ORNL/TM-2018/1026

Advancing the Science and Impact of Blockchain Technology at Oak Ridge National Laboratory

Jesse T. Ault
Alvin M. Weinberg Fellow
BSEC Group, CSED

October 5, 2018

**Approved for public release.
Distribution is unlimited.**

OAK RIDGE NATIONAL LABORATORY
MANAGED BY UT-BATTELLE FOR THE US DEPARTMENT OF ENERGY

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

ORNL/TM-2018/1026

Computational Sciences and Engineering Division

Advancing the Science and Impact of Blockchain Technology at Oak Ridge National Laboratory

Jesse T. Ault
Alvin M. Weinberg Distinguished Fellow
Biomedical Sciences, Engineering, and Computing Group

Date Published: September, 2018

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, TN 37831-6283
managed by
UT-Battelle, LLC
for the
US DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

CONTENTS

LIST OF FIGURES

ABSTRACT

Over the last decade, blockchain technology has experienced unprecedented growth from its humble beginnings as the decentralized currency Bitcoin in 2009 to a $500 billion industry today with applications including decentralized cloud computing, peer-to-peer lending, governance, social media, cybersecurity and the development of decentralized, trustless smart contracts and applications. Although it has not yet reached maturity, the blockchain technology industry (sometimes hailed as the "Web 3.0") is experiencing exponential growth and adoption: new projects and partnerships are announced almost daily, and top research institutions are beginning to develop novel initiatives in this space. In this white paper, I will outline a vision for the future of blockchain technology at Oak Ridge National Laboratory (ORNL). Specifically, I will (1) introduce the fundamental concepts of blockchain technology and provide a survey of the current state-of-the-art, (2) identify the wide-ranging applications that blockchain technology can have across groups, divisions, and directorates at ORNL, (3) summarize the newly initiated programs in blockchain technology at ORNL's core partnership universities that may lead to future collaboration opportunities, (4) suggest critical ways that blockchain technology can advance ORNL's strategic objectives for excellence in science and technology, laboratory operations, and community engagement, and (5) outline the most likely funding strategies to support new blockchain initiatives and partnerships at the Lab. Finally, I will propose a vision for the future of a Blockchain Institute at ORNL.

1. INTRODUCTION

Decentralized peer-to-peer systems based on blockchain technology represent a paradigm shift for major institutions including health data sciences, energy generation and distribution, cybersecurity, finance, and social contracts. In this section, I will introduce the fundamentals of blockchain technology as well as a brief survey of several recent successful projects built using this technology. I will also demonstrate the exponential growth and adoption of blockchain technology in both industry and academia, and describe several new government-sponsored initiatives in this space. In Section 2., I describe critical research areas at ORNL that are likely to be impacted by the development of blockchain technology. I also summarize recent research projects and initiatives that have been launched by ORNL's core partnership universities, and I propose two example pilot projects for the Lab. In Section 3., I show how the institution of new blockchain initiatives at ORNL could serve to advance the strategic objectives of the Lab. In Section 4., I outline several possible funding mechanisms that could be used to implement new research and development as well as information technology (IT) modernization programs. In Section 5., I propose the formation of a formal *Blockchain Institute* at ORNL and outline a vision for the future of this initiative and the adoption of blockchain technology and research at the Lab more generally. Finally, in Section 6., I offer several conclusions.

1.1 What is blockchain technology?

At its simplest, blockchain technology may be thought of as a new type of accounting system, based on a continuously growing public ledger that is secured using cryptography. To paraphrase a definition from the Blockchain at Berkeley club [3]: "A blockchain is a digital ledger of transactions that can be shared among a distributed network of computers. It uses cryptography to allow each participant on the network to manipulate the ledger in a secure way without the need for a central authority." Blockchains can facilitate decentralized consensus with impressive inherent security partly due to their high Byzantine fault tolerance, i.e. the ability to achieve consensus in a network when malicious actors are present. Furthermore, blockchains record transactions in a nearly immutable and verifiable way, i.e., modifying the blockchain or falsifying transactions can be made prohibitively costly. Because of this, blockchains have potential applications that include processing financial transactions, managing digital identities, sharing electronic health records, and voting.

In order to better understand these features, we can study the example of Bitcoin, which was the first demonstration of blockchain technology, and the first form of digital money to solve the double-spend problem in a decentralized network. Forms of digital money have existed since 1990, when David Chaum introduced the electronic cash company DigiCash [27]. Since then, a range of digital currency services have existed, including E-gold, Liberty Reserve, PayPal, and others. In any form of digital money, there is a so-called “double-spend problem,” in which the network must verify that no tokens are spent more than once. In all systems before the creation of Bitcoin in 2008, this problem was solved by a centralized authority. That is, users of digital money must trust a centralized authority, such as a bank, to properly account for and distribute their money. For example, an individual may attempt to make a purchase with a credit card. The payment system will then make a request to that person’s bank, which will determine whether appropriate balances are available, authorize the transaction, and extract any relevant fees. This entire process relies on multiple layers of trust, i.e. card holder—merchant, merchant—bank, and bank—card holder.

Bitcoin instead uses blockchain technology to solve this problem in a distributed, peer-to-peer, and decentralized way via a concept called Proof-of-Work (PoW). PoW makes the cost of altering the distributed ledger, the blockchain, prohibitively high for malicious actors so that transactions are effectively verifiable and irreversible. As a result, individuals can directly send funds to another user, the receiving user can know with strong confidence that they received the funds, and the entire network can verify with confidence that the transaction did in fact happen. Such a system simultaneously eliminates the need for a centralized authority, which represents a honeypot for hackers and a central point of failure, and it eliminates the risk of fraud such as chargebacks, which are common with PayPal and credit card transactions. Now, with cryptocurrencies like Bitcoin, it is possible for an individual to send and receive money to and from anyone around the world, whether he or she trusts them or not and determine with confidence the ownership of funds, all through a peer-to-peer network with no central authority or single point of failure.

Although Bitcoin is by far the most popular use of blockchain technology to date, having recently reached new record highs in price along with widespread media coverage, digital money or cryptocurrencies actually represent only one of many potential applications of this technology. Indeed, there are currently over 1500 different existing blockchain network projects, many of which have applications far beyond simply the use as digital money. Many of these projects utilize a concept known as smart contracts. Smart contracts, first proposed by Nick Szabo in 1994, are computer protocols that “digitally facilitate, verify, or enforce the negotiation or performance of a contract” [28]. These allow the execution of trusted triggered code without the use of third parties. Smart contracts make possible the development of general decentralized applications to run on a blockchain network. For example, even with Bitcoin it is possible to insert programmatic language into the metadata of each transaction and thus build applications that run on the Bitcoin network, although much more powerful and efficient blockchain networks have been developed specifically for decentralized applications (or Dapps) based on the concept of smart contracts.

1.2 Example applications of blockchain technology

In order to better understand what types of applications besides digital money are possible with the use of smart contracts and blockchain technology, the following list contains brief descriptions of some of the existing more popular blockchain/cryptocurrency projects:

1. **Namecoin:** Decentralized platform for DNS servers, TLS validation, and identity management.
2. **Ethereum:** Open-source decentralized and distributed computing platform and operating system that provides a Turing-complete virtual machine.
3. **IOTA:** Public network that may serve as a backbone for the Internet of Things, enabling interoperability between all interacting devices through microtransactions.
4. **Bitshares:** Decentralized exchange for asset exchange, price-stable cryptocurrencies, and user-issued assets.
5. **Steem:** Decentralized, censorship-proof social media platform that pays users and content creators to use the network.
6. **Ripple:** Enterprise blockchain solution for global payments. Ripple "connects banks, payment providers, digital asset exchanges and corporations" [21].
7. **Monero:** Decentralized cryptocurrency with built-in cryptographic privacy features. Monero automatically obscures senders, recipients, and amounts, so that all transactions are private, secure, and untraceable.
8. **Augur:** Decentralized prediction markets to aggregate collective information and provide powerful predictive data.
9. **Basic Attention Token:** Blockchain-based digital advertising platform that improves the efficiency of digital advertising by managing exchange between publishers, advertisers, and users.
10. **Golem:** Global, open-source, decentralized supercomputer that anyone can use. Golem "creates a decentralized sharing economy of computing power and supplies software developers with a flexible, reliable and cheap source of computing power" [10].
11. **MaidSafe Network:** Decentralized, secure data management service built from the sharing of unused computer resources of the network participants.

This list provides just a small sample of the potential applications for blockchain technology. Indeed, with the creation of platforms for decentralized applications such as Ethereum, NEO, and EOS, that provide Turing-complete virtual machines, there is now no limit to the types of applications that may be decentralized using blockchain technology.

1.3 Accelerating adoption of blockchain technology

Since the launch of Bitcoin in 2009, the growth of the blockchain industry has exploded, especially in the last 4–5 years. This can be seen through the rapid exponential increase in the number of peer-reviewed journal publications involving blockchain and cryptocurrencies, the expanding numbers of fast-growing blockchain start-up companies, the number of prestigious academic institutions that are beginning to adopt courses in blockchain technology, and the exponentially growing market value of the total cryptocurrency market. The total number of peer-reviewed publications related to cryptocurrencies and blockchain

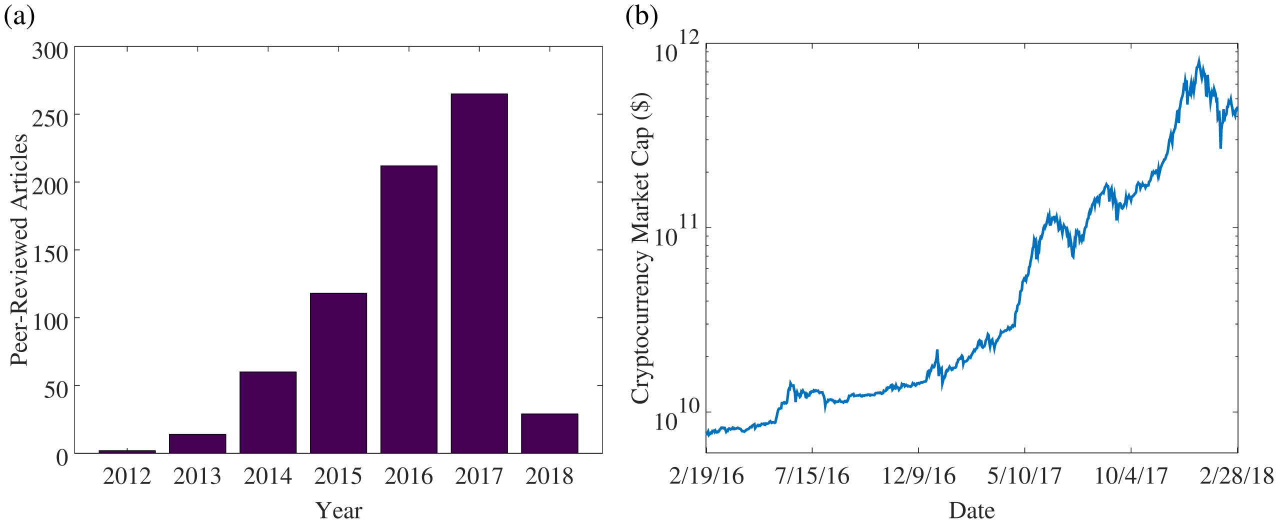

Figure 1. Growth of the blockchain/cryptocurrency technology sector in both industry and academia. (a) Total number of new peer-reviewed journal articles per year focusing on cryptocurrency and blockchain technologies [26]. (b) Growth of the total cryptocurrency market cap showing the growing market value of all blockchain network tokens [6].

technology per year are shown in Figure 1a. As can be seen, the growth has been exponential, and in just five years this research field has grown to one with hundreds of publications per year, and the University of Pittsburgh has also published several volumes of the new blockchain-focused peer-reviewed scholarly journal *Ledger* [23]. The exponential growth of the total market value of all cryptocurrencies is presented in Figure 1b, showing that the value of blockchain network tokens has risen by two orders-of-magnitude in just the last two years.

Numerous prestigious research-oriented universities including MIT, Princeton, Stanford, Duke, UC-Berkeley, and others have also begun to pursue research in blockchain technology and develop new courses, student organizations, and other initiatives in the blockchain space, such as the MIT blockchain initiative [13] and the Blockchain at Berkeley student organization [3]. Some of the newly designed academic courses at top universities related to cryptocurrency and blockchain technology include [5]:

1. **New York University:** *The Law and Business of Bitcoin and Other Cryptocurrencies* and *Digital Currency: Revolution in Money and Payments?*

2. **Duke University:** *Innovation, Disruption and Cryptoventures*

3. **Princeton University:** *Bitcoin and Cryptocurrency Technologies*

4. **Stanford University:** *Bitcoin Engineering*

5. **University of California-Berkeley:** *Blockchain Fundamentals* and *Blockchain for Developers*

6. **University of Illinois at Urbana-Champaign:** *Cryptocurrency Security*

7. **Massachusetts Institute of Technology:** *Shared Public Ledgers and Cryptocurrencies*

8. **George Mason University:** *Blockchain Technologies*

Finally, several United States funding agencies have also begun to solicit grant proposals for funding related to blockchain technologies. For example, the National Science Foundation (NSF) is seeking to support research on the use of blockchain technology to improve the resiliency of cyber-infrastructure [4]. Blockchain technology is an appropriate choice for this research due to its high Byzantine fault tolerance; that is, blockchain networks are exceptionally resilient to system/node failures as well as to malicious actors. The NSF has recently funded research towards the development of a secure infrastructure for medical data for the purpose of translational research [18]. The Department of Homeland Security (DHS) recently funded the startup company Evernym through its Small Business Innovation Program (SBIR) to support the development of a decentralized key management solution for blockchain technologies [8]. Furthermore, the Department of State has recently created a project known as Blockchain@State to provide opportunities for American college and university students to virtually intern at U.S. Federal Agencies and research applications of blockchain technology for the use of foreign policy and data tracking developments [25]. The National Aeronautics and Space Administration (NASA) has expressed interest in blockchain technology, awarding funding to the University of Akron to research the potential to improve space communications with blockchain technology [7]. Finally, the United Nation's World Food Programme has administered a program using blockchain technology to deliver vouchers to Syrian refugees [9]. Although the scope of government funding of blockchain technology programs remains relatively small, these initiatives certainly signal a move towards the adoption of blockchain technology at major funding agencies. Thus, among both private research universities, industry, and government agencies, blockchain and cryptocurrency technologies are seeing adoption at an ever-accelerating rate.

2. OPPORTUNITIES FOR BLOCKCHAIN RESEARCH AT ORNL

In the previous section, I introduced a variety of existing blockchain projects, as well as several examples of research initiatives that have been funded by government agencies. In this section, I will describe some of the key application areas where blockchain technology may impact ORNL, and I will highlight specific groups and projects that may benefit from a new research focus involving blockchain technology. First, I will present an overview of how blockchain research can fit into the Lab's organizational structure. Then, I will summarize some of the key blockchain initiatives being undertaken by ORNL's core partnership universitites that may lead to future collaboration opportunities. Finally, I will describe two example pilot projects involving blockchain technology to illustrate in more detail several specific application areas for the Lab.

2.1 Overivew

A brief overview of some of the potential opportunities for innovative research and development of blockchain technology at ORNL is shown in Figure 2. The major sections of the Lab where immediate opportunities for innovation in blockchain technology exist are the Computing and Computational Sciences Directorate (CCSD), the Exascale Computing Project (ECP), the Energy and Environmental Sciences Directorate (EESD), and the Partnerships Directorate.

In CCSD, the main areas where blockchain technology may have potential applications are the Computer Science and Mathematics Division (CSMD), the Computational Sciences and Engineering Division (CSED), the Oak Ridge Leadership Computing Facility (OLCF), and the Joint Institute for Computational Sciences (JICS). For example, groups in CSMD have research projects related to future technologies,

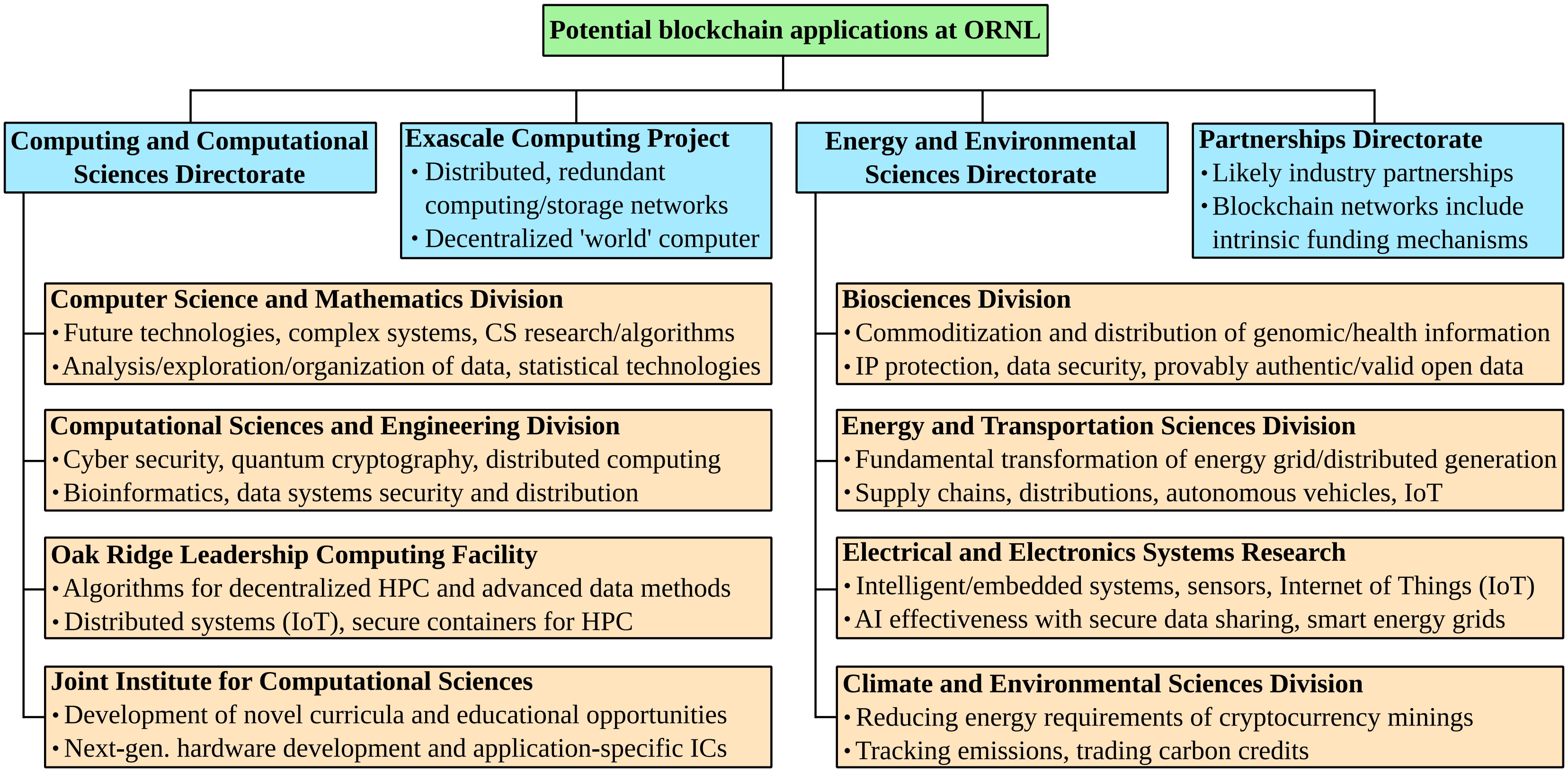
Potential blockchain applications at ORNL
Computing and Computational Sciences Directorate
Exascale Computing Project
• Distributed, redundant computing/storage networks
• Decentralized 'world' computer
Energy and Environmental Sciences Directorate
Partnerships Directorate
• Likely industry partnerships
• Blockchain networks include intrinsic funding mechanisms
Computer Science and Mathematics Division
• Future technologies, complex systems, CS research/algorithms
• Analysis/exploration/organization of data, statistical technologies
Computational Sciences and Engineering Division
• Cyber security, quantum cryptography, distributed computing
• Bioinformatics, data systems security and distribution
Oak Ridge Leadership Computing Facility
• Algorithms for decentralized HPC and advanced data methods
• Distributed systems (IoT), secure containers for HPC
Joint Institute for Computational Sciences
• Development of novel curricula and educational opportunities
• Next-gen. hardware development and application-specific ICs
Biosciences Division
• Commoditization and distribution of genomic/health information
• IP protection, data security, provably authentic/valid open data
Energy and Transportation Sciences Division
• Fundamental transformation of energy grid/distributed generation
• Supply chains, distributions, autonomous vehicles, IoT
Electrical and Electronics Systems Research
• Intelligent/embedded systems, sensors, Internet of Things (IoT)
• AI effectiveness with secure data sharing, smart energy grids
Climate and Environmental Sciences Division
• Reducing energy requirements of cryptocurrency minings
• Tracking emissions, trading carbon credits

Figure 2. Overview of several opportunities for innovative research and development of blockchain technology at ORNL.

complex systems, algorithms, statistical technologies, and the analysis, exploration, and organization of data, all of which represent areas potentially affected by blockchain technology. Blockchain networks have already proven themselves to represent an entire new class of future technologies, and as they decentralize existing systems and industries, new complex, dynamic, many-actor systems are being created to take their place. Furthermore, blockchains represent a fundamentally new type of data store which can simultaneously be public and secure based on cryptography.

In CSED, cyber security, quantum algorithms, distributed computing, bioinformatics, and data systems can all benefit from blockchain technology. For example, as demonstrated by the NSF's call for proposals previously mentioned, blockchain technology represents a new type of system for securing networks. As the market value of blockchain technology grows, the applications for quantum computing and quantum-resistant cryptography will grow. Furthermore, projects like Golem have demonstrated the capability of blockchain networks to economize and manage global distributed computing networks. Many applications of blockchain to the field of bioinformatics have been proposed such as providing secure and controlled access to genomic data, or the commoditization and distribution of health data in general. In terms of data security and distribution, blockchain represents a mechanism for rapidly reaching consensus about the state of data in a way that is strongly resistant to errors and resilient to network node failures.

OLCF and the ECP also oversee research with applications to blockchain technology, such as technology for integration in distributed systems (i.e. the Internet of Things), as well as secure algorithms for decentralized high-performance computing. For example, the total computational power potentially available to the Golem network is on the order of 10^{21} FLOPS, or three orders-of-magnitude more powerful than an exascale computing system [1]. This demonstrates that the DOE's mission for exascale computing and beyond may actually lie in the ability of blockchain technology to economize and expand global, decentralized supercomputing resources. Technological innovations of blockchain technology also have application to JICS research, specifically in the areas of next-generation hardware development and application-specific integrated circuits. Furthermore, one of JICS stated aims is to develop novel curricula and educational opportunities. As evidenced by the adoption of blockchain courses at top-tier research institutions, there still remains significant opportunity for innovation in the field of blockchain education.

In EESD, the main areas where blockchain technology may have potential applications are the Biosciences Division, the Energy and Transportation Sciences Division (ETSD), the Climate and Environmental Sciences Division (CESD), and Electrical and Electronics Systems Research (EESR). For example, the Biosciences Division has overlap with CSED regarding applications of blockchain technology to problems related to health data sciences, such as the commoditization and distribution of genomic and other health-related information. Beyond that, blockchain technology can lead to innovations in intellectual property protection, data security, and provably authentic/valid open data, all of which can drive advances in how bioscience research is performed. Regarding applications of blockchain technology in ETSD, energy experts think that blockchain technology can fundamentally transform the generation and distribution of energy with distributed smart networks [16]. Furthermore, blockchain technology has the potential to greatly improve the efficiency of supply chains and distributions through Internet of Things connectivity, and also has potential applications to autonomous vehicles, where redundant, verifiable, immutable transactions are critical.

In CESD, as mentioned, blockchain technology has applications to the development of smart energy grids and to the improvement of emissions tracking, carbon credit trading, etc... Using blockchain, a smart market for carbon credit trading between a network of connected devices and plants can be automated with emission-tracking sensors and lead to improved efficiencies and more sustainable operations based on market principles. Furthermore, optimizing cryptocurrency/blockchain mining operations is critical for environmental/energy security, as the Bitcoin network alone is estimated to consume around 32 TWh of electricity per year, about as much as the nation of Denmark [2]. In EESR, blockchain technology has applications to intelligent/embedded systems and sensors (i.e. Internet of Things applications), as well as to increasing Artificial Intelligence (AI) and machine learning effectiveness through secure data sharing.

Finally, due to the intense degree of ongoing innovation in the blockchain technology industry, there exist many potential opportunities for both industrial and academic partnerships, which have direct application to the Partnerships Directorate at ORNL. Furthermore, since many blockchain projects include intrinsic funding mechanisms, there also exist potential economic opportunities for the Lab to take advantage of this new technology. It still remains for world-class academic and research facilities to establish themselves as world-leaders in blockchain technology and innovation. Significant opportunities for innovative research and development exist in blockchain applications, and these applications are critically relevant to the Department of Energy's core missions. With its tremendous expertise and reputation for excellence in science and technology, ORNL can take a leadership role in this space and emerge as an innovator and pioneer in blockchain technology.

2.2 ORNL's core partnership universities

Having demonstrated the wide-ranging application areas that blockchain technology may have for research groups and divisions across the Lab in the previous section, here I provide a survey of the many blockchain-related research activities and initiatives that exist at ORNL's eight core partnership universities. The purposes of this survey are to demonstrate that each of the Lab's partner universities has active programs in blockchain technology, to identify future potential research projects and collaborations, and to support the formulation of a clear vision for the future of blockchain technology at the Lab. An overview of several of the key initiatives from each of ORNL's eight core partnership universities is presented in Figure 3.

2.2.1 Duke University

At Duke University, the student-run organization the *Duke Blockchain Lab* is dedicated to empowering and educating both students and professors to use the tools of blockchain technology to revolutionize their fields. In addition, several new courses have been developed in finance and business including *Blockchain and Innovation* and the Law & Policy Lab: *Blockchain, Innovation, and Cryptoventures*. On the technical side, the Computer Science Department has just made a new strategic faculty hire of Kartik Nayak from the VMWare Research Group who does research in blockchain technology.

2.2.2 Florida State University

At Florida State University, the student-run organization the *Cryptocurrency Club* is dedicated to educating students about the future, technology, and economic impacts of cryptocurrencies. The university is also partnering with IBM to co-host the Collegiate Blockchain Conference with a mission to advance education of blockchain. Several faculty members are pursuing academic research on blockchain technology such as

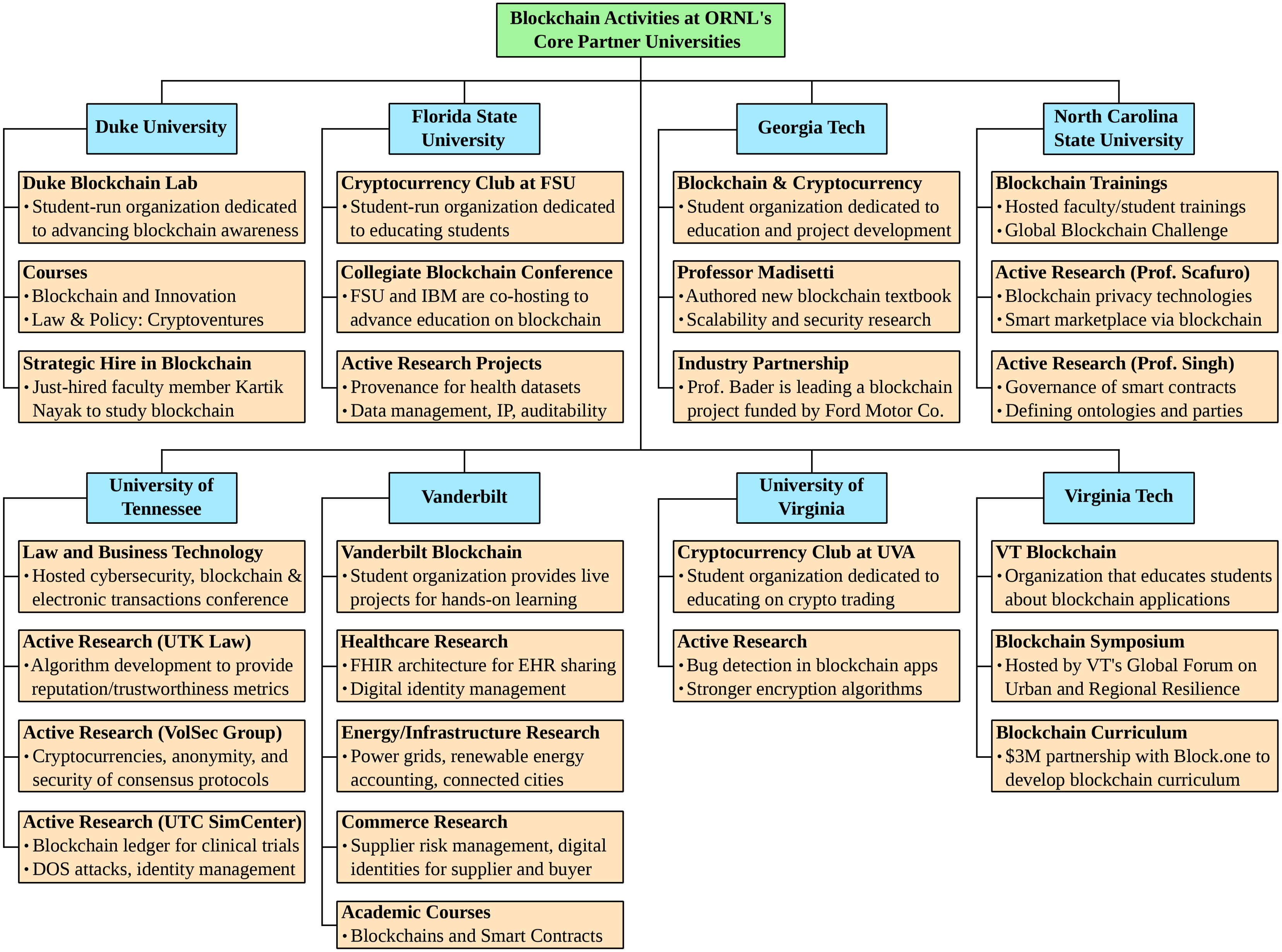
Blockchain Activities at ORNL's Core Partner Universities
Duke University
Duke Blockchain Lab
• Student-run organization dedicated to advancing blockchain awareness
Courses
• Blockchain and Innovation
• Law & Policy: Cryptoventures
Strategic Hire in Blockchain
• Just-hired faculty member Kartik Nayak to study blockchain
Florida State University
Cryptocurrency Club at FSU
• Student-run organization dedicated to educating students
Collegiate Blockchain Conference
• FSU and IBM are co-hosting to advance education on blockchain
Active Research Projects
• Provenance for health datasets
• Data management, IP, auditability
Georgia Tech
Blockchain & Cryptocurrency
• Student organization dedicated to education and project development
Professor Madisetti
• Authored new blockchain textbook
• Scalability and security research
Industry Partnership
• Prof. Bader is leading a blockchain project funded by Ford Motor Co.
North Carolina State University
Blockchain Trainings
• Hosted faculty/student trainings
• Global Blockchain Challenge
Active Research (Prof. Scafuro)
• Blockchain privacy technologies
• Smart marketplace via blockchain
Active Research (Prof. Singh)
• Governance of smart contracts
• Defining ontologies and parties
University of Tennessee
Law and Business Technology
• Hosted cybersecurity, blockchain & electronic transactions conference
Active Research (UTK Law)
• Algorithm development to provide reputation/trustworthiness metrics
Active Research (VolSec Group)
• Cryptocurrencies, anonymity, and security of consensus protocols
Active Research (UTC SimCenter)
• Blockchain ledger for clinical trials
• DOS attacks, identity management
Vanderbilt
Vanderbilt Blockchain
• Student organization provides live projects for hands-on learning
Healthcare Research
• FHIR architecture for EHR sharing
• Digital identity management
Energy/Infrastructure Research
• Power grids, renewable energy accounting, connected cities
Commerce Research
• Supplier risk management, digital identities for supplier and buyer
Academic Courses
• Blockchains and Smart Contracts
University of Virginia
Cryptocurrency Club at UVA
• Student organization dedicated to educating on crypto trading
Active Research
• Bug detection in blockchain apps
• Stronger encryption algorithms
Virginia Tech
VT Blockchain
• Organization that educates students about blockchain applications
Blockchain Symposium
• Hosted by VT's Global Forum on Urban and Regional Resilience
Blockchain Curriculum
• $3M partnership with Block.one to develop blockchain curriculum

Figure 3. Overview of ongoing blockchain activities at ORNL's core partnership universities.

Professor Burmester, whose research focuses on the use of cryptography and blockchain for data provenance of large-scale health data records. A student group is also developing a blockchain application for data management, intellectual property management, and auditability.

2.2.3 Georgia Tech

At Georgia Tech, the student-run organization *Blockchain & Cryptocurrency @ Georgia Tech* is dedicated to expanding awareness about the fundamentals and applications of blockchain technology, as well as investing in cryptocurrencies. Professor Madisetti, whose research is in the areas of scalability, identity management, and security issues, recently authored the textbook "Blockchain Applications: A Hands-On Approch." Finally, Professor Bader is leading a project funded by Ford Motor Company to evaluate the use of blockchain for various use cases related to next-generation automobiles.

2.2.4 North Carolina State University

North Carolina State University has hosted blockchain trainings for students and professors and also participated in the Generation Blockchain Challenge. Furthermore, Professor Scafuro in the Computer Science Department is currently pursuing research projects related to privacy technologies in blockchain applications and the development of a smart marketplace via blockchain. Professor Singh is also exploring the blockchain space and researching the governance aspects of smart contracts.

2.2.5 University of Tennessee

At the University of Tennessee, the College of Law hosted the Cybersecurity, Blockchain, and Electronic Transactions Conference, and several students have developed an algorithm to determine trustworthiness and reputation scores based on blockchain transactions. Furthermore, the VolSec computer security research group led by Professor Schuchard is pursuing research in the areas of resilient cryptocurrencies, anonymity, and consensus protocol security. At the Chattanooga campus, the SimCenter led by Professor Skjellum is developing a novel Lightweight Mining (LWM) algorithm to provide data integrity and provenance with minimum hardware resource requirements. They are also working in the areas of security and identity management.

2.2.6 Vanderbilt University

At Vanderbilt University, the student-run organization *Vanderbilt Blockchain* is dedicated to educating the students about blockchain technologies and cryptocurrencies and providing hands-on learning opportunities through live projects. Vanderbilt has also begun to offer courses in blockchain technology such as *Blockchains and Smart Contracts*. Academic research on blockchain technology at Vanderbilt can be summarized in three main application areas: (1) Healthcare: medical record sharing and digital identify management for healthcare participants, (2) Energy and infrastructure: power grids, renewable energy accounting, and connected cities, and (3) Commerce: supplier risk management and digital identity management for both suppliers and buyers.

2.2.7 University of Virginia

At the University of Virginia, the student-run organization *Cryptocurrency Club at UVA* is dedicated to educating all of its members on trading and investing in cryptocurrencies. There is also some academic research in the Mathematics Department related to cryptography aspects of blockchain, such as finding bugs in blockchain and cryptocurrency applications and designing stronger encryption algorithms.

2.2.8 Virginia Tech

At Virginia Tech, the *VT Blockchain* organization led by Adjunct Instructor Nicholas Brown is dedicated to educating students about blockchain technology and its potential industrial applications. Virginia Tech's Global Forum on Urban and Regional Resilience also hosted the Blacksburg Blockchain Symposium to discuss emerging problems, questions, and applications of blockchain technology. One of the most exciting developments at Virginia Tech is the recently announced $3 million partnership between the university and Block.one, one of the leading providers of high-performance blockchains and the developer of the EOS software. The purpose of this partnership is to develop a full blockchain curriculum for the university in order to offer an undergraduate blockchain major, boot camps, and short courses.

2.3 Potential pilot blockchain projects at ORNL

Having demonstrated the wide-ranging application areas for blockchain technology at ORNL, as well as the various ongoing blockchain research and initiatives at the Lab's partner universities in the previous sections, I will now propose two pilot projects that represent examples of the types of research the Lab could pursue: facilitating data networks for biomedical data and developing the energy grid of the future.

2.3.1 Facilitating efficient and secure data networks for biomedical and health data sciences

Health data security and privacy are crucial and central components to every research program that utilizes individual, sensitive health care information. To date, the vast majority of these programs rely on centralized, secure data stores such as the secure enclave at ORNL that houses sensitive data for the Million Veteran Program. Furthermore, these systems rely on a large degree of trust in users and lack efficient mechanisms for auditing and verifying each user's specific interactions with the private data. Facilitating efficient, secure, and accountable access to these sensitive data stores remains an essential element of ORNL's independent and multi-institution collaborative programs such as the three pilot projects launched in partnership with the National Cancer Institute (NCI) under the Cancer Moonshot initiative. Blockchain technology represents a fundamental revolution in the sharing of private and sensitive data. Through the use of smart contracts, blockchain networks can be designed to guarantee the security of private health data, while simultaneously facilitating an unprecedented level of access to the high-value, potentially life-saving information. One can imagine, for example, a blockchain network for the sharing of pathology reports for use in natural language processing (NLP) algorithms. In such a network, the private reports may be stored encrypted on- or off-chain, with the blockchain itself providing an immutable record of the validity of the health data.

The use of private and public keys may then be used to provide access to different parts of the data set, as well as provide a reliable record of each user's interactions with the data. Furthermore, a blockchain network can be designed to guarantee that no access to the sensitive data is possible, or even necessary. For example, through the use of smart contracts, NLP algorithms and tool sets can be containerized in secure smart contract containers which can then be used to operate on the secure data in such a way as to guarantee that private, unencrypted data is never leaked to users. Such a system eliminates the need for secure hardened networks and eliminates the need to trust users, since every possible operation and transformation of the data is pre-defined in secure containers. The benefits of such a system include decentralization (elimination of a single point of failure or "honeypot" for hackers), accountability (the blockchain provides an immutable record of all interactions with the data), and security (rather than using hardened networks, restricted access, and trust to limit unlicensed access to the data, the core protocol of the blockchain network can guarantee that only authentic interactions with the data occur). Finally, because inappropriate usage and access to the data are restricted at the protocol level, it is possible to greatly increase access to the data to other researchers. In this way, blockchain networks can potentially accelerate innovation and novel discoveries in biomedical engineering, while guaranteeing the security of private health data.

The need for and utility of blockchain-based health data networks is evidenced by the growing number of healthcare-related blockchain startups seeking to capitalize on the efficiency and security gains that may be realized through the adoption of blockchain technology. For example, the Zenome project is developing a blockchain network for storing and commoditizing its users' private genomic data [17]. Another recent project named Medicalchain will use blockchain technology to create a user-focused electronic health record and to maintain a single version of the users' personal health data [14]. This will enable users to give their healthcare professionals access to their personal data in an auditable, transparent, and secure way. Medrec is another blockchain project designed out of MIT that gives transparent and flexible access to users' personal electronic health records [15]. Finally Health Nexus is another open-source blockchain protocol designed to focus on HIPAA compliance and provide a more efficient and secure network for healthcare data [22]. The common theme of these projects is the secure, private, and efficient use of blockchain technology for storing, sharing, and facilitating the usage of personal health data. As a steward for multiple sensitive health data repositories and as a leader in health data sciences research, ORNL has a unique position and clear opportunities to innovate in the development of blockchain networks for private health data.

2.3.2 Developing and securing the energy grid of the future

With total energy consumption at near record highs and a continuously evolving energy landscape, developing, maintaining, and securing America's aging energy grid infrastructure remains a critical issue under the stewardship of the Department of Energy. Growing numbers of significant power outages per year continue to plague our energy grid (less than five per year from the 1950s to the 1980s, 76 in 2007, and more than 300 in 2011) [19]. Furthermore, the U.S. energy grid currently lacks the capability to fully benefit from and integrate the growing boom in renewable energy sources. For example, enough homes in Hawaii are equipped with solar panels to provide more electricity than the entire state needs on sunny days, but the power grid cannot efficiently use or store that power [19]. Furthermore, utility companies in some states actually pay wind farms to shut down their turbines on windy days because the power grid cannot handle the surge in power that they produce [19]. Under the auspices of the U.S. Department of Energy, major programs such as the Grid Modernization Initiative (GMI) have been put in place to coordinate a portfolio of activities and objectives to advance the power grid [24]. Solving these significant challenges of efficiently and securely generating and distributing power remains a critical mission towards securing the energy grid of the future.

Blockchain technology represents a novel secure peer-to-peer network protocol that has the potential to revolutionize certain aspects of our energy grid infrastructure. The need for and advantages of decentralized energy generation/distribution microgrids have been recognized by, for example, the $5 million support in 2015 from the Office of Energy Efficiency and Renewable Energy for projects developing microgrids for the sharing of solar energy [20]. The Brooklyn Microgrid developed a novel solution to this problem by successfully using blockchain technology to demonstrate a fully functioning community microgrid for efficiently and securely distributing solar energy between neighbors [11]. The use of smart contracts allows the blockchain network to seamlessly distribute the solar energy through microtransactions; smart sensors continuously sell electricity to or purchase from neighboring houses. Such a system has multiple advantages. For example, the blockchain-based microgrid has a load-leveling effect that tends to reduce power surges, and it improves energy efficiency because excess energy does not need to be first sold back to the utility before it can be sold to another consumer. Utility companies have also begun to express interest in blockchain technology. A partnership between the blockchain startup Electron and the Tokyo Electric Power Company (TEPCO) demonstrates the industry’s move toward “smart grid infrastructure and new market norms of decarbonization, decentralization, digitization and democratization" to encourage efficient power sharing through the use of blockchain technology [12].

With a mandate to provide innovative solutions to the nation’s critical energy problems and to develop an efficient, secure, and reliable power grid for the future, ORNL’s energy research divisions stand to benefit from the integration of blockchain research for smart grid development. Specifically, blockchain-based microgrids involve the integration of electric systems engineering, power and energy systems, and sensors and embedded systems. As this research area is entirely novel, significant research questions remain to be answered including: (1) How can the concept of blockchain-based microgrids be integrated with the distribution systems of a public utility? (2) What types of gains in terms of efficiency, reliability, and security are possible through the integration of blockchain technology? (3) Can blockchain-based microgrids lower the costs of upgrading our aging energy infrastructure? (4) How can the integration of blockchain technology into our energy infrastructure improve our national energy security? These significant research questions suggest that the decentralized energy distribution systems made possible by blockchain technology have direct relevance to the Lab, as well as to the DOE through its mandate to develop and secure an efficient and reliable energy grid for the future.

3. STRATEGIC OBJECTIVES FOR THE LAB

The ORNL Lab Agenda provides a framework that identifies both the major long-term initiatives and the short-term research and development missions for the Lab with respect to science and technology, laboratory operations, and community engagement. In this section, I will briefly show how adopting innovative blockchain technology programs can advance these initiatives.

3.1 Excellence in science and technology

As stated in the Fiscal Year 2018 Laboratory Agenda, ORNL’s critical outcome for excellence in science and technology is to “Deliver scientific discovery and technical breakthroughs that support DOE missions in clean energy and global security, creating economic opportunity for the nation." As I described in the previous sections, blockchain technology has direct applications to both clean energy and global security. Some of the specific initiatives to further this critical outcome that will be impacted by blockchain technology include scaling computing and data analytics, advancing the development of integrated and inter-operable energy systems and connected devices, addressing complex security challenges, especially those revolving around mission critical data, managing the deployment of intellectual property and strategic engagements among industry and universities, and advancing ORNL's culture of science and innovation.

3.2 Excellence in laboratory operations and ES&H

ORNL's critical outcome for excellence in laboratory operations and ES&H is to "sustain and improve ORNL's ability to serve the needs of the DOE and the nation through responsible stewardship," which includes initiatives to improve efficiencies and reliabilities of systems, modernize and sustain Lab infrastructure, and build ORNL's nuclear infrastructure. Blockchain technology has the potential to advance each of these initiatives, especially through information technology modernization programs. Blockchain networks represent redundant, resilient data systems with verifiability and immutability. Such systems can improve the efficiency and reliability of mission-critical networks that require accurate and secure data such as identity management and nuclear infrastructure systems that demand reliable data availability, security and verifiability.

3.3 Excellence in community engagement

ORNL's critical outcome for excellence in community engagement is to "Be viewed by our neighbors as a highly valued partner in the region," which includes initiatives to strengthen ORNL's reputation for scientific excellence and enhance recognition of ORNL's value to the region. While major research institutions and universities have begun to implement a variety of blockchain-oriented research projects, academic courses, and student-led organizations, very few have announced major programmatic initiatives in blockchain technology such as the establishment of a *Blockchain Engineering Department* at a university or a *Blockchain Science and Technology Group* at a national lab. ORNL has the opportunity to launch unprecedented programs in blockchain science and technology and stand out as a leader in this space, which will reinforce and enhance our reputation for scientific excellence. Furthermore, as evidenced by the recently announced partnership between Block.one and the Computer Science Department at Virginia Tech, significant opportunities exist to extend and develop the Lab's university partnerships and innovate in the development of curricula and degree programs in blockchain technology, which would enable our partners to emerge as leaders in blockchain education. There is currently a tremendous demand for blockchain engineers since there are no specific comprehensive educational training programs in this space at major universities, and working to form such programs with our partner institutions would absolutely enhance recognition of ORNL's value to the region.

4. FUNDING OPPORTUNITIES

In this section, I will briefly discuss potential mechanisms to fund research and development projects in blockchain technology at the Lab, as well as other initiatives such as educational partnerships. While funding opportunities in blockchain technology include many of the traditional mechanisms, such as government funding, industrial partnerships, and technology transfer, blockchain is unique in that several particular funding opportunities exist that have not existed before, such as mining for cryptocurrencies, developing a new open-source blockchain project for the lab, and serving as a trusted block producer for a well-respected existing network. A brief discussion of the most likely funding mechanisms for blockchain initiatives at the Lab is given here:

4.1 Laboratory Directed Research and Development (LDRD)

The purpose of the LDRD program is to support cutting-edge research across ORNL. Through the Director's R&D Fund, the Seed Money Fund, and the Named Fellowships, the LDRD program can guide the direction of research across the Laboratory, open new research areas for innovative ideas and technologies, and secure the Lab's ability to support the missions of the Department of Energy. Just as the Lab is currently advancing its artificial intelligence initiative through a special round of LDRD funding, the Lab could likewise drive new initiatives in blockchain technology by putting forward a call for proposals related to blockchain technology. Based on the communications I have had throughout the Lab, I am confident that interest in such a call would be substantial, and multiple excellent proposals would be submitted. Even if this funding is limited in scope initially, it will make a statement about future research directions for the Lab and lead to future innovations.

4.2 Government funding through traditional calls for proposals from major agencies

As mentioned in the previous sections, government agencies including the NSF and NASA are beginning to issue calls for proposals related to blockchain technology. These funding calls tend to be very focused in scope, and academic institutions have thus far been the main recipients of such funding. Nonetheless, Laboratory staff scientists and researchers with an interest in blockchain technology should be aware that such funding calls are being made and advertise them around the Lab when they appear.

4.3 Industrial partnerships and/or consulting for the blockchain industry

Over the last few years, millions of dollars have been pouring into the blockchain technology sector, and tremendous opportunities exist for various partnerships, such as the $3 million partnership between Block.one and Virginia Tech to develop a novel blockchain curriculum for the Computer Science Department. With its trusted leadership role in computational sciences, ORNL may have significant opportunities to develop such partnerships.

4.4 Mining cryptocurrencies

Most existing blockchain projects use a process known as 'mining' to secure the network and produce new tokens. Miners effectively offer up their computing power to secure the network by solving cryptographic problems, and in exchange they are paid with newly created network tokens or from transaction fees. Since supercomputing resources typically do not run at full capacity, ORNL could use novel dynamic load-balancing algorithms to effectively mine cryptocurrencies with unused computing power to earn financial rewards in exchange for the unused computing power. These funds would effectively be ‘no-strings-attached’, and could be used to fund any number of initiatives in blockchain development.

4.5 Developing a novel blockchain project for the lab

ORNL itself or an individual research group could propose a novel blockchain technology project and use an Initial Coin Offering (ICO) to raise funds to support the project. This funding mechanism has been used successfully by dozens of start-up companies. The way such a proposal would work would be that ORNL researchers would propose a novel cryptocurrency/blockchain application. Then, an Initial Coin Offering would be launched on a platform such as Ethereum or EOS. In this process, placeholder tokens for the proposed network are sold to the public to raise funds to support development of the project. Once the project is ready to be launched, a snapshot of the current distribution of placeholder tokens is taken, and everyone who purchased those can then redeem them for the real utility tokens when the network launches. This would be a viable option if any ORNL researchers have a specific open-source blockchain application in mind.

4.6 Hosting a block producer or witness node for an existing blockchain network

A final potential funding mechanism for the Lab would be to host a trusted ‘witness’ node or block producer for an existing well-respected blockchain network such as the EOS network. In some ways this is similar to mining, but it requires a much lower investment of resources (i.e. much less risk), and it has different associated connotations. Whereas miners are typically seen as competitors trying to earn as much money as possible, ‘witnesses’ or block producers have a vested interest in the network and are frequently the most respected members of the community. Witnesses receive funding for hosting a trusted, secure server for the community as well as for undertaking initiatives that benefit the community, such as the R&D and partnership programs mentioned in this paper.

5. BLOCKCHAIN INSTITUTE AT ORNL

As part of an initial investigation into the potential role of blockchain technology at ORNL, Sean Oesch and myself have co-founded an informal *Blockchain Initiative @ ORNL* with initial funding from EESRD and CSED to investigate possible applications and collaborations involving blockchain technology around the Lab. As part of these discussions, one point became clear: there already exists significant interest in blockchain technology around the Lab in application areas ranging from health data sciences, advanced manufacturing, and energy and environmental sustainability to data provenance and cyber security. Now that this initial investigatory project phase is ending, our intention is to serve as a resource to the Lab with expertise in blockchain technology and to develop collaborations and make connections across the Lab and with academic institutions and industry partners. Given the exponentially growing interest in and adoption of blockchain technology in high-tech sectors, I believe the need will arise for the formation of a formal Blockchain Institute at ORNL to facilitate multi-disciplinary projects across groups and divisions and to establish and maintain external partnerships in blockchain technology. By moving in this direction sooner rather than later, I believe the Lab has the opportunity to establish itself as a leader in this field and to significantly advance the science and impact of blockchain technology.

6. CONCLUSIONS

Nobel prize-winning economist Paul Krugman once famously quipped that he thought the impact of the internet would ultimately be less than that of the fax machine. This is not to disparage the man, but to note that it is notoriously difficult to predict the future, especially with regards to economics and technology. However, based upon this research, I am confident that there are significant application areas for research and development in blockchain technology at ORNL. Of course, since the entire field is so new, a vast number of unknown application areas and technologies are waiting to be discovered. ORNL has the potential to be a leader and pioneer in the field of blockchain technology, especially since the applications of blockchain technology extend across cyber security, bioinformatics, data systems, energy generation and distribution, intelligent/embedded systems, and complex systems. I have detailed the different groups and divisions across the Lab that may benefit from new programs in blockchain technology, I have surveyed the current state of blockchain initiatives at ORNL's core partnership universities, and I have summarized the different potential funding mechanisms that exist to support blockchain research and development, which includes several novel mechanisms unique to this field. By taking an active leadership role in this field and establishing new research programs and collaborations in blockchain technology, the Lab will advance the strategic objectives for excellence in science and technology, laboratory operations and ES&H, and community engagement, and furthermore, these new initiatives will advance the core missions of the DOE.

7. ACKNOWLEDGMENTS

I would like to thank Sean Oesch, Jason Carter, Arvind Ramanathan, and Vladimir Protopopescu for valuable discussions and feedback, which have been tremendously helpful for putting together this white paper, as well as the other members of the informal *Blockchain Initiative @ ORNL* including Adam Malin, Joel Reed, Brian Ray, and Dave Richardson.

8. REFERENCES

[1] AI Impacts. Global computing capacity. Accessed: 2018-3-2.

[2] arsTechnica. Bitcoin's insane energy consumption, explained. Accessed: 2018-3-2.

[3] B@B Student Organization, University of California-Berkeley. Blockchain at Berkeley. Accessed: 2018-3-1.

[4] Coindesk. National Science Foundation to fund blockchain security research. Accessed: 2018-3-2.

[5] Coinify Newsroom. 10 universities that offer blockchain courses. Accessed: 2018-3-1.

[6] Coinmarketcap. Cryptocurrency Market Capitalizations. Accessed: 2018-3-2.

[7] Coinsquare. NASA fund researches the potential of blockchain technology in space. Accessed: 2018-3-2.

[8] Cointelegraph. Blockchain startup receives US government grant for blockchain key management system. Accessed: 2018-3-2.

[9] Cointelegraph. US government to host federal blockchain forum. Accessed: 2018-3-2.

[10] Golem development team. What is Golem? Accessed: 2018-3-2.

[11] Hubertus Breuer. A MicroGrid Grows in Brooklyn. Accessed: 2018-4-7.

[12] Mario L. Major. Energy Giant TEPCO Partners with Blockchain Startup Electron in Decentralization Bid. Accessed: 2018-4-7.

[13] Massachusetts Institute of Technology. blockchain.mit.edu. Accessed: 2018-3-2.

[14] Medicalchain. Own your health. Accessed: 2018-4-11.

[15] Medrec. What is Medrec? Accessed: 2018-4-11.

[16] MIT Technology Review. How blockchain could give us a smarter energy grid. Accessed: 2018-3-2.

[17] Nasdaq. Building the blockchain of genetic data. Accessed: 2018-4-11.

[18] National Science Foundation. Building a secure and compliant cyberinfrastructure for translational research. Accessed: 2018-3-2.

[19] NPR. Aging and unstable, the nation's electrical grid is 'the weakest link'. Accessed: 2018-4-12.

[20] Office of Energy Efficiency and Renewable Energy. Community and Shared Solar. Accessed: 2018-4-7.

[21] Ripple development team. Meet RippleNet. Accessed: 2018-3-2.

[22] SimplyVital Health. A healthcare-safe blockchain to lower costs and empower patients and providers across the globe. Accessed: 2018-4-11.

[23] University of Pittsburgh. Ledger. Accessed: 2018-3-2.

[24] U.S. Department of Energy. Grid Modernization Initiative. Accessed: 2018-4-12.

[25] Virtual Student Federal Service. Blockchain@State. Accessed: 2018-3-2.

[26] Web of Science. Blockchain key word search. Accessed: 2018-3-2.

[27] Wikipedia. Digital currency. Accessed: 2018-3-1.

[28] Wikipedia. Smart contracts. Accessed: 2018-3-2.