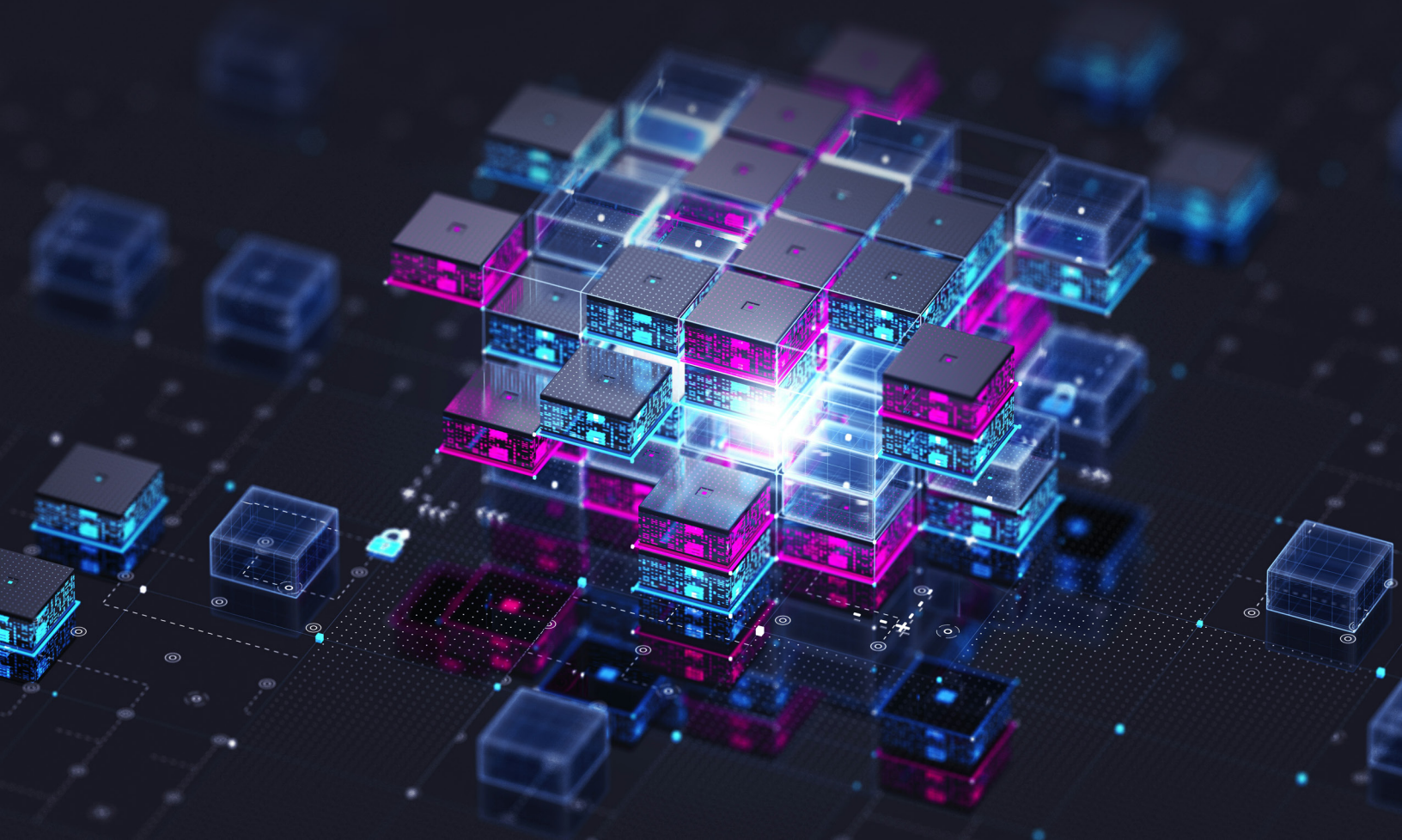
Centre for International
Governance Innovation

CIGI Paper No. 325 — July 2025

Decentralization, Assets and Privacy in the Twenty-First Digital Century

Andreas Veneris



Centre for International
Governance Innovation

CIGI Paper No. 325 — July 2025

Decentralization, Assets and Privacy in the Twenty-First Digital Century

Andreas Veneris

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

President, CIGI Paul Samson
Research Director, Digital Economy S. Yash Kalash
Director, Program Management Dianna English
Program Manager Jenny Thiel
Publications Editor Christine Robertson
Publications Editor Susan Bubak
Graphic Designer Sami Chouhdary

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Author

Andreas Veneris is a Connaught Scholar and professor in the Department of Electrical and Computer Engineering, cross-appointed with the Department of Computer Science and the Munk School of Global Affairs & Public Policy at the University of Toronto. He obtained a Ph.D. from the University of Illinois, Urbana-Champaign. Previously, he held joint faculty positions with the Athens University of Economics and Business (Department of Informatics, 2006–2016) and with the University of Tokyo (Department of Electrical and Computer Engineering, 2010–2011). For more than 20 years, he worked in the field of computer-automated design for very large-scale integration synthesis, verification and debugging using formal methods, publishing more than 120 conference and journal papers. Today, he focuses on central bank digital currencies (CBDCs), mechanism/economic design of distributed systems, formal methods for smart-contract verification, and techno-legal blockchain policy/regulatory questions. In February 2021, his work with the Bank of Canada became public, proposing Canada's central bank digital Loonie — the first work of its kind that presented a comprehensive technological, regulatory/legal and economic model for a CBDC. On March 1, 2022, he was acknowledged for his contributions on a classified report by the Hoover Institution, prefaced by former US Secretary of State Condoleezza Rice, titled *Digital Currencies: The US, China, and the World at a Crossroads*; a week later, President Joe Biden signed Executive Order 14607 following many recommendations of this report. Andreas engages with many Group of Twenty central banks on the topic of CBDCs and Web 3.0, and his work has been featured in publications by the Bank for International Settlements and the International Monetary Fund, among others.

Acronyms and Abbreviations

AI	artificial intelligence
AML/CFT	anti-money laundering/combatting the financing of terrorism
BIS	Bank for International Settlements
BRICS	Brazil, Russia, India, China and South Africa
CBDCs	central bank digital currencies
DeFi	decentralized finance
DLT	distributed ledger technologies
DoJ	Department of Justice
e-CNY	digital yuan
FATF	Financial Action Task Force
G20	Group of Twenty
IDs	identifications
IMS	international monetary system
IoT	Internet of Things
KYC	know-your-customer
mCBDCs	multiple central bank digital currencies
MiCA	Markets in Crypto-Assets
P2P	peer-to-peer
RTGs	real-time gross-settlement systems
SDR	special drawing right
SEC	Securities and Exchange Commission
TradFi	traditional finance
UAE	United Arab Emirates
UBI	universal basic income

Executive Summary

This paper examines the evolving landscape of digital privacy, decentralization and digital assets in the twenty-first century. It explores the transformative impact of those technologies — driven by the exponential growth of semiconductors — in the past decades on the widespread adoption of artificial intelligence (AI), the Internet of Things (IoT) and blockchain today. The analysis highlights how these advancements challenge traditional regulatory frameworks and reshape social, economic and governance structures both domestically and internationally. It emphasizes the rise of centralized digital oligarchies and the implications of decentralized finance and central bank digital currencies (CBDCs) on financial stability, privacy and monetary sovereignty. The brief also provides a geopolitical perspective on privacy, security and digital assets by emphasizing the strategic role of cryptography. It concludes with policy recommendations for Canada and reflects on the need for a "Digital Bretton Woods" to ensure financial stability and social welfare in the digital age.

Alice in Digital Land: Trends and Challenges

Although still at its dawn, the twenty-first century will be remembered by history as the "digital century" due to the transformative and pervasive impact of digital-driven technologies on human lives. The exponential transistor-count growth in semiconductor chip design since the 1970s has allowed for today's technologies (such as AI, cloud computing, smart devices and the IoT) that have reshaped how we live, work and interact. Further, the internet's introduction into daily life over the past three decades has evolved into it becoming the backbone of an interconnected society supporting commerce, finance, entertainment, education, health care, governance and real-time interaction without geographical boundaries. This phenomenon has redefined the social fabric of human interaction while also generating vast volumes of structured and unstructured data for powerful AI tools to thrive upon. The digital century is poised not only to shape economic and societal progress for decades to come but also to perpetuate the regulatory gap with past "analogue" legal frameworks. The convergence of digital assets and privacy has become both a challenge and an opportunity, radically testing the individual rights, social norms, welfare systems and ethical accountability secured through painstaking legal and political advocacy in the twentieth century.

Historically, the internet truly reached its potential with the introduction of Mosaic (later Netscape) in 1993. This was the first web browser that was developed at the University of Illinois at Urbana-Champaign, the author's alma mater, where he was fortunate to contribute to its early stages. Soon after, universities around the world began to adopt it for their courses, and it was not long before the public followed suit. At that time, the internet was unidirectional, censorship free, non-intermediated and decentralized: it freely produced content for consumption while a diverse range of content producers held a balanced market share. This "unfiltered" information exchange had strong network effects as evidenced by the rise of novel communication, social and commerce platforms. There were no monolithic social networks and dominant AI-based search engines acting as "curation middlemen."

Today, the internet is cracking under its own weight and straying from its original vision. The zero-marginal-cost society for goods and services — championed by corporate conglomerates of internet platforms that concentrate data, news, micro-suppliers and consumers within unified ecosystems — has resulted in significant network centralization. This is further compounded by the proliferation of IoT through AI-driven smart devices (in our phones, homes, cars, wearables, health care, supply chains and so on.), which transmit vast amounts of data to these private entities in exchange for nominal internet-based services. The net effect of this zero-cost culture is the aggregation of audiences and their social attention into the hands of a few dominant middlemen. Cases in point for this digital oligarchy: nearly 57 percent of Western internet traffic is consumed by just five entities, namely Google, Amazon, Facebook, Microsoft and Netflix (Weissberger 2022); and nearly 65 percent of the news in the West is curated by two players (Google and Facebook) (Majid 2023). In China, a handful of companies (Baidu, JD.com, Renren, Alibaba, Tencent) dominate

online attention. Whereas Google accounts for about 90 percent of the global search market,[1] in China, Baidu's search market share is at 54 percent, followed by Bing (a Western product) with about a 30 percent share (MarketMeChina 2024).

It therefore comes as no surprise that in June 2021, within the context of digital currencies, the Bank for International Settlements (BIS) encouraged central banks to consider issuing government-backed digital money. According to its annual economic report, "the most significant recent development has been the entry of big techs into financial services. Their business model rests on the direct interactions of users, as well as the data that are an essential by-product of these interactions…[T]he user data in their existing businesses in e-commerce, messaging, social media or search give them a competitive edge through strong network effects. The more users flock to a particular platform, the more attractive it is for a new user to join that same network, leading to a Data-Network-Activities or DNA loop" (BIS 2021, 67). The report emphasizes concerns such as the risk of currency substitution, in which government money is replaced by "private money'' with resulting repercussions to a nation's sovereignty (ibid., 77). Arguably, money derives its value from network effects and, thus, concentrating financial activity and data on a few platforms may lead to reliance on a single form of money, rendering monetary policy ineffective.

The concentration of internet traffic — coupled with pervasive data collection often stored in siloed cloud services located in foreign jurisdictions — has fostered a dependency on an economy centred around "digital leisure" and the illusion of a "global celebrity status." Despite appearing free, this model exacts a cost: the public pays with their time, personal data and privacy. At the same time, some executives of the very corporations driving this model started to advocate for a universal basic income (UBI) (Nolan 2024). If this UBI materialized, it would become a taxpayer-funded initiative ultimately financed by the public itself. This dynamic not only commodifies individuals as being mere "data producers/consumers" but also risks deepening these individuals' dependency on public debt. In addition, it challenges the traditional role of state-issued money — historically earned through labour and exchanged for social welfare — by weakening the reciprocal control citizens have over their time, data and money.

While digitization initially promised increased competition, greater opportunities, broader choices and citizen empowerment, current trends reveal a starkly different reality. The modern monolithic digital landscape has become increasingly concentrated, with large tech firms leveraging regulatory frameworks with lobbying practices (Pilkington 2025; Mullins 2015) to advance their own interests, shape social norms (Cuthbertson 2024) and stifle competition. This phenomenon is aptly described in modern political economy as one of surveillance capitalism (Zuboff 2019).

Decentralization, Web 3.0 and Cryptography: When Bob Met Alice

Alice was feeling lost navigating this digital labyrinth, but one day, she met Bob.

Alice and Bob are fictional characters commonly used as placeholders in cryptographic research papers. They are important role players who symbolize the exchange of power and trust within digital systems; as Phillip Rogaway (2015, 1 [italics in original]) observes: "Cryptography rearranges power: it configures who can do what, from what. This makes cryptography an inherently *political* tool, and it confers on the field an intrinsically *moral* dimension."

Enter Satoshi Nakamoto, who, in 2008, developed the first peer-to-peer (P2P) network that enabled a new form of asset called bitcoin. Bitcoin represents a groundbreaking new asset class, where value is determined by the market, and its exchange occurs without the need for intermediaries. Instead, a decentralized P2P consensus network ensures system validation. Building on this foundation, Vitalik Buterin, an 18-year-old University of Waterloo dropout prodigy, introduced Ethereum in 2013, a blockchain that executes software code known as smart contracts (Szabo 1999), in a trustless fashion using its own cryptocurrency

1 See https://gs.statcounter.com/search-engine-market-share.

Ether (Wood 2025). Bitcoin and Ethereum blended networking technology, game theory, mechanism design and economic principles — all secured by cryptographic protocols — to radically reshape power in computing, trust, finance and social interaction through decentralization. Today, there are more than 1,000 actively traded cryptocurrency derivatives of bitcoin and Ethereum, collectively approaching a US$4 trillion market cap.[2] To address the volatility often associated with cryptocurrency prices, stablecoins have emerged as a new class of digital asset to mitigate the volatility risk by pegging their value to either to real-world benchmarks, such as the US dollar or gold, or to other cryptocurrencies algorithmically.

Distributed-ledger technologies (DLT), also referred to as *blockchain* or *Web 3.0*, offer a counternarrative to centralized cloud computing and data collection. By decentralizing data storage and system validation, DLT enhances security and transparency. Because users can access these networks directly, holding custody of their own assets, DLT vastly expands individual autonomy and enables value transfers without the need for a "central" authority. Smart contracts make money programmable by autonomously executing predefined rules. Modern layer-2 DLT solutions aid scalability and allow for microfinance to cater to IoT needs.

Decentralized finance (DeFi) disrupts the costly legacy model of traditional finance (TradFi) by offering similar services (lending/borrowing, value exchanging, yield earning, liquidity, insurance, derivatives and so on.) more cheaply and without relying on costly middlemen such as banks, brokers or centralized exchanges (Di Maggio 2024). DeFi also enables efficient *asset tokenization*, where digital tokens represent ownership of real-world assets such as real estate, stocks, bonds, art, commodities and intellectual property. By allowing fractional ownership and significantly reducing overhead costs, tokenization presents the potential to make trading and investing more accessible, reaching broader markets and promoting a level of financial inclusion and economic feasibility not efficiently available with legacy TradFi today (Carstens and Nilekani 2024).

Arguably, in TradFi, intermediaries play a critical role. They facilitate the implementation of central bank monetary policies, conduct know-your-customer (KYC) checks to prevent fraud, ensure accountability with anti-money laundering and combatting the financing of terrorism (AML/CFT) policies, and offer products that drive economic growth while maintaining market integrity. As access points, intermediaries contribute to the stability and development of the overall financial system. By contrast, DeFi operates on the self-fulfilling blockchain premises that include self-custody of assets, decentralization, transparency and universal access to the financial ecosystem, often without KYC.

Blockchains are usually pseudoanonymous, although contrary to popular belief, they do allow for the tracing of their users and transactions with proper effort. However, when cryptographic enhancements are added, either to their core technology or through specialized DeFi composable tool kits, this tracing can become intractable. This renders existing guidelines, such as the FATF travel rule, practically unfeasible. All these characteristics add significant complexity to financial regulation and law enforcement when handling elements of the Web 3.0 ecosystem. If DeFi assets become widely adopted, they risk destabilizing the monetary system, triggering financial instability and encouraging more illicit activity (Aquilina et al. 2025; Almeida et al. 2024). In addition, the points that follow are also of importance.

- Virtually all the KYC features in DeFi networks occur at the on-/off-ramps where fiat money enters/exits the ecosystem through TradFi (Duffie, Olowookere and Veneris 2025). However, the cryptographically protected trail of asset transactions and user identities, especially when combined with sophisticated cryptographic tools called mixers, greatly complicates AML/CFT sanctions and tax law enforcement.

- Most DeFi products offer virtually no customer/user protection. Unlike traditional trading systems, DeFi platforms have no central authority to intervene during crises, making contagion effects more severe. As those software protocols are usually composable, history shows that a failure in one heterogenous component (such as a malicious oracle manipulation) can cascade across others as they do not employ traditional "backstop" mechanisms (Ogbuonyalu et al. 2025).

- Blockchain products are often affiliated with jurisdictions that have lenient regulations,

2 See https://coinmarketcap.com/.

thus exhibiting jurisdictional ambiguity and regulatory arbitrage. This weakens corporate transparency and investor/user protection.

- In the hypothetical scenario that a significant portion of the economy shifts to DeFi-native assets, as noted earlier, they may weaken monetary transmission mechanisms as central banks may lose effectiveness in influencing inflation, employment and interest rates through traditional tools.

- Despite the introduction of stablecoins a decade ago, major issuers "oiling" the ecosystem still lack proper reserve audits, raising questions about their credibility (Protos Staff 2024; Crypto Anonymous 2021; Faux and Gillespie 2025). Due to their opaque nature, history shows that some stablecoins have lost their peg momentarily, or have collapsed with no recovery, causing financial harm (Korobova and Fantazzini 2024).

- Many DLT systems are not technically maintained by a central authority, and many deployed smart contracts lack formal software audits. This has resulted in financial losses for users due to bugs, hacks and malicious code. In 2024 alone, those losses exceeded US$3 billion — a 15 percent increase from 2023 (Devitt 2025).

- The transparent and immutable nature of Web 3.0 often conflicts with data protection frameworks such as the European Union's General Data Protection Regulation (Berberich and Steiner 2016).

The regulatory landscape for crypto assets varies widely across jurisdictions, reflecting geopolitical tensions and regional financial stability priorities. Singapore and Switzerland have maintained a pro-blockchain stance since the early days of its inception and introduced concise frameworks in 2018 and 2019, respectively. In January 2025, the European Union implemented the Markets in Crypto-Assets (MiCA) Regulation. Following its introduction, stablecoins that are said to lack MiCA compliance, such as Tether (USDT) and PayPal's PYUSD, now face delisting from European exchanges. The United Kingdom aims to position itself as a global hub for crypto technologies, with plans to introduce a comprehensive framework by 2025. Conversely, China introduced restrictive regulation in 2017, and although personal possession of cryptocurrencies remained legal at that time, the country fully banned any type of transactions (including trading) to protect against financial instability, capital flight and illicit activities in August 2021. More recently, in May 2025, reports indicate that China banned even the private ownership of a crypto asset (FE Business 2025). Nevertheless, in recent years, China has encouraged Web 3.0 sandboxing efforts by the Hong Kong Monetary Authority, signalling its ambitions to become a global digital asset hub.

In the United States under the Biden administration, the Securities and Exchange Commission (SEC), the Department of Justice (DoJ) and the Commodity Futures Trading Commission, among other federal agencies, set an aggressive policy against cryptocurrencies with many lawsuits for securities law violations and other claims of unlawful activities. This approach rapidly changed under the second Trump administration, first with the appointment of crypto advocate Paul Atkins as head of the SEC, and then with the issuing of a pro-crypto executive order (The White House 2025). Soon after this order, the US Congress introduced legislation (the GENIUS Act of 2025 at the Senate and the STABLE Act of 2025 at the House) that attempts to integrate the mass adoption of stablecoins into the financial-compliance framework of the Bank Secrecy Act (Massad 2025). More recently, on April 7, 2025, Deputy Attorney General Todd Blanche issued a memorandum titled "Ending Regulation by Prosecution" that indicates that the DoJ will significantly scale back its enforcement actions related to cryptocurrencies. Meanwhile, as in the United States, Canada balances innovation with regulation through a mix of federal and provincial oversight, although these efforts still seem to remain a work in progress.

In just over a decade, Web 3.0 has catalyzed transformative change across industries, evoking excitement reminiscent of the mid-1990s when the internet entered the mainstream. Dubbed the "Internet of Value(s)" (Tapscott and Euchner 2019) or the "Internet of Money" (Antonopoulos 2017), blockchain has the potential to replace legacy financial infrastructure by removing layers of intermediation. If fully realized, this promise could have profound ripple effects on privacy, national security, law/regulation, property rights, taxation, health care, diplomacy and global affairs. In this way, Web 3.0 promises to again democratize the internet, creating a more equitable and transparent digital economy.

CBDCs

Legacy payment systems remain slow, clunky and expensive (Carstens and Nilekani 2024). Consumers often receive digital services, or even physical goods, faster than merchants receive payment, and these systems were never originally designed to handle micropayments for the modern IoT economy. Similarly, in middle-/low-income countries, remittances can accelerate growth, but inefficiencies in cross-border payment systems drive their costs high when compared to costs for developed economies. In effect, this limits their social welfare impact (Rühmann et al. 2020). Similarly, studies by the Federal Reserve confirm a disparity in TradFi costs for low-income US citizens (Calem, Henderson and Wang 2025).

At the same time, the use of traditional cash by the public has been decreasing in favour of digital alternatives such as debit or credit cards and wire or electronic fund transfers. In some jurisdictions, such as Canada and Sweden, the decline has been stark (Engert, Fung and Segendorf 2019). In response to this fintech-driven digitization, central banks seek to protect their raison d'être by updating their monetary transmission channels and financial stability mechanisms, exploring the tokenization of fiat currencies through CBDCs in a quest to rediscover the very essence of fiat cash (Kosse and Mattei 2023; BIS 2020).

By way of a brief technical introduction, the literature distinguishes between *wholesale* and *retail* CBDCs. Wholesale CBDCs function as settlement mechanisms between financial institutions (FIs) for interbank transfers, typically involving large value fund transfer systems such as those handled by existing real-time gross settlement systems (RTGs). Retail CBDCs (hereafter "CBDCs" unless otherwise noted) are designed for everyday public use, and they are considered the most transformative of both kinds of digital currency, representing an evolution in how central banks can transmit monetary holdings and other policies to social welfare.

In terms of their architecture, a CBDC can be either a *one-layered (or direct)* system, in which the central bank directly manages all aspects of its life cycle (including distribution, KYC and settlement), or a *two-tiered* one. In the latter case, non-government entities such as financial institutions, payment service providers and other non-government organizations act as intermediaries for market placement, compliance, distribution and settlement, a practice that resembles the status quo for cash today. A two-tiered system can be a *hybrid* one, in which the central bank holds the CBDC ledger but distribution and payments are provided by private actors, or it can be *synthetic*, in which the private sector periodically settles underlying CBDC reserve accounts with the central bank (as in RTGs) but handles all transactions and updates of the ledger. For this reason, synthetic CBDCs share many attributes with stablecoins (Garratt and Shin 2023). Simply put, a stablecoin issuer with access to a central bank reserve account for its stablecoin reserves could be practically issuing a CBDC in all but the name.

The literature agrees that a CBDC represents the digital equivalent of a referenced fiat currency: it constitutes a digital liability of the central bank (akin to physical cash), denominated in an existing unit of account, and serving as both a medium of exchange and a store of value. Advanced economies prioritize objectives for their CBDCs differently from emerging ones, but all initiatives intersect in their goals to improve payment efficiency and security while enhancing monetary policy transmission channels. CBDCs are also envisioned to enhance financial inclusion; introduce programmability (i.e., conditional payments and automated compliance); accommodate microfinance; and bolster interoperability with other digital asset forms, including cryptocurrencies. Of particular importance is CBDCs' ability to make offline transactions without requiring network connectivity (for example, internet or cellular). This is because they need to ensure payments in remote areas with limited connectivity and during system failures (i.e., natural disasters) to cross-border visitors and minorities (i.e., those who are unbanked or who have digital accessibility challenges) (Michalopoulos et al. 2024).

The cross-border feature of this tokenized fiat money is also important in both CBDCs' wholesale and retail incarnations (Carstens and Nilekani 2024). Cross-border CBDCs, or *multiple CBDCs* (mCBDCs), generate a new set of challenges that the BIS centres around the foundations of *interoperability* and *standardization* (Auer, Haene and Holden 2021; Auer et al. 2021). Systems devised by different jurisdictions ought to communicate so that they can offer cross-currency exchanges, ensure compliance with international law and avoid

creating closed payment silos — particularly when the private sector is involved in their operation.

Arguably, the future of cross-border payments will likely hinge on a choice between mCBDCs (either through interlinked CBDC systems or a unified multi-currency mCBDC platform), or the dominance of a global private sector stablecoin. The former option gained momentum in June 2019 with the watershed announcement of Facebook's now defunct "mega-stablecoin" Libra (later Diem). The news sent shockwaves through regulators and central banks alike, largely due to Facebook's repeated history of data privacy breaches. Facebook's effort came to a halt on January 31, 2022, when the Diem association confirmed that it had sold its technology assets to Silvergate Capital Corporation in response to being under political/regulatory pressure to do so since its inception. It is against this backdrop that CBDC initiatives were put forward by monetary institutions all over the world in recent years, and why the BIS opined for mCBDCs as the preferable path forward.

The global focus on CBDCs is illuminated in the Atlantic Council's CBDC Tracker, which reports that 134 countries, representing 98 percent of the world economy, have explored digital versions of their fiat currencies.[3] The same tracker indicates that 36 countries are actively conducting CBDC pilots, collectively accounting for approximately 60–65 percent of global GDP. The Bahamas, the Eastern Caribbean Union, Jamaica and Nigeria have already launched public CBDCs. Among the Group of Twenty (G20) nations, China leads with its digital yuan (e-CNY) launched in February 2022 and now running in 29 pilot cities (Huang 2024). In May 2024, the e-CNY recorded a monthly transaction volume of about 400 billion yuan (US$56 billion) (Ledger Insights 2024). More recently it was reported that by June 2024 it had reached a total volume of nearly US$1 trillion as it gradually gets a bit more of a toehold in China (Li 2025). Notably, all sizeable members of the BRICS+ group (namely, Brazil, China, India, Iran, Russia and the United Arab Emirates [UAE]) are in the late pilot stages and/or public tests of their own CBDC projects. Announcements by the European Central Bank and the Bank of England have led to speculation about the launch of their public pilots by 2026–2027. Meanwhile, Project mBridge, a collaboration between the monetary authorities in China, Hong Kong, Thailand and the UAE, has reached a minimum viable product phase. It is also the most advanced project to explore the impact of digital fiat money on the international monetary system (IMS).

By contrast, the prospect of CBDCs in the United States and Canada has sparked heated political debates that have quashed their implementation (Shapero 2024; Omelchenko 2024). In May 2024, the US House of Representatives passed the CBDC Anti-Surveillance State Act to prohibit the Federal Reserve from issuing a retail CBDC without the authorization of Congress. Although the Senate has not advanced it yet (Emmer 2024), a recent executive order by the new administration reiterates this anti-CBDC sentiment in strong favour of private stablecoins (The White House 2025). As another bellwether, some US states have already "banned" CBDCs (Andersen 2024; Singer 2024; Ward 2024). Therefore, it is not a surprise that in May 2025, reports indicated that Facebook plans to revamp its failed Diem stablecoin effort (Schwartz and Weiss 2025). Similarly, Canada introduced Bill C-400 in July 2024 which prohibits the implementation of a CBDC by the Bank of Canada.[4] In September of that same year, the Bank of Canada, a thought leader with CBDC research widely cited by other global monetary authorities, paused its decade-long CBDC research discovery work to focus on other payment innovations.[5]

The main concern of the political forces behind the bills relates to public privacy and government overreach. Although there have been no CBDC pilots in the United States and Canada to justify such claims, critics argue that CBDCs give governments excessive "big brother" control over financial data, along with a level of public control and surveillance that could be misused to track and/or restrict personal financial activities. They allege that this fear originates from China's "e-CNY surveillance model," but no published evidence has been provided to show that the Chinese Communist Party indeed uses the e-CNY to "spy" on its people.

In essence, the argument against CBDCs is that they could erode individual freedoms and rights. Given that data is often called the "oil of the

3 See www.atlanticcouncil.org/cbdctracker/.

4 Bill C-400, *An Act to establish a framework for the continued access to and use of cash in Canada and to make related amendments to other Acts*, 1st Sess, 44th Parl, 2024 (first reading 13 June 2024), online: <www.parl.ca/documentviewer/en/44-1/bill/C-400/first-reading>.

5 See www.bankofcanada.ca/digitaldollar/.

twenty-first century," respectfully, this claim reads as an oxymoron when viewed alongside today's private "digital feudalism." It is also ironic because the same political forces that raise concerns about government overreach with CBDCs have largely failed to promote public awareness and enact adequate data protection regulations to address the private sector's vulgar control over digital products. Of course, the restrictions on banking during Canada's 2022 state of emergency, along with the United States' Operation Choke Point 1.0 and 2.0, lend a level of credibility to allegations behind potential government overreach if CBDCs materialize without the tangible cryptographic guarantees in place. At the same time, the literature indeed demonstrates how privacy-enhancing software and hardware techniques (for instance, zero-knowledge proofs, multi-party computation, trusted executed environments, secure elements and so on) can be used to provide such public guarantees that a CBDC is indeed private and yet adheres to regulation. In fact, technology today allows for such a level of privacy and anonymity akin to physical cash (Pocher and Veneris 2021; Michalopoulos et al. 2024). Clearly, this debate represents another angle of the innate conflict between privacy, anonymity, security and social egalitarianism today.

Much like Web 3.0, CBDCs raise a host of complex techno-legal questions (Veneris et al. 2021). Should e-cash and/or offline transactions preserve the anonymity of physical cash? Will CBDCs rely on government-issued digital identifications (IDs) to enable citizens to monetize their own data fairly? Who will safekeep this data, and how will it interoperate with the less regulated Web 3.0? How will these systems be governed, and how will they affect AML/CFT, financial stability, taxation, sanctions, monetary policies, social welfare and diplomacy?

The Digital Asset Privacy, Security and Anonymity Conundrum: A Geopolitical View

Privacy, security and anonymity have been cornerstones of financial autonomy, allowing individuals to transact without undue scrutiny. However, these principles also pose a paradox: while they protect freedoms and rights, they can inadvertently facilitate illicit activities. This problem lies at the centre of debates on digital assets, with interpretations varying based on the regulatory lens and the interests of the underlying actors involved.

Is security needed against government surveillance, or to guard against malicious private entities? Is anonymity utilized to protect personal data, or to facilitate fraud? Is privacy a shield for freedoms and rights, or an obstacle to law enforcement? At the individual level, "privacy" mainly involves protecting personal information such as names, addresses, phone numbers and government IDs. For corporations and institutions, it includes safeguarding transaction data such as payment amounts and patterns and counterparties. Admittedly, disclosing this information can undermine competitive and strategic interests. Further, for industries where confidentiality is critical for client obligations or legal compliance, privacy is also a requirement (Duffie, Olowookere and Veneris 2025).

Today, privacy (often safeguarded by anonymity) creates new tensions between individual freedoms, regulatory oversight and governance. In the physical world, mass surveillance carries a high cost, but in the digital realm it is inexpensive — and often profitable — as demonstrated by social media, smart devices and digital payments today. As revealed by the Federal Bureau of Investigation's COINTELPRO program in 1956, by Edward Snowden a decade ago, and by the Cambridge Analytica scandal more recently, surveillance can become a tool to suppress dissent and maintain political order. But history shows that dissent is essential for social progress. It is under this veil that cryptography emerges as a tool with profound social and political implications (Rogaway 2015).

One cannot ignore geopolitical trends before making proper determinations. Unfulfilled expectations from macroeconomic monetary and fiscal policies since the Great Recession have produced historic public debts, balance-sheet recessions in both the West and the East, "everything bubble" asset distortions, and acute income and welfare inequalities (Chancellor 2022; Piketty 2022; Koo 2014). These signs of our times — in tandem with an aging population, the degradation of the twentieth century's social systems (pensions, public education, universal health care and so on) and the rapid shift from globalization to deglobalization— all signify political upheaval. This sentiment has resulted in military expansions, unilateral geographic rearrangements that disregard post-Second World War laws and institutions, and new regional alliances. It has also promoted trade and currency wars that disrupt global value chains and leverage payment systems as tools of diplomatic coercion. Additionally, it has fuelled anti-establishment right-wing propaganda (such as elections in Austria, France, Germany, Italy and the Netherlands, and the United States' Project 2025) that is often reinforced by the same corporate leaders that profit from this new digital economy.

After all, it is not a coincidence that following the weaponization of the Society for Worldwide Interbank Financial Telecommunication and the US dollar (as a reserve currency) through sanctions against Russia in 2022, many bilateral trade and currency-swap agreements emerged between BRICS+ members (Berwick and Foldy 2024; Helms 2024; Reuters 2024; Sharma 2024; Wong 2024; Donovan and Nikoladze 2024). Such novel payment and currency channels are expected to evolve with the adoption of mCBDCs as many BRICS+ members have either launched or actively piloted CBDCs. In recent years, BRICS+ countries have also increased their gold reserves to mitigate systemic risks associated with US dollar-denominated assets, reflecting a broader effort to reduce dependence on US currency (Baccarini et al. 2024).

These trends illuminate that digital asset proliferation can reshape the financial landscape and disrupt status quos. CBDCs tied to regional blocs may bypass legacy payment systems, enabling sanctioned nations to trade with their own sovereign currencies outside the scrutiny of "policing" jurisdictions (National News Agency 2025). In effect, this will weaken sanctions, rearrange diplomacy and challenge the dominance of the existing IMS. The introduction of private "exotic" or vaguely regulated stablecoins as CBDC substitutes risks fostering unfavourable scenarios for the IMS (Massad 2025), as colloquially forewarned by Gresham's law, which holds that bad money drives out good money. Because cryptography can provide transparent guarantees for privacy-centric CBDCs and Web 3.0 assets, properly designed projects may attract foreign users, encourage currency substitution for satellite economies, destabilize monetary policies and create defacto economic dependencies.

In the context of digital value transfers, there is an inherent tension between privacy, transparency and compliance (Pocher and Veneris 2021). Nevertheless, this tension is not an either/or choice but can instead balance on a spectrum as enabled by regulation and the underlying cryptographic hardware and software primitives that tailor it. While anonymity alone does not make a transaction illicit (for instance, physical cash remains the purest form of an anonymous fungible asset), FATF has identified this trait as a "red flag" under established AML/CFT practices (FATF 2020). At the same time, in recent decades, applied cryptography has evolved to accommodate many of its promised premises. New research and development projects are expected to make more complex compliance techniques computationally feasible at scale while preserving privacy for "compliant actors'' (Duffie, Olowookere and Veneris 2025).

However, in the era of deglobalization, de-dollarization (Siqi 2025), surveillance capitalism and crypto assets, the intrinsic complexity of this trade-off has not only deepened but has also evolved into a strategic tool for power projection (Lowery 2023). International multilateral collaboration is needed not only to balance civic freedoms, privacy, social welfare and economic stability, but also to set regulation and standardization (Carstens and Nilekani 2024) that protects members of the public from state-sponsored terrorism and large-scale criminal enterprise activities while allowing them to monetize their data fairly. Achieving this requires exorbitant global political will that currently seems to be in short supply. Thus, it is likely that blocs of nations will continue forming based on strategic interests, existing global institutions will be reformed, and new institutions with regional spheres of influence will arise in a multipolar world. In this fragmented landscape, competing

blocs and/or nations are likely to capture economic or technological market share more equitably.

Privacy-preserving cryptographic tools will inevitably evolve alongside the proliferation of digital assets, with applications beyond merely protecting one's P2P/DLT transactions from prying eyes. Much of this progress will likely be made by *cypherpunks*, the early 1990s social movement that wants cryptography with "attitude and value" for the public (Levy 1993). In fact, significant innovations of Web 3.0, including bitcoin (whose creator remains unknown) were driven by cypherpunks; if they bypassed the Great Firewall of China, they are determined to bypass anything. Governments, already struggling with cryptography in communication media and Web 3.0, will be fundamentally challenged. Over time, nations may have no other option than to adopt a "good actor" last resort approach to said privacy tools as an inevitable equilibrium between utility and regulation. However, amid the turbulence in the dusk of the post-Second World War era, arriving at this approach will likely be a long, disorderly process.

Ultimately achieving a necessary balance will most likely require nothing less than a twenty-first century's "Digital Bretton Woods" to restore financial order and introduce globally accepted standards for digital assets and data protection. Within this context, it is conceivable, and probably desirable, for the International Monetary Fund's special drawing right (SDR) to re-emerge as a principal reserve asset of the IMS as envisioned in the Second Amendment to its 1978 Articles of Agreement (Veneris and Park 2019; Coats 2016; Xiaochuan 2009). This would likely require expanding the SDR's composition beyond its current basket of five currencies, which remains tied to the twentieth century's "analogue" economics, competing monetary policies, questionable fiscal strategies and Triffin's dilemma. For instance, areas of expansion could include precious metals, agricultural commodities and environmental pricing metrics. As tangible human needs change slowly over longer time horizons, such anchoring is expected to foster greater stability and promote global growth. This approach could also incorporate digital assets that are transparent, truly limited in supply but also not hoarded (causing network/wealth centralization/concentration as is what seems to be happening today (Sheridan 2025; Venturini et al. 2025; Chernoff and Jagtiani 2024) and are built on fundamentals that can earn public trust. As Friedrich Hayek said, "good money drives out bad," and such a monetary reserve standard could offer more benefits and fewer drawbacks to the defunct Bretton Woods one, including the promotion of prudent monetary and fiscal policies, fair competition, egalitarian democratic practices tailored for the digital world and public welfare.

Finally, while this discussion acknowledges the impact of global warming on all of the above, it remains agnostic on its effects. It is a known-unknown phenomenon that will inevitably add complexity due to humanity's primordial quest for natural resources.

Where Does Canada Fit in This Global Picture?

In this fluid landscape, Canada is asked to defend its monetary identity, nourish its past investment in social values, capitalize on its vast natural resources and safeguard its physical and digital boundaries. The reluctance of the United States to issue a CBDC, instead focusing on private stablecoins as a proxy, presents Canada with both unique risks and opportunities. The more notable risk is the real scenario of currency substitution being in geographic and economic proximity to the United States (Brownell 2025). On the other hand, there is also an opportunity for Canada to become the continent's digital asset hub, following the paradigms of Hong Kong, London and Singapore.

With most of the world's largest economies (in terms of GDP) actively exploring CBDCs, and with a current prime minister having been one of the premiere central bank governors globally in recent history, Canada should not only restart work on the digital Loonie but should also develop federal regulatory frameworks that prioritize privacy protection, compliance and data security for its digital currency and other Web 3.0 tools and assets. Extensively documented in literature but also confirmed by the success of the Pix payment system in Brazil and Aadhaar/Unified Payments Interface in India (Kempinsky 2025), a digital Loonie — ideally complemented with a new federal digital ID to support it — will create novel payment channels, new transactional communities

and safe networks of relations both domestically and internationally (Carstens and Nilekani 2024; Bank of Canada et al. 2020; Veneris et al. 2021).

A digital currency, coupled with a federal digital ID, has tremendous potential not only to further secure Canada's monetary identity and nourish its extensive investment in democratic social values, but also to safeguard its geopolitical digital boundaries in a competitive and fast-evolving global techno-economy. It also offers a unique opportunity to attract global users seeking financial autonomy and safe sheltering in a digital era dominated by surveillance capitalism: Canada can present them with an innovative and provenly safe alternative. Indeed, public polls on CBDCs consistently highlight the demand for strong privacy guarantees (Choi et al. 2023; European Central Bank 2021; Bank of England 2024)[6] — a paradox when contrasted with the public's willingness to share data freely with conglomerates. This anomaly underscores the need for effective outreach to the Canadian public as a necessary first step to adopting a CBDC.

Canada is well-positioned for this opportunity. It already has a seat at the table in global fora such as the Group of Seven, the G20 and the BIS's Committee on Payments and Market Infrastructures. What remains for success is political will, swift regulatory reform and leadership. After all, Ethereum was born in a basement in Toronto and then it conquered the decentralized world. Canada can repeat this same feat of digital innovation once again.

Concluding Remarks

On September 7, 2024, Bill Burns (Central Intelligence Agency director) and Richard Moore (MI6 chief) issued the first joint statement in the history of the two agencies. Among other observations, they noted: "There is no question that the international world order — the balanced system that has led to relative peace and stability and delivered rising living standards, opportunities and prosperity — is under threat in a way that we haven't seen since the cold war" (Burns and Moore 2024). Admittedly, the views expressed in this statement extend beyond the realms of the IMS, reflecting the diminishing roles of democratic awareness and egalitarian practices that underpinned the unprecedented economic prosperity of the second half of the past century.

Facing this crossroads, the current order appears to have two choices: either disregard, lobby against and contain developments to preserve the status quo, or acknowledge historical intricacies and adapt their practices. This paper posits that macroeconomic, geopolitical, technological and social trends place digital assets, decentralization and cryptography at the heart of this dilemma. It contends that the second option is the prudent approach forward.

At this juncture, it may be worthwhile to revisit the music industry at the dawn of this century (International Federation of the Phonographic Industry 2024), a sector in which the author served as a computer science student. The introduction of BitTorrent in 2001, the first widely adopted P2P medium, disrupted an industry reliant on excessive costs, numerous intermediaries and inequitable payments to artists — the source of its income. In the aftermath of BitTorrent's early adoption, the industry became preoccupied with protecting its traditional revenue streams through lawsuits against its consumers for using this new technology. Consumed by its own dogma, the industry failed to embrace innovations such as streaming, thus paving the way for visionary new players who captured market share by bringing value to all stakeholders. After massive consolidation, the legacy music industry of the 1990s has now lost half of its market cap. History confirms that misunderstanding digital P2P innovation can backfire — it is those who adapt through strategic, principled and equitable

6 See www.bankofcanada.ca/digitaldollar/a-digital-canadian-dollar-what-we-heard-2020-23-and-what-comes-next/.

practices who are ultimately best positioned to harness the full potential of digital change.

Acknowledgements

The author remains thankful to valuable comments by Andreas Park (Rotman School of Management, University of Toronto); Odunayo Olowookere (Osgoode Hall Law School, York University); and the anonymous reviewers who improved the presentation of this writing.

Works Cited

Almeida, João, Joel Alves, Carlos Bettencourt, Maria Bettencourt, Madalena Borges, Filipa Castilho, Sónia Correia et al. 2024. *Occasional Paper on Decentralised Finance*. Lisbon, Portugal: Bank of Portugal. www.bportugal.pt/sites/default/files/documents/2024-08/OP202402_0.pdf.

Andersen, Derek. 2024. "Missouri bill would ban CBDCs, make gold and silver legal tender." Cointelegraph, December 4. https://cointelegraph.com/news/missouri-cbdc-ban-gold-legal-tender-sb194.

Antonopoulos, Andreas M. 2017. *The Internet of Money Volume Two : A collection of talks by Andreas M. Antonopoulos*. Merkle Bloom LLC.

Aquilina, Matteo, Giulio Cornelli, Jon Frost and Leonardo Gambacorta. 2025. "Cryptocurrencies and decentralised finance: functions and financial stability implications." BIS Paper No. 156. April. www.bis.org/publ/bppdf/bispap156.htm.

Auer, Raphael, Codruta Boar, Giulio Cornelli, Jon Frost, Henry Holden and Andreas Wehrli. 2021. "CBDCs beyond borders: results from a survey of central banks." BIS Paper No. 116. June. www.bis.org/publ/bppdf/bispap116.pdf.

Auer, Raphael, Philipp Haene and Henry Holden. 2021. "Multi CBDC arrangements and the future of crossborder payment." BIS Paper No. 115. March. www.bis.org/publ/bppdf/bispap115.pdf.

Baccarini, Victor, Thibauld Christin, Xavier Denis and Gabrielle Labat. 2024. "How can we account for the increase in the price of gold?" Bank of France, September 13. www.banque-france.fr/en/publications-and-statistics/publications/how-can-we-account-increase-price-gold.

Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors Federal Reserve System et al.. 2020. *Central bank digital currencies: foundational principles and core features*. Report No. 1. Basel, Switzerland: BIS. www.bis.org/publ/othp33.pdf.

Bank of England. 2024. "Response to the Bank of England and HM Treasury Consultation Paper — The digital pound: A new form of money for households and businesses?" January 25. www.bankofengland.co.uk/paper/2024/responses-to-the-digital-pound-consultation-paper.

Berberich, Matthias and Malgorzata Steiner. 2016. "Blockchain Technology and the GDPR — How to Reconcile Privacy and Distributed Ledgers?" *European Data Protection Law Review* 2 (3): 422–26. https://doi.org/10.21552/EDPL/2016/3/21.

Berwick, Angus and Ben Foldy. 2024. "The Shadow Dollar That's Fueling the Financial Underworld." *The Wall Street Journal*, September 10. www.wsj.com/finance/currencies/tether-crypto-us-dollar-sanctions-52f85459?mod=hp_lead_pos10.

BIS. 2021. "CBDCs: an opportunity for the monetary system." BIS Annual Economic Report. June. In BIS Annual Economic Report 2021, 65–95. www.bis.org/publ/arpdf/ar2021e3.pdf.

Brownell, Claire. 2025. "Canada's banks are about to get hit by a trillion-dollar stablecoin tsunami." *The Logic*, July 2. https://thelogic.co/news/canada-banks-stablecoin-tsunami/.

Burns, Bill and Richard Moore. 2024. "Bill Burns and Richard Moore: Intelligence partnership helps the US and UK stay ahead in an uncertain world." *Financial Times*, September 7. www.ft.com/content/252d7cc6-27de-46c0-9697-f3eb04888e70.

Calem, Paul, Chris Henderson and Jenna Wang. 2025. "Who Remains Unbanked in the United States and Why?" Working Paper 25-02. Federal Reserve Bank Philadelphia. January. https://doi.org/10.21799/frbp.wp.2025.02.

Carstens, Agustín and Nandan Nilekani. 2024. Finternet: the financial system for the future. BIS Working Paper No. 1178. April. www.bis.org/publ/work1178.htm.

Chancellor, Edward. 2022. *The Price of Time: The Real Story of Interest*. London, UK: Penguin.

Chernoff, Alan and Julapa Jagtiani. 2024. "Beneath the Crypto Currents: The Hidden Effect of Crypto 'Whales.'" Working Paper 24-14. Federal Reserve Bank Philadelphia. August. www.philadelphiafed.org/-/media/frbp/assets/working-papers/2024/wp24-14.pdf.

Choi, Syngjoo, Bongseob Kim, Young-Sik Kim and Ohik Kwon. 2023. "Central Bank Digital Currency and Privacy: A Randomized Survey Experiment." BIS Working Paper No. 1147. November. www.bis.org/publ/work1147.htm.

Coats, Warren. 2016. "What is wrong with our monetary policy?" Center for Financial Stability, October 5. https://centerforfinancialstability.org/research/Coats_CFS_100516.pdf.

Crypto Anonymous. 2021. "The Bit Short: Inside Crypto's Doomsday Machine." Medium, January 14. https://crypto-anonymous-2021.medium.com/the-bit-short-inside-cryptos-doomsday-machine-f8dcf78a64d3.

Cuthbertson, Anthony. 2024. "Elon Musk appears to have tweaked X's algorithm to promote Trump, study claims." *The Independent*, November 4. www.independent.co.uk/tech/elon-musk-trump-x-algorithm-bias-b2640976.html.

Devitt, Conor. 2025. "Losses From Crypto Hacks and Scams Soar in 2024, Exceeding $3,010,000,000: Blockchain Security Firm." The Daily Hodl, January 10. https://dailyhodl.com/2025/01/10/losses-from-crypto-hacks-and-scams-soar-in-2024-exceeding-3010000000-blockchain-security-firm/.

Di Maggio, Marco. 2024. *Blockchain, Crypto and DeFi: Bridging Finance and Technology*. Hoboken, NJ: John Wiley and Sons.

Donovan, Kimberly and Maia Nikoladze. 2024. "The axis of evasion: Behind China's oil trade with Iran and Russia." *New Atlanticist* (blog), March 28. www.atlanticcouncil.org/blogs/new-atlanticist/the-axis-of-evasion-behind-chinas-oil-trade-with-iran-and-russia/.

Duffie, Darrell, Odunayo Olowookere and Andreas Veneris. 2025. "A Note on Privacy and Compliance for Stablecoins." SSRN, May 7. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5242230.

Emmer, Tom. 2024. "Emmer's Flagship CBDC Anti-Surveillance State Act Passes House of Representatives." Press release, May 23. https://emmer.house.gov/media-center/press-releases/emmer-s-flagship-cbdc-anti-surveillance-state-act-passes-house-of-representatives.

Engert, Walter, Ben Fung and Björn Segendorf. 2019. "A Tale of Two Countries: Cash Demand in Canada and Sweden." Bank of Canada Staff Discussion Paper 2019-7. August. www.bankofcanada.ca/2019/08/staff-discussion-paper-2019-7.

European Central Bank. 2021. "ECB publishes the results of the public consultation on a digital euro." Press release, April 14. www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210414~ca3013c852.en.html.

FATF. 2020. *Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets.* FATF Report. September. Paris, France: FATF.

www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html.

Faux, Zeke and Todd Gillespie. 2025. "Commerce Nominee Lutnick Is Backer of Outlaws' Favorite Cryptocurrency." Bloomberg, January 18. www.bloomberg.com/news/features/2025-01-18/trump-commerce-nominee-lutnick-is-backer-of-outlaws-favorite-cryptocurrency.

FE Business. 2025. "China imposes fresh ban on holding crypto, including Bitcoin: Report." May 30. www.financialexpress.com/market/cryptocurrency/china-imposes-fresh-ban-on-holding-crypto-including-bitcoin-report/3862209/.

Garratt, Rodney and Hyun Song Shin. 2023. "Stablecoins versus tokenised deposits: implications for the singleness of money." BIS Bulletin No. 73. April 11. www.bis.org/publ/bisbull73.pdf.

Helms, Kevin. 2024. "China and Russia Push for Increased Local Currency Use in Trade, Deepen BRICS Cooperation." Bitcoin.com, August 23. https://news.bitcoin.com/china-and-russia-push-for-increased-local-currency-use-in-trade-deepen-brics-cooperation/.

Huang, Roger. 2024. "A 2024 Overview Of The E-CNY, China's Digital Yuan." *Forbes*, July 15. www.forbes.com/sites/digital-assets/2024/07/15/a-2024-overview-of-the-e-cny-chinas-digital-yuan/.

International Federation of the Phonographic Industry. 2024. *Global Music Report 2024: State of the Industry*. https://ifpi-website-cms.s3.eu-west-2.amazonaws.com/IFPI_GMR_2024_State_of_the_Industry_db92a1c9c1.pdf.

Kempinsky, Polina. 2025. "Learning from Brazil and India's Instant Payment Systems." Working Paper No. 254. Mossavar-Rahmani Center for Business and Government. May. www.hks.harvard.edu/centers/mrcbg/publications/awp/awp254.

Koo, Richard C. 2014. *The Escape from Balance Sheet Recession and the QE Trap: A Hazardous Road for the World Economy*. Singapore: John Wiley & Sons.

Korobova, Elena and Dean Fantazzini. 2024. "Stablecoins and credit risk: when do they stop being stable?" Munich Personal RePEc Archive Paper No. 122951. December 15. https://mpra.ub.uni-muenchen.de/122951/1/MPRA_paper_122951.pdf.

Kosse, Anneke and Ilaria Mattei. 2023. "Making headway – Results of the 2022 BIS survey on central bank digital currencies and crypto." BIS Paper No. 136. July. www.bis.org/publ/bppdf/bispap136.pdf.

Ledger Insights. 2024. "Digital RMB transaction volumes hit $56 billion for one month." September 6. www.ledgerinsights.com/digital-rmb-transaction-volumes-hit-56-billion-for-one-month/.

Levy, Steven. 1993. "Crypto Rebels." *Wired*, Februrary 1. www.wired.com/1993/02/crypto-rebels/.

Li, Alice. 2025. "The world is going all in on stablecoins. Is China's digital yuan any different?" *South Morning China Post*, July 2. www.scmp.com/economy/china-economy/article/3316651/world-going-all-stablecoins-chinas-digital-yuan-any-different.

Lowery, Jason P. 2023. "Softwar: A Novel Theory on Power Projection and the National Strategic Significance of Bitcoin." Master's thesis, Massachusetts Institute of Technology. https://dspace.mit.edu/handle/1721.1/153030.

Majid, Aisha. 2023. "Search vs social: How referral traffic to news sites has changed in five years." *Press Gazette*, April 13. https://pressgazette.co.uk/media-audience-and-business-data/media_metrics/news-referral-traffic-breakdown/.

MarketMeChina. 2024. "Baidu search engine market share in China Nov 2024." December 5. www.marketmechina.com/baidu-search-engine-market-share-in-china-nov-2024/.

Massad, Timothy G. 2025. "The Golden Age of Digital Assets: Charting a Path Forward." Testimony before the Subcommittee on Digital Assets, Financial Technology and Artificial Intelligence of the Committee on Financial Services, US House of Representatives. February 11. https://docs.house.gov/meetings/BA/BA21/20250211/117872/HHRG-119-BA21-Wstate-MassadT-20250211.pdf.

Michalopoulos, Panagiotis, Odunayo Olowookere, Nadia Pocher, Johannes Sedlmeir, Andreas Veneris and Poonam Puri. 2024. "Compliance Design Options for Offline CBDCs: Balancing Privacy and AML/CFT." Osgoode Legal Studies Research Paper No. 4770513. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4770513.

Mullins, Brody. 2015. "Google Makes Most of Close Ties to White House." *The Wall Street Journal*, March 24. www.wsj.com/articles/google-makes-most-of-close-ties-to-white-house-1427242076.

Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin.org. https://bitcoin.org/bitcoin.pdf.

National News Agency. 2025. "Chair's Statement — Meeting of Ministers of Foreign Affairs/International Relations of BRICS Member Countries." May 1. https://nna-leb.gov.lb/en/politics/776607/chair-s-statement-meeting-of-ministers-of-foreign.

Nolan, Beatrice. 2024. "The tech industry wants to create an an AI utopia. Its leaders think Universal Basic Income is the answer." Business Insider, July 30. www.businessinsider.com/ubi-universal-basic-income-ai-risks-destroying-jobs-solutions-2024-7.

Ogbuonyalu, Uchenna Obiageli, Kehinde Abiodun, Selorm Dzamefe, Ezeh Nwakaego Vera, Adewale Oyinlola and Igba Emmanuel. 2025. "Integrating Decentralized Finance Protocols with Systemic Risk Frameworks for Enhanced Capital Markets Stability and Regulatory Oversight." *International Journal of Innovative Science and Research Technology* 10 (4): : 762–77. https://doi.org/10.38124/ijisrt/25apr1165.

Omelchenko, Denis. 2024. "Trudeau's rival pushes to ban CBDC in Canada, preserves cash use." crypto.news, August 12. https://crypto.news/trudeaus-rival-pushes-to-ban-cbdc-in-canada-preserves-cash-use/.

Piketty, Thomas. 2022. *A Brief History of Equality*. Cambridge, MA: Harvard University Press.

Pilkington, Ed. 2025. "Elon Musk's Doge team granted 'full access' to federal payment system." *The Guardian*, February 2. www.theguardian.com/technology/2025/feb/02/elon-musk-doge-access-federal-payment-system.

Pocher, Nadia and Andreas Veneris. 2021. "Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme." *IEEE Transactions on Network and Service Management* 19 (2): 1776–88. https://doi.org/10.1109/TNSM.2021.3136984.

Protos Staff. 2024. "Tether: Ten years, 100,000,000,000 USDT, and still no audit." Protos, March 5. https://protos.com/tether-ten-years-100000000000-usdt-and-still-no-audit/.

Reuters. 2024. "Russia, China find payments workaround as US sanctions net widens, sources say." June 20. www.reuters.com/world/russia-china-find-payments-workaround-us-sanctions-net-widens-sources-say-2024-06-20/.

Rogoff, Phillip. 2015. "The Moral Character of Cryptographic Work." Paper 2015/1162. https://eprint.iacr.org/2015/1162.

Rühmann, Friederike, Sai Aashirvad Konda, Paul Horrocks and Nina Taka. 2020. "Can blockchain technology reduce the cost of remittances?" OECD Development Co-operation Working Paper No. 73. April. Paris, France: OECD. https://doi.org/10.1787/d4d6ac8f-en.

Schwartz, Leo and Ben Weiss. 2025. "Exclusive: Meta in talks to deploy stablecoins three years after giving up on landmark crypto project." *Fortune*, May 8. https://fortune.com/crypto/2025/05/08/meta-stablecoins-exploration-usdc-circle-diem-libra/.

Shapero, Julia. 2024. "Trump vows to block creation of digital dollar." *The Hill*, January 18. https://thehill.com/business/4416139-trump-vows-to-block-creation-of-digital-dollar.

Sharma, Ritu. 2024. "Loaded With Massive Reserves Of Rupees In Indian Banks, Russia Buys 'Sensitive' Goods From New Delhi Despite Embargo — Reports." *The EurAsian Times*, September 6. www.eurasiantimes.com/ne-loaded-with-massive-reserves-of-rupees/.

Sheridan, Eamonn. 2025. "58 wallets made over $10 million each from Trump's meme coin vs. 764,000 wallets that lost." Forexlive, June 5. www.forexlive.com/Cryptocurrency/58-wallets-made-over-10-million-each-from-trumps-meme-coin-vs-764000-wallets-that-lost-20250506/.

Singer, Andrew. 2024. "North Carolina resists the CBDC tide with new payments ban." Cointelegraph, September 13. https://cointelegraph.com/news/north-carolina-cbdc-ban-law-us.

Siqi, Ji. 2025. "Trump's threats will only drive countries away from US dollar, economists warn at Davos." *South China Morning Post*, January 22. www.scmp.com/economy/global-economy/article/3295754/trumps-threats-will-only-drive-countries-away-us-dollar-economists-warn-davos.

Szabo, Nick. 1999. "Formalizing and Securing Relationships on Public Networks." http://myinstantid.com/szabo.pdf.

Tapscott, Don and Jim Euchner. 2019. "Blockchain and the Internet of Value: An Interview with Don Tapscott." *Research Technology Management* 62 (1): 12–19. www.jstor.org/stable/26586510.

The White House. 2025. "Strengthening American Leadership in Digital Financial Technology." Executive Order, January 23. www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/.

Veneris, Andreas and Andreas Park. 2019. "Special Drawing Rights in a New Decentralized Century." *arXiv*, June 25. https://arxiv.org/abs/1907.11057.

Veneris, Andreas, Andreas Park, Fan Long and Poonam Puri. 2021. "Central Bank Digital Loonie: Canadian Cash for a New Global Economy." Osgoode Legal Studies Research Paper. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3770024.

Venturini, Marco, Daniel García-Costa, Elena Álvarez-García, Francisco Grimaldo and Flaminio Squazzoni. 2025. "Mapping network structures and dynamics of decentralised cryptocurrencies: The evolution of Bitcoin (2009–2023)." *arXiv*, January 20. https://arxiv.org/abs/2501.11416.

Ward, Susie Violet. 2024. "Louisiana Passes Bill To Defend Bitcoin Rights And Ban CBDCs." *Forbes*, June 24. www.forbes.com/sites/digital-assets/2024/06/24/louisiana-passes-bill-to-defend-bitcoin-rights-and-ban-cbdcs/.

Weissberger, Alan. 2022. "Sandvine: Google, Facebook, Microsoft, Apple, Amazon & Netflix generate almost 57% of Internet traffic." *IEEE ComSoc Technology Blog*, February 1. https://techblog.comsoc.org/2022/02/01/sandvine-google-facebook-microsoft-apple-amazon-and-netflix-generate-almost-57-of-internet-traffic/.

Wong, Kandy. 2024. "Saudi Arabia 'open' to petroyuan, closer China ties, minister says." *South China Morning Post*, September 9. www.scmp.com/economy/global-economy/article/3277788/saudi-arabia-open-petroyuan-closer-china-ties-minister-says.

Wood, Gavin. 2025. "Ethereum: A Secure Decentralised Generalised Transaction Ledger." Yellow Paper. January 4. https://ethereum.github.io/yellowpaper/paper.pdf.

Xiaochuan, Zhou. 2009. "Reform the international monetary system." BIS Review 21/2009. March 23. www.bis.org/review/r090402c.pdf.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY: PublicAffairs.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org