Computing Community Consortium's Response to RFI "Digital Assets Research and Development"

March 3rd, 2023

Written by: Hank Korth (Lehigh University), Rajmohan Rajaraman (Northeastern University), Catherine Gill (Computing Community Consortium), and Ann Schwartz (Computing Community Consortium).

This response is from the Computing Research Association (CRA)'s Computing Community Consortium (CCC). CRA is an association of nearly 250 North American computing research organizations, both academic and industrial, and partners from the professional societies. The mission of the CCC is to enable the pursuit of innovative, high-impact computing research that aligns with pressing national and global challenges.

This response primarily pertains to questions 1, 4, 5, and 6 from the Request for Information.

Introduction: A Framework for Digital Assets

In order to consider the technological needs, challenges, and opportunities in the domain of digital assets, it is important to assess the range of current and potential applications. Assets take many forms: money, equities, bonds, real estate (and other physical property), intellectual property (patents, books, etc.), carbon-offsets, etc. Some of these assets are largely in a digital domain. Most monetary transactions, and virtually all large, legal ones, are digitally created and stored, and operate over digitally represented assets. The link between physical assets and their digital representation is created, managed, and maintained by some (usually centralized) authority, such as a registrar of deeds for real estate.

Beyond a traditional view of assets is the concept of information as an asset. Whether that information is health data, financial data, or data shared on social media, those data are indeed assets with real value. As is the case with other assets, information is managed in most cases by a central authority, with the individual about whom the information pertains possibly losing control of its use.

The connection between digital assets and blockchain technology[1] rests in the use of cryptographically secure methods to replace some or all of the centralization with a trust based upon code, typically, though not necessarily, open-sourced and publicly verifiable. The design of a blockchain framework can enable a degree of decentralized control versus a central authority. There is a full spectrum of control – from highly centralized to purely decentralized. Where a specific deployment of a framework rests in this spectrum varies among current blockchains. Some existing blockchains mandate a particular mix of decentralization and centralization. Others allow a degree of flexibility that is subject to parameters set by policy makers. Who those policy makers are and how they make their choices is beyond the scope of this paper, which focuses on technology and the need for investment in research. Taken as a whole, blockchain technology can serve as an efficient enabler of policy choice and can empower both governments and enterprises to operate in accordance with their core values. To ensure that digital assets and blockchain technology enable fair and equitable systems, these technologies must be employed in a trustworthy fashion. We recommend a framework emphasizing three properties: *privacy*, *transparency*, and *regulatability*.

Supporting a Mix of Privacy, Transparency, and Regulatability

While privacy and transparency may sound like antithetical goals to implement in a single system, the unique properties of the blockchain allow for each to be achieved without compromising the other. Blockchains can offer privacy and transparency simultaneously using zero-knowledge (ZK) proofs, a breakthrough technology in cryptography that allows a party to prove a guarantee to another party convincingly (hence offering transparency) without revealing any private information (hence maintaining privacy). ZK proofs were introduced in 1985[2] and formed a body of contributions to cryptography leading to the 2012 Turing Award being presented to Shafi Goldwasser and Silvio Micali. The underlying mathematics is highly complex but the concept has been illustrated in a highly intuitive way using interactive examples in a human domain rather than code[3].

In our context of digital assets, ZK proofs allow proof of compliance while preserving privacy. Consider the example of a sanction list from the US government. A financial institution could use ZK to prove that no transactions in a set of transactions interacts with any party on that list without having to reveal anything more about the transactions themselves. Later, if due process

[1] We use the term *blockchain* here rather than *digital ledger*, though both terms are applicable in most of our contexts. The term *digital ledger* is used, often in an enterprise setting, for a blockchain with no cryptocurrency and some degree of centralized access control.

[2] Goldwasser, S., et al. “The Knowledge Complexity of Interactive Proof-systems.” *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing - STOC ’85*, USA, ACM Press, 1985. *Crossref*, https://doi.org/10.1145/22145.22178.

[3] “Computer Scientist Explains One Concept in 5 Levels of Difficulty | WIRED.” *YouTube*, 18 Jan. 2022, www.youtube.com/watch?v=fOGdb1CTu5c.

allows for audits, that institution could reveal a transaction and show that it was a part of the set for which the ZK proof applies without having to reveal the entire set of transactions[4].

While many ZK systems exist, they fall short of the scale needed to support both mass adoption and application to large-scale datasets, both of which are important to maximize societal benefits. The challenge here is that ZK proofs, though relatively easy to verify, are computationally hard to generate, and that difficulty grows with the complexity of the computation about which a proof is being generated. Many of the mathematical computations needed to generate ZK proofs are highly parallelizable but also require large amounts of memory. Considerable research is needed in cryptography and cryptographic algorithms, and also in the design of highly scalable parallel hardware and software systems in order to enable broad deployment of ZK technology.

Trustworthy Markets and Financial Leadership

The US' post World War II leadership role in financial markets has benefited the nation in many ways. The continuance of the leadership depends on the US maintaining its trustworthy markets in the face of advancing technologies that may enable new leaders to emerge. China is clearly pursuing a leadership role with its e-Yuan and various Western nations, including those in the European Union, are developing digital-asset prototypes and policies. Continued US leadership will require a prudent mix of policy and regulation that both protects investors and supports continued experimentation and technical innovation. Prudent regulation requires a deep understanding of how policy goals can be achieved with minimal impact on positive, useful aspects of markets and industries. The ability of blockchain systems to create trust among untrusting parties and the power of zero-knowledge to prove compliance while maintaining privacy can combine to create a regulatory framework that is both transparent and privacy-preserving. The impact of such a framework is a continued faith in the fairness of markets while enjoying the benefits of technological advances. A technologically-aware approach to regulation that supports both trustworthy markets and further innovation is of particular importance for blockchain and cryptocurrencies, since those technologies and the markets they enable have a high degree of global mobility.

Information: The Foundational Digital Asset

Much of the discussion on digital assets thus far has focused on the applications of digital assets and the blockchain in financial markets and cryptocurrency. The term “digital assets” itself may imply a financial leaning in its application area, but we believe that this focus is unnecessarily limiting, and biases the discussions surrounding the potential impacts of these technologies. Blockchain technology is not simply about currency. Blockchain technology is about information and the privacy and transparency thereof. Information that supports a digital

[4] The full technical details include cryptographic data structures such as Merkle trees.

currency is only one such application. Efforts are underway to employ blockchain technology to a variety of information management applications both in government and in enterprises. Most of the latter applications do not even have an associated cryptocurrency. We are aware of ongoing projects and products in secure health records, verifiable accounting, supply chain, real-estate registration and transfer, academic transcripts, and more. Certainly, central-bank digital currencies are an extremely important application, but that and other currency-based applications can all be viewed from the standpoint of a blockchain being an information-management system handling data about the currency and transactions in that currency.

It is important to distinguish between the concept of information management as in a typical enterprise database and information management within a blockchain setting. A database system facilitates storage, retrieval, update, and sharing of information. Applications run on top of the database possibly using stored procedures within the database that applications can call. Blockchains enable code to run with partial or total autonomy. Such code is called a *smart contract*[5]. This enables a business contract to be coded as a smart contract that implements the terms of the agreement. A simple example is a weather insurance contract that pays a farmer if the contract-specified period of no rain occurs. The real-world information about rainfall would be provided by a trusted real-world provider (say the National Weather Service) or a crowd-sourced "oracle" implemented by another smart contract. The tamper resistant properties of blockchains protect against a party to a contract reneging; rather the smart contract directly enforces the contract.

Smart contracts are a powerful concept. They enable publicly verifiable implementation of agreements, automated "organizations" providing services, and the ability to replace high-fee centralized services with code. That power comes with challenges. Bugs in a smart contract are forever due to the immutability of blockchain data. Careful code verification can reduce this threat. However, unless the deployer of a smart contract includes calls to control the contract's operation after deployment, the contract is autonomous, leading to the term *decentralized autonomous organization* (DAO). Even if autonomous, smart contracts can provide proof of compliance with regulations if so coded, making them valuable resources for efficient management of complex agreements.

Much discussion surrounding digital assets and cryptocurrency recently has been tainted by scandals such as the FTX collapse, the direct loss of billions of dollars of investor’s money, and follow-on collapse of other centralized firms that relied on FTX. While these examples display a clear misuse of cryptocurrency, they do not point to faults in the digital-asset technologies, but rather the risks of these technologies being used by bad actors in nefarious schemes. The technologies we suggest here for our three-part goal of privacy, transparency, and regulatabilty have the ability to mitigate and, ultimately, eliminate the financial and accounting fraud behind the FTX scandal.

[5] Or, in the terminology of Hyperledger, *chaincode.*

The true value of digital assets and blockchain technology lies in their ability to establish trust between the untrusting. An example of this is in the healthcare industry. According to a 2016 report by Johns Hopkins University[6], the 3rd leading cause of death in the United States is due to medical errors, "resulting from poorly coordinated care, such as planned actions not completed as intended or errors of omission in patient records"[7]. Various reports since that study provide evidence that the problems are not diminishing despite a move to electronic health records. Although records may be electronic, access to those records is limited even in cases where there is a clear medical necessity to access them. The root cause of this problem is that health records are stored in separate repositories that have their own data access controls and authentication framework. A single central national health data repository would raise numerous privacy concerns. A solution to this problem would be creating a blockchain-based medical-records system, which could store patient information while also only being accessible if the patient gives consent (directly or via an authorized representative or a personally carried access code). This would allow all patient information to be accessible through one system, enabling medical practitioners to provide better informed care and limit errors in a patient's medical history due to omission of records. Ultimate ownership of medical data would be with the individual, with each entry digitally signed by the health provider involved.

This example of health information is one of many that detail the need for blockchain technology use and competency in the United States, and also prove the risk of not furthering R&D in this area. By simply listening to popular debate of blockchain technologies and the misuse of cryptocurrency in nefarious financial schemes, it is easy to view these technologies negatively, and even become jaded against allocating them further funding towards research and development. However, it is also important to realize the risks of limiting this research in the United States, and allowing foreign nations to become dominant in this field. Said differently, it is important to recognize that technologies of all types have both uses and misuses. Policy goals should seek to maximize positive use and minimize misuse. Simply running from a valuable technology because misuses exist is not likely to be the best policy choice; rather it leads to the benefits from positive use accruing to other nations.

The earlier discussion of smart contracts is another illustration of the need and value of further R&D in blockchain technology. Autonomous smart contracts (DAOs) are, by design, immune from external control post-deployment. That provides a high degree of valuable functionality, but presents challenges for regulatabilty. Integrating the power of smart contracts in an open, global blockchain setting with a trustworthy market framework remains a challenging problem. Placing legal and regulatory constraints on DAOs risks limiting their benefits and creating added risks for individual participants, yet lack of regulation presents participants with other potentially serious risks. Creating a framework for effective incorporation of this technology in a modern market remains an area of research that crosses the barriers between computing, finance, and

[6] Makary, Martin A., and Michael Daniel. "Medical Error—the Third Leading Cause of Death in the US." *BMJ*, BMJ, May 2016, p. i2139. *Crossref*, https://doi.org/10.1136/bmj.i2139.

[7] "5 Blockchain Healthcare Use Cases." *STL Partners*, stlpartners.com/articles/digital-health/5-blockchain-healthcare-use-cases.

the law. The nation that leads in research in that space will be the one best positioned to mix policy and technology in a way that allows that nation to win the global competition to create the most attractive markets. Here, too, running from a technology because of possible misuses is not the best policy choice.

Innovation and Leadership: Technology, Commerce, Social Values

Those countries that innovate tend to benefit the most from their innovations. From the days of the innovative use of assembly-line technology in manufacturing through to the invention of the technologies underlying the internet, US technical leadership in innovation led to US industrial leadership. So, tying back to the topic of digital assets, we are left with one question: are we willing, as a nation, to take a backseat and let foreign nations innovate in the field of digital assets, leading us to scramble to catch up, or should we lead the way and reap the benefits?

Leadership in the blockchain space has value beyond the specific examples cited here. As the Internet developed into a decentralized utility providing a communication-link for commerce and society, blockchain technology promises to be a decentralized trust-utility for commerce and for society. Recent supply-chain challenges show both the importance and potential frailty of the way businesses depend upon each other. Blockchain technology offers a means for timely, reliable sharing of supply-chain data enabling smoother supply chains. Blockchain's key contribution in this space is that members of a supply chain can collectively validate information that is digitally signed by firms, creating a trusted source of information spanning all firms participating in the supply chain and integrating with those firms enterprise databases and ERP systems. While this automation and auditability cannot prevent physical disruption to a supply chain, it can not only smooth normal operation, but also enable accurately informed rapid response to disruption. In an economy driven by long, complex supply chains, leading-edge technology in supply-chain infrastructure and its effective use becomes a competitive advantage. Several leading US technology firms are already active in this space and foundational research can provide the basis for continued US leadership in supply-chain systems.

Because blockchain-based information systems encode and automate policy decisions, leadership in blockchain is not only the economic issue that we noted above, but also one of advancing national values, including the rights and freedoms of individuals, and the access of the most disadvantaged to information-based services, most importantly the financial system. Blockchain technology can bring access to the financial system to the unbanked (this is already happening in the developing world and played out dramatically at the time of Russia's invasion of Ukraine). Blockchain technology can provide cryptographic proof of payment of a fair wage to workers along with a conveyance of that proof along the supply chain to the consumer, thus ensuring fair treatment of workers and reducing the chance of corruption. All these possibilities exist or are being prototyped. Systems of this sort can go beyond just wages to include certification of working conditions, not only in farms but also along the supply chain delivering products to end users. At each step, digital signatures combined with digital identities enable

documented public assertion regarding the path products take from raw materials to store shelves.

The value of blockchain technology for social good and financial inclusion is perhaps an even stronger justification for the US to seek R&D leadership in this space. While blockchain technology *can* be used for good, it can be used in other ways. The structure of the e-Yuan has a more centralized and less private design that could enable a stronger surveillance state and stronger access restrictions. Several prototype central-bank digital-currency systems instead enable maintenance of the decentralized ("two-tier") framework of today's western financial systems, with parameters that grant policy-makers a strong degree of policy choice. Technologies of this sort need continued R&D so that these positive properties can scale to the level of global finance and commerce.

Training the Next-Generation Workforce

The position of the US as the world's industrial and financial leader rests to a large degree on its leadership in data management and computing. The global nature of information and of digital assets implies that leadership entails not only technological leadership but also a world-class workforce trained to use (and extend) this technology. Historically, US leadership in computing technology in all its varied aspects has rested heavily on the contributions of academic research in the US, research that in large part has been funded by Federal agencies (NSF, DARPA, and others). Another significant source of support has been US-based firms in the computing field. That R&D funding enables not only research but also an educational framework to train the next generation of researchers and workers.

Earlier, we noted the foundational role of federal R&D support for the Internet. In 2011,[8] the CRA participated in an event showing how federal R&D support enabled the game-changing innovation in the iPad. In 2019, the CCC released "*A 20 Year Community Roadmap for Artificial Intelligence Research in the US*," which presented recommendations for increased funding of AI research and cited successful examples, such as the NSF and ARPA funding of the Linguistic Data Consortium (LDC), which created a repository for natural language datasets to train AI technologies in speech recognition[9]. The recent federal support for research in Artificial Intelligence (AI) and its impact on society, through grants, National AI Research Institutes, and initiatives such as the National AI Research Resource, is enabling US leadership in AI. Today, the nation has a similar opportunity to stimulate not only research but also the skilled human infrastructure needed for effective development of research into digital-asset products and the deployment of those products in the market.

---

[8] Melissa Norr. “Deconstructing the iPad.” *GovAffairs*, 20 Sept. 2011, cra.org/govaffairs/blog/2011/09/deconstructing-the-ipad.

[9] Y. Gil et al. “A 20 Year Community Roadmap for Artificial Intelligence Research in the US.” *Computing Community Consortium*, August 2019, https://cra.org/ccc/wp-content/uploads/sites/2/2019/08/Community-Roadmap-for-AI-Research.pdf

The computing technology underpinning blockchain includes many areas already strongly supported by Federal initiatives, including distributed computing, parallel computing, cryptography, among others. Blockchain systems combine these technologies in unique ways that create new programming paradigms and new user-computer interaction paradigms. Translating technology to impactful practice requires educational excellence at all levels: user experience, application design (especially novel and disruptive applications), along with the system internal structure itself (cryptographic mathematics and algorithms, verification of blockchain smart contracts, high-performance systems, etc.). At present only a modest fraction of universities offer a strong set of courses in blockchain systems, technology, and applications. In the 2022 CoinDesk ranking of the top 50 universities in blockchain only 1/3 are US-based. US-based schools typically occupy at least half of top-50 rankings of universities in general. Anecdotal evidence suggests that blockchain education remains largely absent below the top "elite" universities in the US. College and university student clubs focus more on trading than on the technology and its impact.

Most discussion of technology and workforce development focuses on the "STEM" disciplines, and the CRA's focus certainly reflects that. However, blockchain education is not just a STEM issue. As noted above, blockchain-based information management enables richer enterprise collaboration, better targeted monetary and fiscal policy, and documentable values-based social policies. While leadership in business and policy may not need training in the mathematics of esoteric technologies like zero-knowledge proofs, leaders do need a strong factually grounded understanding of the capabilities of the technology not just to do old things better but rather to do things that could not be done effectively before. Though there are a few examples of knowledgeable leaders on these topics in business and government, such leaders are still sorely lacking in these fields. A spinoff effect of investment in R&D in an academic setting is an increased amount of training for the next-generation workforce.

Arguably, federal R&D support for research in technologies underlying digital assets should be partnered with support for development of courses and experiential learning addressing both the technologies themselves and their applications. Much of the mathematics underlying blockchain is from branches of mathematics that tend to be less-covered in computing curricula (groups and fields, cryptography). The computing subdomains of parallel consensus and software verification need greater emphasis. Relatively few business curricula cover blockchain and its applications in supply chain, finance, etc. Beyond the technical and business disciplines, the applications of blockchains for social good could inspire new generations of policy leaders.

Conclusion

At present, the US is behind the world as a whole in blockchain technology research, education, and policy. There is a strong industrial and entrepreneurial presence that needs to be nurtured and developed. Past experience with R&D investment and supportive policy at the government level in computing technology has, and is paying dividends. This has been demonstrated with the internet, digital commerce, chips, personal devices such as the iPhone, and most recently,

AI. The area of digital assets is the next open frontier for innovation in computing and information technology.

The largest open question is who will be the leader in this next frontier for innovation in computing and information technology? Will it be the US, as it has largely been in the post World War II era? The answer depends on how the US reacts both in its policy decisions and in its investment decisions. This report focuses on the second of those two: investment. The US tradition of strong federal R&D investment at an early stage has paid huge dividends both in the economy and in world leadership. At key points in the past, federal investment in education and workforce development has allowed the nation to be the first-mover in taking advantage of the research developed in the US.

There are concrete steps that the federal government can take to help ensure that the era of digital assets is led by the US:

- Direct support for research and development in the blockchain technologies that support digital-asset management, particularly investment in academic research.
- Encouragement of the development of digital-asset systems that enable a mix of privacy, transparency, and regulatabilty by creating a framework that enables policy choice and appropriate levels of decentralization.
- Augmentation of R&D support with support for educational initiatives and expansion of educational offerings in blockchain and digital-asset technologies both in the STEM disciplines and in the disciplines impacted by digital-asset technology.
- Promotion of positive-use-case examples in the digital-asset space to inspire projects to enhance national economic competitiveness and social good.

A recurring theme in a discussion of digital assets is decentralization. Examples above have shown how such decentralization and disintermediation can positively impact many aspects of society. Open, accessible systems that use blockchain technology to combine that openness with the critically important properties of privacy and regulatability offer the potential of creating fairer, freer, and more just systems from finance to healthcare. But that potential can be achieved only if the leadership in the technology comes from nations with such traditions and values.