Infusion Lawyers

Your Partner in Innovation

Blockchain Technology:
Can it really solve the problem of trust in a centralized world?

Blockchain Street. Published monthly.
Chain One: Block 1. *June 2020*

.... a walk into an emerging decentralized economy

Blockchain Technology: Can it really solve the problem of trust in a centralized world?

Distrust is a major problem in transactions.

For centuries, man has always distrusted man. In our personal and public life, we don't trust easily. Between kingdoms and fiefdoms, tribes and clans. Between slave merchants and slave agents. Between the church and the state. Between nations. Between the state and its citizens. Between Big Tech like Amazon, Facebook, Google, and their users. Distrust reigns, even between a husband and a wife who each needs a marriage contract to *trust* the other to keep his or her vows; yet just about anything could still happen to that marriage. Anything. And today, there is increasing distrust between man and robots. Distrust is virtually everywhere. There is a problem of trust.

Trust is invaluable, and it is scarce. If trust were a commodity, people would chase it with lots of money. If trust were a currency, it would trump any other currency in the world. But trust is neither a commodity like gold nor a currency like the Naira or Dollar. Trust is an intangible, priceless value. It is so highly-demanded in the society—and increasingly so—that the business of trust today is a trillion-dollar industry. From accountants to lawyers, bankers to brokers, insurers to agents, the business of trust has become the innovation of middlemen or trusted third parties whose *innovative* solutions have continued to help parties essentially manage distrust. A simple scenario: For Party A to do business with Party B, it goes through party C. This is a typical contract between two parties, such as for example, a Chinese manufacturer and a Nigerian distributor who each consults a lawyer to *safely* complete a transaction for delivery of goods to Lagos. In a

variant scenario, for Party A to enjoy access to object C, it must go through Party B. For example, a bank customer and his or her bank for the purpose of accessing financial services, including savings. What the bank, a central authority, does with the bank customer's savings is beyond his or her control.

Commercial and investment banks, trusted third parties, typically use people's hard-earned savings to offer loans and invest in mortgage securities. Where these loans and investments are high-risk, sooner or later, things go south. The banks declare bankruptcy. There is massive job loss. The economy becomes unstable. Panic. Dreading an impending contraction of the economy, the government deeps hands into the people's money—taxpayer's money—to bail out the eligible banks. The same government, for economic stimulus, then instructs the central bank to print more money. In economic matters such as this, political considerations must be factored in too. So, quantitative easing is preferred to tighter regulation. The side effects? Crisis. Economic stimulus soon stimulates inflation, consequently making the hard-earned money of the people lose value. Significant value. A familiar scenario? Indeed.

That was the Financial Crisis of 2008 in the United States. The crisis led to the global financial squeeze that left many people negatively affected. Seeing how financial institutions lost customers' money and the government simply printed more money, distrust set in. Dissatisfied, many people started demanding a currency that was not under the control of any central authority. Not the banks; not the government. Neutral money.

Enter a cryptocurrency in 2009. Decentralized and limited, this cryptocurrency was the opposite of fiat currency. Enter the people's money. Money without a central bank. Money without a government. Money without borders. Enter bitcoin ('b' in lower case, denoting the cryptocurrency, not the network, Bitcoin, with 'B' in upper case).

Decentralization, the key to trust.

Satoshi Nakamoto. This man, woman, or group believed, in 2008, that it was high time the problem of trust was solved. This time, not by trusting man, but by removing the need for trust in the first place.

The underlying technology behind the invention of bitcoin has been described as a distributed ledger technology that will change the way information is stored, managed, and transferred; a third-generation internet that will make exchange of anything of value possible; a trustless technology that will make for a peer-to-peer, secure, and transparent transaction without any trusted third parties. That underlying technology is blockchain.

Because blockchain is like that hardworking technical person in the team always working behind the scenes, the concept is not often easy to grab compared to other emerging

technologies. PwC hit this point squarely in 'Blockchain is here. What's your next move?', when it observed that "[b]lockchain's role as a dual-pronged change agent—as a new

Image source: Bitcoin Magazine

form of infrastructure and as a new way to digitise assets through tokens, including cryptocurrency—is not easy to explain. Think about other new technologies: users can try on virtual reality goggles or watch a drone take flight. But blockchain is abstract, technical and happening behind the scenes."

Blockchain is simply a digital book, whether private or public, laid open, not in one place, but shared on various computers. It is essentially a ledger but one with replicated copies. Each transaction is linked in a chronological order as a *chain of blocks*, with each block containing data of each completed transaction. Every transaction is timestamped, immutable, and practically irreversible. Blockchain is a cryptographically protected database for recording, processing, and transferring anything of value.

Because it is not built to rely on trusted third parties such as a bank or a government for example, blockchain is called a ''trustless technology''. Technically, this ''trustless technology'' is cryptographic or mathematical trust i.e. algorithms or sophisticated mathematical equations. Cryptography, the process of writing using various methods, helps us keep messages secret. With cryptography, secret keys are used to encrypt and decrypt data. This enables authentication and anonymity in our communications.

Although blockchain is often described as a ''trustless technology'', trust is still required. But as aptly captured by Don Tapscott and Alex Tapscott in their book, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business and the World*, this time ''[t]rust is established through mass collaboration and clever code rather than by powerful intermediaries like governments and banks." Trust in third parties,

especially in commerce, breeds distrust. Disintermediating transactions, therefore, logically brings trust, claims its proponents.

The weakness of the trust-based model especially in financial transactions was exactly the problem Satoshi Nakamoto, inventor of Bitcoin and author of the Bitcoin whitepaper 'Bitcoin: A Peer-to-Peer Electronic Cash System', came to solve with a peer-to-peer network, cryptocurrency, and incentive system. In the words of Satoshi Nakamoto:

> *"Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. ….With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party."*

So the question is this: What is needed to replace the trust-based model?

Satoshi Nakamoto asked the same question 12 years ago, with financial transactions in mind. Below is the answer proffered, developed, and gifted to the world in 2008:

> *"What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions."*

In other words, decentralizing trust is considered the solution to the problem of distrust, since distrust has become the evil of centralization or trust in third parties.

Decentralization is the (cryptographic) key to trust.

To be sure, blockchain is not the same as bitcoin.

Many people, especially in the early days—and we are still arguably in the early days—often confuse the two. Blockchain powers bitcoin. But it was the invention of bitcoin that brought about the creation of a peer-to-peer electronic cash system for which blockchain became a by-product. (This is why there is such a phrase as the 'Bitcoin blockchain').

Beyond the electronic cash system i.e. digital currencies or cryptocurrencies, blockchain can also be applied across other industries. So by way of analogy, you may think of blockchain as crude oil. Apart from the use of crude oil to fuel that engine, it is also applied in various industries for clothing, fertilizer, furniture, insulation, kitchen items, plastic, and others. In the same way, blockchain, today, is being applied in various industries as a solution to management of criminal justice, digital identities, dispute resolution, intellectual property rights, land registries, medical records, real estates, securities, supply chain, voting, and others.

Blockchain powers what is known as the token economy. Through tokenization, tangible assets like real estate and intangible assets like intellectual property are given digital representation. Blockchain-powered token economy enables rights to an asset to be converted into digital tokens or forms. The token economy continues to grow. This is bringing solutions to problems in various industries, from finance to supply chain; legal to health.

But blockchain is not—and never will be—a solution to everything.

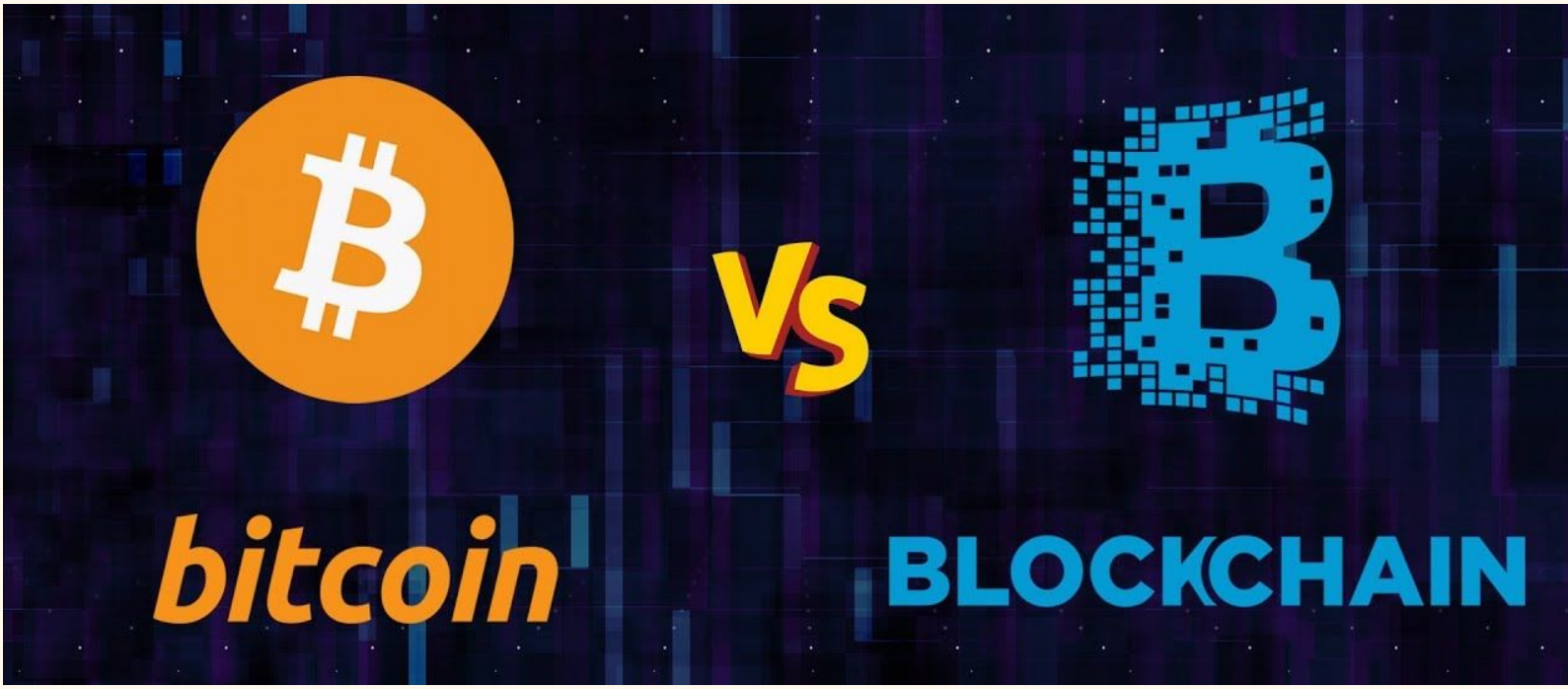

Image source: i.ytimg.com

That majority of blockchain projects that sought crowdfunding through initial coin offerings (ICOs) in 2017 failed is perhaps instructive. A recent study by Status Group reports that up to 80% of ICOs in 2017 were scams. Of course, not every failed project is a scam. Sometimes a project fails due to poor team, poor structure, poor strategy, poor advice, poor planning, poor execution, poor product, poor market, poor regulatory compliance, poor information or even poor idea. In a significant way, this massive failure resulted in distrust in blockchain technology, thus affecting mass adoption. Of course, people who understand how blockchain works know that it wasn't blockchain technology that wasn't the problem here, but rather, the mostly hyped blockchain projects. In most cases, these projects only had whitepapers detailing the big picture. It's the same way blockchain sites have been hacked since 2008.

Indeed, the human is literally the weakest link in the chain of blocks.

But hacking a blockchain site such as a cryptocurrency exchange or platform is different from hacking the blockchain itself. This is not to say that blockchains such as bitcoin, Ethereum, Litecoin, Zcash, etc are unhackable. Blockchain is hackable, with the right incentives.

Perhaps trustless technology is not completely trustless. Nothing is 100%, they say.

In a centralized world, decentralized trust struggles for mass adoption.

The reality is that we are neither in blocktopia nor cryptopia. In fact, there may never be such utopia in the powerful world of fiat. Our world is largely centralized. From central governments to central banks, centralized forces reign. They determine what constitutes trust and what doesn't. Trust is sovereignty—as far as it understands it—and no one is about to question the sovereign. Government, the supreme power, is the genesis trust that licenses trust to other trusted third parties, from banks to lawyers. Government is trust.

Blockchain: Blocked out and chained down by centralization?

Therefore, any trust model independent of the government or the government's trust licensees—including banks and other centralized institutions—will struggle for mass adoption. With the powerful instrument of regulation, government could snuff out life from any instrument of trust independent of it.

It should therefore not be a thing of wonder that today central governments will not accept bitcoin, a decentralized digital currency, as money. Similarly, central banks, largely government representatives, central banks will prohibit or restrict licensed financial institutions from having any dealing in cryptocurrencies. Though not declared illegal in most countries, including Nigeria, cryptocurrencies continue to suffer lack of recognition from the government and other central institutions.

Apart from lack of recognition by the government, there is also increasing criminalization, intimidation, and victimization of cryptocurrency or cryptocurrency-related endeavours around the world. In Nigeria, there have been cases of law-enforcement agents intimidating, victimizing, and criminalizing persons who deal in bitcoin and other cryptocurrencies, even though there is no law in Nigeria that makes dealing in bitcoin or other cryptocurrencies illegal. Also, a number of banks in Nigeria (who should know better) now easily hand over their customers to the police once a law-enforcement agency contacts them to freeze or restrict their customers' accounts, without any court order, as soon as there is an allegation of fraud. As long as the transaction is crypto-related, the burden of proof becomes less on the party alleging fraud while in some occasions, the constitutional right to innocence until proven guilty is thrown out the IPO's and prosecution's window. Even outside Nigeria, Google will suspend your YouTube account if you publish cryptocurrency contents or run cryptocurrency ads. And it's not just Google. Facebook implements the same ban on its platform. Similarly, other centralized platforms now implement crypto-is-prohibited-here policies. Just last week, Mailchimp suspended an account owned by a group that publishes an educational newsletter on blockchain, *cryptocurrency*, and FinTech. Over the weekend, a web-hosting company in Nigeria suspended a user's account when the user bought web hosting for a domain name containing the word 'crypto'. Cryptocurrency now seems even bigger than the elephant in the room. Meanwhile, traditional media (must) look away. After all, they too rely on the goodwill of the genesis trust—the government.

So it is gradually becoming a case where a ''trustless technology'' that was originally created to solve the problem of trust in our commercial lives is now bringing up a new level of distrust. Why? Largely because the genesis trust does not trust it. As long as this distrust remains or to put it better as long as there is a conflict between the genesis trust and the decentralized trust or trustless technology, tension will remain. This perhaps partly explains why there is rising regulatory tension in the blockchain/crypto space today—from privacy-troubled Facebook's earth-shaking Libra to Telegram's SEC-troubled TRON Blockchain.

But as soon as the same government realizes the advantages and power of digital currencies and how their revolutionary trust models could enhance or boost the trust people will have in the government's fiat currency, the same government begins to embrace innovations such as central bank digital currencies (CBDCs), for example. CBDCs are centralized digital currencies that will enable central banks to operate a fiat equivalent of decentralized cryptocurrencies. The People's Republic of China—which interestingly introduced the harshest and strictest regime against the proliferation of decentralized cryptocurrencies—is planning to launch its own CBDC.

Apart from CBDCs, there are other applications of the blockchain that the government could leverage on to become more efficient. From public contracts to public finance, cross-border trade and commerce to national identity management, transportation to customs, law enforcements to taxation, governments can turn things around. The Dubai government is already on this path. This is the future.

Way Forward: The future is the best of two worlds.

Image source: lse.ac.uk

Maybe—just maybe—what the world needs is neither a completely decentralized world nor a completely centralized world, but a world with the best of two worlds. A neutralized world.

Where do we start?

"I know that I know nothing", says the Socratic Paradox. That's where to start, otherwise the future may become increasingly empty of meaning in every aspect of human existence.

To get started on the journey to the future and not throw away the baby with the bathwater, each world needs learning, and unlearning too. Each world must learn from the other. Learning starts with humility. But between the centralized world and the decentralized world, who will demonstrate the humility required for the meaningful and fruitful learning that the world needs for a better, safer, and sustainable future?

Contact Person

Senator Ihenyen
Lead Partner and Head of Blockchain Practice
senator@infusionlawyers.com
+2348098764066 (WhatsApp)
info@infusionlawyers.com

Contact us at:
23 Water Corporation Drive,
Victoria Island,
Lagos

Telephone: +234816 995 1792

Email: info@infusionlawyers.com

Website: www.infusionlawyers.com

Infusion Lawyers is a virtual intellectual property and technology law firm for the knowledge economy and the digital age.

We are exclusive expert contributor (Nigeria Chapter) to the *Comparative Legal Guide on Blockchain 2020* in partnership with Dentons; exclusive expert contributor (Nigeria Chapter) to the *International Comparative Legal Guides (ICLG) on Data Protection 2019* in partnership with White & Case.

Infusion Lawyers
Your Partner in Innovation