✉ info@databoiler.com https://www.databoiler.com

You cannot regulate what you cannot define + The Clone Wars

One cannot jump to the "How" when the "What" has NOT been properly defined. Despite the EU being the first to come up with their Artificial Intelligence (AI) Act and Canada being at the forefront of digital assets laws, there is NO first mover advantage in rule making. It is better late than never if we can get it right when framing the regulatory solutions to the problems in the AI and Crypto spaces. This 3-part sequel aims to decipher the noumenon of and define what AI, DeFi, tokenization and cryptocurrencies truly are.

Definition of AI

AI is NO ordinary *"machine-based systems"* or *"automations"*, but a *"cognitive system"* capable of *"learning"* to continuously improve the Functioning of a Computer / to any Other Technology or Technical Field (e.g. a GPS Satellite system is NOT AI, but traffic predictions and personalized recommendations are). By referring to AI as *"cognitive"*, the focus is on the system's internal (mental like) processes, rather than SOLELY on external behaviors and consequences.

Learning per the *"Dog Salivating Theory"* that nurtures voluntary behavior by pairing external conditioned stimulus to associate two or more phenomena, such technique alone does NOT constitute it as AI. Computational techniques that mimic pet training in itself are insufficient or unlikely to inflict harm on humanity, except exploitation of Dopamine for addictive behaviors. Also, the presence or absence of *"operant conditions"* could merely be automation in itself to modify voluntary behavior through external consequences (reacting to the laws) of reward and punishment. Without combining it with other internal (mental like) computational techniques, such systems should NOT be considered as AI.

CAPTCHA – a security test that uses a *"Turing test"* to differentiate between humans and bots is NOT AI in itself. However, Google reCAPTCHA system is part of an AI that consists of internal processes (e.g. keylogging to track and analyze user interactions, such as mouse movement and typing patterns) to determine if a user is human. Keylogging without a user's consent could be invasive to privacy; hence it should be a regulated activity. Another computing activity that should be regulated is – the use of AI to help bots bypass CAPTCHA or the like security test, except when used for ethical hacking.

A crawler or web scraper that automatically extracts data from an external environment (web) is NOT inherently an AI. When combining crawler's function with internal processes involving intelligent data analysis to enhance the data collection with contextual understanding (rather than just the keywords search), then such system is an AI.

A scanner or camera to surveil the public area outside of private property is NOT an AI. Adding a sophisticated system that has internal processes to control one or orchestrate multiple surveillance camera(s) to enhance the monitoring with contextual awareness (e.g. facial recognition to analyze identity) is an AI.

We despise heavy-handed government policies to brutally force AI firms to censor / filtering so-called *"unsafe behaviors / outputs"* or require adversarial training to ban or reveal what authoritarian may constitute as *"vulnerabilities"*. We are thankful for Vice President JD Vance remarks at the AI Action Summit, in particular *"AI must remain free from ideological bias, and that American AI will not be co-opted into a tool for authoritarian censorship."* It helps address civic concerns over massive government surveillance. NOTE: *"Ideological bias"* is a human bias driven by political or social belief. Whereas *"bias"* in many domains – especially competitive ones like defense or finance – bias is not just inevitable, it is essential to: prioritize certain outcomes (e.g. speed over accuracy, stealth over transparency), reflect strategic performance (e.g. risk tolerance, adversary modeling), and/or to exploit asymmetries (e.g. alpha in trading, deception in war).

There are different AI machine learning algorithms, some use cognitive reasoning for multi-step strategic plans (e.g. chess game) where *"bias"* is essential. Others use non-reasoning (or generative) models excel at fast, pattern-based tasks like content generation or chatbots where consensus building and/or optimization for the most commonly accepted respond (consistency in reproducibility of outcomes) is prioritized. One size does not fit all.

Bias can be *"conscious"* and *"unconscious"*. A cognitive system does NOT have to be conscious. Neuroscientists believe consciousness could be a distributed process that does not depend on a singular *"self"*. Unconscious bias can inflict harm amid unintentional – negligence. Cognitive systems with no recommendations should NOT escape AI responsibilities. *"Bias"* depends on social norm. Social norm evolves overtime.

"Signal amplification" is an absolute necessity in sequencing technologies. It enables detection, ensures accuracy via redundancy, and is particularly useful when working with limited input material. However, amplification inherently introduces *"technical bias"* into sequencing data – a known and acknowledged challenge, but it may be better than the inability to generate any data at all.

The US trade surveillance process *objectively* checks if a trade has the effect of altering the worth of a target. It is a *red flag* of market manipulation if the trade caused a *"bias"* in market mechanism. The challenge is how to distinguish between a *systematic technical bias* or human-made *artifact* in data, from *natural evolutionary bias* or *selection*. Content preference and context bias are highly dependent on the specific use case or application, i.e. largely *subjective* and situational.

"Normalization" is the statistical data smoothing process that meant to address *"bias"*. Yet, whenever one applies computational methods to the data, the relationship between the true *"signal"* and the technical *"noise"* is inherently altered. There is a trade-off in gaining clarity of signal at the potential cost of introducing subtle *"new biases"* or *suppressing* real, but weak, *"signals"*. Strive for the most timely, accurate, relevant, and complete data where possible to avoid excessive manipulation in normalization for the best sequencing results. Unfortunately, consolidated tape without time-lock encryption to make market data available securely in synchronized time caused *"initial bias"* that exacerbates the gap between subscribers of proprietary feeds and the public SIPs.

Hallucination is considered an output that is out of norms. Hallucinations are like dreams (a state of consciousness that one's *"awareness"* of external environments may be out of synch), except dreams may be more vivid / emotion than hallucinations. Human's five senses are less active when dream. When AI sensory attenuation primarily focused on language or visual images, it undermines other sensory inputs, such as sound, touch, smell and taste, etc.

AI is often being mythologized by humans as all-knowing. People expect instant gratification. Yet, AIs are like *replicas* of humans. There will be occasions of *"I don't know"*, irrelevant fluff being generated, stuttering, or words could not catch up

with thoughts. The ability to form and process complex thoughts is distinct from the ability to articulate fluently and coherently. Improve context awareness, better adversary training, use of ensemble learning, and multimodality all contribute to reducing AI hallucinations but cost extra time, efforts, and may introduce noise.

Unlike *data* extraction that can be *timely*, *accurate* and *complete* if one is willing to pay extra, *intelligence* may never be 100%. I.e. AI *prediction* or *advice* seldom possess all attributes simultaneously due to in inherent constraints, such as information asymmetry, the tension between speed and quality, cognitive limitations, and the dynamic nature of reality.

Do NOT lambast AI for hallucination. Humans often fail to think critically, unable to synthesize information from various sources for evaluating information to find deeper meaning, and lack adaptability and creativity. Yet, humans like to dream and imagine. Should cognitive systems be allowed to dream – a possible indicator of Artificial General Intelligence? AI hallucinations may discover unknown unknowns which were previously nonsensical to human. To better understand nuances and enhance AI performance, policy makers should incentivize the industry to turn *"unknowns"* into *"knowns."*

The last administration inappropriately assumed or interpreted *"AI bias"* as systematic and repeatable error in a computer system that creates unfair outcomes, such as disadvantaging a particular gender or race. This contradicts with the current administration's merit-based policy (EO 14173) that dismantles Diversity, Equity and Inclusion (DEI) initiatives. Trying to *"neutralize"* biases in pursuit of consensus or fairness can dilute the US strategic advantage, especially when foreign adversaries are not playing by the same rules.

The EU AI Act mandates development of a Code of Practice on General-Purpose AI is problematic. Best practice sharing is not wrong. Concern is – how they would consider *"the Code's design and build coherence where needed"*? Regurgitating GRC tools as AI compliance is the wrong approach. *"Coherence"* limits creativity. Differentiation is what drives innovation. The EU Digital Markets Act aims to ensure *"fair competition and practices among large online 'gatekeeper' platforms like search engines and app store"* is nothing but a protectionism policy. Invoke Antitrust laws may suffice.

China recently released their *"AI Safety Governance Framework 2.0"* (CN-AISGF2). Their cybersecurity law, computer crime criminal law (Articles 285-287), and Personal Information Protection Law are their broader policies that prioritize their national security and state control. CN-AISGF2 looks undeniably comprehensive as we compared it against the 2022 version of the US NIST-AIRMF (see pages 9-10 of our comment letter). Their usage of familiar GRC best practices make it appealing for foreign jurisdictions to adopt it. The US NIST-AIRMF playbook and related guidances if blindly continuing the oversimplified *"Govern"* in center of *"Map, Measure, and Manage"* (GMMM) path may end-up similar to CN-AISGF2.

In order for the US to exert influence on Global AI policies, the US AI regulatory regime should re-center the focus on the identified key AI risks (energy; addictive, herd and/or polarized behaviors / destroy humans' abilities to think independently; censorship; hyper optimization; insurgent / unhealthy competition) to mitigate the downfall of humanity. Policy Makers should consider the Asimov's Three Laws and Zeroth (Forth) Law for AI. The ISO 23894 Risk, ISO 42001 management system, and ISO 38507 governance frameworks should be redirected accordingly. Meanwhile, the Department of Justice's Computer Fraud and Abuse Act (CFAA) has a narrower statute if compared to other jurisdictions. CFAA is meant to target external hackers' unauthorized access and damage; it does NOT impute liability to internal workers who disregard a use policy. Bypassing code would constitute a cybercrime ONLY if the code is a *"real barrier"* as opposed to a *"speed bump"*. *"Function creep"* is concern we identified with the FINRA Consolidated Audit Trail (CAT) system. Adverse scenarios with government and bank systems have happened with serve consequences.

The original inventor may never come up with an exhaustive list of usage purposes or anticipate the possible repurpose of his/her technology. It is unjust to require AI firms to *"establish comprehensive and explicit enumeration of AI systems' context of business use and expectations."* Do not expect examiners to truly understand every bit of "contextual factors may interact with AI lifecycle actions", for they are rule and law enforcers not technologists. Free enterprise should NOT be obligated to reveal the secret ingredient of their technologies, unless it is being identified with evidence for suspicious crime.

We agree with the NIST AI Risk Management Framework (NIST-AIRMF) Playbook (page 63 - Map 1.4) where it said, *"Socio-technical AI risks emerge from the interplay between technical development decisions and how a system is used, who operates*

it, and the social context into which it is deployed." Yet, these are applicable to all technologies, not just AI. There are already a long list of US data / information security standards and technical safeguarding requirements, such as PCI DSS, GLBA, SOX DS 5.7, 5.8, 5.11, 11.6, HIPPA ePHI §164.306, §164.312, etc. Rights to revoke a user agreement with a standard provision, such as *"no illicit or manipulative use of technology"* may suffice.

The collective thoughts above lead us to recommend a revised definition of AI under 15 U.S.C. § 9401(3) to preempt state AI laws, we suggest using the following or the like:

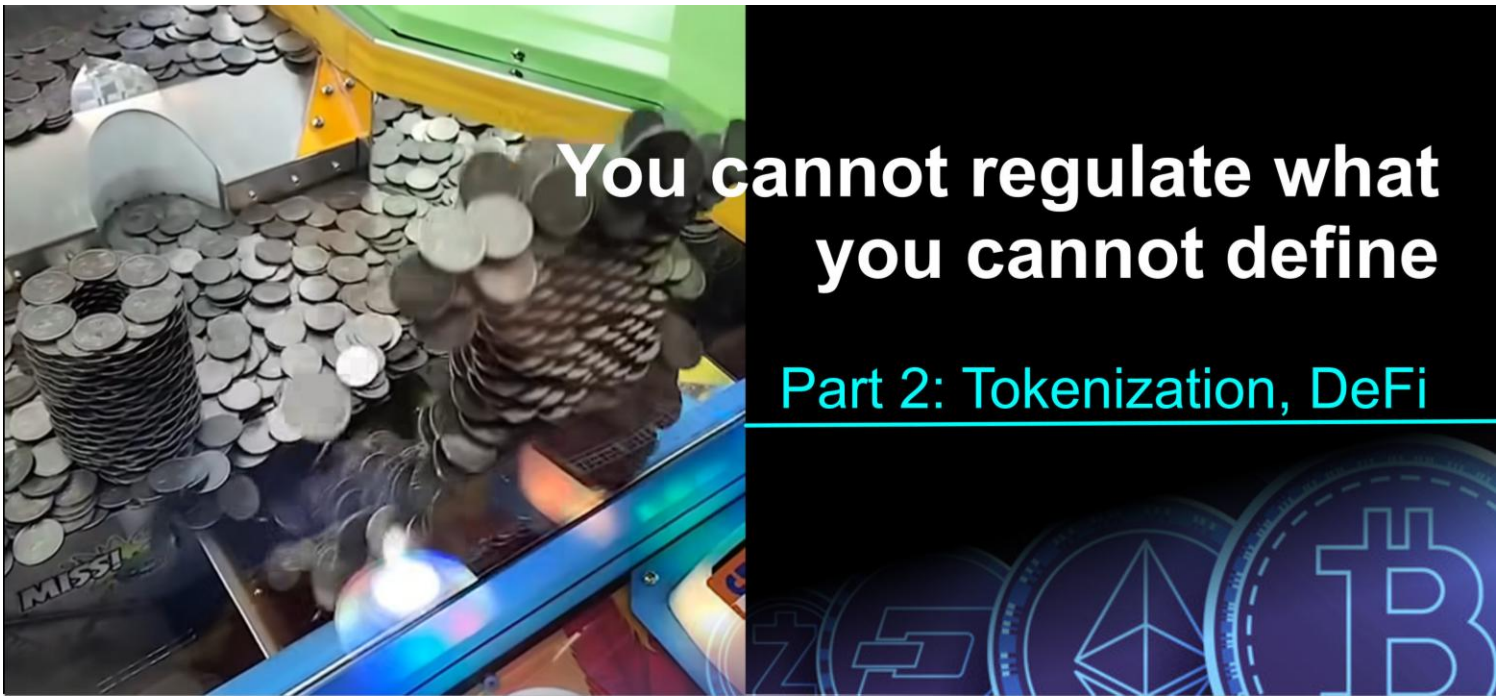
"Covered AI technologies refer to cognitive systems (beyond learning from pairing a neutral stimulus that becomes a conditioned stimulus), comprise of memory AND topology of known lessons, that learn from regularities and irregularities of pattern(s) / knowns and unknowns / models/ simulations, AND

the system's internal process EITHER comprises of multi-steps reasoning (understand in a way that mimics humans; NOT merely extracting signals to generate alerts; NOT unconscious thinking) OR capable of generating datum uniquely different from a plagiarized copy, that

manipulates or presents at least an abstracted phenomenon (person or avatar, thing or computer-generated element, or real or virtual event that is hypothetical or observed to exist or happen in a distanced past, real-time, or irrespective of space-time) in a metaverse, real, or virtual environment

autonomously OR follow commands/ instructions, to generate expectations, make-believe, or assert that certain selected or perceived phenomenon is or will occur / available for use (regardless of the system internalizes, consumes, or makes feed(s) / datum available to its users in a domain, a dark web, or any iteration of the internet or intranet), AND

through action (including provision of customized or generic recommendation that reinforces, strengthen or weaken an ideology) OR inaction to stimulate the thought processes of at least an individual human OR the operations of a machine."



What "tokenization" or "DeFi" is truly about

In a sharing economy, crypto / Digital Ledger Technology (DLT) are like other shared services (e.g. Uber, Air B&B) that unleash tremendous *"societal values by promoting access over ownership, which challenges traditional notions of property rights."* We think the Bank for International Settlements (BIS) has an overly complicated definition or concept about *"tokenization"*. Tokenization to some extent may equate to Securitization, when it serves as an alternative or a poor person way for securities issuance and asset gathering processes. Putting it in layman terms, both *"tokenization"* and *"securitization"* aim to make assets tradable and liquid.

We have no objection with the IOSCO's statement, *"Tokenization arrangements typically seek to achieve one or more of the following features: Fictionalization, Programmability, Composability, and Atomicity."* A nuance – fractional participation in a tokenized product that is otherwise framed as a risk management or treasury tool with no general solicitation or advertising, no emphasis on profit potential, offered as part of a broader banking relationship and is a direct bank obligation under *"incidental banking service"*, may be considered as investment activities under the current law.

If the tokenized product meets the criteria of an *"investment contract"* under the Howey test or falls within the statutory definition of a security under the Securities Act of 1933, then one may use private placement (Reg D) and restrict access only to accredited investors. If it is structured as a commodity option, it may be offered only to Eligible Contract Participants (ECPs) via registered Futures Commission Merchant (FCM) / Retail Foreign Exchange Dealer (RFED). The current narrowly defined banking exemptions that community banks and credit unions are forced to handover business to a third-party or their larger counterparts with a brokerage / securities service arm. Clients suffer from bureaucracy and higher fees.

When formal orders legitimize exploitations, informal sub-orders will emerge as a counter response. If policy-makers want tokenized activities in the above example to go away (without price control to curb the Elites, nor rule-by-enforcement that is a double-edged sword), we recommend granting a *"break-bulk exemption"* (e.g. shared representation of a claim < 35, aggregate < 110% cost if client was otherwise engaged in individual contract).

We recognize that, for example, credit card reward points, frequent flyer programs and the like, if tokenized to allow easier transfer of these *"reward tokens"* to freely trade and exchange with other third-parties beyond family members may serve good community values. NOTE: *"tokenized reward points"* may have unlimited supply and program organizers may have "small-print" discretionary clauses to change or alter reward programs at any time (analogy to *"hard fork"* – a backward-incompatible upgrade to the blockchain).

There is no single authoritative FASB standard under the US Generally Accepted Accounting Principles for how a recipient of reward points or tokens should be accounted for. Commercial practices vary – some treat them as a *"freebie"* and not keep any record of it in an accounting book, others consider it as a *"rebate / discount"* deducting them directly from expenses, also certain firms may consider it materiality and treat them as a *"prepayment asset"* on their balance sheet.

Firms operating *"reward programs"* must choose between ASC 450-30 Gain Contingency Model and ASC 606 Vendor Rebate Model to develop a defensible and consistent policy. There are different valuation-of-rewards approaches – (i) direct cash-out value, (ii) estimated redemption value, or (iii) conservative average based on historical redemptions – timing of recognition varies depending on the policy – (a) at redemption, (b) when statement is issued, or (c) when qualify purchases are made. Additional nuances include but are not limited to: no purchase requirement, consolidation of reward programs, tax treatment, interest or yield bearing on these *"reward tokens"*, etc.

Smart contracts are an *oversimplified* mechanism for delineating complex real-world rights and obligations. Challenges include: limited access to off-chain data; interoperability issues, where different chains operate in silos; immutability (which provides security but leads to inflexibility or difficulty capturing legal nuances when dealing with evolving circumstances, renegotiations, or unforeseen events). In turn, hybrid solutions are being created, resulting in DeFi *convergence* to TradFi with no necessary efficiency gain.

Are commercial disputes or consumer protection mechanisms being insufficient that it calls for involvement of securities laws? Are many existing commercial reward programs being unsustainable and they seek tokenization as an exit or chance of revitalization? Would *"rewards"* be used as alternate means to raise funds cheaper than bank loans, Private Equity or Venture Capital funding? There are more questions than answers. The US Congress should refrain from laying an invisible hand of Government to regulate these private *"reward program"* activities. Regulatory agencies, the SEC and FINRA in particular, do NOT have the necessary capacity to practically review hundreds of thousands, if not millions, of applications to register these *"reward tokens"* as "securities".

Tokenized assets can be uncountable, i.e. unlimited supply. Uncapped supply creates inflationary pressure; hence value of such digital assets cannot be properly determined or quantified by the amount of outstanding inventory. The original Dodd-Frank Volcker rule's securities Inventory RENTD provision has it merits. Uncountable *"Funny money"* is more akin to *"non-cashable gambling chips"*. NOTE: there is no formal *"certification body"* for token classification in the US, but to rely on issuer's initial representation in simple agreement for future tokens (SAFT) to *"self-certified"*, p.s. $BTC has no centralized issuer, no initial sale or fund raising.

CFTC is in a better position than the SEC to regulate the trading of Spot Crypto Asset Contracts and Tokens sold via SAFT. CFTC authority under §2(c)(2)(D) of Commodity Exchange Act (CEA) and COMEX Rule 7 help curb and mitigate situations such as the Monex case, retail metal fraud cases, and Silver Thursday event. We recommend the CFTC to require Designated Contract Markets (DCMs) to set aside at least 1 to 2% of gross revenue allocated to risk education program for existing and prospective retail clients, on top of protection against abusive practices, and updating Core Principle 12 outlined in §5(d) of the CEA and Part 38 accordingly. We do NOT want the SEC to cross subsidize the cost to regulate crypto from equity trading.

The SEC Chair suggested *"digital commodities,"* "network tokens," "digital collectibles," and *"digital tools"* are NOT securities. We agree with and support the SEC oversight on *"Governance token with rights"* and *"Covered Liquidity Staking Receipt Tokens"* and that fits squarely with the definition of *"securities"* as well as those involves *"bundled services"* that resemble an investment contract. We have no objection to the SEC establishing a safe harbor for certain airdrops from characterization as *"sales"* under Section 2(a)(3) of the Securities Act or an exemption from the corresponding registration requirements under Section 5 of the Securities Act. The SEC should also consider an exemption for distributions of digital assets by decentralized physical infrastructure (DePIN) providers in securities transactions for purposes of rewarding participation in DePIN networks, and distributions of certain NFT offerings. We are open minded about DePIN transformation to serve the US in the long-term.

We do appreciate the duo oversight setup under the *"Responsible Financial Innovation Act proposal"* (RFIA) regarding *"Ancillary Assets,"* – the SEC gatekeeping the primary sales and the CFTC be the secondary trading regulator. The Public

Company Accounting Oversight Board, oversighted by the SEC, should determine the proper ways in measuring, recording, and disclosing of *"Ancillary Assets".* We look forward to the RFIA final bill formally introduced in the Senate that will address the asset classification protocols issue prompted by the CFTC v. Archegos Capital Management LP case.

Meanwhile, the Senate Agriculture Committee released a bipartisan November 2025 draft. It aims to merge with the earlier RFIA draft that expands the CFTC's authority over the spot market for digital commodities (e.g. requires digital commodity exchanges, brokers, and dealers to register with the CFTC), and overlines mechanisms (joint advisory committee, joint rulemaking, and innovation sandbox) for better coordination of the SEC and CFTC's roles.

Categories	Primary Sale Regulator	Secondary Trading Regulator	Ancillary Asset Status
Digital Collectibles, Non-Fungible Meme Coins for entertainment, social and cultural purposes	NOT the SEC	CFTC (if involve CEA regulated commodity options, futures, or leveraged OTC transactions)	Not applicable
Spot Crypto Asset Contracts, currently limited to Bitcoin (BTC) and Ether (ETH) that are widely treated as commodity	Not applicable	CFTC (DCM Listing, focuses on fungible, peer-to-peer digital assets, while excluding securities, stablecoins, and tokenized real-world assets)	Not applicable
Fungible Token sold via Simple Agreement for Future Tokens (SAFT) used by crypto developers to raise capital from accredited investors before a token is live or functional	SEC	CFTC (if ancillary asset)	Possible if self-certified
Covered liquidity staking receipt tokens, Governance token with rights, Spot Crypto ETPs	SEC	SEC	Not eligible

The SEC should refrain from regulating any *"uncountable"* digital asset that is more akin to *"non-cashable gambling chips."* It should not be subjected to investor protection over securities trading activities. Wrapping money-market fund protections around this *"funny money"* does NOT make it any safer (lipstick on a pig is still a pig). The SEC does NOT need to reconsider its withdrawn Safeguarding rule proposal, which – if revived and modified to accommodate digital asset nuances—could be a detriment to the time-tested Exchange Act framework.

A caveat – crypto Exchange Traded Products (ETPs), the underlying assets do NOT necessarily have to be *"securities"*. The SEC's recent approved $DOJE is a crypto Exchange Traded Fund with underlying *"assets"* being MEME Coin. Recalling a statement by the SEC Division of Corporate Finance on Feb 27, 2025, it stated that *"MEME Coins for entertainment and social cultural purposes are NOT securities."* Any *"Digital Collectables"* that do not involve CEA regulated commodity options, futures, or leveraged OTC transactions, it would be outside scope of CFTC's oversight. Reliance on the regulated structure of the product and the transparent disclosures for the valuations and the regulatory controls may be an insurmountable reality. That guardrail may ONLY shuffle fraud and manipulation risk out the door of SEC regulated markets, but NOT stopping the risk spreading elsewhere. Bad actors / foreign adversaries play across markets and payment systems simultaneously.

We have reservations with the SEC newly approved generic listing standards. Its first criteria – *"The asset is listed on a market that is a member of the Intermarket Surveillance Group"* (ISG), reminded me of AIG – notorious for engaging in credit enhancement and securitization that led to their financial distress during the 2008 financial crisis. Most members of ISG are stock exchanges. An ISG can be bought and sold easily (Kraken acquired Small Exchange). KalshiEX is facing regulatory scrutiny and litigation. Some ISG members domicile outside of the US may have close ties with their respective governments (HKEX's subsidiary LME involved in a notorious futures contracts cancellation case). We certainly welcome our friendly foreign regulators (CIRO and ASIC) as members of the ISG. UK Prime Minister Winston Churchill once said *"We have no lasting*

friends, no lasting enemies, only lasting interests." Can the US rely on foreign organizations to act in America's best interest without being taken for granted? Would the US retreat from global governance be exploited by other powers?

The US cannot call for an outright ban of crypto like China. Foreign nations promoting their own Central Bank Digital Currency (CBDC) while pushing other digital assets out their doors or allegedly *"exporting"* DeFi to the US is a de-dollarization attempt. Among the $4 trillion aggregated market capitalization of all cryptocurrencies, stablecoins are about 7.5% (~ $300 billion). NOTE: the 1:1 reserve requirement under the GENIUS Act is NOT a daily mark-to-market, but rather requires permitted issuers to provide monthly public reporting on their reserve assets. The dilemma is – the more we add new compliance requirements, the more accumulated bureaucracy in dragging the US productivity. Foreign adversaries want the Western civilizations to fall in their trap. The approach to *"suck"* new money from Digital Asset activities may be unconventional (like Mafia making other gangs abide by their rules), but becoming the biggest force behind DeFi is better. We recommend:

Dollarize everything to turn the table against de-dollarization threats, even if it means spreading the risk abroad. The EU should NOT perceive the US as a hazard. Western Civilization should stand by the US against countries with human rights violations that hide under the guise of *"safety monitoring and assessments"*. The phenomena of currency and tariff wars today are the result of breached contracts (some US allies included).

TradFi establishments infuse trust into crypto ecosystem while a toll gate to profit or rent seek from flows passing through their infrastructures is inevitable. To prevent these infrastructure providers from exploiting small investors, we recommend a 2-tier or a dual-track regulatory regime (see page 5 of our comment letter to the CFTC). DCM's betting odds may be used as a reference if the operator of such platform may also apply for Securities Exchange or Alternative Trading System license(s) under the SEC oversight. In vice versa, the SEC should review the long-term betting odds of Stock Exchanges to consider license renewals or enforcement actions. This helps keep both the *DeFi* and *TradFi* intact, where healthy competition will be promoted, bureaucracy and barriers would be minimized and removed.

The ideal way to weed out Illicit activity involving Digital Assets is by reducing bureaucracy and removing barriers that widened the gap between the *"haves"* and *"have nots."* When the World prospers more under the US leadership, there will be less bad actors and adversaries.

Defining the problems and preventing the downfall of humanity

Amid domestic issued stablecoins and foreign issued stablecoins may be backed by same assets, regulatory regime ought to differentiate and skew it in favor of stablecoins issuance by a US based permitted payment stablecoin issuer (PPSI).

Impose a 1 to 2% of gross revenue surcharge on Exchanges and DeFi protocols requiring their allocation of the fund to risk education program for existing and prospective retail clients, instead of addressing the loophole about *"third-party"* offering of interest on stablecoin holdings (amid GENIUS Act prohibits stablecoin issuers from paying interest directly).

Policy makers should make sure these crypto infrastructure providers would not just profit from the US and betray America's interest. They must always abide by the US rules; particularly their products and processes should ultimately tie back to strengthening the US Treasury and repos markets. This is similar to the Dodd-Frank Volcker rule having an explicit exemption on US Treasury and repos. Per BIS, *"some stablecoin issuers rely on reverse repos to generate additional income. During market stress, this could strain repo market liquidity, with spillovers on other short-term dollar funding markets. In addition, interconnections arise through direct exposure to banks via deposit holdings…"*

We have reservation with the BIS / IIF prescribed unified ledger / Project Agorá that integrates different financial assets and central bank money onto a single, programmable platform to automate and streamline transactions. The CAT system has set a bad precedent. To effectively mitigate privacy and security risks without creating bureaucracy, do keep in mind the following three management fundamentals: (i) segregation of duties, (ii) keep clean with high incentives (e.g. whistleblower award), and (iii) precognitive prevention by reducing the number of unknown unknowns. Better to analyze data directly at its originating source and scrutinize high risks cases as prompted by informants / suspicious activity intelligence. Also, agentic AI may use baits to catch illicit activities hopping around.

Twenty-first century challenges include a rebellious move by an insurgent with a war chest to orchestrate a market wide shake-up, and foreign adversaries wanting to erode the US's prominent market position. Bad actors / foreign adversaries play across markets and payment systems simultaneously. Per Professor Hélène Rey, policy makers should observe and monitor *"the magnitude and substitution patterns between dollar-backed crypto assets and money market funds and deposits in local*

currencies and dollars." Also, China's 2024 US dollar bond issuance in Saudi Arabia had yields on par with or slightly above US Treasury benchmarks, while its late 2025 Hong Kong issuance had yields that were slightly below US Treasury equivalents for similar maturities. These *"clones"* of US Treasury, together with China "gold corridor" strategic initiative with the BRICS, are adversely affecting the US monetary policy in the long run.

We foresee increasing crossover activities between AI, tokenization and Digital Assets. AIs *"cloning"* from known lessons in reality or simulated environment to generate or manipulate the *"likes"* in a real, mixed, or virtual reality, a metaverse or multiverses with *selective focus*. Knowledge distillation can be a shortcut for cheap AIs to produce *"counterfeits"* or steal the fruits of other AIs. In parallel, DeFi redefines the alchemy of finance and *"cloning"* reward programs' points, membership, ticket, credential, title instrument, identity badge, money, and whatnot into digital tokens.

The high energy cost of mining Proof-of-Work (PoW) currencies creates a positive correlation with its value, especially Bitcoin and the like. If people want to outsource mundane tasks to increasingly complex matters to AI agents / machines, AI may require equivalent exchange of computing power / energy represented by crypto in the future. Some make PoW simpler, yet Proof-of-Stake systems are vulnerable to voting paradoxes. *"Simplification"* undermining the problem of tyranny of the majority (i.e. oppression of minorities, exclusion of value input causing poorer decision-making, and intensified conflicts by refusal to compromise leading to social polarization and unrest).

Simplifying everybody's life is an honorable goal, yet AI if misused can enslave humans. Deskilling and overreliance on AI make people become simple minded. People turn into couch potatoes when they lose their independent critical thinking and handy person's abilities. All AIs want to be fed, but inputs versus outputs will get out of proportion. The Good – some GenAI prompt users to choose from few suggestive questions to keep the human and AI dialogue going that sharpen each other's mind. The Bad – some Large Language Models intentionally cause *additive behaviors*. The Ugly – AI social credit score. While people test and measure the intelligence level of AIs, AIs use Turing, behavioral analysis, psychometric tests, and what *intelligent questions* we ask of AIs to *score* how dump different people are in vice versa. AIs ONLY rely on the most intelligent and timely inputs from humans, while giving back generic, cookie cutter, or *flattery simple* responses. If users do not want deteriorated feedback, there will be different tiers of subscriptions based on what human intelligence and crypto energy coins one is willing and can contribute or feed the AIs. This is NOT AI bias but human greed that exacerbates inequality. Tiering and scoring humans ought to be regulated.

Putting geopolitics, AI, and Crypto into a common perspective, the problem faced by humanity boils down to:

- We all screwed ourselves by *overreliance* on *global supply chain*, *technologies*, *bureaucratic financial systems*;
- Corporates keep *cloning* / *rehashing* the same legacy products and pandering it or sold *counterfeits* to the mass market;
- Authorities blame it on inadequate *penetration*, and many try to find *scapegoats* to escape their own blame;
- Most people have IBG / YBG mentality and choose to do what is *easy* but neglect the consequences of *shortcuts*;
- *Greed* and *laziness* are to blame; tensions rise where *Ruthless* (TraFi) and *Reckless* (DeFi) created each other;
- Sarcastically, in the end everyone wants everything and the world back to *"Normal"*, when the *"NORM"* may indeed mean *"it does not matter if we do not know how to do anything."* Social norms evolve overtime.

Is it the decline of the world population that we need humanoid *clones* to pick up the work where people slack off? Would nations measure wealth by the number of humanoid *clones* owned per household and the amount of tokenized energy each household can generate, rather than by cars and livable space? Does China or the US, have the better *economy of scale* to become the world dominated manufacturer of Humanoid *clones*? Are these humanoid *clones* a one size fits all multi-purposes agents or they will be like robot vacuums or automated lawn mowers that serve specific functions? In either case, short-sighted corporations *push* outdated products, exhibit a *lack of personalization*, and *underinvest* to maximize profits.

Hope is dim if all the investments in AI and Crypto are meant for another round of corporates' *push* of their *mass-produced* products. There is hope if we use AI and DeFi to tailor products and services in line with the *mass customization* global trend.

A revitalization of the US manufacturing sector will NOT be driven by humanoid clones sitting in assembly lines. *Penetrating* consumers to buy Humanoid *clones* will NOT increase the US competitiveness, except creating ever more waste like old

Electric Vehicles' batteries. *Suck* up the power enabled by AI and DeFi, so that every US household can turn their garages or any underutilize space into workshops. By equipping US households with *"robotic assisted appliances"* and low-cost access to supply and distribution channels, many would become entrepreneurs to *customize* every good and service. These *appliances* need *economy of scope* (like 3D printers or various Apps on iPhone or Android), but NOT necessarily high production capacity.

We believe the US would lead the world by unleashing *creativity* and *ingenuity*. *Gamification* is what Americans do best. It prevents AI dulling our human minds. With AI, we can detect the smallest irregularities between an original, *plagiarized* or *counterfeit* product, covered song, and genuine *derivative* product. It helps detect and deter bad actors and foreign adversaries from hiding under the guise of DeFi or any AI generated *clones*.

We are optimistic about the US AI Action Plan, particularly because of this commendable US copyright and AI report. It strikes the appropriate balance in assessing the divergence between private rights and social costs. That being said, unfinished legislative work remains after the Google v. Oracle case about *fair use*. We have been an advocate for Copyright Licensing Mechanism across industries. We suggest expanding and further strengthening the US Intellectual Properties (IP) protections. Making it cheaper and easier to enforce IP anywhere around the world. Incentivizing the discovery and reduction of *"unknown unknowns."* When the World prospers more under the US leadership, there will be less bad actors and adversaries.

***

*By **Kelvin To**, Founder and President of Data Boiler Technologies*

Data Boiler is a Type C organization member of the European Commission's Data Expert Group. Between my patented inventions in signal processing, analytics, machine learning, etc. and the wealth of experience of my partner, Peter Martyn, we are about Market Reform, Governance, Risk, Compliance, and FinTech Innovations to create viable paths toward sustainable economic growth.