

RUSI-ACAMS

CRYPTOCURRENCY RISK & COMPLIANCE SURVEY





Disclaimer & Acknowledgements

ACKNOWLEDGEMENTS

This survey would not have been possible without the support of the RUSI team and the ACAMS Global Chapters, Marketing and Operations teams. Special thanks go to Katie Norton-Williams, and project sponsor Lashvinder Kaur, VP Global Strategic Communications, ACAMS, for their support on this project.

Thanks also to Jesse Spiro and Gemma Rogers for their helpful comments on the initial draft of this survey, and to Dr William Scott Grob and Emil Dall who reviewed the report.

In addition, special thanks to the ACAMS global membership community of over 81,000 members spread across 175 countries, and its 70 chapters for being part of this landmark initiative. Appreciation also goes out to the organisations that assisted in disseminating this survey, namely Global Digital Finance, the FinTech FinCrime Exchange and Coin Center.

RUSI

The opinions expressed in this work are the responsibility of the authors and do not in any way reflect those of RUSI, its directors or its employees. Neither RUSI, nor the authors assume responsibility or liability for the contents of this report, or its reading, use or interpretation. While every effort has been made to verify the data used in this report, no guarantee or warranty is made on its accuracy. You should seek your own professional advice before acting on any of the content in this report.

ACAMS

This report is intended for general guidance and information purposes only and under no circumstances should this report be used as or considered legal or regulatory advice. Each recipient should consult with its legal, business, investments and tax advisors as to the legal, business, investment and tax implications when making any legal, business, financial decision. The information contained in this report is based on survey responses which have been assumed to be reliable. ACAMS, its directors, employees or authors, make no representation or warranty on the responses and such data should be taken "as is". We do not validate the accuracy, completeness or reliability of the survey responses.

This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. You are free to copy and redistribute the material for non-commercial purposes, but you must give appropriate credit to RUSI and ACAMS. If you remix, transform, or build upon the material, you may not distribute the modified material.

For more information, see <<http://creativecommons.org/licenses/by-nc-nd/4.0/>>



Table of Contents

Introduction	4
Key Observations	5
Methodology	6
Cryptocurrencies as an Alternative to Fiat Currencies	10
Global Use of Cryptocurrency	14
Risk or Opportunity	18
Types of Criminal Risks	22
Cryptocurrency Compliance	26
Guidance & Best Practice	34
Regional Perceptions by Banks	41
Future of Cryptocurrency	45
Annex: Definitions	50



Introduction

The RUSI-ACAMS Cryptocurrency Risk & Compliance Survey provides unprecedented insight into how governments, the cryptocurrency industry, traditional financial institutions, and others view the use of cryptocurrency, including its inherent risks and the robustness of compliance controls within the cryptocurrency sector.

As with any survey, it should be recognised that there are certain limitations. Individuals may choose to opt in or opt out of participation and those who participated will reflect that. However, the survey was conducted in collaboration with YouGov, a respected independent research agency who followed the Market Research Society's code of conduct. As such, the findings can be taken to offer an illustrative view of industry attitudes to cryptocurrency risk and compliance, and the results provide a very rare insight into both the challenges and opportunities in this emerging financial crime risk. The purpose of conducting this survey is to help shape and inform the policy dialogue on cryptocurrency.

Please note, the term “cryptocurrency”, as used in this survey, specifically refers to payment tokens (such as Bitcoin) as opposed to stablecoins (such as Libra) or central bank digital currencies, unless otherwise specified. Further definitions of terms used in the survey can be found in the annex.



ACAMS

ACAMS is the largest international membership organisation dedicated to enhancing the knowledge, skills and expertise of AML/CTF, sanctions and other financial crime prevention professionals through training, best practices and professional development. ACAMS is present in over 175 countries and regularly works with global think-tanks and other like-minded organisations in the quest to end financial crime.



RUSI

RUSI is an independent defence and security think tank based in the United Kingdom. RUSI's Centre for Financial Crime and Security Studies has conducted work in an effort to combat a plethora of cryptocurrency-based financial crime risks, mainly terrorist financing, money laundering, and proliferation financing. To read more about RUSI's work visit www.rusi.org/CFCS.



YouGov

RUSI and ACAMS partnered with YouGov to deliver this survey.



About the Authors

Kayla Izenman, Research Analyst, Centre for Financial Crime and Security Studies, RUSI.

Rick McDonell, Executive Director, ACAMS and Former Executive Secretary of FATF.



Key Observations

The cryptocurrency industry remains materially divided from other sectors over the perception of risk. Governments and financial institutions view cryptocurrency as a significant source of risk.

All respondents accept that cryptocurrencies are vulnerable to criminals. Still, the sharpest distinction between the cryptocurrency industry and the other surveyed sectors is on the significance of the inherent risks and the effectiveness of the cryptocurrency industry's internal controls. Cryptocurrency industry respondents optimistically view their AML/CTF preparedness and the comprehensiveness of their internal controls.

Cryptocurrency industry respondents also appear significantly more confident than other sectors about the business use and inherent vulnerabilities of cryptocurrency. The potential downside to this is that the cryptocurrency industry may materially underestimate the types of threats posed. On the other hand, other sectors may be overestimating how exposed cryptocurrencies are to different criminal activities.

Respondents all expressed concern regarding the use of cryptocurrency by various illicit actors, ranging from terrorist groups to sanctioned actors and human traffickers. While cryptocurrency use by criminals only accounts for around 1% of all transactions, it remains an attractive venue for those avoiding the traditional financial system.¹ It is interesting to see that perceptions of risk remain so high.

All respondents are expecting more guidance and best practices from both governmental bodies and non-governmental organisations.² This is largely in line with the current and future efforts of international organisations, most importantly the Financial Action Task Force (FATF). There appears to be a consistent approach between the FATF and national regulators³ on the implementation of cryptocurrency regulation, with the expectation that the industry should look to both their national regulator and the international standard setter for guidance.

Respondents also indicate that despite current skepticism over the role of cryptocurrency in promoting financial inclusion, there might be more space for it in the future. Respondents predict both an increased role for cryptocurrency in day-to-day payments in the future as well as a decrease in cryptocurrency use for illicit activities, especially as compared to how it is viewed now.

1. Chainalysis, *The 2020 State of Crypto Crime*, p. 5.

2. During the survey period from 3rd June to 22nd July 2020, FATF published "12 Month Review of Revised FATF Standards - Virtual Assets and VASPs", retrieved from <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html>. Also published was the "FATF Report to G20 on So-called Stablecoins", retrieved from <https://www.fatf-gafi.org/publications/fatfgeneral/documents/report-g20-so-called-stablecoins-june-2020.html>

3. For example, see FinCEN Director Kenneth A. Blanco's remarks on the FATF's Travel Rule from May 2020: <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-consensus-blockchain>

METHODOLOGY





Methodology

The survey was distributed to ACAMS members, members of RUSI's Centre for Financial Crime and Security Studies' mailing list, as well as to individual government and cryptocurrency stakeholders for distribution. This report is based on 566 individual responses received between 3rd June 2020 and 22nd July 2020, with survey respondents indicating they are located in North America (32%), South America (8%), Europe (23%), Asia (22%), Africa (7%), Middle East (5%), and Oceania (3%). There was very little difference in how respondents from different regions responded to the survey, and as a result this report generally avoids regional breakdowns.

Where the largest difference in answers was observed is among different sectors and occupations. The survey asked respondents to identify the type of institution they work in. The largest group of survey respondents (49%) work in financial institutions (FIs), while other respondents work in government (24%) or the cryptocurrency industry (10%). The remaining survey respondents (18%) work in other private sector roles, including law, insurance companies, and non-banking FinTechs or RegTechs.⁴ Over two-fifths (42%) of all respondents bar government indicated they would consider their organisation a FinTech.

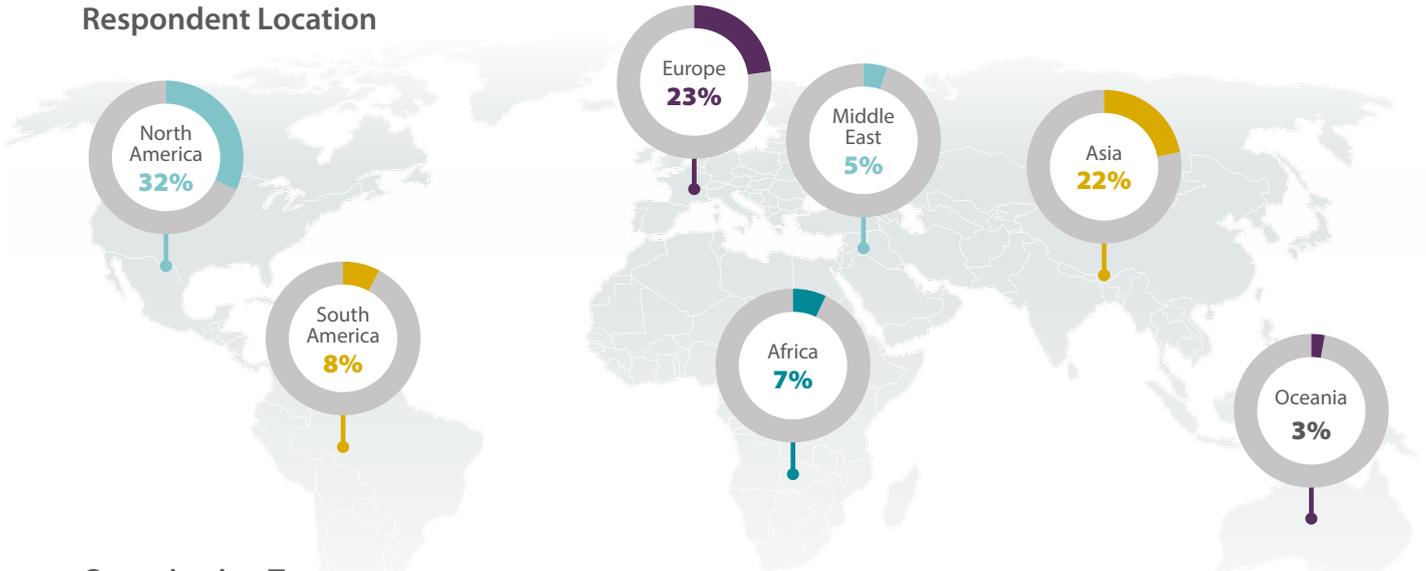
When asked to identify their position within their organisation, private sector respondents chose the following categories: mid- to junior-level (38%), senior management (34%), legal/regulatory/risk management (14%), executive leadership (6%), and other roles (8%) which included trade finance. Government respondents were mostly composed of those working for financial regulatory authorities or financial intelligence units (61%), followed by law enforcement (18%), international organisations (7%), policy (5%), justice (3%), and other areas (6%).⁵ Respondents' answers did not vary greatly depending on their position in the private sector or which part of government they work for and therefore this report does not analyse responses by position.

Almost all respondents (97%) are familiar with at least one type of cryptocurrency, with Bitcoin being the most recognised (96%). The least recognised cryptocurrency was Zcash (24%).

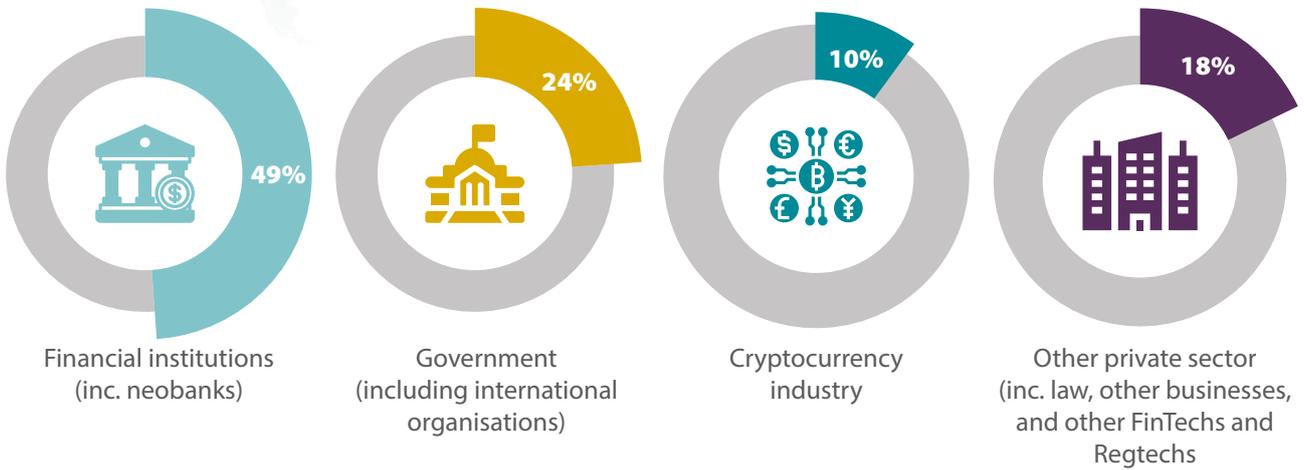
4. Given the purpose of this survey is to understand various industries' attitudes towards cryptocurrency, responses from four sectors (listed above) have been analysed. Please note that while some sectors, such as the cryptocurrency industry, have lower participation numbers, this is likely due to the smaller size of the industry and their relatively recent engagement with compliance issues.

5. For more detail on government positions, please see the following full survey options for government respondents: financial regulator; supervisor and/or financial intelligence units (FIUs); law enforcement (police); international organisation; policy (ministries of finance, foreign affairs); justice (including prosecutors); and other (including export controls, customs, and border agencies).

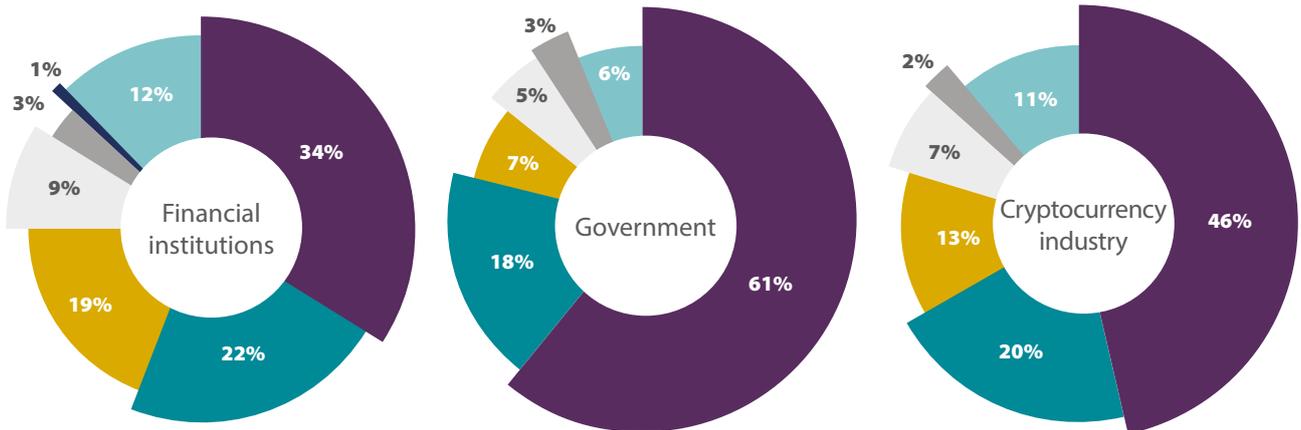
Respondent Location



Organisation Type



Sector



- International bank
- National bank
- Regional bank
- Payment service provider
- Neobank
- Insurance company
- Other

- Financial regulator
- Law enforcement
- International organisation
- Policy
- Justice
- Other

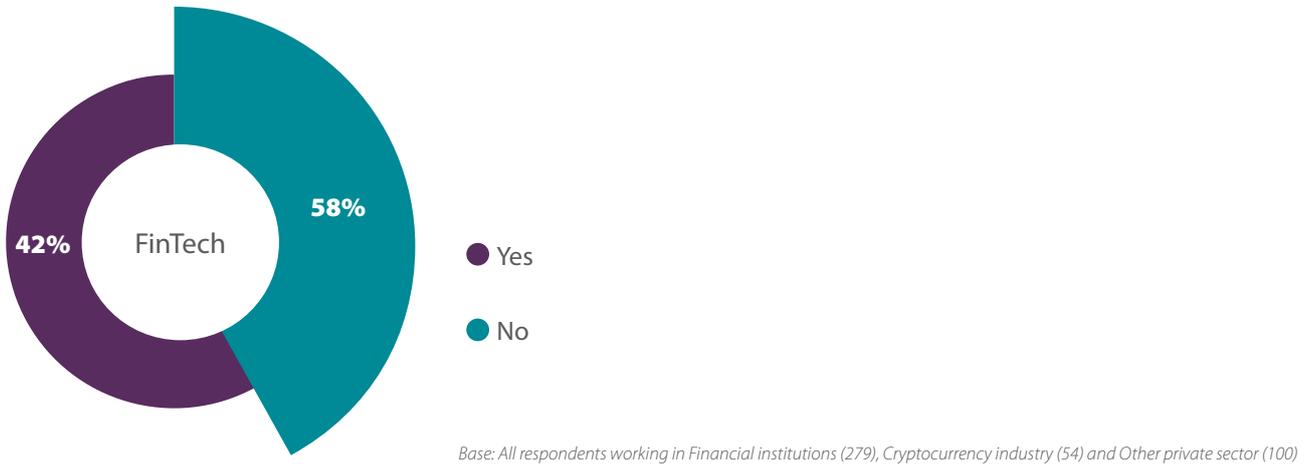
- Cryptocurrency exchange (Crypto-fiat AND crypto-crypto)
- Blockchain analytics company
- Cryptocurrency exchange (ONLY crypto-fiat)
- Custodial wallet provider
- Non-custodial wallet provider
- Other



Which of the following best describes your position?

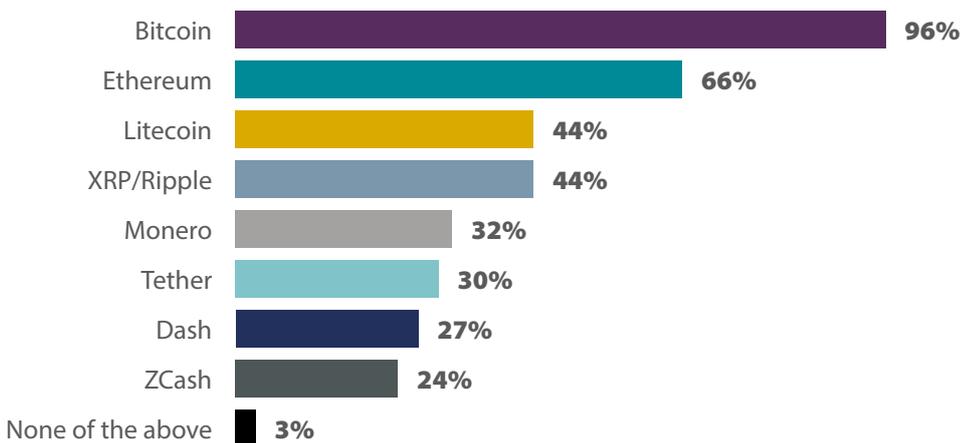


Would you consider your organisation a FinTech?



Virtually all respondents are familiar with Bitcoin, and two-thirds have heard of Ethereum

Which of the following cryptocurrencies, if any, are you familiar with?



CRYPTOCURRENCIES AS AN ALTERNATIVE TO FIAT CURRENCIES



Cryptocurrencies as an Alternative to Fiat Currencies

The survey asked respondents a series of questions about the usefulness of cryptocurrencies for various purposes, and as an alternative to fiat currencies. Respondents generally agreed (69%) that the value of cryptocurrencies is currently too volatile to be an effective alternative to fiat currencies.

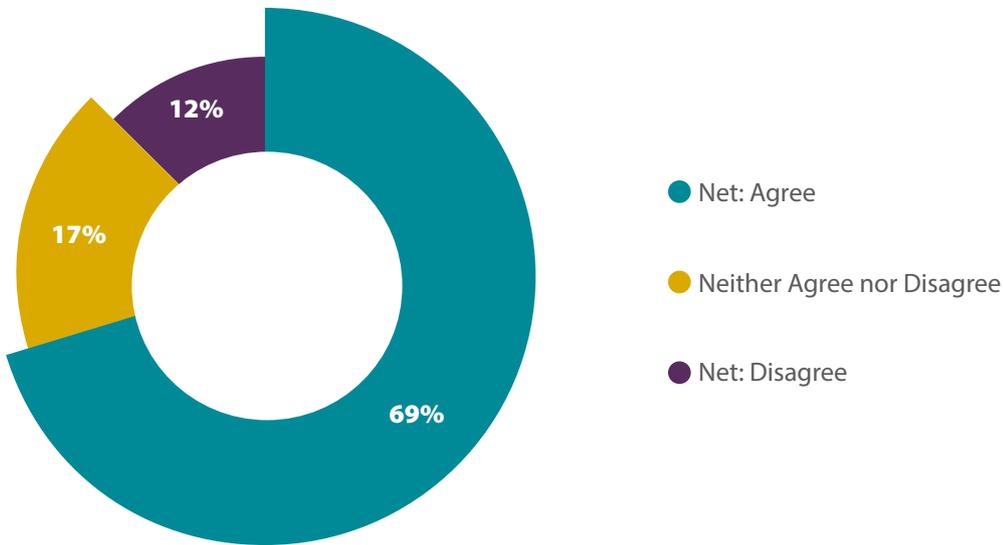
Responses from the cryptocurrency industry overwhelmingly indicate that cryptocurrency should be considered legal tender (76%), while just under half (44%) of FI respondents agree that cryptocurrency should be legal tender, with governments even more cautious (37%).

When asked about financial inclusion, a large majority (89%) of respondents from the cryptocurrency industry agree that cryptocurrency can be an effective tool to secure financial inclusion. Of those agreeing, over half (59%) *strongly* agree with this statement.

Other sectors are less convinced about the effectiveness of cryptocurrency in driving financial inclusion efforts. Around half (42% of FIs, 47% of governments, and 52% of other private sector) of the other respondents agree with the ability of cryptocurrency to address financial exclusion.

Respondents generally agree that the value of cryptocurrencies is currently too volatile to serve as an effective alternative to fiat currencies

The value of cryptocurrencies is too volatile to be an effective alternative to fiat currencies



Base: All respondents

Less than half of respondents agree cryptocurrencies should be considered legal tender, although this jumps to three-quarters among those working in the cryptocurrency industry

Cryptocurrencies should be considered legal tender

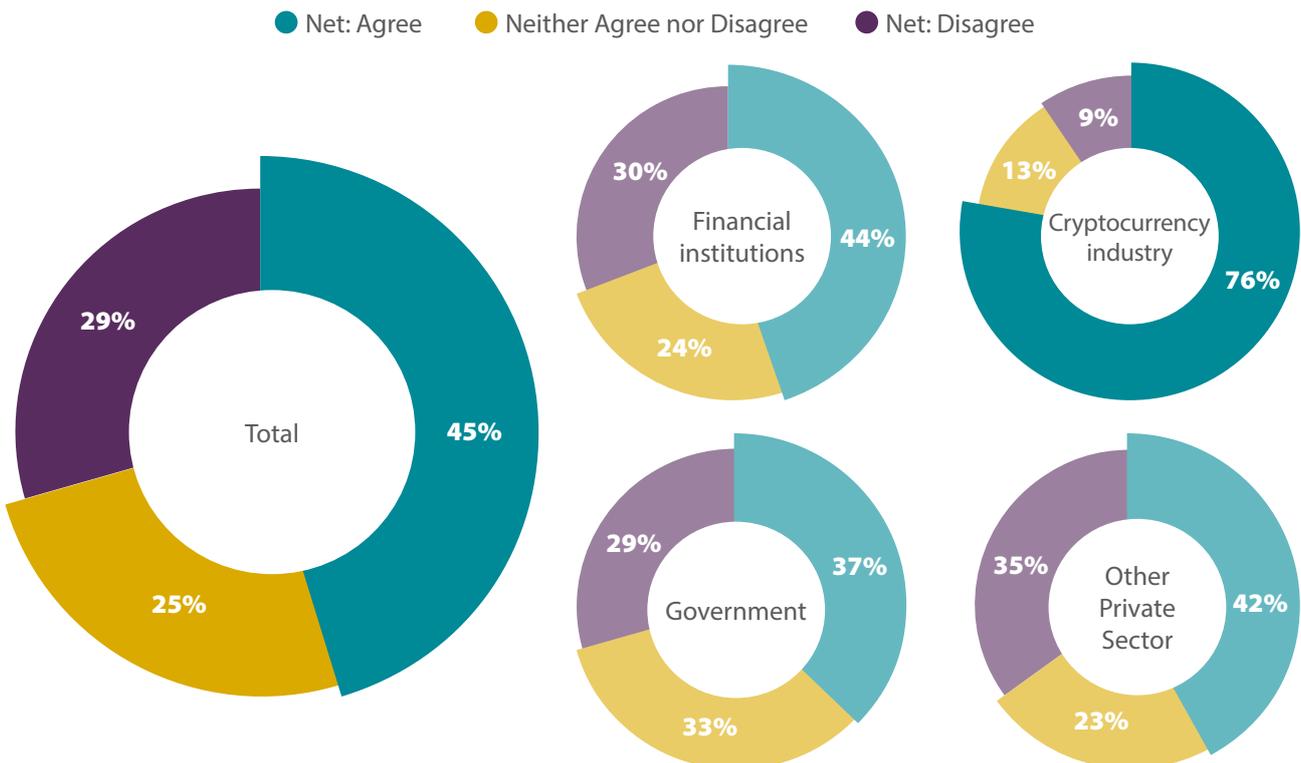
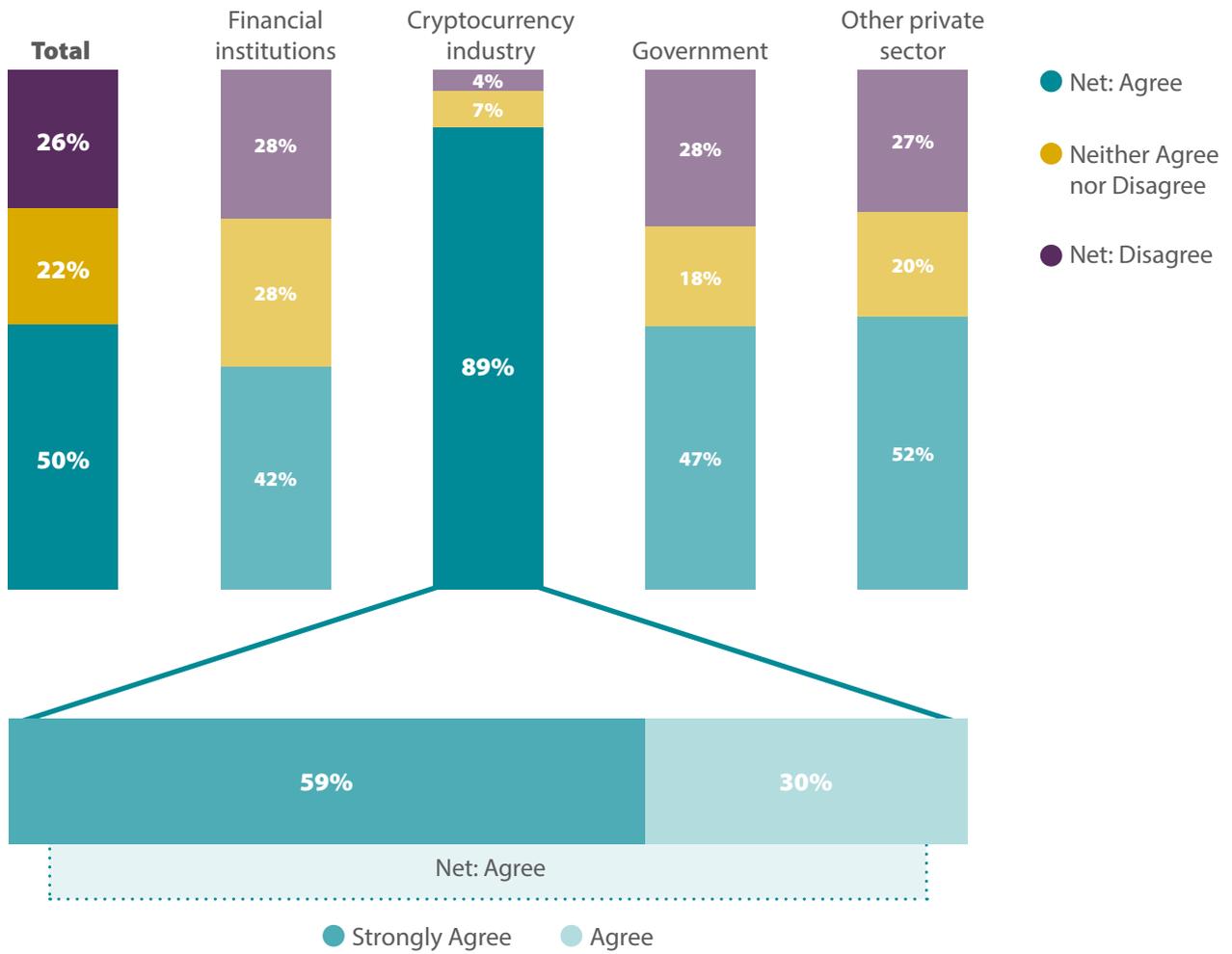


Chart excludes 'Don't Know' responses
Base: All respondents

Half of respondents agree that cryptocurrencies can be an effective tool to secure financial inclusion

Cryptocurrencies can be an effective tool to secure financial inclusion



Base: All respondents

GLOBAL USE OF CRYPTOCURRENCY



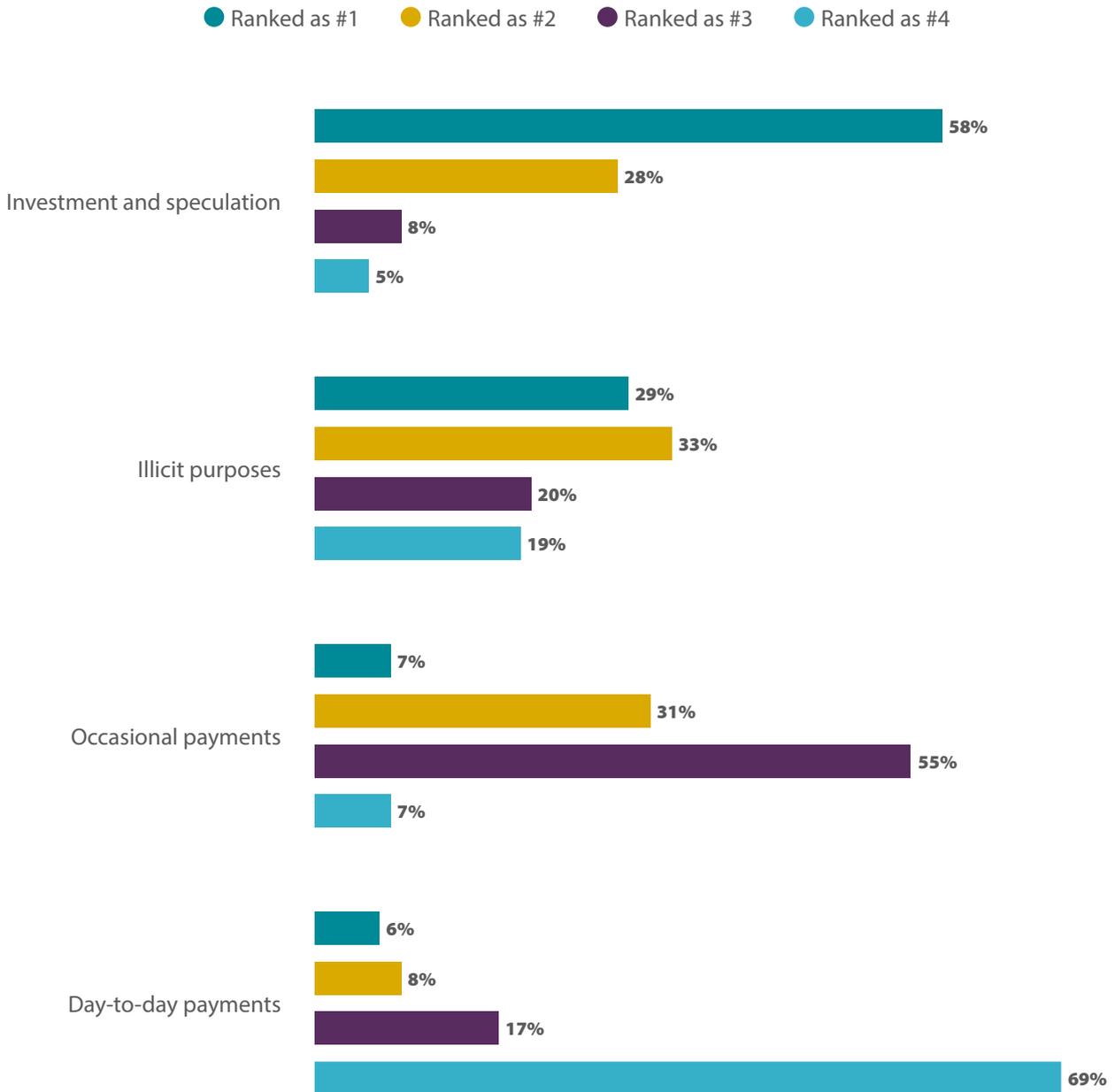
Global Use of Cryptocurrency

Respondents were asked to rank the possible uses of cryptocurrency according to what they believed to be the main uses. Three-fifths (58%) of all participants believe that cryptocurrency is mainly used for investment and speculation, with illicit purposes ranking overall at number two. When respondents are split into their respective occupations, every sector ranks investment and speculation first. However, opinions diverge when considering each sector's second ranking.

Respondents from FIs and government both rank illicit purposes second, followed by occasional payments and day-to-day payments. Respondents from the cryptocurrency industry, however, rank occasional payments second, with illicit purposes ranked last in terms of what cryptocurrencies are mainly used for.

Three-fifths of respondents believe that cryptocurrency is mainly used for investment and speculation

Cryptocurrency is mainly used for...

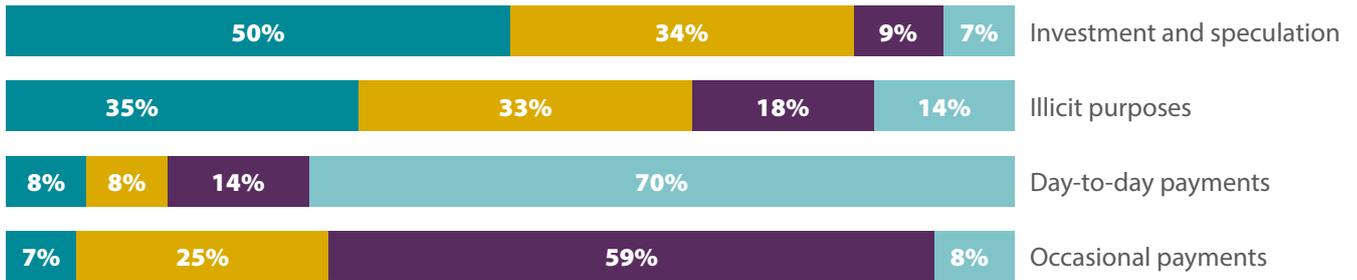


Base: All respondents

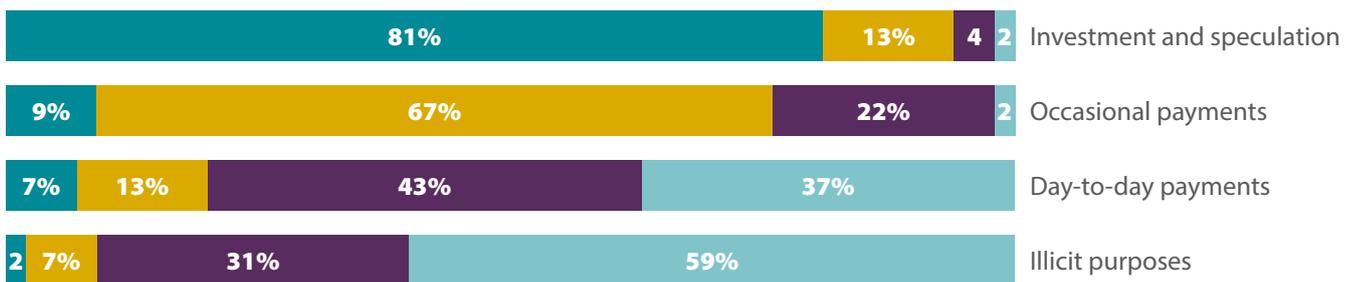
All respondents think cryptocurrency is mainly used for investment, but those not in the cryptocurrency industry are more likely to believe cryptocurrency is mainly used for illicit purposes

Cryptocurrency is mainly used for...

Financial institutions



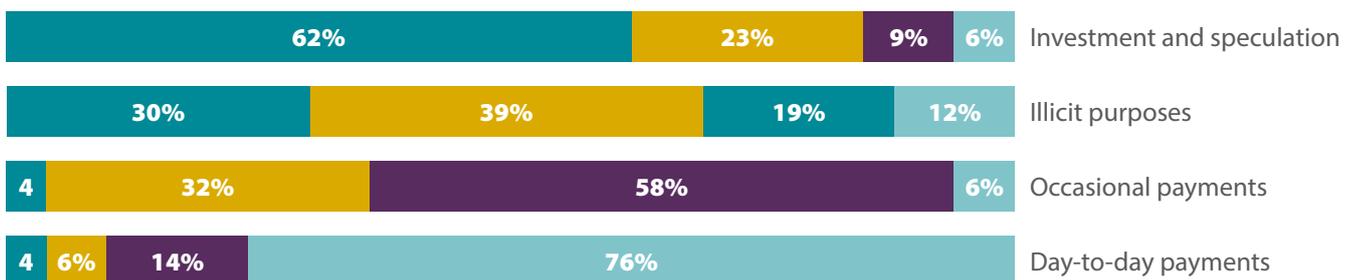
Cryptocurrency industry



Government



Other private sector



● Ranked as #1 ● Ranked as #2 ● Ranked as #3 ● Ranked as #4

Base: All respondents

RISK OR OPPORTUNITY





Risk or Opportunity

When asked if they consider the use of cryptocurrency as a risk or opportunity, the cryptocurrency industry continues to view cryptocurrency more favourably compared to other sectors.

While over three quarters (80%) of cryptocurrency industry respondents say cryptocurrency is an opportunity, only a fifth of respondents from other sectors (19% of FIs, 23% of governments, and 20% of private sector) view cryptocurrency use as an opportunity. More significantly, these sectors overwhelmingly view cryptocurrency as a risk (63% of FIs, 56% of governments, and 59% of other private sector).

Respondents are generally more concerned with criminal activity than consumer protection when thinking about cryptocurrency risk, with only the cryptocurrency industry indicating a significant amount of concern for consumer protection (46%).



Respondents working in the cryptocurrency industry are the only audience to see cryptocurrency as more of an opportunity than a risk

When thinking about the global use of cryptocurrency, do you think of it mainly as a RISK or as an OPPORTUNITY?*

Total



Financial institutions



Cryptocurrency industry



Government



Other private sector

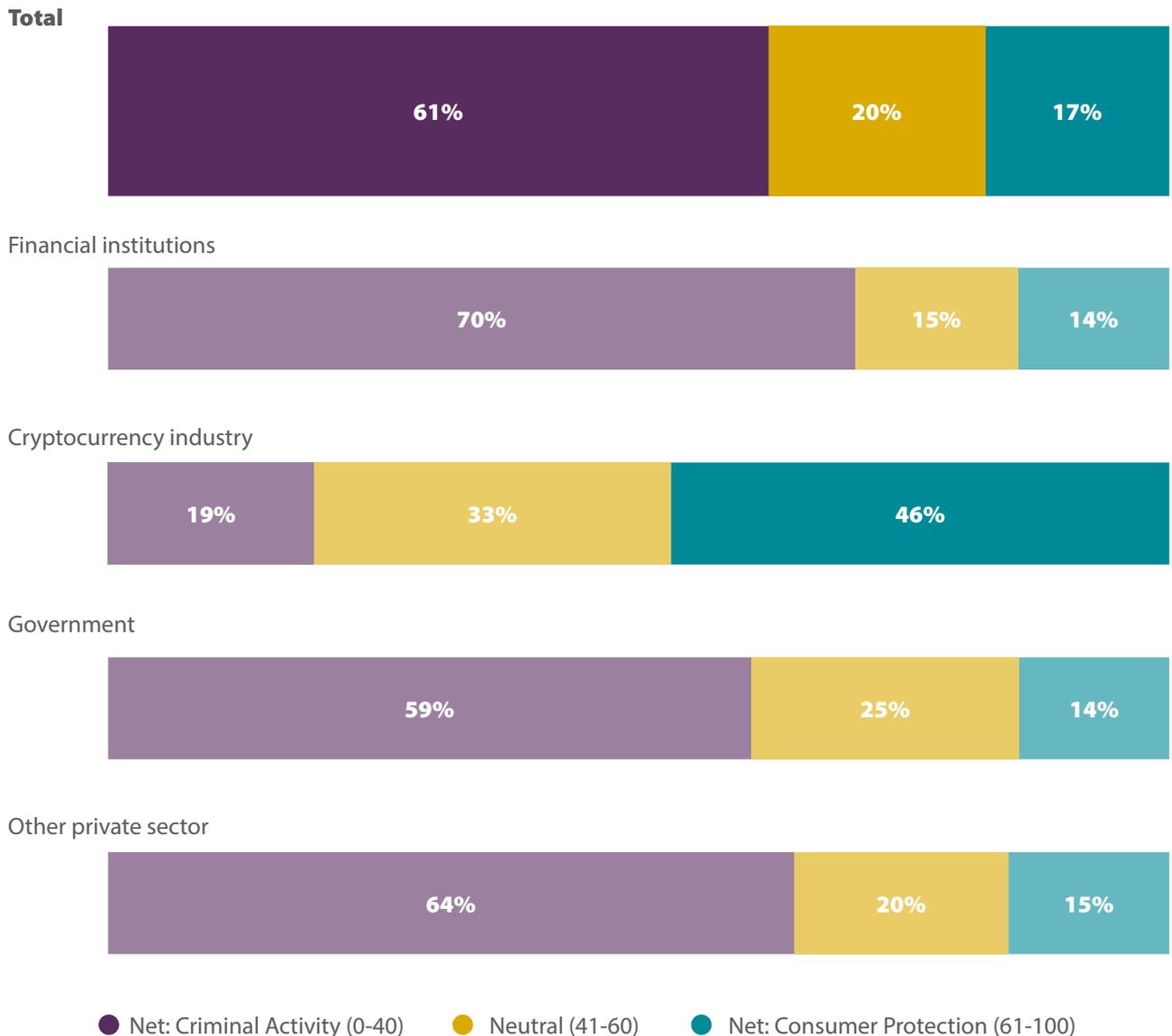


● Net: Risk (0-40) ● Neutral (41-60) ● Net: Opportunity (61-100)

*Respondents selected where they fell on a scale of 0-100, RISK being at 0 and OPPORTUNITY being at 100
 Chart excludes 'Don't Know' responses
 Base: All respondents

Respondents are generally more concerned with criminal activity than consumer protection when thinking about cryptocurrency risk, although cryptocurrency industry disagrees.

When thinking about cryptocurrency risk, are you mainly worried about **CRIMINAL ACTIVITY** or **CONSUMER PROTECTION**?*



*Respondents selected where they fell on a scale of 0-100, CRIMINAL ACTIVITY being at 0 and CONSUMER PROTECTION being at 100
 Chart excludes 'Don't Know' responses
 Base: All respondents

TYPES OF CRIMINAL RISKS



Types of Criminal Risks

There is fundamentally more alignment in responses from different sectors when asked how concerned they are about the risk of cryptocurrency being used for specific criminal activities.

When asked if they are worried about specific criminal activities that cryptocurrency can be used for, most respondents indicate they are concerned about cryptocurrency and money-laundering (84%) and use of cryptocurrency on the dark web (84%), followed by the procurement of illicit goods (83%), use of cryptocurrency by sanctioned actors (82%), use of cryptocurrency by terrorist organisations (79%), use of cryptocurrency to fund human trafficking (76%), and cryptocurrency use in fraudulent initial coin offering scams (75%). Across all of these different criminal activities, the cryptocurrency industry is, however, still less worried about each of these risks compared to respondents from other sectors, appearing most concerned about sanctions evasion (59%).

Respondents do not feel strongly that they would be more or less concerned about the previous risks if asked about stablecoins instead of payment tokens.

Respondents also indicated particular concern with online fraud (74%) and ransomware (73%) when asked about types of cybercrime involving cryptocurrency.

Respondents are mainly concerned with the use of cryptocurrency for money laundering, although this varies by audience

When thinking about criminal activity and cryptocurrency risk, how concerned, if at all, are you about each of the following?

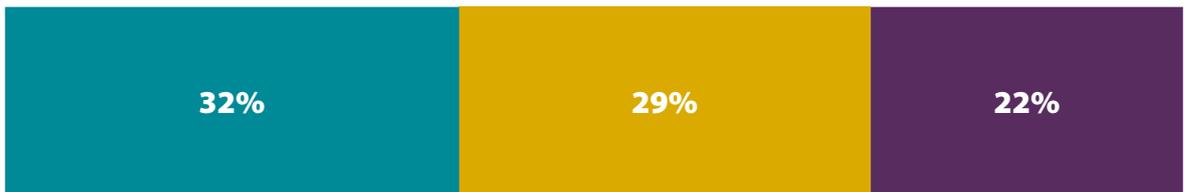


Base: All respondents

Only one-third of respondents believe that if the aforementioned risks were addressing stablecoins rather than payment tokens, they would be less risky

If the previous table on cryptocurrency financial crime risks was addressing stablecoin rather than cryptocurrency as a payment token, would you view the categories as LESS RISKY or MORE RISKY, generally?*

Total



Financial institutions



Cryptocurrency industry



Government



Other private sector



● Net: Less Risky (0-40) ● Neutral (41-60) ● Net: More Risky (61-100)

*Respondents selected where they fell on a scale of 0-100, LESS RISKY being at 0 and MORE RISKY being at 100

Chart excludes 'Don't Know' responses

Base: All respondents

CRYPTOCURRENCY COMPLIANCE



Cryptocurrency Compliance

Overall, the cryptocurrency industry is much more confident in cryptocurrency service providers' tools and preparedness than other sectors are.

Half of respondents (51%) believe cryptocurrency exchanges are unprepared to deal with the aforementioned cybercrime activities, although respondents from the cryptocurrency industry are significantly more confident in their own preparedness.

The majority of cryptocurrency industry respondents (83%) agree that cryptocurrency transactions offer more transparency than traditional financial transactions, while FIs and governments are much more skeptical, with only one-fifth of each sector (20%) agreeing. The cryptocurrency industry also agrees (85%) that cryptocurrency is compatible with sanctions screening and transaction monitoring, while all other industries were more likely to disagree with that statement.

Almost three-quarters (72%) of cryptocurrency industry respondents believe that cryptocurrency service providers have a firm grasp on AML/CTF compliance. This is compared to FIs and governments, where under one-fifth of respondents in each sector agree to the same.

However, other actors are found to be lacking by all respondents. Less than one fifth of respondents think the media (16%), politicians (11%), or the public who do not own cryptocurrency (5%) understand cryptocurrency financial crime risks well.

Around three-quarters of respondents are concerned with online fraud and ransomware, while the cryptocurrency industry is generally less concerned about all risks

When thinking about types of cybercrime involving cryptocurrency, how concerned, if at all, are you about each of the following?

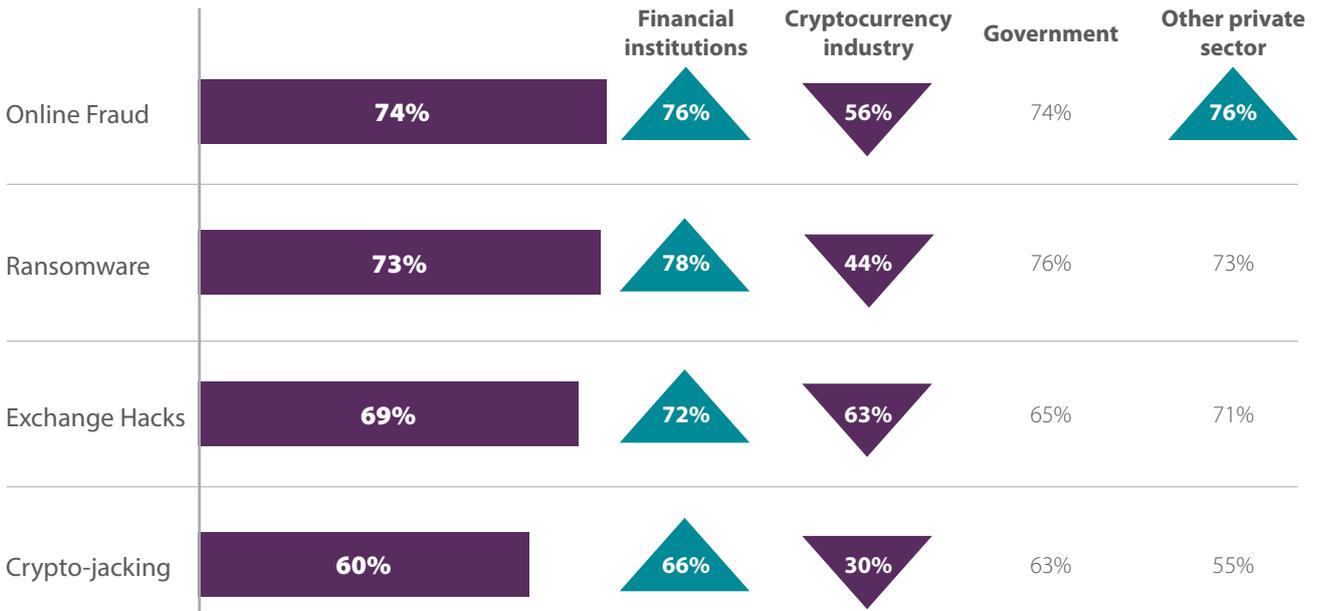
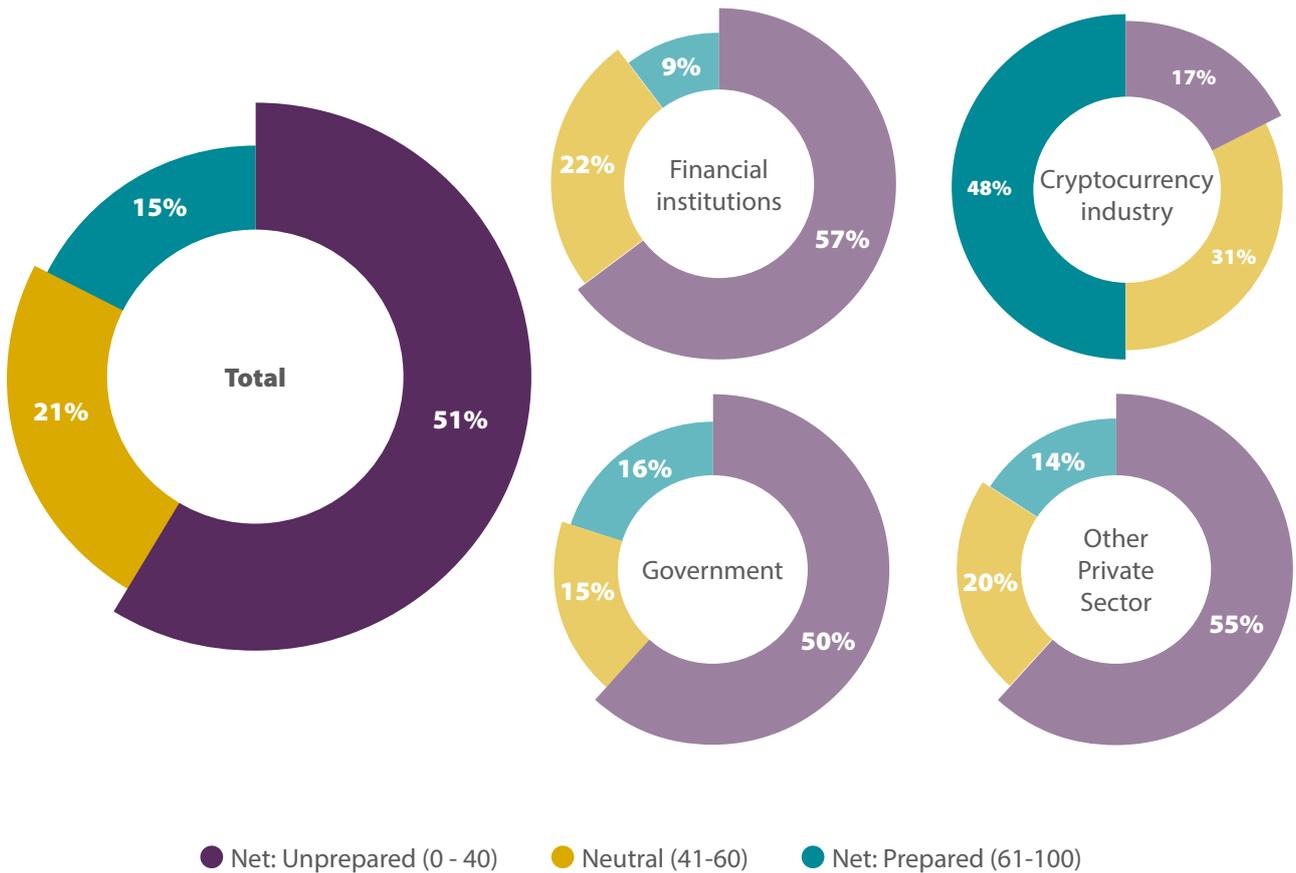


Chart excludes 'Don't Know' responses
Base: All respondents

Half of all respondents believe cryptocurrency exchanges are unprepared to deal with the aforementioned cybercrime activities. Those in the cryptocurrency industry are a lot more confident in their own preparedness

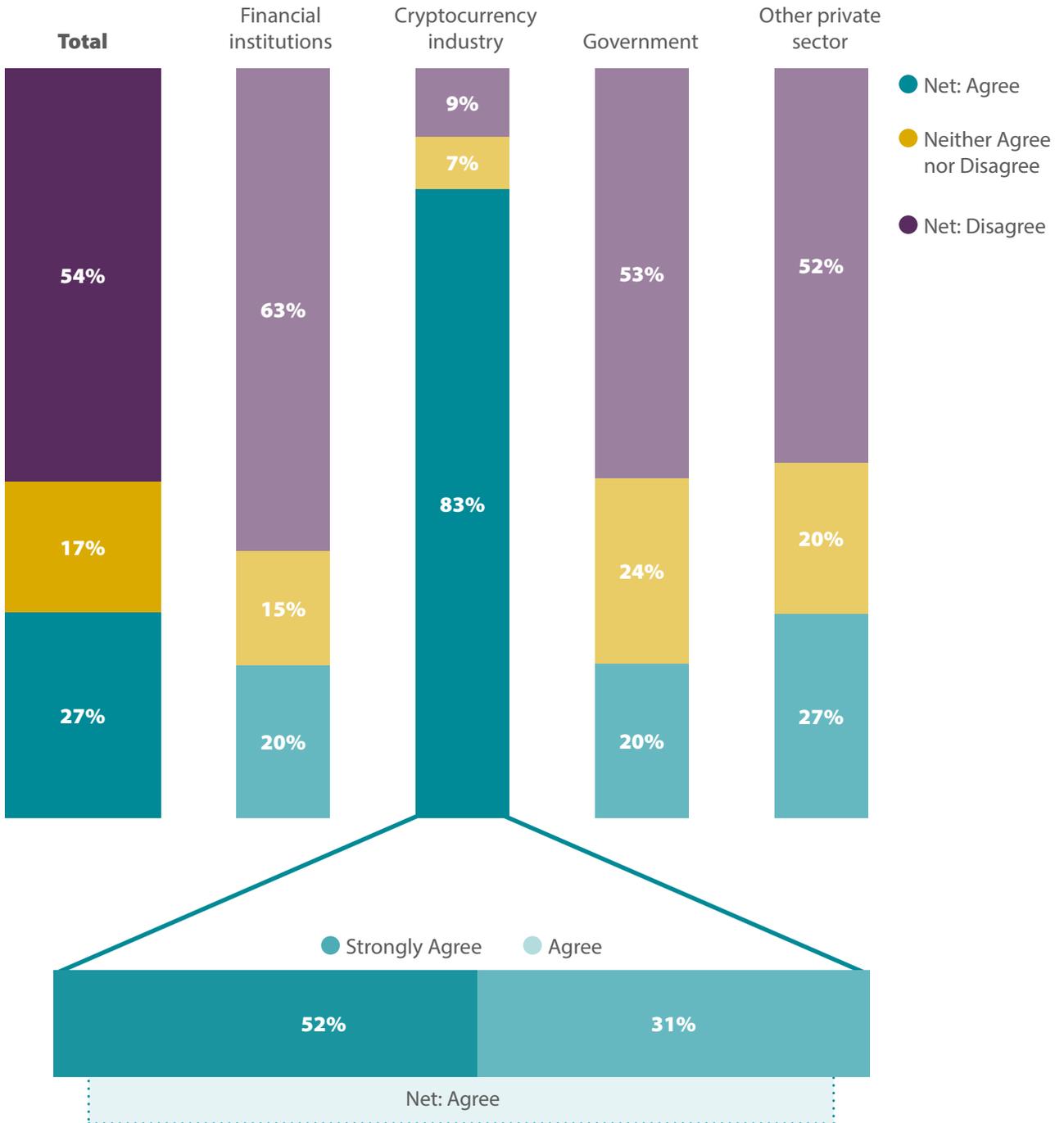
How prepared do you feel cryptocurrency exchanges are in dealing with and protecting against the above cybercrime activities?*



*Respondents selected where they fell on a scale of 0-100, UNPREPARED being at 0 and PREPARED being at 100
 Chart excludes 'Don't Know' responses
 Base: All respondents

Over half of respondents do not believe cryptocurrency transactions offer more transparency than traditional transactions, although four-fifths of those in the cryptocurrency industry think they do

Cryptocurrency transactions offer more transparency than traditional financial transactions



Base: All respondents

All audiences except those in the cryptocurrency industry largely disagree that cryptocurrency transactions are compatible with sanctions screening and transaction monitoring

Cryptocurrency transactions are compatible with sanctions screening and transaction monitoring

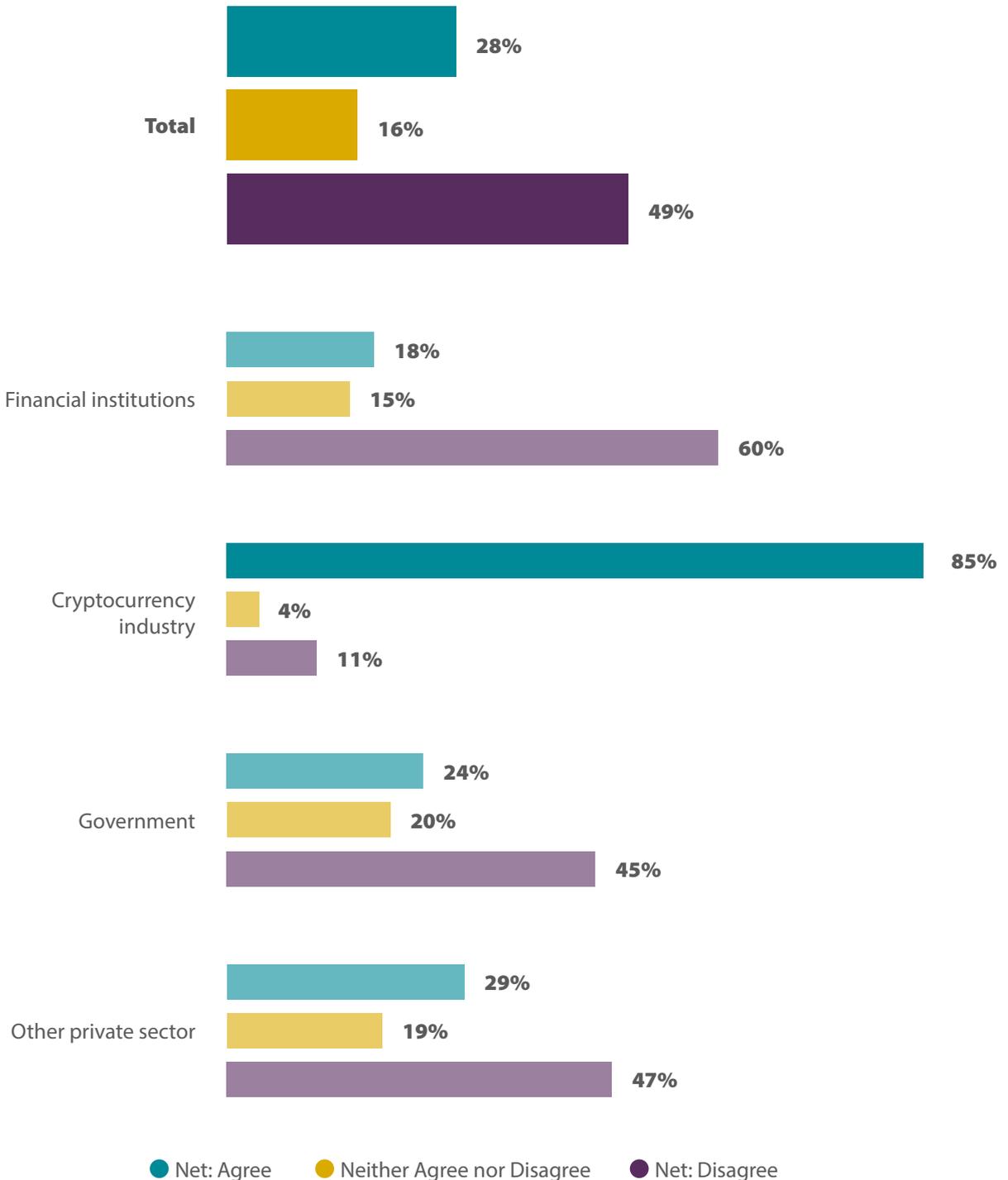


Chart excludes 'Don't Know' responses
Base: All respondents

Around half of respondents from financial institutions, government, and other private sector disagree that cryptocurrency providers have a firm grasp on AML/CTF compliance

Cryptocurrency service providers have a firm grasp on AML/CTF compliance

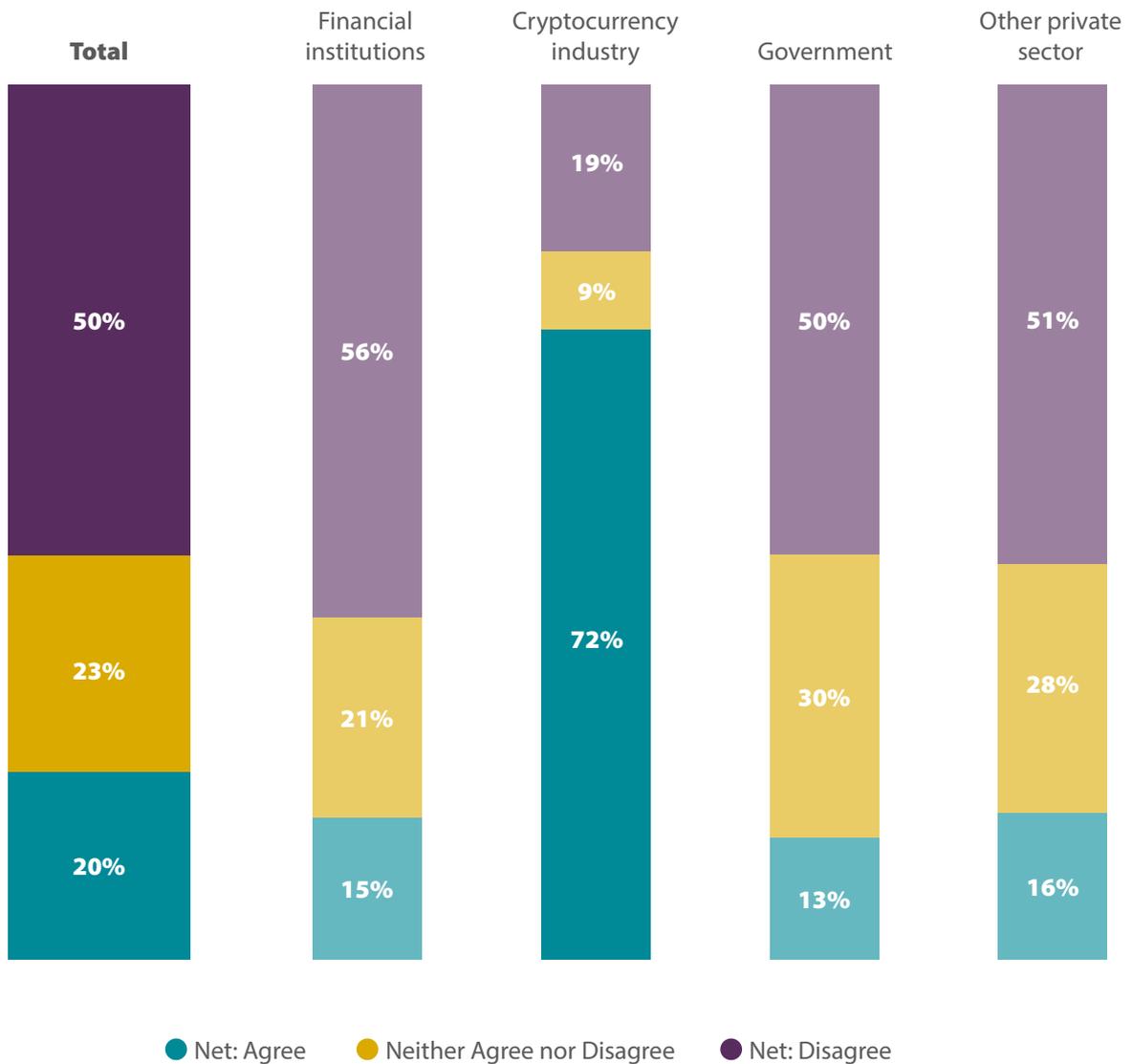


Chart excludes 'Don't Know' responses
Base: All respondents

Respondents generally believe that the cryptocurrency industry best understands cryptocurrency financial crime risk, and politicians and the non-cryptocurrency-owning public understand the risks the least

How well do you feel cryptocurrency financial crime risks are understood by each of the following actors in your jurisdiction?

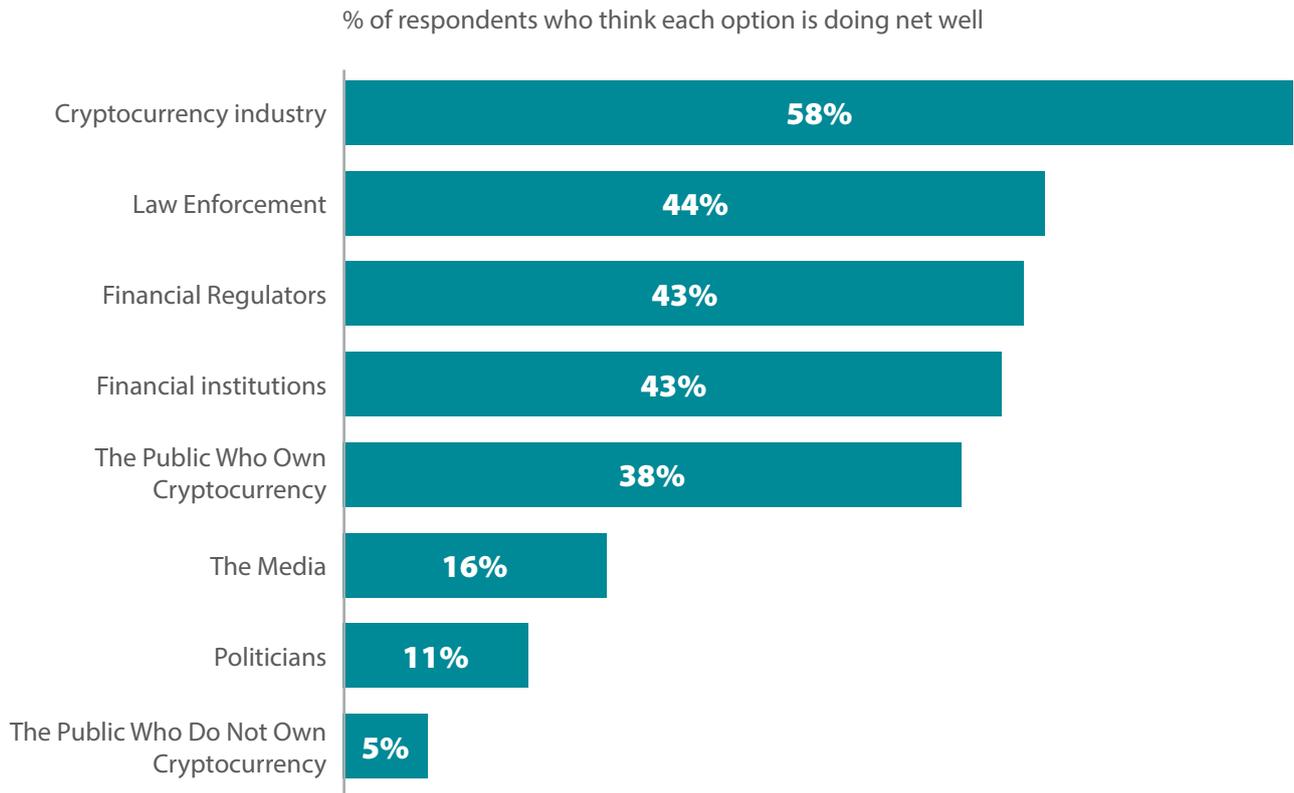


Chart excludes 'Don't Know' responses

Base: All respondents

GUIDANCE & BEST PRACTICE



Guidance & Best Practice

A significant number of all respondents, look for guidance from other governments to guide best practice. More than half (56%) of all respondents, across all groups, look to other governments or individual jurisdictions, to provide guidance.

Even more of all respondents (78%) indicate that they seek guidance from non-governmental organisations (and FATF, trade bodies, or blockchain associations) to guide best practice.

Half (52%) of all respondents believe risks related to cryptocurrency are best countered at an international level by organisations such as FATF. While FI and government respondents believe the responsibility lies primarily with international organisations, followed by national governments and then individual exchanges, respondents from the cryptocurrency industry are split on where the responsibility lies, indicating that international organisations (41%) and individual exchanges (41%) both hold responsibility.

When looking at specific regulation, over half of all respondents (59%) agreed that FATF's Recommendation 16 ("The Travel Rule") will be an effective way to mitigate AML/CTF cryptocurrency risk. Over half of those in the cryptocurrency industry, however, disagreed (54%) with this statement.

Over half of respondents look for guidance from other government to guide best practice. Three-fifths of government respondents look for best practice guidance from other government

I look for guidance from other Government to guide best practice

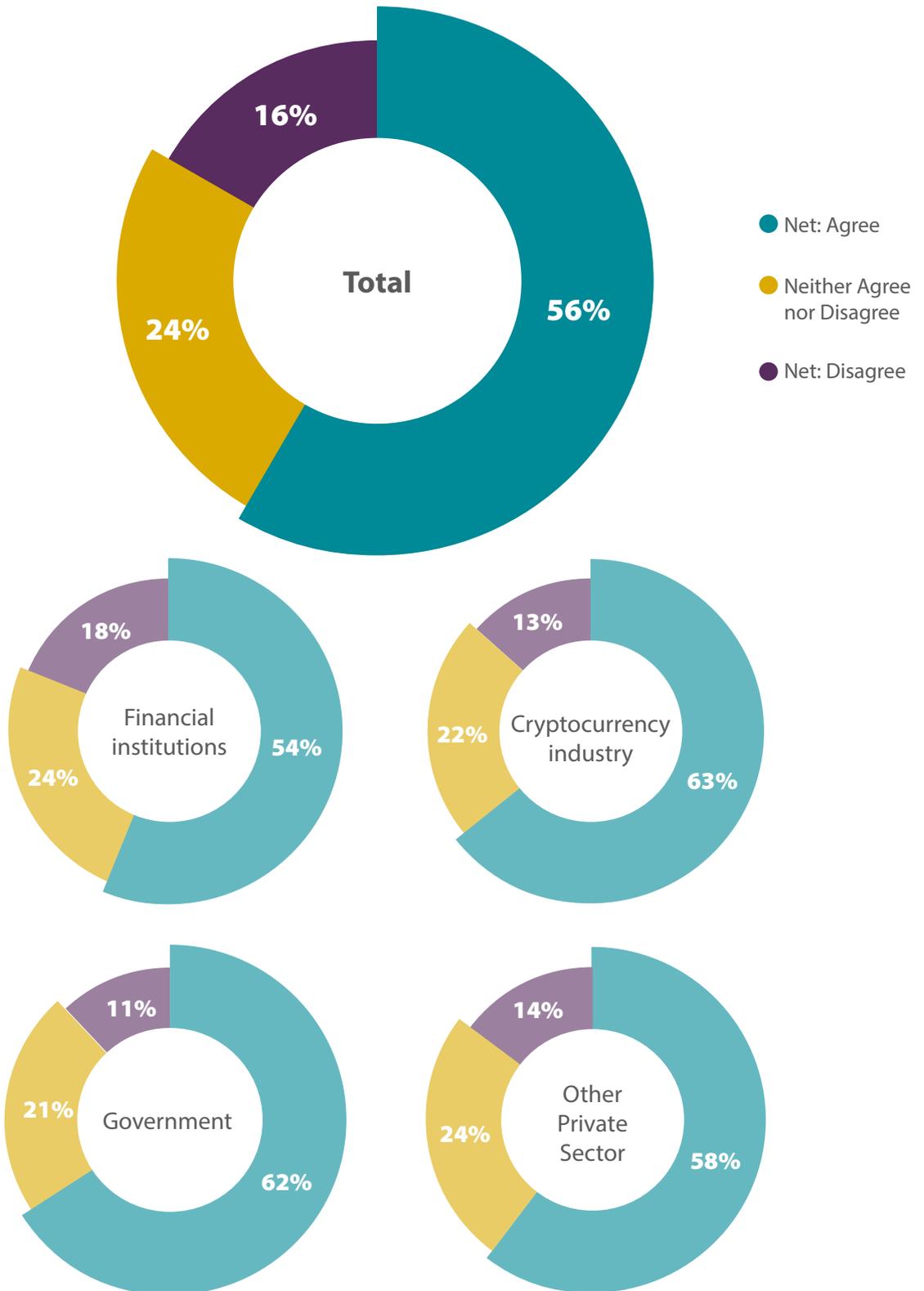


Chart Excludes 'Don't Know' Responses
Base: All respondents

Over three-quarters of all respondents seek best practice guidance from non-governmental organisations.

I look for guidance from non-Governmental organisations (e.g. FATF, trade bodies, blockchain associations) to guide best practice

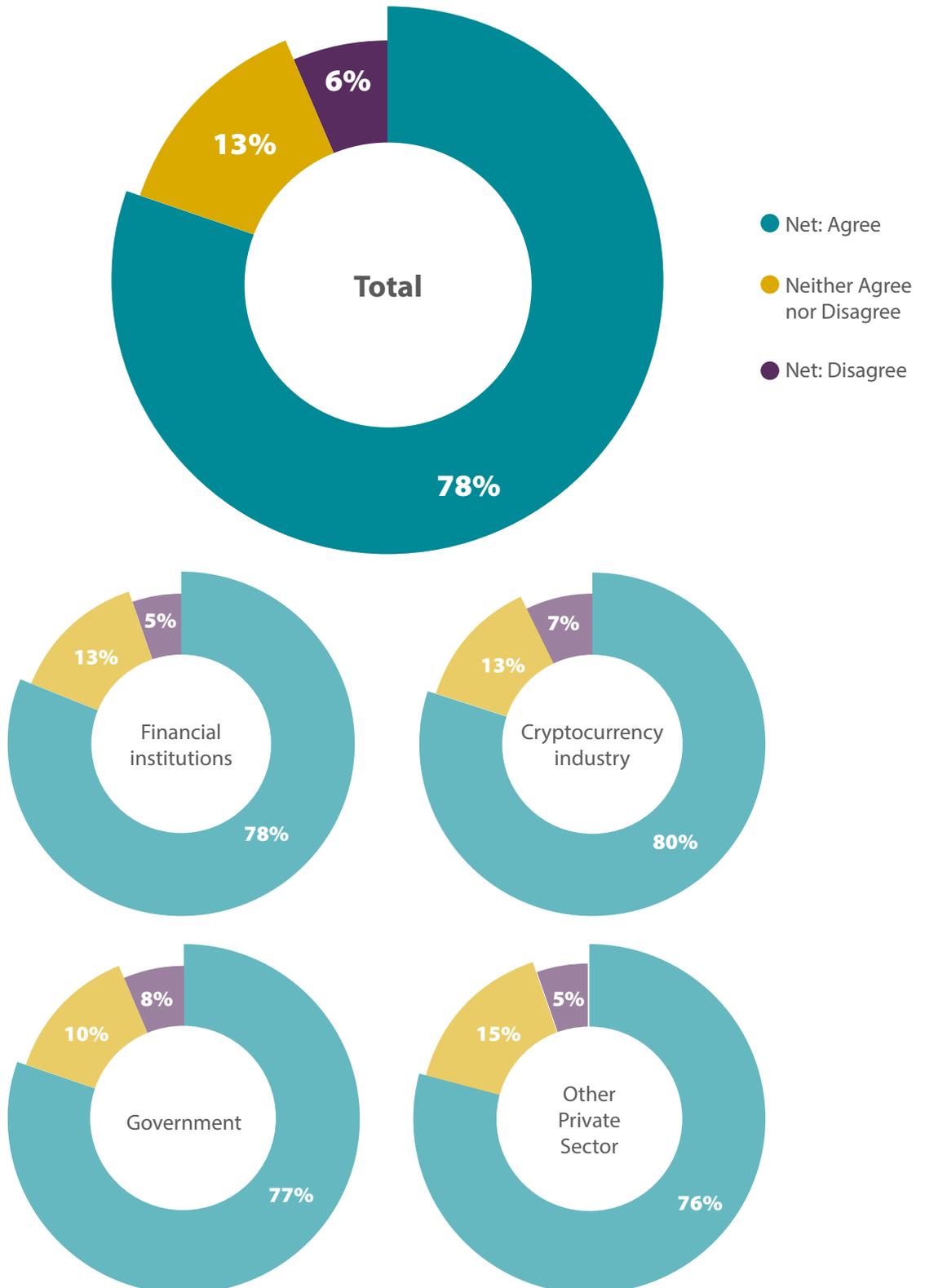


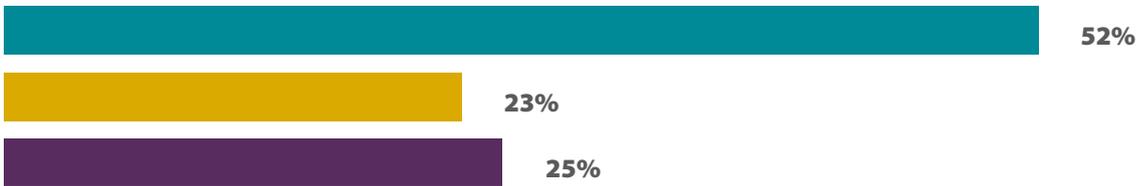
Chart Excludes 'Don't Know' Responses
Base: All respondents

Half of respondents think risks to cryptocurrency are best countered at international level by organisations such as the FATF

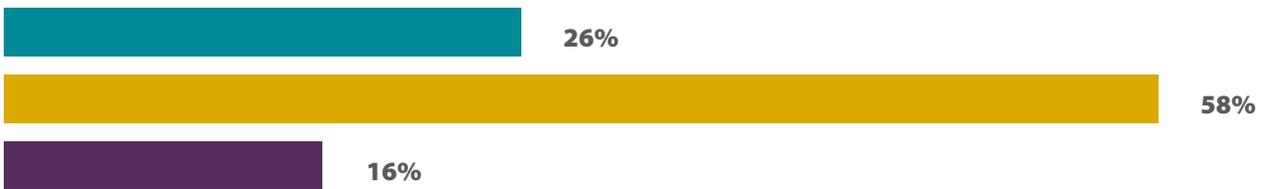
When thinking about the best way forward to counter cryptocurrency AML/financial crime risk, who is mainly responsible for improved regulation and compliance?

● Ranked as #1 ● Ranked as #2 ● Ranked as #3

Any risks related to cryptocurrency are best countered at an **international level/by international organisations like FATF**



Any risks related to cryptocurrency are best countered at a **national level/by individual Government**



Any risks related to cryptocurrency are best countered at a **company level/by individual exchanges**



Base: All respondents

Half of all respondents think that cryptocurrency AML/financial crime risk is best countered at the international level, by organisations such as FATF. Those working in the cryptocurrency industry are twice as likely as other respondents to think risks are best countered at company level by individual exchanges

When thinking about the best way forward to counter cryptocurrency AML/financial crime risk, who is mainly responsible for improved regulation and compliance?

Financial institutions

Any risks related to cryptocurrency are best countered at an **international level/by international organisations like FATF**



Any risks related to cryptocurrency are best countered at a **national level/by individual Government**



Any risks related to cryptocurrency are best countered at a **company level/by individual exchanges**



Cryptocurrency industry

Any risks related to cryptocurrency are best countered at an **international level/by international organisations like FATF**



Any risks related to cryptocurrency are best countered at a **company level/by individual exchanges**



Any risks related to cryptocurrency are best countered at a **national level/by individual Government**



Government

Any risks related to cryptocurrency are best countered at an **international level/by international organisations like FATF**



Any risks related to cryptocurrency are best countered at a **national level/by individual Government**



Any risks related to cryptocurrency are best countered at a **company level/by individual exchanges**



Other private sector

Any risks related to cryptocurrency are best countered at an **international level/by international organisations like FATF**



Any risks related to cryptocurrency are best countered at a **national level/by individual Government**



Any risks related to cryptocurrency are best countered at a **company level/by individual exchanges**



● Ranked as #1 ● Ranked as #2 ● Ranked as #3

Respondents are generally more likely to agree than disagree that the Travel Rule will be an effective way to mitigate cryptocurrency AML/CTF risk. Over half of those in the cryptocurrency industry, however, disagree

The Travel Rule, once fully implemented, will be an effective way to mitigate AML/CTF cryptocurrency risk

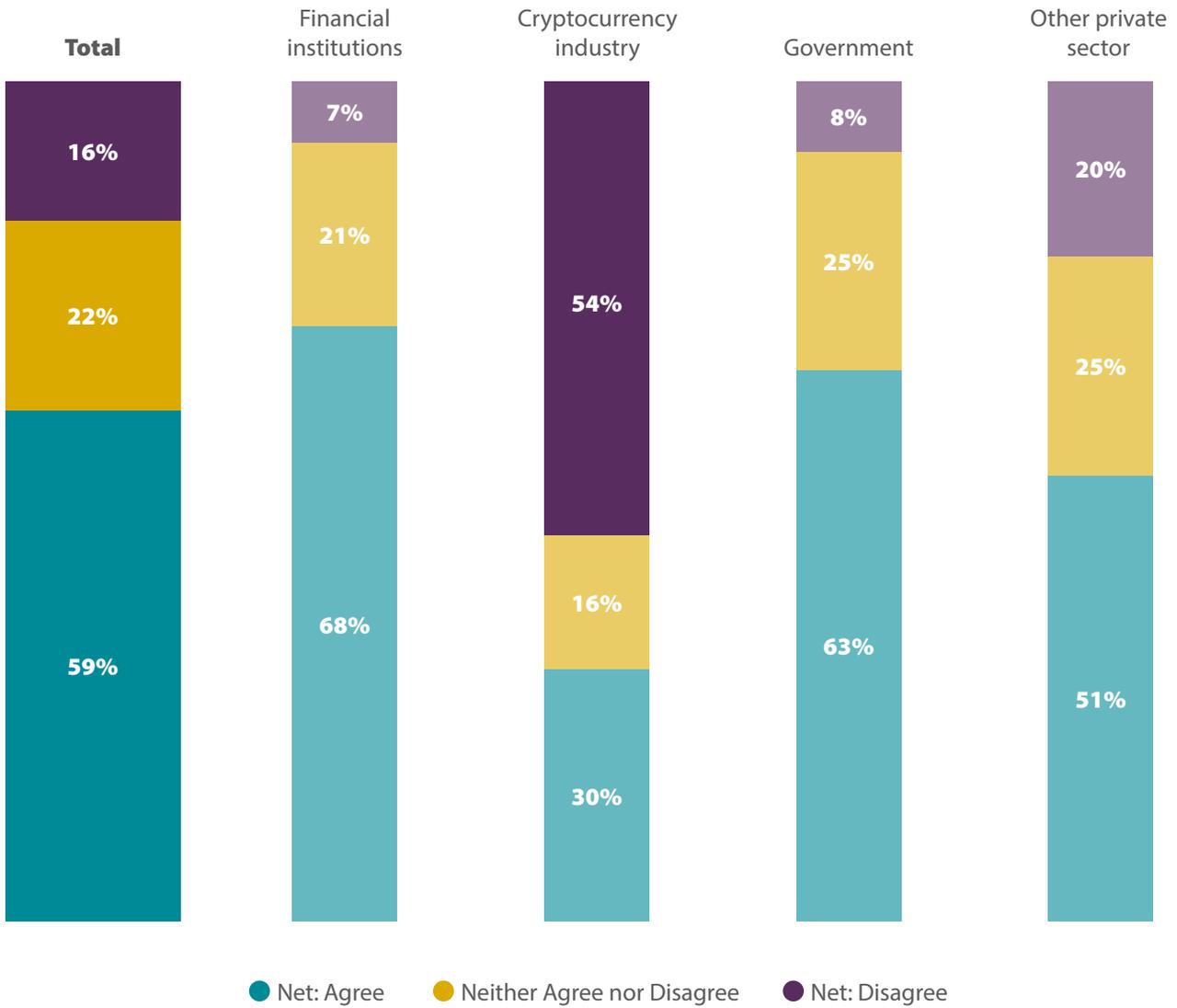


Chart excludes 'Don't Know' responses
Base: All respondents familiar with Travel Rule (352); Financial institutions (169), Cryptocurrency industry (50), Government (72) Other private sector (61)

REGIONAL PERCEPTIONS BY BANKS



Regional Perceptions by Banks

Due to the large number of responses received from individuals working in financial institutions, it was possible to able to break down answers for this group based on their geographic location.⁶ For the following questions, there are distinct differences in how respondents in financial institutions in different regions of the world responded.

Respondents working in North American (43%) and European (48%) FIs are more confident than respondents in Asian FIs (38%) in financial institutions' understanding of cryptocurrency risks.⁷

However, respondents working in Asian FIs appear to be the most friendly overall towards cryptocurrency. When asked if cryptocurrency is easier to use than fiat currency, a large percentage (43%) of respondents working in Asian FIs agree, while less than one-fifth of respondents working in North American (9%) and European (15%) FIs agree.

Respondents working in Asian FIs are also more optimistic about future cryptocurrency ease of use and its role in financial inclusion. Almost half (46%) of respondents working in Asian FIs indicate that they think cryptocurrency will be easier to use than fiat currency in five years, and over half (53%) say that cryptocurrency will be an effective tool for financial inclusion in the future.

6. Geographic location refers to the continent in which the Financial institutions is based/headquartered, not the respondent's personal location.

7. Other regions did not have large enough sample sizes of FI respondents to create statistically significant data.

Overall, those working in financial institutions are likely to think their industry understands cryptocurrency risks poorly

How well or poorly do you feel the previous cryptocurrency financial crime risks are understood by Financial institutions in your jurisdiction?

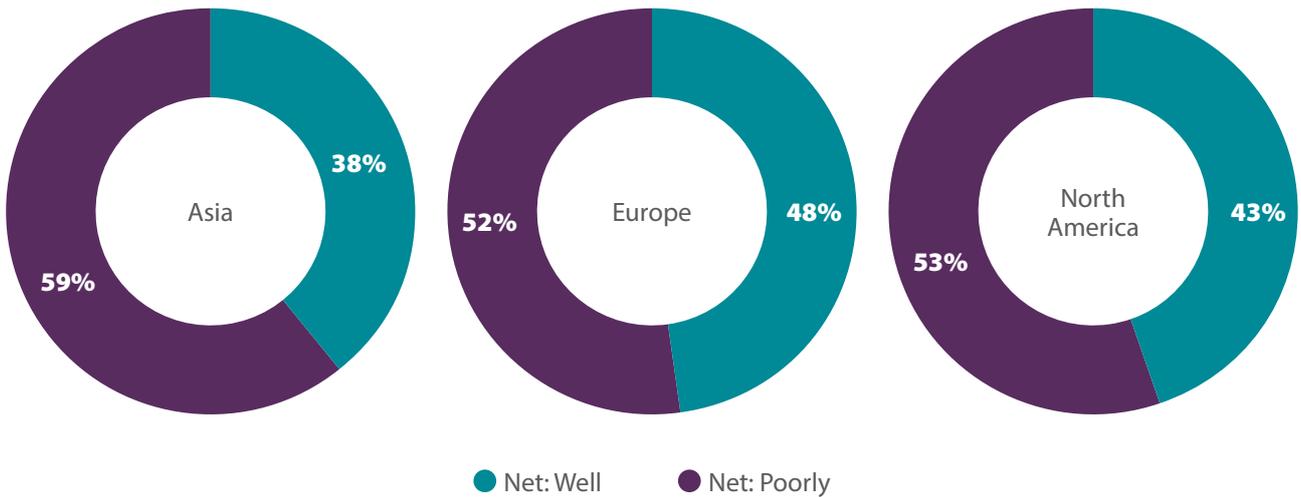


Chart excludes 'Don't Know' responses
 Base: All respondents at financial organisations based in North America (92), Europe (62), Asia (68)

Respondents in Europe are most likely to disagree that cryptocurrency is easier to use than fiat currency, while respondents in Asia are more confident in cryptocurrency's ease of use

Cryptocurrency is easier to use than fiat currency

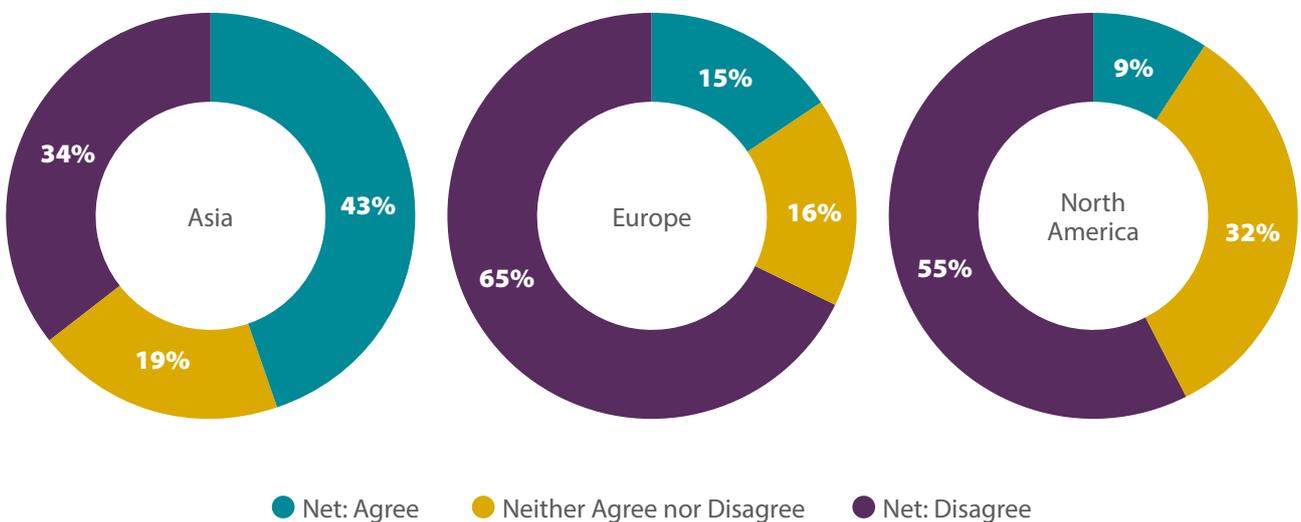


Chart excludes 'Don't Know' responses
 Base: All respondents at financial organisations based in North America (92), Europe (62), Asia (68)

Respondents in Asia are more likely to agree that cryptocurrency will be easier to use than fiat currency in five years, while respondents in Europe and North America disagree

In five years, cryptocurrency will be easier to use than fiat currency

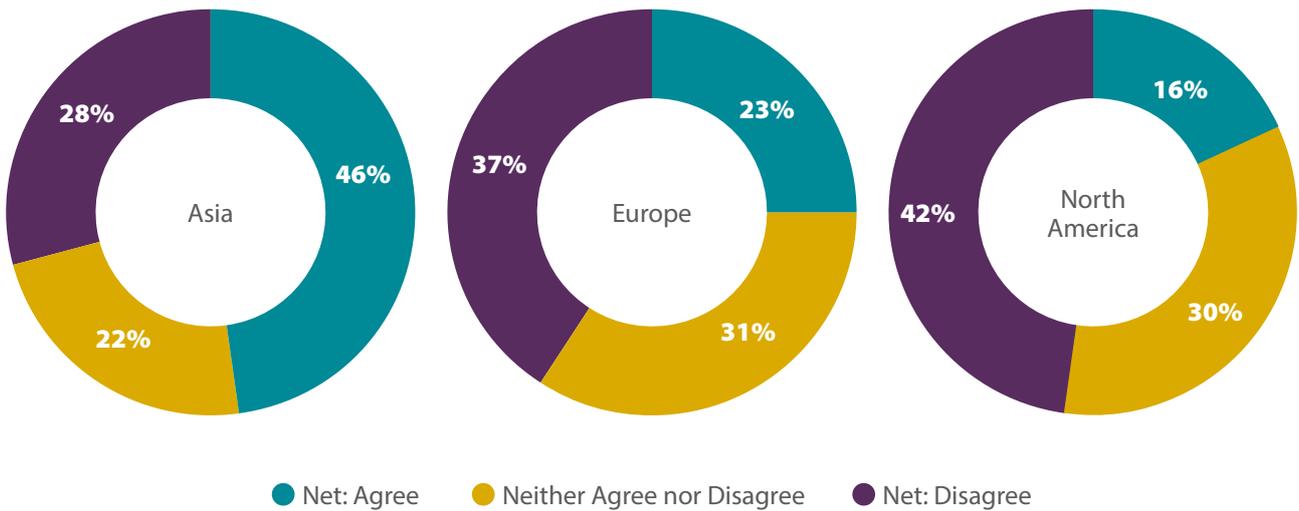


Chart excludes 'Don't Know' responses
 Base: All respondents at financial organisations based in North America (92), Europe (62), Asia (68)

Financial institutions respondents in Asia are more likely to agree than disagree that cryptocurrencies will be an effective tool to secure financial inclusion in five years, while respondents in North America and Europe are split

In five years, cryptocurrencies will be an effective tool for financial inclusion

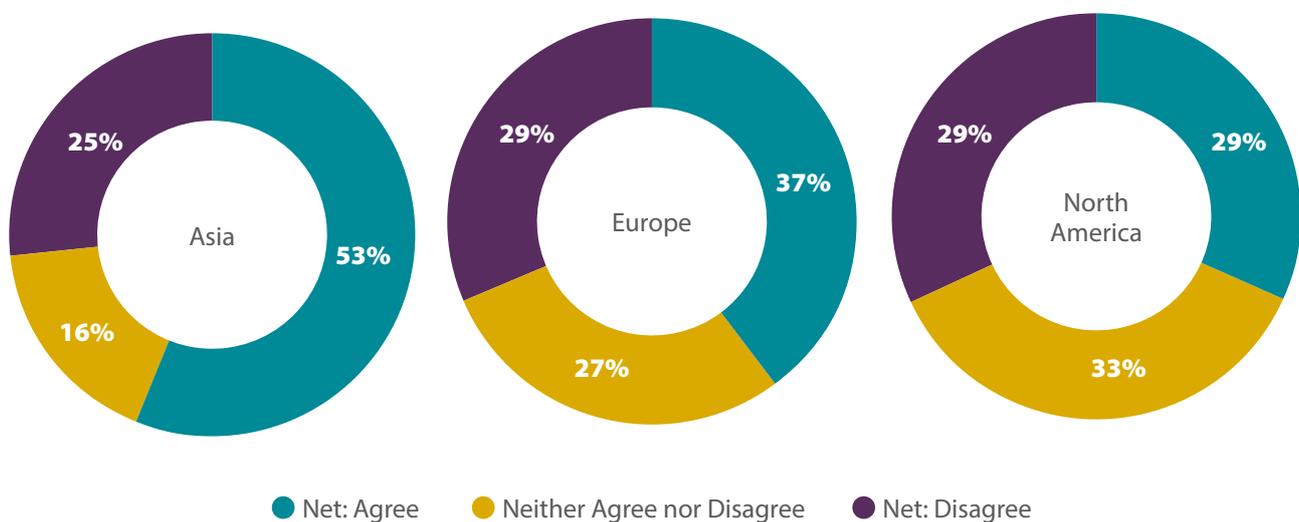


Chart excludes 'Don't Know' responses
 Base: All respondents at financial organisations based in North America (92), Europe (62), Asia (68)

THE FUTURE OF CRYPTOCURRENCY



Future of Cryptocurrency

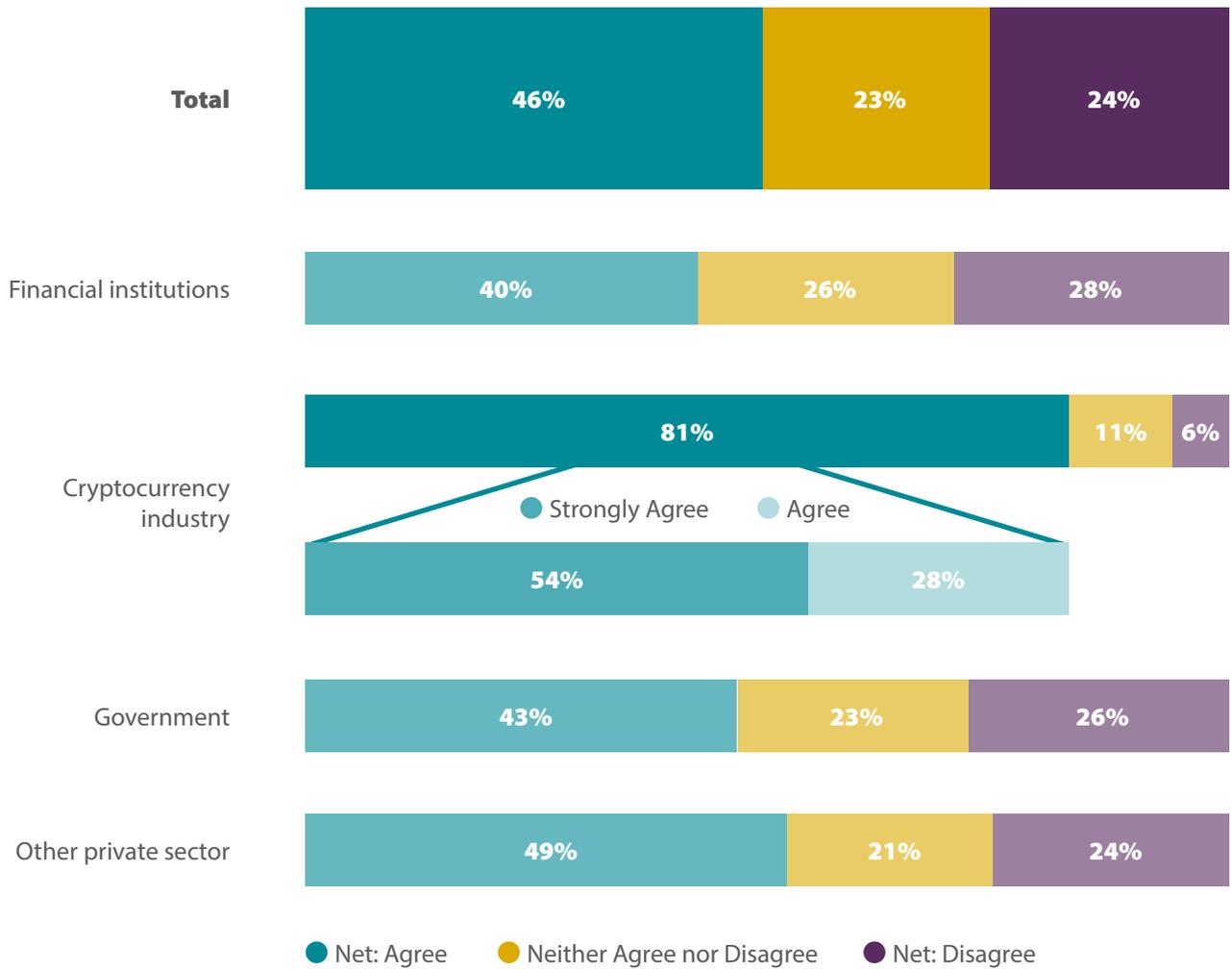
The survey asked respondents for their views on what the cryptocurrency landscape will look like in five years' time.

Overall, respondents are more likely to agree than disagree that in five years, cryptocurrency will be an effective tool for financial inclusion. The cryptocurrency industry overwhelmingly agrees (81%) with this statement, echoing their views on the current role of cryptocurrency in financial inclusion currently.

Respondents still believe that the main use of cryptocurrency in five years will be investment and speculation, but day-to-day payments ranks second, with illicit purposes moved to third. The cryptocurrency industry specifically said that day-to-day payments will become the main use of cryptocurrency.

All respondents are more likely to agree than disagree that in five years, cryptocurrencies will be an effective tool for financial inclusion

In five years, cryptocurrencies will be an effective tool for financial inclusion



N.b. Chart excludes 'Don't Know' responses

Base: All respondents

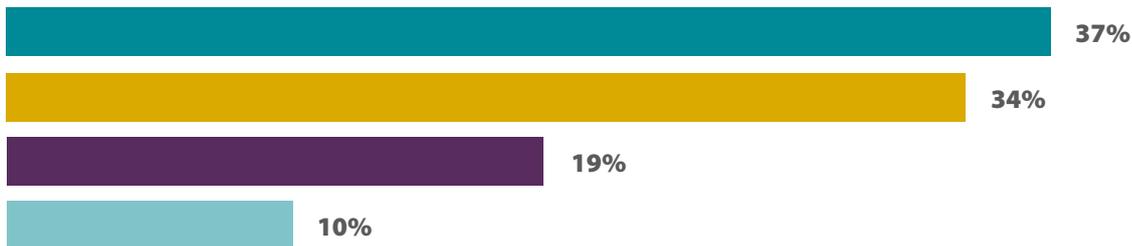


In five years, respondents still believe the main use for cryptocurrency will be investments, although three-tenths believe it will mainly be used for day-to-day payments

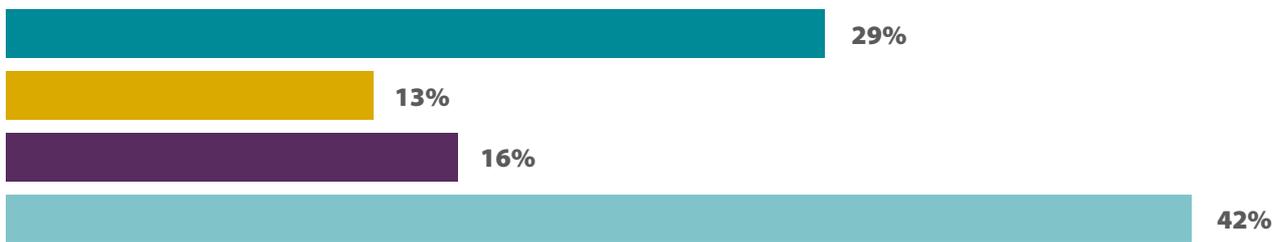
In the future, cryptocurrency will be mainly used for...

● Ranked as #1 ● Ranked as #2 ● Ranked as #3 ● Ranked as #4

Investment and speculation



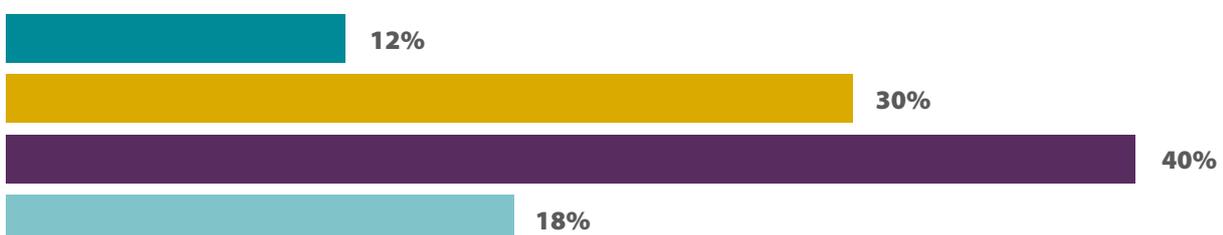
Day-to-day payments



Illicit purposes



Occasional payments

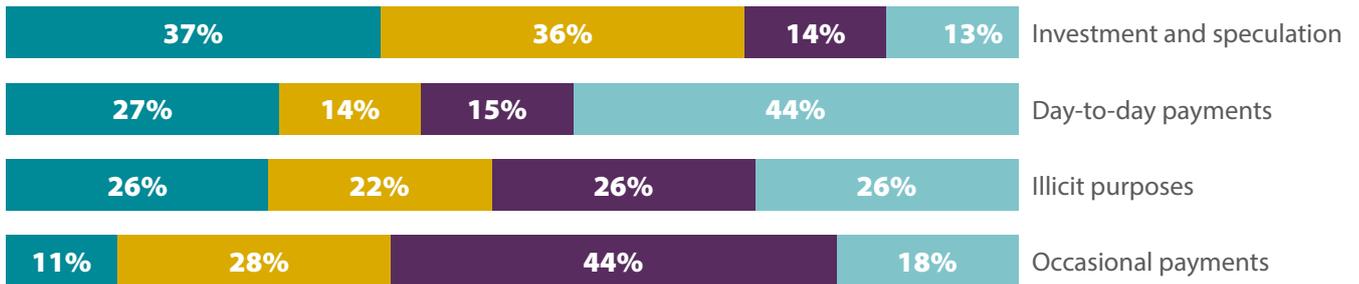




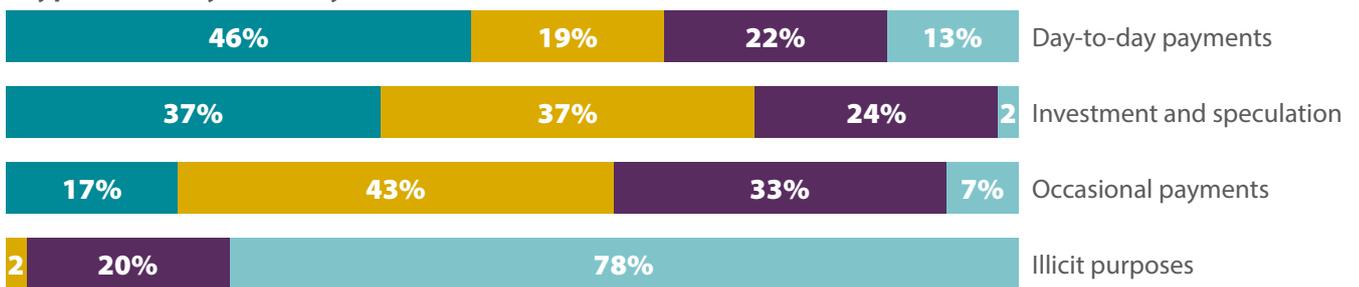
All audiences except those in the cryptocurrency industry believe that cryptocurrency will be primarily used for investment and speculation in the future. However, there is an increase in the proportion of respondents thinking cryptocurrencies will be used in day-to-day payments

In the future, cryptocurrency will be mainly used for...

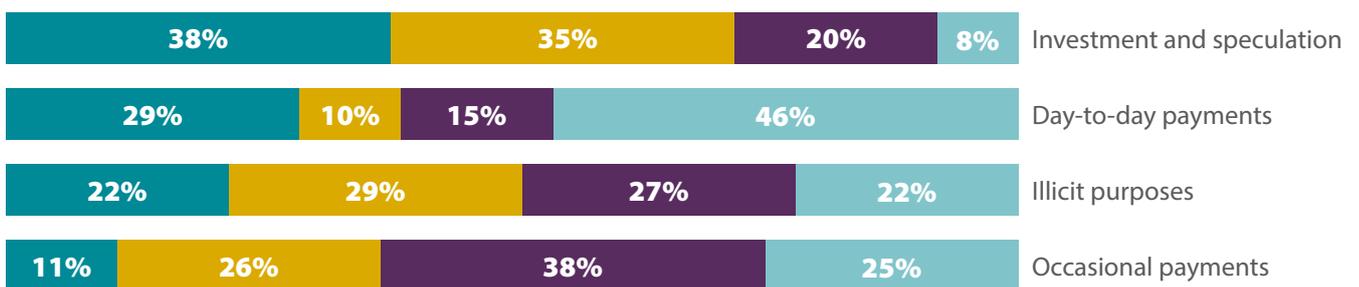
Financial institutions



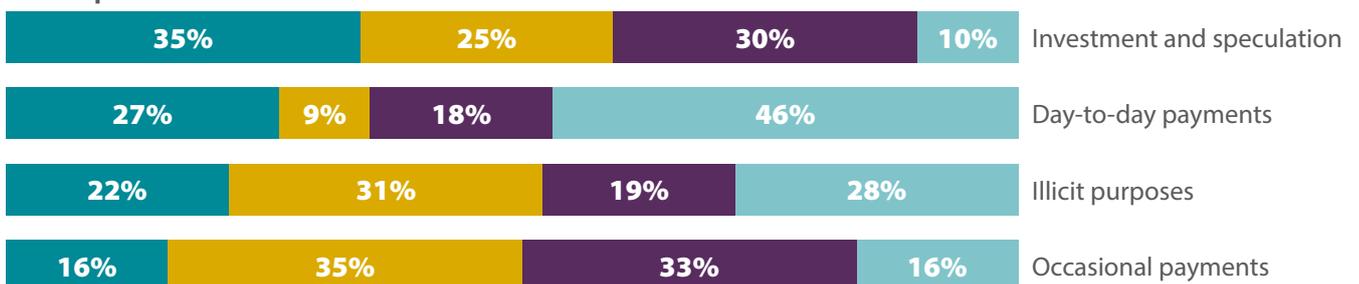
Cryptocurrency industry



Government



Other private sector



● Ranked as #1 ● Ranked as #2 ● Ranked as #3 ● Ranked as #4

ANNEX: DEFINITIONS



Annex: Definitions

The following is the list of terms as provided to survey respondents in hover text.

- Blockchain analytics/tracing:** The process of analysing and tracking cryptocurrency transactions through the blockchain, in order to discover useful information about the actors involved in the transactions. Private sector companies accomplish this at large scale, offering their services to other actors, including law enforcement and cryptocurrency exchanges.
- Cryptocurrency exchange:** A service provider that allows cryptocurrencies to be converted to fiat currencies and/or other cryptocurrencies.
- Cryptocurrency mixer:** A service that “mixes” cryptocurrencies of numerous users together prior to sending to the recipient, allowing for increased anonymity in the transaction. Also known as a tumbler.
- Custodial wallet:** A cryptocurrency service in which a user’s private keys are stored by a third party.
- Fiat currency:** Legal tender whose value is backed by the issuing government (such as the GBP or USD).
- FinTech:** A financial services provider with incorporated technology.
- Initial Coin Offering (ICO):** Similar to an IPO (initial public offering), this is a fundraising tool used by the cryptocurrency industry in which tokens are purchased (either with cryptocurrency or fiat currency) by investors. The value of these tokens increases as popularity of use increases.
- Neobank:** A type of financial institution that operates exclusively online and does not have traditional physical branch networks.
- RegTech:** A company providing technological services to assist financial institutions with compliance under regulatory obligations.
- Stablecoins:** A cryptocurrency whose value is either fixed to a specific fiat currency (e.g. the US dollar) or backed by other assets (e.g. a basket of currencies) in order to provide increased security and thus decrease price volatility. The most well-known example of this is Facebook’s proposed stablecoin, Libra.