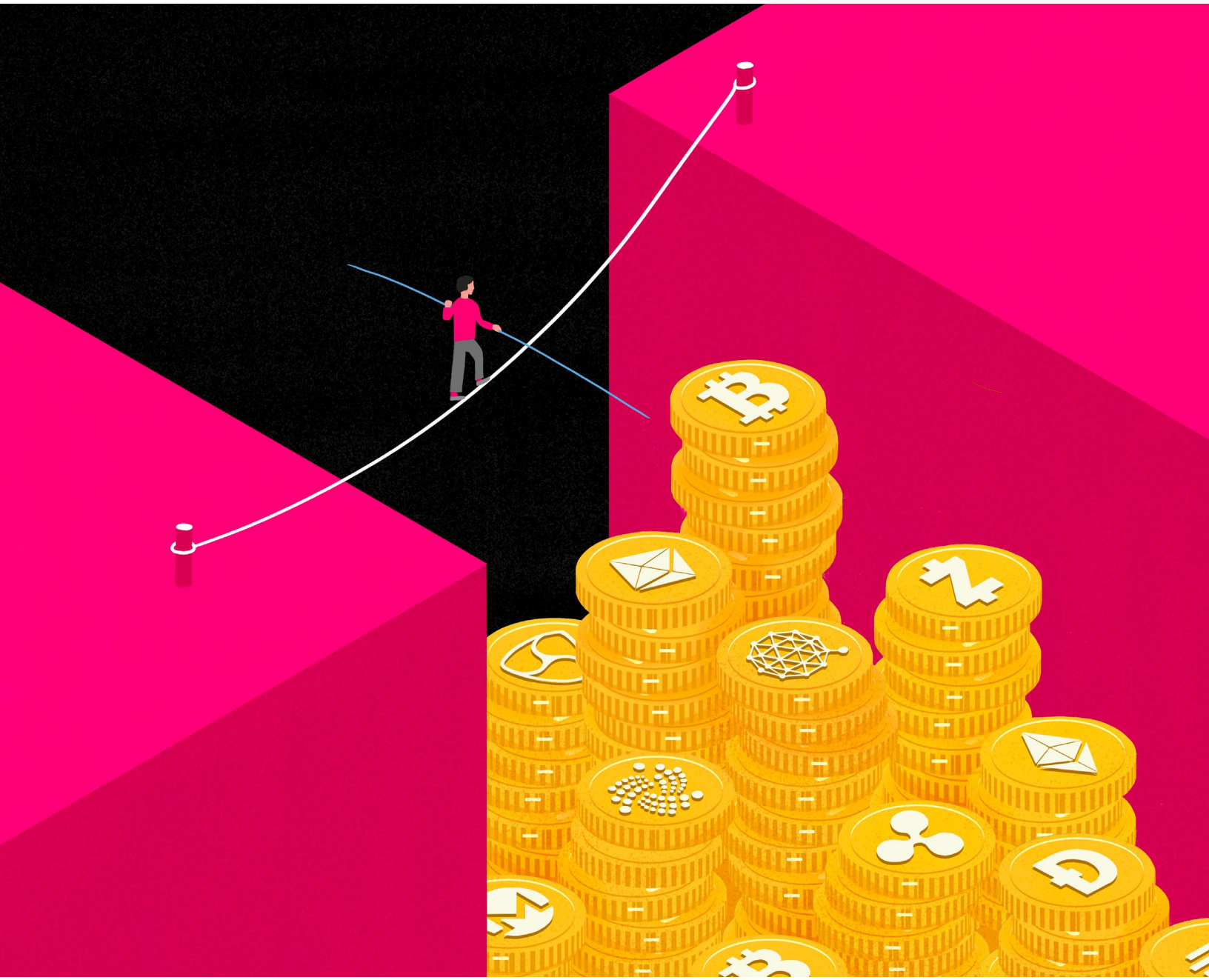
Risky Business:

The Cyber And Sociotechnical Security Threats Of Crypto-asset Trading

Tiffany Kwok, André Côté | June 2023



Toronto Metropolitan University
the dais
ROGERS cybersecure catalyst

Acknowledgements

The Dais is Canada's platform for bold policies and better leaders. We are a public policy and leadership institute at Toronto Metropolitan University, connecting people to the ideas and power we need to build a more inclusive, innovative, prosperous Canada.

For more information, visit **dais.ca**
20 Dundas St. W, Suite 921, Toronto, ON M5G 2C2

@daisTMU
/daisTMU
The Dais at Toronto Metropolitan University

Headquartered in Brampton, Ontario, and offering programs and services across Canada, the Catalyst empowers individuals and organizations to seize the opportunities and tackle the challenges of cybersecurity. Together with our partners and collaborators, we work to realize a vision of healthy democracies and thriving societies, powered by secure digital technologies. Through our groundbreaking training and certification programs; unique commercial accelerator for cybersecurity start-ups and scale-ups; first-of-its-kind cyber range; wide-ranging public education programs; and influential policy development platform, the Catalyst helps drive Canada's global competitiveness in cybersecurity.

For more information, visit **cybersecurecatalyst.ca**
2 Wellington St W, Brampton, ON L6Y 1M8

@Cybersecure_CA
Rogers Cybersecure Catalyst, Toronto Metropolitan University

Design and Illustration
Zaynab Choudhry

Copy-Editing
Cathy McKim

Contributors
Sam Andrey, Managing Director, the Dais
Karim Bardeesy, Executive Director, the Dais
Sumit Bhatia, Director of Innovation and Policy, Rogers Cybersecure Catalyst
Charles Finlay, Executive Director, Rogers Cybersecure Catalyst
Nina Rafeek Dow, Communications and Marketing Specialist, the Dais
Yuan Stevens

Reviewers
Dr. Ryan Clements, Assistant Professor, Chair, Business Law and Regulation, University of Calgary Faculty of Law
Dr. Ori Freiman, Post-Doctoral Fellow, Digital Society Lab, McMaster University
Matt Goerzen, Harvard University
Shermineh Salehi-Esmati, VP of Growth, TODAQ

How to Cite this Report
Kwok, T. & Côté, A (2023, June). Risky Business: The Cyber and Sociotechnical Security Threats of Crypto-asset Trading. Cybersecure Policy Exchange. https://dais.ca

ISBN: 978-1-77417-067-0

© 2023, Toronto Metropolitan University
350 Victoria St, Toronto, ON M5B 2K3

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. You are free to share, copy and redistribute this material provided you: give appropriate credit; do not use the material for commercial purposes; do not apply legal terms or technological measures that legally restrict others from doing anything the license permits; and if you remix, transform, or build upon the material, you must distribute your contributions under the same license, indicate if changes were made, and not suggest the licensor endorses you or your use.

Authors

Tiffany Kwok
Policy and Research Assistant

Tiffany (she/her) is a policy and research assistant at the Dais. She is passionate about tech and urban policy, service design, and research, and has experience working in the public sector and various non-profit organizations. Tiffany holds a Bachelor's degree in Political Science and Urban Studies from the University of Toronto and a Master's degree in Digital Technologies and Policy from University College London.

André Côté
Director of Policy and Research

André (he/him) has worked in a variety of roles at the intersection of policy, education, finance and tech. He's been a strategy consultant, senior advisor, chief operating officer, ed tech innovator, and author of numerous articles and reports. André is a graduate of the Munk School's Master of Public Policy (MPP) program and Queen's University.

Table of Contents

1 Executive Summary

From origins of blockchain technology decades ago to earliest use cases of digital or e-cash and the introduction of Bitcoin as the first cryptocurrency in 2008, few could have predicted the cultural phenomenon and dramatic market growth for crypto-assets of the last few years — or the dramatic and wrenching collapse of crypto-asset values and firms last year. While policymaking and oversight of crypto-asset trading has understandably been through a financial regulatory lens, this report offers policymakers and policy-focused industry leaders and technologists a new perspective: assessing the technical cyber security risks and threats, as well as the sociotechnical security interactions between technological and human dynamics.

As part of a basic primer for readers on blockchain and crypto-asset trading, this report offers novel new insights from a national representative survey conducted in October 2022 about the demographic profile of crypto users in Canada, levels of public trust in crypto asset platforms, and the types of harms purchasers of crypto-assets report experiencing.

Key findings include:

- Only one in ten Canadians have owned a crypto-asset such as Bitcoin, Ether or a non-fungible token.
- A larger share of self-reported crypto owners are men, younger, university educated and higher income.
- Owners do not express significantly different views on the political spectrum, or a greater likelihood to believe misinformation than other Canadians.
- One in three (35%) owners reported experiencing crypto fraud or scams, with higher rates among lower-income and less-educated populations;
- Nearly one in five (19%) owners report having been targeted with online harassment that caused them to fear for their safety, compared to 6% of those who have not owned crypto; and
- Canadians generally express extremely low levels of trust in crypto-asset exchanges, even before the collapse of the FTX exchange in late 2022.

Using a mixed method approach including an extensive literature review and a scan of crypto-asset policy and regulatory government initiatives, security risks and threats were assessed through two lenses. The first is more traditional **cyber security** - the technical threats and vulnerabilities related to blockchain or specific applications, typically targeted by purely malicious actors. The research identifies four categories of risk to the blockchain network, the crypto exchange, 3rd party services like crypto wallets, and to users directly, with numerous examples of cyber attacks and hacks exploiting technical vulnerabilities for financial theft, data breach, and other criminal purposes. Some attacks that are covered include spam attacks, deanonymization attacks, and crypto jacking attacks.

The second lens is **sociotechnical security**, which uses the terminology of cyber security but captures risks that reflect the interdependencies and entangled interactions of technology and social conditions. Here the research and numerous use cases from media and other sources were synthesized into four more categories: user anonymity, privacy and harassment; financial scams and fraud; high-risk behaviour, misinformation and deceptive promotion; and externalities and systemic threats.

A policy scan through the aforementioned lenses reveals the policy landscape for crypto regulation through a security lens related to the findings above. The key finding is that there has been significant financial regulatory action in Canada for crypto-asset trading, primarily in the application and enforcement of securities law, which is also having the effect of addressing certain cyber and STsec risks. There has, however, been little direct policy initiative related to cyber security for crypto-assets, and Canada can learn from jurisdictions like the EU that are introducing more integrated regulatory packages for both crypto-assets and distributed ledger technologies (DLTs), or the U.S. with a comprehensive Framework for digital assets directing federal government efforts. Standards-setting initiatives for DLTs and crypto offer potential to address security risks as well.

For policymakers and other stakeholders, the report concludes with the following recommendations:

1. Conduct further research on the security threats and harms associated with crypto-asset trading, and increase public engagement with communities of crypto users to inform policymaking.

2. Ensure crypto-asset policymaking is timely and iterative, to allow for innovation in blockchain and fintech while assuring market integrity, security and consumer protection.

3. Enhance public transparency and cyber security-aligned consumer protection requirements for crypto-asset investors and users.

4. Align financial regulation of crypto-assets with other Canadian policy and legal regimes, including cyber security, privacy and data protection, and online safety.

5. Coordinate and collaborate on crypto-asset policymaking with peer jurisdictions and transnational governance and standards.

2 Introduction

The origins of blockchain technology date back to the 1990s, when the earliest use cases included digital or e-cash and time-stamping documents. A key milestone in this evolution of blockchain technology was in 2008 with the introduction of Bitcoin. In the wake of the Great Recession of the late 2000s, an individual (or a group of people) using the pseudonymous name Satoshi Nakamoto published a white paper called *Bitcoin: A Peer-to-Peer Electronic Cash System*.[1] This blueprint for Bitcoin established the initial design and logic for blockchain and the first cryptocurrency. These origins that set the technology on its course have contributed to a path dependence, with initial decisions related to the design and function of the blockchain influencing the evolution and development of the technology in the years since. The evolution has contributed to the emergence of a broader marketplace for decentralized finance (DeFi).

While Bitcoin adoption remained relatively niche in the years after its launch in 2009, there has been rapid growth of the crypto asset market and acceleration in consumer purchasing and trading of cryptocurrency in recent years. A Bank of Canada survey in 2021 found that 13% of Canadians owned Bitcoin, a figure that had more than doubled from the prior year.[2] Surveys in the U.S. indicate similar proportions of the population trading and investing in cryptocurrencies in 2021.[3] The rapid growth of the crypto-asset market has also seen the emergence of new types of blockchain-based tradable assets. Stablecoins have been introduced in an effort to reduce the volatility of cryptocurrencies by pegging them to a reference asset, such as a national currency.[4] Central bank digital currencies (CBDCs) have launched in a select few jurisdictions, and are being explored in many others including Canada, to act as a digital form of a country's fiat currency.[5] Non-fungible tokens (NFTs) — unique digital identifiers, like digital artwork or collectible, recorded on a blockchain to certify authenticity and ownership — briefly exploded in popularity, with one study finding that globally the number of NFT purchasers increased from 75,000 to 2.3 million people in 2021.[6]

Yet, the crypto boom that peaked in late 2021 and early 2022 has since transitioned to spectacular bust. The decline in crypto market values through 2022 led to the cascading failure of numerous exchanges and crypto market intermediaries, culminating in the shocking insolvency of the second largest crypto exchange in the world, FTX Trading Ltd., at the end of 2022. The failure of FTX led to losses of more than $8 billion for its customers, some of which were diverted to fund undisclosed venture investments, resulting in charges of financial impropriety and fraud against the company's CEO.[7] Overall, the "crypto winter" that befell the global crypto market in 2022 resulted in declines of $2 trillion in total market value

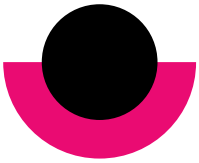
from the peak,[8] as well as the collapse of other assets like NFTs whose trading volumes fell by 97% in 2022 from a January peak.[9]

The events of the past two years have placed a heightened focus on the governance of crypto assets, as stakeholders — crypto entrepreneurs, investors and consumers, policymakers and regulators — seek to balance the innovative potential of the blockchain-based products with appropriate guardrails to protect against the range of risks that have emerged. In the Canadian context, policy for crypto assets has primarily been through a financial regulatory lens, focusing on aspects such as securities law, taxation and anti-money laundering provisions.[10] However, crypto assets have introduced a whole other domain of technological and cyber security risks, surfaced through both experiences in the crypto asset marketplace over the past decade reported in media and other sources, and through a growing body of academic study.

This report focuses on the technological risks and related policy implications associated with blockchain and crypto-asset trading, focusing on two particular types of risks: cyber security threats from technical vulnerabilities of the blockchain or a specific application (e.g., more traditional hacks and breaches), and a new category of sociotechnical security risks resulting from the entangled interactions of technical and social or human factors (e.g., scams, misinformation, or higher order threats).

The report begins with a brief primer on blockchain, crypto-asset trading and insights about Canadian users of crypto, introducing key terms and concepts for readers. The next section examines the two sets of cyber and sociotechnical security risks related to crypto-asset trading, and the types of threats, attacks and harms they have resulted in. The section that follows describes the state of policy and regulation for crypto-assets in Canada and a selection of other key jurisdictions, focusing on policy and regulatory interventions and gaps to address cyber and sociotechnical security risks. The final section provides concluding findings and recommendations for policymakers and other stakeholders.

To explore this relatively new and complex field, we employed a mix of methods: an extensive literature review; a scan of crypto-asset policy and regulatory initiatives introduced by governments and public institutions, industry and standards-making bodies; and a representative survey of Canadians and their experiences with crypto-asset trading. A small group of academic and industry experts graciously reviewed a draft of the report to offer their feedback and insights. We alone are responsible for the analysis and findings in the report, and any errors or omissions.



The rapid recent emergence of crypto assets, both as a social phenomenon within Canadian and global public consciousness and as a hugely volatile and lightly-regulated financial asset class, has created a great imperative to better understand the associated risks and policy considerations.

The rapid recent emergence of crypto assets, both as a social phenomenon within Canadian and global public consciousness and as a hugely volatile and lightly-regulated financial asset class, has created a great imperative to better understand the associated risks and policy considerations. While policy attention has centred on the financial regulation of crypto-asset trading, this report focuses on the less explored domain of cyber and sociotechnical security. This ought to be of significant interest to policymakers and regulators, industry, technologist and consumer communities in Canada and beyond, for informing the development of policy and regulatory approaches for crypto-assets, but also for other uses of blockchain as part of the next wave of decentralized digital innovation many are calling Web3.

3 A Short Primer on Blockchain Technology and Crypto-asset Trading

Blockchain technology is, at its core, a records-management system. A type of distributed ledger technology (DLT), the development and maintenance of the digital database is carried out by participants connected through a peer-to-peer network, rather than held by a centralized third party.[11] In addition to the Bitcoin blockchain, many other blockchain networks have emerged over the past decade, with some most active for crypto trading and other uses being Ethereum, Solana, BNB Chain, Arbitum and Avalanche.[12] While the original Bitcoin white paper did not use the term "blockchain," referring instead to chains of blocks and digital signatures, many of the attributes described in the Bitcoin white paper are common in other blockchain networks. These include: consensus-based transaction verification, user anonymity (or "pseudonymity"), transparency of the public ledger, and unalterable ("immutable") records once added to the blockchain. These attributes, and their rationale, are explored in more detail below, with a **Glossary of Terms** for unique vocabulary we encounter in the report.

A note for readers: in this report, the term *blockchain* is used to refer to the technology *generally*, rather than to specific *networks* such as Bitcoin or Ethereum.

Glossary of Terms

Consensus Mechanism: A method of forming consensus that guarantees a state, value, or piece of information is correct in a distributed ledger technology. Some popular consensus mechanisms include proof-of-work (PoW) and proof-of-stake (PoS).

Crypto-asset Exchange: A firm or individual who provides services and operates a machine to exchange crypto-assets for money or vice versa, and holds private cryptographic keys on behalf of its customers.

Crypto Mining: A process that uses computers or specialized hardware to confirm cryptocurrency transactions. If a miner's blocks are accepted and become part of the blockchain, the miner usually receives payment in the cryptocurrency they are validating.

Decentralized Finance (DeFi): An emerging ecosystem of crypto-asset based financial products and services, which are delivered through applications built on the blockchain using smart contracts.

Distributed Ledger Technology (DLT): Used in payments, issuing debt and equity, trade finance, and post-trade processes. This technology performs the functions of banks and governments in verifying and managing currency transfer and supply. Blockchain is a type of DLT.

NFTs (non-fungible token): Digital assets that represent real-world objects like art, music, in-game items and videos that can be bought and sold. They are generally built with the same kind of programming as cryptocurrency, like Bitcoin or Ethereum, but have a digital signature that makes it impossible for them to be copied (non-fungible).

Risk, Threat and Vulnerability: *Risk* expresses potential for loss, damage or destruction of assets or data caused by a cyber threat. *Threat* is a process that magnifies the likelihood of a negative event, such as the exploit of a vulnerability. *Vulnerability* is a weakness in the infrastructure, networks or applications that potentially exposes you to threats.

Smart contracts: Digital contracts, stored on the blockchain, that automate the execution of an agreement when precoded conditions are met and verified. They can define rules and are automated to enforce them by code.

Stablecoins: Cryptocurrencies where the price is pegged to another asset deemed to be more stable, such as fiat currency, another cryptocurrency, or to exchange-traded commodities.

Wallets: Crypto wallets store and safeguard a combination of cryptographic public and private keys that grants access to a user's crypto-assets. The type of wallet can differ based on the method or location of storage. Internet connectivity defines whether a crypto-asset wallet is 'hot' or 'cold'.

Web3: A phase of the internet following Web2, intended to replace centralized, corporate platforms with decentralized networks and increased ownership over content for users.

Sources: (Bains, 2022); (GOV.UK, 2023); (Canada Revenue Agency, 2022); (Conti and Broverman, 2022); (Alexander, 2021); (IBM); (@wackerow, 2022); (White); (Roose, 2022).

The Unique Attributes of Blockchain for Crypto-asset Trading

When Nakamoto introduced the Bitcoin concept on what would later be called blockchain technology, it sought to address at least four particular challenges.

The first was to reduce reliance on traditional finance. In the wake of the 2007-08 global financial crisis, there was heightened distrust of the financial system and its institutions. Bitcoin sought to reduce or eliminate the need to rely on traditional financial institutions that acted as centralized authorities for the processing, recording, and verification of financial transactions. Instead, Bitcoin would be a peer-to-peer electronic cash system, built on open-source software that would enable transactions to be facilitated by a decentralized network of computers.[13]

The second was to establish a trusted verification system for peer-to-peer transactions. In place of a centralized authority for validating transactions, cryptographic technology would allow "chains'' of transactions to be formed into "blocks'' of data that are posted to the blockchain ledger at regular time intervals. Each transaction or block is affixed with a unique identifier that confirms the sender and receiver (called a "signature" or cryptographic "hash"). Transactions are time stamped and publicly accessible to provide transparency and address the problem of 'double-spending' (i.e. using the same electronic cash twice).[14] Multiple computers (called "nodes") temporarily store information about proposed transactions as a verification step, prior to the permanent record posting on the blockchain.

The third was to address risks of fraud and tampering through consensus verification. To address the risk of editing or insider tampering with transaction blocks in an effort to steal from users, verification of each block occurs through a decentralized "consensus mechanism." Blockchain network users must contribute their computational energy (called "mining") to solving "moderately hard, but not intractable" cryptographic equations to verify transactions.[15] In this "proof-of-work" consensus model, users are incentivized through the potential cryptocurrency payments, as block rewards or transaction fees.[16] Once verified and posted to the blockchain, records are then non-reversible (or "immutable"), so they cannot be altered later.

The fourth was ensuring the privacy of transactions and the 'pseudonymity' of users. The solution was the use of a "public key" (username) and "private key" (password) model. Each user is represented by a string of random numbers, functioning like a self-generated username and password that are not stored by a centralized intermediary.[17] To complete a transaction, a user's private key generates their digital 'signature,' which demonstrates their ownership of a public key without requiring them to reveal their private key. Each transaction requires the use of a unique digital signature, which cannot be reused. While the identity of a user is not revealed, the record of the transaction on the public blockchain reveals their unique cryptographic 'signature', representing a type of virtual pseudonym (if not complete anonymity).

Variations in the Design of Blockchain Projects

While Bitcoin has informed the design of blockchain and distributed ledger technologies since its introduction in 2009, there have been significant variations in the design of blockchain networks over time.

- **Consensus mechanisms.** Common to the trust and verification for blockchain networks, other consensus mechanisms have been introduced in addition to the initial Bitcoin 'proof-of-work' protocol.[18] The most widely used variation is 'proof-of-stake', where users "stake" digital currency (rather than "mining" it) as collateral in a smart contract to verify transactions on the blockchain, incentivized by digital currency rewards.[19] A primary benefit of 'staking' is that it does not demand the energy intensive hardware systems and computing capacity for 'mining', reducing electronic waste, energy consumption and carbon dioxide pollution.[20] In September 2022, the largest blockchain network, Ethereum, transitioned to proof of stake through a process they called *The Merge.*[21]

- **Public versus private blockchains**. Bitcoin and Ethereum are *public* blockchains, where peer-to-peer transactions are posted on a publicly accessible ledger and users can participate in consensus verification.[22] Other networks have been developed as *private* or *semi-private* blockchain projects, limited to a certain group of users.[23] Private blockchains are more comparable in concept to a traditional financial intermediary, with examples including R3 Corda and Hyperledger.

- **Pseudonymous versus anonymous.** Privacy is an attribute of the Bitcoin blockchain and other public networks where users do not have to provide name and identity information. Yet, users' cryptographic public key does represent a form of pseudonym that can be traced, as multiple transactions can be linked to a single user and could potentially be linked to a legal identity.[24] As a result, variations such as Monero, Dash, and Bitcoin Private have emerged that use technical features to provide full anonymity.[25]

- **Immutable versus alterable records.** Blockchain's cryptographic protocols typically apply the attribute of "immutability," where recorded data cannot be modified or manipulated.[26] However, some experts note that there have been work-arounds to this principle, such as when Ethereum was "hard forked"[27] - or re-coded - through a software update to reset the funds for users that had been stolen during a hack.[28]

Other Examples of Blockchain Use Cases

The blockchain's attributes have made it appealing for applications beyond crypto assets, with numerous other real or potential use cases.[29] In Brazil, a **land registry system** was trialed, with timestamping on the blockchain providing both the owner and legal administrative system with assurance of the authenticity and reliability of the land title record.[30] For **identity management**, a Canadian example is SecureKey's blockchain-based online identification service, which is in use in financial services with many potential future public sector applications such as driver's licenses, passports, and other official documents.[31]

Another use case is in **health care** for hospital and clinic information systems, with the potential to decentralize health record databases and shift control of personal data to patients. In British Columbia, blockchain technology was introduced for a project of the Centre of Excellence for Prevention of Organ Failure (PROOF), where the intention was to provide patients the ability to secure ownership of their personal health data, yet the actual execution showed that the institution retained some control of the hospital records.[32] Blockchain has also been used in the realm of **humanitarian aid** as part of digitization efforts, including in the provision of cash transfers to refugees in refugee camps, and linking biometric data to verify identity-related information.[33] As with crypto assets, each of these use cases offers both potential benefits and risks in applying blockchain technology.

The blockchain's attributes have made it appealing for applications beyond crypto assets, with numerous other real or potential use cases.

What are Crypto-assets?

"Crypto-asset" is a widely-used umbrella term that refers to digital assets that are issued and transferred on blockchain and other distributed ledger technology systems.[34] Designed to be used as a medium of exchange and a store of value,[35] they include cryptocurrencies (e.g., Bitcoin, Ether, CBDCs), non-digital assets like utility and governance coins, security tokens, and non-fungible tokens (NFTs). Crypto-assets can be transacted on exchanges, marketplaces, and during online games.[36] They are held in wallets. Key actors in the crypto-asset ecosystem include its users, miners and stakers, cryptocurrency exchanges, brokers, wallet providers, coin inventors (who develop the technical foundations of a cryptocurrency), and coin offerors (who offer coins to users, for free or for a fee, upon a coin's initial release).[37]

How Crypto-assets Are Traded

Crypto-assets are traded on exchanges, which are digital platforms for buying and trading cryptocurrency and other digital assets. NFTs are traded on marketplaces, rather than exchanges.[38] Forbes' 2022 report on global crypto exchanges reported approximately 600 cryptocurrency exchanges operating worldwide.[39] There are broadly two types of exchanges:

1. **Custodial exchanges**, which function like traditional stock or foreign exchange brokers but for crypto-assets, and manage wallets on behalf of users. These exchanges tend to require account registration and identity verification, similar to other types of online trading platforms for financial products.[40] Examples include large global exchanges such as Binance, Kraken and Coinbase, and Canadian exchanges Coinsmart and Bitbuy.

2. **Non-custodial or peer-to-peer exchanges**, where no centralized platform facilitates interactions. Users transact directly with each other and must manage their own wallets, safeguarding their private and public keys, in order to access and trade their assets.[41] Accounts are generally not needed to trade on non-custodial exchanges, nor is there a need to provide personal information to an exchange. Uniswap, IDEX, SimpleSwap, and Localbitcoins are examples of non-custodial exchanges.[42]

Crypto-asset Users in Canada

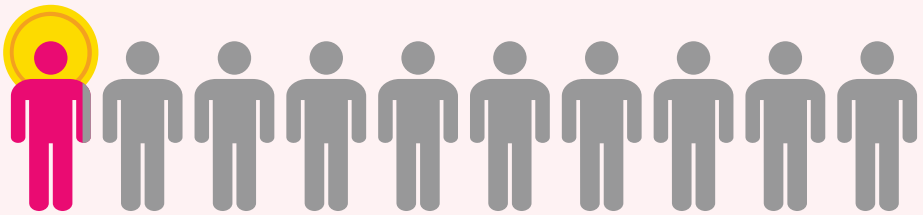
While cryptocurrency exploded as a cultural and market phenomenon over the past two years, research and analysis of the goals, profiles, attitudes and experiences of crypto market participants remains limited. Experts who have studied why people buy crypto-assets have found that motivations range from the potential for long-term investment gains to a sense of social and emotional belonging within the crypto-asset community, in some cases encouraged by celebrities and other influencers.[43] Elon Musk's tweets and online interactions, for instance, about the cryptocurrency Dogecoin are attributed to significant buying and price fluctuations (not to mention countless Twitter memes).

Others have described an emotional and peer-driven "lean in" philosophy among crypto enthusiasts. The scholar Simon Mackenzie describes how the risk-taking culture in crypto-asset markets has been an attractive feature for many participants: the "society of traders [...] celebrate their 'degeneracy' and make investment decisions based on motifs like 'yolo' (you only live once) into 'moonshots' (risky bets on crypto with potentially huge upside)."[44] A study by the UK financial regulator in 2019 found that many crypto users find the market risks attractive, though few have explicit strategies in place to manage the financial risks.[45]

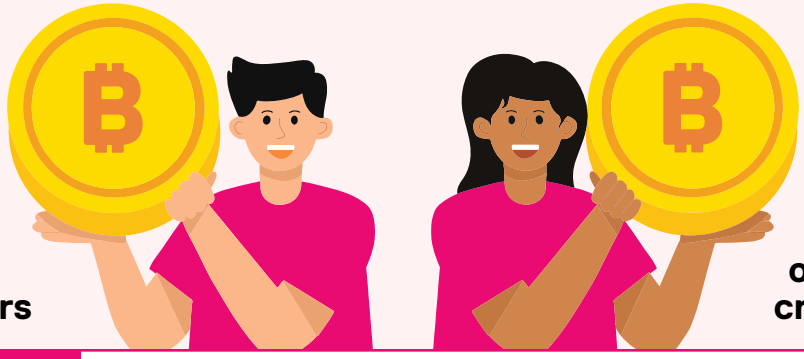
In Canada, there has been little substantial analysis to date of the attitudes or experiences of crypto-asset users. Last year, however, the Bank of Canada published a report on Bitcoin ownership and use in Canada between 2016 and 2020, finding that users tend to be younger, educated men with higher than average household income and lower levels of financial literacy.[46] Like the UK study, the Bank of Canada report found that participants sought to invest in and profit from crypto-assets without a comprehensive understanding of the technology and the associated financial risks, including price crashes, lost funds, or scams.[47]

This report provides a new contribution to our understanding through a representative survey of 2,000 Canadian residents aged 16 and older, conducted online in October 2022. The profile of crypto users closely reflects the Bank of Canada's findings. Our research found that, even by late 2022 after the crypto market peak, a minority (9%) of Canadians reported having purchased a crypto-asset, such as Bitcoin, Ethereum or an NFT. A larger share of crypto owners were men (14% of Canadian men compared with only 5% of women), and in particular men between 25 and 35 years old (26%). A higher percentage were university-educated (13%) than college or below (8%), and are from households with incomes of over $100,000 (14%).

Profile of Crypto-asset Users in Canada



9% of Canadians reported having purchased a crypto-asset, such as Bitcoin, Ethereum or an NFT



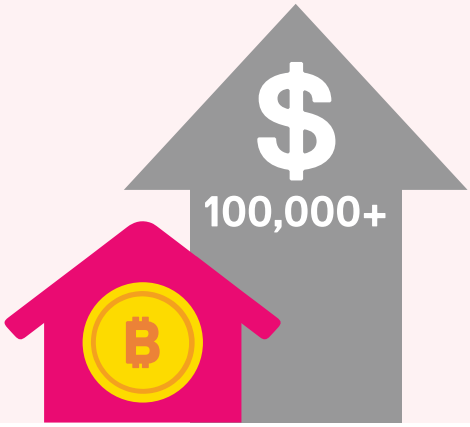
14%
of men are crypto owners

5%
of women are crypto owners

26% of men between 25 and 35 years old are crypto owners

13%
of university-educated Canadians are crypto owners

8%
of college-educated or below Canadians are crypto owners



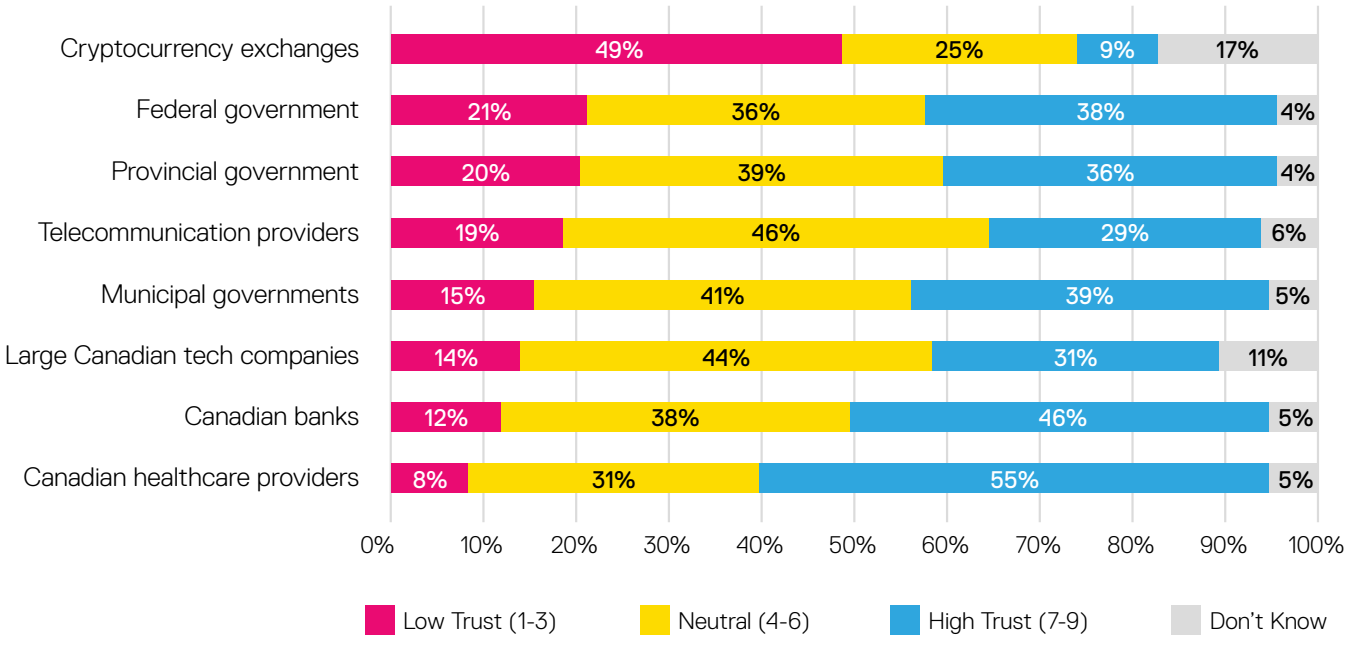
14%
of Canadians from households with incomes of over $100,000 are crypto owners

In terms of political orientation or ideology, owners of crypto reported very similar views to the overall population — despite some public perceptions connecting crypto enthusiasm to right wing ideologies or protest movements like the Truckers' Convoy.[48] We also sought to understand the relationship between crypto-asset ownership and belief in misinformation. We asked survey respondents about their belief in eight statements concerning vaccines, immigration, climate change and the Russian invasion of Ukraine, and somewhat surprisingly found no significant difference between those who have and have not owned crypto-assets (owners of crypto average 5.1 correct answers out of eight, compared to 5.2 of non-owners).[49]

The survey also sought to understand Canadians' levels of trust in cryptocurrency exchanges to offer secure and responsible technology, compared with other types of businesses and public institutions. The findings were revealing. Across the full sample of respondents, about half (49%) reported "low trust" in cryptocurrency exchanges, far higher levels than for all other categories. While crypto-asset owners did report 'high trust' in exchanges more than the general population, a greater proportion of owners still reported 'neutral' (43%) or 'low trust' (27%). It is important to note that these survey responses were collected *before* the FTX collapse and other related crypto events in late 2022, which presumably has further eroded trust in crypto exchanges and markets. The FTX failure also reportedly resulted in financial losses for an estimated 30,000 Canadian users and numerous businesses.[50]

Figure 1

Canadians Trust in Offering Secure and Responsible Technology



4 Cyber and Sociotechnical Security and Crypto-asset Trading

Alongside the interest, investment and general exuberance about crypto-assets have emerged countless reports of its harms — some dating back years, and others entirely new. Financial scams, frauds and reckless speculation; criminal hacks on blockchains and crypto exchanges compromising funds or personal information; illicit uses of crypto, for dark web purchases or ransomware payments; or devastating environmental impacts of crypto mining, to name a few. These have typically been regarded as challenges to be dealt with by financial regulators, law enforcement, or the market letting the chips fall where they may. But this neglects the uniquely technology-enabled nature of these challenges with blockchain and crypto-asset trading.

The focus of this report, this section will assess these technology-enabled risks, assessing two categories of risks and potential harms associated with blockchain technology and crypto-asset trading. The first category is **cyber security**, which relates to technical risks, threats and vulnerabilities related to the blockchain or a specific application: at the blockchain protocol level, the hardware or software supporting the application or platform, or a third-party application like a crypto wallet. This more traditional lens of cyber risk analysis focuses on threats of attacks or hacks with expressly malicious intent, such as financial theft, data breach, and others.

The second category, **sociotechnical security (STsec)**, offers a new analytic framework. Introduced by US-based security scholars Goerzin, Watkins and Lim, this lens of inquiry reflects a perspective that "social systems and technological systems [are] interdependent and co-constituted."[51] They use the terminology of risk (of loss or harm), threat (of negative event) and vulnerability (to a threat) from the cyber security domain, but also other disciplines including policy, psychology, behavioural economics, sociology and law. The STsec framework, and its application in this report, will be described in greater detail in the section below.

The Cyber Security Lens

Dating back to the early days of crypto-assets, the cyber security of exchanges and trading services has been a significant area of risk for users and other crypto market participants. In 2011, the first major Bitcoin exchange, Mt. Gox, was hit with a cyber attack that resulted in the theft of Bitcoin valued at USD$400,000 from nearly 500 user accounts. The Mt. Gox exchange failed in 2014 when another hack resulted in a vastly larger theft of 850,000 Bitcoins, valued today in the billions of dollars.[52] The relatively short history of crypto-assets has been littered with examples of cyber attacks, targeting various threat surfaces, with motivations ranging from financial gain and data theft to harassment of users and hacker prestige.

Our research found a large number and variety of cryptocurrency-related cyber attacks documented in the literature, media, and through other sources. The malicious aims of these attacks included, for instance, denying service to certain users, double-spending coins, or profiting from the creation of fraudulent refunds or invalid transactions.[53] While they reflect a diversity of threat actors, motivations, targets, exploits and impacts or harms, there are commonalities across many of the attacks and related risks. Rather than comprehensively listing them all, the cyber threats are grouped by their common targets, which are blockchain networks, crypto-asset exchanges, individual users, and third-party applications. Each is described below with examples, and a short summary.

Experts identify **blockchain networks** as a common target for technical cyber exploits. Vulnerabilities sometimes relate to outdated software common to digital systems, but in other instances to unique blockchain-specific attributes.[54] For example, hackers have identified vulnerabilities in code written into smart contracts that have allowed for theft of crypto-assets and, in some cases, larger ramifications like bankruptcy of organizations.[55] Spam attacks seek to disrupt or slow transactions on the network. Cryptoanalysis advances by malicious actors have identified exploits in broken primitives (the low-level algorithms such as one-way hash functions),[56] compromising the security and authenticity of data and transactions on the blockchain. A number of types of attacks target technical or protocol vulnerabilities in mining and consensus processes (e.g., pitchfork, 51% or Vector 76 attacks) , usually to enable cybercriminal theft from exchanges and users.[57]

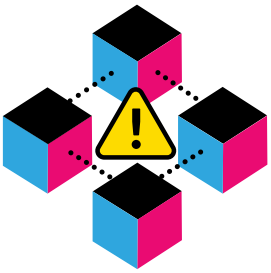
Crypto exchange mobile applications have been found to have insecure data storage, communication, authentication and authorization, insufficient cryptography, and poor code quality.

Crypto-asset exchanges have been targeted by threat actors, resulting in lost currency, stolen assets, data breaches or misuse, and other criminal activity.[58] Crypto exchange mobile applications have been found to have insecure data storage, communication, authentication and authorization, insufficient cryptography, and poor code quality.[59] In another example, North Korean state-sponsored criminal actors have used modified cryptocurrency trading applications to pose as legitimate trading platforms in order to deceive users for financial theft.[60]

Third-party crypto applications are another target. For example, there have been attacks on crypto wallets that enable trading on exchanges or peer-to-peer platforms, typically with the aim of financial theft or compromise of user data.[61] Deanonymization attacks seek to connect the wallet with a user IP address to surveil their transaction activity. Experts highlight vulnerabilities with the various types of wallets: hacks on hardware wallets that virtually safeguard assets, the (non-cyber) risk of destruction or loss of "paper" wallets, or the compromise of cloud service providers hosting cloud-based wallets.[62]

Another set of threats target **individual crypto users** directly. One type of attack, called Crypto Jacking, seeks to covertly infiltrate a user's device in order to steal computing power for crypto mining. Other threat actors seek to steal user data, either for direct benefit, or to target users with other types of threats or scams. Experts note that threat actors have been able to link users' pseudonymous signatures on the public blockchain to personal identity information, allowing for surveillance, abuse and misuse by cybercriminals and other threat actors.[63] Cyber attacks exploiting *technical* vulnerabilities to gain access to users often enable scams, frauds, or other types of social engineering attacks that blend technical and human interaction, and are explored in the next section on sociotechnical security.

Summary of Types of Cyber Security Threats and Attacks

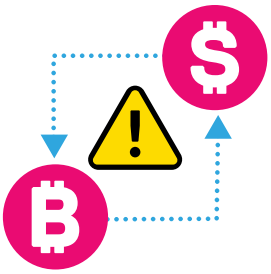


Threats targeting blockchain networks

Attackers exploit vulnerabilities with the decentralized network or 'proof of work' consensus mechanism, seeking to influence the verification of transactions with the aim of reversing transactions, denial of service (DoS) to specific participants, and other malicious purposes.

Example:

51% attack: Groups of attackers gain "majority" control of consensus mechanisms, for the malicious purposes of reversing transactions to allow double spending of coins or denying service to certain users.[64]

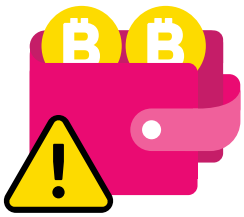


Threats targeting crypto-asset exchanges

Attackers target the software, hardware, mobile applications or other attack surfaces of crypto-asset exchanges, motivated by cryptocurrency or data theft, or other malicious aims.

Example:

DDoS attack: When an attacker attacks the platform, it affects the availability of the platform, leading to a decrease in the number of transactions that can be made.[65]



Threats targeting 3rd party applications

These attacks take advantage of vulnerabilities created by the use of a 3rd party wallet as a tool for cryptocurrency trading, and linked addresses, leading to user privacy violation.

Example:

Deanonymization attacks: The attacker links IP addresses with a Bitcoin wallet to listen to transaction traffic, violating user privacy and potential further targeting.[66]

Threats targeting individual crypto users

These threats target users directly, seeking to gain access to their devices or their identity information, in order to victimize them directly or conduct scams and frauds.

Example:

Crypto jacking attack: The threat actor uses malicious JavaScript code to infiltrate a user's device in order to covertly mine cryptocurrency without the user's consent or knowledge.[67]

The Sociotechnical Security Lens

As introduced earlier, the sociotechnical security lens of inquiry developed by Goerzen, Watkins and Lim, extends the cyber security frame of analysis, recognizing that "vulnerabilities are either primarily technical or social in nature, and when combined by threat actors, constitute uniquely sociotechnical exploits."[68] The sociotechnical security lens is described to "not only to edge out the vulnerabilities in code, but also the vulnerabilities in the social systems that design, inform, and use the code or its applications - with the pointed goal of securing individuals and communities, with regards to their situated evaluation of harms."[69] This framework is useful when analyzing information and communication technologies that are increasingly participatory in nature, because the lens helps to identify (and address) emergent types of harms that are enabled by sociotechnical systems, such as the dissemination of false information, harassment, or at times even physical attacks. This section begins by exploring the sociotechnical security (STsec) lens, and then examines five areas of risks and threats related to crypto-asset trading.

The STsec Framework

Sociotechnical security focuses on the interdependencies and entangled interactions of technical and social conditions, using terminology such as exploit, threat and vulnerability from the cyber security domain.[70] It recognizes that certain social and technical conditions may enable actions that are desirable in some scenarios, but these same conditions may demonstrate substantial capacity for harm or abuse by threat actors in another context. In this primer, it is a useful framework to analyze emergent harms enabled by blockchain technology and crypto-asset trading.

In adapting their framework to crypto-asset trading for this report, two "tests" are applied in determining whether an issue should be analyzed through the STsec lens:

1. A sociotechnical security risk must result from not just a technical vulnerability, but from the *interdependencies and entangled interactions* of technical and social conditions. Or, put another way, from how humans interact with the technology.

2. While cyber risks are typically understood as purely harmful to the developers and users of a technology, *STsec risks are more ambiguous*. The interaction of technical and social conditions may be desirable in some scenarios or for certain people, but these same conditions may demonstrate substantial capacity for harm or abuse in another context or from another perspective. Take, for example, the 'immutability' attribute of blockchain technology. Where this characteristic can be perceived as beneficial (for transparency and security of records), it can also be exploited in other scenarios (if a transaction is fraudulently completed and can not be reversed).

Four Categories of STsec Harms and Threats

This section outlines four categories of existing or emergent STsec harms and threats associated with blockchain technology and crypto-asset trading that emerged from the research scan. We note that these categories are imperfect and fluid, with many examples below clearly affected by multiple technical or social factors.

1. User Anonymity, Privacy and Harassment

The first STsec category relates to the interactions of crypto users and threat actors with unique public blockchain technology attributes that blend user anonymity (or pseudonymity) with transparency. The blockchain design sought to offer users the privacy of not revealing personal identities in crypto trading, while also ensuring transaction records are irreversible and unalterable on the public ledger to protect against challenges such as the double-spending of coins, fraudulent transactions and tampering, or reversing crypto-asset transactions. The benefits have been touted for crypto trading and other use cases (e.g., verifying the accuracy of real estate records), but research also highlights a number of real or potential harms that have resulted.

Users risk having their privacy or personal identity information compromised. As noted in the cyber security section, tracking and identity compromise can open users up to other types of threats, including scams and frauds employing social engineering tactics (explored further below). Where crypto-assets are stolen through fraud or coercive transactions, the immutable record has typically left users with no recourse to reverse transactions as they would with a bank (though there are exceptions).[71] Other types of risks relate to unwanted monitoring leading to traceability, harassment and abuse. Researchers highlight real or potential examples of user privacy exploitation including algorithm-based marketing, prospective employers, or snooping Tinder dates.[72] Others pose much more severe risks to user safety and security. Scholars have identified cases involving intimate partners or estranged family members, where sensitive data like financial and transactional information allows for potential tracking to enable online harassment and extortion, or physical violence and other threats to personal safety.[73]

Nearly one in five (19%) Canadian crypto owners report having been targeted with online harassment that caused them to fear for their safety.

Crypto-related harassment is common, with the survey of Canadian crypto owners finding that nearly one in five (19%) report having been targeted with online harassment that caused them to fear for their safety, compared to 6% of those who have not owned crypto. Threats in cyberspace have also migrated to the offline world. Examples include "swatting" (a hoax call to law enforcement), crypto muggings, extortion, and armed robberies. Some attacks have targeted well-known actors in the crypto trading realm. Engineers and developers with crypto companies have been victimized by swatting, while armed robbers have attacked crypto experts.[74] Other attacks are more opportunistic. In London, UK, crypto muggings have been frequently reported, with attackers using the threat of violence to take victims' phones and transfer cryptocurrency to their accounts.[75] Law enforcement have begun to investigate and respond to these attacks, with rare cases of successful tracing and retrieval of stolen crypto-assets.[76] Still, users generally recognize that they are largely responsible for protecting their assets and personal safety.

Conversely, the privacy afforded users through anonymity (or pseudonymity) in transacting crypto has been widely exploited to enable criminal activities and other types of harms through crypto trading, particularly in an environment where regulation of crypto-assets has been in early stages of development. It has also been a significant enabler of money laundering and other criminal activities such as ransomware payments. For instance, the U.S. Department of Treasury recently sanctioned a cryptocurrency market intermediary, a cryptocurrency mixer called Tornado Cash that allowed users to move tokens anonymously, as it was found to be obscuring the identities of criminal actors, including some aiding in North Korea's money laundering efforts.[77]

2. Financial Scams and Fraud

The blockchain's design features for transaction verification sought to enable a decentralized system for peer-to-peer interactions. The perceived benefit was distributed trust, authority and autonomy for users in transacting crypto-assets and the management of records and data, while also reducing or eliminating reliance on traditional financial institutions as the centralized authorities for the verifying, clearing and recording financial transactions. Yet, researchers have found that these technical attributes create the conditions for malicious actors to exploit users in various ways, with evidence of widespread financial scams and fraud.

The peer-to-peer dynamic creates the conditions for users to be targeted by scams or other forms of deception. For instance, media reports describe the initiation of scams through online engagements or the formation of 'friendships' through anonymous crypto chats.[78] Users have been deceived into investing through fraudulent crypto-asset exchanges or trading platforms, with assets then stolen by the scammer. Other examples include investment, romance, and business and government impersonation scams, using common types of social engineering exploits like phishing attacks that lure users with narratives of wealth and sophistication, or impersonation of banks, border patrol agents and other authorities.[79]

One in three Canadians (35%) that reported purchasing crypto reported at least one experience of fraud, scam or criminal activity.

Figure 2

Fraud or Scam Experiences Reported by Crypto-asset Purchasers

A person claiming to be an experienced crypto-asset investment manager stole the fee for using their services	14%
The price of a crypto-asset I purchased was artificially inflated through false information	11%
I shared my crypto-asset wallet information through a request for information (e.g., by email or text) that turned out to be a scam	10%
I was encouraged to recruit new investors for a crypto-asset exchange in exchange for money	8%
I purchased a crypto-asset and lost my funds from a person who later disappeared	7%
A crypto-asset exchange stole my funds	4%
Any of the above	35%

The survey undertaken for this report found that one in three Canadians (35%) that reported purchasing crypto reported at least one experience of fraud, scam or criminal activity. As summarized in Figure 2, common experiences included fraudulent crypto investment advisors, artificial inflation of assets, or scams seeking access to crypto wallets. Survey showed that negative experiences were most common among crypto purchasers with lower incomes (reported by 51% with less than $50,000 household income) and less education (reported by 78% with high school or less), illustrating some disparity across demographic groups.

When users fall prey to these cryptocurrency scams, significant financial loss can result, sometimes compromising large amounts of money from lines of credit, credit cards, and life savings.[80] Not only are there financial losses, but also the risk of personal and financial information being stolen.[81] The scale of these types of fraud and scams seems substantial in Canada. The Canadian Anti-Fraud Centre, a public body that is a partnership of the Royal Canadian Mounted Police and other authorities, recently reported a "staggering" total of over $500 million in reported losses from fraud in 2022, with crypto fraud as the top category.[82]

3. High-Risk Behaviour, Misinformation and Deceptive Promotion

Though understanding of the social dynamics of crypto-asset user communities is still limited, expert analysis, media coverage and social platform activity have all highlighted a brash, risk-taking crypto culture among market participants. Advocates, often expressing a countercultural ethos, see a new technology that enabled a decentralized form of exchange, offering user autonomy, profitable investment opportunity, and freedom from the shackles of traditional financial services. It has also created ripe conditions for speculative hype and wild volatility in cryptocurrency markets often resulting in significant financial loss for users.

One set of risks relates to direct financial loss from speculative or imprudent crypto trading behaviour. Some risks are relatively banal but can result in substantial loss of crypto assets, such as the loss of a user's private keys through personal error and misplacement.[83] Others relate to investment motivations and approaches, with research finding that users can be prone to extreme, emotional reactions, and volatile decisions when trading crypto-assets.[84] The psychological tendency to be attracted to risk can result in large and imprudent buy and sell orders.[85] This high-risk and emotionally-charged investment attitude has made users particularly vulnerable to misinformation and various forms of deceptive promotion.

Numerous examples of "pump-and-dump" schemes have repurposed a time-worn financial grift to the new crypto marketplace. Malicious actors artificially inflate the price of an asset through misleading statements (pump),[86] followed by a rapid sell-off (dump) of the asset to profit at the expense of the deceived purchasers.[87] In the "rug pull" version of the scheme, a crypto-asset developer anonymously promotes the asset with buyers to inflate the price, then rapidly sells tokens leading to a project's failure and significant financial loss for buyers.[88] Other versions have reportedly been carried out by celebrities and public influencers, with U.S. regulators charging Kim Kardashian and the boxer Floyd Mayweather Jr. and reaching significant financial settlements with both.[89]

Crypto exchanges and lending companies have deceptively promoted high or guaranteed investment returns with low risks. A high profile example in 2022 was the failure of the Luna crypto network, which deceptively promoted the TerraUSD algorithmic stablecoin as a safe haven for investors, and then crashed wiping out an estimated $60 billion in investor value.[90] A Wall Street Journal study found that almost a quarter of digital coin offerings have disclosure or transparency problems.[91] Other high profile recent cases resulting in enormous financial losses to users, like the collapse of the FTX exchange, have combined misleading promotion with outright financial mismanagement, governance failure, lax investor and regulatory oversight, and alleged criminal fraud.[92]

Other studies have explored how claims of the decentralization and consensus attributes promoted to users are actually deceptive. Cyber security scholar Bruce Schneier and others have reported on cases where small numbers of intermediaries (i.e., small mining pools) have disproportionate authority and control over blockchains.[93] A study by researchers at Cornell University found that over 50% of the mining power was distributed among eight miners in Bitcoin, and only five in Ethereum.[94] This creates risks around cyber security, privacy and data protection, as well as concerns about the transparency and accountability for crypto users.[95]

4. Externalities and Systemic Threats

The final category to assess through the STsec lens relates to higher order risks to society, the economy and critical institutions associated with blockchain and crypto-asset trading. Bitcoin and the blockchain have introduced not just a new technology and alternative digital currencies, but a philosophy and movement towards decentralized internet (sometimes called "Web3") backed by an enormous amount of ambition and investment among technologists and users alike, whether motivated by profit or a fundamental desire to transform or disrupt financial and monetary systems, governments and state power, or individual identities and forms of virtual interaction.[96] This philosophy is highly contested, however, and brings with it not just perceived threats to existing systems and institutions, but real negative externalities. While these higher order considerations are largely beyond the scope of this report and require further analysis, two examples will be briefly explored.

The first are the environmental externalities of blockchain verification methods. The Proof-of-Work (PoW) consensus mechanism enabled trusted verification of transactions while also providing a significant financial incentive for users to contribute computing power ("mining") to the crypto community and become users of cryptocurrency. While many financially benefit, it has resulted in enormous increases in energy usage with significant consequences for environmental pollution and human health.[97] The greenhouse gas (GhG) emissions and potential demands on electricity systems risk undermining progress on climate action.[98] Prior to Ethereum's recent shift to a proof-of-stake consensus mechanism, the computational demands of the PoW mining consumed nearly the same amount of energy as the Republic of Ireland.[99] In Canada, there has been increasing interest from cryptocurrency miners to operate — with Quebec and Manitoba seeing the highest number of requests for electricity supply due to its relatively cheap costs.[100]

The second example is the perceived threats that digital currencies pose to the financial system. As far back as 2018, the head of the Bank for International Settlements, a prominent global financial body, argued that cryptocurrency cannot be allowed to undermine trust in central banks and the financial system, suggesting that they do not meet the basic definition of a currency.[101] More recently the International Monetary Fund (IMF) called for stronger financial regulation and supervision of crypto-assets in response to the recent collapse in market value. The Fund noted that "crypto assets, including stablecoins, are not yet risks to the global financial system," but some developing economies are already materially affected by "cryptoization" where digital assets are substituted for domestic currency and circumvent foreign exchange and monetary policy controls.[102] Both cases offer examples of STsec threats whose implications are of a scale and complexity far greater than the use cases or examples described in previous categories.

Summary of Categories of STsec Threats

User Anonymity, Privacy and Harassment

Interactions of crypto users and threat actors with blockchain technology attributes that blend user anonymity (or pseudonymity) with transparency and immutability, resulting in real or potential threats of user privacy compromise, online and offline harassment, and exploitation by criminal actors.

Example:

Swatting: Malicious actors harass a user by gaining access to their address and calling 911 to falsely report a serious crime to attract law enforcement (the "SWAT" team) to their home.

Financial Scams and Fraud

The blockchain's attributes that enable decentralized networks for peer-to-peer interactions create the conditions for malicious actors to exploit users in various ways, including social engineering attacks and financial scams and fraud.

Example:

Phishing: An attacker sends an email or text message request for information about another user's crypto-asset wallet in order to gain access and enable theft of crypto-assets.[103]

High-Risk Behaviour, Misinformation and Deceptive Promotion

The risk-taking crypto culture creates conditions for speculation and volatility in cryptocurrency markets, informed by misinformation and deceptive promotion, resulting in financial loss for users.

Example:

Pump-and-Dump Schemes: A malicious actor (sometimes high profile influencers) seeks to inflate the price of an asset and invite buyers, only to sell assets quickly to gain profit.[104]

Externalities and Systemic Threats

Higher order externalities and systemic implications of blockchain and crypto-asset trading for society, the economy and critical institutions, largely beyond the scope of this report and requiring further analysis.

Example:

Environmental Externalities: Environmental externalities of blockchain verification through Proof-of-Work consensus, which financially benefit many but demand enormous energy consumption with significant consequences for environmental pollution and human health.

5 The Policy Landscape: A Security Lens on Crypto-asset Regulation

In recent years, efforts at regulation and industry standards-setting for crypto-asset markets, exchanges and firms have become a major priority for policymakers, regulators and the financial services industry. The collapse of major crypto exchanges and platforms in 2022, and the resulting billions of dollars lost, has only amplified urgency for governments and transnational bodies to establish regulatory regimes. Crypto market integrity firms like Elliptic, Chainalysis, and Ciphertrace have emerged to support regulators and financial institutions with detection and prevention of financial crime and compliance violations. There have been significant enforcement actions in Canada and worldwide related to crypto financial crime, with significant seizures or recovery of illicit assets.[105]

To date, however, regulatory initiatives in Canada and other major jurisdictions have focused primarily on cryptocurrency and digital assets through a financial services lens. There has been less policy attention on the cyber and sociotechnical security of blockchain technology and crypto-asset trading explored in this report. This section provides a scan of the crypto-asset regulatory landscape *through this security lens*, focusing on cyber security policy specifically for crypto-assets and financial regulatory policy where it seeks to address the cyber and sociotechnical security threats surveyed in the previous section. It surveys the policy landscape in Canada and two other jurisdictions of particular relevance for Canadian policymakers — the European Union and United States — as well as security-related industry standard-setting that is emerging for blockchain and distributed ledger technologies.

Canada

To date, regulatory oversight of crypto-assets in Canada has largely been under securities legislation. Provincial securities regulators — and collectively under the Canadian Securities Administrators (CSA) — were relatively early movers in pursuing actions with crypto-asset exchanges, due in part to the collapse of Quadriga, then Canada's largest exchange, and the shocking revelations of mismanagement that followed.[106] Other key actors in Canada's policy landscape for crypto-asset trading include the Self-Regulatory Organization of Canada (formerly IIROC, the Investment Industry Regulatory Organization of Canada) that oversees investment dealers and trading activity in Canada, the Bank of Canada, the federal Department of Finance, provincial finance ministries, Financial Consumer Agency of Canada (FCAC), Office of the Superintendent of Financial Institutions (OFSI), the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), and other federal agencies who have proactively monitored risks posed by crypto-asset activities.[107]

Cryptocurrencies are not deemed a legal tender in Canada,[108] and there has been policy uncertainty across jurisdictions about whether crypto-assets should be treated as securities or derivatives for regulatory purposes.[109] Yet, CSA Staff Notices dating back to 2017 have provided regulatory guidance regarding the trading of crypto-assets on centralized platforms, applying traditional investment dealer, marketplace and clearing rules in a hybrid fashion.[110] For crypto-asset trading platforms (CTPs), requirements have included registration with IIROC, a focus on disclosure and reporting of assets, advertising and marketing, reporting suspicious transactions, and 'Know-Your-Client' (KYC) verification requirements to enforce anti-money laundering (AML) provisions.[111] Regulatory sandboxes have also been introduced by the CSA and Alberta government to encourage innovation and development of the technology.[112] Dr. Ryan Clements' comprehensive expert report for the national Public Order Emergency Commission provides an authoritative assessment of the crypto-asset financial regulatory landscape.[113]

Through the security lens, key federal institutions for cyber security, such as lead department Public Safety Canada and the Canadian Centre for Cyber Security (CCCS) within Canada's national cyber intelligence agency, do not appear to have established policies or programs specifically aimed at addressing cyber risk associated with cryptocurrency and trading. CCCS ransomware awareness briefs address cryptocurrency as a common form of payment, and the 2018 National Cyber Threat Assessment identified unauthorized crypto mining as a threat and digital currency as an AML risk.[114] The most recent National Cyber Threat Assessment for 2023-2024 likewise acknowledges the ways in which decentralized finance and related tools (e.g., privacy coins, mixers) are used to facilitate crime by users and state actors.[115]

The most recent National Cyber Threat Assessment for 2023-2024 likewise acknowledges the ways in which decentralized finance and related tools (e.g., privacy coins, mixers) are used to facilitate crime by users and state actors.

Still, numerous areas of current and emerging financial policy intersect with the cyber and sociotechnical security risks identified in this paper. This is particularly the case for financial fraud and scams, deceptive promotion, financial consumer protection and increasing user awareness of the financial risks of crypto trading and the range of hacks and social engineering threats targeting users. For example, the application of KYC and AML provisions will require greater scrutiny of malicious actors using crypto for criminal purposes. In early 2023, the CSA announced further strengthening of crypto trading platform investor protection commitments in the wake of the insolvencies and market turmoil in late 2022.[116] The FCAC Financial Consumer Protection Framework, released in June 2022, set out strengthened or new requirements relating to crypto, such as notification and information sharing requirements for regulated entities offering crypto-assets.[117] The FCAC has also released an informative page on digital currency, with basic definitions, risks, and general tips for using digital currency.[118] There have also been initial steps to address environmental externalities, such as Hydro-Québec's imposition of energy restrictions on crypto miners.[119]

Other emerging policy initiatives offer the potential to incorporate cyber and STsec lenses. In Fall 2022, Finance Canada announced a public consultation on the digitization of money, focused on ensuring financial sector stability and security, and minimizing use of crypto-assets for illegal activities.[120] The Bank of Canada has been conducting initial exploration of a Central Bank Digital Currency (or CBDC), in response to the changing digital society but also concern about systemic risks, and trust and security of money, with cryptocurrency. In 2021, the Ontario government was considering new legislation, called the *Capital Markets Act*, that would provide the provincial securities regulator greater discretion and authority to enforce rules over cryptocurrency, which reportedly received considerable pushback from crypto companies including Wealthsimple, Shakepay and Dapper Labs.[121] Provincial securities regulators across the country have been stepping up public awareness campaigns to warn about crypto fraud, focusing on social engineering-type tactics, use of social media platforms, and targeting of vulnerable population groups.[122]

There is another important point of intersection for addressing crypto security-related issues with other foundational technology policy legislative initiatives, including the Consumer Privacy Protection Act (Bill C-27) and related provincial laws, the cyber security act (Bill C-26) that is focused on critical industries including financial services, and the forthcoming online safety bill for regulating large social media platforms. While crypto-asset trading is not central to any of them, there are opportunities for alignment with the financial and other policymaking efforts.

The European Union

The European Union appears to be the most advanced jurisdiction in developing policy regimes that directly assess both crypto-assets and trading, and the digital technology and cyber security related risks. In 2020, the European Commission announced a package of digital finance initiatives to address crypto-asset regulation, digital security, and regulatory innovation for blockchain.[123] A first element, the Markets in Crypto Asset (MiCA) regulation, is among the most comprehensive regulatory frameworks covering crypto-assets and their issuers and service providers. MiCA, to be voted on in 2023, builds on the EU's financial directive from 2014, which covered virtually all aspects of financial investment and trading.[124] Key financial sector actors include the European Securities and Markets Authority (ESMA), European Banking Authority (EBA), the Financial Stability Board, the European System of Central Banks (ESCB), and crypto-asset service providers (CASPs).[125]

MiCA's broad aims are protecting investors, preserving financial stability, and enabling the use of innovative technology, covering market abuses related to transactions or services, setting guidelines for crypto-asset service providers, and addressing the environmental and climate footprint of actors in crypto-asset markets. Specific provisions relating to STsec risks aim to limit deceptive promotion and protect consumers by requiring crypto service providers to share accurate, transparent, and fair information with clients, and provide warnings about crypto trading risks.[126] Entities offering services under MiCA would be required to follow existing EU anti-money laundering regulations.[127] To address environmental impacts, ESMA and EBA would develop technical regulatory standards tied to sustainability indicators for crypto mining and various types of consensus mechanisms.[128]

Related legislation, the Digital Operational Resilience Act (DORA), which takes effect in 2025, focuses on financial sector ICT requirements for the security of network and information systems of companies and third-party organizations.[129] The requirements set out in DORA are applicable to all financial institutions, including crypto-asset service providers and issuers of asset-referenced tokens. Areas mentioned in DORA include ICT risk management, ICT-related incident reporting, updating ICT systems, and encouraging the exchanging of cyber threat information and intelligence among financial entities.[130]

A third initiative, called the Distributed Ledger Technology (DLT) Pilot Regime Regulation, is designed to develop and test crypto-assets and market infrastructures based on blockchains. Taking effect in March 2023, it allows for temporary exemption of certain DLT market infrastructures from financial services legislation that could hinder the development of the technology, requiring these DLT market infrastructures and operators to have safeguards protecting investors and clients. The ESMA and other authorities will also be able to draw lessons from the pilot regime related to risks and opportunities from crypto-assets that qualify as financial instruments, to aid in refining legal regulations for DLT financial instruments.[131]

The United States

In 2022, the Biden Administration released the country's first comprehensive crypto-assets policy guidance, through a Presidential Executive Order called the Framework for Responsible Development of Digital Assets.[132] The Framework focuses on consumer and investor protection, promoting financial stability, countering illicit finance, the country's leadership in the global financial system, financial inclusion, and responsible innovation across various federal agencies. In the United States, key federal regulatory and oversight bodies for crypto-assets include the Securities and Exchange Commission (SEC), Commodity Futures Trading Commission (CFTC), Federal Trade Commission, Department of the Treasury, Internal Revenue Service (IRS), Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency (OCC), and Financial Crimes Enforcement Network (FinCEN).[133]

Specific actionable elements of the Framework that directly or indirectly address cyber and sociotechnical security include direction to:

- the Treasury Department to work with financial institutions to address cyber vulnerabilities, and analyze strategic risks with digital asset markets;
- the Financial Literacy Education Commission (FLEC) to lead awareness-raising efforts for consumer protection related to digital assets;
- the US Federal Reserve to assess benefits, consequences, and potential future use of a central bank digital currency (CBDC);
- the Department of Commerce to assess the establishment of an expert forum to coordinate and consult on federal regulation, standards, and research for digital assets;
- the National Science Foundation (NSF) to support research to support the design of usable, inclusive, equitable, and accessible digital asset ecosystems; and
- establish tracking of digital assets' environmental impacts.

Importantly, while the Executive Order directs activity through the federal government, the Framework does not have the permanence of law. Consequently, there is regulatory uncertainty in the United States, with little success to date in passing legislative initiatives for crypto-assets and related technology policy [...]

Importantly, while the Executive Order directs activity through the federal government, the Framework does not have the permanence of law. Consequently, there is regulatory uncertainty in the United States, with little success to date in passing legislative initiatives for crypto-assets and related technology policy such as consumer privacy and data protection. For instance, two bills that were not passed by the last Congress — the Digital Commodities Consumer Protection Act of 2022 and the (Lummis-Gillibrand) Responsible Financial Innovation Act — both sought to enhance consumer protections, with the latter proposing cyber security standards for digital asset intermediaries.[134] Another legislative proposal aimed at protecting consumers and markets by classifying and setting regulatory provisions for stablecoins also failed to pass.[135]

There are other ongoing federal initiatives of note. The SEC has been active and growing in their pursuit of enforcement actions related to fraudulent and unregistered crypto-asset offerings and platforms, levying significant fines in high profile pump-and-dump and other deceptive promotion cases.[136] In early 2023, federal agencies joined forces in issuing a statement to the financial sector warning of liquidity risks resulting from crypto-asset market vulnerabilities.[137] An illicit finance risk assessment on decentralized finance was expected to be completed by early 2023, with an assessment of non-fungible tokens to follow in July 2023.[138]

As in Canada, state governments play an important policymaking and regulatory role with crypto-assets. In the majority of the states (37), legislation to regulate 'digital assets' has been proposed, though not always passed.[139] These state bills have addressed general issues such as crypto-assets definitions, tax treatment, and licensing and registration; as well as issues that intersect more directly with security issues, such as consumer protections, disclosure rules to limit deceptive advertisements, specific crypto-related offenses such as money laundering, virtual token fraud, illegal rug pull scams, and other forms of fraud, and environmental impact assessments and moratoriums on proof of work authentication. However, research finds that only a handful of states, including Connecticut, Missouri, and New York, have taken meaningful legislative steps to address consumer protection and digital asset-related offenses.[140] The state of Wyoming has introduced the most legislative measures to date for digital assets, including a special purpose depository framework for crypto-assets, establishing a select committee on blockchain, technology and innovation, and a regulatory sandbox.[141]

Industry Initiatives and Standard-Setting

Beyond state-led actions, industry groups and standard-setting bodies have been playing an important role in establishing national and transnational rules and technical guidance for distributed ledger technologies (DLT) and crypto-assets, including for addressing security vulnerabilities. Some initiatives have focused on the financial regulatory side. The Financial Stability Board (FSB), a body that oversees the global financial system, has been proactively monitoring the decentralized finance (DeFi) ecosystem supporting the international regulatory activities for crypto-assets.[142] The summary report of the February 2023 G20 summit, held in India, identified a series of ongoing crypto market analysis and policy coordination initiatives of the FSB, International Monetary Fund (IMF), and Bank for International Settlements (BIS).[143]

A number of other initiatives focus on standard-making for blockchain and its security. The most prominent is the International Standards Organization (ISO) standards for Blockchain and distributed ledger technologies (ISO/TC 307). It covers, for example, technical standards for security management of digital asset custodians, governance guidelines, and identity management.[144] The technical committee leading this work is developing on other standards for blockchain and DLT, such as smart contracts and security practices. Other examples include the Institute of Electrical and Electronics Engineers (IEEE) Blockchain Initiative and the International Electrotechnical Commission (IEC)'s working group on the integration of IoT and DLT/blockchain use cases.

In Canada, the Digital Governance Council, a membership-based body representing technology leaders with governments and large companies, is developing standards for the design and operation of digital assets and non-fungible tokens, among many other standards for the digital economy.[145] Other national or regional standards-making bodies, such as the European Telecommunications Standards Institute (ETSI), British Standards Institution (BSI) and Standards Australia, have been both contributing to ISO standards and developing their own blockchain-related standards proposals and committees.[146] A recent white paper by the World Economic Forum mapped the numerous examples of blockchain standards development initiatives globally, and their alignment to cyber security as well as other issues like interoperability, governance, internet of things, and technical taxonomies and terminologies.[147]

6 Findings and Policy Recommendations

This report offers policymakers and policy-focused industry leaders and technologists in Canada and beyond a new perspective on blockchain-based crypto-asset trading, assessing the cyber security risks and threats as well as through an emergent sociotechnical security lens that focuses on the interactions between technological and human dynamics. The first section offers readers a basic primer on blockchain and crypto-asset trading, with design features (e.g., peer-to-peer networks, transparency and immutability, user pseudonymity) that address certain challenges but give rise to others. It also offers novel new insights from national survey research about the demographic profile of crypto users in Canada, levels of public trust in crypto asset platforms (very low), and the types of harms that purchasers of crypto-assets report experiencing (most often related to financial fraud or loss and harassment).

Security was assessed through two lenses. The first is more traditional **cyber security** — the technical threats and vulnerabilities related to blockchain or specific applications, typically targeted by purely malicious actors. The research identifies four categories of risk to the blockchain network, the crypto exchange, 3rd party services like crypto wallets, and to users directly, with numerous examples of cyber attacks and hacks exploiting technical vulnerabilities for financial theft, data breach, and other criminal purposes. The second lens is **sociotechnical security**, which uses the terminology of cyber security but captures risks that reflect the interdependencies and entangled interactions of technology and social conditions. Here the research and numerous use cases from media and other sources were synthesized into four more categories: user anonymity, privacy and harassment; financial scams and fraud; high-risk behaviour, misinformation and deceptive promotion; and externalities and systemic threats.

The last section scanned the policy landscape for crypto regulation through a security lens related to the findings above. The key finding is that there has been significant financial regulatory action in Canada for crypto-asset trading, primarily in the application and enforcement of securities law, which is also having the effect of addressing certain cyber and STsec risks. There has, however, been little direct policy initiative related to cyber security for crypto-assets, and Canada can learn from jurisdictions like the EU that are introducing more integrated regulatory packages for both crypto-assets and distributed ledger technologies (DLTs), or the U.S. with a comprehensive Framework for digital assets directing federal government efforts. Standards-setting initiatives for DLTs and crypto offer potential to address security risks as well.

For policymakers and other stakeholders, the report offers the following recommendations:

1. **Conduct further research on the security threats and harms associated with crypto-asset trading, and increase public engagement with communities of crypto users to inform policymaking.** This report offers an initial effort building on existing academic literature, media reporting and other sources. But policymakers and market actors would benefit from deeper analysis of cyber and STsec threats, solutions in policy and regulation or technology design and standards, and deeper understanding of the motivations and behaviours of crypto users and threats to marginalized and other communities. As there are unique cultural dynamics, attitudes and communities among crypto-asset users, entrepreneurs and technologists in Canada, engagement with these groups is important in informing the development of policy for crypto-asset markets and security.

2. **Ensure crypto-asset policymaking is timely and iterative, to allow for innovation in blockchain and fintech while assuring market integrity, security and consumer protection.** While this report focuses on security risks and real or potential harms, policymaking should not discount the potential value of DLT and digital assets and the perspectives of Canadian crypto-asset industry and user communities. The aim should be to strike the right balance.

3. **Enhance public transparency and cyber security-aligned consumer protection requirements for crypto-asset investors and users.** The recent collapse of FTX and other crypto-asset platforms resulted from interrelated factors including financial transparency and disclosure gaps, deceptive promotion, and a risk-taking culture among investors. This calls for continued efforts to increase financial disclosure requirements and limit deceptive promotion of crypto-assets, increased financial consumer protection by FCAC and others, and alignment of these activities with cyber security awareness efforts through bodies like the Canadian Centre for Cyber Security.

4. **Align financial regulation of crypto-assets with other Canadian policy and legal regimes, including cyber security, privacy and data protection, and online safety.** The nature of the cyber and STsec risks outlined in this report illustrate how they extend beyond financial services regimes into many other domains of policy. Policymakers should consider how other existing and emerging policy regimes align, including legislative proposals for cyber security in critical sectors like finance (C-26), consumer privacy and data protection (C-27), and online safety on social platforms (forthcoming).

5. **Coordinate and collaborate on crypto-asset policymaking with peer jurisdictions and transnational governance and standard-making bodies.** As a mid-sized player in a rapidly digitizing global economy and market for digital assets, Canada should closely follow policy and regulatory development in the EU, U.S., other peer jurisdictions and standards bodies, to both adapt good practices and ensure Canadian financial and technology regulation are as interoperable as possible while reflecting domestic interests and values.

Appendix 1: Survey Methodology

The survey was conducted online with 2,022 residents in Canada aged 16 and older, from October 24 to 28, 2022 in English and French. A random sample of panelists was invited to complete the survey from Leger's research panel, with response quotas set by region, language, age and gender to ensure the sample reflected Canada's population. The data were weighted according to Census data to ensure that the sample matched Canada's population according to age, gender and region. This project was conducted by our team with Pollara Strategic Insights and supported by the Government of Canada.

Q1. Have you ever owned a cryptoasset, such as Bitcoin, Ethereum or an NFT?

Category	Yes
Overall (n=1,979)	9%
Men (n=931)	14%
Women (n=1,023)	5%
University education (n=557)	13%
College education or apprenticeship (n=778)	8%
High school education or less (n=624)	8%
Household income $100,000+ (n=510)	14%
Household income between $50-100,000 (n=652)	10%
Household income below $50,000 (n=578)	7%
Left political spectrum (1-3 on 1-9 scale, n=390)	10%
Centre political spectrum (4-6 on 1-9 scale, n=1,279)	8%
Right political spectrum (7-9 on 1-9 scale, n=310)	13%

Q2: (n=1,979) Have you ever been targeted with online harassment that caused you to fear for your safety?

Crypto-owners (n=186): 19% yes
Not crypto-owners (1,793): 6% yes

Q3: (n=2,022) On a scale of 1-9, where 1 means you have no trust at all and 9 means you have a high degree of trust, how do you feel about each of the following when it comes to trusting them to offer secure and responsible technology:

- federal government
- your provincial government
- your municipal government
- Canadian start-up businesses
- Large Canadian technology companies
- Canadian banks
- Cryptocurrency exchanges
- Canadian telecommunications providers
- Canadian healthcare providers

Q4: (n=186) Have you ever experienced any of the following incidents related to cryptoassets (e.g., Bitcoin, Ethereum, NFTs)?

- I shared my cryptoasset wallet information through a request for information (e.g., by email or text) that turned out to be a scam
- A person claiming to be an experienced crpytoasset investment manager stole the fee for using their services
- The price of a cryptoasset I purchased was artificially inflated through false information
- I purchased a cryptoasset and lost my funds from a person who later disappeared
- A cryptoasset exchange stole my funds
- I was encouraged to recruit new investors for a cryptoasset exchange in exchange for money

End Notes

[1] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [White paper]. https://bitcoin.org/bitcoin.pdf.

[2] Bank of Canada. (2022). *Financial System Review - 2022*. Bank of Canada. https://www.bankofcanada.ca/2022/06/financial-system-review-2022/#Overview.

[3] Reinicke, C. (2021, August 24). 1 in 10 people currently invest in cryptocurrencies, many for ease of trading, CNBC survey finds. *CNBC*. https://www.cnbc.com/2021/08/24/1-in-10-people-invest-in-cryptocurrencies-many-for-ease-of-trading.html.

[4] Rossow, A. (2018, September 7). Stability in Volatile Markets: What You Need to Know about Stable Coins. *Forbes*. https://www.forbes.com/sites/andrewrossow/2018/09/07/stability-in-volatile-markets-what-you-need-to-know-about-stable-coins/.

[5] Bank of Canada. *Central bank digital currency (CBDC)*. Bank of Canada. https://www.bankofcanada.ca/research/digital-currencies-and-fintech/projects/central-bank-digital-currency/.

[6] Browne, R. (2022, March 10). Trading in NFTs spiked 21,000% to top $17 billion in 2021, report says. *CNBC*. https://www.cnbc.com/2022/03/10/trading-in-nfts-spiked-21000percent-to-top-17-billion-in-2021-report.html.

[7] Chow, A.R. (2022, December 21). Where did FTX's Missing $8 Billion Go? Crypto Investigators Offer Clues. *TIME*. https://time.com/6243086/ftx-where-did-money-go/. ; U.S. Securities and Exchange Commission. (2022, December 13). *SEC Charges Samuel Bankman-Fried with Defrauding Investors in Crypto Asset Trading Platform FTX*. https://www.sec.gov/news/press-release/2022-219.

[8] Nicolle, E., Kharif, O., Ishmael, S. (2022, December 21). All The Ways That Crypto Broke in 2022. *Bloomberg*. https://www.bloomberg.com/graphics/2022-crypto-contagion-from-bitcoin-to-FTX/?leadSource=uverify%20wall.

[9] Shukla, S. (2022, September 28). NFT Trading Volumes Collapse 97% From January Peak. *BNN Bloomberg*. https://www.bnnbloomberg.ca/nft-trading-volumes-collapse-97-from-january-peak-1.1824840.

[10] See e.g., House of Commons. (2018). *Don't Block the Blockchain: How Canada can Guard against Money Laundering while Maintaining Global Competitiveness*. https://www.ourcommons.ca/Content/Committee/421/FINA/Brief/BR10007367/br-external/IJWAndCoLtd-2018-09-17-Updated-Final-e.pdf.

[11] Rauchs, M., Glidden, A., Gordon, B., Pieters, G., Recanatini, M., Rostand, F., Vagneur, K., Zhang, B. (2018). *Distributed Ledger Technology Systems: A Conceptual Framework*. University of Cambridge: Cambridge Centre for Alternative Finance. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3230013, on page 15.

[12] See e.g. Bertagnoli, L. (2022, August 25). *20 Blockchain Platforms Driving the Industry*. Builtin. https://builtin.com/blockchain/blockchain-platforms.

[13] *About*. (n.d.). Bitcoin Core. https://bitcoincore.org/en/about/.

[14] All transactions can be viewed online. See *Bitcoin*. (n.d.). Blockchain.com. https://www.blockchain.com/explorer?view=btc.

[15] Quote from this piece: Dwork, C., Naor, M. (2001). Pricing via Processing or Combatting Junk Mail. *Advances in Cryptology - Crypto '92*. CRYPTO 1992. Lecture Notes in Computer Science, vol. 740. (pp.139-147). Springer. doi:10.1007/3-540-48071-4_10.

[16] See also: Interestingly, the proof of work system was originally proposed to prevent spam email and denial-of-service (DDoS) attacks on websites. Finney, H. (n.d.). *Reusable Proofs of Work*. Nakamoto Institute. https://nakamotoinstitute.org/finney/rpow/index.html.

[17] Walker, G. (n.d.). *How does Bitcoin work?*. Learn me a bitcoin. https://learnmeabitcoin.com/.

[18] The most common are proof of work and proof of stake, but other variations include delegated proof of stake, proof of activity, proof of authority, proof of burn, proof of capacity or proof of space, proof of elapsed time, proof of history, and proof of importance. *What is Consensus? A Beginner's Guide*. (2022, May 13). Crypto.com. https://crypto.com/university/consensus-mechanisms-explained.

[19] Napoletano, E., and Broverman, A. (2022, July 12). Proof of Stake Explained. *Forbes*. https://www.forbes.com/advisor/ca/investing/cryptocurrency/proof-of-stake/.

[20] Platt, M., Sedlmeir, J., Platt, D., Xu, J., Tasca, P., Vadgama, N., Ibañez, J.I. (2021). The Energy Footprint of Blockchain Consensus Mechanisms Beyond Proof-of-Work. *IEEE*. doi: 10.1109/QRS-C55045.2021.00168.

[21] Chow, A. (2022, September 7). Why the Ethereum Merge Matters. *TIME*. https://time.com/6211294/ethereum-merge-preview/?utm_medium=email&utm_source=sfmc&utm_campaign=newsletter+metaverse+default+ac&utm_content=+++20220915+++body&et_rid=223916983&lctg=223916983. ; *The Merge*. (2022, September 15). Ethereum.org. https://ethereum.org/en/upgrades/merge/.

[22] Guegan, D. (2017). Public Blockchain versus Private blockchain. *HAL Open Science*, 1-6. https://halshs.archives-ouvertes.fr/halshs-01524440/document.

[23] Jayachandran, P. (2017, May 31). The difference between public and private blockchain. *IBM*. https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/.

[24] Schinckus, C., Nguyen, C.P., Chong, F.H.L. (2021). Are Bitcoin and Ether Affected by Strictly Anonymous Crypto-Currencies? An Exploratory Study. *Economics, Management and Financial Markets* 16(4), 9-27. doi: 10.22381/emfm16420211._

[25] Fauzi, P., Meiklejohn, S., Mercer, R., Orlandi, C. (2018). Quisquis: A New Design for Anonymous Cryptocurrencies. In *Advances in Cryptology - ASIACRYPT 2019, 25th International Conference on the Theory and Application of Cryptology and Information Security*. (pp 649-678). doi:10.1007/978-3-030-34578-5_23.

[26] Shin, D. and Ibahrine, M. (2020). The socio-technical assemblages of blockchain system: how blockchains are framed and how the framing reflects societal contexts. *Digital Policy, Regulation and Governance* 22(3), 245-263. https://www.emerald.com/insight/content/doi/10.1108/DPRG-11-2019-0095/full/html#abstract.

[27] When a blockchain project is "forked", this splits the blockchain into two separate networks. Intentional forks and hard forks are used to implement new consensus mechanisms, and require nodes to be upgraded to new consensus mechanisms, respectively.

[28] White, M. (2022, January 9). *Blockchain-based systems are not what they say they are*. Molly White. https://blog.mollywhite.net/blockchains-are-not-what-they-say/. ;Ore, J. (2016, August 28). How a $64M hack changed the fate of Ethereum, Bitcoin's closest competitor. *CBC News*. https://www.cbc.ca/news/science/ethereum-hack-blockchain-fork-bitcoin-1.3719009.

[29] Hirsh, S., Alman, S., Lemieux, V., Meyer, E.T. (2019). Blockchain: One emerging technology - so many applications. *Proceedings of the Association for Information Science and Technology* 55(1), 691-693. doi:10.1002/pra2.2018.14505501083.

[30] Lemieux, V. (2017). Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems: An Archival Theoretic Evaluation Framework. *Future Technologies Conference (FTC) 2017*. https://www.researchgate.net/profile/Victoria-Lemieux/publication/317433591_Blockchain_and_Distributed_Ledgers_as_Trusted_Recordkeeping_Systems_An_Archival_Theoretic_Evaluation_Framework/links/593aa6450f7e9b3317f4d860/Blockchain-and-Distributed-Ledgers-as-Trusted-Recordkeeping-Systems-An-Archival-Theoretic-Evaluation-Framework.pdf

[31] Jackson, B. (2019, May 1). Canada's 'big 5' banks launch blockchain-based digital identity service with SecureKey. *IT World Canada*. https://www.itworldcanada.com/article/canadas-big-5-banks-launch-blockchain-based-digital-identity-service-with-securekey/417406/.

[32] Lemieux, V. (2020). Caught in the middle? Strategic information governance disruptions in the era of blockchain and distributed trust. *Records Management Journal* 30(3), 301-324. doi:10.1108/RMJ-09-2019-0048.

[33] Nabben, K. (2021). Blockchain Security as "People security": Applying Sociotechnical Security to Blockchain Technology. *Frontiers in Computer Science*. doi:10.3389/fcomp.2020.599406.; Thylin, T., Duarte, M.F.N. (2019). Leveraging blockchain technology in humanitarian settings - opportunities and risks for women and girls. *Gender & Development* 2, 317-336. doi:10.1080/13552074.2019.16277.; Cheesman, M. (2022, June 8). Blockchain for Refugees. *Medium.com*. https://points.datasociety.net/blockchain-for-refugees-a46b41594eee.

[34] Blandin, A., Cloots, A.S., Hussain, H., Rauchs, M., Saleuddin, R., Allen, J.G., Zhang, B.Z., Cloud, K. (2019). Global crypto-asset Regulatory Landscape Study. *University of Cambridge Faculty of Law Research Paper No. 23*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3379219.

[35] *Crypto Assets*. (n.d.). Canadian Securities Administrators. https://www.securities-administrators.ca/investor-tools/crypto-assets/.

[36] *What is Crypto Gaming?* (2023, January 23). Bitbuy. https://bitbuy.ca/guides/what-is-crypto-gaming.

[37] Houben, R. and Snyers, A. (2018). *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion*. European Parliament, Policy Department for Economic, Scientific And Quality of Life Policies. https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf.

[38] This report uses the terms 'exchange' and 'trading platform' interchangeably.

[39] Paz, J. (2022, March 16). The Best Global Crypto Exchanges. *Forbes*. https://www.forbes.com/sites/javierpaz/2022/03/16/the-best-global-crypto-exchanges/.

[40] Woods, J. (2018, March 18). Crypto Exchanges: Custodial vs. Non-Custodial vs. Decentralized. *Medium.com*. https://medium.com/@jacobrobertwoods/crypto-exchanges-custodial-vs-non-custodial-vs-decentralized-3d1d04cf205.

[41] See also *Non-custodial crypto exchange*. (n.d.). PC Mag. https://www.pcmag.com/encyclopedia/term/non-custodial-crypto-exchange.

[42] Woods, J. (2018, March 18). Crypto Exchanges: Custodial vs. Non-Custodial vs. Decentralized. *Medium.com*. https://medium.com/@jacobrobertwoods/crypto-exchanges-custodial-vs-non-custodial-vs-decentralized-3d1d04cf205.

[43] White, M. (2022, May 20). *Predatory Community*. Molly White. https://blog.mollywhite.net/predatory-community/.; Financial Conduct Authority (2019). How and why consumers buy crypto-assets. *FCA*. https://www.fca.org.uk/publication/research/how-and-why-consumers-buy-crypto-assets.pdf. ; Balutel, D., Felt, M., Nicholls, G., Voia, M.C. (2022). Bitcoin Awareness, Ownership and Use: 2016-20. *Bank of Canada*. Doi: 10.34989/sdp-2022-10.; Qureshi, K. and Zaman, T. (2022). Social Media Engagement and Cryptocurrency Performance. *Cornell University*. https://arxiv.org/pdf/2209.02911.pdf.

[44] Mackenzie, S. (2022). Criminology Towards the Metaverse: Cryptocurrency Scams, Grey Economy and the Technosocial. *The British Journal of Criminology* 62(6), 1537-1552. doi:10.1093/bjc/azab118.

[45] Financial Conduct Authority (2019). How and why consumers buy crypto-assets. *FCA*. https://www.fca.org.uk/publication/research/how-and-why-consumers-buy-crypto-assets.pdf.

[46] Balutel, D., Felt, M., Nicholls, G., Voia, M.C. (2022). Bitcoin Awareness, Ownership and Use: 2016-20. *Bank of Canada*. Doi: 10.34989/sdp-2022-10.

[47] Ibid.

[48] These findings were taken from a representative survey of 2,000 Canadian residents aged 16 and older, conducted in October 2022. These survey findings contributed to a published report released in March 2023. See more: Andrey, S. (2023). Survey of Online Harms in Canada. *Leadership Lab*. https://www.ryersonleadlab.com/survey-of-online-harms-in-canada.

[49] For more information on methodology, see https://www.ryersonleadlab.com/survey-of-online-harms-in-canada.

[50] Schecter, B. (2022, November 16). How regulation slowed FTX's growth, limiting the toll of its collapse in Canada. *Financial Post*. https://financialpost.com/fp-finance/cryptocurrency/regulation-slowed-ftx-growth-canada-limiting-toll-crypto-collapse; Rolfe, K. (2023, February 28). FTX includes more than 30 Canadian firms in sprawling creditors list. *The Logic*. https://thelogic.co/news/ftx-includes-more-than-30-canadian-firms-in-sprawling-creditors-list/.

[51] oerzen, M., Watkins, E.A., Lim, G. (2019). Entanglements and Exploits: Sociotechnical security as an analytic framework. *9th USENIX Workshop on Free and Open Communications on the Internet (FOCI '19)*. https://www.usenix.org/conference/foci19/presentation/goerzen.

[52] De Gregorio, I. (2022, July 12). *The event that could change crypto forever is here*. Medium. https://medium.datadriveninvestor.com/the-event-that-could-change-crypto-forever-is-here-9e7edf9c8647#:~:text=On%20June%20the%2013th%2C%20Mt,us%20later%20in%20the%20story.

[53] Kaartemo, V. and Kramer, M. (2020). The sources of cybersecurity threats in cryptocurrency. In J.M. Munoz & M. Frenkel (Eds.), *The Economics of Cryptocurrencies*. Routledge: Taylor Francis. doi:10.4324/9780429200427.

[54] Guggenberger, T., Schlatt, V., Schmid, J., and Urbach, N. (2021). A Structured Overview of Attacks on Blockchain Systems. *Twenty-fifth Pacific Asia Conference on Information Systems, Dubai, UAE, 2021*. https://www.researchgate.net/profile/Nils-Urbach/publication/352733786_A_Structured_Overview_of_Attacks_on_Blockchain_Systems/links/60d5747a299bf1ea9ebade14/A-Structured-Overview-of-Attacks-on-Blockchain-Systems.pdf.; Fernandez, R. (2022, June 28). Pentagon finds concerning vulnerabilities on blockchain. *TechRepublic*. https://www.techrepublic.com/article/pentagon-finds-concerning-vulnerabilities-on-blockchain/.

[55] Weaver, N. (2018). Risks of Cryptocurrencies. *Communications of the ACM* 61(6), 20-24. doi:10.1145/3208095.; Guggenberger, T., Schlatt, V., Schmid, J., and Urbach, N. (2021). A Structured Overview of Attacks on Blockchain Systems. *Twenty-fifth Pacific Asia Conference on Information Systems, Dubai, UAE, 2021*. https://www.researchgate.net/profile/Nils-Urbach/publication/352733786_A_Structured_Overview_of_Attacks_on_Blockchain_Systems/links/60d5747a299bf1ea9ebade14/A-Structured-Overview-of-Attacks-on-Blockchain-Systems.pdf.; Financial Stability Board. (2023). *The Financial Stability Risks of Decentralised Finance*. https://www.fsb.org/wp-content/uploads/P160223.pdf.

[56] Hassan, A., Mas'ud, M.Z., Shah, W.M., Abdul-Latip, S.F., Ahmad, R., Ariffin, A., and Yunos, Z. (2020). A Systematic Literature Review on the Security and Privacy of the Blockchain and Cryptocurrency. *OIC-CERT Journal of Cyber Security* 2(1), 1-17. https://www.oic-cert.org/en/journal/pdf/2/1/211.pdf.

[57] Hassan, A., Mas'ud, M.Z., Shah, W.M., Abdul-Latip, S.F., Ahmad, R., Ariffin, A., and Yunos, Z. (2020). A Systematic Literature Review on the Security and Privacy of the Blockchain and Cryptocurrency. *OIC-CERT Journal of Cyber Security* 2(1), 1-17. https://www.oic-cert.org/en/journal/pdf/2/1/211.pdf.; Houben, R. and Snyers, A. (2018). *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion*. European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies. https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf.

[58] Schipor, G. (2019). Risks and Opportunities in the Cryptocurrency Market. *"Ovidius" University Annals, Economic Sciences Series* XIX(2). https://stec.univ-ovidius.ro/html/anale/RO/wp-content/uploads/2020/02/Section%20V/36.pdf; Perkins, D. (2020). *Cryptocurrency: The Economics of Money and Selected Policy Issues*. Congressional Research Service. https://www.everycrsreport.com/files/20200409_R45427_8469ceaa641685c78bf188b7e5fdbb23004507a4.pdf.

[59] Sai, A.R., Buckley, J., Le Gear, A. (2019). Privacy and Security Analysis of Cryptocurrency Mobile Applications. *IEEE: Conference on Mobile and Secure Services*. doi:10.1109/MOBISECSERV.2019.8686583.

[60] Cyber security & Infrastructure Security Agency. (2021, February 17). *Alert (AA21-048A): Apple Jeus: Analysis of North Korea's Cryptocurrency Malware*. CISA. https://www.cisa.gov/uscert/ncas/alerts/aa21-048a.; Communications Security Establishment. (2022). *National Cyber Threat Assessment 2023-2024*. Canadian Centre for Cyber Security. https://cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf

[61] Sai, A.R., Buckley, J., Le Gear, A. (2019). Privacy and Security Analysis of Cryptocurrency Mobile Applications. *IEEE: Conference on Mobile and Secure Services*. doi:10.1109/MOBISECSERV.2019.8686583.

[62] Hassan, A., Mas'ud, M.Z., Shah, W.M., Abdul-Latip, S.F., Ahmad, R., Ariffin, A., and Yunos, Z. (2020). A Systematic Literature Review on the Security and Privacy of the Blockchain and Cryptocurrency. *OIC-CERT Journal of Cyber Security* 2(1), 1-17. https://www.oic-cert.org/en/journal/pdf/2/1/211.pdf.

[63] Shin, D. and Rice, J. (2022). Cryptocurrency: A panacea for economic growth and sustainability? A critical review of crypto innovation. *Telematics and Informatics* 71. doi: 10.1016/j.tele.2022.101830.

[64] Hasanova, H., Baek, U., Shin, M., Cho, K., Kim, M. (2019). A survey on blockchain cyber security vulnerabilities and possible countermeasures. *Int J Network Mgmt*. doi:10.1002/nem.2060.; Saad, M., Spaulding, J., Nijilla, L., Kamhoua, C., Shetty, S., Nyang, D., Mohaisen, D. (2020). Exploring the Attack Surface of Blockchain: A comprehensive survey. *IEEE Communications Surveys & Tutorials* 22(3). doi:10.1109/COMST.2020.2975999.

[65] Abhishta, A., Joosten, R., Dragomiretskiy, S., Nieuwenhuis, B. (2019). Impact of Successful DDoS Attacks on a Major Crypto-Currency Exchange. *2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)*. doi:10.1109/EMPDP.2019.8671642.

[66] Conti, M., E, S.K., Lal, C., Ruj, S. (2017). A Survey on Security and Privacy Issues of Bitcoin. *IEEE*. https://arxiv.org/pdf/1706.00916.pdf.; Fanti, G. and Viswanath, P. (2017). Deanonymization in the Bitcoin P2P Network. *31st Conference on Neural Information Processing Systems (NIPS 2017)*. https://dl.acm.org/doi/pdf/10.5555/3294771.3294901.

[67] Hassan, A., Mas'ud, M.Z., Shah, W.M., Abdul-Latip, S.F., Ahmad, R., Ariffin, A., and Yunos, Z. (2020). A Systematic Literature Review on the Security and Privacy of the Blockchain and Cryptocurrency. *OIC-CERT Journal of Cyber Security* 2(1), 1-17. https://www.oic-cert.org/en/journal/pdf/2/1/211.pdf.

[68] Goerzen, M., Watkins, E.A., Lim, G. (2019). Entanglements and Exploits: Sociotechnical Security as an Analytic Framework. *9th USENIX Workshop on Free and Open Communications on the Internet (FOCI '19)*. https://www.usenix.org/conference/foci19/presentation/goerzen.

[69] Ibid.

[70] Ibid.

[71] Northcott, P. (2022, May 10). Police help victim of crypto-fraud get money back. *Royal Canadian Mounted Police*. https://www.rcmp-grc.gc.ca/en/gazette/police-help-victim-crypto-fraud-get-money-back.

[72] White, M. (2022, January 22). *Abuse and harassment on the blockchain*. Molly White. https://blog.mollywhite.net/abuse-and-harassment-on-the-blockchain/.

[73] Levy, K. and Schneier, B. (2020). Privacy threats in intimate relationships. *Journal of cyber security* 6(1). doi:10.1093/cybsec/tyaa006.

[74] Biggs, J. (2017, October 17). Bitcoin engineer Jameson Lopp SWATted by angry crypto fans. *TechCrunch*. https://techcrunch.com/2017/10/17/bitcoin-engineer-jameson-lopp-swatted-by-angry-crypto-fans/.

[75] Davies, R. (2022, May 8). 'Crypto muggings': thieves in London target digital investors by taking phones. *The Guardian*. https://www.theguardian.com/technology/2022/may/08/crypto-muggings-thieves-in-london-target-digital-investors-by-taking-phones#:~:text=The%20crypto%20muggings%20took%20place,with%20the%20threat%20of%20violence.

[76] Northcott, P. (2022, May 10). Police help victim of crypto-fraud get money back. *Royal Canadian Mounted Police*. https://www.rcmp-grc.gc.ca/en/gazette/police-help-victim-crypto-fraud-get-money-back.

[77] Vergolina, V. (2022, September 12). Tornado Cash: What it is and why it's been sanctioned by Treasury. *Bloomberg UK*. https://www.bloomberg.com/news/articles/2022-09-12/tornado-cash-what-it-is-and-why-it-s-been-sanctioned-by-treasury?leadSource=uverify%20wall; Reuters. (2022, August 8). US sanctions Tornado Cash over fears of aiding North Korean hackers. *The Guardian*. https://www.theguardian.com/technology/2022/aug/08/us-sanctions-tornado-cash-north-korea-hackers.

[78] Oliver, J. (2022, September 19). The lawless world of crypto scams. *Financial Times*. https://www.ft.com/content/5987649e-9345-4eae-a4b8-9bfb0142a2ab.

[79] Fletcher, E. (2022, June 3). *Reports show scammers cashing in on crypto craze*. Federal Trade Commission. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze.

[80] Waterloo Regional Police. (2022, April 21). WRPS Warn Residents about Cryptocurrency Investment Scams. *Waterloo Regional Police*. https://www.wrps.on.ca/en/news/wrps-warn-residents-about-cryptocurrency-investment-scams.aspx.

[81] Ibid.

[82] Shufelt, T. (2023, March 14). Crypto hype is down, but crypto fraud is proliferating. *The Globe and Mail*. https://www.theglobeandmail.com/investing/markets/inside-the-market/article-crypto-hype-is-down-but-crypto-fraud-is-proliferating/.

[83] Lu, C., Batista, D., Hamouda, H., Lemieux, V. (2020). Consumers' intentions to adopt blockchain-based personal health records and data sharing: focus group study. *JMIR formative research* 4(11). doi:10.2196/21995.; Fröhlich, M., Gutjahr, F., Alt, F. (2020). Don't lose your coin! Investigating Security Practices of Cryptocurrency Users. *DIS '20: Proceedings of the 2020 ACM Designing Interactive Systems Conference*. doi:10.1145/3357236.3395535.; Dai, F., Shi, Y., Meng, N., Wei, L., Ye, Z. (2017). From Bitcoin to cyber security: A comparative study of blockchain application and security issues. *2017 4th International Conference on Systems and Informatics (ICSAI)*. doi:10.1109/ICSAI.2017.8248427.

[84] Mackenzie, S. (2022). Criminology Towards the Metaverse: Cryptocurrency Scams, Grey Economy and the Technosocial. *The British Journal of Criminology* 62(6), 1537-1552. doi:10.1093/bjc/azab118.

[85] Domenico, M.D. and Baronchelli, A. (2019). The fragility of decentralised trustless socio-technical systems. *EPJ Data Science* 8(2). doi:10.1140/epjds/s13688-018-0180-6.

[86] Weaver, N. (2018). Risks of Cryptocurrencies. *Communications of the ACM* 61(6), 20-24. doi:10.1145/3208095.

[87] Kamps, J. and Kleinberg, B. (2018). To the moon: defining and detecting cryptocurrency pump-and-dumps. *Crime science* 7(18). doi:10.1186/s40163-018-0093-5.

[88] Mackenzie, S. (2022). Criminology Towards the Metaverse: Cryptocurrency Scams, Grey Economy and the Technosocial. *The British Journal of Criminology* 62(6), 1537-1552. doi:10.1093/bjc/azab118.

[89] Tidy, J. (2022, October 3). Kim Kardashian pays $1.26m over crypto 'pump and dump'. BBC. https://www.bbc.com/news/technology-63116235.; U.S. Securities and Exchange Commission. (2018, November 29). *Two Celebrities Charged with Unlawfully Touting Coin Offerings*. [Press release]. https://www.sec.gov/news/press-release/2018-268.

[90] Q.ai. (2022, September 20). What Really Happened to LUNA Crypto? *Forbes*. https://www.forbes.com/sites/qai/2022/09/20/what-really-happened-to-luna-crypto/?sh=b5a40c4ff12c.

[91] Shifflett, S. and Jones, C. (2018, May 17). Buyer Beware: Hundreds of Bitcoin Wannabes Show Hallmarks of Fraud. The *Wall Street Journal*. https://www.wsj.com/articles/buyer-beware-hundreds-of-bitcoin-wannabes-show-hallmarks-of-fraud-1526573115.

[92] Betz, B. (2022, November 17). FTX Ventures was a disorganized mess with missing financials, bankruptcy documents say. *CoinDesk*. https://www.coindesk.com/business/2022/11/17/ftx-ventures-was-a-disorganized-mess-with-missing-financials-bankruptcy-documents-say/.; Elder, B. and Scaggs, A. (2022, November 17). The FTX bankruptcy filing in full (updated). *Financial Times*. https://www.ft.com/content/c236d6f9-da5a-4da7-8dc8-5cd450dfe39d.

[93] Schneier, B. (2022, June 24). *On the Dangers of Cryptocurrencies and the Uselessness of Blockchain*. Schneier on Security. https://www.schneier.com/blog/archives/2022/06/on-the-dangers-of-cryptocurrencies-and-the-uselessness-of-blockchain.html.; Brennecke, M., Guggenberger, T., Sachs, A., Schellinger, B. (2022). The Human Factor in Blockchain Ecosystems: A Sociotechnical Framework. *Wirtscharftsinformatik 2022 Proceedings*. https://aisel.aisnet.org/wi2022/finance_and_blockchain/finance_and_blockchain/3/.

[94] Gencer, A.E., Basu, S., Eyal, I., Renesse, R., Sirer, E.G. (2018). Decentralization in Bitcoin and Ethereum Networks. *Financial Cryptography and Data Security: 22nd International Conference, FC 2018, Nieuwpoort, Curaçao*. doi:10.1007/978-3-662-58387-6_24.

[95] Weaver, N. (2018). Risks of Cryptocurrencies. *Communications of the ACM* 61(6), 20-24. doi:10.1145/3208095.

[96] See, for instance, Balaji Srinivasan's writing about how blockchain technologies could be used to create fully decentralized, digital communities while radically subverting existing political systems and state institutions. Srinivasan, B. (2022). *The Network State: How To Start a New Country. Amazon Kindle*.

[97] Goodkind, A.L., Jones, B.A., Berrens, R.P. (2020). Cryptodamages: Monetary value estimates of the air pollution and human health impacts of cryptocurrency mining. *Energy Research & Social Science* 59. doi:10.1016/j.erss.2019.101281.

[98] Mora, C., Rollins, R.L., Taladay, K., Kantar, M.B., Chock, M.K., Shimada, M., Franklin, E.C. (2018). Bitcoin emissions alone could push global warming above 2°C. *Nature Climate Change* 8, 931-933. doi:10.1038/s41558-018-0321-8.

[99] Truby, J., Brown, R., Dahdal, A., Ibrahim, I. (2022). Blockchain, climate damage, and death: Policy interventions to reduce the carbon emissions, mortality, and net-zero implications of non-fungible tokens and Bitcoin. *Energy Research & Social Science* 88. doi:10.1016/j.erss.2022.102499.

[100] Canada Energy Regulator. (2018, August 22). *Market Snapshot: Crypto-currency mining is booming in Canada. Here is why*. CER. https://www.cer-rec.gc.ca/en/data-analysis/energy-markets/market-snapshots/2018/market-snapshot-crypto-currency-mining-is-booming-in-canada-here-is-why.html.

[101] Milano, A. (2018, February 6). BIS Chief Slams Bitcoin As Ponzi Scheme and Threat to Central Banks. *CoinDesk*. https://www.coindesk.com/markets/2018/02/06/bis-chief-slams-bitcoin-as-ponzi-scheme-and-threat-to-central-banks/.

[102] Li, B., Sugimoto, N. (2023, January 18). Crypto Contagion Underscores Why Global Regulators Must Act Fast to Stem Risk. *IMF Blog*. https://www.imf.org/en/Blogs/Articles/2023/01/18/crypto-contagion-underscores-why-global-regulators-must-act-fast-to-stem-risk.

[103] Gilbert, S. (2022). *Crypto, web3, and the Metaverse*. Bennett Institute for Public Policy Cambridge. https://www.bennettinstitute.cam.ac.uk/wp-content/uploads/2022/03/Policy-brief-Crypto-web3-and-the-metaverse.pdf.

[104] Southurst, J. (2021, July 23). Blockchain attacks and reorgs: Experiences from the past. *Coingeek News*. https://coingeek.com/blockchain-attacks-and-reorgs-experiences-from-the-past/.

[105] Financial and Consumer Services Commission. (2022, May 9). *Canadian Anti-Fraud Centre Bulletin: CAFC and WPS Recover $17000 in Bitcoin*. https://fcnb.ca/en/news-alerts/canadian-anti-fraud-centre-bulletin-cafc-and-wps-recover-17000-in-bitcoin#:~:text=On%20March%2017th%2C%202022%2C%20the,both%20CAFC%20and%20local%20police.; Northcott, P. (2022, May 10). Police help victim of crypto-fraud get money back. *RCMP*. https://www.rcmp-grc.gc.ca/en/gazette/police-help-victim-crypto-fraud-get-money-back.; United States Department of Justice. (2022, November 7). U.S. Attorney Announces Historic $3.36 Billion Cryptocurrency Seizure and Conviction in Connection with Silk Road Dark Web Fraud. *U.S. Attorney's Office, Southern District of New York*. https://www.justice.gov/usao-sdny/pr/us-attorney-announces-historic-336-billion-cryptocurrency-seizure-and-conviction.

[106] Ontario Securities Commission. (2018). *Downfall of Quadriga (2018)*. https://www.osc.ca/quadrigacxreport/downfall-of-quadriga.html.

[107] Derk, C., Bogle, J., Gomez, I. (2022, February 22). *Cryptocurrency outlook in Canada - Where we are and where we are going*. BLG. https://www.blg.com/en/insights/2022/02/cryptocurrency-outlook-in-canada-where-we-are-and-where-we-are-going.; Sia Partners. (2021, October 14). Canadian Securities Regulations for Crypto Businesses. *Sia Partners*. https://www.sia-partners.com/en/news-and-publications/from-our-experts/canadian-securities-regulations-crypto-businesses.; Grant, S., Lim, K., Peters, M. (2022). *Blockchain & Cryptocurrency Laws and Regulations 2022*. Global Legal Insights. https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/canada.; Government of Canada. (2022, November 16). *Statement to entities engaging in crypto-asset activities or crypto-related services*. https://www.canada.ca/en/financial-consumer-agency/news/2022/11/statement-to-entities-engaging-in-crypto-asset-activities-or-crypto-related-services0.html.

[108] Sia Partners. (2021, October 14). Canadian Securities Regulations for Crypto Businesses. *Sia Partners*. https://www.sia-partners.com/en/news-and-publications/from-our-experts/canadian-securities-regulations-crypto-businesses. ; Hills, N. (2021, December 20). Canada: A Legal Guide to Cryptocurrency in Canada. *Mondaq*. https://www.mondaq.com/canada/fin-tech/1142772/a-legal-guide-to-cryptocurrency-in-canada.

[109] Derk, C., Bogle, J., Gomez, I. (2022, February 22). Cryptocurrency outlook in Canada - Where we are and where we are going. *BLG*. https://www.blg.com/en/insights/2022/02/cryptocurrency-outlook-in-canada-where-we-are-and-where-we-are-going.

[110] Canadian Securities Administrators. (2017). *Staff Notice 46-307. Cryptocurrency Offerings.* https://www.asc.ca/-/media/ASC-Documents-part-1/Regulatory-Instruments/2018/10/5366029-CSA-Staff-Notice-46-307-Cryptocurrency-Offerings.ashx. ; Canadian Securities Administrators. (2018). *Staff Notice 46-308. Securities Law Implications for Offerings of Tokens*. https://www.asc.ca/-/media/ASC-Documents-part-1/Regulatory-Instruments/2018/10/5404970-CSA-Staff-Notice-46-308.ashx.

[111] Canadian Securities Administrators. (2021). *CSA Staff Notice 51-363 - Observations on Disclosure by Crypto Assets Reporting Issuers*. https://www.osc.ca/sites/default/files/2021-03/csa_20210311_51-363_observations-disclosure-crypto-asset.pdf.; Canadian Securities Administrators. (2021). *Staff Notice 21-330. Guidance for Crypto-Trading Platforms: Requirements relating to Advertising, Marketing and Social Media Use*. https://www.osc.ca/sites/default/files/2021-09/csa_20210923_21-330_crypto-trading-platforms.pdf. ; Grant, S., Lim, K., Peters, M. (2022). Blockchain & Cryptocurrency Laws and Regulations 2022. *Global Legal Insights*. https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/canada.

[112] Canadian Securities Administrators. (2016). *CSA Regulatory Sandbox*. https://www.securities-administrators.ca/resources/regulatory-sandbox/. ; Government of Alberta. (2022). *Innovating the finance sector*. https://www.alberta.ca/innovating-the-finance-sector.aspx.

[113] See Clements, R. (2022). Commissioned Paper: Cryptocurrency: Challenges to Conventional Governance of Financial Transactions. *Public Order Emergency Commission*. https://publicorderemergencycommission.ca/files/documents/Policy-Papers/Cryptocurrency-Challenges-to-Conventional-Governance-of-Financial-Transactions-Clements.pdf. He highlights a number of other CSA Staff Notices (21-327, 21-329, 21-330, 21-332, 46-307, 46-308) that further establish regulatory guidance for crypto-asset trading and exchanges, addressing CTP pre-registration requirements to protect investors, compliance and risk identification, advertising, marketing and social media requirements, the application of securities law to tokens, and other related areas such as the distribution of crypto-investment funds, derivatives on crypto-assets, and custodial controls.

[114] Canadian Centre for Cyber Security. (2021, September). *Ransomware: How to prevent and recover (ITSAP.00.099)*. Government of Canada. https://www.cyber.gc.ca/en/guidance/ransomware-how-prevent-and-recover-itsap00099.; Canadian Centre for Cyber Security. (2018). *National Cyber Threat Assessment 2018*. Government of Canada. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2018.; Public Safety Canada. (2015) *Organized Crime*. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2015-h001/index-en.aspx.

[115] Communications Security Establishment. (2022). *National Cyber Threat Assessment 2023-2024*. https://cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf.

[116] Ontario Securities Commission. (2023, February 22). Canadian securities regulators strengthen oversight, enhance expectations of crypto asset trading platforms operating in Canada. https://www.osc.ca/en/news-events/news/canadian-securities-regulators-strengthen-oversight-enhance-expectations-crypto-asset-trading.

[117] Government of Canada. (2022, November 16). *Statement to entities engaging in crypto-asset activities or crypto-related services*. https://www.canada.ca/en/financial-consumer-agency/news/2022/11/statement-to-entities-engaging-in-crypto-asset-activities-or-crypto-related-services0.html.

[118] Financial Consumer Agency of Canada. (2021). *Digital currency*. Government of Canada. https://www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html.

[119] Grant, S., Lim, K., Peters, M. (2022). Blockchain & Cryptocurrency Laws and Regulations 2022. *Global Legal Insights*. https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/canada.; Arsenault, J. (2018, July 16). Hydro-Québec allowed to charge cryptocurrency miners increased rates. *Montreal Gazette*. https://montrealgazette.com/news/local-news/hydro-quebec-allowed-to-charge-cryptocurrency-miners-increased-rates.

[120] Department of Finance. (2022, November 3). *Government consults Canadians to advance key priorities*. Government of Canada. https://www.canada.ca/en/department-finance/news/2022/11/government-consults-canadians-to-advance-key-priorities.html.

[121] Government Ontario. (2021). *Capital Markets Act - Consultation Draft*. Ontario's Regulatory Registry. https://www.ontariocanada.com/registry/view.do?postingId=38527&language=en ; Victor, J. (2022, August 26). "Startups push back on proposal to give Ontario regulators new authority over crypto." *The Logic*. https://thelogic.co/news/startups-push-back-on-proposal-to-give-ontario-regulators-new-authority-over-crypto/.

[122] Ontario Securities Commission. (2022, March 11). Fraud Prevention Month: Canadian Securities Administrators encourages Canadians to invest in asking questions before investing in crypto assets. https://www.osc.ca/en/news-events/news/fraud-prevention-month-canadian-securities-administrators-encourages-canadians-invest-asking.

[123] European Commission. (2020, September 24). *Digital finance package*. European Commission. https://finance.ec.europa.eu/publications/digital-finance-package_en.

[124] Directive 2014/65/EU. *On markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0065.

[125] European Council. (2022, June 30). *Digital finance: agreement reached on European crypto-assets regulation (MiCA)* [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/.; *Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593.

[126] Ibid.

[127] Ibid.

[128] *Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593.

[129] European Council. (2022, November 28). *Digital finance: Council adopts Digital Operational Resilience Act* [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/digital-finance-council-adopts-digital-operational-resilience-act/.

[130] Regulation 2022/2554. *On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) 909/2014 and (EU) 2016/1011*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554.

[131] Regulation 2022/858. *On a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0858.

[132] The White House. (2022, September 16). FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets. *The White House*. https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/.

[133] Dewey, J. (2022). *Blockchain & Cryptocurrency Laws and Regulations 2022 | USA*. Global Legal Insights. https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/usa.; O'Neal, S. (2018, May 26). SEC, CFTC, IRS And Others: A Guide to US Regulating Bodies. *CoinTelegraph*. https://cointelegraph.com/news/sec-cftc-irs-and-others-a-guide-to-us-regulating-bodies.

[134] Digital Commodities Consumer Protection Act of 2022, S.4760, 117th Congress, 2022. https://www.congress.gov/bill/117th-congress/senate-bill/4760/text. ; Lummis-Gillibrand Responsible Financial Innovation Act, S.4356, 117th Congress, 2022. https://www.congress.gov/bill/117th-congress/senate-bill/4356/text.

[135] Stablecoin Transparency Act, S.3970, 117th Congress, 2022. https://www.congress.gov/bill/117th-congress/senate-bill/4356/text. ; Versprille, A. and Weinberger, E. (2022, July 20). Stablecoins Face US Scrutiny as House Lawmakers Craft Rules. *Bloomberg UK*. https://www.bloomberg.com/news/articles/2022-07-20/stablecoins-face-scrutiny-as-lawmakers-aim-to-advance-plan.

[136] U.S. Securities and Exchange Commission. (2022, May 3). *SEC Nearly Doubles Size of Enforcement's Crypto Assets and Cyber Unit* [Press release]. https://www.sec.gov/news/press-release/2022-78.

[137] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency. (2023, February 23). *Agencies issue joint statement on liquidity risks resulting from crypto-asset market vulnerabilities* [Press release]. https://www.federalreserve.gov/newsevents/pressreleases/bcreg20230223a.htm.

[138] U.S. Department of the Treasury. *Action Plan to Address Illicit Financing Risks of Digital Assets*. https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf.

[139] Morton, H. (2022, June 7). *Cryptocurrency 2022 Legislation*. National Conference of State Legislatures. https://www.ncsl.org/research/financial-services-and-commerce/cryptocurrency-2022-legislation.aspx.

[140] Relevant state bills include: Substitute House Bill No. 5320, *An Act Concerning Virtual Currency*, February Session, (Connecticut 2022).; House Bill No.1638, *An Act to repeal section 574.105, RSMo, and to enact in lieu thereof one new section relating to the offense of money laundering, with penalty provisions*, 2nd Regular Session, 101st General Assembly, (Missouri 2022).; Bill No. S08838, An Act to amend the general business law, in relation to requiring certain disclosures in advertisements involving virtual tokens, U.S.C. § 350-b-2. (2022).

[141] Bill No. HB0074, Special purpose depository institutions, 65th Legislature of the State of Wyoming. (2019).; Bill No. HB0027, Select committee on blockchain, technology and innovation, 65th Legislature of the State of Wyoming. (2020).; Bill No. HB0057, Financial technology sandbox, 65th Legislature of the State of Wyoming. (2019).

[142] Financial Stability Board. (2023). *The Financial Stability Risks of Decentralised Finance*. https://www.fsb.org/wp-content/uploads/P160223.pdf.

[143] G20. (2023). *G20 Chair's Summary and Outcome Document, First G20 Finance Ministers and Central Bank Governors Meeting*. https://www.g20.org/content/dam/gtwenty/gtwenty_new/document/1st%20FMCBG%20Chair%20Summary.pdf.

[144] International Organization for Standardization. (2016). *Blockchain and distributed ledger technologies* (ISO/TC 307). https://www.iso.org/committee/6266604.html.

[145] Digital Governance Standards Institute. *Standards in Digital Assets and Nonfungible Tokens*. https://ciostrategycouncil.com/standards/find-a-standard/standards-in-digital-assets/.

[146] Antipolis, S. (2018, December 18). ETSI Launches new Industry Specification Group on blockchain. *ETSI*. . https://www.etsi.org/newsroom/press-releases/1473-2018-12-press-etsi-launches-new-industry-specification-group-on-blockchain.; Deshpande, A., Stewart, K., Lepetit, L., Gunashekar, S. (2017). Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards. *British Standards Institution*. https://www.bsigroup.com/en-GB/Innovation/dlt/.; Standards Australia. *Blockchain*. Standards Australia. https://www.standards.org.au/engagement-events/sectors/blockchain#:~:text=Standards%20Australia%20is%20playing%20an,a%20public%20and%20secure%20manner.

[147] World Economic Forum. (2020). *Global Standards Mapping Initiative: An overview of blockchain technical standards*. https://www3.weforum.org/docs/WEF_GSMI_Technical_Standards_2020.pdf.