How Blockchain Technology Could Change the World

by **Farhad Hussain**

Technical Specialist (e-government), Leveraging ICT for Growth, Employment and Governance Project, Bangladesh Computer Council (BCC)

Blockchain holds promise for being the latest disruptive technology, and this technology may find applications in areas as varied as transaction processing, identity authentication, government cash management, commercial bank ledger administration and clearing and settlement of financial assets.

We are familiarized with the term 'Bitcoin', an information technology breakthrough that facilitates both a secure, decentralized payment system and a tool for the storage, verification and auditing of information, including digital representations of value. A Bitcoin is also the intangible unit of account that facilitates the decentralized computer network of Bitcoin users. Bitcoin is not a company or a company product. Contrary to many news reports, it is not anonymous and was not built for bad actors, though bad actors have, at times, brought Bitcoin into the headlines.

Bitcoin is important because it represents a new means of forming consensus reliably and promptly across time and geography. As currently designed, Bitcoin is an open and transparent system that allows all users to easily come to an agreement on the authenticity of transactions and information stored on the network, all without the need to involve a trusted third party and without the concern of censorship of information or value transmitted across the network. Adaptations of the Bitcoin technology allow for different controls and access, but the basic premise of reliable and prompt network agreement regarding information (including value) is at the heart of this technology.

The underlying technology of Bitcoin is Blockchain, which is seen as the main technological innovation of Bitcoin. It stands as proof of all the transactions on the network. A block is the 'current' part of a Blockchain, which records some or all of the recent transactions, and once completed goes into the Blockchain as permanent database.

Blockchain is a revolutionary paradigm for the human world, the 'Internet of Individuals,' and it could also be the main driving force of the digital economy.

What is the Blockchain?

Blockchain could be described simply as being a way of storing the information of a transaction, between multiple parties in a trustable way. Recording, sharing, storing and redistributing its content in a secure and decentralized way. Being owned, run and monitored by everybody and without anyone controlling it and thus avoiding modifications or abuses from a central authority.

In short, it is a book-keeping or publicly available ledger, used to keep track of a transaction for trusting reasons, between two entities, being humans back then, and also with and between machines today. The modern financial version, it is that little room where we go and get our paycheck, called accounting, and plays a big role in the nature of the Blockchain and its first implementation with the crypto-currency Bitcoin.

Distributed Ledger - An Application of Blockchain Technology

A distributed ledger is essentially an asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within a network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes, or in some cases, seconds. The assets can be financial, legal, physical or electronic. The security and accuracy of the assets stored in the ledger are maintained cryptographically through the use of 'keys' and signatures to control what can be done by whom within the shared ledger. Entries can also be updated by one, some or all of the participants, according to rules agreed by the network. Underlying this is the Blockchain technology, which was invented to create the peer-to-peer digital cash Bitcoin in 2008. Blockchain algorithms enable Bitcoin transactions to be aggregated in 'blocks' and these are added to a `chain' of existing blocks using a cryptographic signature. The Bitcoin ledger is constructed in a distributed and permission-less fashion, so that anyone can add a block of transactions if they can solve a new cryptographic puzzle to add each new block. The incentive for doing this is that there is currently a reward in the form of ▸

History of Blockchain Technology

In the year 2008 Satoshi Nakamoto, an anonymous person, group of individuals or stand alone complex, published online a whitepaper describing the concept of a new technology, the Blockchain and its implementation in finance. It was the start of Bitcoin, a digital currency, using cryptography and decentralized protocol to control the creation and management of money in a horizontal way, checked by everyone and without a central authority, like banks and governmental agencies, controlling it.

A small drop into the ocean, mainly unnoticed at that time, but growing slowly over the years, all the way to now, ready to give birth to its first off-springs. It has the potential of having major impacts into the social, financial, juridical, scientific, and technological and innovation landscape.

To understand the Blockchain and what's hidden behind its core technology, a quick jump, back into the old days is necessary. The Blockchain by itself is nothing new and this is important to remember. Like any other innovation throughout human history, it was built on top of older bricks of ideas, over the shoulders of curious minds, explorers and innovators. In fact those bricks are quite old. So old, they are part of the fundamental code that gave birth to human civilization itself, and the ongoing update of its operating system.

twenty five Bitcoin awarded to the solver of the puzzle for each `block'. Anyone with access to the internet and the computing power to solve the cryptographic puzzles can add to the ledger and they are known as 'Bitcoin miners'.

Bitcoin is an online equivalent of cash. Cash is authenticated by its physical appearance and characteristics and in the case of banknotes by serial numbers and other security devices. But in the case of cash there is no ledger that records transactions and there is a problem with forgeries of both coins and notes. In the case of Bitcoin, the ledger of transactions ensures their authenticity. Both coins and Bitcoin need to be stored securely in real or virtual wallets respectively - and if these are not looked after properly, both coins and Bitcoin can be stolen. A fundamental difference between conventional currency and Bitcoin is that the former are issued by central banks, and the latter are issued in agreed amounts by the global 'collaborative' endeavor that is Bitcoin. Cash as a means of exchange and commerce dates back millennia and in that respect there is a lineage that links cowry shells, hammered pennies and Bitcoin.

But this article is not only about Bitcoin. It is also about the algorithmic technologies that enable Bitcoin and their power to transform ledgers as tools to record, enable and secure an enormous range of transactions. So the basic Blockchain approach can be modified to incorporate rules, smart contracts, digital signatures and an array of other new tools.

Distributed ledger technologies have the potential to help governments to collect taxes, deliver benefits, issue passports, record land registries, assure the supply chain of goods and generally ensure the integrity of government records and services. For the consumer of all of these services, the technology offers the potential, according to the circumstances, for individual consumers to control access to personal records and to know who has accessed them.

Existing methods of data management, especially of personal data, typically involve large legacy IT systems located within a single institution. To these are added an array of networking and messaging systems to communicate with the outside world, which adds cost and complexity. Highly centralized systems present a high cost single point of failure. They may be vulnerable to cyber-attack and the data is often out of sync, out of date or simply inaccurate.

In contrast, distributed ledgers are inherently harder to attack because instead of a single database, there are multiple shared copies of the same database, so a cyber-attack would have to attack all the copies simultaneously to be successful. The technology is also resistant to unauthorized change or malicious tampering, in that the participants in the network will immediately spot a change to one part of the ledger. Added to this, the methods by which information is secured and updated mean that participants can share data and be confident that all copies of the ledger at any one time match each other.

But this is not to say that distributed ledgers are invulnerable to cyber-attack, because in principle anyone who can find a way to 'legitimately' modify one copy will modify all copies of the ledger. So ensuring the security of distributed ledgers is an important task and part of the general challenge of ensuring the security of the digital infrastructure on which modern societies now depend.

Governments are starting to apply distributed ledger technologies to conduct their business. The Estonian government has been experimenting with distributed ledger technology for a number of years using a form of distributed ledger technology known as Keyless Signature Infrastructure (KSI), developed by an Estonian company, Guardtime.

KSI allows citizens to verify the integrity of their records on government databases. It also appears to make it impossible for privileged insiders to perform illegal acts inside the government networks. This ability to assure citizens that their data are held securely and accurately has helped Estonia to launch digital services such as e-Business Register and e-Tax. These reduce the administrative burden on the state and the citizen. Estonia is one of the 'Digital 5' nations, of which the other members are the UK, Israel, New Zealand and South Korea. The business community has been quick to appreciate the possibilities. Distributed ledgers can provide new ways of assuring ownership and provenance for goods and intellectual property. For example, 'Everledger' provides a distributed ledger that assures the identity of diamonds, from being mined and cut to being sold and insured. In a market with a relatively high level of paper forgery, it makes attribution more efficient, and has the potential to reduce fraud and prevent 'blood diamonds' from entering the market.

An important challenge for this new set of technologies is communication of its significance to policymakers and to the public. The first difficulty in communication is the strong association of Blockchain technology with Bitcoin. Bitcoin is a type of crypto-currency, so called because cryptography underpins the supply and tracking of the currency. Bitcoin creates suspicion amongst citizens and government policymakers because of its association with criminal transactions and 'dark web' trading sites, such as the now defunct Silk Road. But digital crypto-currencies are of interest to central banks and government finance departments around the world, which are studying them with great interest. This is because the electronic distribution of digital cash offers potential efficiencies and, unlike physical cash, it brings with it a ledger of transactions that is absent from physical cash.

In practice, there is a broad spectrum of distributed ledger models, with different degrees of centralization and different types of access control, to suit different business needs. These may be permission-less ledgers that are open to everyone to contribute data to the ledger and cannot be owned; or permission requiring ledgers that may have one or many owners and only they can add records and verify the contents of the ledger.

The key message is that, by fully understanding the technology, government and the private sector can choose the design that best fits a particular purpose, balancing security and central control with the convenience and opportunity of sharing data between institutions and individuals.

As with most new technologies, the full extent of future uses and abuses is only visible dimly. And in the case of every new technology the question is not whether the technology is 'in and of itself' a good thing or a bad thing. The questions are: What is the application of the technology? What is the purpose? And how should it be applied and with what safeguards?

Identity Authentication – An Application of Blockchain Technology

The need for Blockchain based identity authentication is particularly salient in the internet age. While there are somewhat imperfect systems for establishing personal identity in the physical world, in the form of Social Security numbers, drivers' licenses and even passports or national identity ▸

cards, there is no equivalent system for securing either online authentication of our personal identities or the identity of digital entities. Facebook accounts, now often used as login for different digital applications, and media access control (MAC) addresses, may come close, yet both can hardly function as trustworthy forms of identification when they can be changed at will.

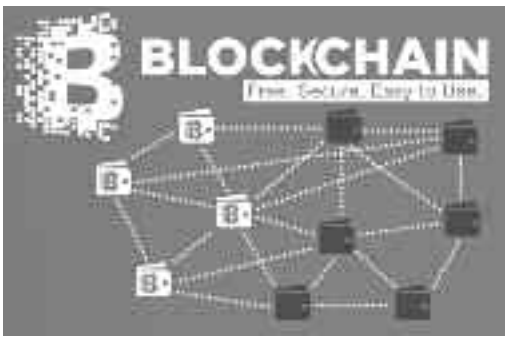
So while governments can issue forms of physical identification, online identities and digital entities do not recognize national boundaries and digital identity authentication appears at first look to be an intractable problem without an overseeing global entity. Yet it would be incredibly difficult, perhaps downright impossible, to establish a global entity overseeing digital identities given that there is common backlash against even national identity cards. Blockchain technology may offer a way to circumvent this problem by delivering a secure solution without the need for a trusted, central authority.

Several Blockchain startups are looking to use Blockchain for online identity. A 'ShoCard', for example, is a digital identity that protects consumer privacy. 'ShoCard' strives to be as easy to understand and use as showing a driver's license; and simultaneously be so secure that a bank can rely on it. The key is that the 'ShoCard' Identity Platform is built on a public Blockchain data layer, so as a company it is not storing data or keys that could be compromised. According to 'ShoCard' all identity data is encrypted, hashed and stored in the Blockchain, where it cannot be tampered with or altered. A start-up in a similar vein that bridges the gap of both human and digital entities is 'Uniquid'. 'Uniquid' allows for the authentication of devices, cloud services, and people. Its aim is to provide identity and access management of connected things, as well as humans, utilizing biometric information for the latter.

One implication of this trend for financial institutions is a growing need for improved identity authentication, particularly for compliance purposes. For compliance, Blockchain technology may enable financial institutions to better verify customers during the on-boarding process known as Know Your Client (KYC), and to better verify parties in a transaction and the transactions themselves to prevent fraudulent activities and more effectively comply with anti-money laundering (AML) regulation. Better AML/KYC systems can be used to help extend banking services to the world's 2 billion unbanked.

Privacy-Preserving Identity on Permissioned Blockchain

Increased transparency does not necessarily mean the end of privacy. Some cryptographic identity schemes offer strong privacy protection through identity anonymity and unlink-ability of transactions. A new model for privacy-preserving identities is needed if Blockchain systems are to operate at a global scale. It must allow entities in the ecosystem to (a) verify the 'quality' or security of an identity, (b) assess the relative 'freedom' or independence of an identity from any given authority (e.g. government, businesses, etc.), and (c) assess the source of trust for a digital identity. Yet, a part of identity is derived from physically identifying a person, and part is from their behaviors. As we allow for behavioral identity models, how can systems address people who behave inconsistently - perhaps, a good person who behaves badly sometimes? As people adopt digital avatars or personae, what is the identity that is being validated?



Massachusetts Institute of Technology (MIT) researchers have proposed 'ChainAnchor', a new means of establishing a trusted, yet privacy-preserving, identity. Designed for permissioned Blockchain (such as those now being developed by several banks and trading platforms), the 'ChainAnchor' architecture adds an identity and privacy-preserving layer above the Blockchain. An anonymous identity verification step allows anyone to read and verify transactions from the Blockchain but only anonymous verified identities can have transactions processed. Economic incentives, similar to those used in mining itself, help create resiliency in the system to defend against attacks and preserve the integrity of the identity network.

This system creates the potential for compliance with AML/KYC regulations without compromising the individual identities of counterparties in a transaction.

Conclusions

Blockchain has a transformative potential in terms of businesses and societal functions. The technology could in many areas allow the transition from centrally controlled hierarchical structures to decentralized peer-to-peer organization and interactions. Global network-distributed consensus algorithms can eliminate the need for trust between parties, offering the Internet an additional functionality level with significant implications.

Blockchain puts every user on the same level playing field as a peer in the network. It can be regarded as a global spreadsheet, or an incorruptible digital ledger, where not only financial transactions but also ownership rights and legal documents can be stored. Blockchain technology can also contribute to improved mechanisms for governance. If public institutions enable the registration of property titles, business licenses, educational degrees, birth certificates, and so forth utilizing Blockchain technology, citizens could perform transactions that today require lawyers, notaries, banks, and government paperwork.

As the technology is still in its nascent stages, regulations need to both enable innovations based on Blockchain and to restrict potential illicit use. The government agencies that at first point of departure could benefit from monitoring the developments are financial regulatory bodies and tax authorities. With the current momentum and development trend in Blockchain technology, nations that remove barriers for experimentation around smart contracts and peer-to-peer solutions may benefit from the progress of entrepreneurs and ventures built on top of Blockchain. Countries that hinder its development may lose out on the first-mover advantage to jurisdictions that are more permissive.

Blockchain technology is complicated, requiring an advanced understanding of computer science, peer-to-peer network technology, cryptography, and economics. Few people in the world currently have a good understanding of how this technology functions; systems and nations that might benefit the most lack the capacity in many cases to take full advantage of the technology's potential. The technology is free and open for anyone to use, build upon, improve, and come up with new applications and use cases. It will likely take many years, and many improvements to the user experience are needed, until we see mainstream adoption of more mature Blockchain technology ■