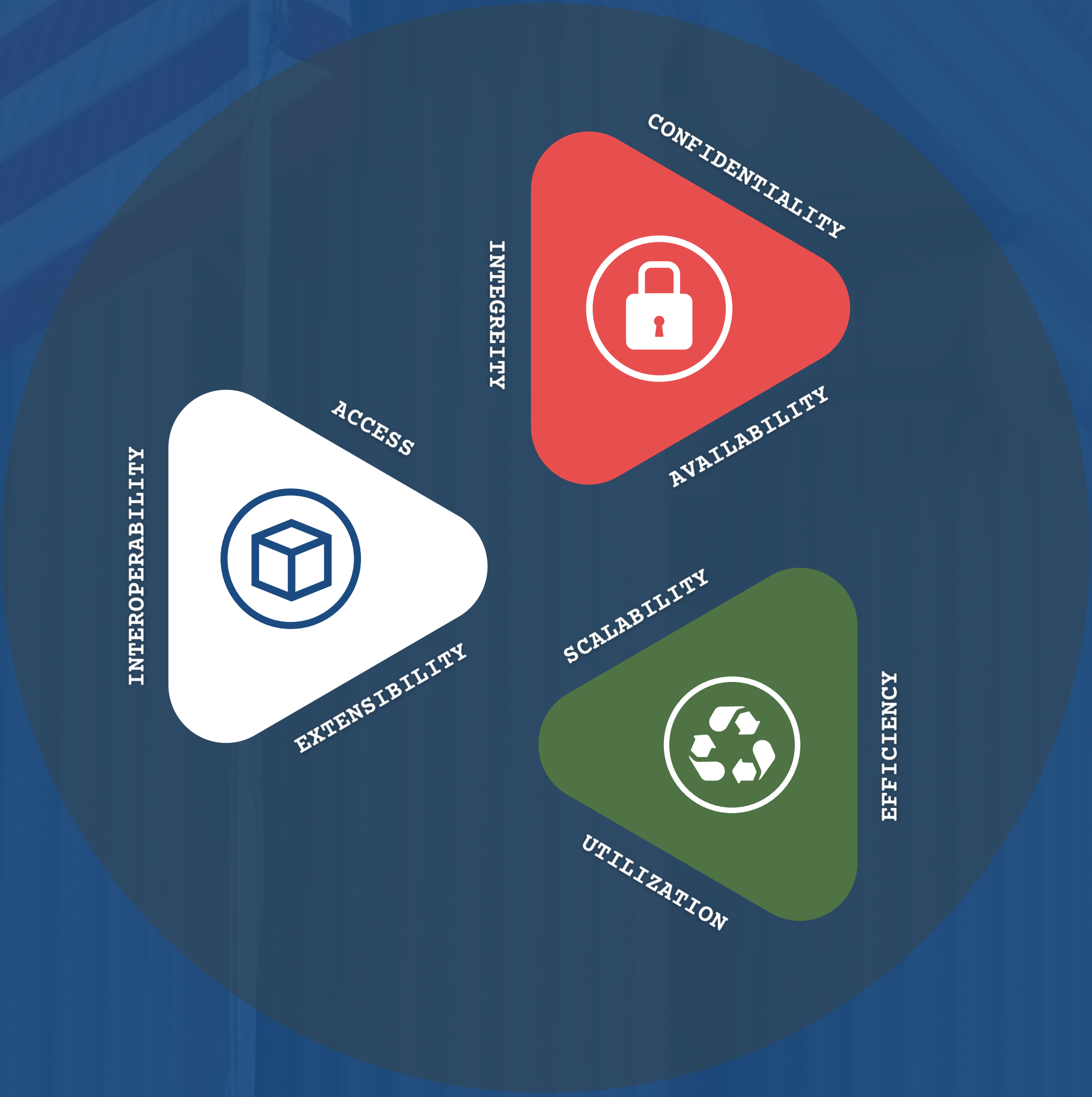
NATIONAL BLOCKCHAIN STRATEGIC REVIEW

A COMMONSENSE APPROACH TO BLOCKCHAIN LEGISLATION



The following framework has been designed to assist any investigative body to review and compare blockchain technologies through a utility-based prism of Security, Stability, and Sustainability.

TERMS & DEFINITIONS:

Blockchain is the technology that serves as a distributed ledger that forms the network. This network creates the means for transacting and enables transferring of value and information

Cryptocurrencies are the tokens used within these networks to send value and pay for these transactions.

AUTHOR:
BRYAN DAUGHERTY

Co-Founder of Proof-of-ESG
Co-Founder of Certihash
Co-Founder of SmartLedger
Public Policy Director for Bitcoin Assoc.
Subject Matter Expert for CSIAC
Certified Cryptocurrency Investigator

Bryan is a certified cryptocurrency and Bitcoin investigator and serves as Global Public Policy Director for a blockchain educative non-profit based in Zug, Switzerland providing technical outreach. Bryan serves as a Subject Matter Expert on blockchain-based information security technologies for several organizations including the Cybersecurity and Information Systems Information Analysis Center (CSIAC), a component of the U.S. Department of Defense (DoD).

Bryan is the Co-founder, Chairman and Technical Advisor for SmartLedger, the world's leading blockchain distribution channel and Founder of Proof-of-ESG, an initiative to reimagine ESG reporting through strategic blockchain reinvention and business transformation.

His expertise includes: Blockchain Information Security, Cybersecurity, Enterprise Blockchain Integration & Implementation, and Commercial Blockchain Application Development.

A COMMONSENSE APPROACH TO BLOCKCHAIN LEGISLATION

Technology and innovation are oftentimes seen as the primary drivers for a country as well as for an organization's next stage of economic growth. As we rapidly transition from the 'big data' era to a global data-based economy, the debate on the security, stability, and sustainability of blockchain technologies has again taken center stage – this time within the halls of policymakers (many of whom have only just begun their journey to navigate this complex, typically 'tribal' industry.)

Sourcing reliable data about blockchain technology

Within this topic, policymakers are frequently finding themselves unarmed and unable to call upon their regular resources to provide the latest information and research. Instead, staffers are being tasked with attempting to retrieve relevant data and insight, often from inaccurate, outdated, and one-sided sources.

The false conflation of blockchain technology and cryptocurrencies

There are important and distinct differences in perspectives and motivations between the proponents of blockchain technology vs the proponents of so-called 'cryptocurrencies', an important difference that can be quite confusing for anyone newly entering this space.

Whereas cryptocurrencies offer a never-ending supply of tradable and highly marketed tokens, primarily focused on exchanging or 'hodling' value, blockchain evangelists see the tokens as a means to access a non-exhaustive list of potential application utility which aims to replace today's legacy infrastructure.

Unfortunately, for the policymakers who now must interpret these technologies, it will require a developed understanding of a complex system that requires the ability to identify the interrelationships while understanding the whole and the parts of the system at the same time.

The public social discourse and media coverage following the topic intimately entwine these terms while almost always focusing on the volatile crypto casino and token economics aspects.

One of the extreme examples of this debate is whether to ban Proof-of-work consensus mechanisms used in cryptocurrencies and blockchains such as Bitcoin Core (BTC) and the BSV blockchain (BSV).

Is proof-of-work scalable and sustainable?

The leading argument that is fueling the ban on proof-of-work surrounds the idea that 'Bitcoin' runs on an energy-intensive network. This is highlighted by respected online resources such as Digiconomist's Bitcoin Energy Consumption Index which details the latest estimates of total energy consumption on the Bitcoin Core (BTC) network.

Their latest research conclusions, which were calculated based on Bitcoin Core (BTC) as benchmark, would lead you to believe that 'a rapid solution to Bitcoin's carbon footprint is not within sight'. This concern has also been expressed by various politicians, technology entrepreneurs, and even within the text of the recent EU MiCA regulation proposal.

As one can see, this is a very common theme and conclusion that has been echoed in countless articles, research papers, and public talks on the subject for quite some time. Some would point to the proliferation of other digital ledger technologies and consensus mechanisms as a means to solve the inherent scalability issues presented with the Bitcoin protocol.

In fact, there was an entire "civil war that occurred over the Bitcoin protocol" which saw competing versions of Bitcoin emerge, with very different attempts to scale the technology.

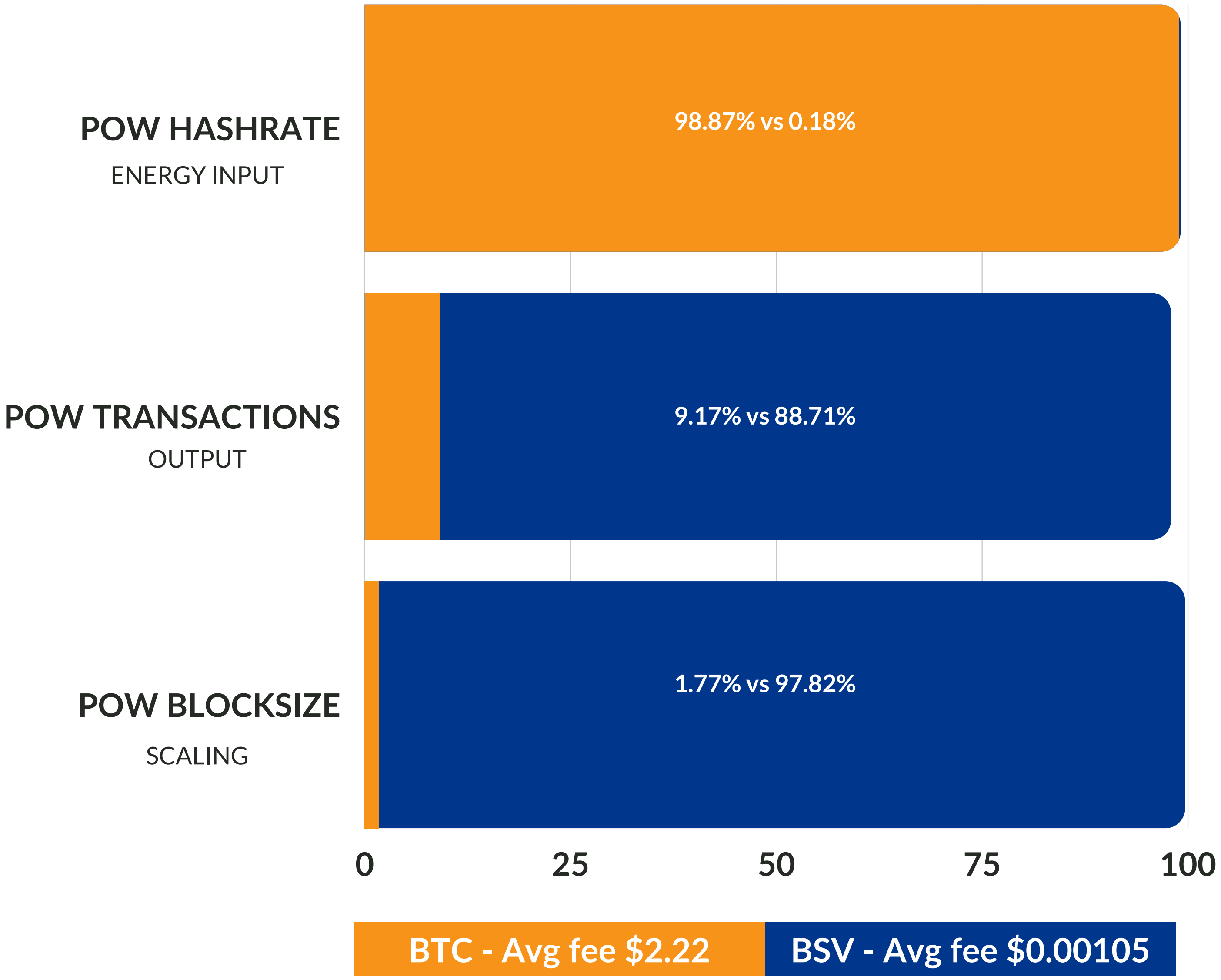
That was over three years ago – what has happened since?

Proof-of-work can scale, just not on all blockchains

Depending on one's persistence to navigate the mix of social crypto influencers, ponzi-schemes, and illegal security offerings, it would be difficult, if not almost impossible to truly follow along. This is due to blockchain being a different type of story, one less volatile and speculative, quietly mirroring some of the greatest innovative technology leaps that mankind has experienced – just without the fanfare of crypto.

As for whether proof-of-work can scale – the answer is not as complicated as the journey.

Using BTC as the benchmark proof-of-work, it is nearly impossible to justify the incredible amount of energy consumed in return for the questionable utility provided. Conversely, when BSV is included within the same modeling, we discover an entirely different outcome.



Throughput is a rate that measures how many actions are completed in a unit of time, in Bitcoin's case, it refers to how many transactions can be processed per second (TPS).

BTC currently offers between 4 – 7 TPS yet consumes a significant amount of energy due to the speculative cryptocurrency mining taking place. Scaling efforts by BTC developers have primarily been focused on creating off-chain solutions which continue to cause fluctuations in the cost to transfer and exchange BTC – this is due to the restrictive capped 1mb blocks that BTC has maintained.

Since block #556767 was mined on November 15th 2018, BSV developers have been breaking proof-of-work scaling barriers which were once believed to be inconceivable, including just recently on February 6th 2022 when TAAL, an enterprise blockchain service provider mined block #725511, a 3.8 GB block which contained over 188,000 transactions, and had an average transaction fee of $0.005.

	BITCOIN SV (BSV)	BITCOIN CORE (BTC)	ETHEREUM (ETH)
Consensus Model	Proof-Of-Work	Proof-Of-Work	Moving to Proof-Of-Stake
Permission Type	Public	Public	Public
Regulatory Compliant	✓	Questionable	Questionable
Data Privacy	✓	✓	✓
Tokens	✓	✓	✓
Smart Contracts	✓	✓	✓
Throughput Capacity	5,124 TPS / 100K TPS	7 TPS	15-20 TPS
Transaction Fee per kb	$ 0.00051 (Stable)	$2.22 (Highest $62)	$194 (Volatile)
KWh per Transaction	4 KWh/TX	2253.46 kWh/TX	62.56 KWh/TX
CO2 per Transaction	2 KG/TX	1070.39 KG/TX	73.1 KG/TX

As for BSV throughput, a real-time demonstration during a live June 2021 blockchain conference, showed over 50,000 – 100,000 transactions per second (TPS) could be achieved.

In comparison, Visa processes around 1,700 transactions per second, though claiming to be able to handle 65,000 TPS. BSV on the other hand has shown publicly the capacity to not only handle this volume of financial transactions, but also be the trustless accounting ledger, the shipping and supply chain infrastructure, the means of identity management solutions, and much more.

The BSV blockchain is the most sustainable node implementation

MNP, a leading national accounting, tax, and business consulting firm in Canada has spent a great deal of time researching this topic and have recently published two reports that document why the original Bitcoin protocol matters, how changes to the popular BTC version have affected its capabilities, as well as how another competing version, BSV has been able to unleash the native scaling abilities that were present when the system was initially released.

The new independent blockchain technology energy consumption modeling MNP created confirms that block size and throughput have a significant effect on Proof-of-work efficiency.

Their team leveraged work from several existing frameworks as well as industry experts to determine the electricity consumption of Bitcoin Core (BTC), Bitcoin Cash (BCH), and the BSV blockchain (BSV), validating their new energy consumption model with real-world data from cryptocurrency miners.

Scaling = Sustainability

MNP discovered major distinctions between the protocols, namely that the power consumption per transaction, and equally, per megabyte, decreases when network utilization is higher on proof-of-work protocols with a more permissive block size than on those that are more restrictive. The arbitrary limitations of BTC continue to have a significant impact on the power consumption per transaction.

> *'BSV is the most efficient blockchain network when compared to the other SHA-256 proof-of-work blockchains. With greater utilisation, and throughput these reductions in consumption per transaction, and increase in efficiency will only improve.'*

This is contrary to the sentiments expressed in section 5a of the recent EU MiCA language:

> *The consensus mechanisms used for the validation of transactions can have a substantial environmental impact. That is particularly the case for the consensus mechanism known as proof-of-work, which requires participating miners to solve computational puzzles and compensates them in proportion to their computational effort.*
>
> *Rising prices of the associated crypto-asset, as well as the frequent replacement of mining hardware, create incentives for increases in computational power. As a result, today, proof-of-work is often associated with high energy consumption, a material carbon footprint and significant generation of electronic waste. Those characteristics could undermine Union and global efforts to achieve climate and sustainability goals, until other more climate friendly and not energy intensive solutions emerge. The best-known application of the proof-of-work consensus mechanism is Bitcoin.*

> *Crypto-assets relying on the ‘proof-of-work’ method as consensus mechanism to validate transactions indirectly cause considerable carbon emissions and affect the climate and the environment negatively today. This is due to the proof-of-work method’s currently intensive and inefficient use of electricity.*

Subjective data sources inform poor policies

Without intimate technical knowledge and access to the latest research on the competing Bitcoin protocols, it is likely that regardless of how well-intentioned policymakers are, their pending regulations will lead to stifling blockchain innovation.

The definition detailed by the EU MiCA regulation is only correct in describing BTC’s protocol. The mechanism of proof-of-work used in the original bitcoin, and now representative in the BSV proof-of-work protocol, does not compensate in proportion to added computational work.

Rather, the proportion is related to a combination of the amount of energy imputed into solving the puzzle, combined with the amount of computational effort in validating transactions, and this proportion increases as the block subsidy decreases over time.

> *“At large scale, proof-of-work computation needs to be balanced with the increased validation load. So, the true usage is balanced between multiple aspects of the network. In any network including Ethereum and BTC you will find that transaction validation is several million times more energy inefficient than hashing. Within BSV, the validation load becomes the energy use, and this remains low compared to existing systems including Visa. The issue is the amount of scale and nothing else.” – Dr. Craig Wright, Chief Scientist at nChain*

Is proof-of-stake the next best thing?

Due to the false assumption that proof-of-work consensus mechanisms are computationally unscalable and overly energy consumptive, many have sought to find more ‘environmentally friendly’ ledger systems.

Proof-of-stake networks mimic the structure and processes of real blockchains, however at their core, they are only distributed ledger networks – not blockchains by default.

The design includes highly complex mathematical models and algorithms to compensate for the lack of security of the system. This is to hide centralisation and offers very little except marginal security since governance of the system is achieved through ‘staking’ or ‘voting’.

This consensus model facilitates control by ownership to those who hold the ‘majority’ of staked coins, opening the network to sybil attack and subjective decision-making processes.

In proof-of-stake, the concept is to continually bring on new nodes to validate transactions, which over time results in a direct increase of electricity, with no end in sight. Having 50,000 nodes, especially when most of these nodes do not participate to validate transactions or produce blocks, is unnecessary and unsustainable.

To re-emphasise, proof-of-stake hardware that seeks to join the network, will only increase the energy consumption of the ledger by several kilowatt hours, not to mention creating an even larger carbon footprint due to the additional surrounding infrastructure required.

The proof-of-stake argument leans on the misunderstanding that the consumption of power is removed when you take the Proof-of-work out of the equation. Not only is that nonfactual, but if we analysed the full power usage of some of the proof-of-stake protocols, we would see the argument sorely fall apart at the seams.

Proof-of-stake is not more energy efficient than a scalable proof-of-work system, and most experts would agree that it also fails to provide the robust and resilient economic and cryptographic security that is inherent with proof-of-work.

Security: proof-of-stake vs proof-of-work

At a time when the world is seeking solutions for data integrity and protection from cyber-attacks and data breaches, we simply cannot ignore the scalable blockchain solutions available to us today, nor can we afford to forfeit security and stability for a false sense of sustainability.

Whereas proof-of-stake opens up numerous additional cyber-security attack vectors, proof-of-work perfectly mirrors and improves upon the CIA Triad and NIST Cybersecurity frameworks that guide many companies and government contractors today.

The original Bitcoin protocol was designed to allow individuals to exchange data in an entirely new architecture that provides a firewall between the user's identity and the transaction.

This removes the need for a trusted third-party authority and empowers users to maintain control over their identity. This significantly increases the cost to cyber-criminals, as they are required to individually attack millions of customers' networks, instead of targeting one network that exposes millions of customers' information.

Bitcoin is based on a design that protects the network against bad actors by allowing honest nodes to reject blocks that either attempt to double spend coins or violate the established rules governing the network.

This consensus is enforced through the accumulation of proof-of-work, which allows honest nodes to combine their collective hashpower to fend off would-be attackers. This creates a mathematically infeasible as well monetarily impractical situation where the attackers must overpower the honest network for an indefinite period of time, as they attempt to maintain a chain of work that includes fraudulent activity.

A framework to review and compare blockchain technologies

As mentioned previously, navigating this complex system of blockchain and digital ledger technologies is not an easy feat for anyone.

By examining only one aspect of the debate, we can see that there exists a lack of objectivity, scarcity of updated information, and a limited supply of technical expertise surrounding the differences between cryptocurrencies and blockchain, Proof-of-work and proof-of-stake, and how these different consensus models differ when applied to both short term and long-term energy utilization, as well as the impact on global information security.

Beyond the booming crypto-casino tokens and artistic NFT's that currently have most people's attention – including regulators, remains the need for a technological advance to provide next-generation data security as we transition into a global data powered economy.

As more government agencies begin to investigate these technologies, such as the United States has recently embarked upon, I strongly believe that they must strive to synchronize their National Strategic Review Approach with a focus on security, stability, and sustainability.

This requires a framework to identify the interrelationships and understand the whole and the parts of the systems at the same time.

By using a balanced, unified, and standardized approach to review and compare blockchain technologies, I am confident that policymakers will find it entirely unnecessary to forfeit the future security of a nation's network as well as financial and data infrastructure by seeking less secure models of consensus mechanisms than proof-of-work.

It is a matter of national and public interest to assure that stable, secure, and sustainable blockchain technology has the unobstructed lane to meet its inherent design to scale and handle the world's data and financial growing needs, improving beyond the capabilities of today's limited digital infrastructure.

The following framework has been designed to assist any investigative body to review and compare blockchain technologies through a utility-based prism of Security, Stability, and Sustainability.

The framework utilizes terms that do not require a deep technical understanding of blockchain technologies, but rather provide an even-handed framework for policy makers to identify sustainable, utility-based blockchain offerings.

As with most emerging technologies, blockchain and digital ledger technologies can be difficult to begin to understand and compare. This framework helps to identify the interrelationships and understand the whole and the parts of blockchain systems at the same time.

SECURITY: The Triad of Information Security is a benchmark model used to evaluate information security resiliency of data and network integrity.

NATIONAL INFORMATION SECURITY

INFORMATION SECURITY	CONFIDENTIALITY	Blockchain data must remain 100% confidential as needed or required.
	INTEGRITY	Blockchain data must be time-stamped and immutable.
	AVAILABILITY	Blockchain data and network must be redundant and always be available.

STABILITY: The Triad of Stability is a measure of a platform's overall ability to continue to function over time without failure, ensuring accessibility, Interoperability, and extensibility.

NATIONAL ECONOMIC SECURITY

ECONOMIC SECURITY	ACCESSIBILITY	Blockchain by definition must be public, widely publishing on a distributed ledger.
	INTEROPERABILITY	Blockchain protocol must remain stable for interoperability and reduce data silos.
	EXTENSIBILITY	Blockchain protocol must be stable to allow for extensibility into future innovation.

SUSTAINABILITY: The Triad of Sustainability is an environmental standard that governs the social responsibility of an organizational system's scalability, utilization, and efficiency capabilities.

NATIONAL ENERGY SECURITY

ENERGY SECURITY	SCALABILITY	Blockchain data delivery must be nearly instant and able to handle varying data loads.
	UTILIZATION	Blockchain must provide utility while utilizing energy more effectively than alternatives.
	EFFICIENCY	Blockchain network must be more cost efficient than legacy counterparts.