Blockchain/Distributed Ledger Technologies: Where They Came From, Where They Are Heading

Author Shahid Yusuf

By Shahid Yusuf

A need to record transactions and contracts, as well as to maintain an inventory of goods, is of long standing. Five thousand years ago, merchants in the Sumerian city Uruk were inscribing a log of transactions and tracking inventories on clay tablets using cuneiform script. Record-keeping took a giant step forward with the creation by Venetian merchants of double entry book-keeping in the 14th century. This was codified by Luca Pacioli who published a major survey of mathematics in 1494 that included a 27-page description with examples of double entry book-keeping and its utility (*Double Entry, How the Merchants of Venice Created Modern Finance*, by Jane Gleeson-White, W.W. Norton, New York, 2011). The advent of Gutenberg's movable type press facilitated the reproduction of Pacioli's opus and the diffusion of knowledge about book-keeping throughout the European and Middle Eastern business communities. A decline in the cost of paper once the use of wood pulp became widespread further incentivized record-keeping. And double entry book-keeping became firmly entrenched in business practice following the Industrial Revolution and the globalization of trade starting in the latter part of the 19th century.

Fast forward to the last quarter of the 20th century that has witnessed the progressive computerization of transactions and the abandonment of paper records. The Internet and digitization has also substantially widened the scope for innovation. In particular, data gathering, its management and analysis, the recording of transactions, and the entry and execution of contracts, to name just a few, can all be done far more efficiently and swiftly using computer files. But one thing did not change. As with paper ledgers, most if not all financial transactions still involve an intermediary, frequently a bank or the state, to maintain records, vouch for their accuracy, safeguard their integrity and help consummate a transaction. Thus, whenever a transaction involves an intermediary, all parties to a transaction need to put their trust in the integrity of the intermediary. Not all intermediaries can be trusted to keep sound records or to fulfil the terms of a contract to the letter, hence the search for a technology that would dispense with intermediaries while preserving an inviolable record of transactions and of contracts.

Satoshi Nakamoto's seminal nine-page white paper "Bitcoin: A Peer-to-Peer Electronic Cash System" issued in May 2009 — the culmination of 18 months of software engineering — and the subsequent launch of Bitcoin focused attention on distributed ledger technologies (DLTs) that can do away with intermediaries yet provide a potentially tamper-proof record of transactions. Nakamoto (a pseudonym of an individual or a team of researchers who devised the blockchain protocol for computers participating in the Bitcoin network) did not invent a new technology; instead he combined several existing technologies to arrive at a permissionless blockchain that could serve as the basis for a viable cryptocurrency, Bitcoin. The elements that underpin DLTs were under development since the 1980s. Public key cryptography and cryptographic signatures emerged in the early 1980s; other elements such as cryptographic hash functions, the hash chain used for proof of work, cryptographic time stamps, the notion of a shared open repository of transactions, and peer-to-peer (P2P) networks all appeared in the 1990s. Nakamoto's blockchain strings together cryptographic blocks of transactions that are time stamped using a proof of work protocol for arriving at consensus among network participants.

The rest of this paper briefly unpacks the working of blockchain/DLTs, examines their merits and weaknesses and discusses their current applications and future uses.

Bitcoin's Blockchain

A convenient entry point into the world of DLTs is Bitcoin. By tracking a Bitcoin transaction one can gain an understanding of how a blockchain works. To start with, Bitcoin's blockchain is permissionless, meaning that it is open access. Anyone with a computer can join and all participants if they so choose can maintain copies of the ledger recording each and every transaction — blockchain is a massively distributed ledger. Currently, centralized networks that store information provide clients with services. The blockchain used by Bitcoin works on the P2P principle whereby each computer doubles as both server and client and none is a central repository. In a distributed system each node (computer) or a group of nodes (computers) holds a copy of the database. Furthermore, because the network is decentralized, there is no "single point of failure" — i.e. it is more resilient, more expensive to attack and, because of the numbers involved, more likely to discourage collusive behavior.

Bitcoin purchasers first download a Bitcoin wallet from one of the websites such as Blockchain.info. They can then acquire Bitcoin from one of the exchanges such as Coinbase or Xapo, Bitstamp, or Kraken using a standard payment method such as a debit card.

The worth of a blockchain comes into focus when the holder of Bitcoin enters into a transaction involving the transfer of coin to another party. Each participant has a private key that serves to embed a personal digital signature in a transaction. Bitcoin's blockchain consensus protocol then requires that the transaction be validated by all participating nodes of the system — that is the basis of trust. The process of verification using cryptographic tools ensures that the individual entering into a transaction is credentialed and in possession of the Bitcoin to be transferred to the other party. It also eliminates the "double spend" risk that a cryptocurrency is used twice through a falsification of the records.

This transaction plus others are then consolidated into a "block" by a subset of the nodes, the ones that do the "mining", which is the process by which new blocks are added to the chain. Each block includes transactions that have been validated by the network. It is time stamped, contains a cryptographic link to the previous block and requires miners to find an answer to a complex mathematical puzzle generated by the Bitcoin program. This "proof of work" by miners is Nakamoto's key innovation. Its purpose is to finalize transactions, render them irreversible and eliminate or minimize the risk of tampering. Mining entails the application of energy intensive computing power using customized ASICs, many produced by Bitmain, a Chinese company and graphics processing units (GPUs) produced by Nvidia Corp. and Advanced Micro Devices Ltd. (AMD).

Miners take a hash of the data in the block and combine it with a random number and use a "hash function" to generate a result that falls within a certain range. Miners have to guess the random number and keep trying using other random numbers until they arrive at the winning hash that starts with a pre-established string of zeroes and cryptographically references all the data in the block. The winner announces the new block to other miners who then add the block to the chain. The update of the ledger is shared with all nodes. The winning miner is compensated for the work performed with newly minted Bitcoin keyed to the number of transactions in the block. It is this proof of work that ensures the workability of the synchronized consensus protocol and it accounts for the success of a decentralized blockchain that has dispensed with a trusted intermediary.

Every new block contains the hash of the previous block, hence anyone modifying the contents of an earlier block changes and invalidates the hashes of all blocks that follow. To hide evidence of tampering, the hashing and chaining together of all subsequent blocks must be redone and completed before another miner adds a new block. This is theoretically possible by a miner able to marshal a great deal of computing power, but as the blockchain expands it becomes increasingly difficult.

Bitcoin's Progeny & Blockchain Innovation

Bitcoin not only triggered the cryptocurrency mania, it also highlighted the utility of blockchains and DLTs for uses other than the issuance of currencies. Although Bitcoin and its cousins are unlikely to displace fiat currency issued by the state — because no cryptocurrency has proven to be a store of value or is widely accepted as a medium of exchange and a unit of account — the number of cryptocurrencies has mushroomed. To overcome the store of value problem, fully (or partly) collateralized cryptocurrencies such as Tether pegged one-to-one to the dollar are increasingly popular. Some such as Bitcoin Cash and Litecoin have emerged following a "hard fork" from Bitcoin. A hard fork involves a permanent switch to a different blockchain protocol software that is adopted by participating nodes. In the case of Bitcoin Cash, the advantage to users is that it permits larger transactions. Litecoin speeds up transactions to four times the 3-4 transactions per second rate achieved by Bitcoin (up to a maximum of 60). However, both these cryptocurrencies and others such as XRP (1,500 transactions per second), NEO and EOS are more centralized and use different consensus protocols. Ripple uses XRP Ledger settlement technology, the Chinese cryptocurrency NEO employs a "delegated Byzantine fault tolerance" protocol so as to attain speeds approaching 10,000 per second, and EOS relies on a consensus protocol based on "proof of stake" that requires users to establish their trustworthiness by virtue of the amount of cryptocurrency that they hold, for example. Proof of stake does not achieve security through the "burning of energy" as with Bitcoin mining but by demanding that those on the network lock up and put their capital at risk, maintain their nodes and take precautions to protect their private key.

Arguably of greater longer term significance than the standard cryptocurrency-based networks is Ethereum. It too uses a distributed permissionless blockchain protocol similar to that of Bitcoin but is piloting a proof of stake protocol (Casper FFG) that initially involves a parallel functioning of both protocols (proof of work and proof of stake), with proof of stake becoming the sole system protocol two years hence. In addition to issuing a cryptocurrency called Ether, Ethereum also includes a programming language (Turing Complete) that permits users to embed "smart contracts" into the blocks. According to Vitalik Buterin, the developer of Ethereum, the blockchain functions like a large computer — known as the Ethereum Virtual Machine (EVM) — that stores and executes contracts between two or more parties. Contracts executed in the EVM can include the reading of data, computations, and establishing links with other contracts. These functions are simultaneously executed by each of Ethereum's nodes. In the process, much energy (or "gas") is consumed and paid for by contracting parties via Ether and deducted from their accounts. The price of gas varies dynamically and the system places an upper limit on the amount of gas that can be used for each transaction.

Blockchain in the Making

Blockchain technology is still in its infancy with many innovations to come that will tackle a number of salient concerns. Eight deserve to be singled out:

First, when a blockchain/DLT is used, whether for cryptocurrency transactions or others, data privacy and confidentiality can be compromised when the data is linked to a particular party whose identity could be revealed to all network nodes — for example, when a transaction makes known an individual's title to a property. Many organizations are unwilling to put valuable data on a widely accessed blockchain. Moreover, although transactions for some blockchains are in theory anonymous, the record is available, permanent and trackable. Thus, depending on how easy it is to compromise a node in a permissionless blockchain (and thereby access data), the latter can be more or less secure than a permissioned one that limits the number of users.

Second, blockchain cannot verify the accuracy of information that is entered, for example with respect to property ownership. It can only minimize the risk that the information will be tampered with. Likewise, a permissionless, distributed blockchain can instruct that a contract be executed but it cannot enforce a contract. A breach of contract has to be remedied through the intermediation of the legal system.

Third is the vulnerability to attack and to the risk of theft. Since cryptocurrencies first appeared, it is estimated that $15 billion worth of coins have been stolen from exchanges — $800 million worth of cryptocurrencies were stolen in Asia during the first half of 2018 alone. One of the heists, amounting to $400 million, led to the collapse of a major Japan-based exchange called Mt. Gox. Blockchain's intrinsic security derives from the widespread distribution of copies of transactions and the proof of work protocol. The bigger the network, the harder it is for any one party to mobilize the computing power to subvert the entire system. But it is not beyond the realm of possibility — and becoming easier. Attack cartels can coalesce and marshal the computing muscle using their own computers and by renting others. Once the attacker has acquired hashing power that is more than one half that of the entire network, the stage is set for a "51% attack" that can alter transactions, modify the protocol, double spend crypto currencies and hold accounts to ransom by making their contents unusable. Smaller coins and exchanges are at greatest risk but Bitcoin and Ethereum are by no means invulnerable. According to research by Ittay Eyal and Emin Gün Sirer ("Majority is not enough: Bitcoin mining is vulnerable", Communications of the ACM, 2018), the Bitcoin mining protocol is not necessarily incentive compatible: a minority of miners who create a Selfish Mining Pool can pursue strategies that enlarge their share of the revenues earned at the cost of honest miners. Ethereum is no different, with well over half of the mining being conducted by three operations.

Looking ahead, another problem looms, which is the advent of quantum computing that will undermine cryptography in current use by making it easy to break cryptographic locks. As Vitalik Buterin states, "Quantum computing will make a lot of cryptography that's used in modern times just not work anymore. Digital signature algorithms won't work anymore. Public key encryption won't work anymore. Zero-knowledge proof SNARKS (Succinct Non-interactive ARgument of Knowledge), software for privacy protection, won't work anymore. The good news is that for everything that doesn't work anymore, people have already come up with replacements for them over a decade ago. You have hash-based signatures, you have virtual currency STARKS for zero-knowledge proofs, you have fancy elliptic curve isogeny-based public key encryption. So I think it will force a transition, but ultimately, we do know how to adapt. The cryptocurrencies that will suffer the most are just the ones whose governance is the most stalled and dysfunctional and won't be able to figure anything out in time." (*Cryptoeconomics and Markets in Everything (Ep. 45)* at https://medium.com/conversations-with-tyler/vitalik-buterin-tyler-cowen-cryptocurrency-blockchain-tech-3a2b20c12c97).

Fourth, large permissionless blockchain/DLT networks confront governance issues that make it difficult to resolve problems that arise and to promote the further development of the network. Governance involves three sets of participants: developers, miners and users, each with differing interests. Coordination of the decision-making process involving thousands of members whether online or offline can be time intensive, slowing down necessary changes and innovations that can improve network capabilities. Because there are few mining pools, they can form coalitions, increase transaction costs and dominate decision-making to advance their own interests. Developers also have a stake in the network but as they do not receive a financial reward from improving network capabilities — and can be bribed by miners — they are less likely to be proactive. Bitcoin that relies on offline communication has suffered from a cumbersome and centralized governance structure that has inhibited desirable innovation. Any Bitcoin Improvement Proposals (BIP) must be approved by a bloc of participants commanding 95% of mining power. Ethereum is attempting to reduce the risk of excessive centralization by shifting to "proof of work" that will increase the voting power of coin holders and counterbalance that of miners. The network is also attempting to promote innovation by encouraging new developers to play a more active role, and lessening its reliance on Ethereum's creator. Other networks are experimenting with various forms of on-chain and off-chain governance so as to maximize the participation of users and at the same time permit the rapid testing and incorporation of changes to the code when the need arises or to facilitate network enhancing innovation. The speed with which a network adjusts its governance mechanisms and responds to challenges is a source of competitive advantage in a marketplace crowded with blockchain-based coins.

A fifth issue faced by blockchain networks is the difficulty of scaling a network while retaining the benefits of decentralization and security. As the number of users and transactions increases, block sizes tend to grow unless hard capped, which in turn raises energy costs and mining fees, especially during peak periods. Furthermore, P2P verification of each transaction slows down the creation of blocks. Bitcoin, for example, builds a block every 10 minutes. A point is reached when a blockchain network becomes too large, unwieldy and slow to be competitive, at which point a hard fork is needed that spawns a new and independent system with a differentiated software. A hard fork from Bitcoin led to the creation of Bitcoin Cash. These hard-forked creations are tackling the problem of transaction size and scalability in a variety of ways: by trimming the data in each transaction; by using software called SegWit to compress transactions; by conducting verification through a separate channel; by employing the Lightning P2P Network that sits on top of the Bitcoin blockchain and permits micro transfers between users; and by using a technique called sharding that enlarges throughput by partitioning the network with nodes in each of the shards that are created processing a subset of the transactions. Bit by bit, the constraints are being eased but the problem of scalability is many innovations away from being solved.

Energy use by cryptocurrency miners who need to demonstrate proof of work is a sixth issue confronting governments. As of 2018, Bitcoin miners were consuming an estimated 20 terawatts of power globally or about 0.1% of total global electricity. When other currencies are included, the share of global consumption is in excess of 0.5%. A variety of innovations could contain the increase as could rising energy fees and regulations, but when combined with the energy consumed by data centers, the implications of this technology for power use and GHG emissions are non-trivial.

The use of cryptocurrencies for the purposes of money laundering or evading government controls is a seventh worry — albeit specific to currencies. The use of bitcoins on the darknet TOR-enabled platform Silk Road aroused concerns that cryptocurrencies anonymously acquired and traded on shadowy exchanges could provide cover for criminal activity. Although the threat of money laundering and the financing of covert activities using cryptocurrencies remains, evidence that they are being widely used for money laundering is scarce. Bitcoin, for example, could facilitate money laundering because it is portable and safe from confiscation, and the public address of Bitcoin wallets is anonymous; but every transaction is monitored and recorded by the blockchain. The real problem for a money launderer arises when an attempt is made to convert Bitcoin into fiat money at a coin exchange such as Gemini. Law enforcement officials tracking a Bitcoin address suspected of engaging in illegal activity can demand that the exchange reveal the identity of the account holder and have the authority to confiscate the proceeds of the Bitcoin conversion into cash. But loopholes remain. For example, when either Bitcoin or Ethereum is converted by a willing online exchange into an untraceable cryptocurrency such as Monero, it disappears from the radar of regulators and can subsequently resurface as clean Bitcoin on yet another exchange that is not especially scrupulous in monitoring suspicious transactions.

Finally monetary authorities and regulators are concerned as to the implications of cryptocurrencies for monetary policy and financial stability. While this has stirred much debate and considerable research — including into the issuance of digital fiat currency by central banks — as yet there appears to be little likelihood that cryptocurrencies, even collateralized ones, will overshadow fiat money. Moreover, regulators are busy devising rules to control the issuance and circulation of cryptocurrencies, trading on exchanges and Initial Coin Offerings (ICO). China has taken the hardest line and other countries are also adopting a cautious attitude.

DLTs for All Seasons

Worries over cryptocurrencies do not undermine the potential utility of blockchain and other DLTs in safeguarding information and reducing administrative costs. These technologies have many uses beyond the narrow realm of cryptocurrency. However, it is likely that there will be more permissioned DLTs than permissionless ones, with one or a few trusted intermediaries responsible for determining design, managing the ledger, validating its integrity, and resolving disputes (*Blockchain and Economic Development: Hype vs. Reality*, Michael Pisa and Matt Juden, CGD Policy Paper, Washington, DC, July 2017). This goes against the grain of Nakamoto's original protocol, which attempts to strip out the trusted intermediary, and is the likely route that the mainstreaming of DLTs might follow.

Among the many uses of blockchain/DLT, the following deserve prominence:

Securing and protecting property rights to digital products and content and to land. Blockchain can establish and safeguard ownership history by distributing it across a network. With landed property, the transferring of records onto a blockchain would be most effective where a reliable system for recording land rights already exists. This would ensure the accuracy of the information entered.

Blockchain enabled e-voting already in use in a few countries such as Estonia could empower voters and protect against the all too frequent instances of fraud, especially in developing countries. These systems would need to be tailored to the specifics of voting systems and electorates, and for the blockchain to provide maximum security, e-voting would need to be widespread.

Blockchain-based user-centric digital ID systems that allow individuals more control over personal data while at the same time reducing the risk of a central repository being hacked. Michael Pisa makes the case for the storing of certified information provided by a trusted authority on a blockchain-linked digital wallet (*Reassessing Expectations for Blockchain and Development*, July 10, 2018, https://www.mitpressjournals.org/doi/abs/10.1162/inov_a_00269). But he notes that buy-in by governments and other organizations would be critical and the loss of a key by an individual would entail a rebuilding of a digital identity.

Registering, certifying and tracking goods moving through supply chains could be rendered much more efficient and rigorous with the help of blockchains. Moreover, the recording of transactions at every juncture could also streamline fulfillment and settlement of dues. With the help of Everledger, companies trading in diamonds can follow the path a diamond takes from the mine to a retail outlet and in the process circumvent problems of documentation and insurance fraud.

Permissioned DLTs are likely to be favored by users who wish to restrict access to data and enjoy a degree of mutual trust. Providers of financial and non-financial services that engage in a multitude of transactions including payments, settlement of accounts and clearing arrangements have already begun experimenting with DLTs. The R3 consortium's Corda platform is geared towards companies that are looking for DLT solutions in the interest of greater system resilience, to automate certain processes, to develop new lines of business and much else.

Healthcare is another sector that could profit from DLTs to maintain patient health records, while allowing patients to exercise more control over their data. A system called MEDREC devised by the Massachusetts Institute of Technology uses a blockchain that does not store patient records that remain on provider databases, but it facilitates the granting of permission by patients to access the data. DLTs can help the pharmaceutical industry protect IP and the integrity of its supply chain which would reduce the penetration of counterfeit drugs. DLTs also have the potential of enhancing the efficiency of drug distribution.

Last but not least, there is the public sector that in most countries could benefit from DLTs that improve inter-departmental coordination and the sharing of data, allow departments to track transactions and thereby minimize fraud, and open the door to the use of smart contracts, which would reduce bureaucratic delays and red tape.

Conclusion

In their foreword to the 21st Geneva Report on the World Economy (CEPR Press, 2018), Tessa Ogden and Charles Wyplosz comment on the role that blockchain technology can play in the sphere of finance and in other areas. They state, "Despite its infancy, blockchain technology presents an opportunity to fundamentally transform the way financial markets work. The challenge is to reduce the cost of trust, to protect against criminal interference — money laundering and terrorism, for instance — and to ensure that the technology is appropriately adopted, utilized and governed. When and if these problems are solved, blockchains could provide enormous economic, social, and political benefits to society."

In less than a decade since they appeared, the value of crypto assets amounted to $193 billion on Sept. 1, 2018 — with tokens other than bitcoin accounting for 56%. Three thousand ICOs have raised over $20 billion and 200 crypto coin exchanges have been established. There is also plenty of churning and failures as the new technology enters adolescence. A majority of ICOs have failed the market test or are on the brink. Clearly, in the financial sector and in other fields DLTs need more time to innovate, improve and prove their worth. Furthermore, at least in the realm of finance but also in other areas, blockchain/DLTs need to be more fully brought within public policy and legal frameworks. They cannot solely be governed by the rules of code but need to be pulled within the ambit of traditional systems of control that establish liability and responsibility. All participants must remain subject to the rule of law. They cannot coexist in a cyber sphere governed only by code (*Blockchain and the Law: The Rule of Code* by Primavera De Filipi and Aaron Wright, Harvard University Press, Cambridge MA, 2018).

That said, the intensity of innovation — and numbers of blockchain/DLT patents filed — suggest that these technologies could spread across and enhance the efficiency of a range of activities from finance to agriculture. Like cloud computing, blockchain could in its own small way be transformative. More than 70 of the world's largest banks have begun using blockchain to speed up payments by reducing delays caused by compliance checks, inaccurate addresses and missing data. Walmart, for instance, already uses blockchain to track 1.1 million items on sale in stores. Maersk has joined forces with IBM to pilot technology that follows the movement of its containers. Louis Dreyfus used blockchain to finalize the sale of soybeans to a Chinese processor, Shandong Bohi, with financing from ING, Societe General and ABN Amro. And Dubai has declared its intention to become a "blockchain-powered government by 2020". Computer-mediated transactions will only grow and depending on how the remaining challenges are tackled, the role of DLTs could expand alongside them. JS

Dr. Shahid Yusuf is chief economist, Growth Dialogue, George Washington University, adjunct professor, SAIS, Johns Hopkins University and non-resident fellow at the Center for Global Development.