FinTech at Cornell

Cornell Convenes

FINTECH AT CORNELL and CORNELL CONVENES

Report of the Cornell SC Johnson College of Business

Cornell Convenes 2023 Roundtable Forum: Toward a New Bretton Woods

9:00 am - 12:00 pm April 18, 2023 | Washington DC

I | BACKGROUND

DISCLAIMER: This background section is not intended to be comprehensive. It is provided to give the reader some context as to events that occurred before and after the roundtable. The issues raised in *Cornell Convenes: Toward a New Bretton Woods* in April of 2023 continue to be debated.

The World of Central Bank Digital Currencies and Stablecoins

Digital assets, including Central Bank Digital Currencies (CBDCs) and stablecoins, are global phenomena. They are powered by new technologies and touch all types of finance systems, from mature to emerging markets. They offer potential solutions to modernize financial systems, and both private industry and governments are interested in experimenting with them. Private industry has focused on Decentralized Finance (DeFi) and stablecoins while governments are exploring Central Bank Digital Currencies (CBDCs), which are largely in developmental stages.

Benefits often cited for stablecoins include eliminating the need for a third party to be involved in transactions, enabling cost efficient and faster transactions, providing greater user control over privacy and data, and increasing accessibility for those who have historically had limited access to financial services. There are risks, too. There are mixed strong opinions as to whether virtual currencies provide more opportunity for fraud and conversely whether they provide significantly better tools than those that exist in fiat systems to track fraud. What is clear is that the immaturity of the current virtual currency systems, tied with a lack of regulatory clarity and education, have opened the world of digital assets to a distinct set of vulnerabilities.

Despite the current rudimentary state of virtual currency systems, many feel that if employed correctly, these new types of transactions, could be an exponential catalyst for a country's economic growth and influence on the global market, meaning the race is on to establish a harmonious regulatory and interoperable operational environment for digital assets in all countries. Likewise, the race appears to be on for whether CBDCs will be deployed and which countries will dominate, if any.

Regulation Under The Spotlight

Arguably, one of the most significant events in the recent history of digital assets is the fall of FTX in November 2022, with repercussions worldwide. Regulators to this day are being asked why nothing was done concerning the fraudulent activity that led to its collapse. It is notable that Sam Bankman-Fried (SBF) was found guilty of all seven criminal charges brought against him.

In the USA, the Securities and Exchange Commission (SEC) has been active in enforcement actions in the cryptocurrency arena, resulting in court rulings that are often contradictory. The SEC has not provided clear and easy-to-follow rules for this growing sector. Congress is currently debating legislation to provide guidance, but at the time of publishing this paper, no new laws have been passed. This creates uncertainty in the US. Other regions and countries have stepped into the gap left by the US and have led by successfully implementing regulatory frameworks, such as in the EU, Markets in Crypto-Assets Regulation (MiCA), Hong Kong, Japan, and Singapore.

Coupled with the uncertainty of digital assets, there have been bank failures that some argue are targeted to effectively outlaw a bank from engaging with cryptocurrencies or stablecoins.[1] The domino effect of severe mistrust in many financial institutions has contributed to the need for more transparency and accessibility, faster payments, increased control of data privacy, and better-refined questions about who should control the way we can use our assets.

CBDCs

A CBDC is a digital designation of a country's fiat currency. It is issued by the Central Bank of a country and, therefore, is regulated by that country's government. The Atlantic Council states eleven countries, including Nigeria, The Bahamas, and Jamaica, have launched CBDCs.

Many others are playing in the sandbox. The New York Fed published the results of Phase II Project Cedar in May of 2023, concluding that "DLT (Distributed Ledger Technology) could support enhancements to cross-border multi-currency payments and settlements." Interoperability and autonomy, atomic settlement, and near real-time settlement are the findings listed. In April of 2023, Federal Reserve governor Michelle Bowman said in a speech that "While the Federal Reserve plays an important role in these ongoing discussions and technical research, the Fed would not implement a U.S. CBDC without the approval of Congress." See source.

In June 2023, the Bank for International Settlements (BIS) and the Bank of England completed the CBDC trial Rosalind across various use cases, including parent-child wallets and offline payments. This trial addresses privacy concerns by safeguarding Personally Identifiable Information (PII) with the payment provider and sending only pseudonymous information to the central bank.

[1] Potentially targeted banks include Silicon Valley Bank, Signature Bank, and Heartland Tri-State Bank. Other troubled banks with non-crypto issues around that time include First Republic Bank and Credit Suisse from outside the US.

Research on privacy from the Digital Dollar Project for CBDCs describes the characteristics of a CBDC. It states the CBDC should be available without undue government surveillance, and should also be private, secure, accessible, and transparent. The Digital Dollar Project is continuing research on these issues. Their report can be found here.

Stablecoins

A stablecoin is issued by a private entity. The most popular stablecoins by market capitalization are Tether and USDC. Tether, a stablecoin issued outside the US, claims "All Tether tokens (USD₮) are pegged at 1-to-1 with a matching fiat currency and are backed 100% by Tether's reserves." Another company, Circle, issues USDC, and claims "every digital dollar of USDC is always redeemable 1:1 for US dollars."[2]

According to CoinMarketCap, the total market cap for Tether as of November 20th, 2023 is approximately US$87 billion, while for USDC the total market cap is around US$24 billion. Tether has never provided a full audit. USDC has been audited annually since 2018 and is now partnering with Deloitte, as of January 2023.

The private sector sees a clear use for stablecoins. Innovation is profitable. Interestingly, as stablecoin regulation is being debated, Janet Yellen suggested that the dollar was one of the currencies under threat. A USA stablecoin can help strengthen the dollar and benefit national security. Without proper regulation, the US runs the risk of stablecoins being pushed offshore out of US reach. Investors financing stablecoin projects will turn elsewhere in the world if the US does not act now and pass clear legislation.

The dollar has been the strongest global currency for over sixty years (incidentally, the *Bretton Woods* system pegged the dollar to gold, and consequently other countries pegged their currencies to the dollar). Now, other countries are seizing the digital era to overtake the dollar. China (the world's second-largest economy), is forming economic coalitions with other BRICS countries (Brazil, Russia, India, China, and South Africa) to create a stablecoin, some members of which have US-led sanctions against them. As of August 2023, they continued to invite other member countries.

Elsewhere, Hong Kong plans a stablecoin launch for 2024, forging a pathway and potentially "acting as a sandbox for China," while the rest of the world debates how to move forward. The rules surrounding stablecoins place importance on consumer protection, focusing on fiat-pegged stablecoins that can be redeemed for fiat in a short period of time.

[2] Each of these company's claims can be found on their websites.

The Republic of Palau is another nation to pilot test a US dollar-backed stablecoin, with a press release honoring the success of the phase one pilot test in July 2023. The same announcement said that the next phases of the test will be rolled out later this year.

In July 2023, news broke that Circle is set to issue a stablecoin in Japan after new legislation came into effect, teamed with Circle's credibility gained from independent audits. Japan's revised Payment Services Act recognizes stablecoins as legal tender. Singapore has finalized a stablecoin regulatory framework for which issuers must abide by value stability, capital, redemption at par, and disclosure requirements.

Back on US soil, PayPal launched their PayPal USD (PYUSD) stablecoin on August 7th, 2023. This is notable because PayPal has already been dealing with cross-border payments for some of its 435 million users. Just shy of one month following, Visa has also announced the completion of its pilot and the expansion of its stablecoin settlement capabilities with Circle's USDC. The crescendo is building in the private sector with these key industry players showing a keen interest in the technology.[3]

Waiting For Regulation

Stablecoin regulation is hotly debated in the USA. Stablecoin legislation faces a rocky road, but it is moving forward. The Clarity for Payment Stablecoins Act of 2023 has moved out of the House Financial Services Committee and is headed for full debate in the fall of 2023. While there is bipartisan support, so far, there is not as much as hoped for.

The regulatory framework states the following:

"*Only permitted issuers are allowed to issue a payment stablecoin for use by U.S. persons. Permitted issuers must be a subsidiary of an insured depository institution, a federal-qualified nonbank payment stablecoin issuer, or a state-qualified payment stablecoin issuer. In general, permitted issuers must be regulated by the appropriate federal regulator, however, state-qualified issuers must be regulated by an appropriate state regulator. The bill sets forth requirements for (1) the rehypothecation, or reusing, of such reserves; (2) providing custodial or safekeeping services for stablecoins or private keys; and (3) supervisory, examination, and enforcement authority over non-state qualified issuers.*

[3] While not on the subject of stablecoins, other big players are entering the crypto arena, most notably Blackrock with its ETF application in June 2023, followed by many others in the industry.

In addition, the bill places a two-year moratorium on new endogenously-collateralized stablecoins (i.e., stablecoins that rely on the value of another digital asset created or maintained by the same originator to maintain the fixed price).

Under the bill, permitted payment stablecoins are not considered securities under securities law." See source.

It should be noted that while we are awaiting full debate, the Federal Reserve issued bank guidelines for stablecoins issued by banks. Treasury asked for public opinion on proposed regulation which, as drafted, would include stablecoins.

The Federal Reserve has since August 2023 set guidelines for the banks' use of stablecoins. These guideline specifically require state member banks to get a written supervisory non objection from the Federal Reserve before issuing, holding, or transacting in dollar tokens. Lawmakers have criticized the advance, saying that the Fed was undermining congressional efforts to piece together some kind of regulation.

The US Treasury Department of the IRS proposed rules and a public hearing for November 2023. Under those rules, brokers must report in 2026, for the first time, any information on digital asset sales and exchanges that occurred in 2025.

In the courts, Grayscale's recent court win over the SEC has also stirred the industry. Significant institutional and retail demand for Exchange-Traded Funds (ETFs) and the recent win highlighted the SEC's different treatment of similar products, once again confirming that clear and methodical regulation is missing. Analysts believe Bitcoin ETFs may become a reality in the first quarter of 2024.

It is important for the USA to act quickly in its decision-making process because the question is not whether or not there should be a USA dollar stablecoin, but rather whether the USA can bring a stablecoin into circulation while protecting national security and financial stability before issuers elsewhere do.

The April 2023 *Cornell Convenes: Toward a New Bretton Woods* addressed many of the issues surrounding CBDCs and private programmable money. We are delighted to represent the discussion in this Report.

II | EXECUTIVE SUMMARY | THE CHALLENGE

The FinTech Initiative of Cornell SC Johnson College of Business held *Cornell Convenes: Toward a New Bretton Woods* in April 2023, reuniting regulators, former regulators, industry leaders, and academics to converse and offer undiluted insight into Central Bank Digital Currencies and stablecoins.[4] Chatham House Rule was employed to promote unrestrained participation.

Specific topics discussed include CBDC design choices, the implications for economic growth and stability, the effect on financial inclusion, the relationship between public- and private-sector administered digital assets, including CBDCs, the extent to which foreign CBDCs might undermine US financial centrality, and the potential risks insofar as financial crime is concerned. Given the broad global reach of these vigorously debated subjects, frank conversations are especially important across industry, regulation, and academia to foster understanding, with the participants talking with each other, rather than at each other. Where first principles emerged, the editors have noted them in this paper.

The discussion was divided into five chapters, starting with the chapter on *The Future of Money* which covered the implications and applications of CBDCs. The group then debated four more chapters, including *Balancing Surveillance and Privacy in Digital Frameworks*, *Technical Considerations for Digital Frameworks*, *Digital Wallets and the Future of Payments*, and *Ensuring Security and Trust in Digital Asset Transactions.* The group conversation is anonymously transcribed in this report, with the report authors offering summarized principles where they emerged.[5]

[4] The subjects of CBDCs and stablecoins were identified as areas of priority in the President's March 2022 Executive Order.

[5] Note: The contents of this report do not represent the views of Cornell University or the Cornell SC Johnson College of Business but rather those of the individuals participating in the Cornell Convenes Roundtable so listed.

III | LETTER FROM ANDREW KAROLYI

CHARLES FIELD KNIGHT DEAN
CORNELL SC JOHNSON COLLEGE OF BUSINESS

Dear Readers,

I am proud that the Cornell SC Johnson College of Business hosted this second consecutive annual critical dialogue, *Cornell Convenes: Toward a New Bretton Woods*, which focused on CBDCs and stablecoins. This discussion continues the 2022 Cornell Convenes conversation on digital assets spurred by President Biden's March 9, 2022, Executive Order on *Ensuring the Responsible Development of Digital Assets*. The controversy and unclear regulation that gave way to the first Cornell Convenes remains apparent, as does the need for broader and more concise analysis, which we wholeheartedly believe this select group of individuals can supply.

The Fintech at Cornell Initiative was launched by the SC Johnson College of Business a few years ago to deploy scholarly and industry expertise to consider the advancing capabilities of Decentralized Finance (DeFi), CBDCs, stablecoins, and digital assets, and the associated challenges and opportunities for business and society. Its academic fellows and industry collaborators are at the forefront of this rapidly evolving space.

This *Cornell Convenes* white paper will prove constructive to a broader understanding of the concerns surrounding CBDCs and stablecoins, offering responsible insight from a community of industry experts into the priorities and potential approaches to appropriate regulation.

The Cornell SC Johnson College of Business is dedicated to engagement and collaboration, and we will continue to support groundbreaking conversations like this one.

Sincerely yours,

Andrew Karolyi

IV | LETTER FROM SUSAN JOSEPH

EXECUTIVE DIRECTOR OF FINTECH AT CORNELL

Hello, and thank you for your interest in this conversation.

On April 18, 2023, we held *Cornell Convenes: Toward a New Bretton Woods* to address CBDCs and stablecoins. This event follows the structure of our inaugural event in 2022, which was borne of President Biden's Executive Order of March 9, 2022. In the persisting absence of a regulatory framework and new concerns and questions that have arisen in the year since our first meeting, this meeting brought together industry professionals for an enthusiastic and confidential debate.

My thanks and sincere appreciation go to thanks also to Andrew Karolyi and Lin William Cong, and to the Fintech at Cornell sponsors for their unflagging support of this work.

The April roundtable followed Chatham House Rule to encourage free-flowing conversation and purposely promote ungated opinions and input. Unsurprisingly, opinions differed. Our goal was not to achieve agreement on a concrete set of next steps. We aimed to identify and offer ways to consider the most salient issues. We achieved that. We were happy to take the first step in assembling these groups and intend to remain engaged in this dialogue, with future sessions planned.

I hope you'll read on and consider the varied perspectives and priorities expressed. I am eager to hear your thoughts on this conversation and the next iterations of our Cornell Convenes discussions about the potential benefits and concerns CBDCs and stablecoins present.

Yours,

Susan Joseph

V | LETTER FROM LIN WILLIAM CONG

FOUNDING FACULTY DIRECTOR
FINTECH AT CORNELL

Dear Readers,

For the past three years, Fintech at Cornell has been galvanized toward assembling the most comprehensive and engaged cohort of expert perspectives from Cornell and the global fintech community. That community continues growing and proving its commitment to lending cogent and discerning perspectives to this unique financial moment. Our generous sponsors dedicate their knowledge and resources. Executive Director Susan Joseph builds new bridges and strengthens our industry and policy networks. All of this is made possible by the leadership of the Cornell SC Johnson College of Business and the Fintech at Cornell fellows.

Everyone involved can see the profound potential for benefit and harm regarding CBDCs and stablecoins. Responsible action is necessary, especially concerning digital currencies. Responsible design will be essential, along with patient and attentive collaboration.

The Cornell Convenes group who gathered this year expressed seasoned perspectives from the regulatory, academic, and industry angles, and their conversation suggests possibilities for balancing priorities. They highlighted various points on various spectrums: between freedoms and protections, regulation and observation, privacy and transparency. Deliberate and focused communications and education channels will underpin every element of this work.

We hope the report provides an informative anchor for more rigorous studies and lively Debates. This conversation will continue.

Yours Faithfully,

Lin William Cong

VI | TABLE OF CONTENTS

VII | KEY TERMS

AML Legislation
Anti Money Laundering legislation attempts to halt the conversion of illegal money into legal money and is becoming ever stricter in order for financial service providers to eliminate financial crimes.

CBDC
A Central Bank Digital Currency is a form of digital money issued by a central bank. Its value is pegged to the country's currency value.

Decentralized Identity
A decentralized identity system envisions users controlling their identities, rather than central parties doing so, as is the current norm.

Forensics
Forensics, in the context of finance, includes fraud investigation and financial auditing skills to detect, prevent, and/or convict criminal financial activity.

KYC
Know Your Customer is a mandatory framework in traditional finance whereby institutions are to carry out due diligence concerning the identity of their customers.

LEI
A Legal Entity Identifier is a globally-recognized reference number that identifies an entity participating in a financial transaction.

Open-source
Open-source refers to software or source code that is publicly and freely available to access, modify, enhance and use.

Real-time Payment System
Real-time payments are initiated, cleared, and settled within seconds, regardless of the day or time.

Remittance
A remittance is a payment that is sent overseas.

Retail CBDC
A retail CBDC is issued by a central bank to consumers and businesses in a jurisdiction's financial system and is universally accessible.

Self-custodial Wallet
A self-custodial wallet is a place of storage for digital and cryptocurrency whereby only the holder can access the wallet. In contrast, a custodial wallet is one where a third party has the private key and can, therefore, also access the wallet.

Settlement
A settlement in finance is the delivery of securities that complete a trade.

Stablecoin
A stablecoin is any cryptocurrency whose value is pegged (fixed and determined) by another commodity, which could be a fiat currency, security, or cryptocurrency.

TradFi
Traditional Finance is a concept that englobes the traditional retail, commercial, and banking financial system.

Velocity of Money
The velocity of money is the rate, in time, at which money is exchanged in an economy.

Wholesale CBDC
A wholesale CBDC is issued by a central bank to be used for sizable (interbank) transactions and whose accessibility is limited to certain financial institutions.

ZK-Proof
Zero-knowledge Proofs are a cryptographic way to confirm the authenticity of something, such as an identity, without revealing the identity itself.

VIII | DISCUSSION SCOPE AND STRUCTURE

A list of pre-reads was distributed to participants before the event to contextualize the conversation. A list of these can be found in APPENDIX III.

The discussion was divided into five chapters of inquiry:

Chapter One: THE FUTURE OF MONEY: GOVERNMENT AND PRIVATE SYSTEMS
Chapter Two: BALANCING SURVEILLANCE AND PRIVACY IN DIGITAL FRAMEWORKS
Chapter Three: TECHNICAL CONSIDERATIONS FOR DIGITAL FRAMEWORKS
Chapter Four: DIGITAL WALLETS AND THE FUTURE OF PAYMENTS
Chapter Five: ENSURING SECURITY AND TRUST IN DIGITAL ASSET TRANSACTIONS

Each section contains the following:

- Data Visualization
- Discussion Highlights and Editors' Notes
- Anonymous Sticky Notes
- Analysis
    - Strongly Identified Topics
    - Key Takeaways
    - Big Ideas
    - Conclusion

IX | ACKNOWLEDGEMENTS

On behalf of Fintech at Cornell, the editors wish to thank the participants for their unabated collaboration in what was a productive discussion.

We also wish to thank our sponsors Broadridge and Ripple for their generous and full-throated support, and the host of the event, the Cosmos Club, for their warm welcome.

We thank Gary Weinstein for his thought partner leadership support in researching the topics to help refine the agenda.

We also thank the Cornell SC Johnson College of Business, dedicated to responsible and innovative finance at all levels. We hope this work will prove useful in developing an appropriate understanding and regulation of these dynamic financial events.

Tech Policy Institute

We would especially like to thank the Cornell Tech Policy Institute for their financial contribution, collaboration, and sponsorship. Their support was critical to making this event a success.

X | PARTICIPANTS

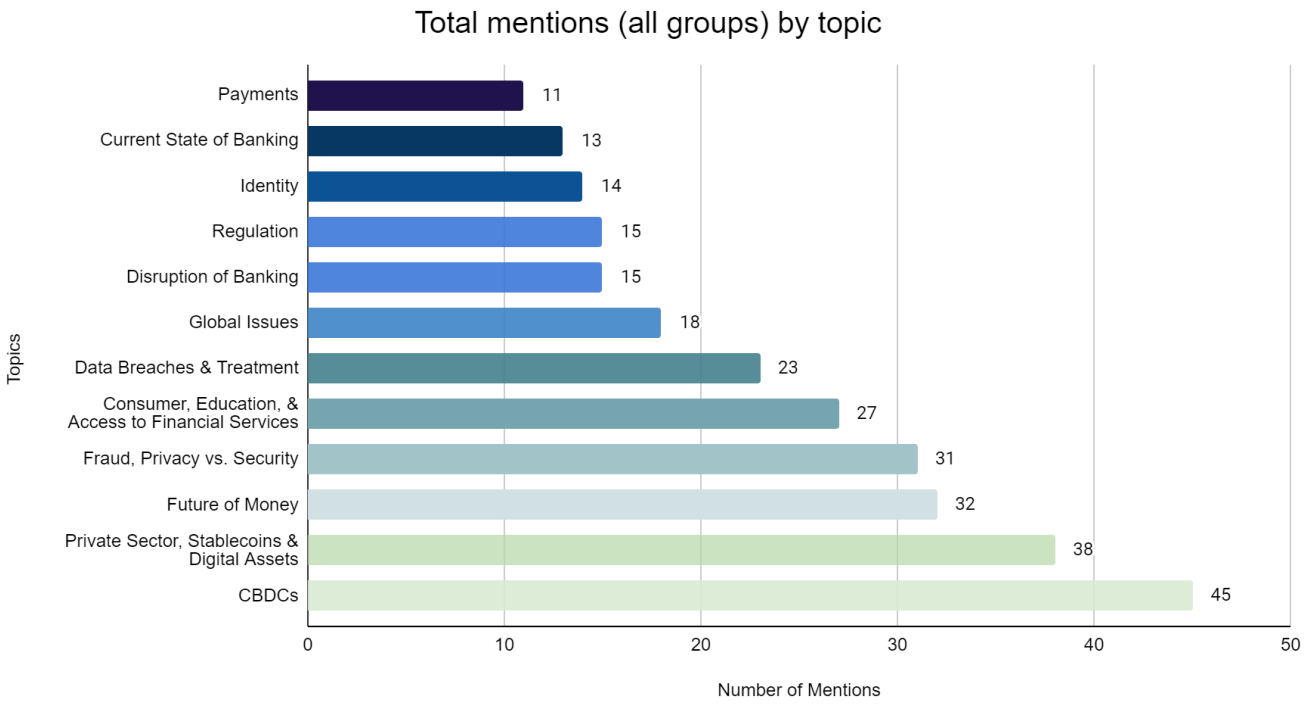
Natassja Aleksy
Jason Cave
Michael Donowitz
Will Drewry
Clark Flynt-Barr
Susan Friedman
Laluy Garduño
Ben Gray
Ashley Gunn
Jorge Herrada
Bill Hinman
Mei Lin Hu
Michelle Jackson
Liang Jensen
Susan Joseph
Jongho Kim
Amy Davine Kim (attending in my personal capacity)
Peter Krieger
Robert Krugman
Ananya Kumar
Simon Letort
Gordon Liao
Evgeny Lyandres
Ian P. Moloney
Dr. Lilly Muller
Prakash Neelakantan
Ijeoma Okoli
Tyler Parente
Anne Marie Pippin (attending in my personal capacity)
Eswar S. Prasad
George Pullen
Nilmini Rubin
Brad Scrivener
Maggie Sklar
German Soto Sanchez
David Taub
Gary Weinstein
Youwei Yang (attending in my personal capacity)
Bobby Yu
Elisha Yu

Fintech at Cornell Executive Director: Susan Joseph
Facilitator: Michelle Jackson
Scribe: Natassja Aleksy
Fintech at Cornell Student Fellows: Bobby Yu, Elisha Yu, Jongho Kim, Mei Lin Hu, Tyler Parente.
Cornell Outreach: Peter Krieger, Senior Director, External Relations, Cornell SC Johnson College of Business
Authors and Editors: Susan Joseph, Will Cong, Natassja Aleksy, Bobby Yu, Elisha Yu, Tyler Parente, Mary Lorson

XI | BEFORE WE BEGIN | DISCUSSION PERSPECTIVES

From the raw conversation, the editors extracted key ideas, classified them, and aggregated them by topic. Using idea and topic-level mention counts by sector (academia, regulatory, industry), we are able to identify priorities and the level of agreement among them. **The top 12 topics were further analyzed into their top two to five subtopics and their mentions in the different discussion chapters.** We discuss several stylized effects in the main body of the paper, leaving the rest to APPENDIX I and II.

Figure 1 presents the total number of mentions by topic with the top three topics being *CBDCs*, *Private Sector & Digital Assets*, and the *Future of Money*.



XII | CORNELL CONVENES | TABLE OF 12 MAIN TOPICS AND CORRESPONDING MAIN SUBTOPIC

Following on from Figure 1, we present the most discussed subtopics for each main topic.

Main Topic	Main Subtopic	Percentage Conversation Dominance of Subtopic
CBDCs	Can stablecoins and CBDCs co-exist?	27%
Consumer, Education, and Access to Financial Services	Financial Inclusion	37%
Current State of Banking	Bank Failure and Reputational Risks	61%
Data Breaches and Treatment	Data Breaches and Accountability	48%
Disruption of Banking	Banking Disruption	87%
The Future of Money	Secure Responsive Infrastructure	44%
Global Issues	CBDCs and The Potential for De-dollarization	44%
Identity	Creating and Verifying Identity	64%
Payments	Money Velocity	64%
Fraud, Privacy Versus Security	Privacy, Surveillance, and Government Control	74%
Private Sector, Stablecoins, and Digital Assets	Stablecoins and Payments	47%
Regulation	Digital Asset Framework	80%

From the table, we can infer that disruption of the financial system was a vigorously discussed topic important to all sectors.

SUBTOPICS

On the topic of CBDCs, the subtopics were: S*tablecoins and CBDC Co-exist? CBDC Research and Design, CBDCs Equal to Real-Time Payments? Surveillance and Privacy,* and *Fed and Dollar Limits*.

We present the subtopics in pie charts in the APPENDIX II and include the pie chart for *Topic 1: CBDC* below for illustrative purposes. For example, the *coexistence of stablecoins and CBDCs* was the most mentioned subtopic, while the notion of *CBDCs equal to real-time payments* was the least discussed.

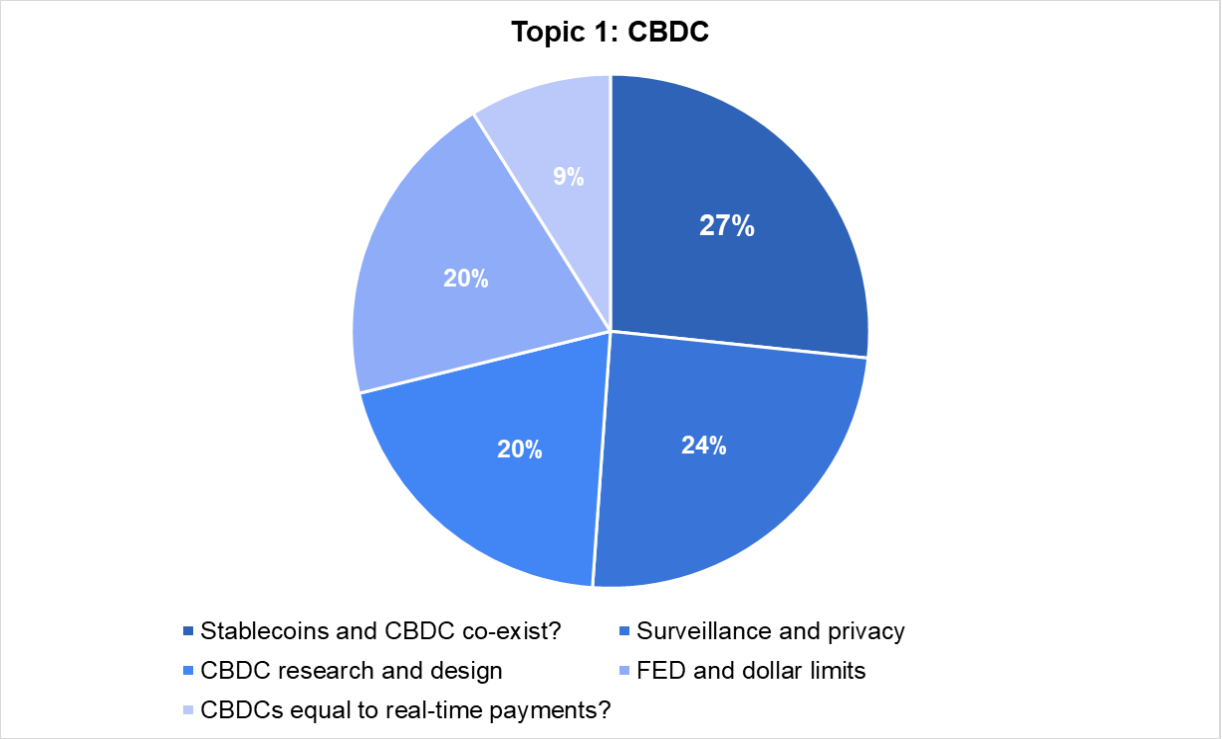
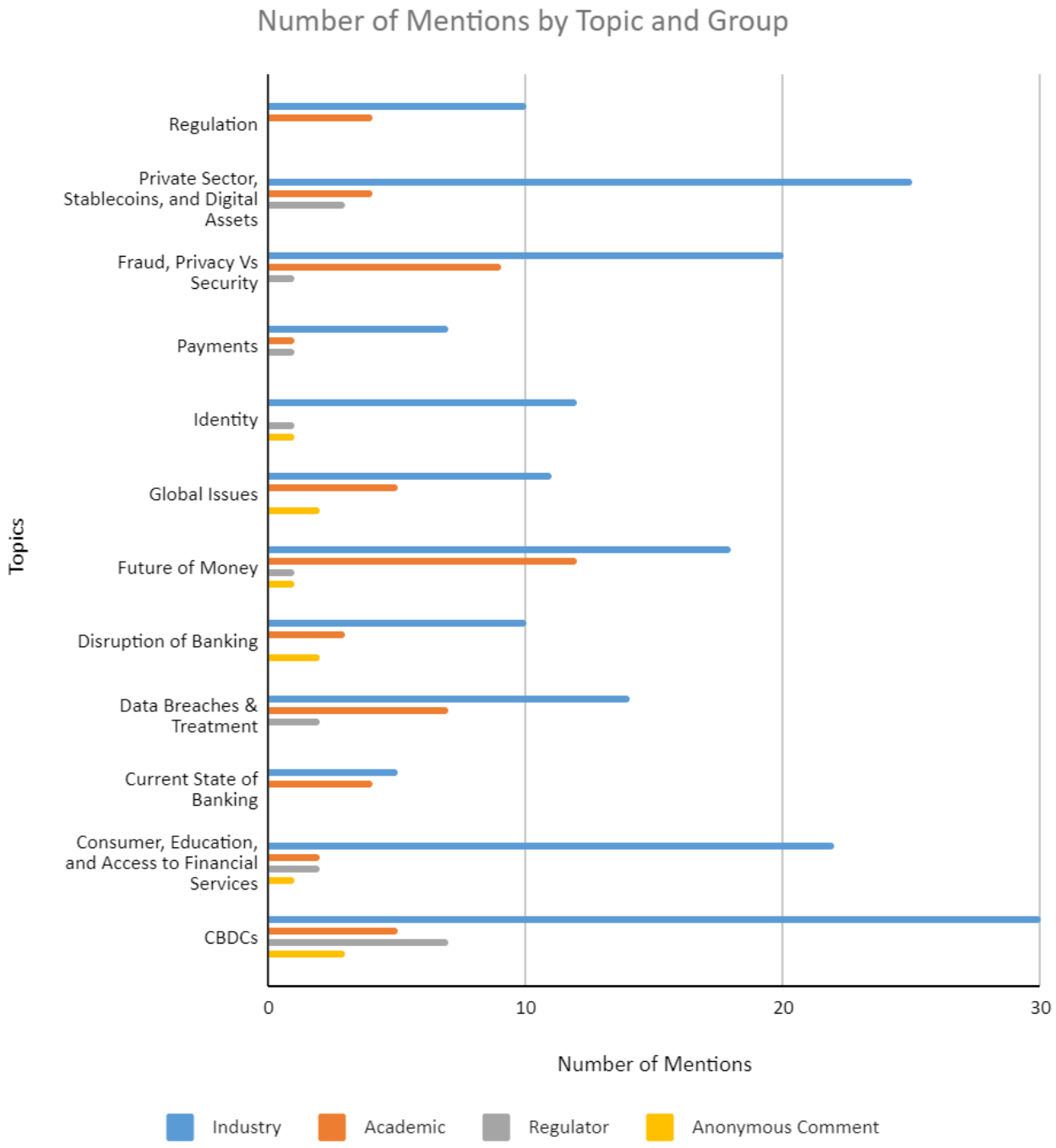


Figure 2: Number of Topic Mentions According to Sector



In *Figure 2,* we dissect the total topic-level mentions into counts by sector. As demonstrated in this figure, the industry led in thinking about *CBDCs*; *Private Sector, Stablecoins, and Digital Assets*; and *Consumer, Education, and Access to Financial Services*. We further include Pearson and Spearman correlation coefficients between idea-level mention count series for each sector. Pearson correlation measures the degree of co-movement (in terms of number of mentions),

while Spearman correlation estimates the ranking agreement (how rankings of ideas co-move between sectors).

Both coefficients range from -100% to 100% with a larger magnitude indicating a stronger effect. We find that the Pearson correlation is the highest at 83% between regulators and industry, indicating a strong correlation in terms of the number of mentions between the two sectors.

Industry and academia have a correlation coefficient of 29%, whereas the correlation between academia and regulators is 4%. This number should be taken with caution, given the relatively low number of mentions by regulators. As for the Spearman correlation, there is a similar pattern, with the industry-regulator coefficient being the highest at 75%, the industry-academia coefficient in the middle at 35%, and the academia-regulator coefficient the lowest at 11%. These patterns indicate a relatively high level of homogeneity between industry and regulators regarding topics of interest.

XIII | FIRST PRINCIPLES

The editors teased out four first principles from the discussion:

1. Balance user privacy and surveillance.
2. Create incentives for adoption.
3. Allocate liability fairly between users and issuers.
4. Provide education and transparency.

XIV | INTRODUCTION TO *CORNELL CONVENES: TOWARD A NEW BRETTON WOODS*

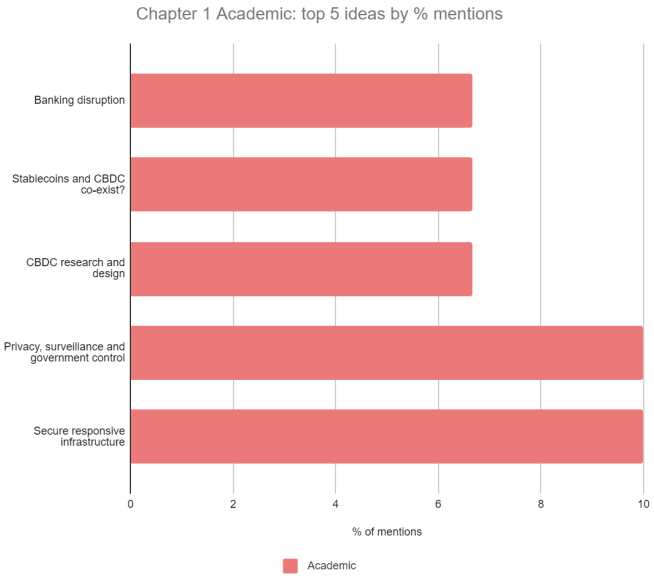
The participants were welcomed to this second series of Cornell Convenes roundtables. After thanking the cosponsors, the participants were reminded that the conversation would follow Chatham House Rule and be transformed into an anonymous report to be published and circulated.

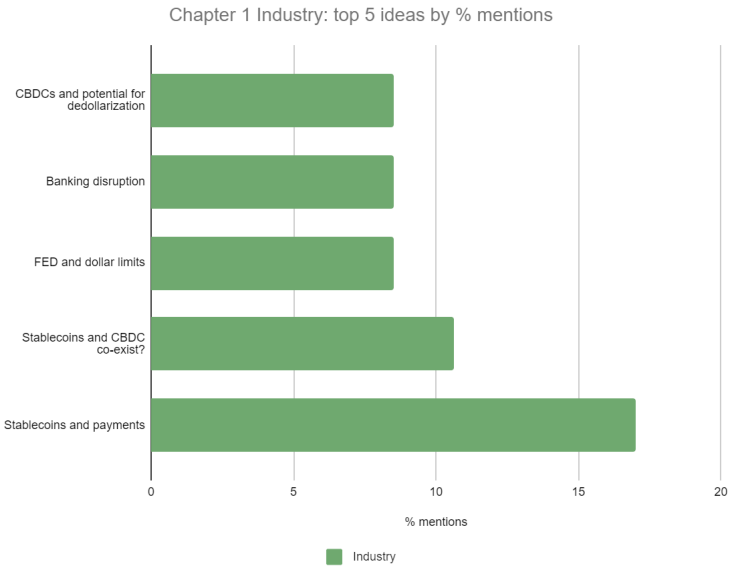
The discussion was opened with the following:

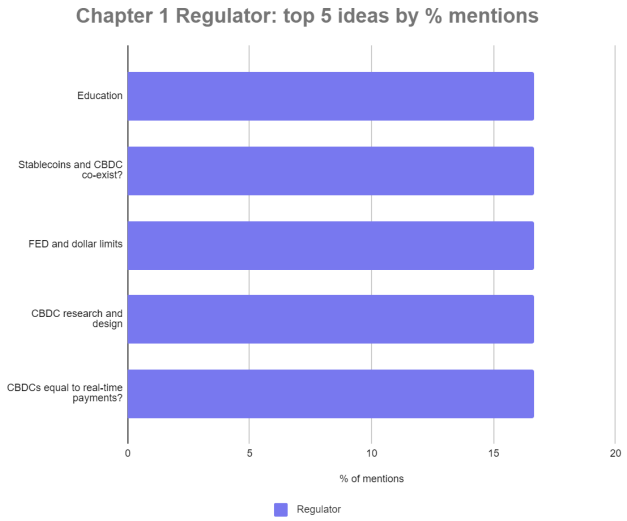
“At the moment, there are a lot of conversations with different points of view, but there aren’t a lot of conversations that unite those who can talk about this and make a change: academics, regulators, and industry experts. The point of this session is to spur this conversation. There isn’t a need to find a one-size-fits-all solution but to allow people to cross-discuss.”

XV | CHAPTER ONE | THE FUTURE OF MONEY: GOVERNMENT AND PRIVATE SYSTEMS DATA VISUALIZATION

In this section, the Cornell Convenes group discussed the broader implications of the implementation of a US CBDC. *Figures 3, 4*, and *5* below show the top five ideas by sector and percentage mentions for chapter one.







For academia, *privacy, surveillance, and government control* and *secure responsive infrastructure* were the most important points. For industry, *stablecoins and payments* was the most important topic. For regulators, each of the points they made were of equal importance. The three groups all agreed that the topic on the *coexistence of stablecoins and CBDCs* was important. Academia

and regulators both placed importance on *CBDC research and design*. Industry and regulators both mentioned *the Fed and dollar limits*.

XVI | CHAPTER ONE | DISCUSSION

The facilitator explained the housekeeping rules to the group and announced that ***The Future of Money: Government and Private Systems*** would be the first area to be discussed and led by an academic in the sector with many publications on this topic.

The academic explained that a lot has changed recently with regard to CBDCs, but also expressed broader thoughts on the structure of money as a whole, as reflected in the recent G20 meeting with central bank governors.

Many countries are going ahead with CBDCs, and The Atlantic Council has been good at keeping track of these. Fundamental value propositions are being questioned because the use case is far from clear to many. The ownership of digital wallets is high, but the transaction volume is comparatively low.

The academic posited that we need broader financial inclusion, but the question is: ***Can CBDCs achieve this objective? Or is there a safer way?*** The academic argued that the answer to these questions is ***without*** the government being involved.

"Conceptual Design Choices"

The academic also said that there are conceptual design choices that could mitigate many of the risks associated with CBDCs. Recent bank failures and deposit insurance system holes have shown risks associated with the current system. CBDCs precipitate financial instability, so we need to mitigate privacy and financial stability concerns.

The academic added that in the US, there is one set of views. With China's digital Yuan CBDC, s/he pondered whether "*the US feels like it is losing the race,"* and offered that *"Just because it is digital doesn't necessarily make it trustworthy*." S/he continued by saying, *"Speed is not a game changer, and perhaps it will be interesting to take things slowly and learn from the experience of others*."

Significant inefficiencies exist within US domestic payment systems. However, the CBDC bridge project for international payments could provide significant user value. S/he added that there is a difference between retail and wholesale CBDC operations.

"Trust Component with Stablecoins"

Stablecoins provide efficient mediums of exchange (thanks to technology and geopolitical development) but, unlike fiat-backed currencies, are not fundamental stores of value, which is where the trust component becomes very important. The dollar plays a less important role in international currencies, leading to what the author refers to as de-dollarization. Still, investors continue to look to the dollar as a point of reference.

China is regressing rather than progressing. A reserve currency requires an institutional framework with the rule of law. Finally, on the regulatory front, what seemed to be in the air at the G20 meeting last week (April 2023) was that the entire industry needs much tighter regulation. A much more constricting approach is coming for the US.

Editors' Note: One editor commented that some may hold different views from the academic's regarding China's status.

Right now, it will be incumbent on the industry to make a case for itself to accomplish the objectives the government wants to achieve while not needing the government involved. In many other market countries, there are even more concerns about what blockchain and crypto will do to their economies.

Editors' Note: CBDCs continue to be a pivotal topic. As of June 2023, eleven countries have launched CBDCs, including a number in the Caribbean, and Nigeria —traditionally lesser developed nations, financially speaking. China's pilot, though with underwhelming adoption, could provide useful insights for major economies. Globally, there has been a lot of politicization in this area; in the US this is magnified as the general election draws near.

"CBDCs and Real-Time Payment Equivalency"

An industry expert responded. "My experience is that CBDCs are equivalent to a real-time payment system and do not seem valuable in countries with existing digital payment systems. It's taken central banks 18 months to realize this. I think there is a discussion on whether there is utility in a fair token, or are we just moving the bits around again?"

Another industry expert disagreed with the previous opinion on the equivalency between CBDCs and real-time payment systems, because the latter are currently restricted to central

banks and are just another way of settling reserve balances. S/he argued that expanding that access to non-banks and other financial institutions could be the basis of a CBDC at a fundamental level. But the basic premise of opening up liabilities to non-banks and other financial institutions separates wholesale CBDCs from more general digital payment systems.

"CBDC Use Cases"

A regulator argued the use case is unclear for the majority of people. S/he listens to podcasts and lots of discussions about how it can appeal to the regular consumer. S/he uses the ATM as an example of the last best innovation because it was very clear what the use case was. "*Essentially, CBDCs need to provide a good User Experience (UX). People putting money at* the Fed *rather than banks will be an issue for people*."

"Disruption of The Current System and User Experience (UX)"

Another participant, also an industry expert, built on a previous comment, adding that "*As we look at the evolution, one thing we see from an infrastructure perspective in financial services is the disruption of how things work*." S/he pondered whether the way this would work would be somewhat "inside out" as large banks and institutions start to recognize that they can replace what is essentially a 40-year-old technology — mainframes running on COBOL for payment processing. S/he believes these large banks and institutions will move towards the underlying technology we're talking about.

S/he agrees with a previous statement made by an industry expert, in that CBDCs have to be opened up to other non bank institutions. To the regulator's point on customer experience, this expert said that they think everyone can agree: looking at the crypto digital asset ecosystem, that the last thing to come along is customer experience, and that it's probably the first thing that needs to be fixed. That said, as people begin to understand that they will have more control over their assets and what they can do with them, the onboarding experience should become easier. It will be an interesting experiment to see what happens, and it will be a different experience in one country compared to another.

"CBDCs in The Global Context"

Another industry expert has been tracking CBDC progress worldwide and offers some statistics to contextualize the conversation. Around 117 countries have started to play with CBDCs, but the estimated number of those getting investment and seriously developing them is

around 60, 19 of which attended G20. We are still very early in the process, and obstacles include financial inclusion and monetary policy issues, which make adoption difficult.

In China, where WeChatPay and AliPay are popular, people are not incentivized to leave those platforms and experiment with new ones. The market is currently for around 260 million people, so China has tried pilot phases in various use cases, including public transport or tax payments. This pilot phase is about testing, not perfecting, and China is far from releasing a fully-fledged CBDC.

Another industry player described how in India, real infrastructure supersedes CBDCs in many forms. The choice of technology may be hindering adoption. Wholesale CBDCs have been made easier with wallets in the capital market infrastructure segment. Actually, people have not figured out how to do T+1 let alone T+0. In this case, you have to design a whole set of risk models around the ecosystem, meaning this will be a long process. They're very useful, but people should think beyond just the use case.

"Government Control"

Another industry expert put aside the question of wholesale CBDCs to focus on the retail side, and believes one of the concerns is their impact on other parts of the financial system, for example, mortgages and credit cards. Banks take deposits and lend them out. With CBDCs, people essentially park them somewhere, and then they can't be used to generate credit. But there are also privacy concerns we don't necessarily have answers to. (With governmental control, there is the risk of abuse; the government could stop your access to your money.) So that's something we need to develop. A potential alternative is a private stablecoin over a retail CBDC.

An academic echoed the points made previously. In China, CBDCs pose two key problems: adoption and privacy. The world thinks the Chinese government already looks at everything its citizens do. Banks already have restrictions on transactions over 50,000 Yuan. Thus, control via CBDCs will damage their reputation in this regard. Having more restrictions through CBDCs is concerning, particularly for high-income individuals. WeChat Pay and AliPay are the chosen payment system for 20% of Chinese citizens. Shenzhen, Nanjing, already gives 200 - 500 yuan for users to adopt the CBDC, but it's not currently attracting users. If CBDCs could overcome certain pain points, it would be helpful for their adoption.

Another participant, an industry expert, reminded the group that stablecoins are not regulated, so we need to trailblaze a framework for that regulation. Interesting how retail

solution operates in parallel. Various purposes. People can access the US dollar, the most popular financial product in the world. Would a US CBDC be accessible outside the US?

Use case: People want to move their assets at the speed of the internet. It's creating new problems. We risk going down a dangerous road if we don't innovate. Problems exist no matter what system you have. Bank runs in TradFi happened because you only need one tweet to create panic.

Is the government or a private entity the right one, or are the two working together the right solution? If the Fed is the regulator and the issuer, how does that look? Can they make a monetary supply?

The facilitator recapped the conversation up to that moment and posited four potential first principles:

- CBDC use cases
- Tension between privacy and surveillance
- Extent of government control
- Incentives for adoption

An academic added that one of the things that has to happen with adoption is the speed of the internet. Think of brick-and-mortar to e-commerce. It has to be driven by the regulation in a 24/7 way. We saw that with a bank run that happened on the weekend, which the regulatory agencies didn't find out about until after the weekend. Governments need the support of their citizens. Look at the recent events in France, where they tried to increase the retirement age. They can't unilaterally do this without the support of their citizens.

An industry expert added: "We keep talking about CBDCs, and sometimes stablecoins will come into play. They are two distinct situations, with private stablecoins similar to retail CBDCs. The other thing I was going to mention is that CBDCs in the US are extremely politicized. Republicans point out privacy concerns. Democrats on the progressive side want everyone to have an account with the Fed. The Republican senator used to be pro-CBDC but is being pulled to the right. It is more viable to have a private stablecoin option."

Editors' Note: The politicization of CBDCs is a factor. Politics are involved and the digital asset world is under strong scrutiny in a large part due to FTX's debacle, its practice of buying political support on both sides of the aisle, and its attempt to become cozy with regulators.

Finally, an academic spoke of use cases of CBDCs, and how they could contribute to DeFi or other areas of the financial system. "*There are risks with DeFi, whether private, algorithmic, or fiat-based, but CBDCs backed by governments would contribute to making DeFi more mainstream*."

— END OF CHAPTER ONE DISCUSSION —

CHAPTER ONE | STICKY NOTES

As time for this part of the discussion ended, the group was offered the opportunity to write additional points on sticky notes for their inclusion in the final report. For this chapter, these were the points made:

- *When considering the impact of retail CBDCs, I recommend reading Cornell Law professor Saule Omarova's paper The People's Ledger. This paper cost her the nomination to head the OCC, but it is an important, thought-provoking piece.*
- *Retail CBDC would benefit from Legal Entity Identifier (LEI) for online merchant transactions to identify the counterparty.*
- *The retail CBDC design could move the burden of monetary security from the operation to the user.*
- *Offline, private, retail CBDCs are technically possible.*
- *Consumer protection should be at the center of a retail CBDC design.*
- *The use case for CBDCs should be split — last mile retail, remittances, and bank-to-bank. CBDC doesn't have to solve every problem.*

XVII | CHAPTER ONE | ANALYSIS

TOPICS STRONGLY IDENTIFIED: banking disruption; stablecoins and CBDCs coexistence; CBDC research and design; privacy, surveillance, and government control; secure responsive infrastructure; potential for de-dollarization; Fed and dollar limits; stablecoins and payments; education; CBDCs equal to real-time payments.

CHAPTER ONE | KEY TAKEAWAYS

Further research is needed.

"We are still very early in the process, and obstacles include financial inclusion and monetary policy issues, which make adoption difficult."

Government surveillance and privacy issues are paramount.

"With governmental control, there is the risk of abuse. The government could stop your access to your money. So that's something we need to develop. A potential alternative is a private stablecoin over a retail CBDC."

CHAPTER ONE | BIG IDEAS

Conceptual Design Choices

CBDC designs should take risk and privacy into account.

Trust Component with Stablecoins

Just because stablecoins are digital, doesn't necessarily mean they are trustworthy.

CBDC and Real-Time Payment Equivalency

Are CBDCs equivalent to real-time payments and what is the role of private industry?

Use Cases

Is there a definitive use case for CBDCs?

Disruption of the Current System and User Experience (UX)

Do people want more control over their assets and what they can do with them? What types of UX would be needed to make people feel comfortable?

CBDCs in the Global Context

Do CBDCs in the global context encourage financial inclusion?

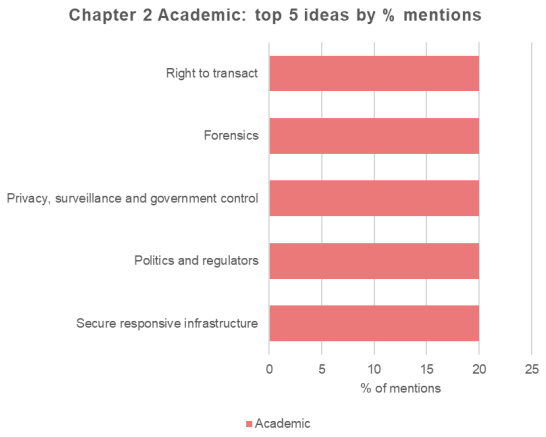
Government Control

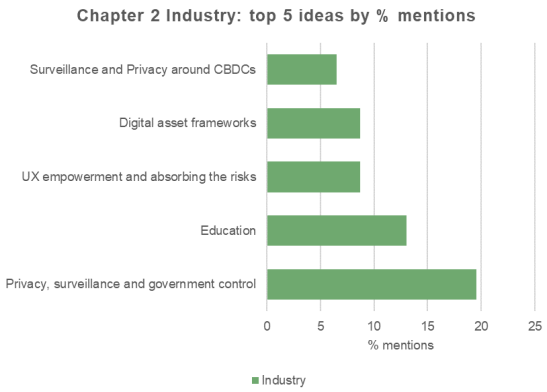
How much, if any, control should the government have when it comes to the issuance of a US CBDC? Further research is needed.

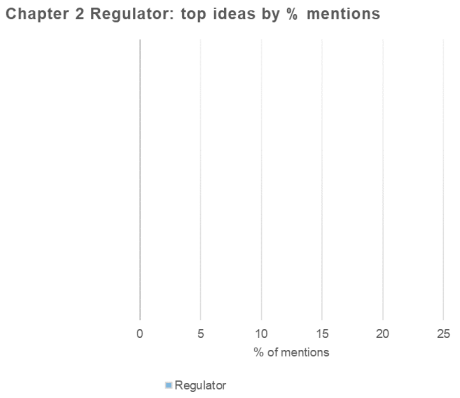
CHAPTER ONE | CONCLUSION: It remains unclear whether CBDCs should be issued and what protections will exist by design and by law. Stablecoins offer an alternative payment system. Trust must be addressed in any system. Should, and how, can CBDC and stablecoin payment systems work together? Finally, and more specifically, the difference between wholesale and retail CBDC use cases should be further explored. Education is needed.

XVIII | CHAPTER TWO | BALANCING SURVEILLANCE AND PRIVACY IN DIGITAL FRAMEWORKS DATA VISUALIZATION

Figures 6, 7, and 8.







From the above figures, the reader can infer that regulators did not offer up thoughts in this chapter of the conversation. Academia and industry both discussed *privacy, surveillance, and government control* in equal measure, making it the most salient topic of this part of the conversation. Industry offered opinions on *education*, *UX empowerment and risk absorption*, *digital asset frameworks*, and *surveillance and privacy surrounding CBDCs*, but overall, academia dominated this chapter with their top five ideas which included *privacy, surveillance, and government control*, *politics and regulators*, *secure responsive infrastructure*, *forensics*, and *the right to transact*.

XIX | CHAPTER TWO | DISCUSSION

The facilitator introduced the second part of the debate: ***Balancing Surveillance and Privacy in Digital Frameworks,*** and invited an industry expert to start the section.

S/he began: "As we gather to discuss the future of digital frameworks, we need to consider the potential risks of increased surveillance and governmental control. We will also discuss key management, digital transactions, and the implications of data used in these scenarios."

"Privacy"

The facilitator had asked them to come up with a provocative statement to begin this section:

"*How about we pretend to open our bank account statements, take a screenshot, and post it on Twitter and LinkedIn so everyone can see the medications we purchased, the milk we purchased, who we purchased from. That is exactly what happens on the Blockchain. How do we bring privacy back to transactions?*"

S/he continued: "We're at the very beginning of the technology. When the internet started, we didn't say this is what we would use it for. How do we preserve privacy? Do businesses need to show their competitors what they are doing? Competitors should be competing and not telling each other what they are doing. We have many former regulators and current regulators at this Cornell Convenes. We need to think about illicit finance and money laundering. We need to do so without stifling innovation."

An industry participant agreed, affirming that we must bring it back to User Experience (UX). Currently, there is an education gap for consumers but also for regulators. Lots of companies have our data. Annual base PII risks cost $5 billion a year.

"Give The Consumer the Anonymity They Want"

Consumers need control, so if they want anonymity, they can have it. Digital wallets make transactions easy, and zero-knowledge (ZK) proofs to open accounts can enable those who want anonymous transactions to have them. Then, as soon as we detect anomalies, we need to immediately stop and figure out what's going on. Rethinking how we do things is important. When the Republican-Democrat divide was mentioned earlier, it was down to education again.

There's a lack of education on both sides. Even educated people make comments and suggestions without knowing the ins and outs. So education first, then you can look at Twitter.

Another industry leader took the perspective that it comes down to providing consumers with optionality. Now a company can look at that data and see how they will market to an individual. It does not allow them to choose what they want to do with their data with the level of protection they would like, but rather a top-down approach. The regulators must step in for consumer protection. If we're going to think about education, we have to think about how liability fits in. If an individual posts their information, there is an issue if they are harmed. The financial institution is the one held liable. They need to recognize that risk. There is an important gap between regulations in the past and those of now. TradFi has held centralized parties responsible. Now we need to hold decentralized parties responsible.

Editors' Note: The role of centralized parties and their responsibility has long been enshrined in the law and followed by industry. In the case of decentralized systems, whom do you hold responsible? There is no direct analogy between centralized and decentralized players. What regulations need to be put in place to accommodate the new industry?

"Protect Data"

An industry expert agreed on the privacy concerns mentioned previously. S/he used this example to illustrate the point: "When I build products, if I use data I have to know why; otherwise, I shouldn't have access to it. Whether we're talking about self-custody wallets or the tech underpinning them, if I have to educate my users on how to use the product, then I fail."

S/he continued by saying that as a consumer, you should be able to use and access your money and not care if there's a server in Belgium. There's also a question behind creating infinite digital wallets because if one uses an iPhone to commit fraud and sells that phone, then what? The whole system needs to be regulated. So regarding liability, there is room for a regulator to come in and propose a framework.

Another industry expert wanted to touch on the shift mentioned about how we view the privacy of financial information. In the 1970s, the government needed access to information only financial institutions had. Now with Blockchain, some of that information is publicly available. The government could keep its own list of transactions over US$10,000. They could maintain their own list of public and private transactions.

This (represents a) shift in the way we think about financial privacy and the considerations we think about — if you go to the liquor store every day, chances are you want that to be kept private – so there are things that you want private and other things that the government could regulate. Education will be important but also scary for some.

An industry expert argued there is nuance, because we have an uphill battle; that is, when blow-ups happen, Congress and regulators think we do not act responsibly in this arena. A higher bar should be in place to capture industry shortfallings. Therefore, it's not just that Know-Your-Customer (KYC) controls are necessary.

“Poor UX”

An industry expert said that we have a good balance between surveillance and privacy. Transactions on the blockchain are different from posting on your Twitter account. One user has to have different wallets, one for receiving, storing, and sending.

Currently, there is a reasonable level of balance, but at the expense of user experience. You have to extend to multiple transactions to keep your privacy. Recent study: we look at transactions over 10,000 dollars. Over 90% of the transactions are to Easily Attainable Identities (EAIs). You can reasonably trace out transactions currently. That’s why users should have multiple wallets, but that’s not a great user experience.

Another industry expert added that there is an important balance for Congress and regulators to consider when talking about KYC. They worry that as we see more requirements imposed, that will make illicit cryptos worse, not better. It will push cryptos abroad to where there is no regulation. There needs to be a balance.

An academic made the following comment: “Besides software encryptions, there is also hardware.”

Another academic highlighted the broader issues about this. Who can transact? Do people have a right to transact? Take a look at food stamps today. They are a government-directed program. We decided that a certain group can only transact in a certain way and for certain things. A whole class of people are used to the government telling them what to do with their money. It may not be us, but people are already surveilled.

“Who Is Watching The Watchers?”

An industry expert continued from the previous comment: “When I think of surveillance, I think of espionage. One question, who is watching the watchers? Who is ensuring that privacy is there? There need to be rules for regulators to avoid mega-state surveillance big brother style. How do we push back on other countries progressing in this sense?”

Finally, another industry expert agreed that we should be educating users. We are talking about empowering people. People need to understand how to manage their assets at their own risk. The other side of the equation is a clear lack of trust in the payments industry. How do we generate that trust in the system? I just want to trust the person sending and receiving the payments. If I pay with a card, I want the right to take the money back. E.g., I want to buy something from Nigeria. How do I trust the other side? We shouldn’t rely on the government only to set up those rules. The private sector should also help to facilitate trust.

The facilitator recapped the themes mentioned:

- Privacy norms
- What liability is or should be
- Education
- Transparency

— END OF CHAPTER TWO DISCUSSION —

CHAPTER TWO | STICKY NOTES

None of the sticky notes corresponded to this section of the conversation.

XX | CHAPTER TWO | ANALYSIS

TOPICS STRONGLY IDENTIFIED: Right to transact; forensics; privacy, surveillance, and government control; politics and regulation; secure responsive infrastructure; surveillance and privacy around CBDCs; digital asset frameworks; UX empowerment and absorbing the risks; education.

CHAPTER TWO | KEY TAKEAWAYS

Balance Between Privacy and Surveillance

> "There is an important balance for Congress and regulators to consider when talking about KYC. They worry that as we see more requirements imposed, that will make illicit cryptos worse, not better. It will push cryptos abroad to where there is no regulation. There needs to be a balance."

Avoid Big Brother-style Surveillance

> "When I think of surveillance, I think of espionage. One question, who is watching the watchers? Who is ensuring that privacy is there? There need to be rules for regulators to avoid mega-state surveillance big brother style. How do we push back on other countries progressing in this sense?"

CHAPTER TWO | BIG IDEAS

Privacy

How much privacy protection should be embedded in CBDCs, stablecoins, or other digital assets?

Give The Consumer the Anonymity They Want

Consumers should have optionality for transaction anonymity. ZK-proofs and segmented approaches to data can help achieve this.

Protect Data

How do we protect privacy since data is publicly available on blockchains?

Poor UX

Multiple wallets are not a great user experience and can limit adoption.

Who Is Watching The Watchers?

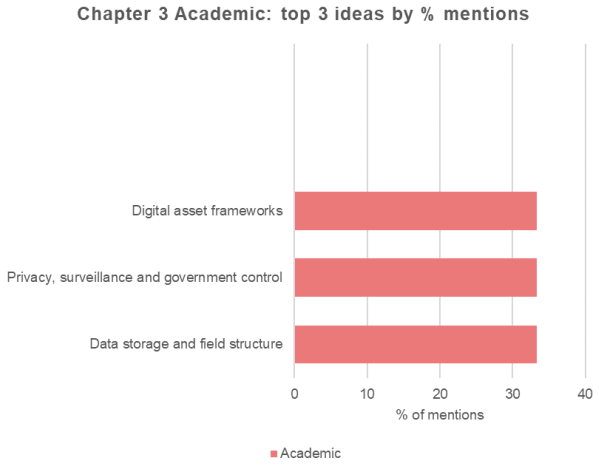
If there is a certain level of surveillance then those watching should also be surveilled.

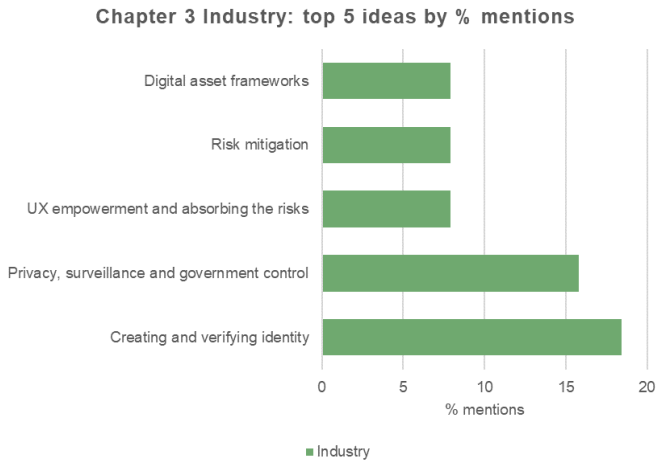
CHAPTER TWO | CONCLUSION : The discussion focussed on privacy, security, and user experience in the context of digital transactions and data management. The overarching questions resided in how much privacy users should have versus how much government or private industry surveillance is acceptable. Participants pondered a combination of heavy government surveillance for certain activities (like transactions over US$10,000) and lighter surveillance for other activities.

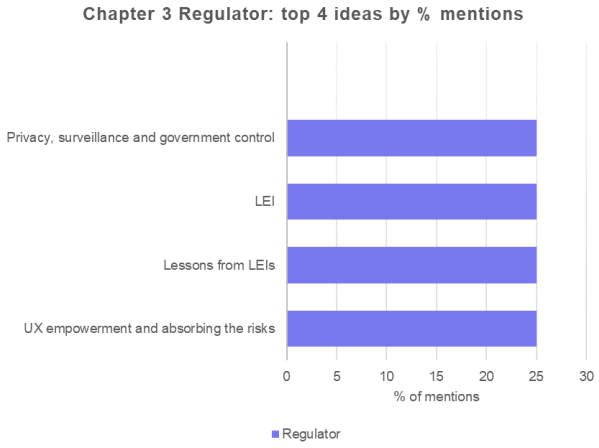
XXI | CHAPTER THREE | TECHNICAL CONSIDERATIONS FOR DIGITAL FRAMEWORKS

DATA VISUALIZATION

Figures 9, 10, and 11







All three groups offered thoughts on *privacy, surveillance, and government control*. For regulators, this was one of four topics that they mentioned in equal measure, the others being *LEIs*, *lessons from LEIs*, and *UX empowerment and absorption of risk*. Industry discussed more themes, the figure above showing the top five. Although the group agreed, with varying intensity, that *privacy, surveillance, and government control* was important, for industry, *creating and verifying identity* was more important. Academia placed equal importance on *privacy, surveillance, and government control* as it did *data storage and field structure*, and *digital asset frameworks*.

XXII | CHAPTER THREE | DISCUSSION

The facilitator welcomed the group back after a brief break and invited an industry expert to begin the section on ***Technical Considerations for Digital Frameworks.***

"Identity"

S/he began: As a human, you have a physical identity. We've been mapping informational identities to physical ones for a long time, starting with your birth certificate. Those same systems are now online with a username and a password. Usually, that password is something you keep in your brain. The problem there is that it is a symmetric secret. There are the foundational problems for that: once you give it away, it's gone.

So now, if we're talking about accounts and digital identities: I want an online account. What method do we use? There are newer standards from W3C worldwide consortium to make identity assertions. That is kind of the *how*. In this space, a digital identity is not always a myth or an extreme.

Imagine I have a digital identity. Fraud happens all the time despite platforms that require you to use your real identity to join. So now that the platform has and holds that data, we can ask, why are they holding it? Why can't I be the one to hold my data? Once one loses his data, that data is gone. There is no way you can get it back. All of these factors underpin digital identity. The question becomes *why*? Why do we need an identity? I think we see the same thing leading into the Blockchain side. There is very little privacy, with Zcash being the exception. It fits nicely with the existing framework that was in place. I think this is because many people evaluated the same framework. This approach enables you to have self-regulating groups. I think the approach is an infrastructure piece. It has not been a user-based technology.

"Zero-knowledge Proofs"

An industry expert continued: "For particularly vulnerable communities, the privacy aspect is very important. Figuring out what those standards are and who would accept them is important. We're so used to government IDs, but they could come from other private sources. Then you need acceptance of those across different organizations. This is where zero-knowledge (ZK) proofs could come in, too — you don't need my actual date of birth, but ZK proofs would work to show I'm over 21 years old for a particular purchase."

Another industry expert expanded on this point: Digital IDs and ZK-proofs could be used innovatively with KYC, (for) entities that cannot do KYC in the traditional manner. There are many interesting ways this could be applied to the crypto space, making certain businesses easier to run.

An industry expert added to the discussion on digital and decentralized ID. Digital IDs exist. Multi-step authentication is annoying, but we do it anyway. Digital IDs like driver's licenses exist in many places. It's a government role. The Ukrainian Ministry of digital transformation has moved passports and birth certificates that prove identities online due to the need caused by war.

Another example is: Imagine I'm Indian. I want to renew my passport and give them my name and ID number. They pull a list of all the places I've lived. They already have a lot of information. The value proposition for the private sector to lead this is unclear to me. The argument for government is clearer.

"Who Owns Our Data?"

To that point, an industry expert said it depends on the country. The US is a different place. This is where traditional financial services can carve a unique role. My partner is a doctor, and I think of HIPAA, a rule put in place because of technology that did not exist previously. S/he wakes up to an emergency call at 2 am and has no idea about the patient, so there are benefits and challenges. Health records should become a digital asset owned by the individual. The use case is we need to retrain people to think about who owns this underlying information. In many cases, the companies think they own this data. That's the first part of the problem.

Editors' Note: Who owns what data and who controls identity? The role of the government should be clearly set out and differs by country. What identity standards should each country abide by, regardless of their level of surveillance? Interoperability is key. Current proposals such as GDPR, CCPA, open data initiatives, etc., are not panacea and need careful evaluation.

A regulator offered the following contribution: Something we can learn from this is that some years ago when people were entering into swaps, they did not know who the other party was. Legal Entity Identifiers (LEIs) then came up. You end up with these sorts of worldwide groups administrating in different countries. The biggest issue is hierarchies. If you take some

place like Goldman Sachs, you have 50,000 affiliates. I just wanted to say there might be a lesson we might be able to take from how LEIs were implemented.

An industry expert built on a previous point: Digital ID is like any data, and the discussion is around having access and ownership, then having privacy. People don't care about the latter until there's a problem. Then they fight to get the data back through lawsuits. They need to understand the trade-off, so consumer education is important. Looking at UX again, there needs to be a discussion about what the consumer has.

If I Google myself, I find a different ID than going to the DMV. Inert information. In the HIPAA context, regulators have access to it, but there isn't any interoperability, and there has to be. You don't have a claim if you don't care about your privacy. But try to get people over that hump. It's different from theory to practice.

An industry expert fully agreed that identity is a key enabler for our use cases. Getting B2B companies to adapt to this concept of verified credentials is very challenging. "It's not that I don't believe it's useful, but that there is a big gap. Some clients don't even have centralized identity systems. If we make migration to these kinds of systems as easy and cheap as possible, we can remove the block to adoption. Otherwise, it is very difficult to implement."

An academic advised the group to look at when GDPR was put in place. That gave law firms an awful lot of money. When discussing identity and money, words have to match tech, and the tech has to match words. They have to be on the same page. You have to know how data fields are structured. Metadata might be captured and might end up disclosed. Is there room for more data fields to be captured and revealed? That's another important conversation.

"TradFi, DeFi, and CeFi"

An industry expert continued: Legal frameworks regarding smart contracts are necessary. When smart contracts are hacked, communities might blame the developers because the programming is bad. With hacked smart contracts, market manipulators can step in, and when they do, they can be arrested as we've seen happen. We expect or maybe desire liability to sit with some party. TradFi, DeFi, and CeFi worlds can offer customer choice, but from a liability perspective, what happens when you convince Grandma to put all her money in a self-custody wallet? The elderly are groomed in TradFi, and banks are the intermediaries that identify those grooming situations. If there's a loss, banks take that. So what happens with this kind of vulnerability in self-custodial wallets? What is the level of KYC going on at exchanges? What is the regulation regarding liability and risk?

Another industry expert went on to say: Blockchain technology flips things in that you know the activity before you know the identity. There is a spectrum that's nuanced on how to separate identity from activity. We had an interesting anecdote — in the wake of FTX, a hacker stole assets from the bankruptcy estate. At any point, we can freeze and essentially seize those assets wherever they exist in the world. So we worked with law enforcement to freeze these assets. We have to grapple with this when it comes to digital identity. There is this concept of informed consent. You don't necessarily sacrifice privacy, but you know this information will be accessible on the Blockchain.

Another industry expert offered this perspective: Teaching a course on DeFi and stablecoins. Students like the anonymity and privacy that DeFi promises, but we're also talking about the tension between the democratization/automation of finance and accountability. I showed a clip from *It's A Wonderful Life*. No one had heard of it. We contrasted the bank collapse in the movie with modern day runs on the bank — Terra and Silicon Valley Bank — that happen so fast. Where is the accountability? Who can you go after? We've talked about the benefits of automation — students seem to want everything fast. And that's in part what CBDC offers. But there is also a concern about preserving privacy.

"Incentives"

A regulator stated that two previous opinions made them wonder what is wrong with user expense incentives. We need to focus on those incentives. Let users sell or haggle their own data, determine prices, and find consensus. The most eager seller and the most willing buyer. If people have a warehouse of data on themselves, which can be verified, they can elect to make this data available. Tip the incentive structure.

Editors' Note: How much data around identities are protected as basic human rights, and at what point does the data that comprises your identity become pieces of transactional data an individual can control?

— END OF CHAPTER THREE DISCUSSION —

CHAPTER THREE | STICKY NOTES

- Activity versus identity reflects the mindset gap between cybersecurity experts and the financial industry.

- Build on identity in a global world and make sure it’s inclusive.

XIII | CHAPTER THREE | ANALYSIS

TOPICS STRONGLY IDENTIFIED: digital asset frameworks; privacy, surveillance, and government control; data storage and field structure; risk mitigation; UX empowerment and absorbing the risks; creating and verifying identity; LEIs; lessons from LEIs.

CHAPTER THREE | KEY TAKEAWAYS

Digital Identity

> "Digital ID is like any data, and the discussion around having access and ownership, then having privacy. People don't care about the latter until there's a problem. Then they fight to get the data back through lawsuits. They need to understand the trade-off, so consumer education is important. Looking at UX again, there needs to be a discussion about what the consumer has."

Zero-knowledge Proofs For Identity Preservation

> "This is where zero-knowledge (ZK) proofs could come in, too — you don't need my actual date of birth, but ZK proofs would work to show I'm over 21 years old for a particular purchase."
>
> "Digital IDs and ZK proofs could be used innovatively with KYC."

CHAPTER THREE | BIG IDEAS

Identity

How should identity be portrayed in the digital world?

Access To Financial Services

How much of our identity do we need to give away in exchange for access to financial services?

Zero-knowledge Proofs

Zero-knowledge proofs offer a solution to protect identity.

Who Owns Our Data?

Medical data is an example of where the individual should be the holder of their own data.

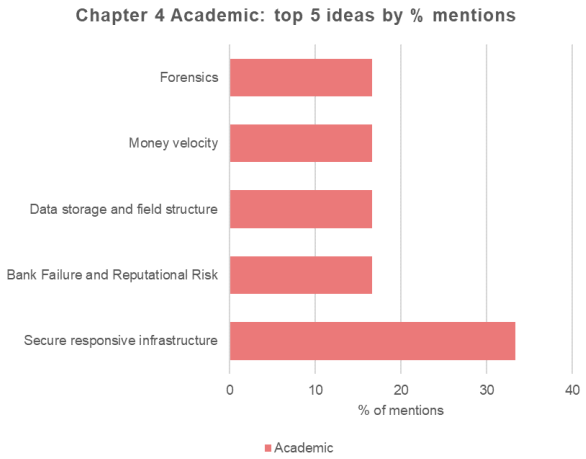
TradFi, DeFi, and CeFi

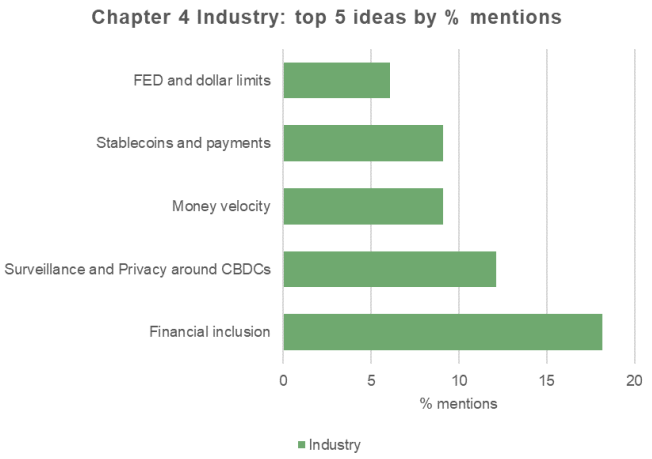
How much security will there be with DeFi? How to balance broader access to financial services to promote inclusion without opening the access to bad actors engaging in grooming and fraud is still undergoing research.

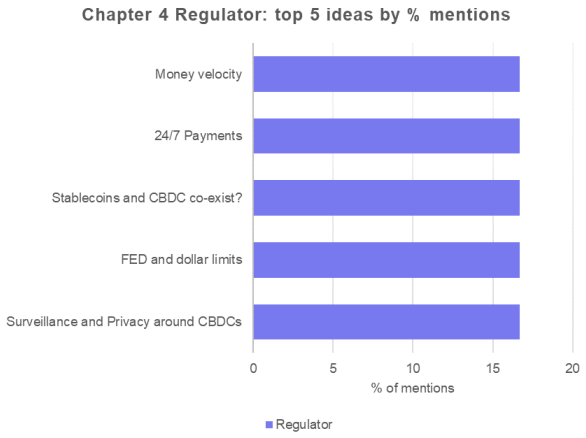
CHAPTER THREE | CONCLUSION: Preserving identity was an important consideration for the majority of the participants. Opinions differed on how much of one's data and identity should be private and under which circumstances. One way to preserve identity and privacy involves ZK proofs and other commitment schemes.

XXIV | CHAPTER FOUR | DIGITAL WALLETS AND THE FUTURE OF PAYMENTS
DATA VISUALIZATION

Figures 12, 13, and 14.







Each of the groups had different top five ideas with some overlap of topics. For example, all three groups discussed *money velocity*. Regulators placed equal importance on *money velocity* and their other top four themes for this chapter — *24/7 payments*, *stablecoin and CBDC coexistence*, *the Fed and dollar limits*, and *surveillance and privacy around CBDCs*. Industry placed its strongest emphasis on *financial inclusion*, followed by *surveillance and privacy around CBDCs*. *Money velocity* and *stablecoins and payments* were equal in importance. Finally, *the Fed and dollar limits* was the least discussed topic in their top five ideas. For academia, *secure responsive infrastructure* was by far the most important topic, followed by *bank failure and reputational risk*, *data storage and field structure*, *money velocity*, and *forensics* in equal measure.

XXV | CHAPTER FOUR | DISCUSSION

The facilitator introduced the next section of the debate on ***Digital Wallets and the Future of Payments,*** inviting an industry expert to open the section with the following:

"The Current Situation"

"The future of payments is something we have thought about quite a bit. There was a shift from cash to a digitized form of money. Yet, despite this digitization, we still see that payments tend to be slow and expensive. They are not behaving properly. 5% of the population is unbanked, and 17% is underbanked. We all can see this evolution. Other digital currencies could have an impact there. A couple of considerations when we think about payments. A payment is more than a transaction.

How do you incorporate all that into the ecosystems and do it at scale? To me, payments involve ecosystems. It's not just how a consumer buys or sells a good. It's also how the institutions sell them. The last part is how to address financial inclusion. Digital currencies will not totally solve it. But even if we solve a piece of it, it is worthwhile. But how we do that is the question. Do you need internet access? Is offline a possibility? Food for thought."

Editors' Note: The current financial system does not work well with speed and people want a 24/7 system. As payment rails change with Web3 being implemented, regulators need to keep up. Does this mean they are on call 24/7/365? How might AI fit in to support this scenario?

"Disruption"

An industry expert surmised that we need to think about the broader financial system. In today's digital age, the speed at which money can move impacts financial institutions. When considering payments, we must consider the financial system as a whole. Non banks are at the center of this trend. We are already seeing disaggregation with the rise of capital markets, syndicated loans, etc. There is already disruption in the financial system. We need to discover how to implement a market-based assessment of this, using the information that comes out from the technology. Leveraging payments to become programmable is the only way to ensure continuation.

An industry expert said that payments are a very important use case. Payments and banking services are impacted by digital assets. The possibility of moving money from the US to Nigeria in seconds is a strong use case. The current financial system has discriminatory components. The DeFi system could allow people to have access to loans.

A former regulator suggested that we need more thought on CBDCs and disintermediating banks; otherwise, who is going to do all the lending? If the funds held in CBDCs go to the Fed that would take money away from the banking system. If the Fed uses banks to issue CBDCs and the banks are allowed to lend on a fractional reserve basis, bank depositors that received the CBDC would have instruments that were 100% guaranteed and backed by the Fed, however safe or risky the banks' lending practices may be. In other words, this creates a "moral hazard problem", which is one of the reasons conventional bank deposit insurance is limited to $250,000 per customer.

An industry expert offered: "It's the liability of the Fed. It's issued and guaranteed by the Fed. I will have access to it through my bank account." The industry expert further said that the government could limit how much CBDC the account can hold to ensure that it can be 100% guaranteed.

The former regulator responded to that idea saying that such an approach would effectively limit any account to $250,000 in CBDCs issued by one bank to you and that could be a problem. It seems to be an issue that they have not seen policymakers address.

An industry expert continued: Financial inclusion, regulation, and banking access. Access has been solved by blockchain. You don't need KYC or a branch to open an account. But there is still the challenge of a cash-in and cash-out system that you can use daily. You receive money daily and need immediacy and interoperability. Can CBDCs or stablecoins solve this need for instant cash-in and cash-out?

"Hardware Versus Software"

An academic added that the core advantage is in settlements. The main disadvantage is data storage and computing volume. First, more chips and more hardware will be needed to help with the disadvantages. Infrastructure is needed. Second, the velocity of money is high. It's not only the speculative part that's driving that, but also the velocity part. Alibaba kept only a 5% reserve, and that's why they were shut down — for using the money 20-30 times, while the banks normally use it 2-3 times.

An industry expert described how when s/he was at the Fed, they had this conversation a lot. The answer then, for many of their colleagues, was *FedNow*. The next question would be, why now? The US has some of the safest banks and decades of experience. But it's a very American-centric idea.

"Easy Payments"

It would be helpful to people in other countries to transfer money between countries and not have to pay 30% remittance. Another example is when s/he was in India, they ran out of change. When you make $2 a day, and you can't get change, it is really a hardship. You overpay for everything. But it would be a lot easier if everyone had a phone and could transfer e-money.

Running out of change is rare in the US, but we ran out of quarters during the pandemic. People would get mad at the airport because they couldn't get their 50 cents back. The Fed encouraged people not to use cash. This is rare in the US, but that happens in other countries.

Think about countries experiencing hyperinflation. Instead of bringing bags of cash, they could just delete zeros from everyone's bank account. There are a lot of technical challenges to opening up bank accounts for everyone. Do you really want to triple or quadruple the size of the Fed? It's tax money in the end. One other thing is the banks have access to central bank accounts. There is not enough staff or resources to give everyone their own account. Central-left papers advocate this, but it is unrealistic.

"Risk"

An industry expert brought the section to a close with the following thoughts: Remittance is a clear use case. When banks are pursuing any activity, risk is at the heart of that engagement. Implementing an additional asset to a remittance payment requires discussing how the parties involved will be served. What kind of risk profile and understanding of the shift from profile and reputational risk (will be necessary)? Does that present any risk to consumers? It comes back to ensuring that examiners understand what they're examining and why they are examining it. A new activity may not be as risky as they see.

— END OF CHAPTER FOUR DISCUSSION —

CHAPTER FOUR | STICKY NOTES

- *Will tokenized deposits be an alternative to both stablecoins and CBDCs?*

XXVI | CHAPTER FOUR | ANALYSIS

TOPICS STRONGLY IDENTIFIED: forensics; money velocity; data storage and field structure; bank failure and reputational risk; secure responsive infrastructure; Fed and dollar limits; stablecoins and payments; surveillance and privacy around CBDCs, financial inclusion; 24/7 payments; stablecoins and CBDC coexistence.

CHAPTER FOUR | KEY TAKEAWAYS

Financial Inclusion

"There was a shift from cash to a digitized form of money. Yet, despite this digitization, we still see that payments tend to be slow and expensive. They are not behaving properly. 5% of the population is unbanked, and 17% is underbanked."

"Financial inclusion, regulation, and banking access. Access has been solved by blockchain. You don't need KYC or a branch to open an account. But there is still the challenge of a cash-in and cash-out system that you can use daily. You receive money daily and need immediacy and interoperability. Can CBDCs or stablecoins solve this need for instant cash-in and cash-out?"

Financial System Disruption and Innovation

"In today's digital age, the speed at which money can move impacts financial institutions. When considering payments, we must consider the financial system as a whole. Nonbanks are at the center of this trend."

"People want to transact in value and are not happy with the current financial system because it's not 24/7. As Web3 and blockchain drive new payments rails, issues come up that should be discussed."

"When banks are pursuing any activity, risk is at the heart of that engagement. Implementing an additional asset to a remittance payment requires not just discussing how examiners will be served. What kind of risk profile and understanding the shift from profile and reputational risk? Does that present any risk to consumers?"

CHAPTER FOUR | BIG IDEAS

Disruption

If banks are disintermediated to a high degree, their lending role is disrupted.

Easy Payments

Payments are not behaving properly so how do we tackle this?

Risk

Who is responsible for the risk?

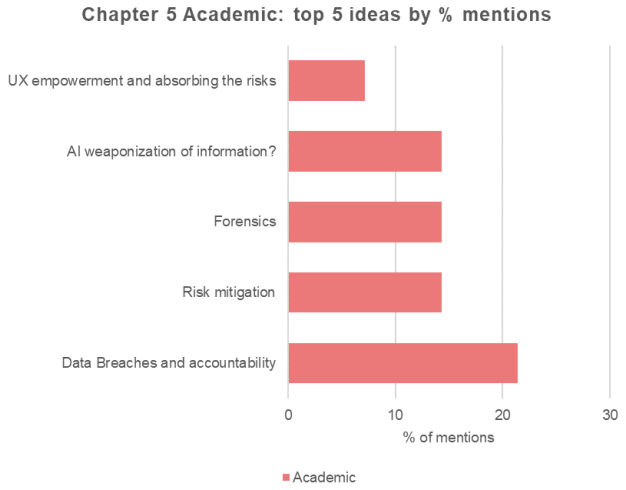
Education

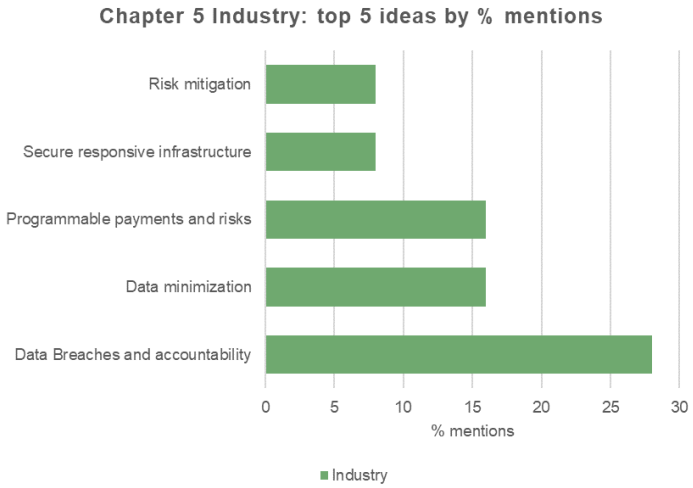
Examiners need to understand what they are examining and why they are examining it.

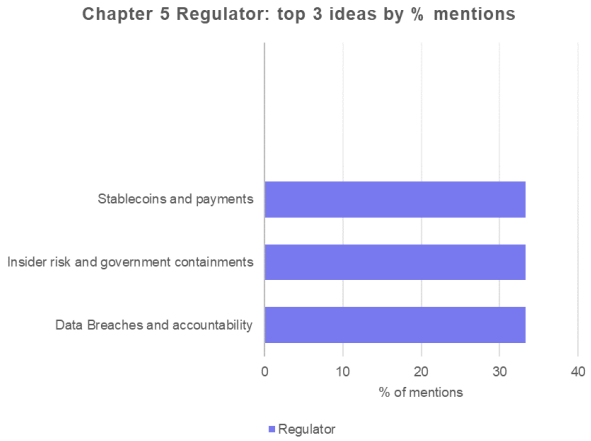
CHAPTER FOUR | CONCLUSION: The future of payments centers on addressing slow and expensive transactions. Nonbanks may play a central role in improving payments delivery. The full extent of their role was vigorously discussed and is yet to be determined both in the US and globally. Infrastructure improvements, such as enhanced data storage and computing resources, are needed for efficient settlements. Education is needed for consumers, industry, and regulators.

XXVII | CHAPTER FIVE | ENSURING SECURITY AND TRUST IN DIGITAL ASSET TRANSACTIONS DATA VISUALIZATION

Figures 15, 16, and 17.







The three groups all agreed that *data breaches and accountability* was the most important topic. However, regulators placed equal importance on this topic as they did *insider risk and government containment*, and *stablecoins and payments*. These were the only topics covered by regulators in this chapter. By contrast, industry and academia differed in their opinions of what was important. They both agreed *risk mitigation* was something to be further explored, and academia viewed this as equally important as *forensics* and *AI weaponization of information*. Of their top five ideas, academia mentioned *UX empowerment and risk absorption* the least. Industry placed the most emphasis on *data breaches and accountability*. Their following two topics — *data minimization* and *programmable payments and risks* — shared an equal percentage of mentions. Finally and similarly, *secure responsive infrastructure* and *risk mitigation* were discussed in equal measure as the least important of industry's top five ideas.

XXVIII | CHAPTER FIVE | DISCUSSION

The facilitator asked an industry expert to introduce the final discussion, ***Ensuring Security and Trust in Digital Asset Transactions***, to which s/he responded:

"Risk"

"When discussing how to ensure the security and trust of digital assets, we're invited to discuss forensics. I want to start by asking everyone in the room about the consequences of data breaches. I believe, from what we've been hearing, that people have quite different perspectives on what a *bad actor* is. How can forensics be used to investigate fraud and abuse of digital assets? For whom are we talking about the risk? Companies? Users? How can forensics be used? Who do we want to create security for? Is it the company? The citizen?"

An industry expert began by saying that when we talk about risk, we mean risk to investors and to financial stability. The SVB situation made us think about the risk the traditional financial sector imposes on the crypto sector. USDC price dropped because of SVB. The price of USDC went up to one dollar after the decision was made to secure all deposits.

Another industry expert added: Sometimes I see that as counterparty credit risk, on the stablecoin side, the issue of data breaches and thinking about those risks. The risks that everybody is focusing on – forget those, because those aren't going to happen. The risk that caused some real credibility was the insider risk. We had employees that took information home. The insider threat is arguably as important as the external threat. I do think that this ties in. You can't recover from some of these credibility risks associated with data breaches.

Another industry expert said that new risks are coming and reducing current risks. We need to remove the current risk. DeFi removes some of the current risks with smart contracts if they're flawless. You *can* reduce risk. They agreed with a previous comment. "It's not about the banking industry with crypto. I think the counterparty risk could be reduced through technology. Something like 40% of FX transactions don't have payment versatility protection. The blockchain systems that we have seen, are already built in. We need to look at new risks and the risks we already had."

The facilitator extracted a first principle in the form of risk reduction.

"AI"

An industry expert introduced the idea of the weaponization of information with the advent of AI. If John Doe has this Bitcoin address or this NFT, a quick search engine result based on these might show me where John Doe lives. Has AI introduced a new set of concerns that need quick attention?

"Security Breaches"

An industry expert added that breaches of exchanges do still happen. Phishing attacks happen. On the DeFi side, we see hacks like the Ronin Axie Infinity attack, where they got control of the keys. The protocol had no security bug, but they could manipulate the price. Then there are all these stories about wallets and people losing their wallet keys. I know someone whose briefcase was stolen, and it had his ledger in it. There are opportunities in crypto that don't exist for traditional assets.

They made reference to a previous example of seeing the Paxos gold move from the hack, you're able to monitor that and see where the transactions are going. You can detect if somebody is trying to bring funds in from ransomware. This is something we don't have access to in traditional finance. This is something that is undervalued in the digital asset space.

An academic proposed a quick survey. "*Raise your hand if you've been a victim of a data breach*." [Lots of hands]. There is some accountability for data risk in GDPR. In internal breaches, there is accountability. For external breaches, there are no incentives for a company to change its behavior. Until incentives are put in place for companies to prevent data breaches, they will continue to happen. This is one of the top five risks that companies can't cover. The people bearing the costs of this are those who raised their hands. We are individually told to take on the risk, but we are not administering our accounts. We are not in control of our own account, but we are in control of our own risk.

An industry expert added that as this sector develops, payment systems become systemic. If this payment system goes down, what are the implications? It's a potentially significant risk. I mean, there are a handful of blockchains offering proof-of-stake payments. What happens if they just decide not to approve transactions? This risk has not been mitigated.

"Access To Data"

An industry expert reminded the group that you can't lose data you don't have and "can't lose data you don't access". Along those lines, I think every incentive over not having a data breach… it's really hard to create large-scale secure systems. To come back to the AI piece: they

are just rearranging bits that we already know. It is just accessing the information we already have. People only care after it hurts. AI can make it hurt faster.

An academic added that AI takes data that already exists. GPT will be more risky when it can organize as a search engine, when it's connected to the internet. How it will use that information to access activity, payments, and everything altogether will be faster. Generative AI creates opportunities for manipulation. This challenges the identity pieces, very much so. Regulating those that have the capabilities to do this in a meaningful way is important for preserving identities.

An industry expert brought us back to a previous point about minimizing the available data. It's not just a data breach. It's an *asset* breach. Who needs to store the data? We think there is a better alternative way of doing things — maybe having a segmented data approach. Only the parties involved should have access to a smart contract. There is an advantage to having a segmented data approach. On many chains, nodes have access to the full chain. If we use a segmented approach, even if there is a breach, the extent of the breach can be contained.

"Government Protection"

An industry expert who worked at the Treasury for six years said they received as many notifications that the government lost their data there as they did at private organizations. The government is not great at storing data and protecting it. There would be tons of data that they would possess. How you control that so it is not subject to breaches is key.

An industry expert made reference to a previous comment on centralized versus decentralized models. With decentralized models, who controls smart contracts? Layer 1 such as the Ethereum? Layer 2? Do we let the transaction go free on Layer 1? What happens with Layer 2? Or with a hybrid model? These are all open questions with no clear answers!

The facilitator thanked the group and congratulated it for covering a tremendous amount of ground in such a short amount of time. They cited optimism that there is an effective compass to map the future of how this will come to us and how it is uplifting.

An academic made a closing comment: "The reason this was a very great event is because of all of you. Thank you for coming to DC and participating. Please send me all your feedback."

— END OF CHAPTER FIVE DISCUSSION —

CHAPTER FIVE | STICKY NOTES

None of the sticky notes corresponded to this section of the conversation.

XXIX | CHAPTER FIVE | ANALYSIS

TOPICS STRONGLY IDENTIFIED: UX empowerment and absorbing the risks; AI weaponization of information; forensics; risk mitigation; data breaches and accountability; secure responsive infrastructure; programmable payments and risks; data minimization; stablecoins and payments; insider risks and government containment.

CHAPTER FIVE | KEY TAKEAWAYS

Risk

"How can forensics be used to investigate fraud and abuse of digital assets? For whom are we talking about the risk?"

"The SVB situation made us think about the risk the traditional financial sector imposes on the crypto sector. USDC price dropped because of SVB. The price of USDC went up to one dollar after the decision was made to secure all deposits."

"The insider threat is arguably as important as the external threat. I do think that this ties in. You can't recover from some of these credibility risks associated with data breaches."

"You can detect if somebody is trying to bring funds in from ransomware. This is something we don't have access to in traditional finance. This is something that is undervalued in the digital asset space."

AI

"If John Doe has this Bitcoin address or this NFT, a quick search engine result based on these might show me where John Doe lives. Has AI introduced a new set of concerns that need quick attention?"

Access To Data

"You can't lose data you don't have and can't lose data you don't access."

CHAPTER FIVE | BIG IDEAS

Risk

How do you allocate risk to everyone involved in a transaction?

AI

Weaponization of information through AI is an immediate risk.

Access To Data

You can’t lose data you don’t have access to.

Government Protection

Data is not necessarily more secure under government protection.

CHAPTER FIVE | CONCLUSION: The question of who bears the risk in the crypto sector was a consistent theme. Various risks, including insider threats, breaches of exchanges, phishing attacks, and the weaponization of AI in information gathering were also discussed. The importance of accountability for data risks, regulatory incentives to prevent breaches, and the potential systemic risks of payment system failures were emphasized. There was also a focus on minimizing data exposure, using segmented data approaches, and the government's role in data protection. Overall, the discussion underscored the complex landscape of digital asset security and the need for careful consideration of risks and solutions in this evolving space.

XXX | CORNELL CONVENES | APPENDICES

APPENDIX I | MAIN THEMES AND SUBTOPICS

For ease of visualization, the 12 main topics that arose in the conversation are listed in the table below, with each of the two to five subtopics that were discussed. The chapters in which each of the subtopics were discussed are also included. For the percentage mentions of each subtopic, look at APPENDIX II.

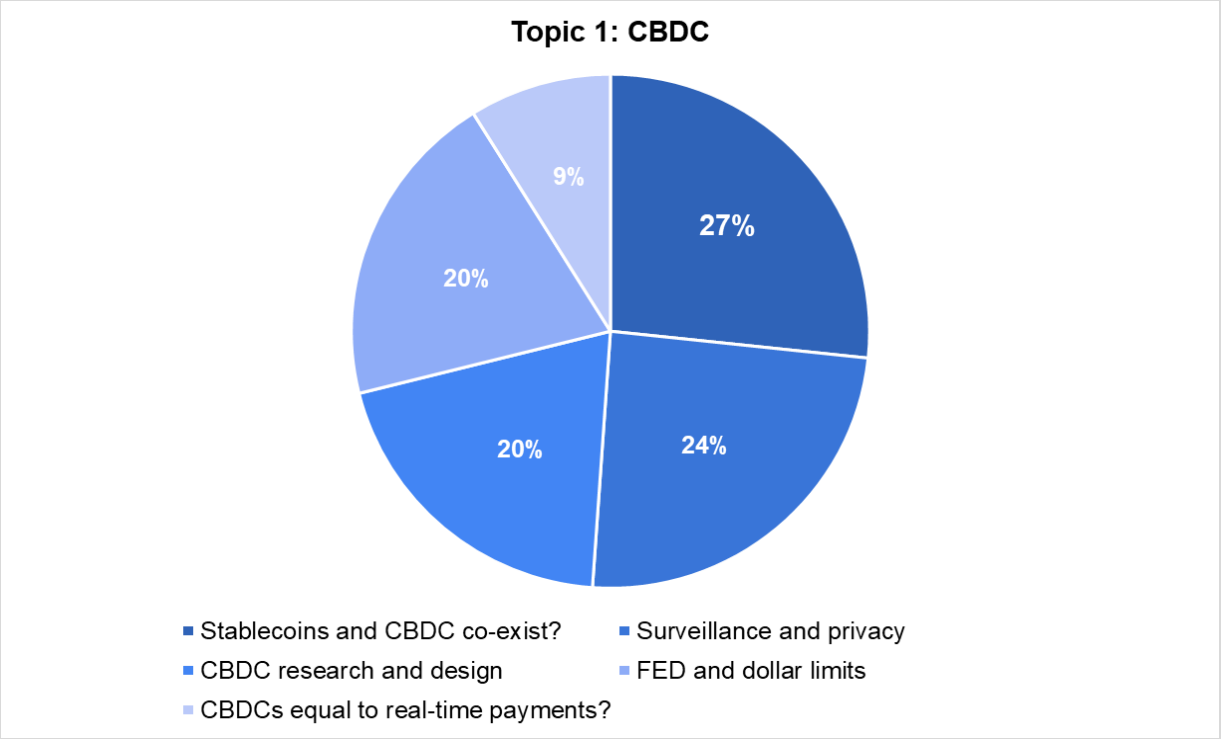
Top 12 Main Ideas	Top 2-5 Subtopics	Subtopics discussed in the following chapters:
CBDCs	Can stablecoins and CBDCs co-exist?	1, 2, and 4
	CBDC Research and Design	1, 2, and 4
	CBDCs Equal to Real Time Payment?	1
	Surveillance and Privacy	1, 2, and 4
	Fed and Dollar Limits	1, 2, and 4
Consumer, Education, and Access to Financial Services	Financial Inclusion	1, 3, and 4
	UX Empowerment and Absorbing the Risks	2, 3, and 5
	Education	1, 2 and 3
Current State of Banking	Bank Failure and Reputational Risks	1,2 4, and 5
	Deposit Insurance	1
	24/7 Payments	1 and 4
	Bank Examiners Education	4
Data Breaches and Treatment	Data Breaches and Accountability	5
	Data Minimization	1, 2 ,3, and 5
	Data Storage and Field Structure	3 and 4
	Government Containment and Insider Risk	5
Disruption of Banking	Banking Disruption	3

	Blockchain Activity View	1, 2, 3, 4, and 5
The Future of Money	Secure Responsive Infrastructure	1, 2, 3, 4, and 5
	Lessons from LEIs	1 and 3
	Store of Value	1
	Risk Mitigation	1, 2, 3, and 5
	Trust	2 and 5
Global Issues	CBDCs and Potential for Dedollarization	1 and 3
	Global Issues and Crypto	1, 2, 3, and 4
	Race with China	1
	Politics and Regulators	2, 3, and 4
Identity	Creating and Verifying Identity	2 and 3
	LEI	1 and 3
	Activity Before Identity	3
Payments	Money Velocity	4
	Payments and Ecosystems	1 and 4
Fraud, Privacy Versus Security	Privacy, Surveillance, and Government Control	1, 2, 3, and 5
	Forensics	2, 4, and 5
	AI Weaponization of Information	5
Private Sector, Stablecoins, and Digital Assets	Stablecoins and Payments	1, 3, 4, and 5
	KYC	2, 3, and 4
	Programmable Payments and Risks	1, 2, 4, and 5
	Incentives for Change	1 and 5
	Other Digital Assets	3
Regulation	Digital Asset Framework	1, 2, and 3
	Right to Transact	2

	Monetary Policy	1

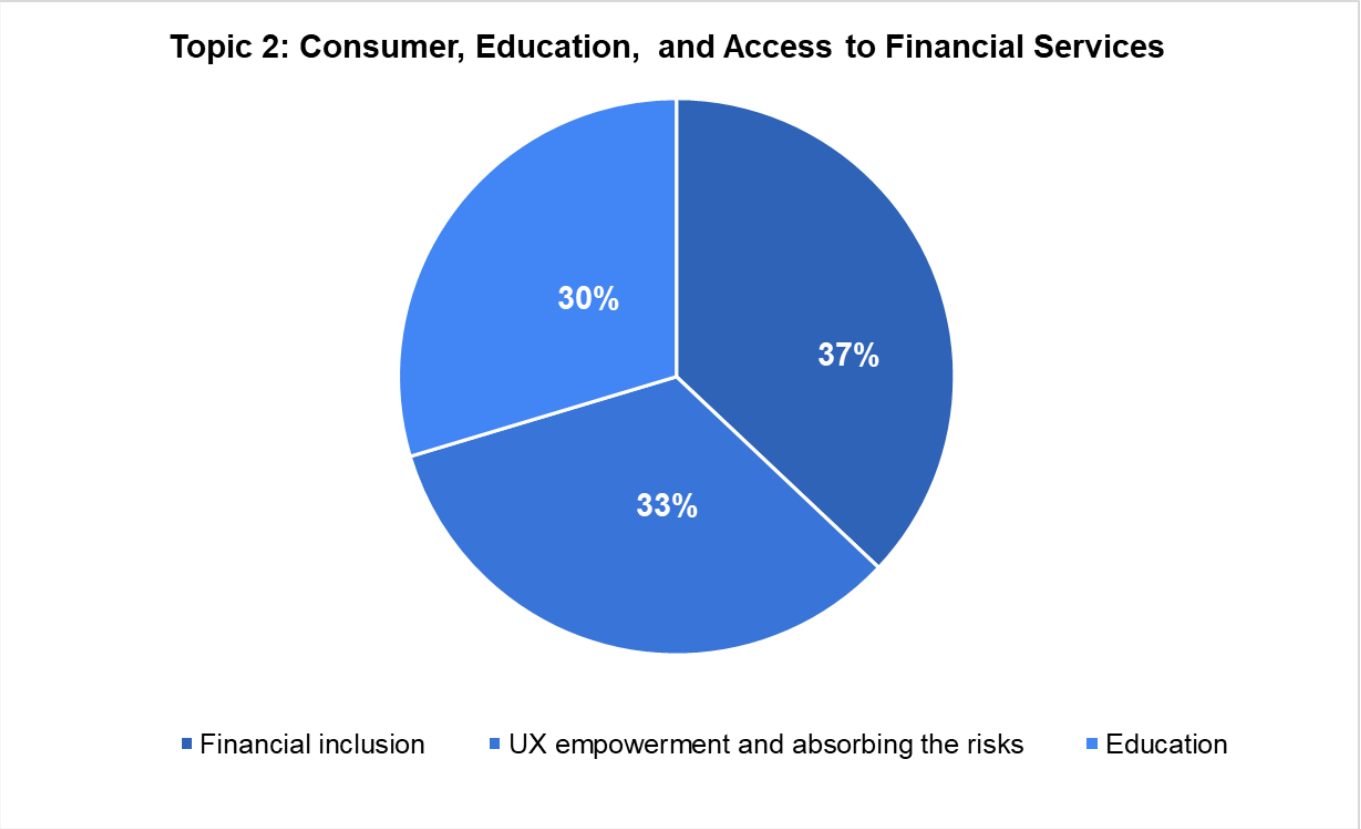
APPENDIX II | PIE CHARTS TO SHOW PERCENTAGE MENTIONS OF EACH SUBTOPIC WITHIN EACH OF THE 12 MAIN THEMES

For ***Topic 1: CBDC***, the editors sought to discover how frequently the subtopics in the key below arose across the five different chapters of the conversation. On the topic of CBDCs, the five main subtopics shared a relatively equal proportion of the conversation, with the exception of *the Fed and Dollar Limits*, which were discussed to a lesser extent.



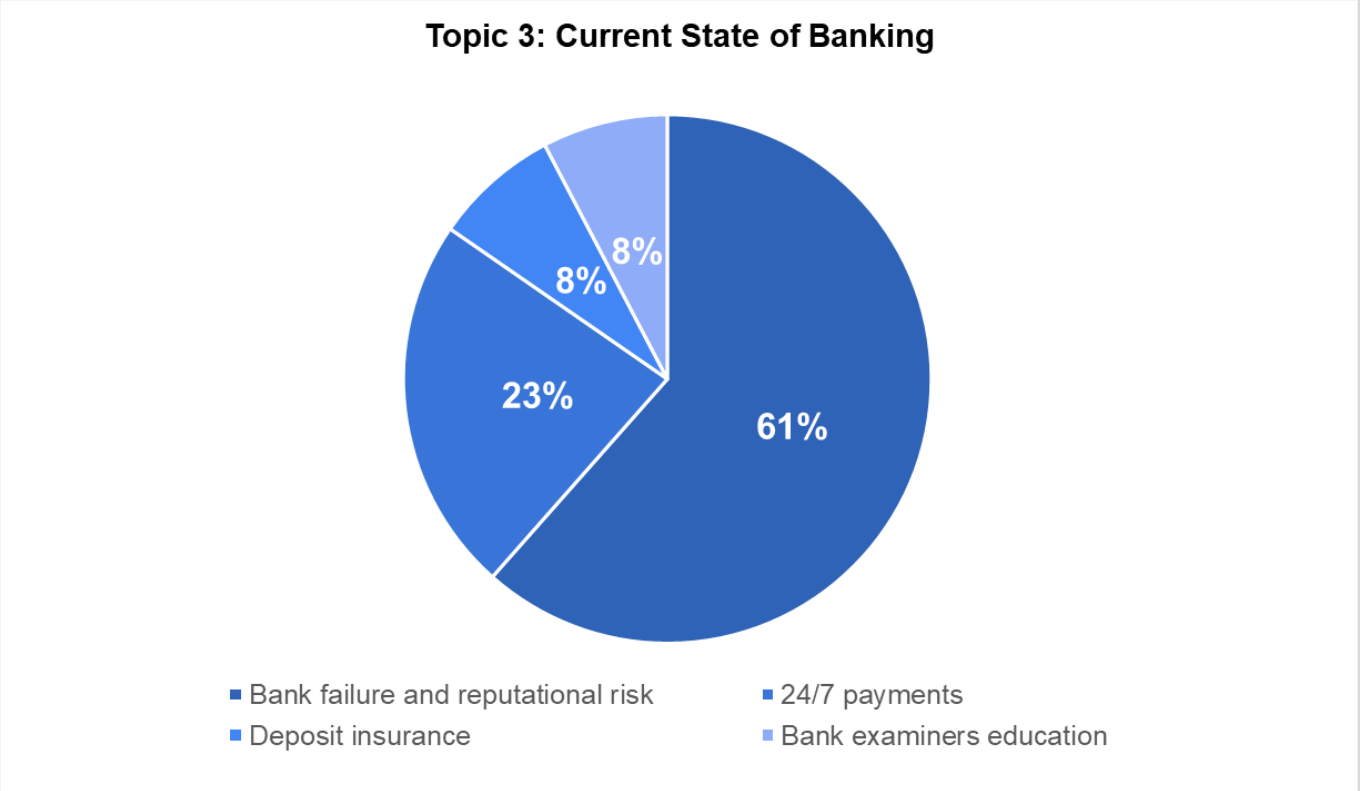
Subtopics of CBDC	Chapter 1	Chapter 2	Chapter 3	Chapter 4	Chapter 5
Stablecoins and CBDC Co-exist?	Yes	Yes	No	Yes	No
CBDC Research and Design	Yes	Yes	No	Yes	No
CBDCs Equal to Real Time Payment?	Yes	No	No	No	No
Surveillance and Privacy	Yes	Yes	No	Yes	No
Fed and Dollar Limits	Yes	Yes	No	Yes	No

For ***Topic 2: Consumer, Education, and Access to Financial Services***, the most popular topic by number of mentions was *financial inclusion*, as shown in the pie chart below. However, *user experience, empowerment, and risk absorption*, and separately, *education*, were almost as prevalent discussion topics as *financial inclusion*.



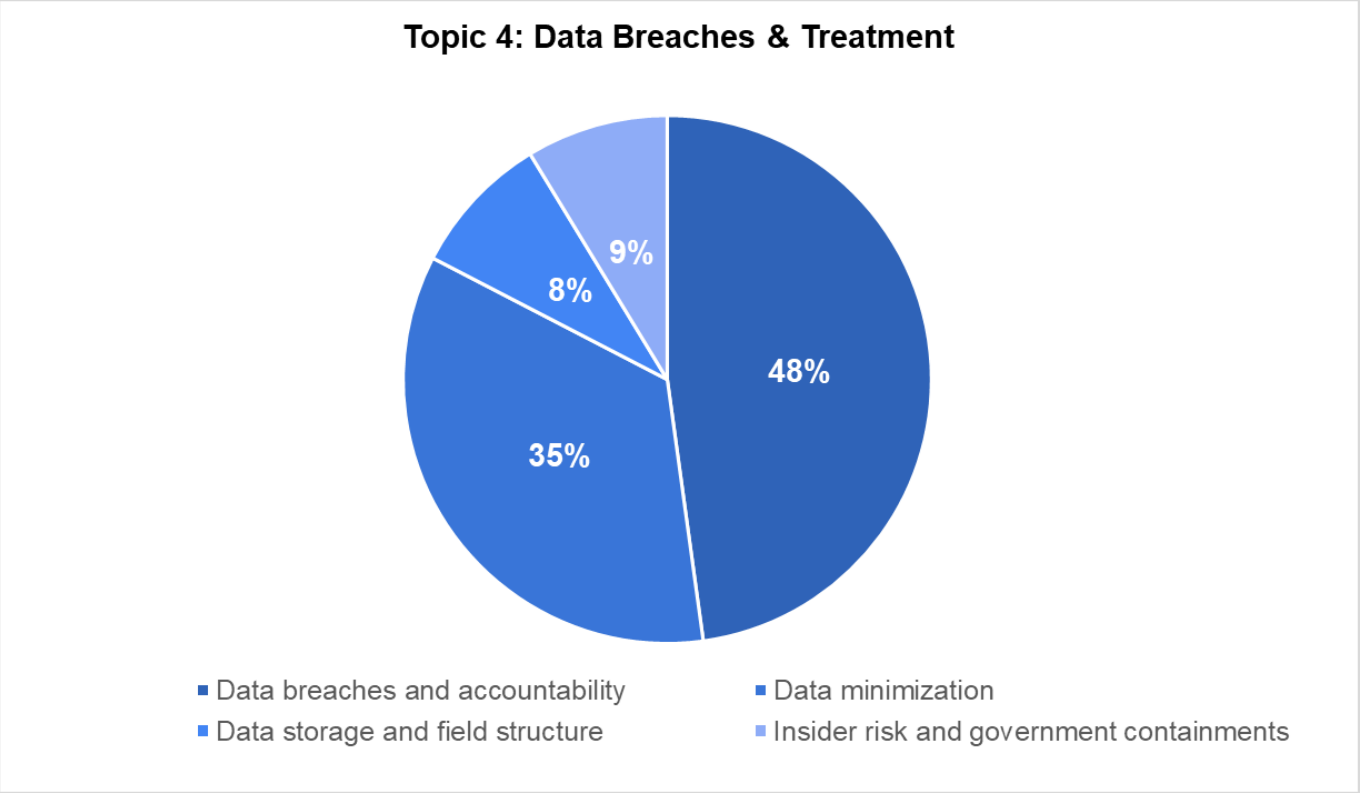
Subtopics of Consumer, Education, and Access to Financial Services	Chapter 1	Chapter 2	Chapter 3	Chapter 4	Chapter 5
Financial Inclusion	Yes	No	Yes	Yes	No
UX Empowerment and Absorbing the Risks	No	Yes	Yes	No	Yes
Education	Yes	Yes	Yes	No	No

For ***Topic 3: Current State of Banking***, *bank failures and reputational risk* stood out as a significant topic for discussion at the roundtable (61%), and the topic was brought up in four of the five chapters. *24/7 payments* were discussed repeatedly.



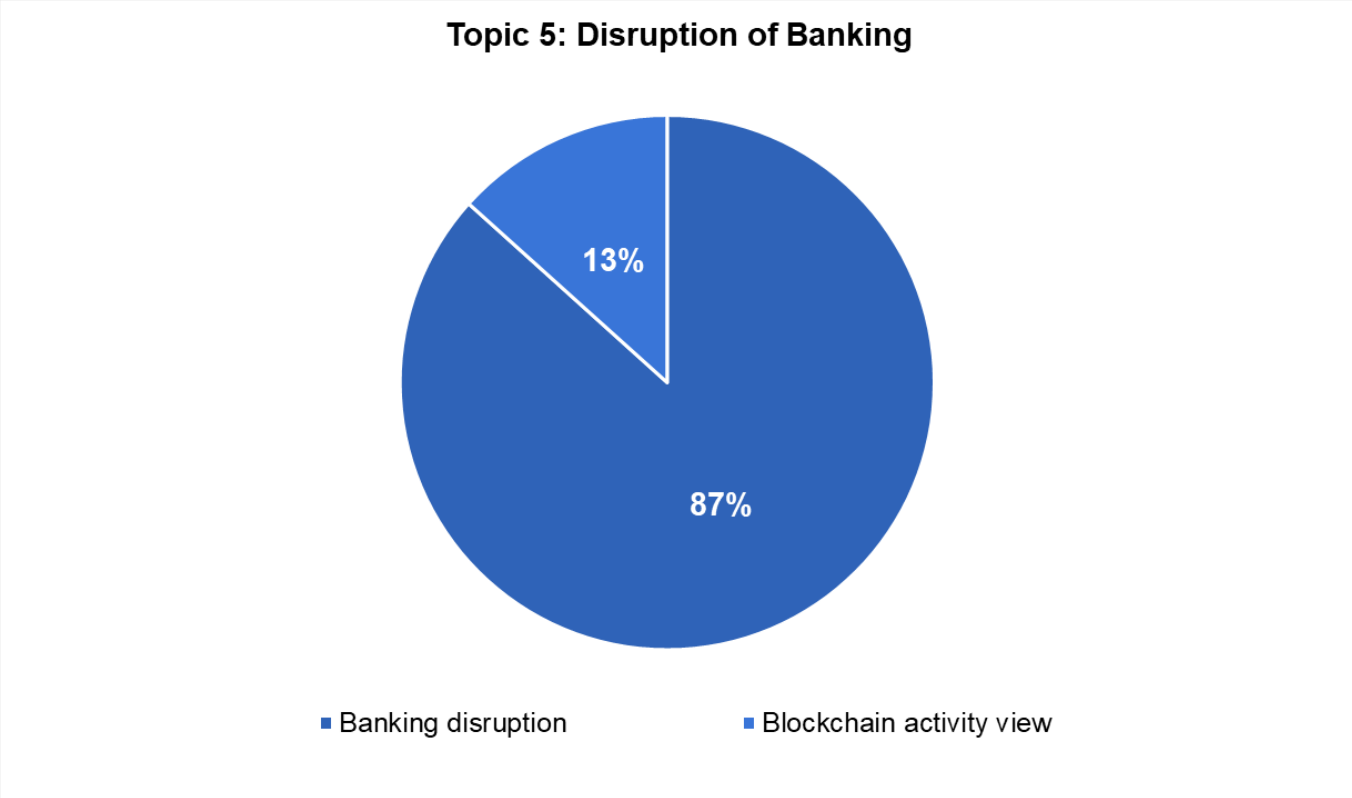
Subtopics of Current State of Banking	Chapter 1	Chapter 2	Chapter 3	Chapter 4	Chapter 5
Bank Failure and Reputational Risks	Yes	Yes	No	Yes	Yes
Deposit Insurance	Yes	No	No	No	No
24/7 Payments	Yes	No	No	Yes	No
Bank Examiners Education	No	No	No	Yes	No

The most popular subtopic within ***Topic 4: Data Breaches and Treatment*** was *data breaches and accountability*, which was heavily discussed albeit only in the final chapter of the conversation. *Data minimization*, and *data storage and field structure* came up in more than one chapter, and finally, *insider risk and government containments* was mentioned in chapter five of the roundtable.



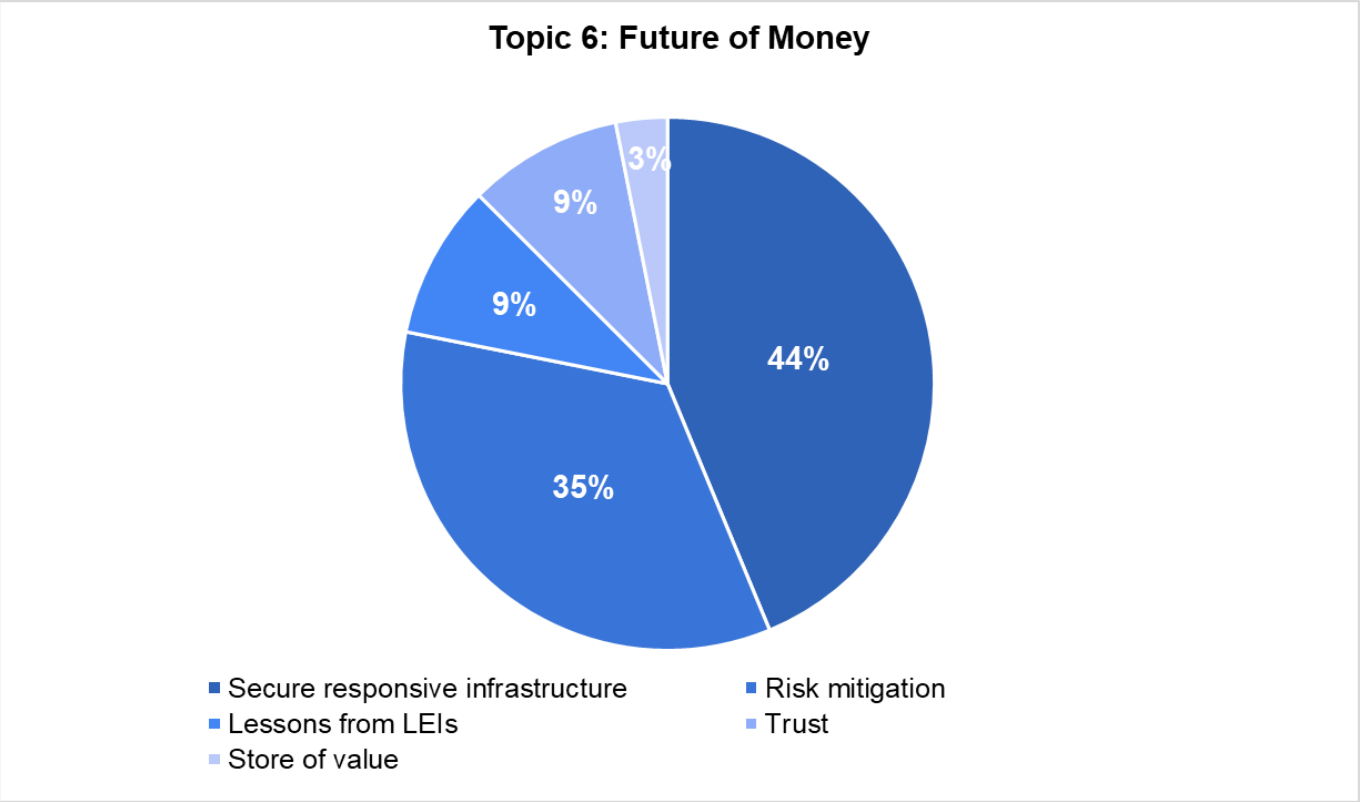
Subtopics of Data Breaches Treatment	Chapter 1	Chapter 2	Chapter 3	Chapter 4	Chapter 5
Data Breaches and Accountability	No	No	No	No	Yes
Data Minimization	Yes	Yes	Yes	No	Yes
Data Storage and Field Structure	No	No	Yes	Yes	No
Government Containment and Insider Risk	No	No	No	No	Yes

For ***Topic 5: Disruption of Banking*** *blockchain activity view* (how one can see an activity on a blockchain before seeing an identity) interestingly came up in all five chapters, but overall was discussed much less than the *disruption of banking.*



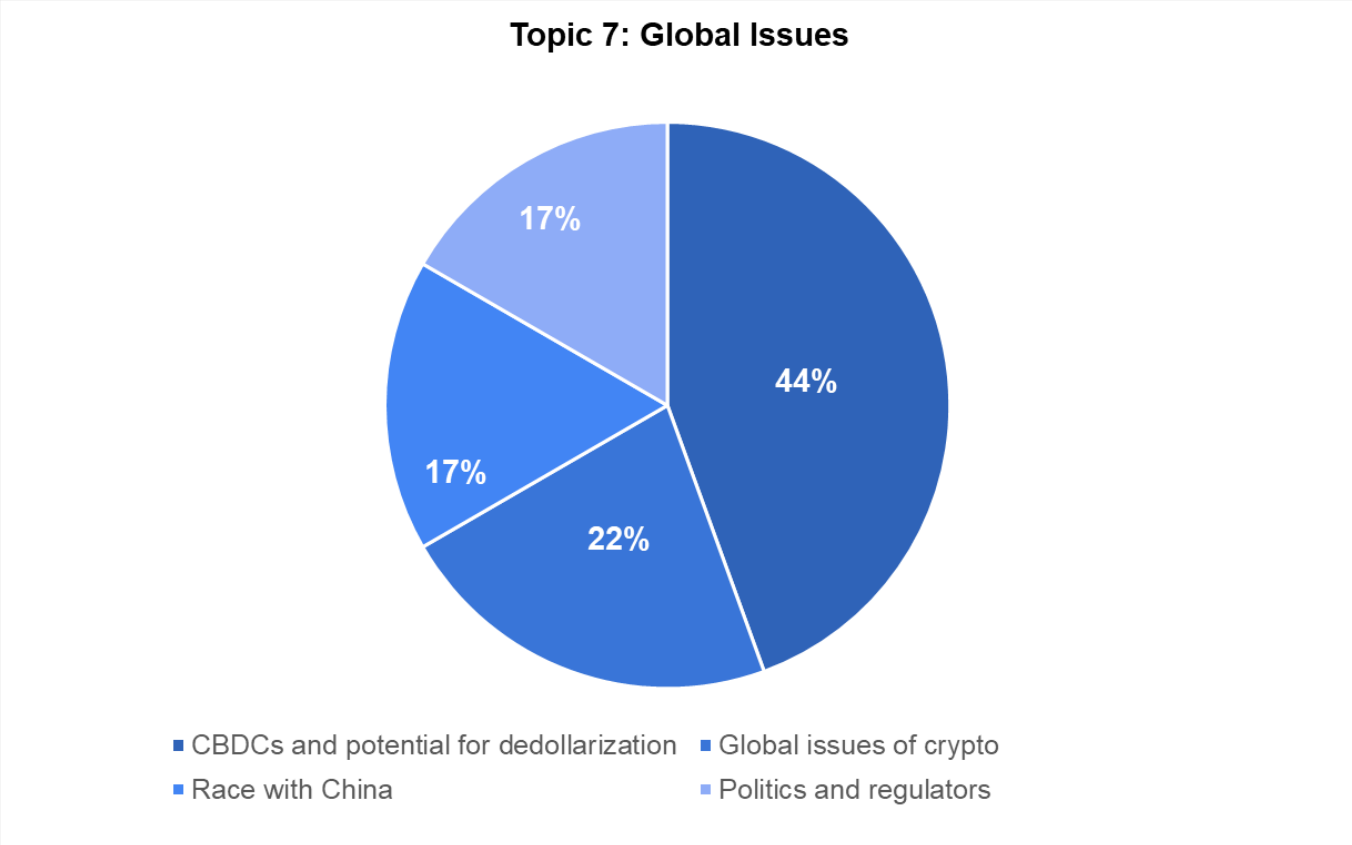
Subtopics of Disruption of Banking	Chapter 1	Chapter 2	Chapter 3	Chapter 4	Chapter 5
Banking Disruption	No	No	Yes	No	No
Blockchain Activity View	Yes	Yes	Yes	Yes	Yes

Topic 6: The Future of Money was spearheaded by dialogue on *secure, responsive infrastructure,* and this subtopic permeated each of the five chapters of the roundtable. While *Legal Entity Identifiers (LEIs)* came up in two of the five chapters, they were discussed numerous times within those chapters.



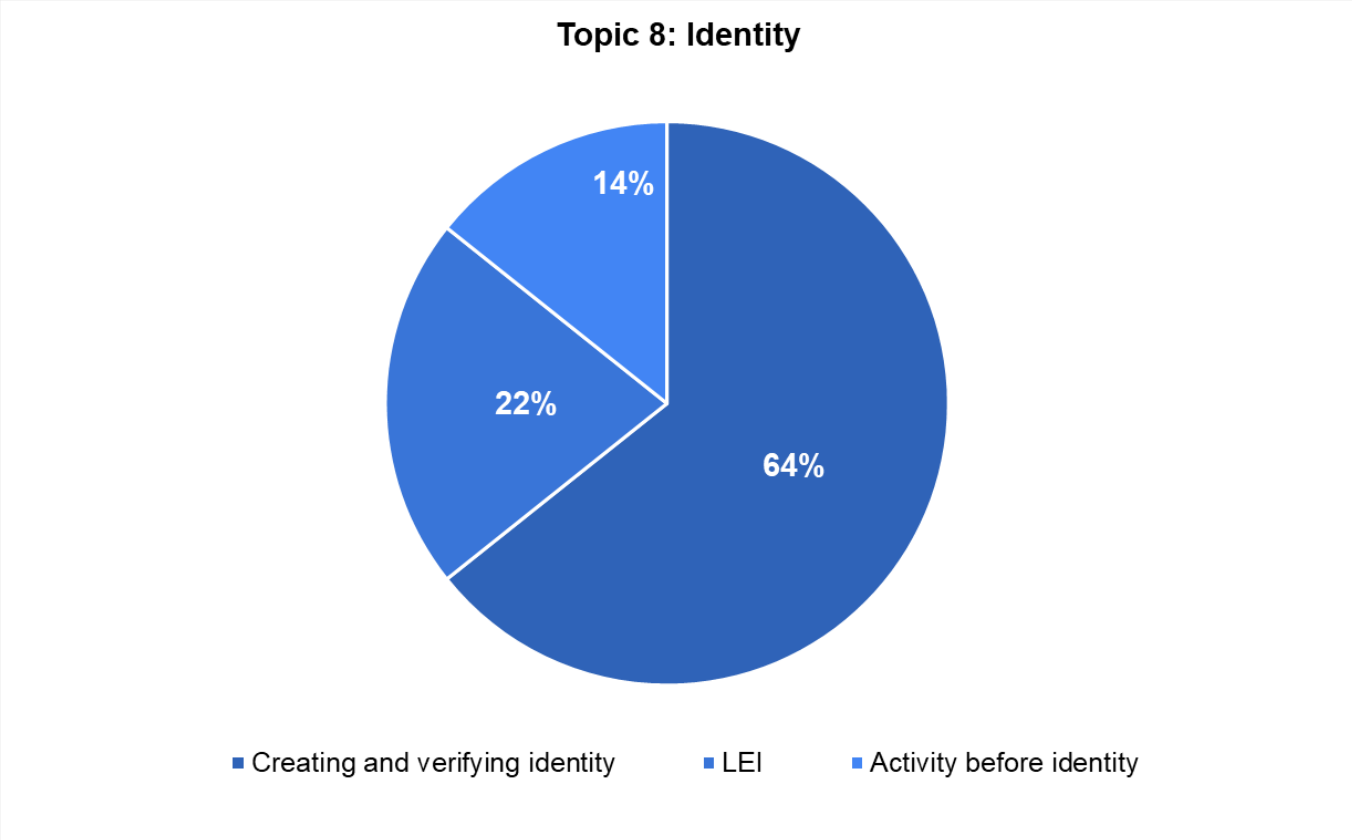
Subtopics of Future of Money	Chapter 1	Chapter 2	Chapter 3	Chapter 4	Chapter 5
Secure Responsive Infrastructure	Yes	Yes	Yes	Yes	Yes
Lessons from LEIs	Yes	No	Yes	No	No
Store of Value	Yes	No	No	No	No
Risk Mitigation	Yes	Yes	Yes	No	Yes
Trust	No	Yes	No	No	Yes

Under ***Topic 7: Global Issues***, *CBDCs and the potential for de-dollarization* headed the conversation although the *global issues surrounding crypto* were mentioned throughout various chapters of the conference.



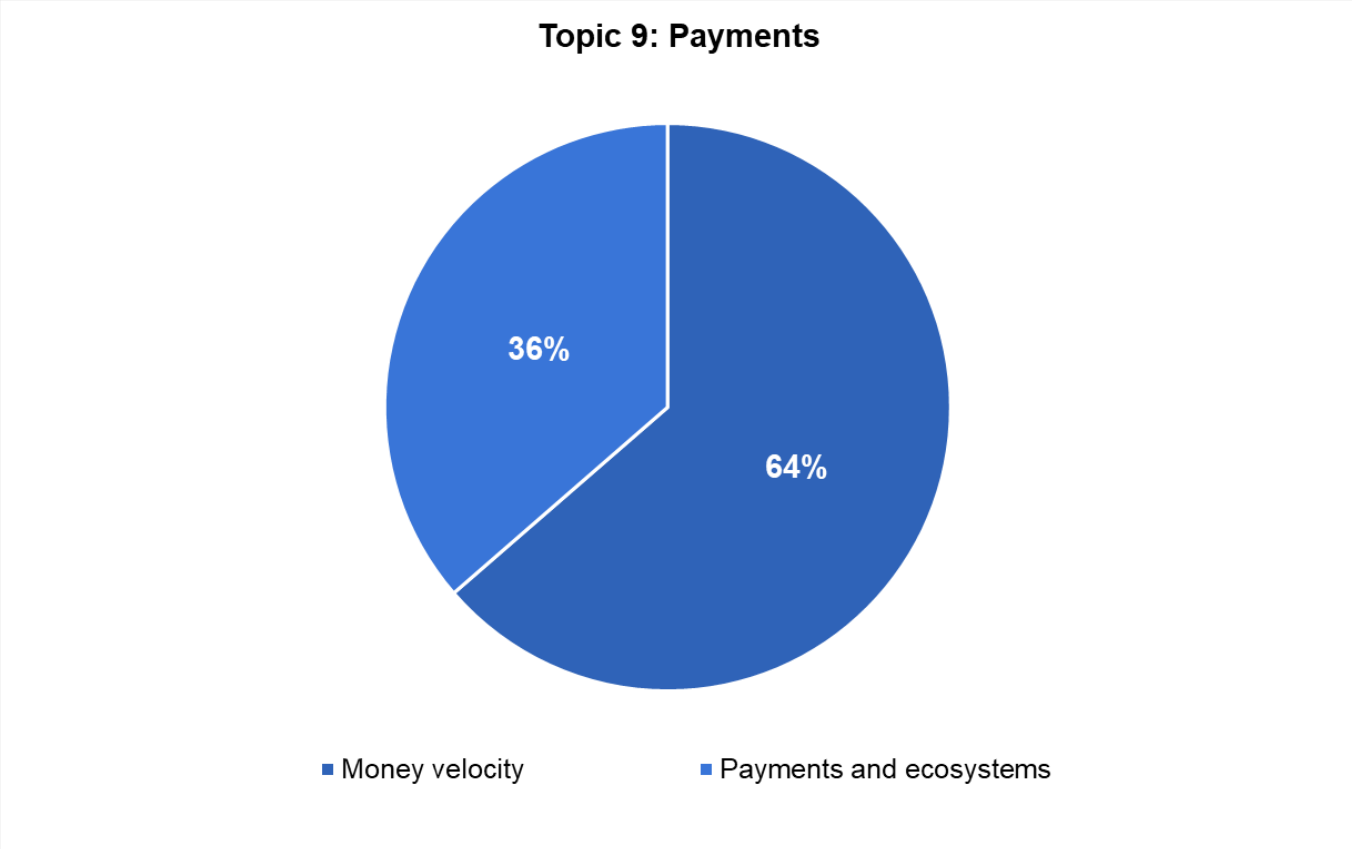
Subtopics of Global Issues	Chapter 1	Chapter 2	Chapter 3	Chapter 4	Chapter 5
CBDCs and Potential for Dedollarization	Yes	No	Yes	No	No
Global Issues and Crypto	Yes	Yes	Yes	Yes	No
Race with China	Yes	No	No	No	No
Politics and Regulators	No	Yes	Yes	Yes	No

For ***Topic 8: Identity***, *Creating and verifying identity* proved to be the most popular subtopic, and was mentioned in two of the five chapters. *LEIs* were also mentioned in two of the five chapters but with less intensity. *Activity before identity* was mentioned in one of the chapters.



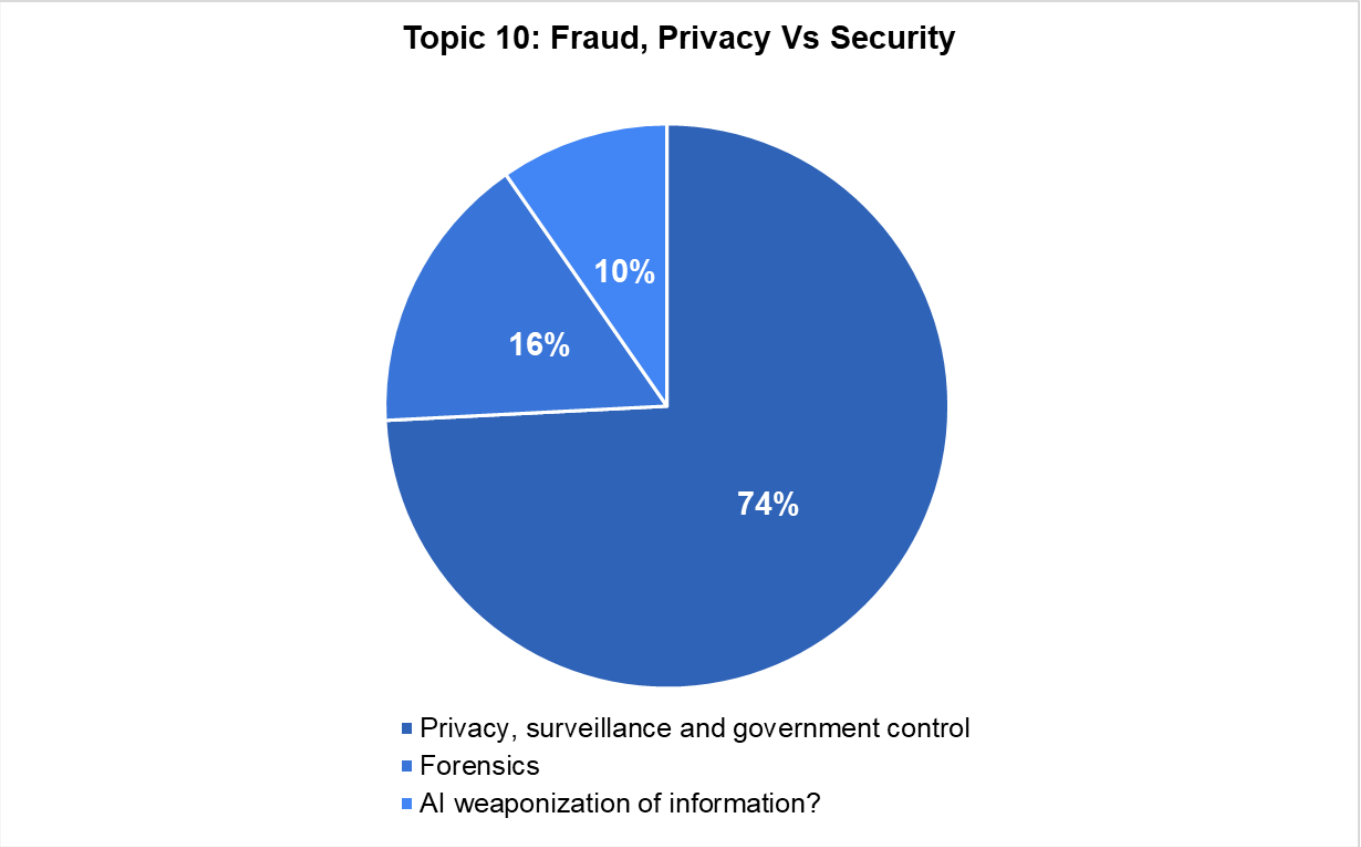
Subtopics of Identity	Chapter 1	Chapter 2	Chapter 3	Chapter 4	Chapter 5
Creating and Verifying Identity	No	Yes	Yes	No	No
LEI	Yes	No	Yes	No	No
Activity Before Identity	No	No	Yes	No	No

For ***Topic 9: Payments***, the editors extracted two subtopics: *Money velocity*, which was heartily discussed in chapter four and represented 64% of the conversation around payments, and *payments and ecosystems*, which was briefly mentioned in two of the five chapters.



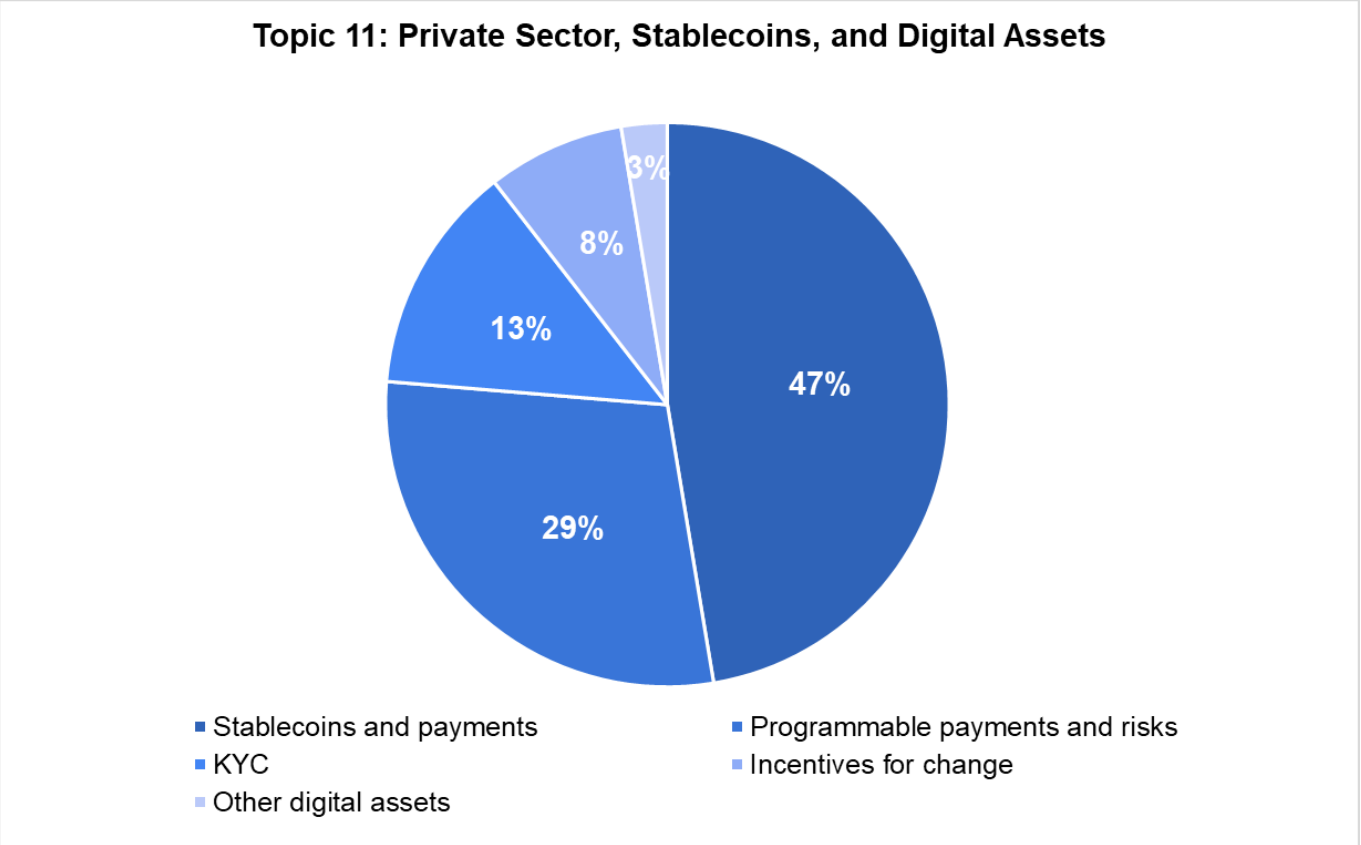
Subtopics of Payments	Chapter 1	Chapter 2	Chapter 3	Chapter 4	Chapter 5
Money Velocity	No	No	No	Yes	No
Payments and Ecosystems	Yes	No	No	Yes	No

For ***Topic 10: Fraud, Privacy Vs Security***, *Privacy, Surveillance, and Government Control* represented 74% of the comments under this heading, and came up repeatedly in the various chapters. *Forensics* was another repeated point, albeit more briefly. The influence of *AI* was also called into question during the final chapter.



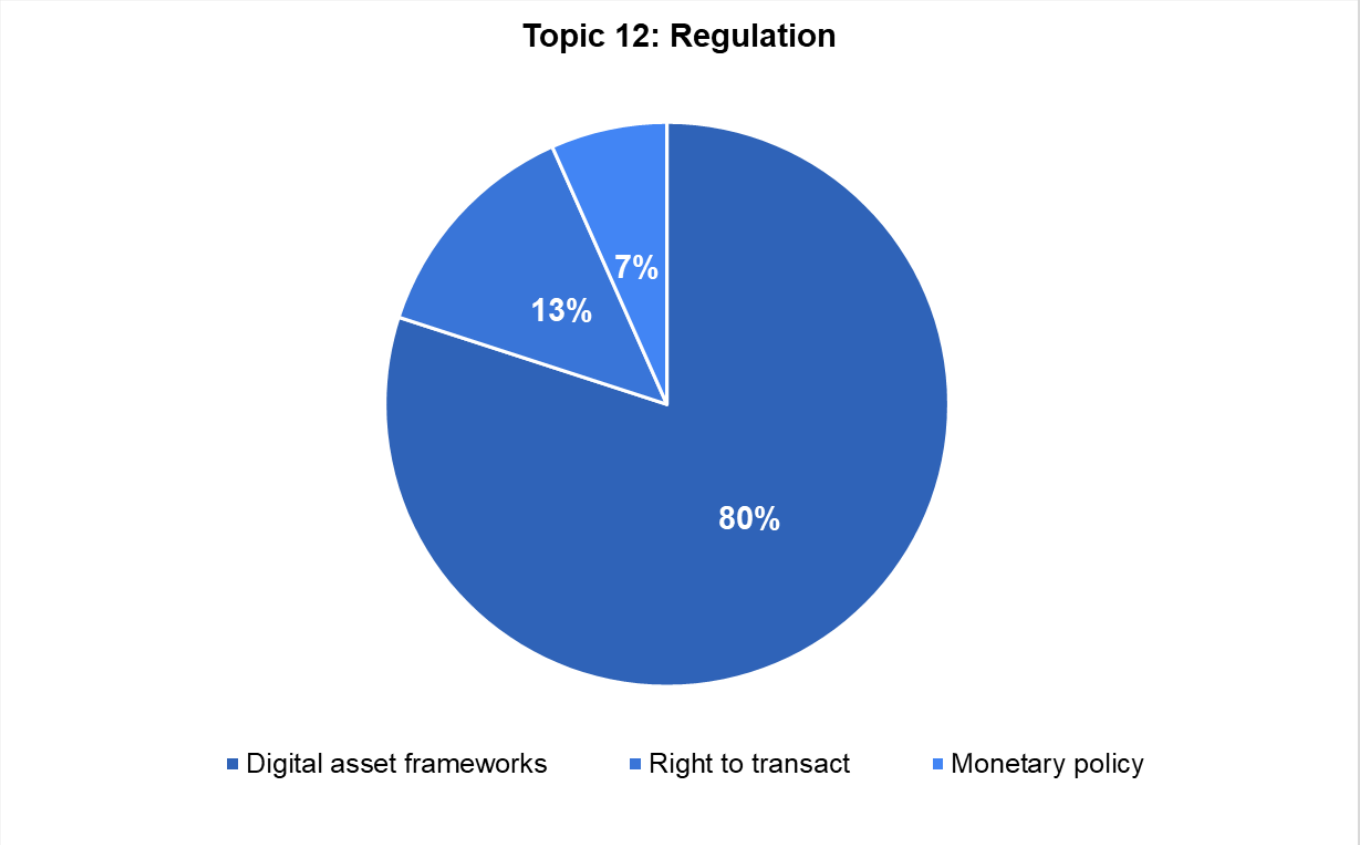
Subtopics of Fraud, Privacy Vs Security	Chapter 1	Chapter 2	Chapter 3	Chapter 4	Chapter 5
Privacy, Surveillance, and Government Control	Yes	Yes	Yes	No	No
Forensics	No	Yes	No	Yes	Yes
AI Weaponization of Information	No	No	No	No	Yes

Topic 11: Private Sector, Stablecoins, and Digital Assets saw just under half of its mentions fall under the subtopic of *stablecoins and payments*. *KYC* was another important aspect of this topic.



Subtopics of Private Sector, Stablecoins, and Digital Assets	Chapter 1	Chapter 2	Chapter 3	Chapter 4	Chapter 5
Stablecoins and Payments	Yes	No	Yes	Yes	Yes
KYC	No	Yes	Yes	Yes	No
Programmable Payments and Risks	Yes	Yes	No	Yes	Yes
Incentives for Change	Yes	No	No	No	Yes
Other Digital Assets	No	No	Yes	No	No

For ***Topic 12: Regulation***, the participants debated what *digital asset frameworks* could look like, with 80% of the conversation on regulation falling under this category. The *right to transact* and *monetary policy* were also briefly discussed.



Subtopics of Regulation	Chapter 1	Chapter 2	Chapter 3	Chapter 4	Chapter 5
Digital Asset Frameworks	Yes	Yes	Yes	No	No
Right to Transact	No	Yes	No	No	No
Monetary Policy	Yes	No	No	No	No

APPENDIX III | PREREADS

Briefing Papers

1. A Report Card on China's Central Bank Digital Currency: the e-CNY
2. An Anatomy of Crypto-Enabled Cybercrimes
3. Blockchain Architecture for Auditing, Automation, and Trust Building in Public Markets
4. Blockchain Forensics and Crypto-Related Cybercrimes
5. Boosting the Technological Infrastructure of Black Minority Depository Institutions Is Critical
6. Central Bank Digital Currency as New Public Money
7. Central Bank Digital Currency. The Risks and the Myths
8. Central Bank Digital Currency Tracker
9. Circle Highlights Role of Innovative Technology in Addressing Illicit Finance
10. Crypto Wash Trading
11. Cryptocurrency Regulation Tracker
12. Expanding Financial Inclusion or Deepening the Divide?
13. Facilitating Wholesale Digital Asset Settlement
14. Federal Reserve Bank of St. Louis: Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers
15. Financial Reporting and Blockchains: Audit Pricing, Misstatements, and Regulation
16. Fuzzy Tokens: Thinking Carefully About Technical Classification Versus Legal Classification of CryptoAssets
17. Global DCA Core Principles 2023
18. Is FedNow replacing cash? Is it a central bank digital currency?
19. It's not Choke Point. It's Crypto Quarantine.
20. Macroprudential Considerations for Tokenized Cash
21. Missing Key: The challenge of cybersecurity and central bank digital currency
22. On-Chain Foreign Exchange and Cross-Border Payments
23. Payment versus trading stablecoins
24. Privacy in cross-border digital currency: A transatlantic approach
25. Project Cedar: Improving Cross-Border Payments With Blockchain Technology
26. Project Mariana: cross-border exchange of wholesale CBDCs using automated market-makers
27. Re: Response to Request for Consultation on FSB's Proposed Framework for the International Regulation of Crypto-Asset Activities
28. Real-time payments can help combat inequality
29. State of the USDC Economy
30. The Case Against Central Bank Digital
31. The Case for Central Bank Digital Currencies

32. The dollar has some would-be rivals. Meet the challengers.
33. The Values of Money: Will Tyranny or Freedom Be in Your Digital Wallet?

Legislative Initiatives

1. Crypto Assets and CBDCs in Latin America and the Caribbean
2. Emmer Introduces Legislation to Prevent Unilateral Fed Control of a U.S. Digital Currency
3. Future financial services regulatory regime for cryptoassets Consultation and call for Evidence
4. Joint Statement on Crypto-Asset Risks to Banking Organizations
5. Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto-Asset Market Vulnerabilities
6. Remarks by Under Secretary for Domestic Finance Nellie Liang During Workshop on "Next Steps to the Future of Money and Payments"
7. The digital pound: A new form of money for households and businesses?

YouTube Videos

1. Computer scientist Amit Sahai, PhD, is asked to explain the concept of zero-knowledge proofs to 5 different people; a child, a teen, a college student, a grad student, and an expert. Using a variety of different techniques, Amit breaks down what zero-knowledge proofs are and why it's so exciting in the world of cryptography. Amit Sahai, PhD, is a professor of computer science at UCLA Samueli School of Engineering.
https://www.youtube.com/watch?v=fOGdb1CTu5c

— END —