COMMONWEALTH OFFICE OF TECHNOLOGY

Blockchain Technology Working Group

Annual Report

December 2024

Blockchain Technology Working Group

Ruth Day*
Chair
Commissioner, Chief Information Officer
Commonwealth Office of Technology

Working Group Membership

Jim Barnhart*
Deputy Commissioner
Commonwealth Office of Technology

David Carter
Commonwealth Office of Technology

Jeb Pinney*
Public Service Commission

Robert Thorne*
Energy and Environment Cabinet

Josh Keats*
Kentucky Office of Homeland Security

James Meece
Louisville Metro Government

Kevin Bass
10XTS

David Brock
Cabinet for Economic Development

Senator Brandon Smith
Kentucky Senate, District 30

Dr. Brian Houillion*
University of the Cumberlands

Christopher Poynter*
Owensboro Municipal Utilities
Designee, Kentucky League of Cities

Chris Hayes*
Kentucky Electric Cooperatives
Designee, Kentucky Rural Electric Cooperatives

Adam Koehler
Reversed Out

Clark Snowden*
Louisville Gas and Electric

John Woeltz
Bluegrass Blockchain

Brian Bates
University of the Cumberlands

Administrative Support

Alice Lawson
Legislative Research Commission

Karen Chrisman
Commonwealth Office of Technology

* Members appointed or designated in compliance with KRS 42.747
++ Members that have retired in the current reporting year.

Blockchain Technology Working Group

Background

The Blockchain Technology Working Group is a collaborative panel of subject matter experts defined in Senate Bill 55, and subsequently codified in Kentucky Revised Statute Chapter 42.747, with the mission to evaluate the feasibility and efficacy of using blockchain technology to enhance the security of and increase protection for the state's critical infrastructure, including but not limited to the electric utility grid, natural gas pipelines, drinking water supply and delivery, wastewater, telecommunications, and emergency services.

The membership of the working group is comprised of nine members defined in KRS 42.747 as well as an array of representatives from state and local government, public utilities, and private sector business who were chosen based on their knowledge and engagement with blockchain technology to ensure a broad depth of knowledge and insight. Through spanning these various government and business sectors, the group can explore and document those opportunities that place the Commonwealth in the forefront in the support and usage of blockchain technology as a tool to empower business in the state.

The group meets on the third Wednesday on a bi-monthly basis. Special meetings may be called when additional collaboration is needed. The Working Group currently conducts open meetings through the state virtualization platform to enhance participation of the geographically diverse membership and to provide open public access to the meetings.

Working Group Mission Statement

The mission of the Kentucky Blockchain Technology Working Group is to evaluate the feasibility and efficacy of using blockchain technology to enhance the Commonwealth by identifying opportunities for the adoption, utilization, and/or regulation of blockchain technology in critical infrastructure, public utilities, telecommunications, emergency services. Through collaborative efforts, with public and private entities, the Working Group will determine through comprehensive research and reporting if blockchain deployment is warranted to demonstrate its value, applicability, and/or efficiency.

Blockchain Technology Working Group

Report Abstract

Blockchain technology is a highly diverse and robust technology that can empower business through the sharing, movement and processing of data or transactions in a highly efficient and secure manner. While the most prevalent use of blockchain technology is digital currency such as Bitcoin, there are significant ways that blockchain technology that can enhance the integrity and security of systems that support critical infrastructure such as transportation, public utilities, healthcare, finances, logistics and emergency services. Through the establishment of the Blockchain Technology Working Group, the Commonwealth is exploring the potential uses of this technology.

This Page Intentionally Left Blank

Blockchain Technology Working Group

Report Summary

Blockchain technology is an innovative mechanism for protecting the confidentiality, integrity, and availability of data. Blockchain is commonly known as a foundation for digital currency, but the technology is well suited for a multitude of purposes where there is a need to share data or track transaction in a highly secure and efficient manner.

The Kentucky State Legislature passed legislation in 2020, codified in KRS 42.747, to establish a working group of subject matter experts to explore this technology. Kentucky Revised Statute 42.747 defined a core group and a clear mission to evaluate the feasibility and efficacy of using blockchain technology to enhance the security of and increase protection for the state's critical infrastructure.

In response to this legislation, the Commonwealth Office of Technology convenes the Blockchain Technology Working Group. Using the legislation to guide the establishment of the initial membership and expanding it to include a range of subject matter experts spanning state and local government, public utilities, private sector business, and academia. Throughout the time that the working group has been in existence additional advisory members have been added bringing a broad spectrum of expertise and experience together to achieve the spirit and intent of this forward-thinking legislation.

Throughout this reporting year, the focus of the group has been to gather information from those in the state and/or nation that are researching or implementing blockchain technology. The final report will expand on the following key points of interest as they relate to critical infrastructure and blockchain technology:

Kentucky Blockchain Technology Working Group

The report will delve into the future composition and scope for the Kentucky Blockchain Technology Working Group based on the research and history of the group since its inception.

Financial Services Sector

The Financial Services Sector includes thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial utilities and services that support these functions. Financial institutions vary widely in size and presence, ranging from some of the world's largest global companies with thousands of employees and many billions of dollars in assets, to community banks and credit unions with a small number of employees serving individual communities. Whether an individual savings account, financial derivatives, credit extended to a large organization, or investments made to a foreign country, these products allow customers to:

1. Deposit funds and make payments to other parties
2. Provide credit and liquidity to customers
3. Invest funds for both long and short periods
4. Transfer financial risks between customers

Government Services and Facilities Sector

The Government Services and Facilities Sector includes a wide variety of buildings, located in the United States and overseas, that are owned or leased by federal, state, local, and tribal governments. Many government facilities are open to the public for business activities, commercial transactions, or recreational activities while others that are not open to the public contain highly sensitive information, materials, processes, and equipment. These facilities include general-use office buildings and special-use military installations, embassies, courthouses, national laboratories, and structures that may house critical equipment, systems, networks, and functions. In addition to physical structures, the sector includes

cyber elements that contribute to the protection of sector assets (e.g., access control systems and closed-circuit television systems) as well as individuals who perform essential functions or possess tactical, operational, or strategic knowledge.

Communication Sector

The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. Presidential Policy Directive 21 identifies the Communications Sector as critical because it provides an "enabling function" across all critical infrastructure sectors. Over the last 25 years, the sector has evolved from predominantly a provider of voice services into a diverse, competitive, and interconnected industry using terrestrial, satellite, and wireless transmission systems. The transmission of these services has become interconnected; satellite, wireless, and wireline providers depend on each other to carry and terminate their traffic, and companies routinely share facilities and technology to ensure interoperability.

Energy Sector

The U.S. energy infrastructure fuels the economy of the 21st century. Without a stable energy supply, health and welfare are threatened, and the U.S. economy cannot function. Presidential Policy Directive 21 identifies the Energy Sector as uniquely critical because it provides an "enabling function" across all critical infrastructure sectors. More than 80 percent of the country's energy infrastructure is owned by the private sector, supplying fuels to the transportation industry, electricity to households and businesses, and other sources of energy that are integral to growth and production across the nation.

Water and Wastewater Systems

Safe drinking water is a prerequisite for protecting public health and all human activity. Properly treated wastewater is vital for preventing disease and protecting the environment. Thus, ensuring the supply of drinking water and wastewater treatment and service is essential to modern life and the nation's economy.

Transportation Systems Sector

The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector Risk Management Agencies for the Transportation Systems Sector. The nation's transportation system quickly, safely, and securely moves people and goods through the country and overseas.

Healthcare and Public Health Sector

The Healthcare and Public Health Sector protects all sectors of the economy from hazards such as terrorism, infectious disease outbreaks, and natural disasters. Because the vast majority of the sector's assets are privately owned and operated, collaboration and information sharing between the public and private sectors is essential to increasing resilience of the nation's Healthcare and Public Health critical infrastructure.

Information Technology Sector

The Information Technology Sector is central to the nation's security, economy, public health, and safety, as businesses, governments, academia, and private citizens are increasingly dependent on its functions. These virtual and distributed functions produce and provide hardware, software, and information technology systems and services, and—in collaboration with the Communications Sector—the Internet. The sector's complex and dynamic environment makes identifying threats and assessing vulnerabilities difficult, requiring these tasks to be addressed in a collaborative and creative fashion.

Regulatory and Legislative Research at a State and National Level
As blockchain technology continues to mature and gain more mainstream adoption, regulations and laws are evolving to address this technology. The report will include an array of updates related to the regulatory and statutory changes that are occurring across the United States.

Blockchain/Emerging Technologies State Initiatives
The report will explore some of the initiatives currently underway in other states.

In the report, the working group expanded on the use cases that align to these areas of critical infrastructure, with the full knowledge that they represent the tip of the proverbial iceberg of what can be achieved through the creative use of blockchain technology. As the technology matures and adoption increases, it is expected that the use cases will evolve and grow exponentially. While these areas of focus are most prevalent today, the working group will continue to maintain monitor the larger picture and explore new avenues that arise.

Lastly, while there are tremendous benefits to blockchain, the benefits do not come without risk. The working group has put thought into identifying those risks. While difficult to quantify, the risk can be considered at a conceptual level while looking at the efficacy of the technology.

In closing, blockchain technology, while in existence in some form beginning in 1982, remains an evolving technology. Over the coming year, the Blockchain Technology Working Group will continue the research needed to identify the more tactical and immediate opportunities for the Commonwealth while maintaining a longer-term search for more strategic opportunities on the horizon. There are recommendations included throughout the detail report, most of which are exploratory in nature, but one overarching recommendation is that the Commonwealth should continue this investment and exploration of blockchain technology to provide real benefit to Commonwealth citizens and to the potential to drive business growth in the state.

Table of Contents

This Page Intentionally Left Blank

Introduction to Blockchain

Blockchain is a highly diverse and secure technology with far reaching potential to enhance and empower business and government. For the purposes of this report, the Blockchain Technology Working Group has adopted the following core definition of blockchain:

> ***'Blockchain** is an encrypted, secure distributed ledger (decentralized database) system that maintains a digital record of transactions. Individual records, called blocks, are linked together in a single list, called a chain. Blockchain is a scalable technology used for recording transactions made with cryptocurrencies, such as Bitcoin, and it has many other applications such as supply chain and logistics monitoring, data sharing, digital voting, real estate and auto title transfer tracking, equities and energy trading, and much more.'*

Blockchain technology is purposely built to protect the integrity and confidentiality of data used in transactional systems. In addition to the security benefits inherent in the technology, there are efficiency and trust gains that help foster data sharing as well as improve the effectiveness and speed of business. Some of these key features are:

- **Decentralized Digital Ledger**
  By design, blockchain does not rely on a single central ledger for the documentation and validation of transactions. That role is shared among the participants in the blockchain enabled system. This allows the system to be highly secure, redundant, and robust. Without a single point of failure and with common knowledge of the transactions across the participants in the blockchain, business continuity and trust in the integrity of transactions can be assured.

- **Industry Standard High Levels of Encryption**
  Industry standard encryption is inherent to blockchain technology and ensures that data in the system is highly protected from exposure or alteration while in transit throughout the system and among the participants in the blockchain.

- **Transactional Trust and Nonrepudiation**
  The design of blockchain imparts an inherent trust between the participants and helps ensure the integrity of the transactions by preventing the interception, alteration, or injection of transactions in the blockchain that cannot be validated by the decentralized ledger. Any alteration of any block of the chain will invalidate the entire blockchain.

- **Low Latency Peer to Peer Transactions**
  Without the requirement that an intermediary server or authority validate the transactions, and with the ability of participants to communicate directly with each other, the flow of data is greatly improved. This simplifies the data flow and removes additional steps in the data path while maintaining the integrity and trust of transactions.

- **Public and Private Options**
  Public blockchains do not rely on a central authority to grant permission to participate in the blockchain to read, write, or proof transactions in the blockchain. One of the most common uses of public blockchain is digital currency such as Bitcoin but can be ideal for any public use system where broad public participation is needed. Private blockchains are restricted networks that require a central authority to grant permission to participants to read and write transactions in the blockchain. This would be most applicable to use cases such as critical infrastructure where the security and efficiency of blockchain is needed but requires high levels of control over who can participate in the blockchain.

Blockchain Potential Use Cases and Areas of Interest

The efficiency and applicability of blockchain can be realized across any number of business and government sectors. Many public and private sector entities are exploring the efficacy of blockchain. The Commonwealth has taken the bold first step in establishing the Blockchain Technology Working Group setting a path to explore the opportunities that this technology may offer. Some of these possible opportunities are:

KENTUCKY BLOCKCHAIN TECHNOLOGY WORKING GROUP

Representatives of the KBTWG, presented information to the Interim Joint Committee on Natural Resources and Energy on November 16, 2023. Part of this testimony was that the statutory scope and composition of the Working Group needed to be amended based on the experience of the group since inception. The initial scope primarily focused on public utilities and infrastructure. This scope meant that an energy focused Working Group was created. However, the current nature of blockchain technology is focused within the financial sector. While there are some opportunities with blockchain based energy credits, the vast current implementation of the technology is in other areas.

The expansion of score would lead to the necessity for different members to be added to the statutory list of members. For example, with the financial aspect of the technology the Commissioner (or designee) of the Department of Financial Institutions would be a needed addition. Also, perhaps the Public Protection Secretary (or designee).

FINANCIAL SERVICES SECTOR

In 2024, blockchain technology and cryptocurrencies have profoundly impacted the financial industry, driving innovation, enhancing transparency, and challenging traditional banking practices. This report examines key developments, trends, and implications through specific examples that illustrate the transformative effects of these technologies on financial institutions, regulatory environments, and consumer behavior.

Introduction

The financial sector has traditionally relied on centralized systems and intermediaries. However, the introduction of blockchain technology and cryptocurrencies is shifting this paradigm towards decentralization and efficiency. This report evaluates the current landscape and future potential of these technologies through real-world examples.

Key Developments in Blockchain Technology

Mainstream Adoption

In 2024, major financial institutions like JPMorgan Chase have integrated blockchain technology into their operations. For instance, JPMorgan's Onyx platform facilitates real-time cross-border payments using blockchain, significantly reducing transaction costs and settlement times.

Interoperability Solutions

Interledger Protocol is gaining traction as a solution for enabling different blockchain networks to communicate seamlessly. Institutions like Ripple are utilizing this protocol to allow various cryptocurrencies and traditional currencies to be exchanged more fluidly, enhancing the efficiency of global transactions.

Enhanced Security and Privacy

The use of zero-knowledge proofs has increased among financial institutions. For example, Zcash and Monero have demonstrated how privacy-focused blockchains can secure transaction data. Banks are looking into similar cryptographic methods to protect sensitive customer information while still ensuring regulatory compliance.

Cryptocurrency Trends

Institutional Investment

Prominent institutional investments in cryptocurrencies have surged in 2024, with firms like BlackRock entering the space. BlackRock's launch of a Bitcoin ETF has increased legitimacy in the market, attracting significant capital from both retail and institutional investors.

Central Bank Digital Currencies (CBDCs)

Countries like China and Sweden have made significant strides with their CBDCs. China's Digital Yuan is being used in real transactions, showcasing its potential to enhance payment efficiency and reduce transaction costs. Sweden's e-krona pilot program aims to modernize its payment infrastructure and promote financial inclusion.

Regulatory Developments

The regulatory landscape for cryptocurrencies and blockchain technology has significantly evolved in 2024, marked by increased clarity, proactive measures, and international collaboration. Governments and regulatory bodies worldwide are establishing frameworks to ensure consumer protection, prevent fraud, and foster innovation in the digital asset space. Below are key aspects of these developments:

Comprehensive Frameworks

Countries like the United States and the European Union have made strides in creating comprehensive regulatory frameworks for cryptocurrencies.

- **United States**: The **U.S. Securities and Exchange Commission (SEC)** has introduced guidelines that classify certain cryptocurrencies as securities. This has implications for how exchanges operate and how tokens can be marketed. In 2024, the SEC launched the **Crypto Regulation Task Force**, aimed at enhancing cooperation between federal and state regulators. Notably, **Coinbase** adapted its business model to comply with these regulations, increasing transparency and building consumer trust.
- **European Union**: The **Markets in Crypto-Assets (MiCA)** regulation, set to be implemented in 2024, aims to standardize cryptocurrency regulation across EU member states. MiCA focuses on consumer protection, market integrity, and financial stability, providing a legal framework for crypto-assets and service providers. This regulation is expected to facilitate innovation while ensuring that consumers are adequately protected.

Focus on Consumer Protection
Consumer protection has become a primary concern for regulators as the cryptocurrency market continues to mature.

- **Financial Conduct Authority (FCA) in the UK**: The FCA has ramped up its efforts to regulate cryptocurrency firms, mandating that companies register with the agency and adhere to anti-money laundering (AML) and counter-terrorism financing (CTF) measures. The FCA has also launched campaigns to educate consumers about the risks associated with investing in cryptocurrencies, emphasizing the need for informed decision-making.
- **Australia's ASIC**: The Australian Securities and Investments Commission (ASIC) has implemented stricter rules for cryptocurrency exchanges, requiring them to disclose information about the products they offer, including risks and fees. This initiative aims to enhance transparency and consumer awareness in the rapidly evolving crypto space.

International Collaboration
As cryptocurrencies transcend borders, regulatory bodies are increasingly collaborating internationally to create cohesive standards and regulations.

- **Financial Action Task Force (FATF)**: The FATF continues to update its guidelines for crypto assets, pushing countries to implement regulations that prevent money laundering and terrorism financing. In 2024, the FATF emphasized the importance of regulating DeFi platforms, urging member countries to include these in their AML frameworks.
- **BIS and Central Bank Collaborations**: The **Bank for International Settlements (BIS)** is facilitating discussions among central banks worldwide to share best practices on regulating CBDCs and cryptocurrencies. These collaborative efforts are crucial as countries explore the integration of digital currencies into their monetary systems.

Regulatory Sandboxes
Many countries are adopting regulatory sandboxes to foster innovation while ensuring consumer protection.

- **United Kingdom**: The FCA's regulatory sandbox allows fintech and cryptocurrency companies to test their products in a controlled environment, providing feedback from regulators without the immediate burden of compliance. This initiative has led to successful projects that enhance financial services while maintaining regulatory oversight.
- **Singapore**: The **Monetary Authority of Singapore (MAS)** operates a similar sandbox that encourages innovation in the fintech sector, including blockchain projects. By allowing startups to trial their technologies, MAS aims to balance fostering innovation with the need for regulatory compliance.

Impact of Regulatory Developments

These regulatory advancements have several implications for the cryptocurrency market and financial institutions:

- **Increased Legitimacy**: As regulations become more robust, cryptocurrencies are gaining legitimacy as a viable asset class. Institutional investors are more likely to engage with the market, as seen with BlackRock's Bitcoin ETF launch in 2024.
- **Market Stability**: A clearer regulatory framework helps mitigate risks associated with fraud and market manipulation, contributing to a more stable market environment.
- **Encouragement of Innovation**: While regulation imposes certain constraints, it also encourages innovation by providing a clear pathway for compliance. Companies that navigate these regulations effectively can leverage new opportunities in the crypto space.

Conclusion

In 2024, regulatory developments in the cryptocurrency and blockchain landscape reflect a growing recognition of the need for oversight and consumer protection. By establishing comprehensive frameworks, focusing on consumer awareness, fostering international collaboration, and promoting regulatory sandboxes, authorities are paving the way for a more secure and innovative financial ecosystem. As these regulations continue to evolve, they will play a crucial role in shaping the future of cryptocurrencies and their integration into mainstream finance.

Impact on Financial Institutions

Disintermediation

Platforms like Aave and Compound are leading the way in decentralized finance (DeFi), allowing users to lend and borrow cryptocurrencies without intermediaries. This trend is challenging traditional banking roles and providing consumers with alternatives to conventional financial services.

Cost Reduction

Financial institutions have experienced significant cost savings through blockchain integration. For example, Santander has reduced its transaction costs by 40% using blockchain technology for international payments, improving profitability and operational efficiency.

Enhanced Customer Experience

Gemini, a cryptocurrency exchange, emphasizes user experience by allowing customers to manage their digital assets easily. Enhanced transparency and reduced friction in transactions have resulted in higher customer satisfaction and retention rates.

Challenges and Considerations

Regulatory Uncertainty

Despite advancements, regulatory challenges remain. For instance, the fluctuating stance of the SEC on cryptocurrency classification creates uncertainty for financial institutions, affecting their strategies in the crypto market.

Security Risks
Cyberattacks on platforms like Binance in 2023 highlighted the ongoing security risks in the cryptocurrency space. This incident underscored the need for robust security measures as financial institutions increasingly engage with blockchain technology.

Environmental Concerns
The environmental impact of cryptocurrency mining has prompted institutions like Tesla and Square to reassess their investments in Bitcoin. Initiatives to explore sustainable mining practices, such as the use of renewable energy sources, are becoming critical in addressing these concerns.

Future Outlook
The financial industry is poised for continued transformation through blockchain and cryptocurrencies. Key trends to watch include:

- Integration of AI and Blockchain: Companies like Chainalysis are combining AI with blockchain analytics to enhance fraud detection and risk assessment, streamlining compliance for financial institutions.
- Growth of DeFi: Platforms like Uniswap and SushiSwap are expected to continue expanding, offering innovative financial services that bypass traditional banking systems, thus reshaping consumer access to finance.
- Expansion of CBDCs: As more countries explore CBDCs, their influence on monetary policy and financial stability will become increasingly significant. The European Central Bank is also conducting research on the digital euro, which may soon enter pilot phases.

Conclusion
In 2024, blockchain technology and cryptocurrencies have firmly established themselves as transformative forces in the financial industry. As adoption increases and regulatory clarity improves, these technologies are set to redefine the landscape of financial services, presenting both challenges and opportunities for institutions and consumers alike.

GOVERNMENT SERVICES AND FACILITIES SECTOR

The Government Services and Facilities Sector includes a wide variety of buildings, located in the United States and overseas, that are owned or leased by federal, state, local, and tribal governments. Many government facilities are open to the public for business activities, commercial transactions, or recreational activities while others that are not open to the public contain highly sensitive information, materials, processes, and equipment. These facilities include general-use office buildings and special-use military installations, embassies, courthouses, national laboratories, and structures that may house critical equipment, systems, networks, and functions. In addition to physical structures, the sector includes cyber elements that contribute to the protection of sector assets (e.g., access control systems and closed-circuit television systems) as well as individuals who perform essential functions or possess tactical, operational, or strategic knowledge.

While this definition speaks primarily to physical security, the associated National Infrastructure Protection Plan extends this to areas of cybersecurity that ensures the security and integrity of government operations. This is where the leveraging of blockchain technology could make a meaningful difference. The following are some examples of this potential.

Contracts

Advancement in electronic technology led to the ability to execute contracts without needing to be present. Previously, the execution of a contract required the signatories of a contract be present and physically sign the contract document. This changed over the last decade with online services such as DocuSign and Adobe Acrobat. These electronic systems allow parties to a contract to sign documents without being physically present.

Though these platforms allowed the execution of contracts to become more efficient there are some basic weaknesses in these systems. The primary weakness is the guarantee of authenticity or validity of the signature. The common process is for the contract documents to be electronically forwarded or supplied to the parties. This is completed through a link provided in an email. The recipient follows the link to the documents that are hosted on a central server. The recipient reviews the documents and then when prepared to sign acknowledges their agreement to the electronic signature process and then attach an electronic signature. The issues in this process are that there is no guarantee the signatory is the actual party intended for the agreement, as the link is usually emailed through unencrypted email. The second issue is that all the signed documents are maintained in a central database that is vulnerable to cyber-attack.

A system that enables blockchain as part of the signature process allows the documents to be maintained in a decentralized system reducing the probability of cyber-attack. Additionally, blockchain will validate the identity of the signer. Blockchain provides a key that is unique to the individual allowing assurance that the signatory to the contract is the party intended.

Accounting/Auditing

Blockchain is widely considered to be one of the most significant innovations to accounting since the invention of the double-entry ledger system. The double-entry ledger has been the basis for accounting practices for roughly 500 years. The basic nature of double-entry accounting is that all credits and debits are recorded in a single ledger. Though this system may work effectively for the parties involved in a specific transaction it provides no transparency to other interested parties such as investors, auditors, taxing authorities, financial institutions, or other similar entities. The maintenance of a single ledger by the individual or corporation leads to many issues including criminal fraud. The idiom “cook the books” long ago entered into common slang. Recent financial crimes in large corporations and even government entities provide testimony to the potential for manipulation.

The nature of blockchain creates a transparent and immutable transaction trail that has been identified as “triple-entry accounting”. This creates an incorruptible link between the transactions recorded in a double entry ensuring the integrity of the transaction record. The only solution to identifying manual errors or fraud in the double-entry system was through costly and time-consuming audits. Even with full, comprehensive audits, intentional malfeasance has gone undiscovered. The implementation of blockchain in the accounting system of corporations, individuals and governments provides a transparent record of transactions that are nearly impermeable to fraud. This reduces the necessity for intensive audits leading to efficiencies and cost-savings in the systems, especially for budget restricted governments.

Recommendation 1.2: The Kentucky Auditor's Office may benefit from the exploration of the benefits of implementing blockchain technology in their auditing processes, especially those that occur annually.

Rationale: The immutable audit trail would allow the Auditor's office to better automate and accommodate the auditing process for the government agencies it is required to audit every year. From the budgeting process through the audit process, a single system built on blockchain could provide significant cost and time savings in completing these regular audits allowing for concentration to be focused on special audits.

Legal Records and Documents

State and local governments are a vast depository of legal records and documents. These governments or associated agencies maintain numerous records including but not limited to state issued IDs, property records and land deeds, motor vehicle registrations, driving records, voter registrations, voting records, occupational and business tax records, corporate and non-profit entity registrations, criminal records, professional and occupational licensing records, alcoholic beverage licenses, gaming licenses, and a myriad of other records and documents. These records, when maintained electronically, are usually located on a local server at the county clerk's office, or a city hall, county courthouse or the state government servers. This central repository is vulnerable to a concentrated cyber-attack. Also, electronic records may be susceptible to loss of information or data through the potential shut down or corruption of the central server. Sharing of these records and documents should be completed through either providing access directly to the database or providing a copy forwarded through an electronic means such as email.

Blockchain provides the opportunity to manage, transfer and store these legal and governmental documents within a distributed ledger addressing the risks of centralized storage as well as maintaining the custody of the records and ensuring the integrity and accuracy of the electronic documents. As a case study, the nation of Dubai, through the Department of Economic Development, initiates all business registrations, business licenses, and other business-related documents entirely by blockchain.

Recommendation 1.3: Leveraging blockchain technologies in creating various electronic records may be a viable use case among government agencies that maintain this records. State agencies may benefit from further exploration of opportunities for blockchain technology to enhance the security and integrity of these records maintenance processes and systems.

Recommendation 1.4: The Kentucky Secretary of State, as custodian of both elections and business filings, should research the benefits of blockchain in the issuance and/or management of these records to ensure the integrity and accuracy of these crucial records.

Rationale: The shift to alternate methods of voting during the Covid-19 pandemic has demonstrated that methods other than in-person voting can be provided. Utilization of blockchain, while not the panacea to cure potential voting issues, could be a large step forward in ensuring that election fraud is impossible. Business registrations and licenses could also be maintained securely and efficiently.

Recommendation 1.5: The Commonwealth of Kentucky should continue to research opportunities that may benefit from blockchain technology in records and document management systems in the state government. To ensure interoperability blockchain will need to be implemented in an organized, centralized and efficient manner.

Licensing

Opportunity may exist in sharing of professional licensure data through a solution to promote portability of licenses which could be achieved through Interstate Compacts. These compacts are agreements between states that would allow compact participants to recognize licenses from other states. The portability only applies to the states that are signatories to the charter. The establishment and maintenance of charters are both costly and legislatively complex. In addition, the information for the licensees is either maintained by the individual states or in some cases may be maintained in a central location managed by an entity that oversees the operations of the compact. In either case, this provides the opportunity for conflicting data, in the case of individual state-maintained data, or vulnerability to hacking if managed in a central database.

A blockchain system removes the centralized database and replaces it with a distributed ledger system which would allow all the states to have access to the same information on licensees and would significantly reduce the risk of corruption or theft of data. The licensee would have responsibility for the maintenance of their license and would allow access to the desired states in which they wish to practice. With a distributed ledger, the states would have access to all licensees that may wish to practice in their states and would be able to immediately share information with other states if there is a change in the licensee status due to an event such as failure to complete continuing education, disciplinary actions, investigations, escrow or any other event that could impact public protection and the licensee's ability to practice.

Recommendation 1.6: The Department for Professional Licensing, the Public Protection Cabinet (PPC) and the Commonwealth Office of Technology (COT) may benefit from researching the opportunity provided by incorporating blockchain technology into Kentucky's licensing systems.

PUBLIC UTILITIES

Modern public utility infrastructure is highly complex, automated, and distributed across wide areas. Ensuring the integrity of communications across this infrastructure is paramount to maintaining critical utility services for citizens and businesses of the Commonwealth. Public utilities spans multiple critical infrastructure sectors, with the following three sectors being the most applicable:

- **Communication Sector**
  The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. Presidential Policy Directive 21 identifies the Communications Sector as critical because it provides an "enabling function" across all critical infrastructure sectors. Over the last 25 years, the sector has evolved from predominantly a provider of voice services into a diverse, competitive, and interconnected industry using terrestrial, satellite, and wireless transmission systems. The transmission of these services has become interconnected; satellite, wireless, and wireline providers depend on each other to carry and terminate their traffic, and companies routinely share facilities and technology to ensure interoperability.

- **Energy Sector**
  The U.S. energy infrastructure fuels the economy of the 21st century. Without a stable energy supply, health and welfare are threatened, and the U.S. economy cannot function. Presidential Policy Directive 21 identifies the Energy Sector as uniquely critical because it provides an "enabling function" across all critical infrastructure sectors. More than 80 percent of the country's energy infrastructure is owned by the private sector, supplying fuels to the transportation industry, electricity to households and businesses, and other sources of energy that are integral to growth and production across the nation.

- ***Water and Wastewater Systems***
  Safe drinking water is a prerequisite for protecting public health and all human activity. Properly treated wastewater is vital for preventing disease and protecting the environment. Thus, ensuring the supply of drinking water and wastewater treatment and service is essential to modern life and the nation's economy.

While it is difficult to predict the impact of Blockchain technology on utilities at this early stage there are some potential implications for financial transactions, energy generation and distribution, renewable energy, infrastructure management, enhanced customer service, and service delivery. It's important to note that energy generation and distribution is heavily regulated by the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), and regional organizations such as the Southeastern Electric Reliability Corporation, therefore any integration of Blockchain technology in this process will need to be endorsed by these and other local regulatory organizations.

Financial transactions could utilize secure, innovative solutions that are automatically triggered by specific requirements being met between buyers and sellers at all levels of the supply chain. Retail consumers could benefit from timely and secure payment transactions. Utilities could also utilize similar transactions to simplify financial exchanges for mutual aid and shared resources. Energy generation and distribution could be improved by incorporating Smart Grid functionality.

Tokens referred to as "Renewable Energy Credits" or RECs are a method of monetizing renewable energy. Currently these tokens are thoroughly audited to ensure the token is only used once. Blockchain enabled RECs would be more efficient and eliminate the need for audits. As carbon emission tracking becomes more common, Blockchain could usher in an acceptable mechanism to track these emissions. The tracking system could be a unified platform offering a single solution for calculations.

Infrastructure management could benefit from far more detailed tracking and easier access to component information such as manufacturer, date and time manufactured, shipping details, time of installation, service life, load capabilities, and so much more. When coupled with augmented reality the real-time benefits of this information are almost inconceivable. Blockchain technology could be incorporated into Automated Metering Infrastructure (AMI) processes that allow customers to access real-time usage data, flexible billing options, automatic disconnection/reconnection functionality, and reliable service transactions.

TRANSPORTATION SYSTEMS SECTOR

The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector Risk Management Agencies for the Transportation Systems Sector. The nation's transportation system quickly, safely, and securely moves people and goods through the country and overseas.

Logistics and Supply Chain Management

Kentucky is geographically positioned as a central point for logistics across the eastern United States, making it an ideal location for businesses looking to expand. The state is recognized as the #1 location in the U.S. for population served within a one-day drive (Source: Claritas) and has a GRADE A rating in Logistics Industry Health (Source: Manufacturing Scorecard 2019, Ball State Center for Business and Economic Research) 1. Kentucky sits within 600 miles of 65% of the U.S. population, personal income, and manufacturing establishments, making it a logistics powerhouse 2.

The Cincinnati/Northern Kentucky International Airport (CVG) is a critical asset, ranked as the 8th largest cargo airport in North America and home to the Amazon Air hub and DHL's North American super-hub 3. Additionally, two Class I railroads (CSX and Norfolk Southern) cross the region, and the Port of Cincinnati and Northern Kentucky is the busiest inland river port in the U.S. (US Army Corps of Engineers Navigation Data Center, 2016) 4. These factors, combined with the rise of blockchain technology, position the region as an increasingly appealing option for businesses aiming to innovate and scale.

Blockchain and Modern Logistics

Modern logistics involves the coordination of multiple origin and destination points, creating complex communication flows that must be secure, validated, and timely. Blockchain is a crucial technological upgrade that can streamline these processes. By integrating blockchain with big data, IoT, smart contracts, and artificial intelligence, companies can reduce costly errors, speed up delivery times, and lower the overall costs that burden large, centralized logistics platforms 5.

Blockchain also ensures greater transparency and security by providing an immutable, shared ledger accessible to all parties involved in the supply chain. These qualities make it a key driver of innovation in logistics, increasing efficiency and trust between stakeholders 6.

Industry-Wide Blockchain Adoption

The logistics industry has been steadily investing in blockchain technology. The establishment of the **Blockchain in Transportation Alliance (BiTA)** in 2017 is a testament to the industry's commitment to setting blockchain standards for the global supply chain. Members of BiTA include leading companies such as UPS, FedEx, Delta Airlines, and Union Pacific Railroad, all of which are pushing the boundaries of blockchain integration in logistics 7.

Key examples of blockchain innovations in logistics include:

- **Maersk and IBM – TradeLens**
  TradeLens is a blockchain-based platform developed to increase efficiency and security in the global supply chain. It provides a tamper-proof record of all transactions, accessible to all involved parties, and is already adopted by major shipping companies worldwide 8.

- **Walmart**
  Walmart uses blockchain to trace the origin of food products in its supply chain. This system helps Walmart quickly identify the source of food safety issues, enabling faster product recalls and increasing transparency for consumers 9.
- **UPS**
  UPS has implemented blockchain to track shipments across its global network. The system provides real-time updates on the status of shipments and creates an immutable record of all transactions, improving transparency and customer satisfaction 10.
- **FedEx**
  FedEx is piloting blockchain to improve freight industry processes by creating a digital, transparent trail for shipments from pickup to delivery 11.

Attracting Blockchain-Based Startups to Kentucky
Kentucky's logistics infrastructure, combined with state-backed incentives and initiatives, creates a fertile environment for blockchain-driven startups in the supply chain sector. Programs like **KY Innovation** support entrepreneurs with capital, mentoring, and other resources necessary for scaling innovative solutions. Kentucky also ranks high for business affordability, with lower-than-average utility costs and a favorable tax environment, making it easier for startups to establish and grow 12.

Key Advantages for Startups in Kentucky:

- **Strategic Location**: Kentucky's location within a day's drive of most U.S. markets reduces logistical costs and time to market for startups 13.
- **Established Logistics Hub**: The presence of Amazon, UPS, and DHL's major hubs offers partnership opportunities and best-practice sharing for startups 14.
- **Support for Innovation**: The state's KY Innovation office and other initiatives provide vital support for emerging companies 15.
- **Growing Tech Ecosystem**: The expanding network of startups and accelerators in Kentucky encourages collaboration and fosters a dynamic environment for innovation 16.
-

By leveraging Kentucky's unique geographic and logistical advantages, along with state-backed support, startups focused on blockchain solutions for the logistics industry are well-positioned to thrive in this ecosystem.

Citations:

1. Claritas, Manufacturing Scorecard 2019, Ball State Center for Business and Economic Research ↩
2. Kentucky Cabinet for Economic Development ↩
3. Expansion Solutions Magazine ↩
4. US Army Corps of Engineers Navigation Data Center ↩
5. Blockchain in Transportation Alliance (BiTA) ↩
6. Site Selection Magazine ↩
7. BiTA Standards Council ↩
8. TradeLens ↩
9. Walmart Blockchain Initiative ↩
10. UPS Blockchain System ↩
11. FedEx Blockchain Pilots ↩
12. KY Innovation Programs for Startups ↩
13. Strategic Location: Kentucky Economic Development ↩
14. Logistics Hub: Expansion Solutions Magazine ↩
15. KY Innovation Office ↩
16. Tech Ecosystem: Site Selection Magazine ↩

HEALTHCARE AND PUBLIC HEALTH SECTOR

The Healthcare and Public Health Sector protects all sectors of the economy from hazards such as terrorism, infectious disease outbreaks, and natural disasters. Because the vast majority of the sector's assets are privately owned and operated, collaboration and information sharing between the public and private sectors is essential to increasing resilience of the nation's Healthcare and Public Health critical infrastructure.

The Commonwealth is home to some of the most progressive and nationally leading healthcare providers and institutions in the country. Anyone seeking treatment in the Kentucky healthcare system, beyond routine health concerns, will experience the disparate nature of a service delivery that includes general practitioners, specialists, hospitals, and more.

The effective and efficient flow of critical treatment data among these providers, typically in disparate institutions, could greatly improve the quality of service and the speed the critical health concerns can be treated. This data is extremely sensitive, profoundly critical to human safety, and heavily regulated by standards such as the Health Insurance Portability and Accountability Act (HIPAA). Blockchain has the potential to rapidly share this critical data with the highest level of protection, while also ensuring patient privacy and compliance with regulatory standards.

Healthcare, with the direct responsibility and commitment to health and human safety, makes tremendous investments in the technology that aids in the diagnosis and treatment of health issues but historically is cautious when it comes to operational technology changes.

- Due to the critical nature of healthcare where speed and consistency of service delivery is critical to human safety, healthcare institutions cannot experience downtime or degradation of services that may be the result of deploying cutting edge technologies such as blockchain. Additional standardization and maturation of the technology is needed to instill the confidence needed to ease these concerns.

- Cost to re-engineer is high. Healthcare institutions leverage high cost and complex technology solutions. Due to the complexity involved with building on Blockchain technology, the transition to such system would require the redesign of the existing architecture and considerable development costs.

While the concerns of the healthcare industry are certainly valid, blockchain is still well positioned to be transformative technology and can have a tremendously positive impact on the delivery of critical health care services.

There still are areas of opportunity as follows:

Data Analytics

The Centers for Disease Control (CDC) is currently exploring the opportunities for using blockchain technology to monitor diseases at a national level. Referred to as Public Health Surveillance by the CDC, there is significant focus on utilizing emerging technologies such an Artificial Intelligence (AI) and Blockchain to foster reliable, secure, and efficient mechanisms to share health data at a national level. Empowering local health officials with actionable real time national level data and analytics could greatly enhance the ability to react to events like were experienced in 2020/2021 during the global pandemic. Through the CDC Office of the Deputy Director for Public Health Science and Surveillance, the CDC is promoting the use of modernized technologies such as blockchain. The Kentucky Blockchain Technology Working Group will continue to monitor opportunities within our state, and at a national level, for potential blockchain opportunities.

Medical Research

The Commonwealth of Kentucky is home to some of the leading research and teaching hospitals in the country. With key healthcare leaders, such as University of Kentucky Healthcare, University of Louisville Health, Baptist Health, Norton Healthcare, and Jewish Hospital to name a few, there is a significant capacity already in place in the state. Finding those opportunities to enhance the existing capabilities in the state with technology advancements such as blockchain can position Kentucky to draw additional healthcare business to the state and help move the Commonwealth to the forefront of the healthcare industry.

While there have been no significant changes observed by the KBTWG in the current reporting year, research proposals published in the National Institute of Health, National Library of Medicine demonstrates continued interest in Blockchain Technology to aid in efficient and secure data sharing at a global level.

- ***A systematic review of privacy-preserving methods deployed with blockchain and federated learning for the telemedicine***

  Authors: Madhuri Hiwale, Rahee Walambe, Vidyasagar Potdar, Ketan Kotecha
  Document Link: https://pmc.ncbi.nlm.nih.gov/articles/PMC10160179/

  Abstract

  The unexpected and rapid spread of the COVID-19 pandemic has amplified the acceptance of remote healthcare systems such as telemedicine. Telemedicine effectively provides remote communication, better treatment recommendation, and personalized treatment on demand. It has emerged as the possible future of medicine. From a privacy perspective, secure storage, preservation, and controlled access to health data with consent are the main challenges to the effective deployment of telemedicine. It is paramount to fully overcome these challenges to integrate the telemedicine system into healthcare. In this regard, emerging technologies such as blockchain and federated learning have enormous potential to strengthen the telemedicine system. These technologies help enhance the overall healthcare standard when applied in an integrated way. The primary aim

  of this study is to perform a systematic literature review of previous research on privacy-preserving methods deployed with blockchain and federated learning for telemedicine. This study provides an in-depth qualitative analysis of relevant studies based on the architecture, privacy mechanisms, and machine learning methods used for data storage, access, and analytics. The survey allows the integration of blockchain and federated learning technologies with suitable privacy techniques to design a secure, trustworthy, and accurate telemedicine model with a privacy guarantee.

INFORMATION TECHNOLOGY SECTOR

The Information Technology Sector is central to the nation's security, economy, public health, and safety, as businesses, governments, academia, and private citizens are increasingly dependent on its functions. These virtual and distributed functions produce and provide hardware, software, and information technology systems and services, and—in collaboration with the Communications Sector—the Internet. The sector's complex and dynamic environment makes identifying threats and assessing vulnerabilities difficult, requiring these tasks to be addressed in a collaborative and creative fashion.

Decentralized Physical Infrastructure Network

Decentralized Physical Infrastructure Networks (DePIN) represent a transformative approach to infrastructure development, leveraging blockchain technology and decentralized systems to enhance efficiency, transparency, and community involvement. This report explores the evolution of DePIN, its potential applications across various industries, and specific examples demonstrating its impact on state government initiatives and local economies.

Introduction

DePIN refers to a decentralized framework for managing physical infrastructure, such as transportation, utilities, and public services. By integrating blockchain technology, DePIN enables direct participation from stakeholders, enhances data security, and reduces reliance on centralized authorities. This report provides an overview of DePIN's development and its implications for industry and state governments.

How DePIN Works

Decentralized Physical Infrastructure Networks (DePIN) operate through a combination of decentralized technologies, community participation, and innovative management systems. Here's a breakdown of how DePIN functions:

1. **Decentralization Mechanism**
   - **Distributed Control**: In a DePIN, control is spread across various stakeholders instead of being held by a central authority. This distribution is facilitated through networks of participants who collectively manage infrastructure.
   - **Peer-to-Peer Interaction**: Participants can interact directly with one another, whether they are consumers, producers, or service providers, eliminating the need for intermediaries.

2. **Blockchain Technology**
   - **Immutable Ledger**: Blockchain serves as a decentralized, transparent ledger that records all transactions and interactions within the network. This ensures data integrity and security.
   - **Transaction Tracking**: Each transaction related to physical infrastructure—such as energy production, usage data, or maintenance records—can be traced in real-time, providing accountability.

3. **Tokenization of Assets**
   - **Digital Representation**: Physical assets (like solar panels, electric vehicles, or communication towers) are represented as digital tokens on a blockchain. This allows for fractional ownership and easier trading.
   - **Incentivization**: Tokenization can include incentives for participants, such as rewards for contributing to the infrastructure or for utilizing resources efficiently.

4. **Smart Contracts**
   - **Automated Agreements**: Smart contracts are self-executing agreements coded on the blockchain that automatically enforce terms when conditions are met. For instance, a smart contract might release payment for energy produced once it is consumed.
   - **Efficiency and Trust**: These contracts enhance trust among participants by reducing the need for intermediaries and minimizing disputes through clear, automated rules.

5. **Community Participation**
   - **Stakeholder Engagement**: Local communities have a significant role in the decision-making process. They can contribute to planning, funding, and managing infrastructure projects, ensuring that their needs are met.
   - **Feedback Mechanisms**: DePIN can implement feedback loops where community input directly influences project adaptations and improvements.

6. **Real-Time Data Sharing**
   - **Data Collection and Analysis**: Sensors and IoT devices can collect real-time data related to infrastructure performance, usage patterns, and environmental conditions. This data is shared across the network.
   - **Optimized Operations**: Analyzing this data allows for better decision-making, resource allocation, and maintenance scheduling, leading to more efficient operations.

7. **Interoperability**
   - **Collaborative Networks**: DePINs can interconnect with other decentralized networks, enabling the sharing of resources and services across different sectors (e.g., energy sharing between communities).
   - **Standard Protocols**: Establishing standard protocols for interaction helps ensure that different DePINs can communicate and operate together seamlessly.

Example Scenario
Decentralized Energy Grid:

1. **Participants**: Homeowners with solar panels, consumers, and local energy providers.
2. **Tokenization**: Homeowners tokenizing their excess energy production, allowing them to sell it to neighbors.
3. **Smart Contracts**: Automatically executing transactions when energy is consumed, ensuring timely payments.
4. **Data Sharing**: Continuous monitoring of energy production and consumption data to optimize usage patterns and reduce waste.
5. **Community Involvement**: Residents participating in decision-making about local energy projects and infrastructure upgrades.

Key Developments in DePIN

Conceptual Framework
The concept of DePIN has evolved from the rise of decentralized finance (DeFi) and blockchain technology. Key characteristics of DePIN include:

- **Decentralization**: Empowering local communities and stakeholders to participate in infrastructure decision-making.
- **Transparency**: Utilizing blockchain for immutable record-keeping and tracking of resources.
- **Incentivization**: Implementing tokenomics to reward participants for contributing to the network.
- **Blockchain Technology**: Many DePIN projects utilize blockchain technology to provide transparency, security, and immutability. Blockchain can record transactions related to physical assets, allowing for real-time tracking and verification without the need for intermediaries.

- **Tokenization**: Physical assets within a DePIN can be tokenized, meaning they are represented as digital tokens on a blockchain. This allows for fractional ownership, enabling more participants to invest in and benefit from physical infrastructure.
- **Smart Contracts**: Smart contracts automate processes and agreements within the network, reducing the need for manual oversight and facilitating trustless interactions. For example, smart contracts can automatically execute payments when specific conditions related to infrastructure usage are met.
- **Community Participation**: DePIN encourages community engagement by allowing local stakeholders to contribute to the planning, management, and operation of physical infrastructure. This participatory model ensures that the infrastructure meets the needs of the community it serves.

Technological Advancements
Recent advancements in blockchain technology, such as the development of smart contracts and decentralized applications (dApps), have made the implementation of DePIN feasible. These technologies allow for automated processes, reducing bureaucracy and enhancing operational efficiency.

Growing Interest and Investment
Interest in DePIN has surged, with significant investments from both public and private sectors. Initiatives such as **The Graph** and **Helium** are pioneering projects aimed at building decentralized networks that support physical infrastructure.

Potential Applications of DePIN

Transportation Networks
DePIN can transform transportation systems by creating decentralized ride-sharing and public transport networks.

- **Example**: **RideShare Protocol** utilizes a decentralized platform for ride-sharing services. By connecting drivers and riders directly through blockchain, the platform minimizes fees, enhances transparency, and allows users to earn tokens for contributing to the network.

Energy Infrastructure
Decentralized energy grids can enhance energy distribution and management.

- **Example**: **PowerLedger** is a blockchain-based platform that enables peer-to-peer energy trading. Households with solar panels can sell excess energy directly to their neighbors, promoting local energy independence and reducing reliance on centralized utilities.

Supply Chain Management
DePIN can enhance transparency and efficiency in supply chains.

- **Example**: **VeChain** leverages blockchain to improve traceability in supply chains. Businesses can track products from origin to delivery, ensuring authenticity and reducing fraud. This is particularly beneficial in industries like food and pharmaceuticals, where safety is paramount.

Smart Cities
DePIN can play a crucial role in the development of smart city initiatives by integrating various services into a cohesive network.

- **Example**: **CityDAO** aims to create decentralized governance structures for urban planning. By allowing citizens to vote on city projects through a blockchain platform, the initiative enhances community involvement in decision-making, leading to more responsive urban development.

DePIN in State Government Applications

Infrastructure Development
State governments can utilize DePIN for efficient management of public infrastructure projects.

- **Example**: In **Wyoming**, the state has embraced blockchain technology for land registry and property management. By implementing a decentralized platform, the government has streamlined the property registration process, reducing fraud and improving transparency.

Public Services
DePIN can enhance the delivery of public services by promoting citizen engagement and accountability.

- **Example**: **Civic** is a blockchain-based identity verification platform that allows citizens to securely share their data with government agencies. This can improve access to services like voting and social benefits while ensuring data privacy and security.

Environmental Monitoring
State governments can leverage DePIN for environmental data collection and monitoring.

- **Example**: **Ocean Protocol** enables decentralized data sharing for environmental monitoring projects. Governments can collaborate with researchers and organizations to access and analyze data on water quality, air pollution, and climate change impacts.

Challenges and Considerations

Regulatory Hurdles
The implementation of DePIN faces regulatory challenges as governments adapt existing frameworks to accommodate decentralized models.

Technical Barriers
Integrating new technologies into legacy systems can pose technical challenges, requiring investment in infrastructure and training.

Community Engagement
Ensuring broad community participation in DePIN initiatives is crucial for success. Governments must focus on education and outreach to engage stakeholders effectively.

Future Outlook

The future of DePIN is promising, with potential for growth across various sectors. Key trends include:

- **Increased Collaboration**: Partnerships between governments, private sectors, and communities to drive DePIN initiatives.
- **Expanded Use Cases**: Development of innovative applications in healthcare, education, and disaster management.
- **Global Adoption**: As success stories emerge, more states and countries are likely to adopt DePIN frameworks.

Conclusion

Decentralized Physical Infrastructure Networks (DePIN) represent a paradigm shift in how infrastructure is managed and developed. By leveraging blockchain technology, DePIN enhances transparency, efficiency, and community engagement, offering innovative solutions to longstanding challenges in various industries and state governance. As this model continues to evolve, it holds the potential to create more resilient and responsive infrastructure systems that benefit communities worldwide. The Kentucky Blockchain Working Group will continue to track this technology as it evolves and matures to identify future opportunities.

Blockchain Risks

This report describes a highly capable and valuable technology, but the technology also has risk. Blockchain is still developing a maturity level needed for a viable solution in some use cases. The technology is in an exploratory state in many industries. While each use case may have specific risks, there are risks that span across most, if not all, lines of business.

COST

Blockchain technology is rarely capable of being layered on top of existing technology. Many times, existing infrastructure and systems require redesign to accommodate the use of blockchain. This represents a high deployment cost in existing complex scenarios.

In addition to the programmatic implementation costs, blockchain technology may impart increased technology overhead requiring increased computing resources. It is likely that additional costs will be incurred to add processing power in systems that leverage blockchain.

LACK OF STANDARDIZATION

While blockchain at a conceptual level is well defined, there are multiple methodologies and mechanisms needed to deploy it. Without standardization and defined common operational standards there exists interoperability concerns.

In addition, there are databases and other software programs/platforms that are being marketed as being blockchain-based but, in reality, are not.

LACK OF CENTRALIZATION

The development of the internet over the last half century has conditioned users to certain expectations with their online experiences. Whether it is email, banking, e-commerce, social media, streaming services or any other of the myriad of platforms developed for the internet, users rely on some central authority to serve as intermediary. For example, Amazon serves this function with online sales transactions, whether through the services they offer, or through the storefronts that they provide other companies and individuals.

Blockchain is a decentralized system of record where individuals or nodes are the responsible entity. A banking customer, in the current system, could potentially lose their log in information to gain access to their account. Because the bank serves as the central authority, the customer follows a process to re-establish their identity and re-gain access to their account. However, in the decentralized system of blockchain, there is no central authority, clearinghouse or repository for this information. A lost key for cryptocurrency could result in that cryptocurrency being lost in the electronic void. This situation has already occurred with lost keys for Bitcoin. As a result, Bitcoin owners lost millions of dollars because they are unable to access their accounts.

REGULATION

Over regulation of a growing technology can be very restrictive to the technology reaching maximum potential. By restricting use, or applying standards that are too narrow, through constricting regulations government, officials can impede the innovation and adoption of the technology and delay or prevent the realization of the benefits of some use cases. However, lack of regulations could have the opposite effect leading to the potential for chaos and uncertainty in the development of a complex technology such as blockchain.

GARBAGE IN, GARBAGE OUT

Blockchain is designed and utilized as a system of record. Its immutable nature allows it to provide a strong, transparent, and auditable record of transactions. However, when logging physical assets on the blockchain, there exists the potential for error or manipulation. For example, in supply chain management, a seller may log a valuable bottle of bourbon on the blockchain ensuring that collectors purchasing the bottle have an adequate record of where the bottle's location and any change of ownership. The blockchain ledger securely records these transactions, however it cannot verify that the bottle originally placed on the blockchain was Pappy Van Winkle and not Kentucky Tavern.

OVER EXUBERANCE

Blockchain is heralded as the next greatest technological development since TCPIP was developed leading to the creation of the Internet. While possible, it is still much too early to predict the technology's scope and influence on everyday lives of individuals. The Internet, through TCPIP, was created in 1972, yet the consumer and public aspects of the Internet were not realized until the mid-1990s when the Dot Com explosion ignited. The Internet initially developed more in isolation through research, academic and military applications. This provided ample time to experiment and create a more usable and unified architecture.

Blockchain is developing in an entrepreneurial manner with corporations and individuals scrambling to be the first to market. Investment, or potentially what is better termed prospecting, is leading to huge influxes of capital into projects that may or may not come to fruition. Where the Internet did not see a bubble/burst cycle until a couple decades into development, blockchain may be seeing it more at its infancy. This may lead to a lack of standardization, as mentioned previously, as well as the risk of failure which may negatively impact future development and investment.

Another facet of over exuberance in the developing technology is that blockchain may be applied in situations where it is not necessarily needed. Blockchain has, or is becoming, a buzzword that attracts attention as something that "you must have". This could be analogous to when Echinacea was identified as having some health benefits and suddenly every herbal remedy, cough drop, nutraceutical or OTC medication began to add it into their blend and market it to capitalize on its perception and gaining popularity.

> **Recommendation 2.1**: Kentucky should explore the benefits of creating a state blockchain leadership position (officer, liaison, coordinator, etc.) to aid in the research and management of potential implementation of blockchain in the state government. This officer would consult with all branches of government, cabinets, agencies and even other local governments to manage the adoption and implementation of blockchain in a smart, methodical and unified manner. In the interim, the work group should identify an intake process for blockchain related inquiries.

Rationale: This report has identified many opportunities for adopting and implementing blockchain to create efficiencies in the systems of the Commonwealth of Kentucky. This report has also identified that there are many risks and potential "landmines" that exist in pursing blockchain adoption. The state blockchain officer can identify opportunities in the state government where blockchain could be beneficial, but likewise rule out cases where it would be either unnecessary or even redundant. The officer could serve as the point of contact for blockchain inquiries, market the state to potential blockchain companies and investment, serve as liaison to blockchain organizations, aid or coordinate the operations of the Kentucky Blockchain Technology Working Group and provide general direction and advice for all things "blockchain". Additionally, with the creation of this position it will send a clear message nationally and globally that Kentucky is in the vanguard of innovation with blockchain technology**.**

ENVIRONMENTAL IMPACTS

The implementation of blockchain in support of some use cases can require large computational and support resources, such as cooling, that consumes large quantities of power. This increased power demand could result in increased carbon emissions and overall carbon footprint.

INCREASED CYBERSECURITY THREATS

As blockchain technology becomes more prevalent, it will likely be seen as an increased area of focus for bad actors in the realm of cybersecurity. As blockchain sees more widespread use in critical infrastructure, bad actors will tailor attacks focused on the blockchain as a means to interrupt, corrupt, or infiltrate these services. These threats can be more pronounced in smaller scale blockchain deployments.

Legislative Analysis 2024

Disclaimer: This legislative analysis is intended to be used as a general reference guide to recent or current legislation only and will be developed more comprehensively over time as the Blockchain Technology Working Group continues to perform its duties under 2020 Senate Bill 55 and KRS 42.747.

Recommendation 3.1: Kentucky should review the legislation adopted or enacted in other states.

Rationale: Blockchain is a highly diverse technology that is still somewhat in its infancy. Because of this, effective legislation can help foster adoption of the technology and its success within the state. By leveraging the experience of other states that have already taken some of the preliminary step, the Commonwealth can craft legislation that defines blockchain effectively and avoid the constrains that can be placed on an emerging technology that can stem from over, or under, regulation.

The following is a brief summation of state legislation enacted in 20204 related to blockchain, cryptocurrencies, DAO structures and similar digital asset/controllable electronic record legislation. This is only a summary of legislation and topics amongst multiple states. A more comprehensive list of legislation adopted, enacted, pending, failed and to governor can be found through the National Conference of State Legislatures website.

Uniform Commercial Code

The following states have enacted the Uniform Law Commission recommended 2022 Emerging Technology amendments to the Uniform Commercial Code:

District of Columbia
Georgia
Iowa
Kentucky
Maine
Minnesota
Nebraska
Oklahoma
Pennsylvania
Rhode Island
South Dakota
Tennessee
Utah
Virginia

Legislation prohibiting use of Central Bank Digital Currencies (CBDC)

Indiana (S 180)
Georgia (H 1053)
South Dakota (H 1161)

Updates to Money Transmission Laws

Connecticut (H 5211)
Maine (S 905)
South Dakota (S 58)

Updates to Banking and/or Insurance Laws

Rhode Island (S 2803)
Vermont (H 659)
Wyoming (S 96)

Laws permitting Decentralized Autonomous Organizations (DAOs)

New Hampshire (L 1317)
Utah (H 318)
Wyoming (S 50)

APPENDIX A
Decentralized Physical Infrastructure Use Case

CONDUIT

Conduit Network

A Decentralized Physical Infrastructure Network (DePIN) for Decentralized Cloud Services

Overview of Conduit Network

Conduit Network is a transformative Decentralized Physical Infrastructure Network (DePIN) that delivers advanced, secure, and resilient decentralized cloud services. By deploying a distributed ecosystem of high-performance hardware nodes operated by independent participants, Conduit Network establishes a decentralized infrastructure for storage, compute, and connectivity services. The network leverages highly secure hardware security modules (HSMs) rated NIST & FIPS 140-2 Level 3 to ensure the highest standards of data integrity and encryption, making Conduit Network a leader in privacy-centric cloud services.

Conduit Network's infrastructure is designed to meet the stringent requirements of Web3 applications, decentralized finance (DeFi), and other applications needing high-performance, secure, and resilient infrastructure. Through its distributed architecture, Conduit Network provides a decentralized alternative to traditional cloud providers, enabling lower costs, enhanced privacy, and distributed resilience for a wide range of industries.

Mission and Vision

Conduit Network's mission is to build a decentralized infrastructure that prioritizes digital sovereignty, privacy, and security. By leveraging a community-owned and operated infrastructure model, Conduit aims to:

1. **Distribute ownership of cloud infrastructure** to a broad community, decentralizing control and mitigating risks associated with traditional centralized providers.

2. **Provide highly secure and scalable cloud services** that serve as the backbone of both Web2 and Web3 - and support the growth of decentralized applications.

3. **Empower individuals and businesses** to participate in the decentralized cloud economy by operating nodes, securing the network, and benefiting from network growth.

The vision for Conduit Network is to become the premier global infrastructure for decentralized digital services, providing secure, scalable, and privacy-focused solutions for applications across blockchain, AI, IoT, and data storage.

Key Components of Conduit Network

1. Core Security Nodes with Advanced Hardware Security

Core Security Nodes form the backbone of Conduit Network, ensuring data security, network integrity, and operational stability. These nodes utilize NIST & FIPS 140-2 Level 3 certified hardware security modules (HSMs), meeting industry standards for data encryption, tamper resistance, and secure key management. Core Security Nodes provide:

- **High-Level Security Protocols**: The FIPS 140-2 Level 3 certified HSMs provide robust security against physical tampering, unauthorized access, and data compromise, securing the network's critical processes.

- **Consensus Mechanisms**: Core Security Nodes operate Conduit's Proof of Economic Activity (PoEA) mechanism, securing the network by validating and recording transactions.

- **Data Integrity and Privacy**: These nodes are responsible for managing and safeguarding data across the network, using encrypted channels to ensure that data privacy is maintained.

- **Trusted Connectivity**: Core Security Nodes facilitate secure, fast connections between distributed nodes, ensuring that services remain accessible and stable for end-users while upholding the network's security standards.

2. Worker Nodes for Scalable Operations

Worker Nodes provide the **primary operational capacity** for Conduit Network, handling storage, compute, and processing tasks. Deployed by independent operators, Worker Nodes provide the flexibility and scalability required for diverse workloads:

- **Storage and Compute Services**: Worker Nodes supply decentralized storage and computational power, supporting a wide array of applications from data processing to decentralized storage.

- **Operational Flexibility**: Worker Nodes distribute tasks efficiently, reducing latency and enhancing the speed and reliability of Conduit Network services.

- **Economic Participation**: Operators can deploy Worker Nodes to earn rewards for their contributions, promoting an inclusive economy where individuals and small businesses play an active role in the network's growth.

3. Conduit Network Temporal Ledger and Asset Tokenization 2.0

The **Conduit Network temporal ledger** is a decentralized system that supports comprehensive data tracking, asset tokenization, and payment mechanisms. This ledger, combined with the security provided by HSMs, ensures that Conduit's financial and operational data remains transparent, auditable, and secure:

- **Asset Tokenization 2.0**: Conduit's temporal ledger supports tokenization of both digital and physical assets within the network, creating a liquid market for tokenized assets underpinned by secure, tamper-resistant records.

- **Smart Contracts for Automation**: The ledger enables smart contracts to automate essential processes such as revenue sharing, dividend payments, and governance, reducing administrative overhead.

- **Revenue Transparency**: The temporal ledger records all network revenues, tracking mining rewards and operational payments to ensure that funds are distributed fairly and promptly to all participants.

Unique Value Propositions of Conduit Network

1. Decentralized Cloud with Advanced Security

Conduit Network provides a highly secure, decentralized alternative to traditional cloud providers, enhanced by its use of NIST & FIPS 140-2 Level 3 certified HSMs. These modules bring encryption and security to each Core Security Node, significantly reducing the risk of data breaches, tampering, and unauthorized access. This decentralized and secure model is ideal for organizations and applications requiring robust data security.

2. Community-Driven Economic Opportunity

The network enables individuals, entrepreneurs, and small organizations to participate by operating Worker Nodes and Core Security Nodes. These operators contribute to network growth and stability while earning revenue, promoting a distributed ownership model that benefits participants directly.

3. Privacy-First and Data Sovereignty Focus

Conduit Network places privacy and data sovereignty at the center of its model, ensuring that all user data is protected from unauthorized access. By incorporating decentralized hardware and software solutions, Conduit enables users to maintain full control over their data, enhancing digital sovereignty and privacy across applications.

4. Optimized Infrastructure for Web3 Applications

Conduit Network is specifically designed to support Web3 applications and blockchain projects. Its infrastructure seamlessly integrates with decentralized applications and DeFi platforms, offering high security, scalability, and low latency for a wide range of use cases.

Revenue Model and Incentive Structure

Conduit Network's economic model is designed to incentivize network growth and participation, while offering multiple revenue streams for node operators and investors:

1. **Node Rewards**: Core Security and Worker Nodes earn rewards for securing the network and providing storage and processing capacity. These rewards are distributed in Conduit tokens, which can be redeemed, traded, or reinvested.
2. **Fees from Cloud Services**: Conduit Network charges fees for decentralized storage, compute services, and data processing, generating revenue that is shared with network participants.
3. **Automated Revenue Sharing**: The temporal ledger system and smart contracts automate revenue distribution, enabling seamless revenue-sharing agreements and transparent income allocation for all network stakeholders.
4. **Tokenization of Assets**: Conduit Network's Asset Tokenization 2.0 framework provides additional revenue opportunities by allowing tokenized fractional ownership of digital and physical infrastructure. The tokens can be traded on secondary markets, creating liquidity for assets and new earning opportunities for investors.

Strategic Partnerships and Growth Potential

To fuel growth and network expansion, Conduit Network is actively building partnerships across key sectors:

- **Blockchain and DeFi Projects**: Conduit provides the infrastructure required to support decentralized applications and DeFi projects, allowing them to run with high performance and security.
- **Enterprise Solutions**: Conduit's decentralized, secure infrastructure is ideal for enterprise clients transitioning to decentralized cloud services, supporting secure data storage and processing with built-in privacy protections.

- **IoT and Government Applications**: With its NIST & FIPS 140-2 Level 3 HSMs, Conduit Network offers a highly secure infrastructure for sensitive applications in IoT, healthcare, and government sectors, where data security is paramount.

Future Outlook and Market Positioning

Conduit Network is uniquely positioned to lead the decentralized cloud services market by combining DePIN technology with a security-first infrastructure approach. With growing demand for privacy-centric and resilient cloud solutions, Conduit Network's integration of advanced hardware security positions it as a robust and trustworthy provider of decentralized services.

As Web3, DeFi, and tokenized assets gain traction and merge with Web2, Conduit Network's infrastructure will provide the foundation needed for these applications, while offering a self-sustaining model that incentivizes community growth and participation. The network's emphasis on security, combined with its distributed ownership model, allows Conduit to serve as a critical backbone for the decentralized digital economy.

Conclusion

Conduit Network redefines cloud services by building a highly secure, decentralized infrastructure powered by a community of independent participants. Utilizing advanced HSMs rated to NIST & FIPS 140-2 Level 3 standards, Conduit Network sets a new benchmark in data security, ensuring that privacy and resilience are embedded in every aspect of its operations. By creating a sustainable, incentivized ecosystem, Conduit Network empowers individuals and enterprises alike to participate in the growth of decentralized services.

Through its unique DePIN model and comprehensive asset tokenization framework, Conduit Network is positioned to drive adoption of Web3, support digital sovereignty, and meet the growing demand for secure, decentralized cloud services. As the decentralized digital economy evolves, Conduit Network will continue to shape the future of cloud infrastructure, offering a secure, efficient, and privacy-respecting alternative to centralized providers.