PERSPECTIVES

includes research articles that focus on the analysis and resolution of managerial and academic issues based on analytical and empirical or case research

Blockchain in Finance

VIKALPA
The Journal for Decision Makers
44(1) 1–11, 2019

DOI: 10.1177/0256090919839897
journals.sagepub.com/home/vik

Jayanth Rama Varma

KEY WORDS

Blockchain

Distributed Ledger

DLT

Crypto Currency

Blockchain—the decentralized replicated ledger technology that underlies Bitcoin and other cryptocurrencies—provides a *potentially* attractive alternative way to organize modern finance. Currently, the financial system depends on a number of centralized trusted intermediaries: central counter parties (CCPs) guarantee trades in exchanges; central securities depositories (CSDs) provide securities settlement; the Society for Worldwide Interbank Financial Telecommunication (SWIFT) intermediates global transfer of money; CLS Bank handles the settlement of foreign exchange transactions, a handful of banks dominate correspondent banking, and an even smaller number provide custodial services to large investment institutions. Until a decade ago, it was commonly assumed that the financial strength and sound management of these central hubs ensured that they were extremely unlikely to fail. More importantly, it was assumed that they were *too big to fail* (TBTF), so that the government would step in and bail them out if they did fail. The Global Financial Crisis of 2007–2008 shattered these assumptions as many large banks in the most advanced economies of the world either failed or were very reluctantly bailed out. The Eurozone Crisis of 2010–2012 stoked the fear that even rich country sovereigns could potentially default on their obligations. Finally, repeated instances of hacking of the computers of large financial institutions is another factor that has destroyed trust. When trust in the central hubs of finance is being increasingly questioned, decentralized systems like the blockchain that reduce the need for such trust become attractive.

It is no coincidence that Bitcoin was launched shortly after the failure of Lehman that marked the peak of the global financial crisis. Over the subsequent decade, cryptocurrencies have grown rapidly: as of early November 2018, Bitcoin alone had a market cap exceeding that of India's most valuable listed company (and Bitcoin was only around half the value of all cryptocurrencies). However, even a

decade after the launch of Bitcoin, we have seen only a few pilot applications of blockchains to other parts of finance. This is because cryptocurrencies (while being extremely challenging technologically) encountered very few legal/commercial barriers, and could therefore make quick progress after Bitcoin solved the engineering problem. The blockchain has many other potential finance applications—mainstream payment and settlement, securities issuance, clearing and settlement, derivatives and other financial instruments, trade repositories, credit bureaus, corporate governance, and many others. Blockchain applications in many of these domains are already technologically feasible, and the challenges are primarily legal, regulatory, institutional, and commercial. It could take many years to overcome these legal/commercial barriers, and mainstream financial intermediaries could use this time window to rebuild their lost trust quickly enough to stave off the blockchain challenge. However, whether they are successful in rebuilding the trust, or why will they be disrupted by the new technology remains to be seen.

BENEFITS OF THE BLOCKCHAIN

The blockchain is a decentralized, replicated, tamper resistant (immutable), append-only ledger of transactions (see Box 1A for a brief description of the technology, and Box 1B for blockchain software and implementation issues).

Box 1A. What Is the Blockchain?

Instead of relying on a central trusted institution to maintain the authoritative record, the blockchain allows all interested parties to maintain their own copy of the ledger that is therefore decentralized and replicated. Cryptographic integrity checks are used to ensure that nobody is able to corrupt or tamper with their copy of the ledger. This is needed because unlike a paper ledger where any overwriting or alteration would be quite visible, digital records can be edited without leaving any visible trails.

The blockchain ensures integrity by chaining blocks of transactions together in such a way that altering any block breaks the link with the next block. It is impossible to change one block without changing the next block, which in turn forces a change in the next and so on till the very last block. This ensures that while new blocks can be added at the end, older blocks remain immutable: the ledger is append-only. The chaining of blocks is obviously not physical, but is based on a cryptographic hash.

The hash is a digital fingerprint that uniquely identifies a piece of text. For example, the SHA-1 hash of the Project Gutenberg Full Text of The Complete Works of William Shakespeare (which contains nearly a million words) is 6799e461c8177d88b6e0c782242642d3450c8b34.

If we edit the file and add a space at the beginning of line 5,000, the hash changes to 5d960169ea490568abf 4ec69c127ae12d57cedc2.

If instead, the first occurrence of 'The' in the file is changed to 'the', the hash changes to 65a835f4845395c929d5076029c a818f614a4119.

It is evident that even tiny changes in a large file cause major changes in the hash, making it suitable for use as a digital fingerprint.

The mathematical properties of hashes that make it a good digital fingerprint are discussed in standard cryptography text books like *Handbook of Applied Cryptography* (Menezes, van Oorschot, & Vanstone [1996]). The most important properties are that (a) it is computationally infeasible to find two distinct texts that have the same hash, and (b) that given a specific hash-value, it is computationally infeasible to find a text with that hash.

The blockchain is a set of blocks that have been chained together with cryptgraphic hashes. Each block (except the first) contains the hash of the previous block. If a crook alters an old block, say block 1000, the blockchain would fail the integrity check because the hash of block 1000 would no longer match the hash stored in the next block (block 1001). So the crook has to alter block 1001 so that the hash of the previous block stored there matches the hash of the altered block 1000. But this changes the hash of block 1001, and so the crook has to correct the hash stored in block 1002. This process goes on until the last block is reached. If all participants in the blockchain keep track of the last block,

they are indirectly guarding the integrity of the entire chain even if it has grown to millions and billions of blocks.

While cryptgraphic integrity checks protect older blocks from being altered, every blockchain needs rules ('consensus mechanisms') that govern how new blocks are added at the end. There are two main categories of blockchains—permissioned and permissionless—that differ in terms of their consensus mechanisms. Cryptocurrencies use permissionless chains that are open to the whole world, and in which there are no privileged participants with special rights. Participants in these chains are also typically anonymous (or more precisely, pseudonymous). Managing consensus in these chains is a very difficult technical challenge because no kind of majority rules can be implemented in an environment where there is no list of voters and where it is hard to prevent impersonation. Nakamoto used the idea of proof-of-work to solve this problem:

The proof-of-work also solves the problem of determining representation in majority decision-making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. (See Nakamoto [2008] for further details of how this works)

Most applications of the blockchain in mainstream finance use a permissioned blockchain. First of all, only the participants in the system are able to even read the data in the blockchain. Second, not all of these participants might have the privilege of adding new transactions to the chain. Third the identity of participants is typically verifiable. It is quite straightforward to implement consensus mechanisms based on majority votes in these chains because the voters are identifiable: usually a majority or super-majority of privileged participants is required for every new transaction.

For readers who want to understand blockchains in greater detail, Chokshi, Dixon, Nazarov, Walden, and Yahya (2018) provide a comprehensive list of resources and reading material organized into various categories.

Box1B. Blockchain Software and Implementation

Almost all of the software used in blockchain applications is open source and is actively maintained and developed. However, most of these are designed to run on the Linux operating systems, and the preferred way to run this software on Windows machines is to use virtual machines or Docker containers that provide a Linux environment in which they can run. This is not a constraint for business applications because financial service companies already run a large number of Linux machines for other applications.

For permissioned blockchain applications, the most common software platforms are Hyperledger Fabric, an open source collaborative effort by a consortium of large technology companies and banks, and R3 Corda, an open source platform with a commercial version (Corda Enterprise).

While permissionless blockchains have found it challenging to achieve high throughput because of the inherent limitations of proof-of-work, the permissioned systems have no difficulties on this score. Depository Trust & Clearing Corporation (2018) report that during their tests, distributed ledgers were able to 'perform at levels necessary to process an entire trading day's volume at peak rates, which equates to 115,000,000 daily trades, or 6,300 trades per second for five continuous hours' (see also GFT Technologies, 2018).

From an application point of view, the blockchain provides the following features: First, decentralization and replication means that a full audit trail is available to all participants. Moreover, the inbuilt cryptographic integrity checks ensure that this audit trail is verified by all of them. The result is a significantly lower need for trust in central hubs.

Second, the blockchain is partition resistant: if a few nodes fail or are disconnected from the network, the rest of the nodes can continue to function because they all have a copy of all the data. In traditional finance, on the other hand, if the central trusted institution is temporarily down for any reason, the whole system grinds to a halt. For example, on 20 October 2014, the real time gross settlement system (RTGS) of the United Kingdom experienced an outage of approximately nine hours (Deloitte, 2014). Though all banks and other entities were functioning, high-value payments could not happen during this period. In its subsequent consultation on building a new RTGS for the UK, the central bank described the advantages of using a distributed ledger: "the chief potential benefit when applied to core settlement in an RTGS system is resilience" (Bank of England, 2016).

The third benefit of the blockchain is Byzantine fault tolerance. While partition resistance deals with nodes that cease to function, Byzantine fault tolerance deals with nodes that malfunction and function maliciously. This has come to prominence with the rise of hacking and cyber-attacks. While criminal gangs might be content to steal money, terrorist group and nation state adversaries might seek to inflict catastrophic damage by corrupting or destroying data. The blockchain provides strong defence against this attack because of (a) replication of the data across large number of nodes running on completely different computer networks and (b) cryptographic integrity checks.

Fourth, the blockchain provides an excellent foundation for smart contracts—contracts embedded in computer code instead of legal language. By automating contract negotiation and enforcement, smart contracts reduce transaction costs and make small value transactions economically viable. Smart contracts can achieve efficiency gains by automating one or more of the key contractual phases of search, negotiation, commitment, performance, and adjudication (see Box 2).

Box 2. Smart Contracts

Nick Szabo coined the term smart contract two decades ago when the internet was still in its infancy.

Smart contracts combine protocols with user interfaces to formalize and secure relationships over computer networks.…These protocols, running on public networks such as the Internet, both challenge and enable us to formalize and secure new kinds of relationships in this new environment, just as contract law, business forms, and accounting controls have long formalized and secured business relationships in the paper-based world.…The contractual phases of search, negotiation, commitment, performance, and adjudication constitute the realm of smart contracts. (Szabo, 1997)

It is possible to have smart contracts without the blockchain, just as it is possible to have computer databases without the blockchain. The problem in both cases is that of trust. Two parties may use the blockchain because neither is willing to trust the other to record the data faithfully. Similarly, neither may be willing to let the smart contract software run on the other's computer. This is where the blockchain helps: it is not only a shared database, but also a shared computer. As Szabo puts it,

A block chain computer is a virtual computer, a computer in the cloud, shared across many traditional computers and protected by cryptography and consensus technology.…A block-chain computer, in sharp contrast to a web server, is shared across many such traditional computers controlled by dozens to thousands of people. By its very design each computer checks each other's work, and thus a block chain computer reliably and securely executes our instructions…. (Szabo, 2014)

A contract is a *meeting of minds* that was traditionally reduced to long written documents in legal language. However, many financial contracts are so complex that they are better described by computer code than in natural/ legal language. In fact, many years ago, the US Securities and Exchange Commission proposed to require that the terms of most Asset Backed Securities be disclosed in the form of computer code in the Python programming language (Securities and Exchange Commission, 2010) so that investors could understand them better.

Smart contracts can also facilitate the search and negotiation phase of contracts. Many financial transactions are today automated, but they depend on a trusted third party to accomplish the automation. Stock trading is today done largely by algorithms that decide to buy or sell based on price signals and other publicly available information. A momentum or trend following algorithm might send a buy order to the stock exchange, while another contrarian algorithm might send a sell order. The stock exchange's order matching software might match these orders based on highly complex rules (e.g., the orders might have price limits and might be partially hidden as well). A stock trade can thus happen without any human intervention at all. But this works only because of the stock exchange that stands in the middle between the two algorithms. Smart contracts running on a blockchain can achieve something similar in over the counter (OTC) markets where there is no exchange in the middle.

Smart contracts can also automate the performance of contracts. In derivative contracts, for example, both the final settlement and the daily mark to market are governed by well-defined rules. With smart contracts, these transactions can be fully automated. If there is no need for human intervention, then the costs of these transactions comes down, and it is feasible to have OTC contracts of much smaller ticket sizes. The International Swaps and Derivatives Association (ISDA), which governs most OTC derivatives, has carried out a great deal of work on smart contracts.

In a recent consultation paper (International Swaps and Derivatives Association [ISDA], 2018), ISDA states:

> Smart contracts could help revolutionize the derivatives market by creating much-needed efficiencies that would benefit the entire industry. But transforming smart contracts from an exciting concept to practical use will present a number of challenges.… For smart derivatives contracts to fulfill their potential, it is important they are developed in a way that is compatible and consistent with the technological, commercial, regulatory and legal standards applicable to both derivatives contracts and smart contracts. This will require knowledge and experience from different disciplines and domains. Expertise in the technology used, the commercial context of its use, the regulation that applies to it and the law that supports its effectiveness, are all critical.

LEGAL/COMMERCIAL CHALLENGES

As mentioned earlier, non-cryptocurrency applications of the blockchain have to overcome some major legal/commercial barriers. First, unlike cryptocurrencies that exist only on the blockchain, in most other applications, assets that exist in the real world (dollars, rupees, securities, real estate) have to be represented by entries in the blockchain. Cryptocurrencies do not need any off-chain (real world) jurisprudence at all; they are able to go beyond the pragmatic idea that *code is law* to the more radical notion that *only code is law*. When we try to move real world finance to the blockchain, code and law have to co-exist. Some real world law has to recognize code as law at least to some limited extent so that transactions on the blockchain can effect change of ownership in the real world. Today's mainstream financial institutions operate under similar legal protection going back to the 19th century. For example, in the United Kingdom, the Bankers' Books Evidence Act of 1879 provided, "Subject to the provisions of this Act, a copy of any entry in a banker's book shall in all legal proceedings be received as prima facie evidence of such entry, and of the matters, transactions, and accounts therein recorded." A similar law was passed in India a decade later. Some law of this kind will be needed to give legal sanctity to the blockchain for assets other than cryptocurrencies.

Second, most blockchain applications in finance will need to ensure regulatory compliance on day one. Regulators are not often clear in their regulatory stance on the new technology, and obtaining their clearance is not always easy. By contrast, for a long time, cryptocurrencies could operate outside the regulatory framework entirely. In recent years, this has begun to change as many cryptocurrency exchanges have become licensed money changers, and as traditional exchanges, securities brokers, and asset managers have begun to offer cryptocurrency related products. For example, in the United States, Cboe Futures Exchange launched Bitcoin futures in December 2017 after obtaining requisite regulatory approvals.

Third, many blockchain applications in finance have to ensure commercial viability in the face of competition from incumbent players who are not only rich and powerful, but also well entrenched in the current legal and regulatory framework. Cryptocurrencies, on the other hand, were (in the initial years) dominated by ideologically motivated computer professionals ('geeks') and anarchists who were not too constrained by commercial considerations. By staying outside the regulatory framework, they also avoided direct confrontation with incumbents defending their monopoly/oligopoly. Only after establishing themselves outside the formal system, did cryptocurrencies become more mainstream and start attracting speculators seeking quick returns.

For the blockchain to succeed in mainstream finance, these critical hurdles will have to be overcome. The blockchain ventures that we have seen so far have been driven by either (a) venture capitalists funding potential disruptors in the hope of large rewards if they succeed or (b) the incumbents themselves launching pilot projects to protect themselves from being disrupted. It remains to be seen whether these projects will achieve sufficient scale and traction to challenge today's entrenched business models.

POTENTIAL APPLICATIONS

Since the blockchain is basically a technology for recording transactions, it can potentially be applied to most parts of finance. However, the following sections describe applications that are most promising because the current system is not working well enough, or because blockchain pilots have been successful.

Fiat Money on the Blockchain

Finance is essentially about money, and much of the financial system can run more easily on the blockchain

if fiat money (dollars, euros, and rupees) could be transacted directly on the chain. There are many ways of doing this, and it is reasonable to assume that one or more of these mechanisms would achieve sufficient liquidity and scale in the near future (see Box 3).

Box 3. Tokenization of Fiat Money

There are three main ways in which ordinary fiat money (dollars or rupees) can be converted into tokens that live on a blockchain. First, the central bank itself could issue digital money that lives on a blockchain. Many central banks around the world have been thinking about this, and have discussed the matter in their reports and documents, but none looks likely to take the plunge soon. The Bank for International Settlements put it very tactfully: "the issuance of a [Central bank digital currency] requires careful consideration" (Bank for International Settlements, 2018). Some market participants have been exploring the idea of a temporary fiat money token that would be redeemed and destroyed at the end of each day. The idea is that, for example, a group of large European banks deposit a few billion euros each with the European Central Bank (ECB) before the markets open, and the ECB issues euro-coins of equal value on the blockchain. During the day, the banks can make euro payments to each other on the blockchain using these euro-coins. At the end of the day's trading, the banks surrender their euro-coins to the ECB that redeems them for euros. There may be less resistance to this idea, but even this will be a bit of a leap into the unknown for the central banks of the world.

Second, a large trusted institution could issue cryptocoins fully convertible into fiat money with its promise backed by a 100 per cent reserve of fiat money. The challenge is to find a way for this institution to make money out of this activity. When central banks issue money, they earn seigniorage revenues because their money issuance does not have to be backed by non-income earning assets. Essentially, the central bank pays no interest on the money that it issues, and is able to invest the proceeds in government bonds that do earn interest. If the issuer of fiat money tokens has to back the issuance with 100 per cent reserves of highly liquid safe assets, the return earned on these reserves might be limited. If the institution is subject to banking regulations, it might be required to maintain capital based on a leverage ratio. Until the issuance reaches a sufficiently large scale (possibly billions of dollars), it might not earn enough to cover its operational costs and the return on its own capital. There is a coin called Tether that claims to be backed 100 per cent with US dollars, but there are questions about the trustworthiness of the issuer (Griffin & Shams, 2018). In February 2019, one of the largest banks in the world announced that it had created and tested a digital coin representing the US dollar but its usage is restricted to the bank's large institutional clients (Morgan, 2019).

Third, decentralized smart contracts can be used to create a token that is pegged to a fiat currency. The Dai Stablecoin (MakerDAO, n.d.) is pegged to the US dollar (1 Dai = 1 US dollar) through a smart collateralized debt contract. Anybody can create new Dai coins by locking up sufficient value of a cryptocurrency (ether) in a collateral contract. For example, a person deposits $200 worth of ether into a smart contract and issues 100 Dai (worth $100). At this point, the contract is 200 per cent collateralized (the locked up ether is worth 200% of the coins issued). The problem is that as the value of the ether fluctuates, this excess collateralization (the liquidation ratio) will also change. If ether drops by more than 50 per cent, the Dai will no longer be backed by adequate ether. To prevent this, the system specifies a minimum degree of excess collateralizion. Suppose the liquidation ratio is 150 per cent, and there is drop of more than 25 per cent in the value of ether. The value of the ether in the collateral contract will now be less than the liquidation ratio, and the system sells the ether for US dollars and uses the proceeds to buy back the 100 Dai that were issued. After deducting a liquidation penalty, the remaining collateral is returned to the original creator. In a decentralized system, the question is who will perform the liquidation, and the answer is that the sale of ether and the buyback of Dai will both be done by smart contracts. Any person can initiate the process of liquidation and earn a small reward for doing this. It is expected that people will set up smart contracts to monitor all the Dai collateral contracts in real time and trigger liquidation as needed. Of course, the creator of the contract can also choose to top up the collateral to avoid the liquidation penalty. The risk to the Dai-Dollar peg is that ether falls so sharply and quickly that in the time between initiation and completion of the liquidation, the value of the collateral drops below

the required 100 dollars. This risk can be reduced by high liquidation ratios. The Dai Stablecoin is backed by further lines of defence designed to minimize the risk of the peg being broken. Details are available in the Dai Stablecoin whitepaper (MakerDAO, n.d.). Again, the issue is whether the economics will work well enough to motivate adequate creation of Dai, particularly when the MakerDAO platform on which the system runs wants to appropriate significant seigniorage income for itself. The creator can sell the Dai for dollars and earn interest on these dollars, but her ether becomes a dead asset locked up in a collateral account. Locking up ether might not matter much when credit and money markets in ether are undeveloped and there is no opportunity cost of locking up ether. As and when cryptocurrency money markets develop, the economics could become challenging. There is, however, the view that cryptocurrencies with hard issuance caps might be structurally deflationary and might therefore exhibit zero or even negative interest rates. Meanwhile fiat currency inflation and interest rates are rising from their post crisis lows, and this improves the economics of fiat currency tokens by increasing the seigniorage income.

Micropayments and Micro Financial Services

Second level networks running on top of existing cryptocurrencies are making it feasible to make very low-value payments. For example, on the Lightning Network (see Box 4), median fees of one Satoshi (less than 0.01 US cents) are being reported. If these low fees can be sustained as the network scales, it would be possible for the first time to make micropayments of 1 US cent or less between complete strangers in near real time. For example, a web search may show you a snippet of an article from a newspaper that you have not even heard of and offer to display the entire article on payment of 1 US cent. Or you might pay 2 US cents for a music to be streamed to you. Micropayments and smart contracts would also open the door to a lot of micro-financial services (micro-lending, -insurance, and -savings) that could facilitate financial inclusion.

Box 4. Lightning Network

From the point of view of mainstream finance, cryptocurrencies appear to be very primitive payment mechanisms that do not incorporate any of the financial innovations that have occurred in payment systems over several centuries. Clearing and netting are integral to mainstream finance: only a small number of high-value payments happen on the RTGS, while almost all retail payments happen on a deferred net settlement that periodically settles net on the RTGS. Real world RTGS' depend on a number of liquidity facilities, queuing mechanisms, and optimization algorithms, so that in actual implementation, efficiency and liquidity economizing are more important than a rigid enforcement of 'real-time' and 'gross-settlement'. Similarly, mainstream payment systems typically involve long chain of payments. For example, a dollar payment by an Indian importer to a Korean supplier will likely involve the Indian importer's bank, the Korean supplier's bank and their respective correspondent banks in the USA. It is only in 2018 that some of these ideas have been applied to cryptocurrency payment systems with the beta launch of the Lightning network on top of Bitcoin, and some other coins. The same idea can be easily applied to any other cryptocurrency including tokenized fiat currencies. First, Lightning uses the idea that if two parties have to make a series of payments to each other on an ongoing basis, it is more convenient to settle the running account periodically (say once a month) than to settle each payment as it occurs. Second, if A and B do not have a running account with each other, but both have a running account with C, then they can route the payment via C without making any immediate settlement. None of these ideas is anything new to anybody conversant with mainstream finance. What is new is the cryptography and smart contracts that are used to implement them. The cryptographic checks eliminate the need for any reconciliation that is the bane of all deferred settlement systems in traditional finance. The automated smart contracts reduce the cost of operations to levels that are unimaginable in normal banking channels. While even a small cross-border payment could cost several dollars of banking fees, a payment over the Lightning network is currently reporting fees of less than 0.01 cents.

Pre- and Post-trade Processes

Securities trading and settlement can be divided into three stages: (a) pre-trade authorization and approval, (b) trade execution, and (c) clearing and settlement. Of these, trade execution is highly automated with stock exchanges having invested huge amounts of money to build technology infrastructure that can match trades with latencies of microseconds. It would be hard for any blockchain to achieve these speeds. Most of the potential is in the pre- and post-trade processes that involve inefficient and fragmented legacy systems.

Blockchains can provide complete transparency on the cash and securities blockchains before and after the

trade. The whole set of legacy system and processes (pre-trade checks and trade confirmations) that exist to ameliorate the opaqueness of this ownership can then be eliminated. Exchanges may still be needed, but we may not need brokers and custodians. With settlement happening on the blockchain on delivery versus payment basis, and corporate actions (dividends and stock splits) being handled by smart contracts, we may not need a depository anymore. Or perhaps, the depository could run the permissioned blockchain on which the settlement happens. The novation provided by the CCPs can be replicated by smart contracts. The challenge will be to design smart contracts that can replicate short selling, margin trading, and net settlement. Depository Trust & Clearing Corporation (2016) and Euroclear (2016) discuss the challenges and opportunities in using blockchain in securities settlement.

Customized Investment Management

Mutual funds have, for long, allowed small investors to participate in asset markets provided they are willing to accept a fixed menu of products. An investor who wants to track a popular benchmark index is well served by this market, but those who want exposure to customized indices or desire non-linear payoffs need a different vehicle. In Europe and other jurisdictions, structured products have emerged as an attractive alternative for investors who seek something more complex than a plain vanilla mutual fund. These customized investment products might have an issuance size of only a million dollars at which scale a mutual fund or a bond issuance might be unviable. Turning these into smart contracts on the blockchain might allow the issuance size to be brought down much further, possibly a thousand dollars or even less. Marex Spectron (2018) describes a structured note (a principal protected note linked to the FTSE 100 index) that was registered, cleared, and settled on the Ethereum blockchain.

Data Registries and Repositories

Modern finance depends on a number of data registries and data repositories that provide verified data needed for a variety of transactions. For example, credit bureaus and loan registries are critical elements of the infrastructure for providing credit. After the Global Financial Crisis, trade repositories have been created to ensure that regulators have data about the risk and inter-connectedness of the financial system. While these entities serve critical functions, they are beset with several problems: duplication, lack of accountability, loss of privacy, and excessive cost. Consumer groups have highlighted the difficulties that consumers face in correcting errors in their own credit information as stored by the credit bureaus. The data breach at the US credit bureau, Equifax, has been described as the worst leak of personal info ever (Goodin, 2017). The blockchain is probably part of the solution to the problems of this kind of financial infrastructure.

TRADE FINANCE: AN INDUSTRY WIDE ERP

Organizations use an enterprise resource planning (ERP) software to integrate the management of all major business processes in an enterprise. At its core is a common database that provides a single version of the truth in real time throughout the organization cutting across departmental boundaries. The blockchain is very similar: it is a real time common database that provides a single version of the truth to all participants in an industry cutting across organizational boundaries.

Within an organization, the ERP typically replaces a bunch of much cheaper department level software, and ERP deployments are often justified not on any rigorous return on investment criterion, but on grounds of internal controls and management. It is easy to see this dynamic playing out with the blockchain as well. There is a need for a single version of the truth across all organizations involved in many complex processes. Clearly, organizations do not trust each other and no organization would like to accept the formats, standards, and processes of another organization. It is a lot easier for everybody to adopt a neutral solution like the blockchain.

One area where we are seeing this happen is in trade finance that involves so many entities (exporter, importer, their respective banks, the shipping company, insurance companies, clearing and forwarding agents, and so on) that it is very hard for all of them to have a consistent view of the data. It is a lot easier to put everything on the blockchain, and then everybody sees the same version of the truth. Trade finance is one area where the blockchain appears to be moving from pilots to real world applications (D'Monte, 2018; Sanghvi, 2018).

More generally, the entire area of cross-border payment with its legacy systems, long chain of correspondent

banks, and attendant fees, delays and unreliability is an attractive target for blockchain technologies. Ripple is a blockchain solution to this problem that boasts of an impressive list of customers including several large Indian banks.

VENTURE CAPITAL AND ALGORITHMIC GOVERNANCE

During 2017, a large number of blockchain ventures raised capital through sale of tokens in what came to be known as initial coin offerings (ICOs). However, securities regulators in the US have taken the view that these tokens are securities and the ICOs need to fulfil all the regulatory requirements of securities offerings: ICOs are just IPOs. Some ICOs continue to be launched that avoided these regulations by focusing on accredited investors or raising money outside the US, but it is doubtful whether ICOs will turn out to be a sustainable form of financing.

Decades in the future, there may lie new forms of corporate governance that can be described as *algorithmic governance* (DuPont, 2017) or *enterprise without entities* (Verstein, 2017). The decentralized autonomous organization (DAO) is a new decentralized business model for organizing both commercial and non-profit enterprises that does not have a formal organizational structure or legal entity and consists only of (smart) contracts (see Box 5). It is too early to speculate on whether DAOs will be viable and important.

Box 5. Decentralized Autonomous Organizations (DAOs)

The establishment of a large business enterprise typically involves: (a) creation of a new legal entity (say a company), (b) investors contributing a pool of funds to this company, and (c) appointment of a group of managers to run the company on behalf of the investors. A few centuries ago, when businesses were much smaller, neither (a) nor (c) might have been necessary as a few partners might have pooled funds to create a business that they ran collectively. Modern communication technology, blockchains and smart contracts are making it theoretically possible for thousands of investors to pool their money and invest it without appointing a bunch of managers to actually run the business. *The DAO* was a short-lived experiment on these lines based on a smart contract running on the Ethereum blockchain. In April 2016, *The DAO* raised about $160 million worth of funding from several thousand investors to be invested and managed by a smart contract incorporating the following keys ideas. First, anybody could submit a proposal for deploying the funds. This could take the form of paying a *contractor* to provide a product or service, or it could take the form of a venture capital type of funding. Second, there were quorum and voting rules specifying the majority requirements for acceptance of proposals. Third, there was a provision for any group of investors to split off from *The DAO* to create a *Child DAO*. This was necessary because in a pure voting governance system, the majority could appropriate the whole money for themselves denying any share to the minority. To prevent this problem, anybody could split off from the main DAO into a child DAO that would receive its share of returns on old investments and returns on its new investments; the child DAO in turn could be split further as often as desired. Finally, one level of filtering safeguard was provided for: *The DAO* had some *curators* who would approve a white list of addresses to which money can be sent, but the splitting process could also be used to change the curator. Unfortunately, there was a bug in the software code for the splitting process, and one hacker exploited this bug to steal money from *The DAO*. The Ethereum developers resorted to some emergency measures to reverse this theft, shut down *The DAO* and return the money to the original investors (see DuPont, 2017 for further details). While this particular experiment failed, it is quite possible, others will build similar contracts with hopefully better tested code to create totally new forms of business organization and corporate governance.

CONCLUSION

Blockchain is still an evolving and therefore immature technology; it is hard to predict how successful it would be outside its only proven use domain of cryptocurrencies. History teaches us that radically new technologies take many decades to realize their full potential. Thus it is perfectly possible that blockchain would prove revolutionary in the years to come despite its patchy success so far. What is certain is that businesses should be looking at this technology and understanding it because its underlying ideas are powerful and likely to be influential.

DECLARATION OF CONFLICTING INTERESTS

The author declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

FUNDING

The author received no financial support for the research, authorship and/or publication of this article.

REFERENCES

Bank for International Settlements. (2018). *Committ ee on payments and market infrastructures—central bank digital currencies*. Retrieved from https://www.bis.org/cpmi/publ/d174.pdf

Bank of England. (2016). *A new RTGS service for the United Kingdom: Safeguarding stability, enabling innovation*. Retrieved from https://www.bankofengland.co.uk/-/media/boe/files/payments/a-new-rtgs-service-for-the-uk-safeguarding-stability-enabling-innovation.pdf?la=en&hash=2FE6ABB33839969FDB3E07C538293DFE31CB4005

Chokshi, S., Dixon, C., Nazarov, D., Walden, J., & Yahya, A. (2018). *Crypto Canon* https://a16z.com/2018/02/10/crypto-readings-resources

D'Monte, L. (2018, November 6). How blockchain puts trade finance deals in fast lane. *Mint*. Retrieved from https://www.livemint.com/Money/aeuKOy0BpNrlFgXyjzTIqJ/How-blockchain-putstradefinance-deals-in-fast-lane.html

Deloitte. (2014), *Independent review of RTGS outage on 20 October 2014*. Bank of England. Retrieved from https://www.bankofengland.co.uk/-/media/boe/files/report/2015/independent-review-of-rtgs-outage-on-20-october 2014.pdf?la=en&hash=95DAB90636DD5D501E135832B54F5C359C8AE72F

Depository Trust & Clearing Corporation. (2016). *Embracing disruption: Tapping the potential of distributed ledgers to improve the post-trade landscape*. Retrieved from http://www.dtcc.com/news/2016/january/25/blockchain-white-paper

Depository Trust & Clearing Corporation. (2018). *DTCC announces study results demonstrating that DLT can support trading volumes in the US equity Markets*. Retrieved from http://www.dtcc.com/news/2018/october/16/dtcc-unveils-groundbreaking-study-on-dlt retrieved 27 October 2018.

DuPont, Q. (2017). Experiments in algorithmic governance: A history and ethnography of 'The DAO', a failed decentralized autonomous organization. In Malcolm Campbell-Verduyn (Ed.), *Bitcoin and Beyond* (pp. 157–177). Routledge.

Euroclear. (2016). *Blockchain settlement regulation, innovation and application*. Retrieved from https://www.euroclear.com/dam/PDFs/Blockchain/MA3880%20Blockchain%20S&M%209NOV2016.pdf

GFT Technologies. (2018). *Performance testing of distributed ledger technology*. Retrieved from https://www.gft.com/dam/jcr:808c4d20-64d8-4633-a0ec-5226b8049ff2/gft_pov_performance-testing-of-distributed-ledger-technology.pdf

Goodin, D. (2017). *Why the equifax breach is very possibly the worst leak of personal info ever*. Retrieved from https://arstechnica.com/information-technology/2017/09/why-the-equifax-breach-is-very-possibly-the-worst-leak-of-personal-info-ever/

Griffin, J. M., & Shams, A. (2018, June 13). *Is bitcoin really un-tethered*? doi: 10.2139/ssrn.3195066

International Swaps and Derivatives Association (ISDA) (2018). *Smart Derivatives Contracts: From Concept to Construction* (Whitepaper). Retrieved from https://www.isda.org/a/cHvEE/Smart-Derivatives-Contracts-From-Concept-to-Construction-Oct-2018.pdf

MakerDAO. (n.d.). *The Dai stablecoin system*. Retrieved from https://makerdao.com/whitepaper

Marex Spectron. (2018). *The first structured product to be transacted and custodied using blockchain launched on Friday 16 March*. Retrieved from http://www.marexspectron.com/about-us/news/2018/03/worlds-first-blockchain-based-structured-product

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC Press. Retrieved from http://www.cacr.math.uwaterloo.ca/hac

Morgan, J. P. (2019). *J.P. Morgan creates digital coin for payments*. Retrieved from https://www.jpmorgan.com/global/news/digital-coin-payments

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved from https://bitcoin.org/bitcoin.pdf

Sanghvi, N., (2018, November 6). *The truth about reliance and India's 'first' blockchain transaction*. Retrieved from https://coincrunch.in/2018/11/06/the-truth-about-reliance-and-indias-first-blockchain-transaction/

Securities and Exchange Commission. (2010). *Asset-backed securities—proposed rule* (release no. 33–9117). Retrieved

from https://www.sec.gov/rules/proposed/2010/33-9117.pdf

Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*, *2*(9). Retrieved from https://firstmonday.org/ojs/index.php/fm/article/view/548/469-publisher=First

Szabo, N. (2014). *The dawn of trustworthy computing*. Unenumerated Blog. Retrieved from https://unenumerated.blogspot.com/2014/12/the-dawn-of-trustworthy-computing.html

Verstein, A. (2017). Enterprise without entities. *Michigan Law Review*, *116*(2), 247.

Jayanth Rama Varma is a Professor in the finance and accounting area at the Indian Institute of Management Ahmedabad (IIMA). His doctorate in management is also from IIMA. His research interests include financial markets and their regulation, mathematical modelling, and computer simulation. He has been a full-time member of the Securities and Exchange Board of India (SEBI). He was a member of the Raghuram Rajan Committee on Financial Sector Reforms and of the Financial Sector Legislative Reforms Commission.

e-mail: jrvarma@iima.ac.in