**HR001123S0053 Office-wide BAA**
**Abstract**

| | |
|---|---|
| **Abstract Title** | Theory of information, money and entropy: a peer-to-peer supranational currency for an information economy |
| **Proposer Organization** | Individual |
| **Thrust Area(s)** | Economics, finance, decentralization, world modelling, AI, cryptography, distributed computing, networking, decentralization, space |
| **Technical Point of Contact (POC)** | Name: Rahul Khatri<br>Mailing Address: 380 Assiniboine Rd., #207 Toronto, ON M3J1L4, Canada<br>Telephone: 437-299-2382<br>Email: adv.rahulkhatri@gmail.com |
| **Administrative POC** | Name: Rahul Khatri<br>Mailing Address: 380 Assiniboine Rd., #207 Toronto, ON M3J1L4, Canada<br>Telephone: 437-299-2382<br>Email: adv.rahulkhatri@gmail.com |
| **Other Team Members (subcontractors and consultants), if known/applicable** | Technical POC Name: N/A<br>Organization:<br><br>Technical POC Name: N/A<br>Organization: N/A |
| **Estimated Total Cost (Base + Options)** | $250,000 |
| **Estimated Period of Performance** | 1 year |
| **Identify any other solicitation(s) to which this concept has been proposed** | DARPA-SN-23-68 Ethical, Legal, and Societal Implications (ELSI) of Emerging Technologies RFI |

**Table of Contents**

## Goals and Impact

The proposal aims to lay down a blueprint for transition of the global economy to a decentralized, peer-to-peer (P2P) data ecosystem that would underly a supranational global reserve data currency ultimately transcending humanity into an information economy in which United States peacefully prospers and avoids strategic surprise of losing hegemony over global finance. It also solves Triffin's dilemma where the reserve currency issuer faces the paradox between domestic and international objectives. Large current account deficits mean cheaper imports and capital but have hollowed out the US manufacturing sector. We propose a neutral protocol that preserves monetary sovereignty of nations and allows them to participate in a shared network for the storage, processing, transmission of data, where nation states can act as oracles and issue central bank digital currencies (CBDCs). It ultimately envisions a shared operating system for humanity that leads to exponential scientific advancement.

The implementation of this proposal would have profound impact on geopolitics, economics, and scientific research. It would be the pinnacle of the intergalactic protocol that became the internet. It will be a monument not to our greatness but to our existence. It would lead to global peace and stability anchored on global financial stability and prosperity. The protocol would act as a neutral mint with predictable inflation and as a buyer of last resort and lender. It would aid a peaceful transition of the global reserve currency from the dollar to the proposed data currency. It will ensure that US leads in development of electronics, software and automated manufacturing and becomes an advanced information economy before other sovereign states can outpace its development and lay down a new international monetary order. China has already established the Blockchain Service Network with city nodes and the e-yuan has gained significant domestic adoption, while CBDC models are being developed by all major nations. It is imperative that the standards for this shared future serve the global economy and not just one sovereign nation.

Large sector of the US economy relies on software development and microelectronics. This lead is being chipped away slowly. For example, TikTok in social media space, Temu in the e-commerce space and Huawei in microelectronics. Similarly, in foreign markets, domestic competitors often imitate and outpace US owned companies and impose arbitrary data laws or regulations. The proposed system would lead to transparent commerce for goods, services and "content/data". It will promote global fair trade and valuation of resources and labor worldwide and lead to the development of a new data economy. The global south would agree to such a proposal as they will escape the effects of the theory of unequal exchange where they end up exporting more labor and resources in actual terms even if they have trade surpluses in actual dollars. The present cryptocurrency ecosystem has increased the hegemony of the US dollar via stablecoins becoming purchasers of US debt, but this could be short-lived with the advent of other CBDCs, loss of faith in US economy and the threat of a BRICs supranational CBDC.

The innovation of the protocol is developing a method of sovereign participation via a pre-mint based on a predetermined formula based on the sovereign's debt and population. It will allow states to maintain monetary sovereignty while engaging in a global digital economy simply by operating a relay if they choose to. Payments may be made in the domestic currency and only international obligations and network fees/gas may be paid in the proposed currency. It will be up to each sovereign nation to decide its pace of adoption and domestic use of the proposed currency. The protocol will operate as the International Clearing Union as envisioned in Keynes' Bancor proposal, but it would be backed by a network of nodes that are incentivized for storage, processing

and transmission of information. This would also incentivize states to invest in their own computational resources and liberalization of their economies. It would lead to a renaissance where scientific research takes the front seat. It also moves beyond simple currency transactions or monetization of a computational resource to an information economy model, encompassing identity, marketplaces, and asset tokenization.

Economies operate on four broad forces, production and consumption and improving methods of production and consumption. Human history is a testament to the fact that improving methods of production and consumption are far more valuable than their counterparts. For example, the knowledge and skill required to make or operate an excavator is far more valuable than labor performed, or skill required to dig a ditch. If data is the new oil, then information is the refined product. Thus, an advanced economy like US should focus on improving the methods of consumption and production through automation, artificial intelligence, scientific research and lay the groundwork for a new information economy.

This proposal is a mosaic of a multitude of existing theories of economics, international law and technologies that are available to humanity for the first time. It builds on the concept of bitcoin and its other iterations that target a specific computational resource but puts the pieces together to make a global economic system enabling participation of sovereign states. It reinvents Keynes' Bancor proposal for an information currency backed by a network of decentralized incentivized nodes. Bitcoin protocol provided a model for a supranational reserve currency which can be anchored to a stable benchmark (proof of useful work) and is issued according to a clear set of rules therefore, ensuring orderly supply (block incentives); second, its supply is theoretically flexible enough to allow timely adjustment according to the changing demand (consensus mechanism); third, such adjustments & issuance are disconnected from economic conditions and sovereign interests of any single country (solution to Triffin's dilemma). DARPA's efforts in HR001123S0035, DARPA-PA-22-02, DARPA-SN-23-97, DARPA-PA-23-04-01, DARPA-RA-23-02, DARPA-PA-24-03, DARPA-EA-23-01-03 and many others are siloed efforts in culmination of the future envisioned in this proposal.

This is simply a new beginning for the human paradigm and cut-off point for the juristic aspect. The resulting scientific data renaissance may soon lead to almost infinite energy, discovery of new physics, space exploration, exploitation and colonization that advances humanity into the final frontier. At this stage the only finite resource will be information. The currency could also serve as the de facto currency for space colonies, incentivizing these colonies to establish nodes/communication with Earth and acting as a catalyst for investment in space by sovereign nations. Even if the very concept of a sovereign state inevitably disappears in centuries or perhaps millions of years, the foundation laid for this information economy will be set for millenniums.

**Technical Plan:**

- **What is the proposed work attempting to accomplish or do?**

Build economic strategy for transition to a supranational data currency that transforms US and the global economy into an information economy. Build network protocol for incentivizing storage, transmission and processing of data and standards for identity. Provide a technical basis for the initial distribution of this proposed information currency. A shared operating system for humanity. Blockchain protocols with these utilities already exist isolated within their ecosystems. The basic components of the digital part of the proposed SATOSHI protocol are.

**a. Storage:** Blockchains are distributed ledgers that record transactions using a shared consensus mechanism. This functionality of merely storing transactions has been further expanded to store

any form of data even in the bitcoin protocol. The noteworthy iterations of this are Filecoin, Chia & Arweave. While Filecoin enables storage of data for a defined period of time, the Arweave protocol provides permanent (up to 200 years) data storage beneficial for verified credentials, tokenized assets & smart contracts. The proposed protocol should support both permanent and temporary storage of data. The data accessible by user using public key cryptography can be shared with services or other consumers or even be sold for training AI models.

**b. Autonomous**: Smart Contracts that exist on the blockchain can be considered autonomous. Even bitcoin protocol contains various OPCODES that enable such autonomous transactions. This has been further advanced by the Ethereum Virtual Machine. It may allow states to operate relays or have multi-sig contracts with their citizens to enable social recovery. We also propose the ability to run various autonomous agents and AI models stored on shared operating system built on the protocol.

**c. Transfer**: This refers to the ability to transfer unique digital & tokenized assets and the prevention of double spending. Bitcoin was the first protocol to provide a solution to the double spending problem without a central entity. It may include interoperable CBDCs, tokenized assets, NFTs & identities where appropriate. This may also enable sovereign states to issue CBDCs that are interoperable and backed by their respective central banks. Central Banks may decide access to CBDCs or capital controls or models they want to pursue to distribute CBDCs in domestic economies or only allow them to be used for international trade.

**d. Operation** (Proof of computation / Useful Proof-of-work): Useful proof-of-work blockchains such as the Ixec Blockchain Network have made it possible to reward users for distributed computing. Apart from general computation and smart contracts, this will provide computation to train new AI models and operate existing ones.

**e. Satellite** (Proof of Coverage/bandwidth): This refers to the ability to send and receive information over the internet via mesh networking. Blockchains that utilize spare bandwidth to enable mesh networking such as Helium already exist. It may also allow nodes & points of sale & commerce to monetize spare bandwidth as well as allow a greater population to access the internet by providing incentives to the public, telecom & satellite operators.

**f. Hashing:** This refers to the cryptographic hash functions and standards of encryption. It may also refer to the consensus mechanisms deployed to add new blocks to the blockchain.

**g. Interface** (Dapps): Nodes may also operate their own interfaces providing front-end services to users. A node/interface may set its own rules & moderation policies regarding the content that is displayed by their interfaces. This also extends to AI models that may be monetized. For example, a marketplace may only allow users from certain sovereign states or credentials to display its products, or a social media interface may only allow verified users or be open to all users. Another example would be AI models for research of novel materials and physics. Popular interfaces may be able to charge a node fee or listing fees for content to be visible on their interfaces.

The other part of proposed protocol enables a marketplace for digitized economies. It is at the physical & digital intersection of commerce. Even though real estate, stocks & identities can be tokenized they hold little value without credible oracles & reputable sovereign institutions verifying such data and enforcing these rights. We propose a single unified protocol which captures data that is shared, compiled and stored by sovereign states in one singular database by providing

uniformity in how the data is captured across various government departments and agencies. It includes a global marketplace protocol to facilitate peer-to-peer commerce in which various kinds of credentials & associations enable consumers to make informed choices. It will also include other stakeholders such as banks, financial institutions, stock exchanges and other entities that may issue verified credentials as authorized by sovereign states. This will enable commerce & capital to flow freely with the counter-party risk that is acceptable to both parties in a transaction. The components of the proposed NAKAMOTO protocol are:

a. **Nationality/Network/Name:** This refers to sovereign states issuing verified credentials to individuals or entities under its control. For example, Social Security number, Aaadhar number or unique identifier for a government agency that may issue verified credentials to users or organizations or a national stock exchange that may issue credentials to companies listed on the exchange. It may also refer to network or networks an individual belongs to or simply a username.
b. **Assets** (Stocks, real estate registries, physical goods etc.): This refers to the tokenization of stocks & other tangible and intangible assets. For example, a stock exchange having verified credentials from sovereign state and it may further issue credentials to companies to tokenize their stocks further enabling capital inflows & foreign direct investment in a country. This may apply to land registries as well as other intangible assets like intellectual property that can tokenized and verified by institutions & entities regulating such assets.
c. **Knowledge** (Doctor / Lawyer / Accountant / Driving License/ Degrees): This refers to the verified credentials issued by educational institutions or trade bodies that may help the service economy to flourish. For example, a decentralized version of uber may require driving licenses or a service marketplace may require plumber/electrician certification. Further, service marketplaces like Upwork may flourish using these verified credentials.
d. **Association:** This refers to various incorporated or unincorporated associations that dominate the economic landscape. For example, industry organizations, political parties, international organizations etc. It may also include Decentralized Autonomous Organizations not incorporated in any sovereign state.
e. **Marketplace**: This refers to a marketplace protocol that may provide listings for physical goods and services. Particl Blockchain Protocol & Openbazaar have already demonstrated these capabilities. It may also include trade licenses, food licenses & other regulatory compliances needed to operate in an economy. A marketplace that is decentralized at the protocol level may be centralized at the interface level as front ends may only include products that are approved by the node administrator or may be open to all.
f. **Oracle**: This may refer to other records & data that is generated by sovereign or private entities in the economy. It may include pricing feeds, insurance records, credit scores, medical records, criminal record, traffic violations etc.
g. **Taxation**: Smart Contracts that enable taxation by sovereign states or Taxation IDs or taxation records that may allow government agencies to view a encrypted transactions. For example, viewkeys in the Monero Protocol. It may also enable determination of income for uncollateralized lending.

h. **Organization**: Employer organizations or other reputable organizations may issue verified credentials to its employees or members providing access to encrypted data or privileged access to certain services.

- **How is the work performed today (what is the state of the art or practice), and what are the limitations?** Bitcoin and similar protocols operate in their individual silos and only try to monetize a specific computational resource or type of cryptocurrency transfer or art in the form of NFTs or gaming assets and protocol development is influenced by untenable token incentives and schemes. They do not provide any method of sovereign state participation or use of real world assets without devaluation or loss of faith in the domestic currency. Triffin's dilemma has further exacerbated the ills of the cyclic nature of the US economy where it can never meet domestic objectives or commit to its obligations as the reserve currency issuer. Everyone has the right to issue their own money, as evidenced by meme coins, on these blockchain protocols. Thus, sovereign states are limited from experimentation and adopting new forms of digital currency to compete with private money which is only backed by speculation and the basic right to transact on the network. The pieces of this mosaic to establish a digital Bancor are already being investigated or experimented upon by various sovereign states in which US lags.
- **Who will care, and what will the impact be if the work is successful?** Humanity as a whole, sovereign states retaining privilege of being valued oracles, United States for leading humanity into a fourth generation economy. The impact would be global prosperity, advances in fundamental scientific research leading to exponential growth and the launch of the space age.
- **How much will it cost, and how long will it take?** The fundamental research proposed will analyze the juristic possibilities of developing such a protocol, standards, and global consensus. The cost of research will be limited to basic research and consultations with experts in their respective fields and the cost is proposed to be $250,000. The cost of developing the protocol and global consensus on the standards of identity and marketplaces will also require diplomatic efforts and estimated to be at least a decade.
- **What is new in your approach, and why do you think it will be successful?** It provides an implementation of a digital Bancor with sovereign state incentives and solves Triffin's dilemma for US while maintaining monetary sovereignty for other nations. It also seeks to achieve global consensus on identity standards and a shared operating system for humanity. We also propose a global injection of liquidity in the global economy via a predefined formula to reflect current economic status of sovereign states. Sovereign States can distribute this currency to local governments and organizations that can provide verified credentials as well as distribute this currency to citizens along with CBDCs or run relays.

- **Technical problems:** Apart from the humongous technical challenges of scalability, protecting privacy and developing this protocol, sovereign participation is essential as trusted providers of verified credentials and oracles. A technical basis for the allocation of the proposed currency advantageous to America and fair to the rest of the world needs to be developed.

- **Milestones:** Final white paper, strategy for US and brief for sovereign states after consultation with domain experts and US stakeholders.

- **Capabilities/Management Plan:** Proposer is an individual and studied law in India and Canada and has worked in US legal system. In a unique position to appreciate American ideals, cryptoeconomics, science, geopolitics and rule of law.

- **Cost and Schedule**

$250,000 Base for 1 year

**Bibliography**


1) Isaac Asimov, "*The Last Question*", https://astronomy.org/moravian/C00-Last%20Question.pdf, 1956
2) Satoshi Nakamoto, "*Bitcoin: A Peer-to-Peer Electronic Cash System*" https://bitcoin.org/bitcoin.pdf, 2009
3) Vitalik Buterin, "*Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*", https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf, 2014
4) Juan Benet, "*IPFS - Content Addressed, Versioned, P2P File System*", https://arxiv.org/pdf/1407.3561.pdf , 2014
5) Sam Williams et al, "*Arweave: A Protocol for Economically Sustainable Information Permanence*", https://www.arweave.org/yellow-paper.pdf , 2018
6) R. Skowronski, "*Fully Distributed GRIDNET protocol, with no trusted authorities*", https://ieeexplore.ieee.org/abstract/document/7899560 , 2017
7) R. Skowronski, "*GRIDNET Operating System*", https://gridnet.org/whitepaper/pdf/whitepaper.pdf
8) Gilles Fedak et al, "*Blockchain-Based Decentralized Cloud Computing*", https://iex.ec/wp-content/uploads/2022/09/iexec_whitepaper.pdf , 2018
9) Amil Merchant et al, "*Scaling deep learning for materials discovery*", https://www.nature.com/articles/s41586-023-06735-9 , 2023
10) Zhou Xiaochuan, "*Reform the international monetary system*", https://www.bis.org/review/r090402c.pdf , 2009
11) State Information Center Informationization and Industry Research Department et al, "*Blockchain-based Service Network (BSN)",* https://bsnbase.io/static/tmpFile/BSNIntroductionWhitepaper.pdf , 2020
12) J. Keith Horsefield , "*The International Monetary Fund 1945-1965 Twenty Years of International Monetary cooperation*", http://imsreform.org/reserve/pdf/keynesplan.pdf,1969
13) MD Boro, "*Triffin: dilemma or myth?*", https://www.bis.org/publ/work684.pdf , 2017
14) E. Glen Weyl, "*Decentralized Society: Finding Web3's Soul*", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105763 , 2022
15) Jason Hickel et al, "*Imperialist appropriation in the world economy: Drain from the global South through unequal exchange*, 1990–2015", https://www.sciencedirect.com/science/article/pii/S095937802200005X , 2022
16) @TBD54566975, "*tbDEX: A Liquidity Protocol v0.1*" https://tbdex.io/whitepaper.pdf , 2023

17) Ido Kaiser, *Particl: "A Decentralized Private Marketplace*", https://github.com/particl/whitepaper/blob/master/decentralized-private-marketplace-draft-0.1.pdf , 2017
18) Amir Haleem, "*Helium A Decentralized Wireless Network*", http://whitepaper.helium.com/ , 2018
19) Kleros, "*Proof of Humanity*", https://blog.kleros.io/proof-of-humanity-an-explainer/
20) Tools for Humanity, "*A New Identity and Financial Network*", https://whitepaper.worldcoin.org/
21) "*Chia Business Whitepaper*" https://www.chia.net/wp-content/uploads/2022/07/Chia-Business-Whitepaper-2022-02-02-v2.0.pdf . 2022
22) "*Steem: An incentivized,blockchain-based,public content platform*" https://steem.com/SteemWhitePaper.pdf , 2017
23) "*A Gentle Introduction to How I2P Works*", https://geti2p.net/en/docs/how/intro
24) Deugh Ausgam Valis, Mirelo "*Representational Monetary Identity",* https://philpapers.org/archive/DEURMI.pdf , 2016
25) Deugh Ausgam Valis, Mirelo, "*Proof-of-Loss*" https://philpapers.org/archive/DEUP-2.pdf , 2017