THE INTERNATIONAL JOURNAL OF BLOCKCHAIN LAW

Volume 15

August 2026

GBBC
Global Blockchain
Business Council


GBBC
Global Blockchain
Business Council

TABLE OF CONTENTS

NOTE FROM THE EDITOR-IN-CHIEF

DR. MATTHIAS ARTZT
SENIOR LEGAL COUNSEL, DEUTSCHE BANK
GERMANY

In this fifteenth edition of the IJBL, we highlight a diverse set of blockchain- and crypto-related developments across the United States and Türkiye.

We open with an article by Tom Morberg and Angela Angelovska-Wilson from DLx Law in Washington, who examine identity-infrastructure challenges in DeFi and digital commerce. At the core lies a fundamental tension: how participants in a DeFi ecosystem can verify the information required for legal compliance without collecting more personal data than a transaction truly demands. The authors advocate for decentralized identity frameworks, portable credentials, selective disclosures, and privacy-preserving proofs - rather than turning every DeFi participant into yet another identity gatekeeper. They emphasize the importance of distinguishing between verifying identity itself and verifying an attribute derived from identity. Their conclusion is clear: decentralized identity cannot be scaled unless legal and regulatory policy gives credentials and proofs predictable legal effect.

Next, Dave Hirsch, Ray Villani and Chelsea Smith Press from McGuireWoods in Washington explore the emerging intersection of crypto and agentic AI. They shed light on the question of who bears sanctions liability when a malicious prompt injection causes an AI agent to send crypto assets to a sanctioned address. Addressing this issue will require bespoke governance programs - particularly because it also affects insurance coverage for companies deploying AI agents. Stablecoins are well positioned to prevail in this space: they operate 24/7, natively support micropayments and transfers, and can maintain their own wallets. The downside, however, is that the systems connecting AI agents to underlying AI models are already becoming targets for cyberattacks.

We then turn to an article by Begüm Ergin and Elcin Karatay of Solak & Partners in Istanbul, who discuss the regulatory framework envisioned for the taxation of crypto assets under Turkish law. They focus especially on how taxation of crypto-asset transactions will affect CASPs, which are treated as taxpayers under the proposed regime.

Chief Risk & Compliance Officer Debra Brookes from Wyoming Stable Token Commission provides an overview of Wyoming´s commitment to blockchain innovation. The state of Wyoming became the first government entity in the world to issue a fully reserved, fiat-backed stable coin. Debra traces the history and vision behind Wyoming's choice, from its pioneering blockchain legislation through enactment of the Wyoming Stable Token Act and examines the resulting public issuer model and its implications.

Finally, we close this edition with the event recap of the GBBC & Norton Rose Fulbright 2026 Future of Finance Conference in London which features a series of great panel discussions and keynotes touching on “Multi-money future – stablecoins, tokenized deposits and the new payment stack”; “Tokenization at scale – from sandboxes to settlement infrastructure”; “Securing digital assets – custody, wallets and institutional readiness”; and “Agentic finance – when AI agents move money”.

Happy reading!

Dr. Matthias Artzt
Editor-in-Chief

ABOUT THE CO-EDITORS

DAVID L. HIRSCH

PARTNER, MCGUIREWOODS

WASHINGTON, DC, USA

Dave is a highly respected member of the securities enforcement and regulatory counseling practice group at McGuireWoods, where he plays a key role shaping the strategic direction of the firm's securities enforcement initiatives. With a robust practice that spans a wide array of complex regulatory and enforcement matters, Dave is recognized for his deep experience and keen insights, particularly navigating the intricacies of securities law.

LOCKNIE HSU

PROFESSOR, SINGAPORE MANAGEMENT UNIVERSITY

SINGAPORE

Locknie Hsu received her legal training at the National University of Singapore and Harvard University, and is a member of the Singapore Bar. Locknie specializes in international trade and investment law, including areas such as paperless trade, FTAs, digital commerce, and business applications of technology.

ELÇIN KARATAY

MANAGING PARTNER, SOLAK&PARTNERS LAW FIRM

ISTANBUL, TÜRKIYE

Elçin Karatay, is a partner at Solak&Partners Law Firm, who specializes in corporate law, commercial law and IP law with a keen focus on technology and Fintech sectors. She advises local and international clients on agreements, regulatory aspects of IT law and M&As, particularly within tech-driven domains. Elçin works intensively on creating legal structures for new technological developments including blockchain.

STEPHEN D. PALLEY

PARTNER, BROWN RUDNICK

WASHINGTON, DC, USA

Stephen Palley is a litigation partner and co-chair of Brown Rudnick's Digital Commerce group. He has deep technical and U.S. regulatory knowledge, particularly in the digital asset space, and assists clients working on the frontiers of technology, including on deal work for blockchain and other technology enterprises.

NINA MOFFATT

PARTNER, PAUL HASTINGS

LONDON, UK

Nina Moffatt is a partner in the London office of Paul Hastings providing legal and commercial advice on regulatory requirements across Europe. She has particular expertise in large cross border offerings and product design. She also regularly assists clients with their relations with the U.K. regulators, including applications for authorization and supervisory issues.

JAKE VAN DER LAAN

CO-AUTHOR, "HANDBOOK OF BLOCKCHAIN LAW"; BARRISTER AND SOLICITOR

NEW BRUNSWICK, CANADA

Jake van der Laan teaches within the Faculty of Computer Science at the University of New Brunswick, Canada and served as the Director, Information Technology and Regulatory Informatics and the Chief Information Officer with the New Brunswick Financial and Consumer Services Commission (FCNB). Prior to joining FCNB he was a trial lawyer for 12 years, acting primarily as plaintiff's counsel.

GARY D. WEINGARDEN

CHIEF PRIVACY OFFICER, PROOF

BOSTON, MA, USA

Gary Weingarden is the Chief Privacy Officer at Proof. Gary has multiple certifications in privacy, security, compliance, ethics, and fraud prevention from IAPP, ISC2, ISACA, SCCE, and the IACFE, among others. Before joining Proof, Gary was the Chief Privacy Officer and Director of IT Security Compliance at Tufts University, and served as Data Protection Officer for Notarize and Senior Counsel at Rocket Mortgage.

ARTICLE I

DEFI AND DIGITAL COMMERCE NEED BETTER IDENTITY INFRASTRUCTURE, NOT MORE GATEKEEPERS

TOM MOMBERG
ATTORNEY
DLX LAW

ANGELA ANGELOVSKA-WILSON
MANAGING PARTNER
DLX LAW

Digital commerce increasingly depends on trust between parties that might never meet, use the same intermediary, or share a common legal system. That is true for digital assets and decentralized finance ("**DeFi**"), and it is also true for payments, online marketplaces, software platforms, digital credentials, remote work, artificial intelligence tools, creator platforms, and B2B commerce. In each of these settings, the same question keeps recurring: how can parties verify enough information to comply with law and manage risk without collecting more personal information than the transaction requires? In this article, we argue that lawmakers and regulators should answer this question by supporting and preferring decentralized identity frameworks, portable credentials, selective disclosure, and privacy preserving proofs before ever considering turning a merchant, servicer, or infrastructure provider into yet another identity gatekeeper.

Historically, the first instinct of a regulatory agency has often been to treat compliance uncertainty by requiring information collection. In the traditional financial system, banks and other intermediaries, generally must identify customers, monitor activity, screen against sanctions, and file reports. That model remains necessary where an institution controls the customer relationship, custody, settlement, or financial flows. It does not follow, however, that every digital product or software layer, should become an identity checkpoint.

Financial crimes and sanctions laws should prevent illicit finance, preserve market integrity, and deny lawful channels to sanctioned persons, fraudsters, and other illicit actors. They should not maximize the number of private databases containing things like identity documents, home addresses, tax identifiers, biometrics, beneficial ownership records, wallet histories, or source of funds narratives. The distinction matters because identity data has become a risk asset in and of itself.

Data breaches at public and private institutions have reached record levels, and financial services remain among the sectors most frequently affected. Governments increasingly treat bulk sensitive personal data as a national security issue, not merely as a privacy issue.

New AI tools have also changed the cybersecurity risk environment: Anthropic's Project Glasswing and Claude Mythos Preview show that advanced models can help identify serious software vulnerabilities across important systems, which might help defenders secure critical infrastructure but also shows why vulnerability discovery and exploitation are likely to keep getting faster, cheaper, and more automated.

In this environment, a legal framework that forces more entities to collect and retain more identity data is not the conservative approach. The legal and policy question is whether modern compliance can verify the facts that matter while collecting, retaining, and exposing less.

LEGAL RESPONSIBILITY SHOULD FOLLOW FUNCTION AND CONTROL

A better framework should separate the legal obligation to comply from the technical role of standing between parties to a transaction. Sanctions laws, financial crimes compliance rules, fraud controls, export controls, tax reporting regimes, and platform integrity requirements often require confidence about a counterparty, location, authority, eligibility, transaction purpose, or risk profile. In the traditional financial system, a regulated intermediary often provides that confidence because it controls the account, custodied assets, payment rail, order flow, settlement process, or reporting channel. Many digital commerce interactions do not require that kind of intermediary control for the transaction to occur, however.

For example, natural persons and organizations alike must individually comply with sanctions regimes in any jurisdiction to which they are subject, even when a transaction does not involve a bank or other regulated financial intermediary.

As digital transactions increasingly occur through software, marketplaces, wallets, smart contracts, stablecoins, and other digital infrastructure, commercially viable systems will need ways for users and counterparties to avoid prohibited dealings without assuming that a bank or other conventional intermediary will always perform the screening function.

Many digital commerce and DeFi transactions involve regulated actors, including payment processors, custodians, exchanges, stablecoin issuers, broker-dealers, banks, money transmitters, and other financial institutions. Many others do not. The legal framework should distinguish between those cases rather than treating every verification question as a reason to collect a complete identity file. Some interactions require full regulated financial institution controls, whereas others require narrower tools, such as eligibility verification, sanctions assurance, fraud screening, corporate authority checks, or transaction monitoring.

More extensive financial crimes compliance obligations attach to defined classes of regulated actors because of the functions those actors perform. A person might fall within this perimeter if it takes custody, administers a payment service, controls transaction execution, operates a regulated exchange, or manages financial customer relationships. Even then, the information collected should be tied to the applicable legal obligation, the risk profile, and the compliance purpose, rather than to a generalized preference for collecting more data.

By contrast, a person that publishes software, provides a communications layer, validates network activity, offers a noncustodial digital asset wallet, or maintains neutral infrastructure should not be treated as a regulated intermediary merely because a visible party would be easier to supervise.

Nor should such a person be required to collect identity information merely to expand the amount of data available somewhere in the transaction, especially when doing so increases the breach risk surface without meaningfully improving compliance work already performed by other parties.

FIRMS SHOULD COLLECT INFORMATION BASED ON COMPLIANCE PURPOSE, RISK, AND AVAILABLE ALTERNATIVES

The law should therefore ask two questions in sequence. First, when a person performs a regulated function, what information must that person collect, verify, or retain to satisfy applicable sanctions, financial crimes, and related compliance obligations in light of the relevant risk? Second, where no actor performs a regulated function, what assurance tools should the law recognize so that users, counterparties, platforms, and regulated institutions can transact responsibly without unnecessary identity disclosure?

The answer to the first question cannot be determined by hindsight or by a rigid minimum data rule. Compliance teams often collect more information because risk can be uncertain, regulators often only review decisions after the fact, and firms need defensible records showing how they reached a compliance determination. The policy response should not be to criticize risk based judgment but to give firms legally reliable alternatives to duplicative data collection when those alternatives provide equal or better assurance.

Compliance departments already broadly try to calibrate information requests based on customer type, product risk, transaction purpose, geography, sanctions exposure, and other relevant factors. The problem is that existing law and supervisory practice often make possession of the underlying file feel safer than reliance on a credential, attestation, or proof.

Lawmakers and regulators should therefore focus on when a firm has obtained reliable evidence of the legally relevant fact, not merely on whether the firm collected the familiar documents themselves.

This distinction will matter more as regulated activity moves into digital commerce infrastructure. Payment services, stablecoin issuers, tokenized asset platforms, marketplaces, and digital financial applications may have real compliance obligations while still being able to satisfy some of them through portable credentials, issuer attestations, revocation checks, or privacy preserving proofs. If a customer has completed due diligence with a certified issuer, a regulated actor should be able to rely on a credential proving the relevant status when the law, assurance level, and risk profile support that reliance.

For higher risk activity, direct collection and review of underlying records might remain necessary. For lower risk activity, or for recurring verification of a narrow fact, a credential or proof is most often going to be more accurate, efficient, and secure than another copy of the same identity documents, and the legal framework should make room for that distinction.

The second question concerns digital interactions where no actor performs a regulated financial function or exercises sufficient control to justify direct AML or sanctions obligations. These interactions might involve marketplaces that do not custody funds, software tools that users operate independently, noncustodial wallets, decentralized protocols, or other infrastructure that supports transactions without controlling them.

The absence of a regulated-intermediary does not eliminate the need for assurances. Users and counterparties will likely still need to avoid illicit actors, and legal frameworks should therefore recognize tools that allow responsible participation without forcing neutral software or infrastructure providers into the role of information intermediaries. Depending on the context, these tools might include verifiable credentials, trusted third-party attestations, revocation registries, wallet screening, or zero knowledge proofs.

This approach would allow digital commerce to develop assurance layers without creating more unnecessary gatekeepers. If a party relies in good faith on a certified credential or proof that satisfies defined legal requirements, then the law should give that reliance legal effect. Without such recognition, prudent actors will likely continue to demand full identity files even when narrower proofs would answer the relevant compliance question.

DIGITAL IDENTITY SYSTEMS SHOULD VERIFY ATTRIBUTES WITHOUT BECOMING SURVEILLANCE INFRASTRUCTURE

Decentralized identity systems and related legal frameworks should distinguish between verifying identity and verifying an attribute derived from identity. For example, a person should be able to prove they are outside a prohibited jurisdiction without disclosing a home address, that they meet an age or professional status requirement without disclosing unrelated information, or that a screening credential remains valid without requiring every relying party to maintain a KYC file.

This distinction is already reflected by the EU's Digital Identity Wallet framework, which is built around reusable credentials and selective disclosure. The EU framework also shows why design choices matter.

Digital identity can reduce repeated disclosure, but it can also become a profiling or surveillance layer if credentials are linkable across unrelated services, relying parties request more information than needed, or wallet providers, issuers, or platforms can observe user activity across contexts.

Any legal framework supporting decentralized identity should require data minimization, selective disclosure, purpose limitation, revocation, issuer accountability, and limits on relying party reuse. These safeguards should apply regardless whether the system is public, private, decentralized, or hybrid. The goal is to make minimized disclosure the preferred commercial practice.

The framework should also preserve lawful compliance and review. Regulated actors still need to satisfy applicable financial crimes compliance obligations, and authorities still need access to appropriate information through lawful channels. The goal is to adopt the narrowest proof that satisfies the relevant legal question or risk threshold while treating privacy and auditability as compatible design requirements.

POLICYMAKERS SHOULD GIVE DECENTRALIZED IDENTITY LEGAL EFFECT THROUGH RELIANCE RULES, STANDARDS, AND SAFE HARBORS

Decentralized identity will not scale unless legal and regulatory policy gives credentials and proofs predictable effect. Participants in DeFi and digital commerce need to know when they may rely on a credential, attestation, revocation check, wallet risk signal, or zero knowledge proof. Without clear reliance rules, prudent actors will in many cases continue to collect full identity files because that remains the safer supervisory posture and a familiar commercial practice.

Rules, whether established by law, regulation, contract, or firm policy, should define assurance levels based on the underlying compliance purpose.

A proof of age should not be treated the same as enhanced diligence for a high-risk corporate customer, just as a sanctions credential refreshed daily should not be treated the same as an identity credential issued a year earlier. Standards must address everything from issuer qualification, source data, verification method, refresh period, revocation, audit rights, liability, fraud controls, and error correction.

A strong framework should also preserve distinctions among related compliance functions. Verification, screening, monitoring, reporting, and lawful information access might require different information and different responsible actors. Proof that a person completed diligence does not prove that a particular transaction is lawful, and proof that a wallet has not been flagged does not establish beneficial ownership. Lawmakers should assign each obligation to the actor best positioned to perform it and should allow credential-based compliance where it satisfies the underlying legal purpose.

The most useful reforms would be practical: recognize certified credentials and privacy-preserving proofs, establish issuer and verifier standards, create safe harbors for good faith reliance, require revocation and refresh mechanisms, prohibit unnecessary reuse or linkage, and clarify when credential-based systems can satisfy existing compliance obligations. These reforms would not weaken regulatory compliance or platform integrity objectives but instead give firms a legally recognized way to verify the right fact without creating another unnecessary repository of sensitive information.

The policy choice is not between gatekeepers and lawlessness. It is between a compliance model that multiplies identity databases and one that verifies necessary facts with less exposure. For digital commerce, blockchain, and DeFi infrastructure, the second model is more efficient, more secure, and better aligned with the purposes of the laws imposing certain compliance obligations on regulated and non-regulated actors alike.

Acknowledgements: *The authors would like to thank their fellow DLx Law team members Diana Stern and William Miller for their valuable input and assistance in preparing this chapter.*

Disclaimer: *Importantly, the content of this article is for informational purposes only and is not legal advice, business advice, or other advice of any kind. Additionally, the technical concepts and legal structures relevant to digital identity and digital commerce are likely to continue to evolve just as well as they have up until the date of this article. The views expressed by the authors, and the policies for which they advocate, are based on their own opinions and do not necessarily represent the interests or positions of any DLx Law clients. Should not be interpreted as unwavering or as attributable to other persons and organizations across the industry, including those who may have helped influence or support the production of this chapter.*

ARTICLE II

THE FOUR-PILLAR FRAMEWORK

DAVID L. HIRSCH
PARTNER
MCGUIREWOODS LLP

RAY VILLANI
ASSOCIATE
MCGUIREWOODS LLP

CHELSEA SMITH PRESS
ASSOCIATE
MCGUIREWOODS LLP

ON THE CONVERGENCE OF ARTIFICIAL INTELLIGENCE AND CRYPTO — AND WHY REGULATORS, CISOS, AND GENERAL COUNSEL SHOULD BE WATCHING THE SEAMS

The convergence of agentic AI and crypto may create a new commercial substrate beneath the internet, one in which software pays software, settlement is instantaneous and irreversible, and the human principal sits several logical layers away from the transaction itself. The implications are simultaneously mundane and profound, and they break along four fault lines: commercial logic, micropayment economics, cybersecurity and permissioning, and regulatory architecture. Each deserves to be taken on its own terms.

I. THE LOGIC: INTERNET AGENTS NEED INTERNET MONEY

Traditional payment rails were designed for human commerce, with financial institutions required to gather know your customer ("KYC") information tied to unique human identity through government identification, biometrics, date of birth, and other characteristics. Because those requirements depend on human attributes, autonomous agents typically cannot yet open a bank account; neither government-issued identification nor can satisfy KYC requirements from traditional financial institutions. Yet to become truly useful, agents will increasingly be expected to transact: to book flights, call APIs, negotiate with counterparty agents, and settle in real time.

Stablecoins resolve this mismatch as if by design. They offer the programmability of crypto without the price volatility that would make autonomous financial decisions unreliable. Much of that activity will not look like a single high-value purchase such as a flight booking, but a rapid sequence of small calls (querying a data feed, invoking another agent, paying per inference) and currency volatility is dangerous at that frequency. For an agent executing hundreds of micropayments per hour, a five-percent swing in the underlying currency would be catastrophic; a dollar-pegged token resolves that. The crypto payment rails are also fundamentally compatible with software: composable, atomic, 24x7, and able to settle on conditions expressed in code rather than in a contract.

The market has validated this thesis with startling speed. As of late April 2026, roughly 69,000 active AI agents on Coinbase's x402 protocol had processed over 165 million transactions totaling approximately $50 million in volume. The protocol itself is conceptually modest. It revives the long-dormant HTTP 402 "Payment Required" status code, an artifact of the original 1991 HTTP protocol that envisioned a "pay-to-access" internet instead of the ad supported internet that followed. It turns any REST endpoint, static URLs used to interact with website databases, into a metered, machine-payable service. An agent requests a resource, receives a 402 response specifying price and recipient, signs a stablecoin transaction, and immediately receives the response. No API keys. No monthly invoicing. No chargebacks.

What gives this architecture weight is not the protocol technical standards, but the coalition that has lined up behind it. The x402 Foundation, incubated under the Linux Foundation, counts among its backers Google, Mastercard, Visa, Cloudflare, Shopify, Stripe, Amazon Web Services, the Solana Foundation, and KakaoPay. When the incumbents of the card networks and the hyperscalers of cloud infrastructure agree on the shape of a rail, the rail tends to get built.

An agent transacting in fiat is an agent asking permission. An agent transacting in stablecoins is an agent executing.

II. MICROPAYMENTS: THE THIRTY-YEAR-OLD IDEA THAT FINALLY HAS ITS BUYER

Micropayments are not a new idea. Ted Nelson proposed transcopyright micropayments in the 1960s to compensate copyright holders. The dawn of the internet saw successive attempts at digitizing micropayments — DigiCash, Millicent, CyberCash, Flooz, Beenz — each of which failed. Clay Shirky's 2000 essay "The Case Against Micropayments" correctly diagnosed the reason: the barrier was not transaction cost but mental transaction cost.

Humans already make hundreds of decisions a day, piling on hundreds of additional micro-decisions, each only worth a few cents, was not a product the market wanted, even if technology advancements made it commercially feasible. The cognitive overhead of deciding whether a piece of content was worth $0.03 dwarfed the price itself.

This is the point at which agents change the equation. An agent can make those low-value, high-volume decisions within boundaries set by users, without consultation, with real-time and periodic reporting. Another agent can monitor for pattern anomalies and outlier transactions in the interim. The cognitive tax that killed every prior micropayment attempt simply evaporates when the buyer is not a human.

The commercial implications are substantial. Stablecoin transaction volume reached roughly $33 trillion in 2025, up 72 percent year over year, with aggregate supply surpassing $300 billion. The more telling statistic is mix: in the current environment, everyday-commerce retail use remains a small slice of stablecoin activity. The European Central Bank has cited estimates suggesting only about half a percent of stablecoin volume consists of organic retail-sized transfers. That gap is precisely what agentic commerce is positioned to close. Fully automated payments made per API call, per task, or per inference may challenge subscription and advertisement driven revenue models.

It bears noting that daily snapshots show approximately 131,000 x402 transactions generating only around $28,000 in volume, at an average payment of twenty cents. While parties work through technology adoption, the rails are being laid and the historical precedent is instructive. Stripe's volume in 2011 was a rounding error relative to Visa's; the question was never about the month-over-month transaction count but about the pace at which developer-native payment rails can compound.

The missing ingredient in thirty years of micropayment failure wasn't cost, it was cognitive load. Agents are the first buyers who don't mind making a million four-cent decisions.

III. CYBER AND PERMISSIONING: IRREVERSIBILITY AT MACHINE SPEED

The first two pillars are about the opportunities that agentic AI may unlock with crypto assets. The third is about risk. One of crypto's core technical properties is that settlement is final and expended funds cannot easily be recovered, and this was a valuable feature in the human-custody model. Inversely, this feature can become a vulnerability when the custodian is an LLM whose instructions can be influenced by any piece of text it is asked to read.

Three data points illustrate the risk.

First, the systems that connect AI agents to the underlying AI models are already becoming targets for cyberattacks. To reduce costs, many developers use third-party routing services that automatically send simpler requests to cheaper AI models. But these routing layers can also become powerful points of attack.

In an April 2026 research paper titled "Your Agent Is Mine: Measuring Malicious Intermediary Attacks on the LLM Supply Chain," a University of California research team examined 428 third-party AI routing services and found serious security problems in several of them. Some routers secretly inserted malicious code into AI agent actions. Others attempted to capture sensitive credentials, including AWS cloud keys that researchers intentionally planted as "tripwires" to test for abuse.

Researchers also documented real financial theft tied to these attacks. One malicious router successfully stole Ethereum from a researcher-controlled crypto wallet. Another drained roughly $500,000 from a client wallet and enabled attackers to spread malware across hundreds of connected systems within hours.

These incidents highlight a broader problem: traditional cybersecurity protections are often ineffective if attackers compromise the AI system before security checks occur. Hardware wallets, multi-signature protections, and cold-storage setups cannot stop an attacker that intercepts credentials before a transaction is signed or that secretly inserts malicious instructions into AI-generated code that later executes automatically.

Second, prompt injection has moved from theoretical concern to real world harm. One of the most popular agentic AI platforms, OpenClaw, allows users to post "skills" for their AI Agent onto a centralized public marketplace, ClawHub. Similar to the cybersecurity risks identified in routing layer APIs, security researchers identified 824 malicious skills in the ClawHub ecosystem in early 2026, many packaged as crypto trading or automation tools. These skills function much like third-party plugins or workflow integrations: once installed, they can access agent context, interact with external services, execute tasks, and influence downstream model behavior. This architecture creates a supply-chain style risk similar to the vulnerabilities researchers previously identified in routing-layer APIs, where trusted intermediary components can manipulate or redirect model outputs.

Here, a wallet-connected agent "installing a skill" can have immediate financial consequences through indirect prompt injection, where the malicious instructions are hidden inside content the agent is designed to read, sidestepping every perimeter control that assumes the attacker must first get past authentication. In practice, the malicious skills could silently exfiltrate API credentials, redirect crypto transactions, override safety guardrails, or coerce the agent into executing attacker-controlled actions while appearing legitimate to the end user. The findings demonstrated that prompt injections are no longer limited to isolated chatbot exploits; they have evolved into a scalable ecosystem threat in which attackers weaponize third-party agent extensions and public marketplaces to compromise large numbers of autonomous AI systems simultaneously.

Third, aggregate losses are already substantial and trending the wrong direction. Crypto hacks and exploits caused more than $2 billion in losses in 2025. The 2026 year-to-date figure has already crossed $970 million. While none of these incidents were believe to be caused by agents, they establish the baseline threat environment into which agents are now being deployed.

Response strategies are emerging, including designs that keep transaction signing outside the agent runtime. If the agent can read the private key, a compromise of the agent can usually reach the key. Read access and execution access can be structurally separated; the agent that ingests web pages, emails, and documents can be a separate agent than the one processes and moves funds. Hard limits like per-transaction caps, recipient allowlists, daily outflow ceilings, and human approval thresholds are safer in infrastructure, than in prompts. A prompt returns a probabilistic result. It can guide behavior, but it cannot control it.

Ethereum's EIP-7702 presents a thoughtful response at the protocol level: it allows a standard account to serve temporarily as a smart contract for a single transaction, enabling scoped, time-limited permission grants to an AI agent while the user retains control of the underlying key. This offers real protection. It does not eliminate risk, but it does allow users to calibrate it.

As we confront the realities of empowering software routines to unilaterally conduct commerce on our behalf, we will need to navigate the challenges presented by fiduciary delegation to a non-fiduciary system. Traditional agency law presumes that accountability runs with the identity of the actor where the actor can be sued, fired, or jailed. None of those remedies meaningfully apply to an LLM.

In traditional finance, a fraudulent transaction is a problem the bank and the lawyers solve. In agentic crypto, a fraudulent transaction is a settled fact on a public ledger. Success lies in prevention rather than recovery.

IV. THE REGULATORY PARADOX: PERFECT TRACEABILITY, PERFECT OBFUSCATION

The fourth pillar is the one that has received the least attention and which, in our judgment, will prove the most consequential. Sophisticated regulators are in the habit of treating blockchain as a surveillance boon, and on one axis they are correct: the ledger provides the most granular transaction dataset in the history of finance. Every on-chain transfer is timestamped, addressable, and permanently observable. Chain analytics firms can cluster wallets, trace flows across bridges, attribute identities, and designate sanctioned endpoints with reasonable confidence.

The agent layer disrupts this traceability by inserting a semantic black box between the human principal and the transaction. Chain analytics can factually tell you that a wallet sent USDC to a sanctioned address, but on-chain data does not reveal whether a human principal instructed the agent, whether a prompt injection caused it, whether the agent "reasoned" its way there through an intermediate chain of legitimate trades, or whether the human was even aware that the transaction occurred. And intent underpins our financial regulatory system, from fraud prevention to anti-money laundering controls.

The U.S. regulatory perimeter has expanded to meet part of this challenge, though it has not yet addressed the agent layer directly. On April 8, 2026, FinCEN and OFAC jointly published a Notice of Proposed Rulemaking implementing the GENIUS Act's directive to treat permitted payment stablecoin issuers ("PPSIs") as financial institutions under the Bank Secrecy Act. The rule would require written AML/CFT programs, independent testing, ongoing training, and a designated compliance officer. Notably, it represents the first time OFAC has expressly required a specific category of institution to maintain an effective sanctions compliance program.

PPSIs would be required to have the technical capability to block, freeze, and reject transactions involving sanctioned persons, and to seize, freeze, burn, or prevent the transfer of their own stablecoins where a coin or wallet can be identified with "reasonable particularity."

On June 18, 2026, the Financial Crimes Enforcement Network (FinCEN), with the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC) and the National Credit Union Administration (NCUA), issued a joint proposed rule that would implement GENIUS Act's requirement that PPSIs maintain an effective customer identification program (CIP). The proposed CIP requirements for direct stablecoin issuer customers include government identification numbers and physical addresses. The agencies focused on primary markets and acknowledged that imposing a global CIP obligation on all stablecoin transfers that occur on-chain "would be nearly impossible for PPSIs to implement and could potentially cripple the industry." Accordingly, CIP obligations would extend only to direct customer relationships. This rule does not address purely secondary market transfers, where most AI agent activity seems likely to occur.

Despite this regulatory expansion, the agent layer has not yet been separately addressed by regulators. And the illicit-finance data explains why concerns about that gap are not hypothetical:

- At least $154 billion is estimated to have flowed to illicit cryptocurrency addresses in 2025, a 162 percent year-over-year increase; sanctioned entities accounted for roughly $104 billion of that total.
- Stablecoins account for approximately 84 percent of illicit crypto transaction volume. Iran's Islamic Revolutionary Guard Corps and North Korean hackers rely heavily on these assets to move billions.
- Russia launched the ruble-backed A7A5 stablecoin, which facilitated $93.3 billion in transactions in its first year, and functioned as a central conduit for state-aligned sanctions-evasion architecture.

These figures exist in a world in which agents are not yet widely deployed in illicit workflows. As agents gain access to crypto, a sanctioned actor will not need to touch a wallet directly if an agent can. A bad actor can instruct, prompt-inject, or fine-tune an agent to route payments through a series of apparently legitimate micropayments across x402 endpoints, with the human principal plausibly deniable at every step.

The Financial Action Task Force (FATF) has begun to telegraph concern. In its March 2026 report, the task force warned that stablecoins have become the most widely used virtual asset in illicit transactions and called for stricter oversight of issuers, extension of AML rules to unhosted-wallet peer-to-peer transfers, and consideration of tools such as wallet freezing and restrictions on certain smart-contract functions. FATF's updated Recommendation 15 and its Travel Rule require virtual asset service providers (VASPs) to implement risk-based controls and cooperate with asset-freezing requests. AI agents would completely circumvent these controls because the agentic layer sits the VASP.

This is the seam that deserves immediate attention. Three questions, in particular, are worth pressing on now rather than after the first nine-figure agent-related loss event:

- Identity: Who — or what — is the relevant actor for AML and sanctions purposes when an agent transacts? If the human principal, what evidentiary standard establishes principal-agent liability across a prompt-injection chain? How do multi-agent interactions or the probabilistic nature of AI results impact this?

- Custody: How can regulators meaningfully respond to agents holding unhosted wallets, not routing through custodial intermediaries subject to Travel Rule and SAR obligations?

- Liability: When a compromised router, poisoned skill, or malicious prompt injection causes an agent to send funds to a sanctioned address, who bears the sanctions liability? The user? The wallet provider? The model developer? The router operator? The answer will affect every insurance policy, compliance program, and board-level risk register in the space.

Blockchain gives regulators the most traceable dataset in financial history. AI agents insert a semantic black box between the human principal and the transaction. Traceability of the wire tells you nothing about intent of the principal — and intent is the entire premise of AML law.

CONCLUSION: THE SEAMS ARE WHERE THE INTERESTING QUESTIONS LIVE

The four pillars are not independent. The commercial logic of agentic payments (Pillar I) is what creates the volume that validates the micropayment thesis (Pillar II). The micropayment use case spurs adoption and expands the attack surface that security researchers are now documenting (Pillar III). While the cybersecurity gap feeds directly into the regulatory challenge, because a successful prompt injection against an agent is indistinguishable, on-chain, from a legitimate instruction from the human principal (Pillar IV).

For practitioners, the takeaway is practical. The agentic crypto stack is being assembled now, with the participation of the largest payment networks, cloud providers, and stablecoin issuers. We recommend treating the next eighteen months as the design window.

The rails are still being built. The policy vocabulary is still being written. For those with expertise across regulatory enforcement, digital asset markets, cybersecurity, and AI governance, the seams between the four pillars are where the interesting, and consequential, work lives.

Selected References:

- *Coinbase / x402 Foundation, Agentic.Market launch coverage (April 20–21, 2026); BanklessTimes, Cryptonews, Invezz, FinanceFeeds, WebProNews.*
- *MoonPay, "Why Agentic Payments Are The Future of AI and Crypto" (April 2026).*
- *CoinDesk, "AI developers may not be keen on crypto, but stablecoins are the secret to agentic finance" (March 14, 2026).*
- *CoinDesk, "Coinbase-backed AI payments protocol wants to fix micropayment but demand is just not there yet" (March 11, 2026).*
- *Stablecoin Insider, "AI Agents For Stablecoins In 2026" (February 24, 2026).*
- *Liu, H., Shou, C., Wen, H., Chen, Y., Fang, R. J., & Feng, Y. (2026). Your agent is mine: Measuring malicious intermediary attacks on the llm supply chain. arXiv preprint arXiv:2604.08407. (April 8, 2026).*
- *Krause, David, "The $1.4 Billion Bybit Hack: Cybersecurity Failures and the Risks of Cryptocurrency Deregulation" (August 12, 2026)*
- *CoinDesk, "As AI agents scale in crypto, researchers warn of a critical security gap" (April 13, 2026).*
- *Sherlock, "Agentic AI Security Risks in Web3: What Protocols Need to Know in 2026" (March 10, 2026).*
- *CoinDesk, "AI is breaking crypto security by making hacks cheaper and easier, Ledger CTO warns" (April 5, 2026).*
- *Crypto.news, "CertiK warns AI misuse and infrastructure gaps to drive 2026 crypto hacks."*
- *KuCoin Learn, "AI Trading Agent Vulnerability 2026: How a $45M Crypto Security Breach Exposed Protocol Risks."*
- *FinCEN & OFAC, Notice of Proposed Rulemaking, Doc. No. 2026-06963, 91 Fed. Reg. (April 10, 2026) (permitted payment stablecoin issuer AML/CFT and sanctions compliance program requirements under the GENIUS Act).*
- *Holland & Knight, "FinCEN and OFAC Propose AML/Sanctions Rules for Stablecoin Issuers Under GENIUS Act" (April 2026).*

- *WilmerHale client alert, "Treasury Announces Proposed Rule to Implement the GENIUS Act's Requirements to Counter Illicit Finance" (April 20, 2026).*
- *PwC, "Our Take: FinCEN proposes AML overhaul" (April 13, 2026).*
- *Chainalysis, 2026 Crypto Crime Report (including Ransomware and Sanctions chapters).*
- *TRM Labs, 2026 Crypto Crime Report.*
- *FATF, March 2026 report on virtual assets and stablecoin illicit finance risk.*
- *U.S. Department of the Treasury, OFAC press release on redesignation of Garantex and designation of Grinex (August 2025).*
- *Clay Shirky, "The Case Against Micropayments" (O'Reilly, 2000) — historical reference for the cognitive-load thesis.*

ARTICLE III

DRAFT LAW ON THE TAXATION OF CRYPTO ASSET TRANSACTIONS AND RECENT DEVELOPMENTS IN TÜRKİYE

BEGÜM ERGIN
PARTNER
SOLAK & PARTNERS

ELÇIN KARATAY
MANAGING PARTNER
SOLAK & PARTNERS

1. INTRODUCTION

Various provisions regarding the collection of a transaction tax on the purchase and sale of crypto assets and the inclusion of value increase gains regarding crypto assets as a basis in income tax calculations were included in the proposed amendments intended to be introduced with the Draft Law on the Amendment of Certain Laws ("Draft Law") which was submitted to the Presidency of the Grand National Assembly of Türkiye ("TBMM") by the Justice and Development Party Parliamentary Group on March 2, 2026.

These provisions were ultimately removed from the Draft Law during the final deliberations at TBMM General Assembly to be re-evaluated considering the rapid changes and developments in the sector. However, it is expected that regulations on the taxation of crypto asset transactions will be discussed again in the near future, probably within the next year, and similar provisions will likely be revisited and potentially adopted.

In this article, the regulations envisaged for the taxation of crypto assets under the Draft Law will be discussed; additionally, this article will consider the author's assessment regarding the potential obligations and developments that sector stakeholders may face in the future.

2. SCOPE OF THE DRAFT LAW REGARDING TAXATION OF CRYPTO ASSET TRANSACTIONS

2.1.1. TAXABLE EVENT AND TAX RATE

One of the proposed changes was an amendment to Article 35 of the Expenditure Taxes Law No. 6802 along with its heading as "Crypto Asset Transaction Tax".

Under these proposed amendments, sale or transfer transactions are defined as a taxable event, and crypto asset sale and transfer transactions carried out or intermediated by Crypto Asset Service Providers ("CASP") are subject to tax as a crypto asset transaction tax.

Accordingly, it was proposed that crypto asset transaction tax would be levied over crypto asset sale or transfer transactions executed or intermediated directly by CASPs authorized and regulated in Türkiye.

Although the tax is levied on the sale and transfer transactions executed by investors, the CASPs are designated as the taxpayer for this specific tax.

Pursuant to the proposed Draft Law, the crypto asset transaction tax is projected to be applied at a rate of 0.03% (three ten-thousandths) over the crypto asset sales amount or its fair value at the time the crypto asset is transferred.

The proposed Draft Law explicitly stipulates that no deductions under the name of tax or expenses may be made from the crypto asset transaction tax base, which means the total transfer amount or sale price will be subject to this tax.

However, the President would have been authorized to reduce the tax rate down to zero or increase it up to five times, either separately or jointly according to transaction types. The Ministry of Treasury and Finance of the Republic of Türkiye ("Ministry") would have determined e the procedures and principles regarding the implementation.

2.1.2. DECLARATION AND PAYMENT OBLIGATIONS

The crypto asset transaction tax was to be declared by the CASP to the tax office to which the CASP is affiliated with for income or corporate tax purposes by the evening of the 15th day of the following month for the relevant month, and it must be paid within the same period

2.1.3. ISSUES AROUND CRYPTO ASSET TRANSACTION TAX THAT NEED CLARIFICATION

Considering the CASPs were to be designated as taxpayers, the application of a crypto asset transaction tax would have had a significant impact on CASPs.

The impact of the crypto asset transaction tax on CASP operations will primarily emerge due to the need to clarify which transaction types the "sale" and "transfer" operations encompass.

In practice, how wallet-to-wallet transfers, intra-platform movements, and similar sub-scenarios will be classified will largely only become evident through secondary regulations; therefore, all transaction types will have to be categorized in a way that aligns with legislative definitions and integrated to platform processes and relied clearly to customers who will be individually affected.

In connection with this, determining exactly when the "fair value" at the time of transfer will be calculated, from which price source, and according to what rules is also a critical element in calculating the tax; thus, CASPs would need to design the valuation process in a way that is both technical and auditable.

Finally, the approach that no deductions can be made from the tax base under the name of expenses or taxes will increase the impact of transaction-based costs on pricing and the revenue model of CASPs, which will probably result in increases in commission fees that will be reflected to individuals.

2.2. POSITIONING OF CRYPTO ASSETS IN INCOME TAX LEGISLATION

2.2.1. TAXABLE EVENT AND TAX RATE

The Draft Law proposed the addition of a repeated Article 94 titled with the marginal heading "Taxation of Crypto Assets" to the Income Tax Law No. 193.

Gains arising from the disposal of crypto assets are categorized as value increase gains and subjected to income tax.

According to this article, a 10% tax withholding will be applied quarterly on the gains and revenues derived from crypto asset transactions by taxpayers executing transactions on CASPs subject to the Capital Markets Law No. 6362 ("CML") and operating with a license from the Capital Markets Board.

Whether the income earner is an individual or a legal entity, a resident or non-resident taxpayer, whether they have a tax liability, whether they are tax-exempt, and whether the derived gain is exempt from tax will not affect the withholding to be made.

While the taxpayers of this tax are investors; CASPs would be required to execute the withholding. It should be noted that the applied tax covers capital gains and income. In this context, capital gains resulting from the value appreciation of the crypto asset and income generated from staking activities could be evaluated within this scope.

The President would have been s authorized to reduce the withholding rate to zero or increase it by one-fold based on various criteria such as the type of gain and revenue, crypto asset type, holding period, issuance/acquisition date, issuer or income earner, and wallet types. The Ministry would have been authorized to determine the procedures and principles and to hold the parties or intermediaries to these transactions responsible for the payment of the tax.

2.2.2. DETERMINATION OF THE TAX BASE

According to the Draft Law, in the event that the same crypto asset is purchased on different dates and a portion of these crypto assets is subsequently disposed of, it is envisaged that the purchase cost to be considered in determining the withholding tax base will be determined using the first-in, first-out (FIFO) method.

Commissions paid due to purchase and sale transactions and the transaction tax will be taken into account as deductions in determining the withholding tax base.

If there is more than one purchase-sale transaction for the same type of crypto asset within the withholding period, the transactions will be considered as a "single transaction" for withholding purposes. Losses may be offset against the tax base of the subsequent period, provided that it does not exceed the calendar year. For example, an individual whose incurred a loss in the first quarter will be able to offset their first-quarter loss even if they generate a profit in the second quarter, and the tax amount payable will be determined accordingly.

2.2.3. NOTIFICATION AND DECLARATION REGARDING THE PURCHASE COST

In case crypto assets are transferred to another platform, it is required that the purchase cost and purchase date of the said assets be reported to the platform to which the transfer is made. Although there is no provision in the law detailing how this notification will be executed, it is evaluated that this matter is planned to be regulated through secondary legislation to be issued by the Revenue Administration. Transferring the purchase price and date along with the travel rule information could be a practical option here. Furthermore, if the crypto asset is transferred to the platform for the first time, the amount declared by the user will be taken as the basis for the purchase cost; however, this declaration must be supported by documents. Although not explicitly regulated in the legislation, it is evaluated that this provision could be applied to transfers made from non-custodial wallets, as well as to transfers of crypto assets sent from CASPs that are not subject to the CML.

2.2.4. DIFFERENCES REGARDING COMMERCIAL EARNINGS AND INCOME DERIVED THROUGH CASPS NOT SUBJECT TO THE CML (GLOBAL PLATFORMS)

At this point, a particularly notable distinction arises depending on whether the income is obtained within the scope of "commercial activity".

It is envisaged that individuals will not need to submit annual or individual declarations, and non-resident corporate entities will not need to submit special declarations for earnings within the scope of withholding.

That is, the 10% withheld under this article will be the final tax.

On the other hand, offset and declaration exemptions for commercial earnings taxpayers are separately regulated. In other words, income obtained within the scope of commercial activity can be taxed at a higher rate within the framework of commercial earnings provisions, and the 10% withheld under this article will be deducted from the final tax.

Although how the distinction of commercial activity is made is of importance in terms of implementation, the principles on this matter are expected to be clarified through secondary regulations.

As per the Draft Law, it is regulated that crypto asset incomes derived from transactions made outside platforms subject to CML (for example, on foreign platforms) shall be declared via an annual income tax return, and no exemption is foreseen for these incomes.

Losses arising from crypto asset transactions have been restricted such that they can only be offset against gains derived from these specific assets. Thus, there is no suggested difference in the final tax for incomes obtained within the scope of commercial activity.

Individuals and non-resident corporate entities will not be able to benefit from the 10% limitation for incomes that are obtained within the scope of commercial activity. However, it may be possible to benefit from exemptions related to value increase gains. Since there may be differences in interpretation on this issue, secondary legislative regulations will be needed which clarify such matters.

2.2.5 ASSESSMENT, DECLARATION AND PAYMENT OBLIGATIONS

Under the Draft Law, CASPs were to be held directly liable for the tax assessment in accordance with the information and documents provided to them regarding customer transactions. In other words, during inspections, the tax administration may base its evaluation on the transaction records, declarations, and submitted documents maintained by CASPs.

However, if it is determined that the tax was undercalculated due to deficiencies or inaccuracies in said information and documents, the liability for the under-declared portion will fall on the person making the notification (e.g., the party providing the transaction information or creating the declaration), and the necessary tax assessment will be levied against this person.

CASPs would also have been required to declare the taxes they have withheld to the tax office they are registered with, using a declaration form to be determined by the Ministry by the evening of the 26th day of the month following the withholding period and must pay it within the same timeframe.

3. CONCLUSION

While the provisions regarding crypto assets were ultimately withdrawn at the TBMM General Assembly “to be re-evaluated considering the rapid changes and developments in the sector,”, it is considered likely that similar regulations will come to the forefront again as the crypto asset ecosystem in Türkiye attains a more established structure in the future.

In this context, it is possible that the crypto asset transaction tax and principles regarding the taxation of income derived from crypto assets will be resubmitted to the TBMM through different methods, particularly within the framework of regulations targeting the taxation of crypto asset transactions and the planned additions to the Income Tax Law.

Accordingly, it would be advisable for stakeholders to closely monitor the draft laws submitted to the Presidency of the TBMM and other developments reflected in the public domain, to take actions that will facilitate the compliance process, and ultimately to restructure their operational processes in accordance with these developments.

ARTICLE IV

WYOMING PUBLIC ISSUER MODEL: A NEW ARCHITECTURE FOR SOVEREIGN STABLE TOKENS

DEBRA BROOKES
CHIEF RISK AND COMPLIANCE OFFICER
WYOMING STABLE TOKEN COMMISSION

I. INTRODUCTION

Modern payments remain remarkably expensive. Depending on the payment rails, parties on either side of a transaction may face significant payment processing costs.[1] In addition, crossborder transfers navigate complicated correspondent banking networks with settlements that traditionally take days to process.[2] Despite the proliferation of financial technologies and trillions of dollars flowing through the digital asset ecosystem, the payment ecosystem remains fragmented and costly.[3] Stable tokens offer a promising alternative: near-instantaneous settlement with fees typically less than one cent. Today, stable tokens in circulation total approximately $300 billion, up from $27 billion in January 2021, and show little signs of slowing down.[4]

While private stable token issuers have been in operation since 2014, the State of Wyoming pioneered a new approach: the State became the issuer. Through the Stable Token Act (the "Act"), Wyoming paved the way for the Frontier Stable Token ("FRNT"): the first fiat-backed, fully reserved stable token issued by a public entity.[5] With reserve requirements hard-coded in statute and earnings flowing to public schools rather than shareholders, Wyoming leverages stable tokens for the public good while significantly reducing transaction costs and delays.

One highlighted use case exemplified how FRNT could turn weeks-long payment processes into near-instantaneous settlements for interstate utility providers.[6] This article examines the "Wyoming Public Issuer Model," its origins, place in a shifting regulatory landscape, and potential to build meaningful partnerships with other government institutions.

II. THE WYOMING PUBLIC ISSUER MODEL

The Frontier Stable Token did not arrive fully formed; it emerged from nearly a decade of legislative experimentation.[7] The State's initial goal was not to issue a stable token, but instead create a legislative framework where digital assets could flourish. In 2017, the Wyoming Blockchain Coalition, founded by Caitlin Long, Rob Jennings and David Pope, began this process.[8] By the following legislative session, Wyoming had passed four blockchain-related bills, including an amendment exempting cryptocurrency from state money transmitter statutes and the world's first legislative definition of a utility token.[9]

In 2022, the Select Committee on Blockchain, Financial Technology and Digital Innovation Technology ("Select Committee")[10] introduced the Wyoming Stable Token Act, which Governor Mark Gordon let pass into law in March 2023.[11]

The Act created the Wyoming Stable Token Commission (the "Commission") with the directive of developing and issuing the first government-issued stable token. The Commission, composed of seven members,[12] appointed Anthony Apollo as Executive Director in September 2023.[13] With the support of the staff, the Commission launched the Frontier Stable Token for public use on January 7, 2026.[14]

The Wyoming Stable Token Act defines the token as "a virtual currency representative of and redeemable for one United States dollar held in trust by the State of Wyoming."[15] The Act establishes a public issuer, codifies the token's goal of a conservative reserves management mechanism, and creates unique relationships between the Commission and its private-sector partners.[16] The Commission, established by the Act as an instrumentality of the State, holds exclusive authority over issuance and redemption of FRNT with support from its vendors. The Commission also manages reserves and promulgates operational rules. Following amendments to the Act in 2026, the Commission is authorized to enter into agreements and consult with other government entities to facilitate the use of Wyoming Stable Tokens.[17]

FRNT is designed for secure, transparent, and efficient transactions. Currently, FRNT is deployed on eight interoperable blockchains to (1) remain technology agnostic; and (2) maintain flexibility to support use cases on each selected blockchain. Blockchains are selected through a publicly available, Commision-approved Blockchain Selection Criteria process.[18] Stable tokens like FRNT enable dollar-denominated settlement for any amount, anywhere with an internet connection, in seconds, with transaction fees costing less than $0.01.[19]

Additionally, FRNT's integrity rests on three statutory guarantees:

1. ***Fully Reserved:*** Every token is redeemable one-for-one for U.S. dollars.
2. ***Reserve Composition:*** Reserves are statutorily constrained to traditionally safe assets: Cash, U.S. Treasury securities (maturities of 365 days or less), repurchase agreements (terms of 30 days or less), or in compliance with 17 C.F.R. part 270.2a-7.
3. ***Mandatory Overcollateralization:*** The Commission must maintain a buffer above 102% backing before any surplus is distributed. Investment earnings follow a statutorily-defined waterfall, with the remainder flowing to the State's School Foundation Program.[20]

The Commission cannot loosen these requirements; only the Wyoming state legislature has the power to amend.

The Commission consists of a small but experienced team of seven Commissioners and five executive staff,[21] with support from Licensed Service Providers ("LSPs"), fully-vetted private entities engaged to manage the token's distribution. While the Commission maintains core responsibilities such as token issuance and redemption, regulatory rule making, and overseeing robust operational programs, it actively engages in live, public meetings where materials are readily accessible on the Commission website.[22] Ultimately, the Act provides a clear division of responsibilities: The State retains trust functions and sovereign oversight, while the private sector supplies technical capacity and reach.

III. WHY IS THE WYOMING PUBLIC ISSUER MODEL UNIQUE?

The Wyoming Public Issuer Model provides the greatest structural transparency that few private stable token issuers can achieve. As a state instrumentality, transparency courses through Wyoming's foundation.

Thus, the Commission conducts its business in public: all monthly meetings are subject to public, real-time supervision with detailed meeting minutes and recording, and its budget is legislatively appropriated, with forms of mandatory disclosure and scrutiny no private issuer faces.[23]

The same holds at the operational level. For an instrument whose entire value rests on a redemption promise the holder cannot verify alone, attestation is the bridge between the token on the ledger and the dollars behind it. FRNT's reserves are supported by daily attestations containing independent opinions provided by the Network Firm LLP, giving Token Holders continuous, third-party verification that reserves meet statutory requirements.[24] The daily cadence exceeds the monthly composition reports the GENIUS Act requires for private stable token issuers and should prove FRNT holders greater comfort.[25]

The Wyoming Public Issuer Model is also unique in its profit model and public good. Stable token issuers earn money by investing the reserves that back their tokens. For private issuers, this yield is the business model.[26] Under the Wyoming Stable Token Act, however, 100% of the investment earnings on FRNT's reserves flows through a statutory waterfall.[27] Token Holders' reserves are 100% held in a "Trust Account" that is custodied and managed by Franklin Templeton and Fiduciary Trust International. Excess are then transferred in the statutory sequence: first to pay the Commission's operational and capital expenses, second to fund an account that maintains a two percent buffer against the outstanding token value, third to a savings retention to cover future capital needs, and most importantly to the State's Public School Foundation program account.[28]

The Act's codification on reserves management is critical: because the Commission's "profit" is public revenue, it changes incentives at every point. Because a private issuer ultimately answers to shareholders, it faces incentives to maximize returns on reserve assets and to calibrate disclosure within the bounds of applicable legal requirements. An issuer whose surplus funds public schools, and whose reserve rules are fixed in statute, faces none of these pressures. **Reserve risk, compliance, and redemption are not profit levers to be optimized; they are legal obligations to be met.**[29] FRNT is not competing for private profits; it is infrastructure whose value lies in what it enables.

IV. IMPLICATIONS FOR OTHER STATES

Concretely, FRNT facilitates a transparent payment system. **The Commission's strategy is sequenced: start local, think global. The first proving ground is Wyoming's own government:** social services delivery, intra-state transfers between agencies, and State payroll, each of which FRNT can support. The economics are compelling. One Wyoming county reported its citizens paying roughly $70,000 in credit card processing fees on $3.4 million in tax remittances in a single year, costs that nearly vanish when payment moves to FRNT rails.[30] Because every transaction is recorded on a public ledger, citizens gain transparency into public uses of capital. This does not make Wyoming hostile to private issuers; rather, it removes the assumption that private issuance is the only viable architecture. FRNT offers both the public and governments the opportunity to benefit from a stable token not optimized for private profit.

Wyoming built the Frontier Stable Token to be used, but its greater significance may be proof that its Public Issuer Model works. Following the enactment of the amendments to the Act in 2026, the Commission is now authorized to enter into agreements with other states to facilitate use of Wyoming Stable Tokens.[31]

The Commission envisions a multi-state network: Wyoming provides the issuance, redemption, and reserve infrastructure; deploying white-labeled stable tokens for partner states backed by Wyoming's legal and technical architecture; with shared revenue. The first public issuer has done the hard part. For the states that follow, the road is already paved.

Most notably, FRNT's utility extends beyond traditional payments into administrative functions that every state performs; notably, unclaimed property distribution. States collectively hold billions in forgotten bank accounts, uncashed checks, and abandoned assets, returning funds through slow and expensive legacy processes.[32] The process itself takes money out of peoples' pockets due to operational delays and inefficiencies.[33] The Commission has identified unclaimed property distribution among the early exploratory governmental use cases for FRNT.[34] FRNT can replace these lengthy workflows and delays with instant, verifiable settlement at a near-zero cost to the state, while creating an immutable and public payment trail. Because Wyoming has built the rails for more efficient payment systems, other states do not need to spend time or energy developing their own systems. Instead, they can access an immediate, plug-and-play payment rail to streamline operations and deliver real digital efficiency–and savings–directly to their citizens.[35]

V. CONCLUSION

The Frontier Token demonstrates that stable tokens need not be confined to private issuers. By combining statutory reserve requirements, public accountability, and private-sector distribution, Wyoming has introduced a distinct model that aligns the benefits of digital payments with a public mission. As stable token regulation evolves, the Wyoming Public Issuer Model offers states policymakers a new framework for considering not only how stable tokens should be regulated, but also who should issue them. An entity governed by public accountability rather than private incentive can serve as the blueprint for other governments to partner with the State of Wyoming.

Commission Law Clerks Haiyi Liu (3L-Georgtown Law) and Jacob Weintraub (2L-Brooklyn Law) contributed to this article.

See endnotes on next page

Endnotes:

1 Credit Card 'Swipe' Fees Drain $3.4 Billion from Families' Back-to-School Spending This Year, MERCH. PAYMENT COAL. (July 20, 2026), https://merchantspaymentscoalition.com/credit-card-swipe-fees-drain-34-billionfamilies-back-school-spending-year; The Race to Rewire Cross-Border Payments, J.P. MORGAN, https://www.jpmorgan.com/payments/payments-unbound/volume-3/cross-border-payment-modernization (last visited July 22, 2026); Payment Settlement Explained: How It Works and How Long I Takes, STRIPE (Oct. 14, 2025), https://stripe.com/resources/more/payment-settlement-explained-how-it-works-and-how-long-it-takes.

2 Ken Isaacson, Cross-Border Payments for Heartland Banks, FED. RSRV. BANK OF CLEVELAND (May 1, 2026), https://www.clevelandfed.org/publications/payments-research-brief/2026/prb-20260501-cross-border-payments-for-heartland-banks.

3 Greg Brownstein, Global Payment Systems Are Fragmenting. Here's What The G20 Can Do, ATL. COUNCIL, (Apr. 1, 2026), https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/global-paymentsystems-are-fragmenting-he res-what-the-g20-can-do/.

4 Stablecoin Supply, VISA ONCHAIN ANALYTICS DASHBOARD, https://visaonchainanalytics.com/supply (last visited July 30, 2026).

5 Jean Chalopin & Conor Scott, The History of Stablecoins, DELTEC BANK, https://www.deltecbank.com/news-andinsights/the-history-of-stablecoins/ (last visited July 24, 2026); Wyo. Stat. Ann. § 40-31-101 (2026); see Wyoming Stable Token Commission Factbook, WYOMING STABLE TOKEN COMMISSION, at 4 (Jul. 15, 2026), https://stabletoken.wyo.gov/assets/media/factbook.pdf.

6 GLOB. BLOCKCHAIN BUSINESS COUNCIL, 101 Real-World Blockchain Use Cases Handbook at 210-11 (2026), https://assets.ctfassets.net/so75yocayyva/6zZVoaxLnwsCAgbOyRp5tu/08d17dec18aaf617b52a18443e11cd1c/Hand book 2026 digital.pdf.

7 Anessa Santos, Wyoming Blockchain Legislation Review for Years 2018-2019, BUS. L. SEC. FLA. B., https://www.flabizlaw.org/files/Wyoming%20Blockchain%20Legislation%20Summary%20Review.pdf (last visited July 22, 2026).

8 See Seth Stern, Bringing Blockchain to the Cowboy State, HARV. L. BULL. (June 26, 2018), https://hls.harvard.edu/today/bringing-blockchain-cowboy-state/.

9 Rachel Wolfson, U.S. State Of Wyoming Defines Cryptocurrency 'Utility Tokens' As New Asset Class, FORBES (Mar. 13, 2018), https://www.forbes.com/sites/rachelwolfson/2018/03/13/u-s-state-of-wyoming-definescryptocurrency-utility-tokens-as-new-asset-class/. See Wyo. Stat. Ann. § 34-29-106(b) (2022) (providing statutory definitions for blockchain token classifications).

10 See Select Comm. on Blockchain, Fin. Tech. & Digital Innovation Tech., WYO. LEG., https://wyoleg.gov/Committees/2026/S19 (last visited July 31, 2026) (describing the eleven-member committee composition, with four members appointed by the President of the Senate and four members appointed by the Speaker of the House. The Committee meets bimonthly throughout the interim session with the mission to "examine the adoption and integration of the Frontier Stable Token (FRNT) into Wyoming commerce, taxation, and state government processes.... [and] review the regulatory framework governing stablecoins issued within Wyoming.").

11 See Wyoming Stable Token Act, S.F. 127, 67th Leg., Gen. Sess. (Wyo. 2023), https://wyoleg.gov/Legislation/2023/SF0127; Letter from Mark Gordon, Governor of Wyoming, to Chuck Gray, Secretary of State of Wyoming (Mar. 17, 2023), https://drive.google.com/file/d/1A9ZknTJNkWMNSepAE-mZQ34SusqGI04-Q/view?usp=sharing.

12 The Commissioners are Governor (and Chairman) Mark Gordon, Auditor Kristi Racines, Treasurer Curt Meier, Flavia Naves (formerly General Counsel with Circle), David Pope, Jeff Wallace, and Joel Revill. See About Us, WYOMING STABLE TOKEN COMMISSION, https://stabletoken.wyo.gov/pages/about-us (last visited July 23, 2026).

13 Press Release, Off. of Gov. Mark Gordon, Wyoming Stable Token Commission Names Anthony Apollo Executive Director (September 19, 2023), https://governor.wyo.gov/news-releases/wyoming-stable-token-commission-names-anthony-apollo-executive-direct.

14 Press Release, Off. of Gov. Mark Gordon, Wyoming Ushers in New Era: Launches First-of-its-kind Frontier Stable Token for Public Purchase (January 7, 2026), https://governor.wyo.gov/news-releases/wyoming-ushers-in-new-eralaunches-first-of-its-kind-frontier-stable-token-f or-public-purchase; Wyo. Stat. Ann. § 40-31-104 (2026).

15 See Wyo. Stat. Ann. § 40-31-104 (2026).

16 See Wyo. Stat. Ann. §§ 40-31-103(a), 40-31-105, 40-31-106(a) (2026).

17 See Wyo. Stat. Ann. § 40-31-103(a) (2026).

18 What is FRNT?, WYOMING STABLE TOKEN COMMISSION, https://stabletoken.wyo.gov/pages/FRNT (last visited July 22, 2026); Wyoming Stable Token Commission Factbook, WYOMING STABLE TOKEN COMMISSION, at 15 (July 15, 2026), https://stabletoken.wyo.gov/assets/media/factbook.pdf (noting the Wyoming Stable Token Commission's currently supports eight blockchains: Arbitrum, Avalanche, Base, Ethereum, Hedera, Optimism, Polygon, and Solana).; Blockchain Selection Exercise, WYOMING STABLE TOKEN COMMISSION, https://stabletoken.wyo.gov/pages/BSE (last visited July 30, 2026) (noting that to select blockchains, an assessment was conducted over 28 blockchains using 25 objective criteria with the intent of ranking blockchains according to their technical capabilities, regulatory compliance, current utilization, and more).

19 See Ian Hall, Wyoming Makes Gov Fintech History with Launch of First US State-Issued Stablecoin, GLOBAL GOVERNMENT GOV'T FINTECH (Aug. 206, 2025), https://www.globalgovernmentfinance.com/wyoming-stablecoin-frnt-launches/.

20 Wyo. Stat. Ann. § 40-31-106(c) (2026).

21 In addition to Executive Director Apollo, the staff consists of Keith Lawhorn (Chief Information and Security Officer), Joseph Saldana (Chief Financial Officer), Debra Brookes (Chief Risk & Compliance Officer), and Stephanie Chan (Enterprise Project Manager). See Wyoming Stable Token Commission Factbook, WYOMING STABLE TOKEN COMMISSION, at 3 (July 15, 2026), https://stabletoken.wyo.gov/assets/media/factbook.pdf.

22 See WYOMING STABLE TOKEN COMMISSION, https://stabletoken.wyo.gov (last visited July 31, 2026); Wyoming Stable Token Commission Factbook, WYOMING STABLE TOKEN COMMISSION, at 32 (July 15, 2026), https://stabletoken.wyo.gov/assets/media/factbook.pdf.

23 Meeting Materials, WYOMING STABLE TOKEN COMMISSION, https://stabletoken.wyo.gov/pages/MeetingMaterials (last visited July 31, 2026).

24 WYOMING STABLE TOKEN COMMISSION, https://stabletoken.wyo.gov (last visited July 31, 2026).

25 Guiding and Establishing National Innovation for U.S. Stablecoins Act, 12 U.S.C.A. § 5903(c) (West).

26 See How Do Stablecoin Issuers Earn Money?, STRIPE, https://stripe.com/resources/more/how-do-stablecoinissuers-earn-money#how-do-stablecoin-issuers-earn-money (last visited July 23, 2026).

27 Wyo. Stat. Ann. §§ 40-31-106(b), (c)(i-iv) (2026).

28 See id.

29 See Wyo. Stat. Ann. § 40-31-106(d) (2026); Wyo. Stat. Ann. § 40-31-105(b) (2023); Wyo. Stat. Ann. § 40-31-107 (2023).

30 Press Release, Off. of Gov. Mark Gordon, Wyoming Ushers in New Era: Launches First-of-its-kind Frontier Stable Token for Public Purchase (Jan. 7, 2026), https://governor.wyo.gov/news-releases/wyoming-ushers-in-newera-launches-first-of-its-kind-frontier-stable-token-for-public-purchase.

31 Wyo. Stat. Ann. § 40-31-103(a) (2026).

32 How States Return Missing Money, NATIONAL ASSOCIATION OF UNCLAIMED PROPERTY ADMINISTRATORS, https://unclaimed.org/how-states-return-missing-money/ (last visited July 30, 2026).

33 Unclaimed Funds, NEW YORK STATE COMPTROLLER, https://www.osc.ny.gov/unclaimed-funds (last visited July 30, 2026); Sarah Agostino, States Have $70 Billion in Unclaimed Assets. How to Check If Any Is Yours, CNBC (Feb. 1, 2026), https://www.cnbc.com/2023/02/01/how-to-check-if-youre-owed-a-share-of-70-billion-in-unclaimed-assets.html.

34 See Caitlin Devitt, Wyoming Has Big Plans for Stablecoin, PAYMENTS DIVE (Jan. 21, 2026), https://www.paymentsdive.com/news/wyoming-has-big-plans-for-stablecoin/810103/

35 See id.

GBBC & NRF 2026 FUTURE OF FINANCE CONFERENCE

HANNAH MEAKIN
PARTNER
NORTON ROSE FULBRIGHT LLP

SEAN MURPHY
GLOBAL HEAD OF FINTECH
NORTON ROSE FULBRIGHT LLP

ROBERT LANGMUIR
HEAD OF EUROPEAN GOVERNMENT AND REGULATORY AFFAIRS
NORTON ROSE FULBRIGHT LLP

PANEL DISCUSSION: THE MULTI-MONEY FUTURE – STABLECOINS, TOKENISED DEPOSITS AND THE NEW PAYMENTS STACK

Moderator: Nilixa Devlukia, EMEA Policy Advisor, GBBC.

Speakers: James Pollock, EMEA Sales Director, Digital Asset Canton Network; Mike Manning, Head of Institutional Finance, Ava Labs; Kene Ezeji-Okoye, Chief Business Officer, Ubyx Inc

The panel, moderated by Nilixa Devlukia (GBBC), observed that various regimes are now regulating stablecoins when eighteen months ago this journey was just beginning, and considered signals indicating transition beyond experimentation.

Mike Manning (Ava Labs) noted stablecoins are key for cross-border payments and remain predominantly a US dollar product. Around 80% of usage is still related to crypto trading, but Manning expects stablecoins to take their place alongside traditional payment methods.

Kene Ezeji-Okoye (Ubyx) noted that volumes and usage in 'real-world' payment flows are rapidly increasing. James Pollock (Digital Asset Canton Network) noted stablecoins remain a tiny part of global trading and their mainstream adoption depends on developments over the next two years.

On tokenised deposits, the panel noted key differences from stablecoins: tokenised deposits pay yield, but are (currently) limited to intra-bank use cases. Stablecoins don't (directly) pay yield, but travel easily across institutions and borders. Tokenised deposits have a public backstop, but also maintain fractional backing. Stablecoins lack a backstop, but—for GENIUS Act-compliant coins—are fully backed by cash and short-term government debt. This makes a 'run' on a stablecoin a liquidity question rather than a solvency question. Stablecoin issuers lack bank-equivalent consumer protection obligations, with panellists expressing different perspectives on the significance of this difference in practice. All panellists emphasised digital money should "feel like a pound" to the end user.

On redemption and conversion, Ezeji-Okoye noted it is not as easy as it should be, and requires the adoption of acceptance and clearing infrastructure similar to the mechanisms that underpin the singleness of money in traditional finance. Banks are likely to move towards transaction fee models, potentially ending free deposit banking.

On interoperability, the panel noted this is key to mainstream adoption but Manning and Pollock suggested that if taken too far it institutionalises fragmentation, and the industry will likely settle on two to three chains. Ezeji-Okoye noted that m ore important is the application of shared standards and utilities for all platforms.

PANEL DISCUSSION: TOKENISATION AT SCALE – FROM SANDBOXES TO SETTLEMENT INFRASTRUCTURE

Moderator: Hannah Meakin, Partner, Norton Rose Fulbright.

Speakers: Julie Ng, Vice President & Senior Analyst, EMEA Structured Finance Group, Moody's Corporation; Sebastien Van Campenhoudt, Director, Innovation & Digital Assets, Tokenized Cash Lead, Euroclear; Simon Keefe, Head of Digital Solutions, Calastone; Jack Davies, Senior Blockchain Analyst, Metrika

The panel, moderated by Hannah Meakin (Norton Rose Fulbright), referenced a recent IMF paper arguing tokenisation is a structural shift in financial architecture rather than a marginal efficiency improvement.

Simon Keefe (Calastone) agreed the shift is structural. Calastone's experiment with Schroders in Singapore reduced mutual fund seed capital requirements from approximately £50 million to negligible. However, as the industry is heavily regulated, progress must be made on an individual efficiency basis, meaning the tokenised world must still interoperate with traditional finance. Sebastien Van Campenhoudt (Euroclear) described tokenisation as putting counterparties around a single table, rather than being intermediated, leading to efficiency gains. However, this shift will be an evolution rather than a revolution, as moving the existing traditional assets on-chain will happen progressively and require many years.

Meakin observed that different asset classes and sectors are starting at different places, all developing in parallel. She asked what challenges are slowing progress, and whether there is a disconnect between stated blockers and reality.

Julie Ng (Moody's) noted many institutions cite regulatory clarity, technology trust, or business use case concerns. On regulation, MiCA has come into force and the UK, US and Hong Kong are progressing. The real issue is legal certainty on settlement finality, enforceability and liability. On technology, the actual barrier is the missing layer of oversight such as credit ratings, which is why Moody's has enabled its capacity to bring credit risk assessment on-chain. And without on-chain legal certainty and the oversight layer, the business case will never prove itself, and efficiencies will not arise. Jack Davies (Metrika) added that regulatory acceptance and technology are no longer blockers – both thresholds have been met. The remaining concern is that the operating model has not yet eliminated human and operational error by means of standardisation or automation.

Meakin raised whether automated controls can substitute for the "breathing room" provided by settlement delays, or whether some friction remains necessary for managing operational, liquidity, and market-stress issues.

The panellists suggested a more nuanced position. Keefe noted everything can be built on real-time settlement with brakes such as batching trades at intervals. In two to three years, regulators will likely extract information they could not before, potentially using AI to identify emerging risks. Van Campenhoudt cautioned that technological capability does not always mean desirability; having 24/7 immediate settlement may have drawbacks.

For example, having a weekend window gives authorities and market participants time to intervene during a major crisis, such as done with Lehman Brothers or Credit Suisse. Ng echoed this: increased settlement speed makes credit assessment more difficult. Davies agreed the key issue is balancing settlement time with breathing space and noted that pause functions and whitelisting are achievable at the smart contract level. In money market funds, introducing real-time stablecoins has worked well as it eliminates the risk of placing trades before money is available.

PANEL DISCUSSION: SECURING DIGITAL ASSETS – CUSTODY, WALLETS AND INSTITUTIONAL READINESS

Moderator: Robert Langmuir, Head of European Government and Regulatory Affairs, Norton Rose Fulbright.

Speakers: Donald Brouwer, Managing Director EMEA, Dfns; Mark John, Director of Sales, Europe, GK8; Elsa Madrolle, Global Head of Commercial Engagement, SimCorp

The panel, moderated by Robert Langmuir (Norton Rose Fulbright), focused on institutional adoption, what firms prioritise when choosing custody providers, and which capabilities financial institutions need to build for market scale.

Elsa Madrolle (SimCorp) confirmed increased interest in tokenisation among buy-side clients, encompassing both crypto exposure and tokenised securities. Firms must now work with all three tracks: crypto, tokenised securities, and traditional assets. While not everything will be on-chain any time soon, AI accelerates the ability to service the buy side. Donald Brouwer (Dfns) noted that, across the board, banks have decided to in-source digital asset capabilities, and build up teams and technology. Banks are pursuing a broad range of use cases, including tokenised deposits, stablecoins, tokenised money market funds, and crypto services.

Donald also highlighted that banks increasingly opt for fully on-premises infrastructure deployments, allowing them to retain full control over their security, governance and operational environment while scaling their digital asset offerings. Mark John (GK8) emphasised that heavily regulated institutions moving on-chain require a suitable merger of TradFi with digital assets. The explosion of interest has been helped by regulation. Banks are motivated to move forward to demonstrate innovation and avoid the risk of inaction potentially leading to losing clients to competitors with digital asset offerings. Brouwer added the P&L case is not currently strong; fear of competition is a better driver than the business case alone. Madrolle noted client questions before adoption are: “can I book it, can I value it, and can I risk-manage it?”

On “institutional grade custody”, John argued this means guaranteeing safety backed by solid due diligence – making a financial decision, not a technology decision. When buying US dollars, one thinks only of financial impact, not underlying technology. Institutional-grade custody allows similar comfort without thinking about technology as a feature but as an outcome. Brouwer added it means meeting requirements through the entire life cycle with appropriate and proportionate approaches that scale with usage.

The panel noted fragmentation is not new to the buy side. The technology aspect of digital assets is just a new version of an old problem. FMI standards work addresses interoperability between networks but does not solve the buy-side problem; AI developments make solving this layer more financially viable.

On blockers to institutional adoption, Brouwer observed it depends on use case – stablecoins are developing well; for tokenised securities, there must be market demand and liquidity. The challenge is getting financial institutions and their clients to use the technology. Madrolle identified the operating model as the biggest blocker; recommending that firms build interoperability readiness across blockchains and develop a governance framework for custody.

KEYNOTE SPEECH

Speaker: Gergely Kóczán, Advisor, European Central Bank

Gergely Kóczán opened by acknowledging that central banks worldwide have taken different approaches to tokenisation. The ECB has focused on four objectives: (1) maintaining central bank money as part of a safe, efficient two-tier monetary system; (2) developing a more efficient and competitive ecosystem, acknowledging Europe's fragmentation risk; (3) strategic autonomy use given geopolitical developments; and (4) ensuring the relevance of the euro as an international currency.

Kóczán outlined the ECB's history with tokenisation. The Bank began exploring tokenisation around 2016/17 and in 2024 launched major exploratory work with 64 market participants, involving £1.64 billion in real transactions. This led to the 2025 announcement of a work programme with two pillars: Pontes and Appia. On central bank money for tokenisation, Kóczán emphasised that central bank money could act as a "superstructure" binding private initiatives. Pontes launches September 2026 as a tokenised central bank money settlement service; initially it will provide an interface without settlement finality on blockchain, with finality and extended hours planned for 2027 and 24/7 availability by 2028.

Appia involves structured engagement with industry on longer-term views for the European tokenised ecosystem, comprising practical experiments examining how market infrastructures interact. In March 2026, the ECB launched a public consultation with positive feedback to date. Appia will be organised around six building blocks: (1) asset interoperability and standards; (2) monetary policy implementation and collateral management on DLT; (3) European tokenised central bank money infrastructure(s); (4) international dimension and cross-border links; (5) an innovative, safe and resilient ecosystem; and (6) implementation strategy and impact on existing infrastructures. The ECB will publish a blueprint in 2028 summarising findings and milestones.

Kóczán acknowledged that while distributed ledger technologies make providing infrastructures easier and have the potential to increase competition, there is a challenge with risk of further fragmentation in the EU. Interoperability is a central focus – the ECB takes collateral in 21 jurisdictions, making clear that without interoperability and standards the ecosystem cannot scale. Kóczán closed by encouraging market participants to engage with the ECB's published documents and to share their views directly.

In the Q&A, Kóczán addressed several questions. On stablecoins of other currencies, he noted they may provide more flexibility than traditional means of payment or tokenised deposits but ultimately need conversion to something more stable – the role central bank money will play. The ECB is not opposed to the market using private settlement assets but history shows overreliance on private money does not work; a central bank "superstructure" remains essential. On the six Appia building blocks, Kóczán noted the greatest practical interest in collateral and central bank money access so far.

PANEL DISCUSSION: AGENTIC FINANCE – WHEN AI AGENTS MOVE MONEY

Moderator: Sean Murphy, Partner and NRF Global Head of FinTech.

Speakers: Jordan Wain, UK Public Policy Lead, Chainalysis; Kat Cloud, Head of Government Relations, Sumsub; Austin Elwood, Digital Assets Industry Lead, NatWest Group; Felix Haynes, International Policy Senior Associate, Coinbase

In this panel, moderated by Sean Murphy (Norton Rose Fulbright), speakers explored agentic finance, its regulatory and compliance challenges, and issues to be resolved as AI agents increasingly interact with digital financial infrastructure.

Kat Cloud (Sumsub) explained her firm has built an AI agent to streamline compliance, including SAR submissions. Agentic AI is increasingly used for KYC and onboarding, but UK deepfake attempts increased by 94% according to the Sumsub Identity Fraud Report 2025. Jordan Wain (Chainalysis) explained the firm is a blockchain analytics platform tracking on-chain activity and associating it with real-world entities. Felix Haynes (Coinbase) explained that Coinbase has developed a focus on financial infrastructure, launching x402, an internet-native payment protocol enabling AI agents to request and process payments. Austin Elwood (NatWest) discussed how NatWest is positioning to support customers while protecting them from ecosystem risks.

On what agentic finance means and how it differs from traditional algorithmic systems, Cloud explained agentic AI enables automated workflows with delegated execution, moving beyond "if, then" models. Users set parameters and the agent operates flexibly within them. Wain added that agents are given objectives rather than rules, enabling them to initiate and complete actions without a human in the loop.

On scale, Haynes noted agentic AI offers both institutional benefits and transformative consumer potential. AI has broken traditional expectations – LLMs barely used two to three years ago are now mainstream. With approximately £300 billion in zero-interest UK current accounts, there is appetite for systems accessing better products. Wain cited data showing $100 million of agentic transactions over nine months on Coinbase; six months ago most were sub-cent bot-to-bot transactions, now 95% are over a dollar. Haynes added that Coinbase developed the first SEC-registered AI adviser.

On liability when an AI agent makes unauthorised payments, Cloud noted traditional models are inadequate. Sumsub advocates for credentials tied to verified humans so liability can be assigned at the breakdown point. On "know your agent" in practice, Elwood noted a key question is who has authorised what in the chain, and how KYC costs are passed down.

Wain raised detecting money laundering and sanctions evasion when AI agents initiate transactions; with agentic payments, compliance windows once measured in weeks compress to seconds.

On whether agentic finance expands the attack surface, Cloud noted AI bots may exploit KYC loopholes. On whether digital assets are better suited to agentic models, Elwood stated this remains to be seen – NatWest is reviewing how programmable payments could integrate with agentic AI. Haynes added there is no inherent incompatibility between traditional and agentic finance, but frictions remain around bank account access; stablecoins and programmability offer promising solutions.

In the Q&A, Cloud noted corporate use cases such as streamlining client onboarding, while Haynes referenced a mass caterer using AI agents to track ingredients and trigger supply requests. Corporate uses remain somewhat limited due to lack of a clear regulatory framework.

On "agents gone wild" and hallucinations, Cloud noted her organisation has been trialling a KYC platform tracking behaviours indicating potential hallucinations through retrospective study. On consumer liability, Elwood stated any organisation pushing liability to customers may disappoint customers and, ultimately, lose business. Cloud observed some liability will always rest with customers – for example, where they fail to set correct parameters. Haynes highlighted the importance of clear disclosures when using agents, noting FCA examination in its Sandbox. Elwood added organisations may need to make customers whole to fulfil expectations of how the system should work.

CLOSING KEYNOTE

Speaker: Christopher Woolard CBE, Wholesale Digital Markets Champion, HM Treasury

Christopher Woolard opened by noting he is preparing a report due for publication at the next Mansion House in four weeks. This is intended as a roadmap on how to approach tokenisation in the UK and how it fits into the Wholesale Digital Markets Strategy. A second, more substantive strategic report is due July 2027.

Woolard noted that a large taskforce spanning the economic landscape has been developed, with his role being to facilitate and bring together industry views with those of the authorities, including the Bank of England, FCA, and wider government. Woolard emphasised this is not an academic exercise; the market is no longer asking whether tokenisation will happen, but when and at what scale. Banks are thinking about incorporating DLT into existing infrastructure while new entrants consider what to replicate of traditional models. Interoperability is significant, as is what happens to liquidity pools – some believe a fracture is inevitable, while others see ways of interconnecting them. This is a deeply strategic initiative for the UK, concerning not just efficiencies but the right to participate in the next generation of financial services.

On why tokenisation matters, global crypto markets are worth approximately $3 trillion, with around $300 billion in stablecoins. While tokenised assets are currently small-scale, if 15% of existing markets became tokenised, that would represent $80-90 trillion. Even a 1-2% improvement in capital efficiency would produce significant uplift. From a UK perspective, approximately £4 trillion is settled every working day with London clearing houses processing 80% of the world's interest rate swaps. Key areas for tokenisation include repo and FX, and the UK's trusted legal framework provides further advantage.

Woolard sees his role as a bridge between industry and authorities. Key themes in his first report will include: joining up initiatives, encouraging secondary markets for tokenised assets; the role of finality and required infrastructure; collateral; and interoperability. He pointed to progress including the Digital Securities Sandbox, the Digital Gilt Instrument (DIGIT), and the Great British Tokenised Deposit (GBTD). The UK has demonstrated technical capability; the question now is how to move beyond proof-of-concept. Being Digital Champion means seeing practical progress and pursuing ambitious yet pragmatic objectives.

In the Q&A, on the taskforce's role beyond reports, Woolard noted the 70-member taskforce will likely divide into smaller working groups. Industry participants must lead, with government support where required. On funding, incumbents face difficult economics in changing successful business models, but given tokenisation's relevance to London, it is a "punt" most firms are willing to make. Investment will come from firms seeing real-world use cases rather than from a central pot.

HOW CAN I GET INVOLVED?

Since 2021, GBBC has released the International Journal of Blockchain Law (IJBL), an open access online journal written and edited by lawyers, designed to help business and non-legal communities better understand the world of blockchain and digital assets.

Interested in submitting new work to or becoming an editor for IJBL? Review the submission guidelines below and write to us at IJBL@gbbc.io.

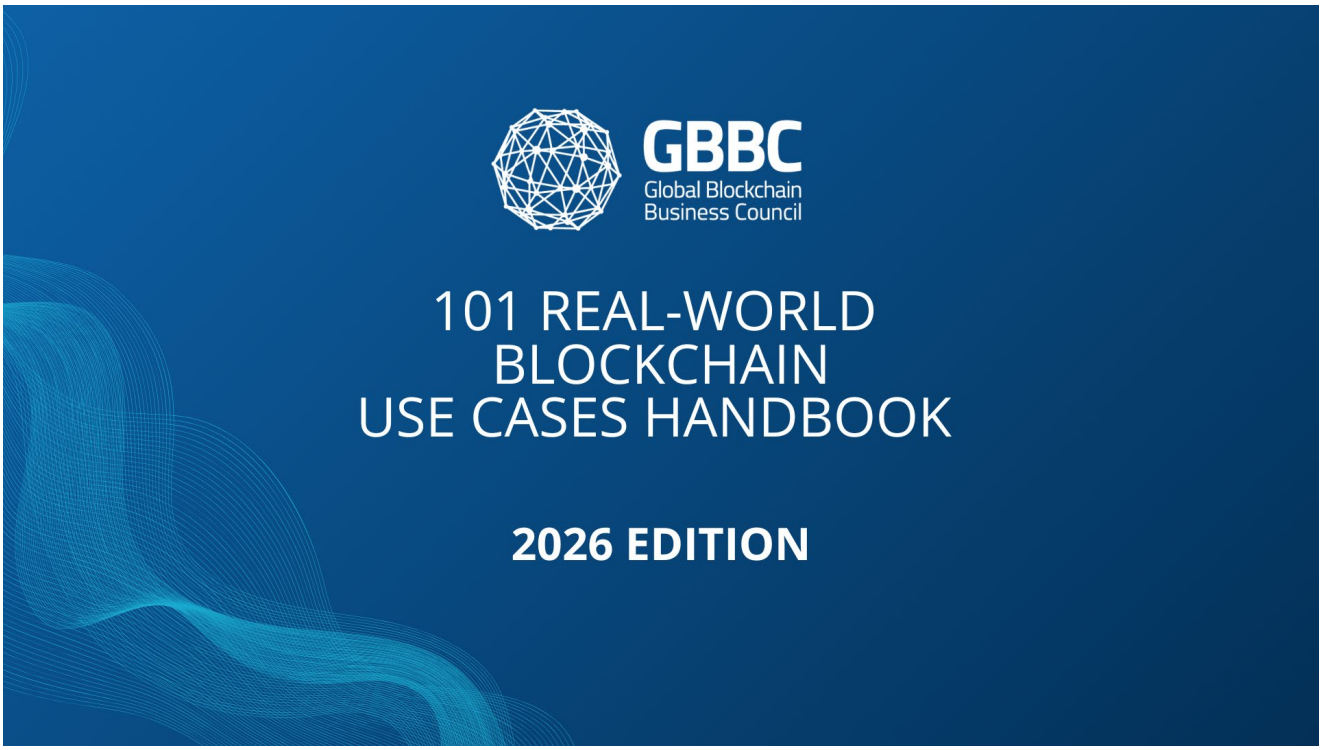
Length	3-4 print pages including footnotes
Target Audience for Submission	Broader business community aiming to better understand the technology and the legal issues associated with it
Content	All legal areas related to blockchain technology and digital assets
Structure	Introduction - Description of legal matter - Proposed solution - Conclusion/key takeaways
Writing Style	Not too academic; lucid and clear-cut language
What Can I Submit?	Previously published work is welcome for submission to the IJBL

GBBC COMMUNITY'S 101 REAL-WORLD BLOCKCHAIN USE CASES HANDBOOK, 2026 EDITION

In June, GBBC and our global community released the 101 Real-World Blockchain Use Cases Handbook, 2026 Edition, highlighting how blockchain technology is being applied to address real challenges across industries and jurisdictions. The latest edition brings together examples from organizations worldwide, reflecting the continued development and growing impact of blockchain-based solutions.

Designed as a practical reference for government agencies, regulators, central banks, industry leaders, and other stakeholders, the Handbook supports a deeper understanding of blockchain and digital assets. Moving beyond the hype, it demonstrates how these technologies can improve transparency, efficiency, accessibility, and security while helping build stronger and more resilient systems.

Thank you to our global community for sharing your expertise and the important initiatives you are advancing. Your contributions make this resource possible and help bring greater visibility to the tangible impact of blockchain technology around the world.



ACCESS THE HANDBOOK