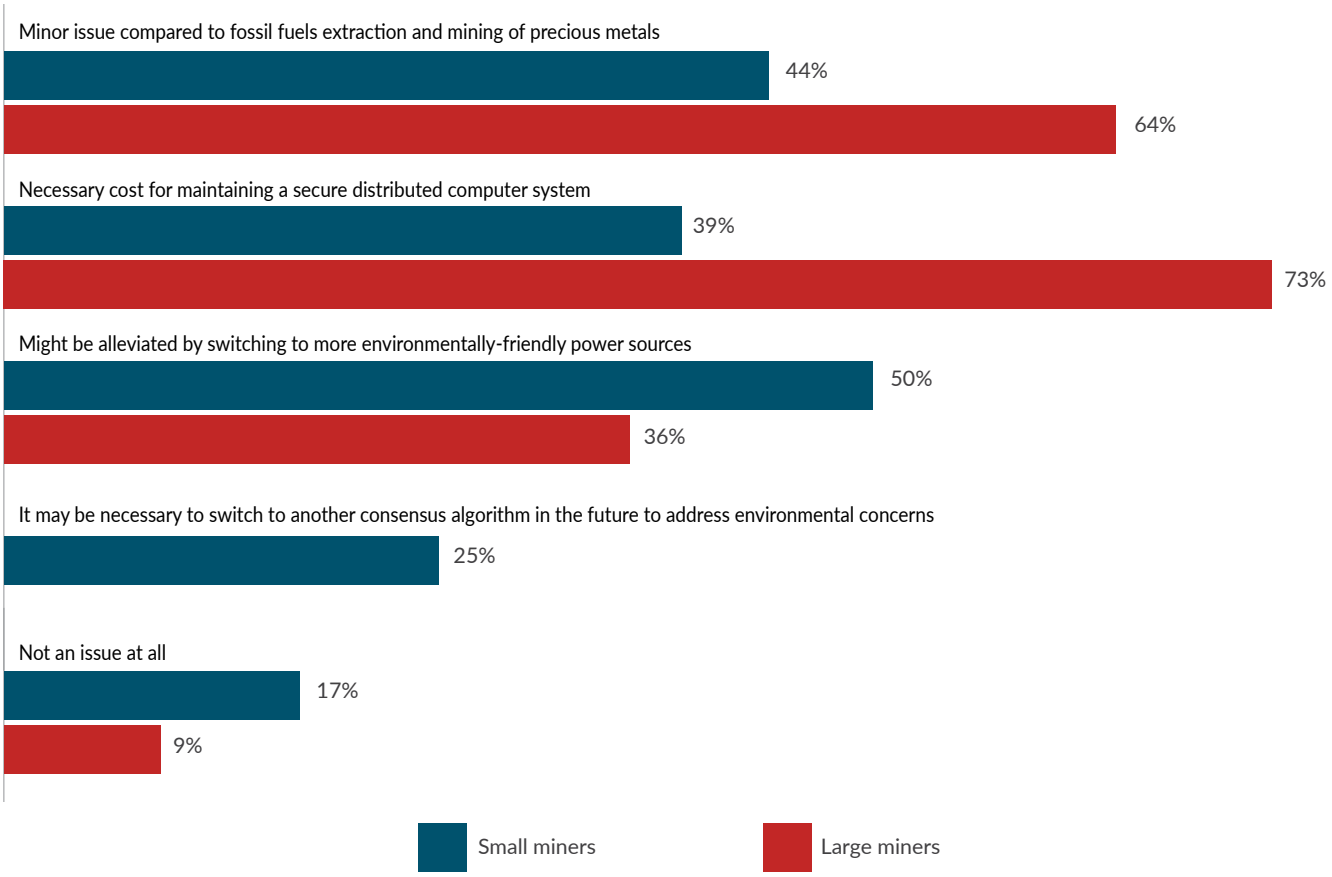
Survey participants were presented with a list containing various legal and regulatory challenges that the mining industry may be facing, and asked to rate them (Table 10). In general, it appears that miners are not particularly concerned at present about potential legal and regulatory risk factors, as weighted average ratings merely range from low to medium risk. It is worth noting that small miners (including individuals) rate risk factors consistently higher than large miners.

The two highest ranked factors by both small and large miners are the possibility that governments will increase taxes on mining profits, as well as the potential introduction of tighter regulations that create barriers to either mining and/or cryptocurrency adoption in general. Large miners are least worried about a potential government ban of cryptocurrencies, a scenario that small miners rate as third highest risk factor. Miners are not concerned about mining becoming a money transmission service, which would require them to hold a money transmission license.

> Tighter regulation to create barriers to mining/cryptocurrency adoption and increased taxation of mining profits are considered the highest regulatory risks by both small and large miners

There are geographical differences as well: in general, large miners based in Asia-Pacific and North America are

Figure 91: Negative environmental externalities of proof-of-work (PoW) algorithm are recognised by the mining industry




considerably less concerned about legal and regulatory risk factors than large miners from Europe and Latin America. With regards to small miners, the opposite is true: miners based in North American and Asia-Pacific tend to be more concerned about legal risks and challenges than small miners from Europe and Latin America.

Interestingly, the two highest ranked risk factors are inversely correlated: small miners based in Asia-Pacific consider a government ban of cryptocurrencies as well as the seizure of mining facilities to be the highest risks, whereas small miners from North American rank these as lowest risks. At the same time, small miners based in North America believe increased taxation of mining profits to be the highest risk factor, while this is the factor that small miners from Asia-Pacific are least concerned about.

## ENVIRONMENTAL EXTERNALITIES OF PROOF-OF-WORK ALGORITHM

Most cryptocurrency systems are currently using an energy-intensive proof-of-work (PoW) algorithm that serves as a lottery to determine which miner gets the right to add his block to the blockchain and earn a reward. When mining difficulty rises a larger amount of electricity is required to generate a valid PoW. As a reference, it is estimated that Bitcoin alone currently consumes about 10.41 TWh per year, which is close to the yearly energy consumption of Uruguay, a country with 3.3 million inhabitants.[12]

The large energy footprint of PoW cryptocurrency systems has attracted criticism for 'wasting' electricity to perform 'useless' calculations. Proponents, however, argue that this is a necessary cost for maintaining a secure, distributed computer system. In fact, 39% of small miners and 73% of large miners state that the benefits of having a secure distributed computer network outweigh the environmental costs (Figure 91). Similarly, 44% of small miners and 64% of large miners believe that cryptocurrency mining represents a minor issue when compared to the environmental damage caused by the extraction of fossil fuels and the mining of precious metals.

Half of small miners believe that the negative environmental effects from PoW mining could be alleviated by using more environmentally-friendly power sources such as hydroelectric and solar power, an opinion that is shared by 36% of large miners. An interesting observation is that a quarter of small miners are open to the possibility of switching to another, less energy-intensive consensus algorithm in the future – no large miner agrees with this statement, though. Changes to the consensus algorithm may lead to a loss of investment in mining equipment that is specifically designed to only perform the calculations required by the current PoW algorithm.

## Large miners in particular are aware of the environmental impact of their activities

Findings show that only a minority of miners think that the negative environmental externalities from PoW mining do not constitute an issue at all. Small and large miners alike have commented that they are thinking about ways to reduce mining's significant carbon footprint, although for now most agree that this is a minor concern compared to other challenges that cryptocurrency systems currently face. It should be noted that several energy companies are leveraging energy overcapacities in some regions in China (often from coal plants and hydroelectric dams that had been built to supply large industrial projects that never materialised) to mine cryptocurrencies in order to prevent energy from getting entirely wasted.[13]

Table 11: Operational risk factors and challenges rated by miners

Respondents Scored these Categories on a 1 - 5 Scale

1: Very low risk | 2: Low risk | 3: Medium risk | 4: High risk | 5: Very high risk

Lowest average score — Highest average score

| | Weighted average | Small miners | Large miners |
|---|---|---|---|
| Sudden large price drop (e.g., 25%) | **3.30** | 3.40 | 3.00 |
| Fierce competition among miners of the same cryptocurrency (constant arms race) | **3.20** | 3.17 | 3.30 |
| Insufficient availability of capital to continually replace/upgrade mining infrastructure | **3.00** | 3.20 | 2.30 |
| Unexpected market-driven increase in electricity costs | **2.98** | 3.00 | 2.90 |
| Regularly scheduled reductions in block rewards | **2.89** | 2.94 | 2.70 |
| Cyber attacks (e.g., DDoS) | **2.83** | 2.77 | 3.00 |
| Lack of immediate availability of state-of-the-art mining hardware | **2.82** | 2.94 | 2.40 |
| Natural disasters (e.g., flooding, lightning) | **2.50** | 2.50 | 2.50 |
| Competition with other cryptocurrencies than the one(s) they mine | **2.30** | 2.56 | 1.60 |
| Unexpected change to protocol (e.g., change away from SHA-265) | **2.30** | 2.52 | 1.64 |

# OPERATIONAL CHALLENGES

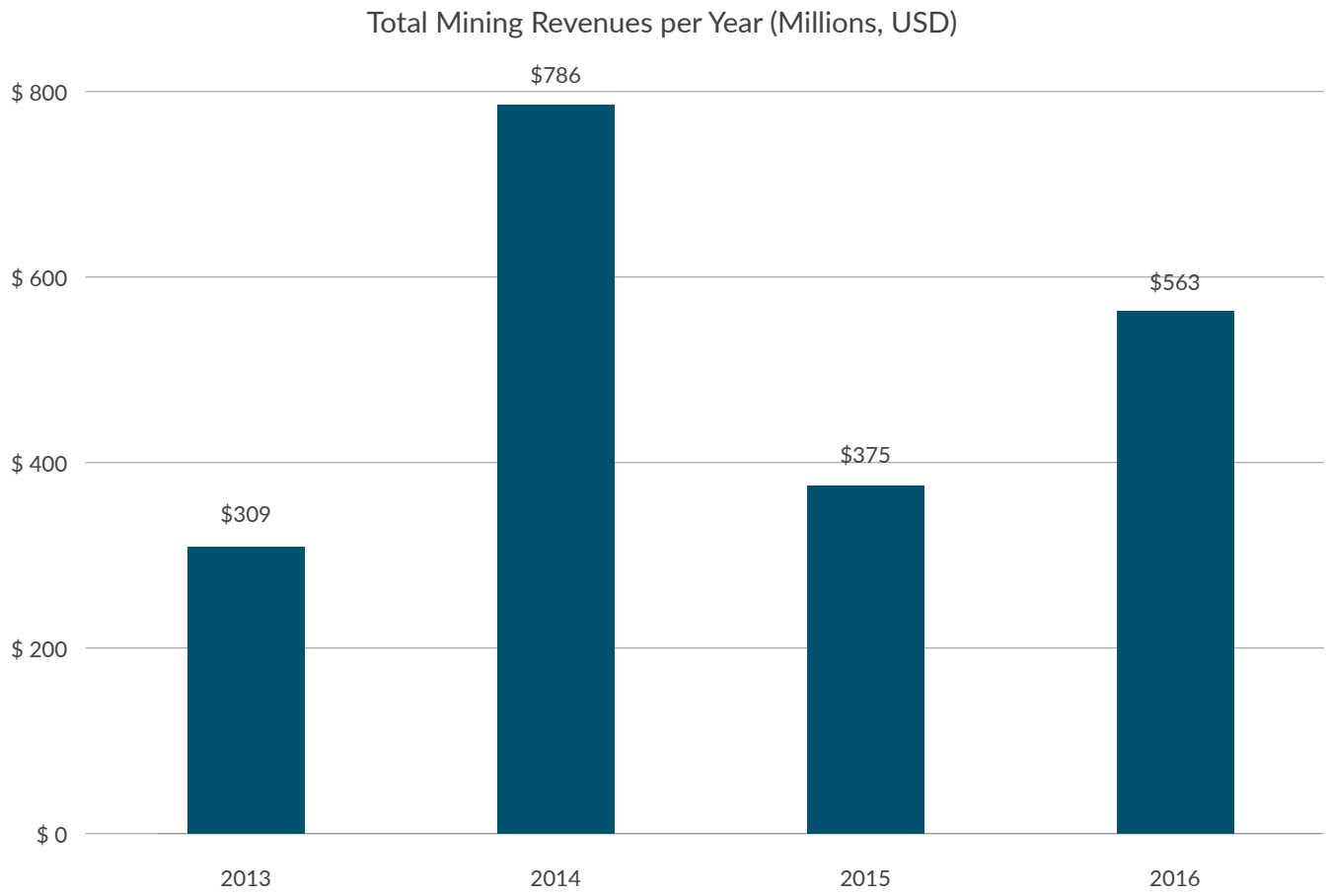
### OPERATIONAL RISK FACTORS

There are a variety of factors that can have a negative impact on both the operational functioning and the profitability of mining activities. Participating miners were presented with a list of potential risk factors that they were asked to rate according to the risk that they might pose to miners' daily operations (Table 11). Findings show that small miners tend to rate operational risk factors slightly higher than large miners, but in some cases there are divergences as well.

One noteworthy observation is that large miners consider the fierce competition among miners of the same cryptocurrency to pose the highest risk to their operations, while small miners deem a sudden large price drop of the cryptocurrency they are mining a higher risk than the constant arms race between miners.

> The fierce competition among miners of the same cryptocurrency poses the highest risk to large miners, whereas small miners are more concerned about sudden large price drops

Figure 92: Total bitcoin mining revenues per year (block reward + transaction fees) if immediately converted to USD




*Data sourced from Blockchain.info*

The largest discrepancy between small and large miners can be observed with regards to the insufficient availability of capital that is needed to continually upgrade and/or replace mining equipment: this poses a major risk to small miners, while large miners tend to have sufficient capital available to invest in their mining infrastructure.

Large miners appear to run the risk of getting attacked more often than small miners (e.g., DDoS attacks against mining servers). They rate an unexpected change to the protocol (e.g., changing the current PoW algorithm so that their equipment will be worthless) as well as the competition with other cryptocurrencies than the ones they mine considerably lower than small miners. Natural disasters do not pose a major risk to both small and large mining operations.

There are regional differences as well: North American and Latin American miners tend to rate risk factors lower than Asian-Pacific and European miners. One interesting observation is that there are no major regional differences in terms of the risk of not immediately having access to the latest state-of-the-art mining equipment, although small miners from Asian-Pacific rate this factor higher than miners from other regions. This suggests that the location of mining hardware manufacturers (the majority are based in China) is not a crucial issue at present.

## North and Latin American miners tend to rate operational risk factors lower than miners based in Asia-Pacific and Europe

The regularly scheduled reductions in cryptocurrency mining rewards (e.g., Bitcoin's reward halving that occurs roughly every four years) are considered a 'medium' risk by both small and large miners, probably because these events are well known in advance and preparations can be taken to smooth the transition. When comparing total bitcoin mining revenues per year, we can observe that they have been higher in 2016 compared to 2015 despite the block reward being reduced from 25BTC to 12.5BTC in July 2016 (Figure 92).[14]

## Table 12: Level of concern regarding general challenges affecting the cryptocurrency industry

Respondents Scored these Categories on a 1 - 5 Scale

1: Not concerned at all 2: Concerned 3: Moderately concerned 4: Highly concerned 5: Extremely concerned

Lowest average score — Highest average score

| | Weighted average | Small miners | Large miners |
|---|---|---|---|
| Centralisation of hashing power in the hands of a few (control) | **3.77** | 3.89 | 3.30 |
| Centralisation of hashing power in a particular geographical area (location) | **3.59** | 3.70 | 3.11 |
| Scaling | **3.41** | 3.44 | 3.30 |
| Mining fees not compensating for decreasing block rewards in the long run | **3.17** | 3.41 | 2.22 |
| Centralisation of mining equipment production in a particular geographical area | **3.09** | 3.35 | 2.10 |
| Implementation bugs in mining firmware/ hardware | **2.98** | 3.11 | 2.55 |
| Design bugs/weaknesses at the protocol level | **2.83** | 2.92 | 2.55 |
| Lack of liquidity in cryptocurrency markets | **2.57** | 2.72 | 2.09 |

### VIEWPOINTS

In addition to purely operational risk factors, we also asked participating miners to rate a number of higher-level issues that in most cases also apply to the cryptocurrency industry as a whole (Table 12). Again, it can be observed that small miners are generally more concerned than large miners with regards to the listed factors.

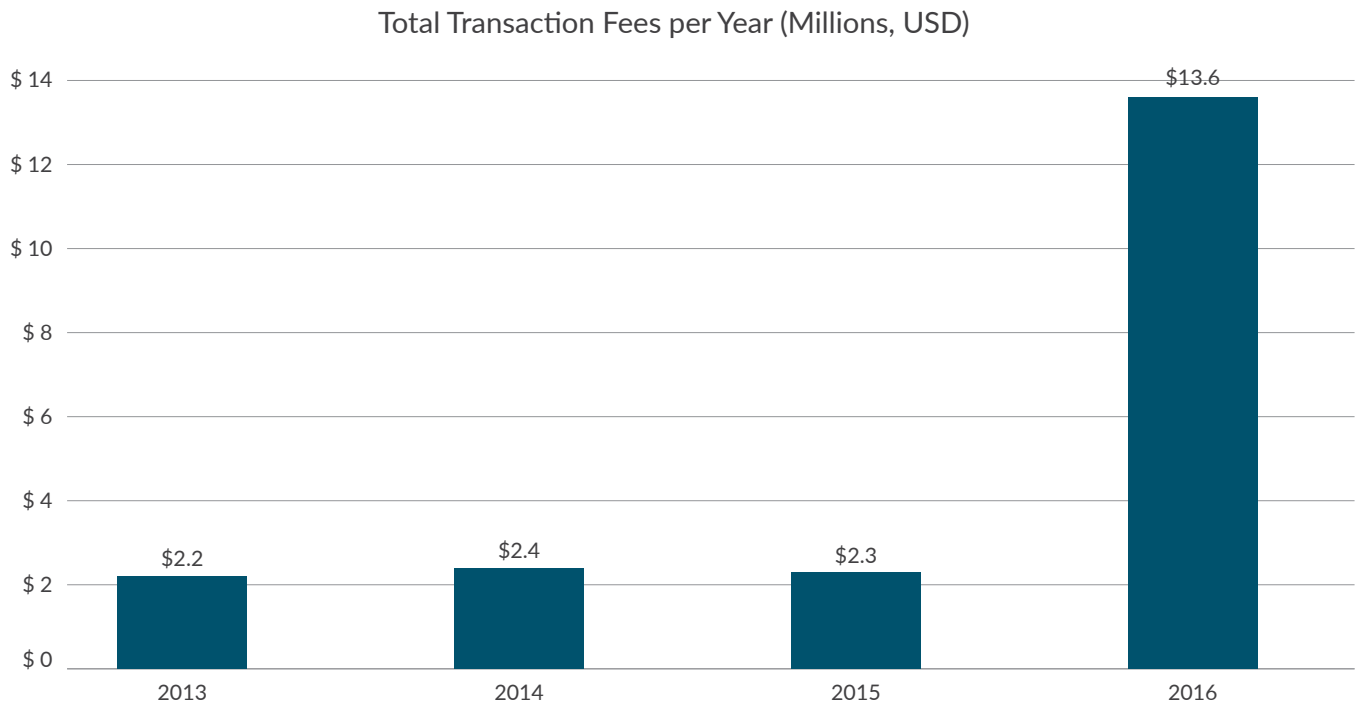
One of the main concerns in any PoW-based cryptocurrency system is the potential centralisation of hashing power that could effectively undermine the censorship-resistance property that is considered an essential feature of many cryptocurrencies. In essence, there are three different types of potential mining centralisation that are rated differently by participating miners.

As expected, the centralisation of hashing power in the hands of a small number of pool operators is the highest ranked factor, followed by the centralisation of hashing power in particular geographical areas.[15] An interesting observation is that miners are less worried about the centralisation of mining hardware manufacturing within a particular geographical area, although a substantial difference between small and large miners can be observed with regards to the level of concern. Miners based in Europe as well as North and Latin America appear to be more worried about the three types of centralisation than Asian-Pacific miners.

> Of the three potential types of mining centralisation (control of hashing power, location of hashing power, and location of mining equipment manufacturing), miners are least concerned about the last

Implementation bugs in mining hardware and firmware are slightly more of a concern to miners than design weaknesses at the protocol level. The latter would constitute a major debacle to the entire cryptocurrency industry and system depending on the severity of the bug, but is less likely to happen thanks to the thorough codebase review of numerous developers.

Figure 93: Total bitcoin transaction fees have significantly increased in 2016




*Data sourced from Blockchain.info*

On average, miners are not much concerned about the lack of liquidity in cryptocurrency markets (used to convert their minted cryptocurrency for national currencies to fund operations), but significant regional differences between small miners can be observed: small miners from North America and Europe seem to be able to easily convert their mined cryptocurrencies to national currencies, but small miners based in Asia-Pacific are concerned about apparently illiquid cryptocurrency markets in their region.

A major concern of both small and large miners is the debate about how a cryptocurrency system should scale, and what methods should be used. This is exemplified by the smouldering block size debate that sees opposing camps advocating different scaling solutions and effectively stalls any significant protocol update. Moreover, small miners are concerned that mining fees will not be able to compensate for decreasing block rewards in the long run. However, transaction fees are becoming a growing source of revenue for miners. While transaction fees have been low for most of Bitcoin's life cycle, they have significantly increased in 2016 (Figure 93).

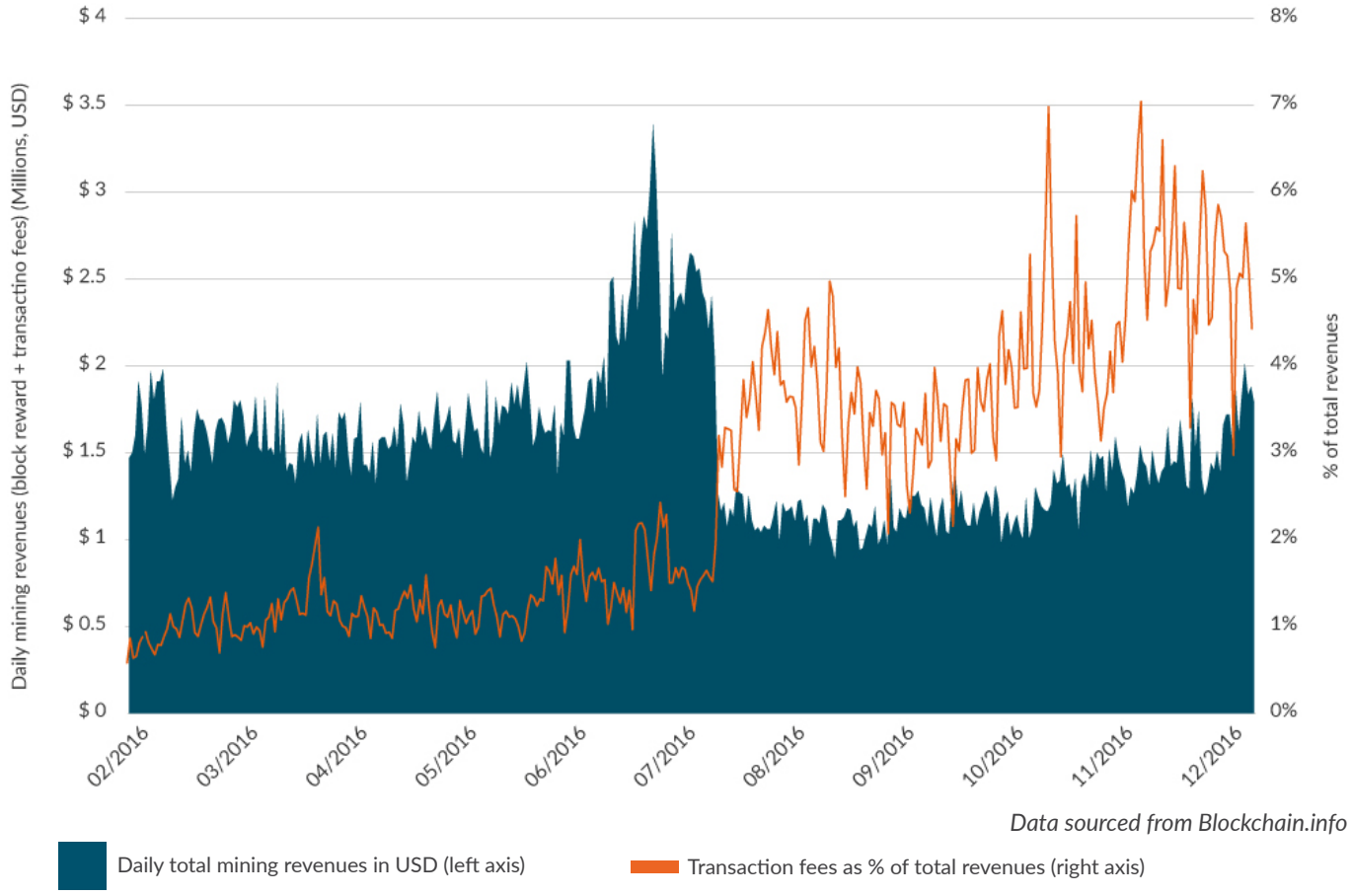
Transaction fees have historically represented only a very small proportion of total bitcoin mining revenues: on average, they constituted 0.63% of total mining revenues from 2013-2015. However, after the bitcoin block reward halving event in July 2016, transaction fees have increased over three times as a proportion of total mining revenues, which indicates that transaction fees are increasing more than what would have been expected solely as a consequence from the block reward halving (Figure 94).

## The unsolved matter of how to scale transaction capacity is cited as a major concern by both small and large miners

The major surge in transaction fees is also likely a result of the increasing number of daily transactions competing to be included in a block whose size is limited to 1MB, which is the most contentious issue of the scaling debate. Based on current growth figures, bitcoin transaction fees are projected to constitute nearly 10% of total mining revenues at the end of 2017 (Figure 95).

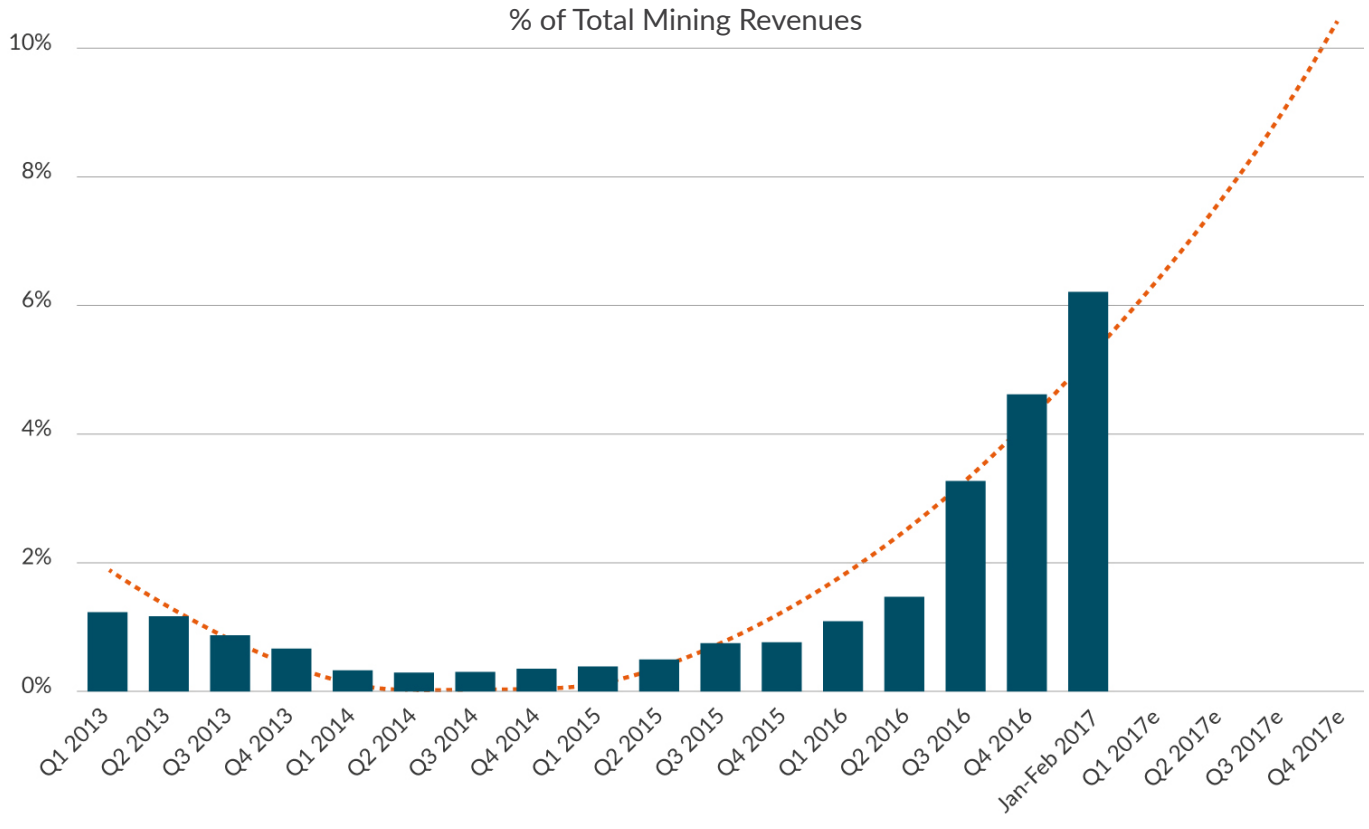
While this poses significant challenges to cryptocurrency payment companies and users who perform a considerable number of on-chain transactions, the emergence of a fee market might be necessary to maintain bitcoin's security model in the long run. As block rewards decrease miners will need to have economic incentives in order to continue providing hashing power to secure the system.

Figure 94: Growth in the proportion of bitcoin transaction fees as a % of total mining revenues




*Data sourced from Blockchain.info*

Figure 95: Transaction fees as a % of total bitcoin mining revenues are rising




*Data sourced from Blockchain.info*

# APPENDICES

## APPENDIX A: BRIEF INTRODUCTION TO CRYPTOCURRENCIES

**CONCEPT**

Cryptocurrencies are the result of a combination of multiple achievements in various disciplines that include, but are not limited to computer science (P2P networking), cryptography (cryptographic hash functions, digital signatures) and economics (game theory).

In short, a cryptocurrency is a digital token that exists within a specific cryptocurrency system which generally consists of a P2P network, a consensus mechanism and a public key infrastructure. There is no central authority that governs the system; instead the rules governing the system (e.g., defining what constitutes a valid transaction, specifying the total supply of the digital token and its issuance scheme, etc.) are enforced by all network participants (also called 'nodes'). The entire transaction history can be independently verified by each node as everyone has a copy of the shared ledger. This shared ledger, generally taking the form of a chain of blocks comprised of transactions ('blockchain'), is constantly updated via a process called 'mining', through which new units of the native token (i.e., the cryptocurrency) are created. Anybody is free to join and leave the system at any time, and there are no identities attached to users.[1]

Table 13: Key properties of cryptocurrencies

| Property | Description |
|---|---|
| Digital bearer asset | User who controls the private key owns the cryptocurrency, which can be used as a *speculative asset* as well as a *medium of exchange*. Funds cannot be seized and transactions cannot be censored. |
| Integrated payment network | Generally offers fast, cheap, global and irreversible payments. |
| Non-monetary use cases | Enable use cases that go beyond currency and assets, and provide them in a decentralised, censorship-resistant manner without a central authority. |

The main property of a reasonably decentralised cryptocurrency is that the native token constitutes a censorship-resistant, digital bearer asset (Table 13). It is a *bearer asset* in the sense that the person who controls the respective private key controls the particular amount of cryptocurrency associated with the corresponding public key, and *censorship-resistant* in the sense that, in theory, nobody can freeze or confiscate cryptocurrency funds nor censor transactions performed on the integrated payment network.[2]

As cryptocurrency systems are not bound to a particular location or jurisdiction, the integrated payment network has a global reach and can be used to transfer funds within a short time (ranging from seconds to several minutes depending on a variety of factors) all over the world.[3] In general, transactions fees are substantially lower than fees charged by traditional payment network operators, and fees are not based on the amount transferred, but generally on the transaction size measured in bytes. This means that a multi-million dollar transaction can be processed for the same fee as a $1

transaction. As a result, cryptocurrency systems can be used for cost-effective micropayments.[4] Payments are irreversible once funds have been transferred and received enough confirmations. This poses significant advantages for merchants as they can benefit from lower fees and avoid chargebacks. In addition, no personally identifiable information such as contact details, credit card numbers and passwords need to be stored on insecure servers that can be subject to security breaches, as users are only identified by their cryptocurrency address derived from the public key.

Finally, some cryptocurrency systems have additional properties and functionality that enable non-monetary use cases that go beyond digital assets and currencies. Bitcoin, for example, can be used as an immutable data store by embedding specific metadata (usually in the form of hashes) into transactions that carry special meaning outside of the bitcoin network and can serve as a decentralised timestamping service. This mechanism also enables the creation of 'overlay networks' or 'embedded consensus systems' that are built on top of the core network and have distinct functionality and use cases, often featuring their own native token or cryptocurrency (*dApp tokens*). Some cryptocurrency systems have also been developed with the explicit aim of enabling specific non-monetary use cases (e.g., a decentralised domain name registry, a decentralised computing platform, etc.). These systems use a native cryptocurrency primarily as a monetary incentive for participants to keep the system running.

# APPENDIX B: THE CRYPTOCURRENCY INDUSTRY

**EMERGENCE OF A BUSINESS ECOSYSTEM/INDUSTRY**

For each of the properties and value propositions introduced in Table 13 in appendix A, a multitude of projects and companies have emerged to provide services that facilitate the use of cryptocurrencies for mainstream users and take advantage of the innate properties of the systems that power them. A cryptocurrency ecosystem has emerged that is composed of a diverse set of actors ranging from volunteering developers, academics, non-profit and media organisations to registered companies, among others. This study primarily focuses on the evolving *business ecosystem* that features economic actors providing products, services and applications that involve the use of cryptocurrency.

Initially, a cryptocurrency exists in a vacuum; a closed system that has no connections to other systems (e.g., other cryptocurrency systems, traditional finance, the real economy). In order to participate, users need to start mining in order to earn the cryptocurrency, which can only be used for transacting with users of the same system as there is no way to spend or sell them.

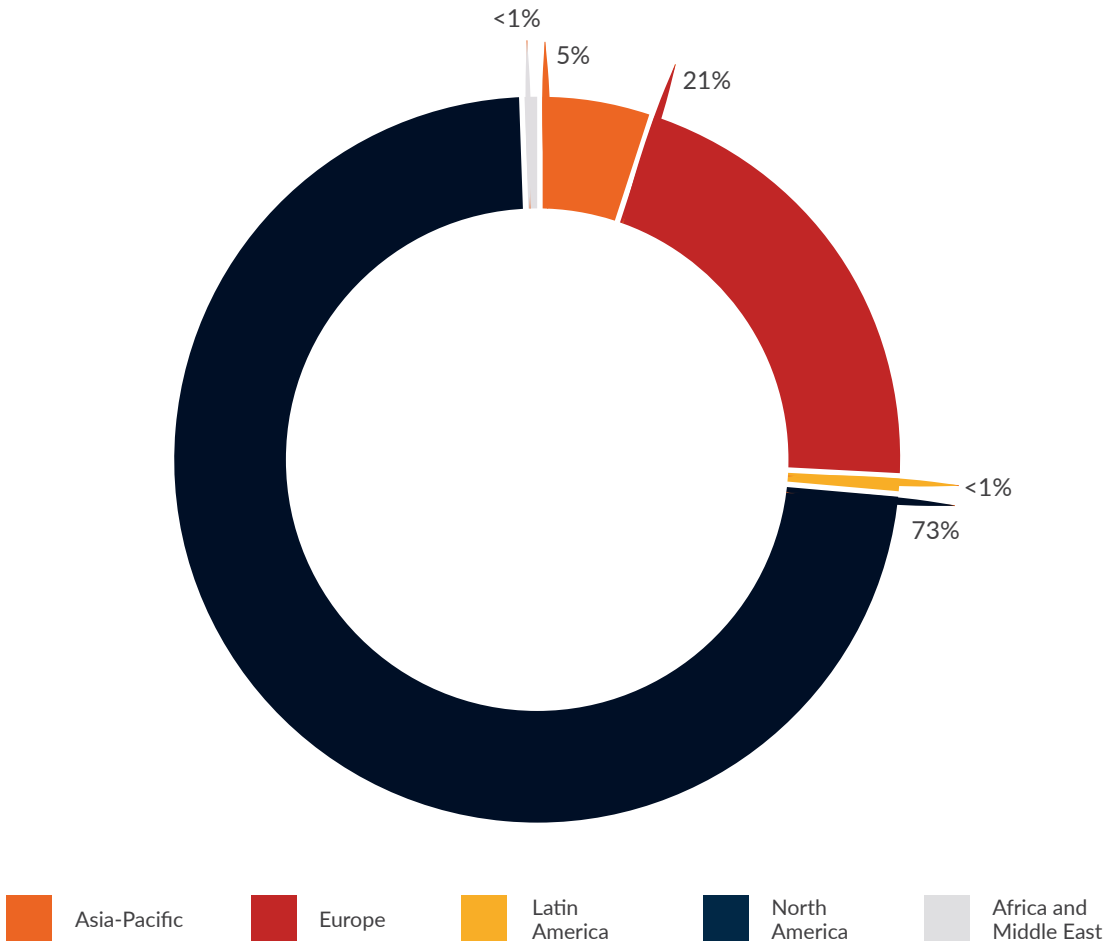
To counter this, exchanges are established that let users trade cryptocurrency for other cryptocurrency and/or national currencies. As a result, a price can be established for these tokens and they become *digital assets* that have a certain value. Exchanges provide on-off ramps for new users to join the system and thereby opening up the initially closed system by connecting it to traditional finance. With increasing transaction volumes, merchants begin accepting cryptocurrency as a payment method, thus making the token a *medium of exchange*. Payment companies that emerge to help merchants facilitate cryptocurrency payments and reduce exposure to price volatility, act as gateways and provide bridges between cryptocurrencies and the global economy.

> Cryptocurrency industry actors build interfaces between cryptocurrency systems, traditional finance and the global economy, thereby establishing and boosting the value of the cryptocurrency

In parallel, a variety of actors emerge to provide supporting services, such as data services (e.g., block explorers, market data sites), media and consulting. Moreover, projects emerge that build complex overlay networks on top of existing cryptocurrency systems and expand the utility of these systems by enabling non-monetary use cases. Fuller-featured cryptocurrency platforms are launched to remove the inherent complexities of using cryptocurrency and make it easier for mainstream users to use cryptocurrencies. The sheer range of projects, activities, products, services and applications in the cryptocurrency industry make it difficult to comprehensively catalogue everything taking place.

> The cryptocurrency industry builds the infrastructure and services to make cryptocurrencies more accessible to mainstream users

Figure 96: Bitcoin ATM share by region




*Data provided by CoinATMRadar*

# APPENDIX C: THE GEOGRAPHICAL DISPERSION OF CRYPTOCURRENCY USERS

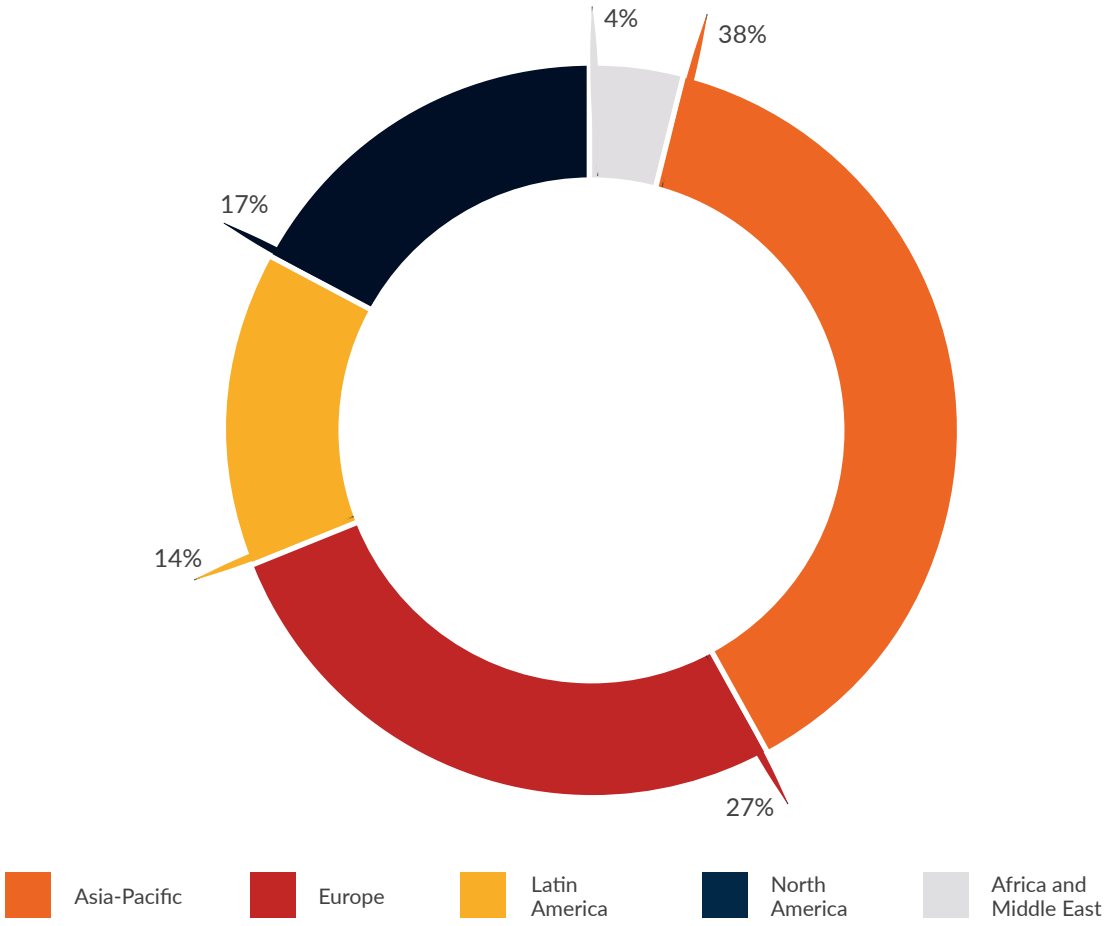
Establishing an exact picture of where cryptocurrencies are used and in which countries the level of activity is highest constitutes a challenging if not impossible task. A lot of cryptocurrency companies and platforms do not share user data for a variety of reasons, including protecting user privacy, or the nature of their services prevents the collection of location-based data (e.g., wallet providers that offer software downloads and do not require users to sign up for the service). However, various public resources are available that if combined can contribute to providing a rough estimate of where most activity is taking place.

One indication of activity can be drawn from LocalBitcoin volumes, a P2P exchange platform that connects users in 249 countries and lets them meet in person or electronically exchange cryptocurrencies. While volumes are small compared to large exchanges, they are reaching all-time highs since early 2017 and provide an indicator of where interest in cryptocurrencies is growing. Volumes have experienced particularly high growth in emerging countries located in Asia (China, India, Malaysia, Thailand), Latin America (Brazil, Chile, Colombia, Mexico, Venezuela), Africa and the Middle East (Kenya, Nigeria, Saudi Arabia, Tanzania, Turkey) and Eastern Europe (Russia and Ukraine).[5]

Looking at the geographic distribution of bitcoin and other cryptocurrency ATMs, it turns out that 94% of all publicly known ATMs are based in North America and Europe, with the US and Canada having a total share of 59% and 15% of all ATMs, respectively (Figure 96). Africa and the Middle East as well as Latin America host less than 1% of worldwide cryptocurrency ATMs.

According to Coinmap, a website listing nearly 9,000 known venues across the world that accept cryptocurrencies, a significant concentration of merchants can be observed in North America and especially Europe.[6] Some activity can also

Figure 97: Cryptocurrency user share by region (based on combined wallet and payment provider data)




be observed in the Asia-Pacific region (mostly concentrated in South Korea, Japan and Australia), Latin America (mainly Brazil and Argentina) and Africa and the Middle East (notably in Kenya, South Africa, and Israel). However, it should be noted that only a minority of the more than 100,000 merchants accepting cryptocurrency worldwide are represented on Coinmap.

Running a full node is another measure of where activity is taking place. Looking at the distribution of bitcoin full nodes over a time window of one year, we can observe that the US has the highest number of full node operators of all countries.[7] From a regional perspective, node figures are in-line with the merchant figures as the majority of full nodes are run in North America and Europe, with some activity being observed in other regions. However, it should be noted that the origin of a full node can be obfuscated.

Finally, based on user data obtained from some participating incorporated wallet providers and payment platforms, we can break down customer share by world region. It turns out that nearly 40% of cryptocurrency users are based in the Asia-Pacific region, followed by Europe with 27% (Figure 97). The share of North American users is surprisingly low and not in-line with the above mentioned figures. However, it should be noted that these figures only represent data from a limited number of wallet providers and payment platforms, and do not take into account users from exchanges as well as mining pools. In addition, figures are not weighted by the number of users as these are mostly secret and/or difficult to establish given the type of service that the respective companies are providing.

In conclusion, it appears that cryptocurrency adoption is most advanced in North America and Europe, but an increasing number of activity (and users) can be observed in other regions as well, with activity growing relatively quickly in some emerging countries in Asia, Latin America, and Africa and the Middle East.

# ENDNOTES

## ACKNOWLEDGMENTS

[1] Some study participants prefer not to disclose their participation.

## SETTING THE SCENE

[1] Data site *CoinMarketCap* lists 579 cryptocurrencies that have a market capitalisation above $1,000 (available at https://coinmarketcap.com/all/views/all/; accessed: 22 March 2017). *CryptoCoinCharts* has indexed 4,077 cryptocurrencies, of which many are unclear to still exist (available at http://www.cryptocoincharts.info/coins/info; accessed: 22 March 2017).

[2] For example, under this definition Ethereum Classic can be considered an altcoin as well, as it offers no substantial improvement over the original cryptocurrency system its source code is based on (Ethereum).

[3] Available at: https://coin.dance/stats/marketcaphistorical (Accessed: 24 March 2017).

[4] 'dApp' is short for *decentralised application*.

[5] Available at: https://coinmarketcap.com/historical (Accessed: 24 March 2017).

[6] Available at https://www.cryptocompare.com/coins (Accessed: 24 March 2017).

[7] Available at: https://coin.dance/nodes/unlimited (Accessed: 24 March 2017).

[8] Bitcoin transaction data available at: https://blockchain.info/en/charts/n-transactions; Ethereum transaction data available at: https://etherscan.io/chart/tx; DASH transaction data available at: https://chainz.cryptoid.info/dash/#!overview; Monero transaction data available at: http://moneroblocks.info/stats/transactions/m/34; Litecoin transaction data available at: https://chainz.cryptoid.info/ltc/#!overview (All accessed: 20 March 2017).

[9] This is not to diminish the importance of other industry segments and their respective actors (which include among others retailers and commerce facilitators, cryptocurrency ATMs, supporting services such as data analytics and media organisations, decentralised application developers, and many more), but rather due to practical considerations that covering the entire industry is not feasible.

[10] Burniske, C. & White, A. (2016) Bitcoin: Ringing the Bell for a New Asset Class. Available at http://research.ark-invest.com/bitcoin-asset-class (Accessed: 20 March 2017).

[11] Schuh, S. D. & Shy, O. (2016) U.S. Consumers' Adoption and Use of Bitcoin and Other Virtual Currencies. Unpublished; slides of preliminary findings (state: April 2016) available at https://payments.nacha.org/sites/payments.nacha.org/files/files/Virtual%20Currency.pdf (Accessed: 20 March 2017).

[12] A 2016 report studying payment relationships based on transaction flows on the bitcoin network has estimated that the use of crypocurrency as a medium of exchange for online gambling and darknet black markets has been most popular from mid-2012 until late 2013, but that the 'legitimate' economy has taken over since. Tasca, P., Liu, S., & Hayes, A. (2016) The Evolution of the Bitcoin Economy: Extracting and Analyzing the Network of Payment Relationships. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2808762 (Accessed: 20 March 2017).

[13] 377 dApps are listed on http://dapps.ethercasts.com/ (Accessed: 25 March 2017).

[14] Figures available at http://opreturn.org/ (Accessed: 25 March 2017).

[15] See 'Wallet' section for an explanation of the methodology used.

**EXCHANGES**

[1] List of exchanges available at https://coinmarketcap.com/exchanges/volume/24-hour/all/ (Accessed: 7 March 2017).

[2] This figure does not include the over-the-counter (OTC) market whose size is unknown due to its informal nature.

[3] Available at https://data.bitcoinity.org/markets/ (Accessed: 15 March 2017).

[4] There is reasonable doubt among the bitcoin community and professionals about the real nature of these figures, as volumes seem to have been inflated because of a 0-fee trading policy and the excessive use of margin trading. This is further evidenced by the significant drop in Chinese market share in early 2017 after the Chinese central bank effectively banned margin trading and forced major exchanges to introduce trading fees.

[5] In this context, we define large exchanges as entities that have more than 20 employees and/or have a non-negligible market share.

[6] This figure includes employees from *universal* cryptocurrency companies that are also active in industry sectors other than exchanges.

[7] Moore, T., & Christin, N. (2013). Beware the middleman: Empirical analysis of Bitcoin-exchange risk. In: Sadeghi AR. (ed) *Financial Cryptography and Data Security*. FC 2013. Lecture Notes in Computer Science, vol. 7859. Springer: Berlin, Heidelberg.

[8] However, it is important to note that this only applies to users' cryptocurrency holdings, but not the national currency holdings which remain under the control of the exchange.

[9] These factors generally are something one 'knows' (e.g., password), something one 'has' (e.g., hardware device for one-time passwords/tokens) and something one 'is' (e.g., biometrics).

**WALLETS**

[1] There are also other types of 'non-software' wallets such as paper and brain wallets.

[2] Before being able to use the reference wallet, the user needs to download the entire blockchain, and thereafter is required to keep in sync with the network each time he wants to use the wallet. At present, the Bitcoin blockchain requires 120 gigabytes of hard drive storage space. Many individuals also find reference wallets more difficult to use.

[3] This figure includes employees from *universal* cryptocurrency companies that are also active in industry sectors other than wallets (e.g., payment processing). The numerous volunteers that contribute to open-source/volunteer wallet projects are excluded from this figure.

[4] For 2016 and 2017, the lower bounds were established with self-reported figures from incorporated wallet providers. There is no active wallet data for some wallets prior to 2016, which makes it difficult to make year-by-year growth rate comparisons and explains the large gap between 2015 and 2016.

[5] It is worth noting that these figures do not include transactions from wallet users that are performed 'off-chain', i.e., transactions between users of the same wallet platform that do not occur on the public blockchain, but in a centralised ledger of the wallet provider. Moreover, these figures do not include transactions initiated from some open-source wallets as well as the wallet included in the reference implementation. Transactions on the bitcoin network are performed by a variety of actors other than wallet users, such as for instance exchanges, miners and payment companies.

[6] We define large wallets as organisations that have more than 10 employees.

[7] Multi-signature is a mechanism to split access to stored cryptocurrency to two or more keys and is frequently used for trustless escrow.

[8] Hierarchically deterministic (HD) key generation allows the creation of infinite private key 'childs' based on a single 'parent' key. This removes the need for constantly backing up the wallet file once a new key has been added, as all newly generated keys can be calculated using the parent key. Another development in parallel has enabled the possibility of encoding a private key into a so-called mnemonic word sequence (also referred to as a 'seed'), which is a collection of multiple words that represent the private key in human-friendly format. These two innovations together make it possible to easily backup an entire wallet by remembering a single passphrase and migrate the wallet file to another provider.

[9] This does not necessarily mean that wallet providers have no possibility of confiscating user funds: they could freeze the accounts of users that are suspected to violate terms and conditions, in which case the national currency holdings would be inaccessible. Similarly, cryptocurrency holdings would also be inaccessible if users had not backed up the wallet externally.

[10] This does not necessarily mean that the non-licensed wallets that are providing centralised national-to-cryptocurrency exchange services are not regulated.

[11] Know your customer (KYC) and anti-money laundering (AML) checks. Some wallets that provide national-to-cryptocurrency exchange services using the P2P or the integrated third-party exchange model do also perform KYC/AML checks.

[12] 'Hybrids' (wallets that offer customer the option to control private keys) have been removed from the analysis.

**PAYMENTS**

[1] These include, among others, removing the need to understand the technical specifics of the underlying system, convenient use and easy user interface, availability of additional features, avoiding hassle of managing keys, etc.

[2] Although the boundaries between exchanges and payment platforms are blurred as most general-purpose cryptocurrency platforms enable currency conversion within the platform interface (usually by connecting to various third-party exchanges), we consider payment service providers in this context to be *exchanges* as well only if they operate a cryptocurrency exchange themselves.

[3] This figure includes employees from *universal* cryptocurrency companies that are also active in industry sectors other than payment services (e.g., exchanges, wallets, etc.).

[4] In this context, the term *national-to-national* refers to payments entirely denominated in national currencies from the perspective of the user, although cryptocurrency might be used at the backend (e.g., national-to-cryptocurrency-to-national).

**MINING**

[1] Self-built mining rigs composed of GPUs (graphical programming units) in 2010 and FGPAs (field-programmable gate arrays) in 2011 quickly replaced mining with CPUs (central programming units) used by the first miners. In mid-2012, the first organisations with very small budgets started developing customised ASIC (application-specific integrated circuit) equipment that was specifically designed for solving Bitcoin's mining puzzle and made previous mining hardware obsolete. For further information, see Taylor, M. B. (2013). Bitcoin and the age of bespoke silicon. In *Proceedings of the 2013 International Conference on Compilers, Architectures and Synthesis for Embedded Systems* (p. 16). IEEE Press.

[2] This figure uses the assumption that mining revenues (block rewards and transaction fees) have been immediately converted to national currency using the exchange rate of the day the block has been mined. Although miners cannot spend newly created bitcoins (i.e., bitcoins issued from the 'coinbase transaction' of a new block) until that specific block has received 100 confirmations, we believe this to be a reasonable assumption as on average, 144 blocks are added to the blockchain every day.

[3] This designation was made based on the mining organisations' scale and the position they occupy in the industry.

[4] The 'economic majority' is a term commonly used to describe the significant power that economic actors (cryptocurrency companies such as exchanges, wallets and payment service providers, but also merchants and users) have in case of a fork as they can decide - if unified - which 'version' of the cryptocurrency they will accept.

[5] Available at https://bitcoinchain.com/pools (Accessed: 8 March 2017).

[6] Market share for pools can change as a result of changes in the distribution of hashing power across mining pools.

[7] Low-cost electricity data is mainly based on industrial electricity prices in members of the IEA (December 2016). Fast internet connection data is based on the Akamai Q4 2016 State of the Internet report and includes countries with an average network connection above 10Mbps. Low temperature zones are determined by a yearly average temperature below 3°C, based on averages from 1960-1999 from the Climatic Research Unit. The location and estimates of power consumption in MW per mining facility are based on a combination of data from a Bitcoin Forum thread (available at https://bitcointalk.org/index.php?topic=1328580.0; accessed: 5 March 2017), a mining map of Chinese facilities from Tsinghua University and our own research.

[8] It should be noted that this map only takes into account mining facilities that are publicly known and reported. The power consumption (in MW) of countries is indicated on the mining map when there is data publicly available.

[9] This calculation is based on the assumption that all miners use the Antminer S9 which consumes 0.1 J/GH. In addition, we consider the parasitic power consumption by the equipment (e.g., motherboard, power supply) which is estimated at around 10% of total consumption, as well as co-location power usage efficiency (PUE) which is set at 1.05 based on estimates of the currently most efficient facilities. Combining all these factors together with the current bitcoin network hash rate of around 4,000 PH/s (4,000,000 GH/s), the lower-bound power consumption of the bitcoin network can be estimated at 462MW. We would like to thank Sveinn Valfells for sharing the methodology originally used in Valfells, S. & Egilsson, J. H. (2016) Minting Money with Megawatts. *Proceedings of the IEEE*, *104(9*), 1674-1678.

[10] However, this figure should be considered as 'lower-bound', because it is reasonable to assume that a considerable number of miners are still using older (and thus less efficient) equipment, and it is unlikely that all mining is being performed in the most efficient colocation centres. As a result, the real power consumption of bitcoin mining (and cryptocurrency mining in general) is likely substantially higher.

[11] Latin America has been removed from the analysis because of the low number of respondents.

[12] Data and methodology available at http://digiconomist.net/beci (Accessed 8 March 2017).

[13] Mentioned in 8btc interview with Chinese miner and angel investor Chandler Guo: available at http://news.8btc.com/bitcoin-mining-now-decentralized-in-china-chandler-guo (Accessed: 8 March 2017).

[14] As total mining revenues are dependent on the market price, they are fluctuating with the latter. This explains the differences between each year, given our assumption that miners convert newly minted coins immediately to fiat currency. However, it is likely that mining revenues have been higher than these figures suggest as many miners hold at least a certain percentage of newly minted coins, and cash them out later when the price is rising.

[15] The latter is different from the former in that even though the control of hashing power might be distributed among multiple, non-colluding pool operators, the fact that the majority of hashing power is physically located in the same country or region makes it vulnerable to state interventions and operational risk factors affecting the country or region as a whole.

**APPENDICES**

[1] Not every cryptocurrency can be considered ‘decentralised’ as this depends on multiple factors such as the proportion of independent and non-colluding nodes and miners, as well as the amount of hash power securing the blockchain, among others.

[2] There are potential scenarios in which a transaction could get censored by miners, and/or specific units of the cryptocurrency could be ‘tainted’ or 'blacklisted' which would break fungibility; but these are beyond the scope of this report.

[3] The exact speed depends on a variety of factors that include among others the average block time, the size of the mempool (i.e., the number of transactions that are waiting to get confirmed) and the number of confirmations (i.e., additional blocks mined on top of the block in which the transaction is included) one would like to wait to consider the payment to be final and irreversible.

[4] It should be noted that there are major differences between cryptocurrencies with regards to the size of transaction fees – see the discussion of bitcoin transaction fees in the Mining section. This means that micropayments via 'on-chain' cryptocurrency payments do not always make economic sense.

[5] Available at https://coin.dance/volume/localbitcoins (Accessed: 20 March 2017).

[6] Available at https://coinmap.org/ (Accessed: 20 March 2017).

[7] Available at https://bitnodes.21.co/ (Accessed: 20 March 2017).