NTT Research

# Three Studies on Blockchain Development

by Kevin L. Jackson

1 **Cryptoasset and Blockchain for Building Business Trust**
–Published December 4, 2020

2 **Blockchain for Business Trust**
–Published February 25, 2021

3 **Researching Future Blockchain "The Blockchain Trilemma"**
–Published April 23, 2021

**Kevin L. Jackson is a globally recognized Thought Leader, Industry Influencer, and Author.** He has also been recognized as a "Top 5G Influencer", "Top Cloud Computing Expert", and "Top Digital Transformation Expert" by multiple sources. Mr. Jackson also provides integrated social media and management consulting services to many advanced technology companies. His most recent book on digital transformation, "Click to Transform", was ranked #1 on multiple Amazon bestseller lists.

NTT Research

# Cryptoasset and Blockchain for Building Business Trust

by Kevin L. Jackson, CISSP®, CCSP®

Published December 4, 2020

Cryptocurrencies and their underlying blockchain technology may be essential to online business because they can serve as fundamental building blocks of business trust. Dr.Shin'ichiro Matsuo, head of blockchain research in the Cryptography & Information Security (CIS) Lab at NTT Research, is focused on this as crucial basic research. Dr. Matsuo also serves as a research professor at Georgetown University, where he is a director of the CyberSMART research center and blockchain technology and ecosystem design lead. As a component of NTT Research, the CIS Lab conducts basic research that advances technologies that can best promote humankind's positive change. Although they are new in Silicon Valley, NTT Research comes from a rich lineage of ground-breaking research and development. The NTT R&D Lab in Tokyo, Japan, boasts over 1600 patents. In many ways, that makes them uniquely qualified to research technological advancements that support businesses.

Dr. Matsuo has focused on technology research since 1996 when he implemented an E-Cash system as an experiment with the Bank of Japan. Based on theories developed by NTT Fellow and CIS Lab Director, Dr. Tatsuaki Okamoto, he designed the first Central Bank DigitalCurrency (CBDC). The goal then was to create a centralized digital cash system, which is the opposite of the decentralized bitcoin currency and the underlying blockchain technology, he works on today. *(Figure 1)*


*Figure 1 - Shin'ichiro Matsuo, Head of Blockchain Research, Cryptography & InformationSecurity (CIS) Lab, NTT Research.*

According to Dr. Matsuo, blockchain is an essential technology for all telecommunications companies. As he explained it to me during our discussion, the evolution of blockchain in business will be like electronic commerce (e-commerce) on the internet.

Before the internet, telecommunications companies like NTT and AT&T controlled the global communications infrastructure. This control also gave them the power to influence international business communications and any associated commerce transactions. After the internet, anyone could create a new network node capable of independently conducting business. This new reality positioned the internet as a critical catalyst for permission-less business innovation and the growth of e-commerce. This shift also diminished the control of business transactions that Telco's previously enjoyed. *(Figure 2)*

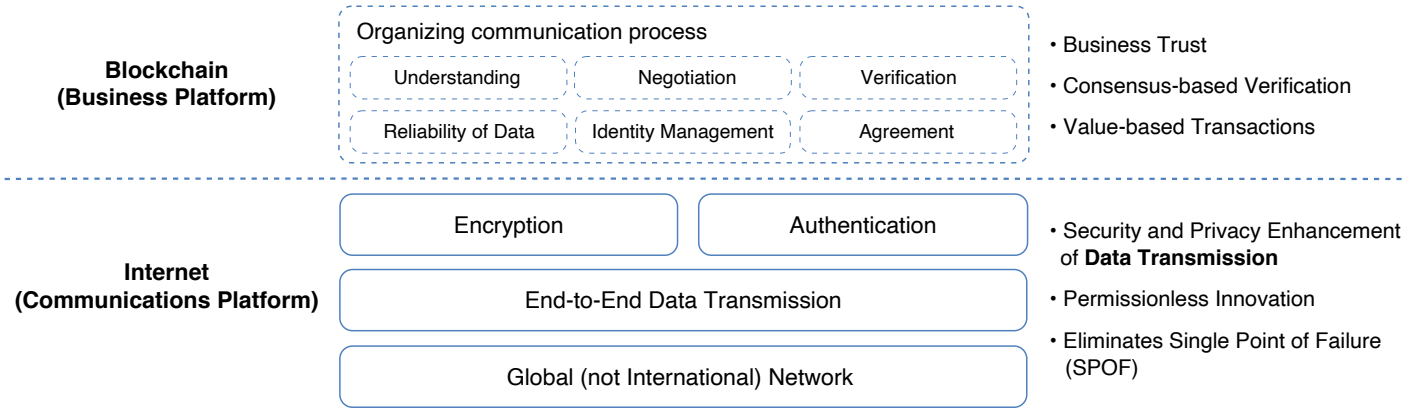



*Figure 2 - Internet Communications Platform vs. Blockchain Business Ecosystem.*

Shin'ichiro Matsuo believes that blockchain has a similar role in finance and creating business. The key lies in the ability of blockchain's shared ledger technology to instill trust into e-commerce by providing consensus-based verified business data. Just as internet technology served as the communication platform for e-business, blockchain will serve as the essential platform for business trust.

The 2008 global financial crisis brought business trust into stark relief. At that time, international agents of trust and authority with decades-long track records experienced a severe credibility crisis. G7 finance ministers and central bank governors met in Washington,DC to "Take decisive action and use all available tools to support systemically important financial institutions and prevent their failure." During the same period, Satoshi Nakamoto introduced Bitcoin as a payment system that could be constructed fully peer-to-peer, with no trusted third party. This approach eliminated most of the traditional finance system components and led to today's rapidly escalating use of Bitcoin and other cryptocurrencies.

Another area of basic research that is well-suited for NTT Research's CIS Lab is Bitcoin's apparent ecological unsustainability. As cryptocurrencies and blockchain become more mainstream, society needs to find a way to address these technologies' potential negative environmental impact at scale. As is well documented, the energy consumption and carbon intensity associated with building business trust through "proof-of-work" in online and offline financial transactions are massive.

## Proof-of-Work: Online and Off-line


*Figure 3 - Basic research in the generation of business trust through "proof-of-work" is critical to both offline and online business.*

For offline transactions, one crucial building block for trust is the face-to-face meeting. These intimate events provide rich information on our counterparts, which builds our confidence in interpreting any related business information. We emit tons of electricity and CO2 is consumed in preparation, travel, holding meetings, and holding a social event and dinners. However, the global pandemic has replaced many face-to-face meetings with online communications requiring an online trust-building mechanism. In the online model, trust is trust has come to depend on the enormous electricity and microchips deployed by cryptocurrency miners. Emitting trillions of tons of CO2 and spending a corresponding amount of money is now required to give the impression of online trustworthiness. This is a transition of the source of trust, and we face fundamental questions regarding the sustainability of online trust mechanisms based on blockchain. Widespread adoption of green practices within the blockchain industry and global finance is sorely needed. As business leaders address the irresponsibility to reduce energy consumption, basic research by labs like NTT Research's CISLab makes perfect incubators for this work.

As highlighted in the organization's mission statement, NTT Research aims to conduct primary research and advance the technologies that become second nature to promote humankind's positive change. These are just two examples of how basic research in blockchain and cryptocurrency is crucial to global business growth.

Kevin L. Jackson is a globally recognized Thought Leader, Industry Influencer, and Author. He has also been recognized as a "Top 5G Influencer", "Top Cloud Computing Expert", and "Top Digital Transformation Expert" by multiple sources. Mr. Jackson also provides integrated social media and management consulting services to many advanced technology companies. His most recent book on digital transformation, "Click to Transform", was ranked #1 on multiple Amazon bestseller lists.

NTT Research

# Blockchain for Business Trust

by Kevin L. Jackson, CISSP®, CCSP®

Published February 25, 2021

Late last year, I had the opportunity to discuss blockchain and crypto assets with Dr. Shin'ichiro Matsuo, head of blockchain research in the Cryptography & Information Security (CIS) Lab at NTT Research. In 1996, Dr. Matsuo implemented an E-Cash system based on theories developed by NTT Fellow and CIS Lab Director, Dr. Tatsuaki Okamoto. This work convinced Dr. Matsuo that the key to using blockchain for business lies in blockchain's shared ledger technology's ability to instill trust into e-commerce by providing consensus-based verified business data. That concept was so impressive that I welcomed the opportunity to continue the conversation with Dr. Go Yamamoto, a senior scientist in the NTT Research Cryptography & Information Security (CIS) Lab.

Since joining NTT in 2002 as a member of the blockchain research group, Dr. Yamamoto has focused on establishing and maintaining "trust" across digital infrastructures. The required components for establishing trust consistency are dependability, accessibility, and ubiquity. Since cloud service providers deliver a significant percentage of digital business infrastructure services, CSPs are central to the business trust model.

According to Dr. Yamamoto, the CSP's essential infrastructure role fundamentally changes the nature of all digital business ecosystems.

This change is due to cloud-based IT infrastructure services' economic advantages, which essentially forces many business model owners to adopt the cloud computing model to deliver an economically viable product or service. The adoption of cloud services means that the business model owner no longer retains control of many vital elements of the business model, including:

- Customer relationship management;
- Supply chain management;
- Emergency response; and
- Cybersecurity

Handing these essential elements to the provider also gives the hyperscale CSPs control of global commerce through their ability to control the global IT infrastructure. This evolution establishes trust between business model owners and cloud service providers essential to a successful digital transformation. Therefore, using blockchain to develop digital ecosystem trust can be beneficial to every business.


*Figure 1 - Dr. Go Yamamoto, NTT Research and Kevin L. Jackson- discuss blockchain for business trust.*

## Digital Business Ecosystems

Before going further, it's essential to appreciate the role that ecosystems play in modern business. Research by the BCG Henderson Institute found that in annual reports, the term "ecosystem" occurs 13 times more frequently now than it did a decade ago. The success of iconic examples such as Google, Apple, Facebook, and Amazon fueled this increase. A "business ecosystem" is a dynamic group of largely independent economic players that create products or services that together constitute a coherent solution. There are two types, solution and transaction, and both represent governance models for organizing members to realize a specific value proposition. (*Figure 2)*

Key business ecosystem characteristics include:

- Modular components that operate independently yet function as an integrated whole;
- Independent components are customized to the ecosystem and made mutually compatible;
- Relationships are multilateral, meaning they are not decomposable to an aggregation of bilateral interactions; and
- Business ecosystems are not fully hierarchically controlled but encompass a coordination mechanism. Coordination is significant to digital ecosystems because application programming interfaces (APIs) regulate access and interaction.

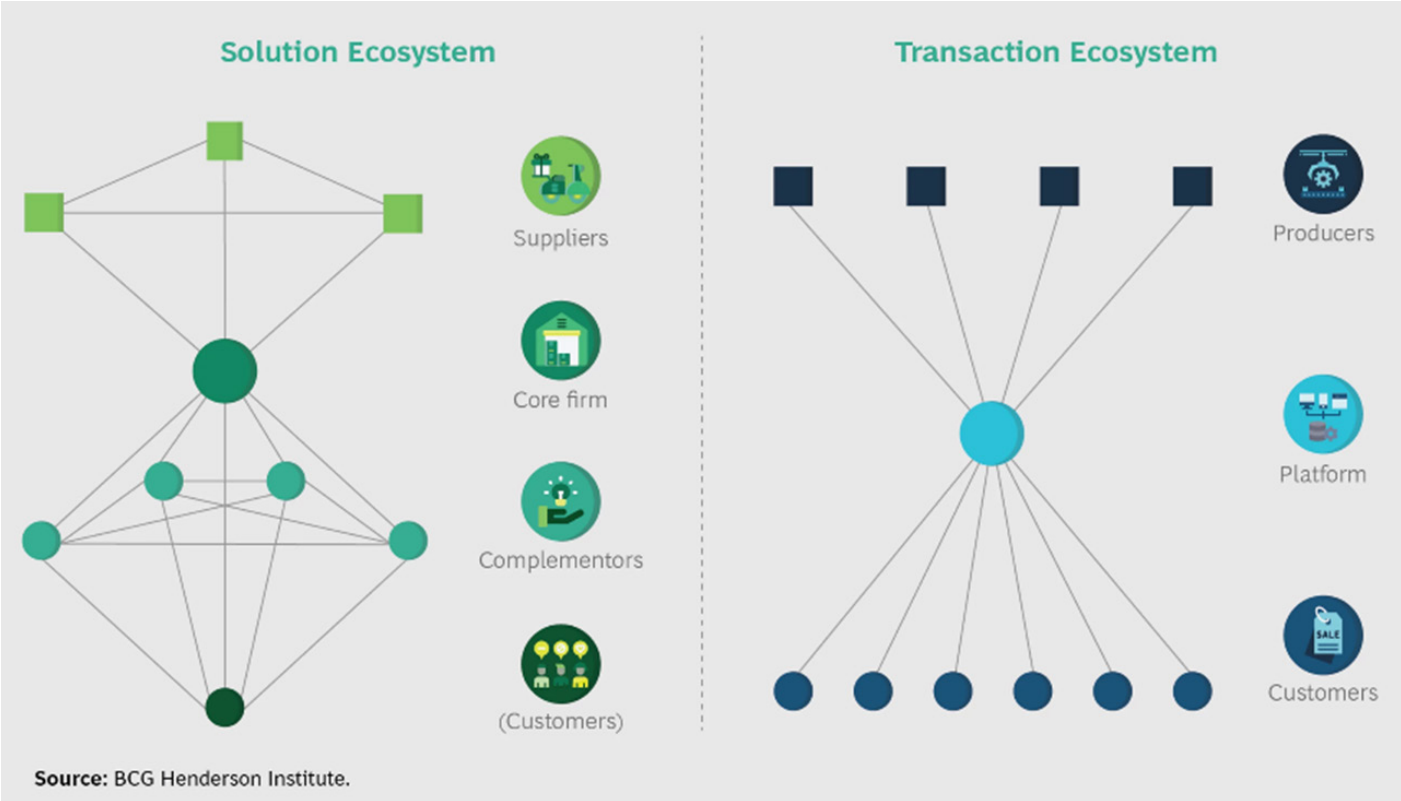


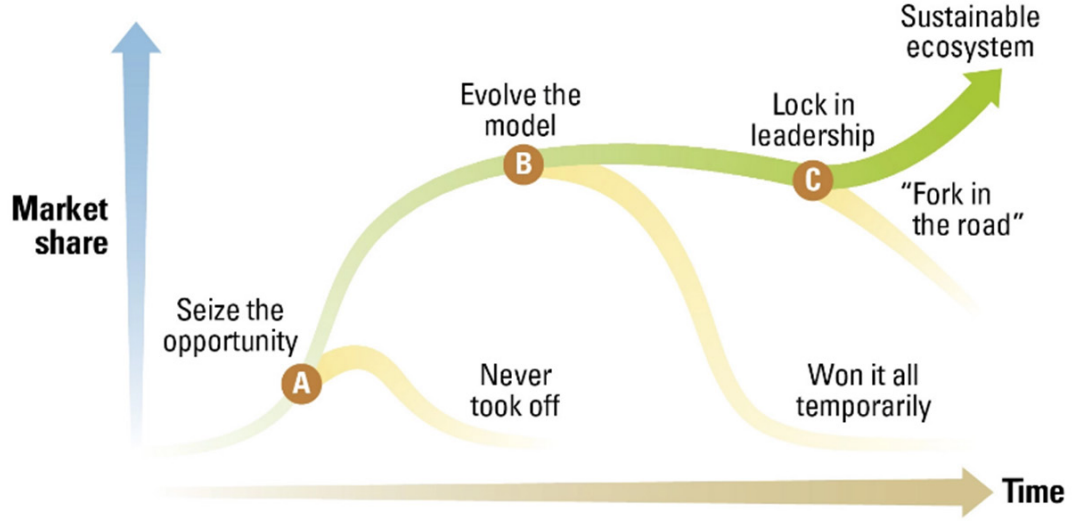

*Figure 2 - Two business ecosystem types.*

Digital business ecosystems broadly leverage APIs to increase the speed, reach, convenience, efficiency, and scalability of the ecosystem members and are thus an essential driver of ecosystems' current growth in general.

Sustainable ecosystems also tend to mature by going through three distinct phases. (*Figure 3)*

1. Successfully seize the opportunity with ecosystem partners by simultaneously capitalizing on a marketplace network effect:
2. Evolve their business model by expanding the scope of the platform and increasing engagement with platform participants; and finally
3. Sustain long-term success through effective leadership capable of managing vested interests among partners and other stakeholders, including regulators and customers.

Successfully navigating these three gates requires establishing trust among all ecosystem members.




| Window | Actions implemented | Success rate: In each stage | Success rate: Cumulative |
|---|---|---|---|
| **Seize the opportunity** | • Be the first or radically disrupt<br>• Scale fast<br>• Invest persistently and sufficiently | 50%* | 50% |
| **Evolve the model** | • Broaden ecosystem scope<br>• Increase engagement | 50% | 25% |
| **Lock in leadership** | • Manage vested interests<br>• Maintain differentiation<br>• Renew the platform | 60% | 15% |

*Figure 3 - The evolution of business ecosystems.*

## Building Trust with Blockchain

Cloud service providers connect customers to digital products and components of those products to each other almost exclusively through APIs. The service delivered by each CSP is unique to that platform. These services are not commodities because they aren't interchangeable between different cloud service provider platforms. (*Figure 4)* The business model owner cannot assume that any cloud service is consistent with any industry standard since none exists. There is no industry-wide mechanism for establishing such a standard.

This lack of cloud service standards gives the cloud computing platform owner unassailable bargaining power across all digital business ecosystems. This ecosystem model is not sustainable for global digital commerce over the long term because those cloud service platforms (and their APIs) will become dominant. By tying any business model innovation to a cloud service implementation and its API, all business model innovation is suffocated. (*Figure 5)*

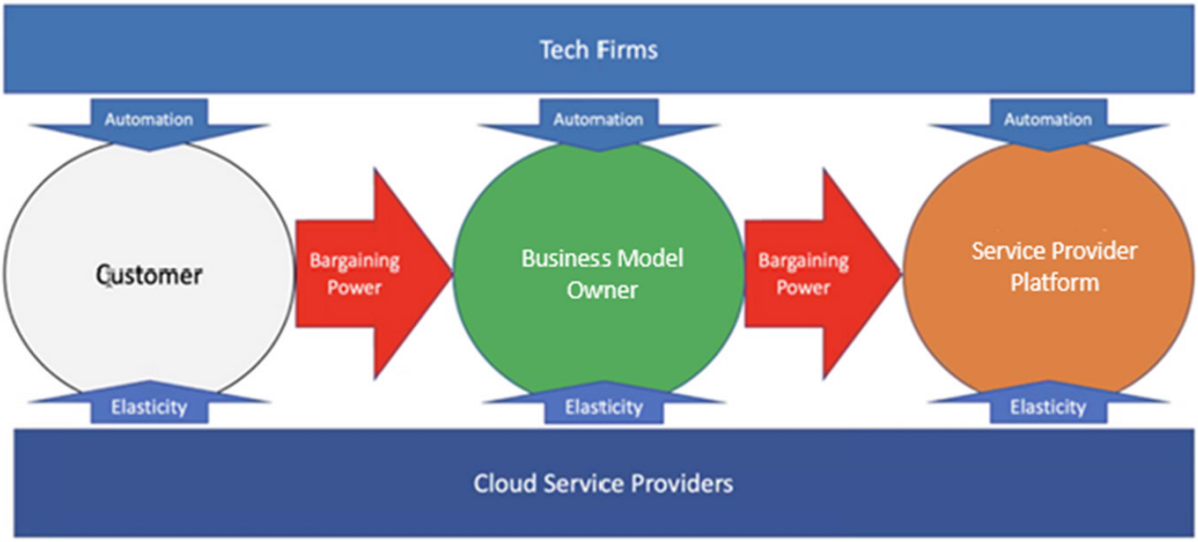



*Figure 4 - Service providers and technology firms support business model innovation.*


*Figure 5 - Business model innovation suffocated by proprietary cloud services that gives digital business ecosystem bargaining power to service provider.*

Suffocation can be prevented by making cloud services a true commodity. Blockchain can enable this by using a concept Dr. Yamamoto refers to as a Common State Layer. (*Figure 6)* This layer is an autonomous, public consensus mechanism used to ensure services are replaceable between different domains. For this digital business ecosystem scenario, the layer implements a standard cloud-based infrastructure between the Business Model Owner (Domain 1) and the Cloud Service Provider (Domain 2), and the Business Owner can propagate the bargaining power to the platform because the Service Provider is replaceable. Blockchain across the public internet can implement this consensus layer. The layer would also provide the needed components of trust in that;

- Dependability of the standard service is assured since the services wouldn't be unique to a specific CSP;
- Service accessibility would be guaranteed in that the business owner could access the standard service from any other CSP; and
- Service would be ubiquitous because it would be provided across the public internet.


*Figure 6 - Business model innovation supported by cloud service standards that preserves business model owner bargaining power within digital business ecosystem.*

While the "common state layer" seems futuristic, cryptocurrencies prove the concept's viability. In that domain, national governments provide fiat currencies like Euros, British Pounds, and US Dollars. Blockchain-based networks represent the autonomous, public consensus mechanism, or state layer, that uses crypto-assets to provide a financial digital services infrastructure.

However, using blockchain to extend this model to global commerce would require multiple public consensus layers across various business domains.

Implementation would also require the development of a "starter kit" for public local blockchain business systems that:

- Anyone can join/take part in (like the internet);
- Exhibits controllable scale (unlike Bitcoin);
- Anyone can start for any desire or specific purpose; and
- Can collaborate with other systems.

Dr. Yamamoto is currently researching current blockchain systems. His analysis will help design a useable protocol for a future business Common State Layer.

This work is just another example of the importance of basic research to the advancement of global business. I look forward to the day when blockchain independently verifies trust between businesses everywhere.

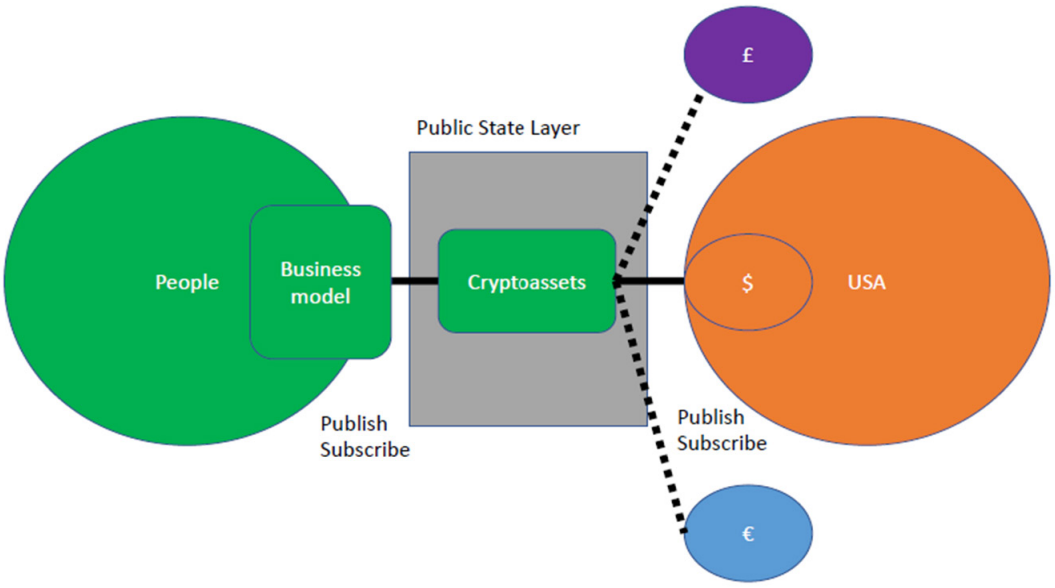



*Figure 68 - Common State Layer for crypto assets.*

Kevin L. Jackson is a globally recognized Thought Leader, Industry Influencer, and Author. He has also been recognized as a "Top 5G Influencer", "Top Cloud Computing Expert", and "Top Digital Transformation Expert" by multiple sources. Mr. Jackson also provides integrated social media and management consulting services to many advanced technology companies. His most recent book on digital transformation, "Click to Transform", was ranked #1 on multiple Amazon bestseller lists.

NTT Research

# Researching Future Blockchain "The Blockchain Trilemma"

by Kevin L. Jackson, CISSP®, CCSP®

Published April 23, 2021

Analysts forecast that the global blockchain market will grow from $3.0 billion in 2020 to $39.7 billion by 2025. That is astonishing growth. Supporting that forecast, a Deloitte 2019 Blockchain Survey showed that blockchain adoption shifted aggressively from experiments toward the development of robust enterprise-ready solutions. (*Figure 1*)

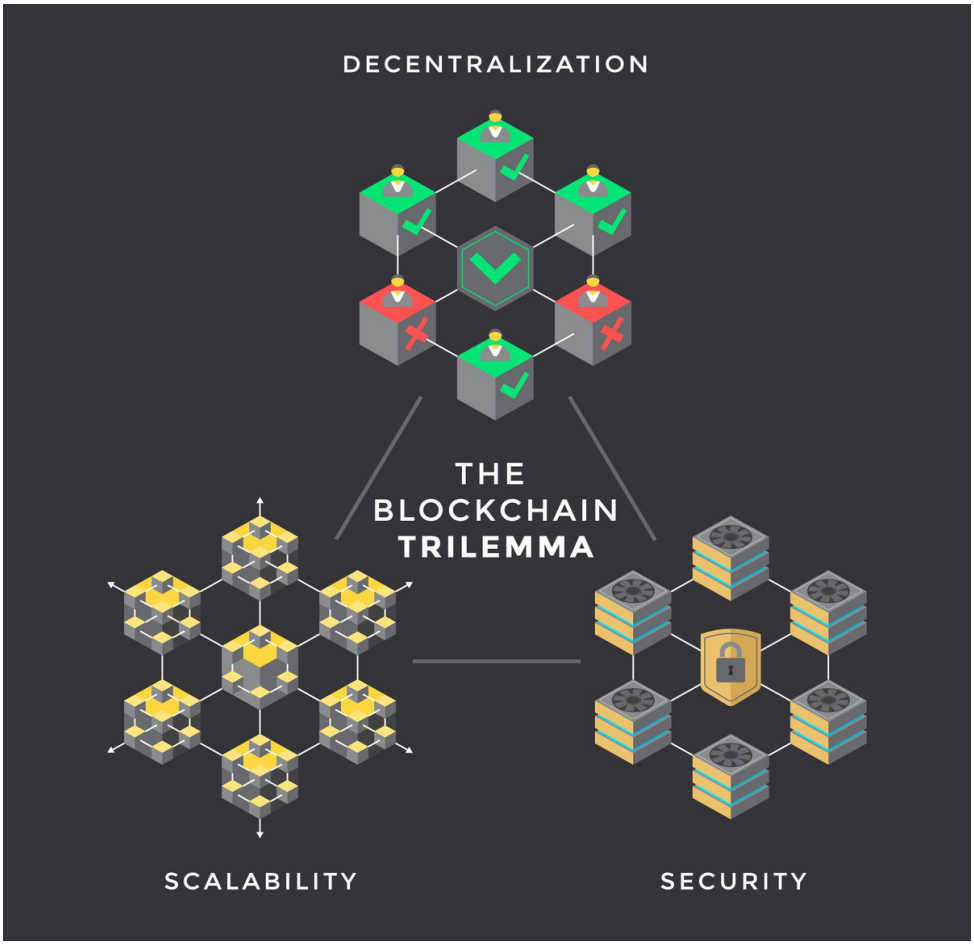



*Figure 1.*

As businesses infuse this exciting technology into their core processes, many don't realize significant differences between blockchain technologies. Referred to as 'the blockchain trilemma,' blockchain solution providers must evaluate a performance trade space bounded by scalability, decentralization, and security.

Maximizing any two of these characteristics will be at the expense of the third. Therefore, business goals and customer sensitivities will play a significant role in determining which vendor will be successful in which industry. There are also critical trades between Permissioned and Permissionless blockchain and between public and private offerings. These variables outline the importance of the blockchain business model research conducted by Aron Laszka at the University of Houston. *(Figure 2)*

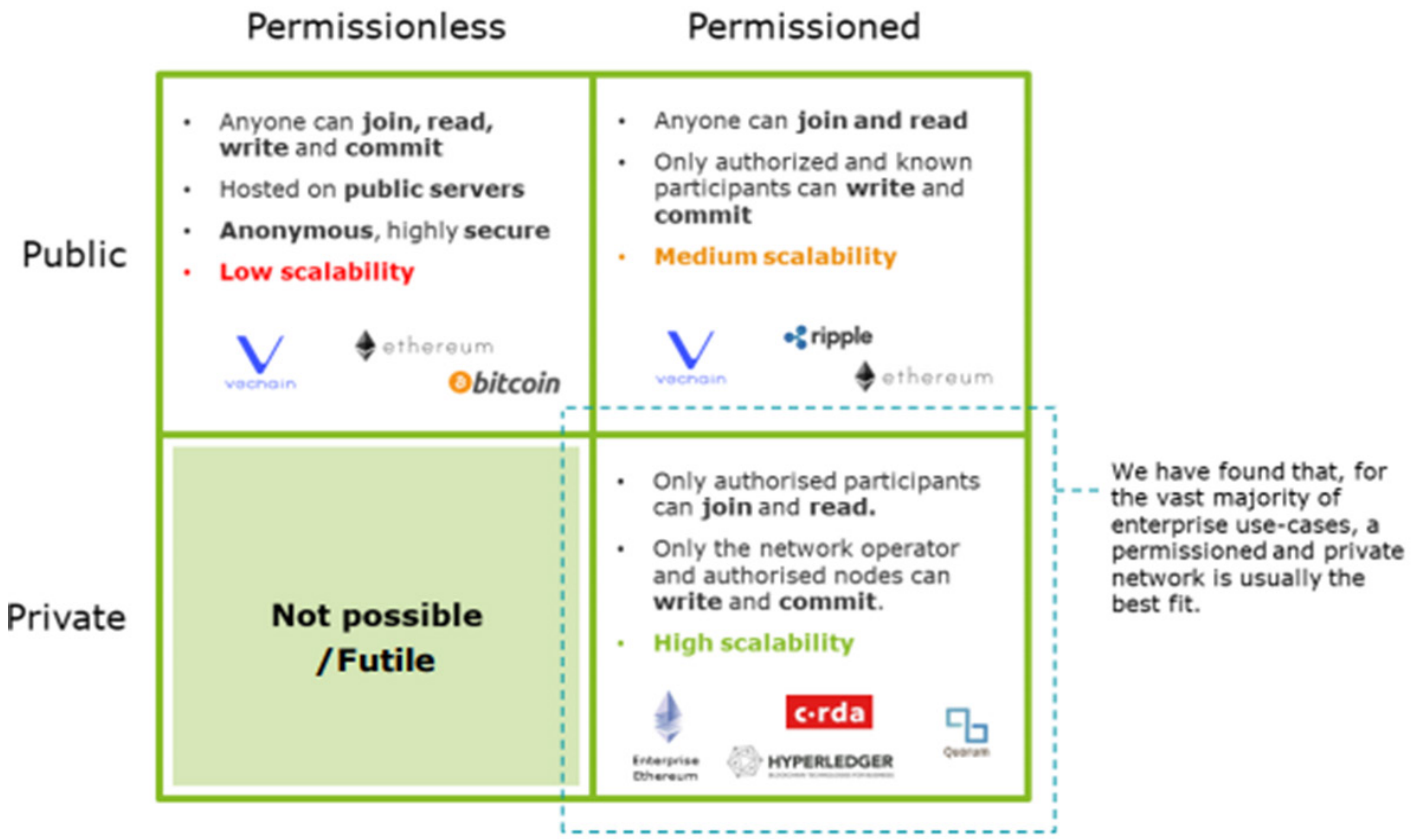



*Figure 2.*

Aron Laszka is an Assistant Professor in the Department of Computer Science at Houston and collaborates broadly with the NTT Cryptography and Information Security (CIS) Laboratories in Silicon Valley. Directed by NTT Fellow Tatsuaki Okamoto, their goal is to become the world's premier cryptography research laboratory.

Previously, Dr. Laszka served as a Research Assistant Professor at Vanderbilt University, aPostdoctoral Scholar at the University of California, Berkeley, and a Visiting Scholar at Pennsylvania State University. His research is funded in part by the U.S. National ScienceFoundation, the U.S. Department of Energy, and the U.S. Department of Homeland Security.

Since Professor Laszka's portfolio is much broader than what we can cover in this article, I asked him to focus on research areas he felt would significantly influence blockchain-based business models. With that, our conversation quickly narrowed down to four specific areas:

- An inability to accurately assess business risks associated with blockchain;
- The lack of a decentralized option for obtaining access to cloud computing services;
- Inefficient and wasteful blockchain protocols; and
- The need to improving information access during natural or human-made disasters.

## Selfish Blockchain Miners

The risk assessment topic squarely falls in the cybersecurity camp. Recent blockchain security incidents and cyber-attacks have centered on smart-contract vulnerabilities. *(Table 1)*

RECENT INCIDENTS AND CYPERATTACKS DUE TO SMART CONTRACT VULNERABILITIES

| Incident | Date | Amount | Vulnerabilities | Mitigation |
|---|---|---|---|---|
| King of Ether Throne | February 6–8, 2016 | 98 Ether | Insufficient gas send, Exception for external call not handled | Manually sending back the failed transactions to participants |
| Rubixi Vulnerability | April 2016 | 1.3k Ether | Wrong constructor name | |
| GovernMental | April 2016 | 1.3k Ether | Insufficient gas | ∼50 ETH transaction fee paid to raise gas limit |
| The DAO Attack | June 16, 2016 | 3.6M Ether | Reentrancy | Addressed with a fork to the Ethereum blockchain |
| Parity Wallet Hack | July 19, 2017 | 150k Ether | Missing access control | |
| Parity Wallet Freeze | November 6, 2017 | ∼500k Ether | Unprotected suicide | |
| POWH Coin Hack | January 28, 2018 | 2k Ether | Integer overflow | |
| BEC Token Attack | April 2018 | | Integer overflow | |
| Fomo3D Attack | August 22, 2018 | 10.5k Ether | Block stuffing | |
| SpankChain Attack | October 8, 2018 | 170 Ether | Reentrancy | |

*Table 1.*

Another critical security risk is the Selfish Mining Attack. Also known as a block withholding attack, it describes a malicious attempt to discredit blockchain network fairness. Selfish mining attacks occur when an individual intentionally withholds a successfully mined block from being broadcast to the rest of the blockchain network in hopes of gaining an unfair share of the blockchain mining profit. Both of these threats target the sustainability and resilience of blockchain solutions.

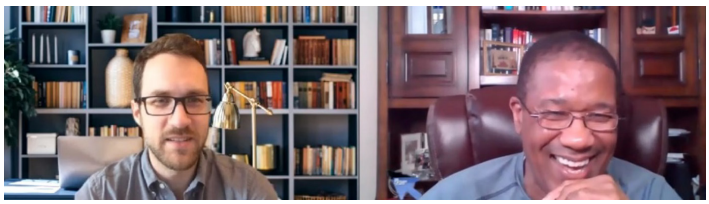
## The Decentralized Cloud

The second study area, decentralized access to cloud computing services, is focused on checking the monopolistic tendency of some global cloud service providers (CSP). Currently, some of these providers can withhold cloud computing services from any customer for any reason. If taken to the extreme, CSPs could control the economic viability of any company in any industry. Similar to how a governmental central bank has direct control of the money supply, cloud service providers could wield their power over the supply of cloud-basedInformation technology services. The counter to this threat is a decentralized alternative to cloud computing based on blockchain. Analogous to decentralized finance (Defi), a blockchain-based finance model that does not rely on central financial intermediaries.Decentralized cloud computing would use smart contracts on blockchains to manage the distribution of cloud-based services. This method of outsourcing computation services could completely replace cloud service providers. A research implementation by a consortium of universities, including the University of Houston, is already up and running.

## Proof-of-Work, Proof-of-Stake, and No Proof At All

The third area of focus for this article is improving blockchain efficiency by designing new blockchain protocols. Most of the current blockchain implementations use a proof-of-work(PoW) consensus mechanism. These deployments use a race between the blockchain nodes, or miners, to solve specific mathematical problems. Miner rewards differ, but on Bitcoin, the first miner to solve the mathematical problem receives freshly minted Bitcoin and a share of the network's transaction fees. Solving the problem verifies the new block of transactions, clearing its addition to the existing chain of previous blocks. Miners use brute force to solve the proof-of-work problems, ensuring that all have an equal chance to solve the problem.However, it also means solving the problem in a reasonable amount of time requires an exceptional amount of computational power, which drives a wasteful use of global energy resources.

A popular alternative consensus mechanism is called Proof-of-Stake (PoS). With this methodology, the creator of the next block of a chain is chosen via various combinations of random selection, wealth, or age (i.e., the stake), which enables more frugal use of energy resources.



A more efficient and simpler alternative to these approaches is to use permissioned blockchains in private settings, where the environment is composed of known entities. As blockchain governance assigns all voting rights, no participant needs proof. Dr. Laszka is working on designing blockchain protocols tailored for private environments, providing an alternative that is simple and efficient with the use of energy resources.

## Consensus Information

The final topic area has nothing to do with traditional business challenges. This research is on using blockchain consensus mechanisms to enhance information during natural and human-made disasters. Such an alternative could be extremely valuable if known trusted entities are destroyed. A decentralized blockchain platform could share, validate, and score information on its validity and accuracy. A compelling use case would be sourcing information from social media networks and scoring the "trust level" of that information using a blockchain-inspired consensus algorithm.

Learn more about how NTT CIS is building the future of blockchain by visiting https://ntt-research.com/cis/. The CIS lab sees cryptography and blockchain as essential to a SmartWorld. As every human being is touched by technology in ways beyond our everyday experience, security and privacy protection are at the core of our shared future. This is whyCIS engages with only the strongest and most dedicated researchers, like Dr. Aron Laszka, to focus on foundational cryptography and blockchain research problems that deliver long-term impact.

Kevin L. Jackson is a globally recognized Thought Leader, Industry Influencer, and Author. He has also been recognized as a "Top 5G Influencer", "Top Cloud Computing Expert", and "Top Digital Transformation Expert" by multiple sources. Mr. Jackson also provides integrated social media and management consulting services to many advanced technology companies. His most recent book on digital transformation, "Click to Transform", was ranked #1 on multiple Amazon bestseller lists.