# Response of the DigiByte Alliance to the Office of Science and Technology Policy (OSTP) Request for Information; Digital Assets Research and Development

**March 3, 2023**

For additional information about this response please contact:

Michelle Dougherty
DigiByte Alliance
2020 Carey Avenue Suite 600
Cheyenne, WYO 82001
michelle@dgballiance.org

## Introduction

The DigiByte Alliance (DGBA) respectfully submits these comments in response to the White House Office of Science and Technology Policy's Notice of Request for Information (RFI) to help identify priorities for research and development related to digital assets.[1] DGBA[2] is a 501(c)(3) public non-profit research and advocacy organization focused on the development and adoption of DigiByte, an open-source, permissionless blockchain network.[3]

DGBA appreciates and supports the development of a National Digital Assets Research and Development Agenda (NDARDA), and recognizes the vital roles of the Office of Science and Technology Policy (OSTP), the Fast Track Action Committee (FTAC) on Digital Assets Research and Development of the Subcommittee on Networking and Information Technology Research and Development (NITRD) of the National Science and Technology Council (NSTC) and the National Science Foundation, and the NITRD National Coordination Office as they endeavor to craft a comprehensive NDARDA.

DGBA's response to the RFI focuses primarily on the benefits and applications of public decentralized permissionless blockchains (DPB) to an overall NDARDA. As stewards of the DigiByte blockchain, we are intimately familiar with the potential of DPBs. We believe that blockchains like DigiByte should be an essential part of any NDARDA and are vital to demonstrate America's global leadership in digital asset innovation and security. Our response focuses collectively on Topics 1, 4, and 6 of the RFI.

Built upon Open-Source Software (OSS), DPBs reinforce the ideals of privacy, individual sovereignty and free market competitiveness and offer the type of access and public accountability that can reinforce rather than hinder American values. History teaches us that innovation and inclusion flourish when participation barriers are lowered or eliminated. DPBs by their very nature fulfill that promise. We believe that it is inevitable that blockchain technology will replace much of todays' information, communication, financial, and storage infrastructure, each of which will demand robust and resilient cyber security and public trust. Since DPBs like DigiByte have immutable encryption technology in their DNA, they are an ideal substrate upon which to research and build future democracy enhancing innovations in the emerging digital economy.

## A. U.S. Government Strategy for Establishing Federal R & D Priorities

### 1. Identify the Problems

DGBA believes it is essential to develop a public framework and common lexicon among public and private stakeholders regarding the key challenges and impediments to the wider adoption and public trust of digital asset technology. Specifically, those areas where a lack of transparency, efficiency, and security cause the greatest misallocation of resources, fraudulent activities, and system exploitation. Expert insights from private and public stakeholders, including the various agencies (e.g., Offices of Inspector General and cyber security related agencies) about current

[1] Office of Science and Technology Policy (OSTP) "Request for Information; Digital Assets Research and Development," *Federal Register*, Vol. 88, No. 17 (January 26, 2023) https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development

[2] https://www.dgballiance.org

[3] https://digibyte.org/en-us/

system or operational vulnerabilities within the Federal Government and beyond should be gathered in parallel. Such a survey would better inform federal resource allocation and priorities for future development of digital asset technology solutions and applications within the Federal Government, and beyond.

Since blockchain technology is by its very nature an evolving "general purpose technology,"[4] a research and development strategy that starts with known problems avoids research and development looking for lesser problems to solve.

### 2. Identify the Technologies with Potential to Solve the Identified Problems

The full potential of DPBs' role is understood among disinterested developers and advocates of a more democratized, secure, fair, and transparent blockchain ecosystem. The future of DPBs like DigiByte and other digital asset technology has been obscured by the lack of regulatory clarity, and the adjacent issuance and trading of private digital assets. DGBA believes that these distractors have hindered private resource allocations and investment in legitimate, long-term platforms and technologies.[5] The value of DPBs enabling technology has been distorted by speculative valuations and misallocated investments that might otherwise have been directed to proving the universal value of permissionless open-source projects.

As NDARDA considers which technologies to prioritize for research and development, DGBA believes that open-source technologies must be the bedrock upon which future blockchain adoption and applications are built. Only then can we harness the creativity of the disinterested developer community and the public trust needed to realize the potential of this nascent technology. If that future is dictated by technologies that are proprietary or opaque, the speed of adoption and trust will be measured in decades.

## B. The Benefits of DPBs

### 1. DPBs Will Unlock American Innovation and Reinforce Democracy in the Emerging Digital Economy

The United States has been the dominant economic leader in the world for the past century because our system facilitates innovation and growth through free market participation. While our most important civilian technologies have been developed and commercialized by the private sector, the government plays a crucial role in funding the basic research and development which makes that success possible. Economic decentralization is a central prong in the story of America's success. Indeed, we export these principles to other economies, particularly those with limited or no access to capital. The US Agency for International Development, for example, rightfully emphasizes economic decentralization as a critical element in its guide to developing democracy in foreign

[4] "[T]he ability to track transaction attributes, settle trades and enforce contracts across a wide variety of digital assets is what makes blockchain technology a general purpose technology." Catalini & Gans (2016), *NBER WORKING PAPER SERIES SOME SIMPLE ECONOMICS OF THE BLOCKCHAIN* Retrieved from https://www.nber.org/system/files/working_papers/w22952/w22952.pdf, p.3

[5] In addition, open-source projects that are likely to have a high degree of application and use by the general public are least likely to garner support by private investors as they cannot guarantee a return on investment. Where "market forces will lead to an underinvestment in R & D from society's perspective, …a rationale for government intervention [is provided]." Speech by Chairman Ben S. Bernanke on Promoting Research and Development: The Government's Role. (n.d.). Board of Governors of the Federal Reserve System. https://www.federalreserve.gov/newsevents/speech/bernanke20110516a.htm

countries.[6] The "cornerstones of economic freedom are personal choice, voluntary exchange, open markets, and clearly defined and enforced property rights."[7] It is axiomatic that the NDARDA create policy supporting technology that reinforces these values.

DPBs are the networks upon which "entrepreneurial experimentation can take place and be rewarded from anywhere in the economy."[8] Research shows that open permissionless networks have a greater likelihood of boosting economic innovation and thereby inclusion in wider segments of the population.[9] Permissionless blockchain networks will become the public utilities upon which economic value can be created without the necessity of a third-party intermediary, unlocking the unprecedented potential for increased economic activity and growth.[10] That DPB's have the potential to create more economic innovation stems from their underlying technological properties which enable distinct commercial aptitudes.

From an economic perspective, "two key costs are impacted by blockchain technology-the cost of verification of state and the cost of networking."[11] While permissioned blockchains can impact the former, it is only permissionless blockchains that can impact both.[12] Permissioned blockchain protocols operate under the same limitations of a traditional database-where trust is placed in intermediaries. DPBs by contrast sustain that trust using the mathematical code of a distributed ledger and have the potential to serve as vehicles for economic growth "by reducing barriers to entry within sectors that are heavily concentrated because of network effects and control over data, [thereby enabling] a new wave of innovation in digital services, and greater consumer choice."[13] As regulatory frameworks become clearer these increased benefits can begin to come to fruition.

## 2. The Open-Source Software Environment of Decentralized Blockchains Can Accelerate Digital Asset Development

OSS contributions lead to a greater escalation of entrepreneurial activity and growth.[14] That "software for the public benefit should be open source by default" has been noted by many[15] and is consistent with the United States' policy about the benefits of using OSS. *See* OMB Memorandum M-16-21 *Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through*

[6] *Democratic Decentralization Programming Handbook | Document*. (2022, December 16). U.S. Agency for International Development. https://www.usaid.gov/democracy/document/democratic-decentralization-programming-handbook

[7] Gwartney, J., Lawson, R., Hall, J., Murphy, R., Djankov, S., & Mcmahon, F. (n.d.). *ANNUAL REPORT*. Retrieved February 28, 2023, from https://www.cato.org/sites/cato.org/files/2022-09/efw-2022-full-issue.pdf

[8] Catalini & Gans (2016), *NBER WORKING PAPER SERIES SOME SIMPLE ECONOMICS OF THE BLOCKCHAIN* Retrieved from https://www.nber.org/system/files/working_papers/w22952/w22952.pdf

[9] Ibid.; KR, Dr. V., & K, M. (2022). The Emergence of Decentralized Business Models: Blockchain Interruption and Decentralized Finance. *International Journal for Research in Applied Science and Engineering Technology*, *10*(6), 2165–2171. https://doi.org/10.22214/ijraset.2022.44168

[10] "A private blockchain is an intranet, and a public blockchain is the internet. The world was changed by the internet, not a bunch of intranets. Where companies will be disrupted the most is not by private blockchains, but public ones." https://bitcoinmagazine.com/business/mit-s-brian-forde-companies-will-be-disrupted-the-most-by-public-blockchains-1466028606

[11] Catalini & Gans, https://www.nber.org/system/files/working_papers/w22952/w22952.pdf, p. 2

[12] Ibid., p. 2 and 19.

[13] Ibid.

[14] Langburd, N., Nagle, W., & Greenstein, S. (n.d.). *Open Source Software and Global Entrepreneurship*. Retrieved from https://www.hbs.edu/ris/Publication%20Files/20-139_bd835fdf-a293-4912-aa21-769e77f2754a.pdf

[15] *Building and Reusing Open Source Tools for Government.* (n.d.). New America. Retrieved March 27, 2022, from https://www.newamerica.org/digital-impact-governance-initiative/reports/building-and-reusing-open-source-tools-government/

*Reusable and Open Source Software*.[16] While the full benefits of an OSS policy in the digital asset arena are articulated in that Memorandum, including cost savings and efficiencies, one benefit stands out:

> Making source code available as OSS can enable continual improvement of Federal custom-developed code projects as a result of a broader user community implementing the code for its own purposes and publishing improvements. This collaborative atmosphere can make it easier to conduct software peer review and security testing, to reuse existing solutions, and to share technical knowledge.[17]

OSS lowers the barriers to entry for disadvantaged income populations, is an opportunity for their participation in the frontier of digital asset development, democratizes access for contribution, and enables a "financial inclusion" strategy that encompasses a "financial participation" strategy with groups who are otherwise excluded from access in closed, private, siloed environments. The White House recently acknowledged the importance of equalizing access to maximize and harness American ingenuity in the context of its National Artificial Intelligence Research Resource Task Force final report: "[w]hile AI research and development (R&D) in the United States is advancing rapidly, opportunities to pursue cutting-edge AI research and new AI applications are often inaccessible to researchers beyond those at well-resourced companies, organizations, and academic institutions."[18] As stated by NSF Director Sethuraman Panchanathan:

> By creating an equitable cyberinfrastructure for cutting-edge AI that builds on-ramps for participation for a wide range of researchers and communities, the NAIRR could build AI capacity across the nation and support responsible AI research and development, thereby driving innovation and ensuring long-term U.S. competitiveness in this critical technology area.[19]

The same holds true for any NDARDA.

DGBA acknowledges the reflexive resistance to use of OSS for non-civilian (national security) applications, [20] but believes that adequate security perimeters can be deployed and weighed carefully in digital asset research and development efforts to take advantage of OSS-led innovations without sacrificing our most sensitive digital data and applications.

[16] MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES FROM: Tony Scott United States Chief Information Officer Anne E. Rung United States Chief Acquisition Officer SUBJECT: Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open-Source Software. (2016). https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_21.pdf

[17] Ibid., p. 2 citing Department of Defense Chief Information Officer. *Clarifying Guidance Regarding Open-Source Software (OSS).* October 16, 2009: "The continuous and broad peer-review enabled by publicly available source code supports software reliability and security efforts through the identification and elimination of defects that might otherwise go unrecognized by a more limited core development team." http://dodcio.defense.gov/Portals/0/Documents/FOSS/2009OSS.pdf.

[18] *National Artificial Intelligence Research Resource Task Force Releases Final Report - OSTP.* (n.d.). The White House. Retrieved February 28, 2023, from https://www.whitehouse.gov/ostp/news-updates/2023/01/24/national-artificial-intelligence-research-resource-task-force-releases-final-report/

[19] Ibid.

[20] Ibid. Subsection 6.2 "The sharing of the source code would create an identifiable risk to the detriment of national security, confidentiality of Government information, or individual privacy..."

## 3. Permissionless Blockchains Are Weapons of Resiliency for Cybersecurity

Single points of failure are the Achilles heel of today's online security architecture. The network encryption properties of blockchain can mitigate these vulnerabilities, and additional research and development of these advantages is of paramount importance.[21] DPBs are built upon decentralized peer to peer networks that enable non-trusting parties to interact with each other without the need for a trusted authority, eliminating the need for a single, centralized third party vulnerable to single points of failure. Stated more simply, "[t]rust in the intermediary is replaced with trust in the underlying code and consensus rules."[22] It is the removal of this single point of failure that is the essence of DPBs whose outcome-agnostic encryption methodologies have the potential to create new avenues of secure online relational realities among and between businesses, governments, and individuals.[23]

DGBA assumes that the use of blockchain technology to mitigate the ongoing epidemic of cyber insecurity is a NDARDA priority. New cybersecurity solutions are of interest to every consumer of the internet, most particularly the U.S. Government. In May of 2021, the President issued Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*[24] initiating a sweeping Government-wide effort to ensure that baseline security practices are in place, to migrate the Federal Government to a zero-trust architecture. The White House's January 2022, *Memorandum Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*[25] further specified the mandate of a new security architecture paradigm. In 2021, cybercrime costs approached 7 billion dollars.[26] Cyber insecurity is a chronic disease in desperate need of a cure.[27] Decentralizing assets, applications, and security infrastructure through blockchain could make it possible to stop hackers in their tracks and beat them at their own game.[28]

The distributed nature of DPBs provides the underlying foundation of resilience upon which to build applications to achieve cybersecurity goals. Decentralized applications can include anything from IOT security, securing private messaging, authentication of software provenance, verification of cyber-physical infrastructures and securing DNS and DDoS.[29] Advances in cryptography, discreet

[21] A significant benefit of public blockchains is the general public's global participation in the security of the network. This eliminates devops requirements for the network, which are replaced with a simplified POW or POS operation. Devops required for POW security operations is simpler than standard server farms, thus producing a significant cost reduction.

[22] Christian Catalini & Joshua S. Gans, https://www.nber.org/system/files/working_papers/w22952/w22952.pdf, p.9.

[23] For an extensive review of current blockchain applications *See* Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, *36*(36), 55–81. https://doi.org/10.1016/j.tele.2018.11.006

[24] *Improving the Nation's Cybersecurity*. (2021, May 17). Federal Register. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[25] https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[26] https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[27] NPR. (2021, May 30). USAID Hack: Former NSA Official Calls U.S. Cyber Insecurity A "Chronic Disease." Retrieved February 28, 2023, from NPR website: https://www.npr.org/2021/05/30/1001748861/usaid-hack-former-nsa-official-calls-u-s-cyber-insecurity-a-chronic-disease

[28] Napoli, R. (n.d.). *Council Post: How Blockchain Could Revolutionize Cybersecurity*. Forbes. Retrieved February 28, 2023, from https://www.forbes.com/sites/forbestechcouncil/2022/03/04/how-blockchain-could-revolutionize-cybersecurity/?sh=6a65937c3a41

[29] Legrand, J. (2020, September 4). The Future Use Cases of Blockchain for Cybersecurity. Retrieved from www.cm-alliance.com website: https://www.cm-alliance.com/cybersecurity-blog/the-future-use-cases-of-blockchain-for-cybersecurity

permissions, and key distribution made possible by blockchains can become a cornerstone of how nation states protect classified information, intellectual property, and critical infrastructure.

## 4. The Potential of the DigiByte Blockchain as a Public Utility for Cybersecurity

DPBs can be considered public utilities like a highway, something for everyone to consume for the benefit of all. To the extent that the NDARDA intends to further explore cybersecurity applications on DPBs, DigiByte's nine year tested distributed ledger technology is perfectly suited to many functionalities due to the speed, security and scalability of its architecture.

The DigiByte blockchain is a DPB whose technology has potential to establish higher levels of protection to the prevalent and often insecure intermediary laden paradigms of today's economic realities.[30] The May 2021 paper *Achieving Cybersecurity in Blockchain Based Systems: A Survey*,[31] evaluated several extant blockchains for their adherence to NIST cybersecurity criteria[32] and found that "all cybersecurity properties are reached in DigiByte."[33] Having a resilient baseline level of technological properties places DigiByte in a unique category of public DPBs to serve a substrate for the development of decentralized solutions that can provide fast, secure, and scalable methods for the transfer, verification, authentication, and storage of data and communications.

### a. Architecture of the DigiByte Blockchain

Since the utility and integrity of any blockchain network is coextensive with the degree of the security and performance capacity of that network, DGBA provides some background on the uncommon architecture of DigiByte.

DigiByte is an American born derivative of the Bitcoin blockchain[34] and is similarly a decentralized peer-to-peer worldwide network enabling transfer of value without third party intermediation. While DigiByte is a UTXO[35] blockchain that uses consensus mining algorithms, enhancements made to its core protocol allow for significantly improved functionality via its 15 second block times, real-time difficulty adjustment, extremely low fees, and distributed mining algorithms. DigiByte's five separate mining algorithms that are geographically distributed across countries across the globe. This mining model increases DigiByte's decentralization by distributing it across distinct types of hardware thereby offering protection against malicious attacks.[36] Since implementation, the DigiByte Blockchain core has had over 16,000,000 transactions validated without interruption to the network. With over nine years of development, DigiByte is the longest and fastest UTXO blockchain in the world.

[30] As one of the only DPBs supported by a 501(c)(3) public foundation, the DigiByte blockchain is uniquely situated to participate in any R & D funding allocation to advance the capabilities of digital asset technology.

[31] Achieving cybersecurity in blockchain-based systems: A survey. (2021). *Future Generation Computer Systems*, *124*, 91–118. https://doi.org/10.1016/j.future.2021.05.007

[32] Based on a review of 272 papers between 2013 and 2020 and 128 business initiatives and specifically evaluating authenticity, non-repudiation and confidentiality elements of the NIST criteria.

[33] Ibid., p. 102; *see also* Ibid., Table 11.

[34] The maximum supply of DigiByte is 21 billion compared to Bitcoin's supply of 21 million.

[35] https://en.wikipedia.org/wiki/Unspent_transaction_output

[36] Spackman, J. (2020, August 2). *Some updated DigiByte mining stats graphs / comparisons*. Medium. https://josiah-digibyte.medium.com/some-updated-digibyte-mining-stats-graphs-comparisons-7f0c902b7554

DigiByte is a rare “layer one” public blockchain whose speed, security and decentralization coexist.[37] DigiByte’s block timings are forty times faster than Bitcoin. The net result of this is a wallet-to-wallet transaction is received within a couple of seconds. Speed is important when implementing blockchain into real-life applications. The same can be said regarding DigiByte’s negligible transaction fees which also bolster its capacity to serve as an instrument of real-world utility.[38]

In April 2017 DigiByte became the world’s first major blockchain to successfully activate Seg Wit (Segregated Witness) which helps to achieve faster transactions. DigiByte also pioneered both Multi Shield and Digi Shield.[39] Demonstrating the power of OSS, many blockchain developments innovated by DigiByte developers have been incorporated into other major blockchain networks. For example, DigiByte’s Digi Shield technology that facilitates predictable block timing performance in the face of fluctuating hash power has been added into over 2-dozen other blockchains.[40]

In 2019, DigiByte implemented a privacy feature Dandelion++ that can protect the privacy and security of DigiByte users. Dandelion++ protects your location by making it difficult to ascertain from a transaction the originating IP address. In addition, DigiByte has added technological features such as an assets layer which enables the issuance of NFTs and a DigiID cryptographic key log in technology that sets it apart as an emerging UTXO blockchain with an unusual capacity for Web3 and cybersecurity applications.

In sum, the unique characteristics of DigiByte include: (1) the difficulty adjustment algorithm is evolutionary compared to that of Bitcoin; (2) a fixed 15 second block timing that is adjusted dynamically block by block providing predictable function execution timing; (3) blockchain nodes are metaphorically comparable to RAID implementations. Each node is a redundant RAID 1 copy of the entire chain; (4) DigiByte’s 5 separate algorithms give developers more options to design and securely optimize their use of the network based upon hardware availability, electrical costs, and infrastructure requirements; (5) dandelion Privacy features and (6) an Assets layer.

### a. DigiByte Applications

DigiByte’s randomized multi-algo UTXO architecture makes it one of the most secure, fast, and scalable and cost-effective networks upon which to build applications and solutions. The breadth of real world DigiByte applications is constantly evolving without proprietary investments, an ICO or

[37] The current Transactions Per Second (TPS) for DigiByte range from 560 to 1066, and the underlying code enables DigiByte’s TPS to be increased to 280,000 with further development.

[38] The precise carbon footprint of DigiByte as compared to other cryptocurrencies is not precisely known due to a lack of funding to conduct a comprehensive environmental audit. However, at the current time it is fair to say that it is significantly less than Bitcoin due to its lower market share. Some theorize that due to its faster block timing, DigiByte inherently consumes less electricity even if it were to increase Bitcoin's market share. However, this theory would require an in-depth environmental audit for confirmation. The countervailing benefits provided by blockchain mining to capture otherwise dormant natural resources, not to mention increase infrastructure resiliency, would have to be factored into any such cost benefit analysis.

[39] Activated in February 2014, this network upgrade allowed for the DigiByte blockchain to protect against multi-pools that mine large numbers of DigiByte at a low difficulty. It achieves this protection by recalculating mining difficulty between each block, allowing for a faster correction when a large amount of hashing power begins or ceases contributing to DigiByte, rather than recalculating once every two weeks as is the case with Bitcoin.

[40] Including Ethereum, Bitcoin Cash, Zcash, Dogecoin, and Bitcoin Gold, among others.

significant premine[41] to fund development efforts.[42] Below, we describe potential, current and past use cases and applications which illustrate the scope of technological advancements provided by the DigiByte blockchain network.

## Document Verification and Authentication

DigiByte can be used to facilitate the issuance and storage of digital documentation in a way that prevents or minimizes fraud, counterfeiting and forgery. In an academic publication from the University of Lausanne, DigiByte is described as a viable blockchain technology to create a tamper proof timestamped provenance ledger for police in Switzerland, illustrating the viability of the DigiByte blockchain to support data integrity and authentication.[43] The Dutch company V-ID has used the DigiByte blockchain to achieve this result using their blockchain validation and verification platform[44] that protects against any form of digital fraud.[45] In 2019 Doewes Fine Art Gallery[46] in partnership with V-ID used the DigiByte blockchain to secure the authentication of a Rembrandt painting,[47] demonstrating the ability to use DigiByte to authenticate not only documents, but physical goods.

DigiByte can similarly be used to securely store government documents, including its archives, using public and private keypairs associated with DigiByte addresses. Public addresses can retain encrypted hashes of stored documents; encrypted using the public key itself. The private key serves as identification for the public address, as well as facilitating the decryption of the encrypted hash. Once decrypted the hash is used to identify the specific stored document to retrieve from firewalled storage.

## Digi-ID – Passwordless Login

Considering the current U.S. government wide effort to move to zero trust cybersecurity principles, Digi-ID may be of particular interest to those working on establishing zero trust protocols. This application was developed specifically for cyber protection.[48] This free, fast, and secure authentication method can be used as an alternative to passwords to sign into online applications. Using a blockchain-based signature, a private key is generated to log into a website or other platform. A multi-factor authentication tool, the keys are securely generated in a decentralized

[41] The .5% premine was for development of the first wallets and given away to early adopters to get the network up and running. See Bitcoin talk forum https://bitcointalk.org/index.php?topic=408268.0...

[42] DigiByte is not a company, and there is no central authority who can control its growth, distribution, development, or usage. This is the foundation upon which DigiByte is based. It is an open-source project, developed and supported by a truly decentralized global community of volunteers.

[43] Jaquet-Chiffelle, D.-O., Casey, E., & Bourquenoud, J. (2020). Tamperproof timestamped provenance ledger using blockchain technology. *Forensic Science International: Digital Investigation*, *33*, 300977. https://doi.org/10.1016/j.fsidi.2020.300977

[44] https://www.v-id.org

[45] *AmSpec And V-ID Verify and Protect Certification in The Petroleum and Petrochemical Industry*. (n.d.). Cryptodaily.co.uk. Retrieved February 28, 2023, from https://cryptodaily.co.uk/2019/06/amspec-and-vid-verify-and-protect-certification-in-the-petroleum-and-petrochemical-industry It is our understanding that V-ID no longer uses DigiByte as an anchor blockchain since it launched a DAO on Ethereum.

[46] https://douwesfineart.com

[47] Team, V. D. A. (2022, August 3). *First Blockchain Validated Rembrandt*. Medium. https://vidtdao.medium.com/first-blockchain-validated-rembrandt-4cca632f6a82

[48] https://www.digi-id.io/integration.html; Digi-ID is based on https://github.com/bitid/bitid and developed further into a user-friendly application. It is currently being used as a sign in method on the website https://changeangel.io

manner and are secured by the DigiByte blockchain protocol. Unlike many solutions on the market, Digi-ID keys are not generated by any private company or stored in a centralized database. Digi-ID can also be used as a complimentary 2FA.[49]

Besides the use to login to different websites, Digi-ID can be used for building security and to replace access cards. With Digi-ID no information is logged or stored on-chain. The power of Digi-ID lies in its flexibility to also be used in connection with the assets layer of the DigiByte blockchain. The architecture of DigiByte enables the leveraging of its blockchain as a credential (or any asset) authenticator through the combined use of Digi-ID and its Assets layer. This potential combination of technologies is currently unique to the DigiByte blockchain.

**Digi Assets**

Digi Assets are metadata tagged fungible or non-fungible tokens issued on top of DigiByte's blockchain.[50] While the concept of assets and tokenization are possible across a wide variety of blockchains, Digi Assets benefits from its unique protocol properties, large global geographical node distribution, and variety of consensus algorithms. Since DigiByte does not have Turing complete smart contract capabilities, Digi Assets are not subject to smart contract attacks.

Digi Assets can be used to securely and cryptographically represent anything we find in the real world from physical assets such as real estate, airplanes and boats to any type of document such as wills and health care records. Governments could distribute any type of benefit via Digi Assets including anything from health care, social security and WIC benefits, and serve as the rails to ensure the distribution of benefits that can thereby effectuate the goal of financial inclusion.

**Identity Verification**

The promise of the DigiByte blockchain as a platform to provide security and combat fraud in identity credentialing was most recently recognized with an Honorable Mention for a presentation by DGBA at the Security Innovation Challenge sponsored by the Homeland Security Technology Consortium in September of 2022.[51] The Assets layer of the DigiByte blockchain is a metadata storage layer upon which credentials like passports and visas can be encrypted and then authenticated using Digi-ID. More specifically, a trusted authority could issue an asset reflecting ownership of a credential. The non-transferable asset, sent to the owner's wallet after encryption on an asset, can be verified by its owner using Digi-ID at a credential check point.

**CONCLUSION**

Due to its security features, blockchain may be used as a trusted infrastructure to develop a large variety of use cases and applications. We have presented some security-related use cases in this response. Just as no one understood how the internet would transform the world economy in 1990, it is difficult to predict how security provided by the asymmetric cryptography of blockchain may be applied in advance.

The NDARDA should integrate DPBs as an integral part of the research and development agenda so that they can reach their full potential as an open-source tool of innovation, particularly to achieve a

[49] See also https://www.thecrimson.com/sponsored/article/digibyte-digi-id/

[50] This application is in a beta stage of development.

[51] https://hstech.ati.org/#1666036158120-146598a3-aee4

higher degree of resilience, protection and cybersecurity in our increasingly online interactions. As the current intermediary laden paradigms of today's internet are restructured, the world will need secure and reliable decentralized blockchains upon which to build solutions.

We are reimagining how value and information can be exchanged and protected on the new "internet of value" freeway. Open source DPBs can provide the rails of a public infrastructure to manifest this new reality while preserving American values of democracy and economic freedom and creating opportunities for financial inclusion and participation.