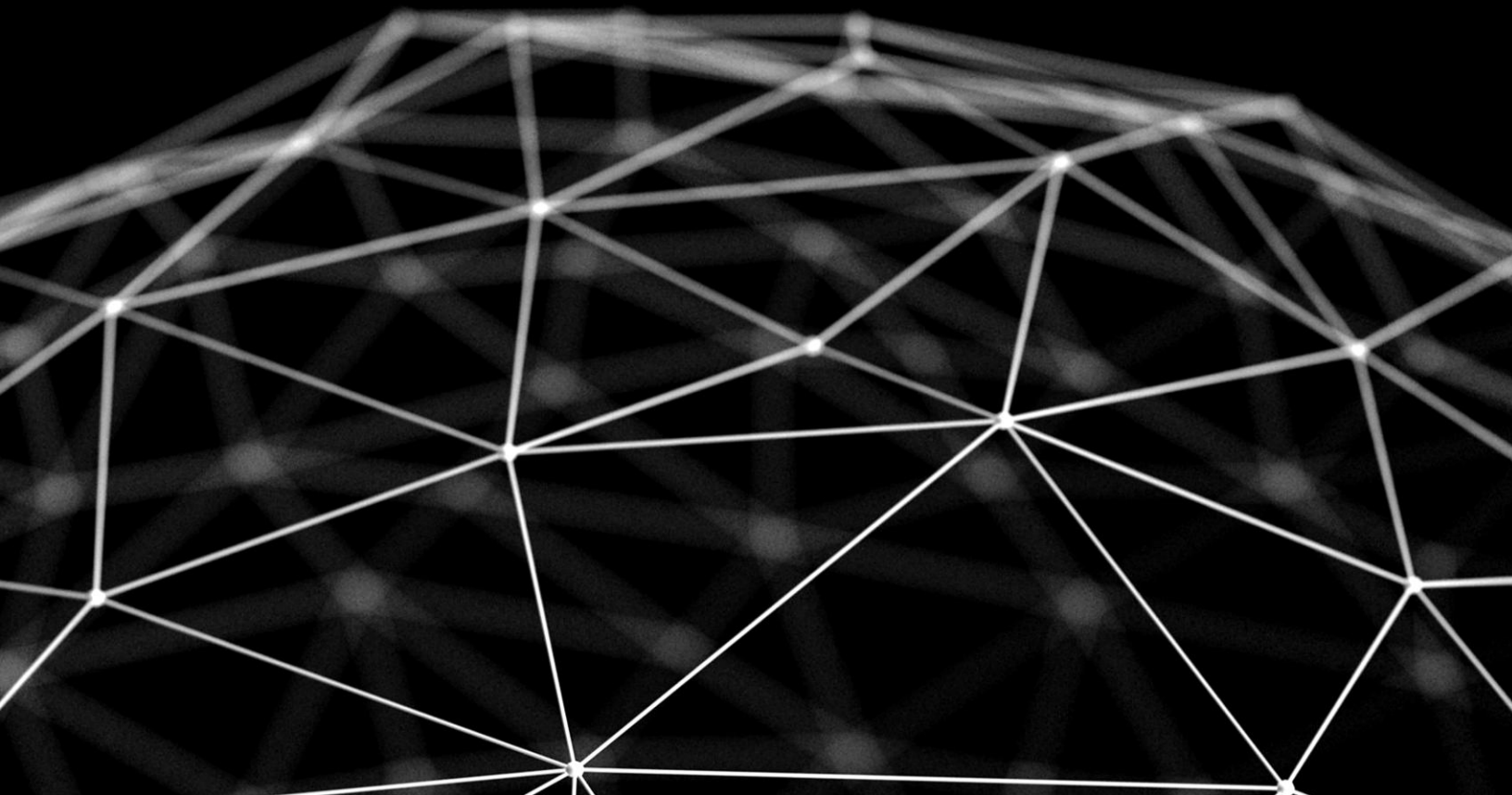
IndraStra
OPEN ACCESS

The Age of BLOCKCHAIN

A Collection of Articles

Kannan Subbiah | Benno Ferrarini | Julie Maupin | Marthe Hinojales
Rahul Guhathakurta | Sanatan Kulshrestha | Danika Wright



The Age of Blockchain: A Collection of Articles

Contact Information: Tel: +1-516-926-0755, Email: *info@indrastra.com* and URL: *www.indrastra.com*

Printed in the United States of America.

Imprint: IndraStra Open Access | Publisher: IndraStra Global

DOI: 10.5281/zenodo.1202390

Index

Authors

Kannan Subbiah is a management professional with 27 years of overall experience in IT Project, Product and Program Management, Enterprise & Solution Architecture and Design & Deployment.

Dr. Benno Ferrarini is a senior economist at the Economic Research and Regional Cooperation Department (ERCD), Asian Development Bank (ADB).

Dr. Julie Maupin is a senior researcher at the Max-Planck Institute for Comparative Public Law and International Law in Heidelberg, Germany. She is also a senior fellow at the UCL Centre for Blockchain Technologies (London) and the Centre for International Governance Innovation (Waterloo) and is an advisor to the IOTA Foundation (Berlin).

Marthe Hinojales is an economics officer at the ERCD, ADB.

Rahul Guhathakurta is a Founder/Publisher of IndraStra Global. He is a seasoned retail and supply chain consultant with cross-industry experience spanning 3 continents.

RADM Dr. S. Kulshrestha (Retd.), Indian Navy, holds expertise in quality assurance of naval armament and ammunition. He is an alumnus of the NDC and a Ph.D. from Jawaharlal Nehru University, New Delhi. He superannuated from the post of Director-General, Naval Armament Inspection in 2011.

Dr. Danika Wright is a Lecturer in Finance, University of Sydney.

 | DOI: 10.5281/zenodo.1202390

Introduction

The *"Blockchain"* is still an emerging revolutionary technology. It is steadily transforming the financial relationships between people and businesses globally.

"The Age of Blockchain: A Collection of Articles" is an eBook, which contains a set of selected articles which were published at *indrastra.com* in recent times. These curated collections are of value because they bring together important point of views on blockchain technologies and explore what this revolutionary technology will mean for global businesses.

The first article is written by *Kannan Subbiah*, discussed some of the key strengths that drive the adoption of the blockchain technology world over.

The second article is about Digital Identity, written by *Dr. Benno Ferrarini*, *Dr. Julie Maupin*, and *Marthe Hinojales*. It provides a cost-benefit analysis of distributed ledger technologies (DLT) and its application in developing and maintaining national or global identification system in the digital world.

The third article by *Rahul Guhathakurta* discusses the application of blockchain technologies in the automotive industry. It highlights the upstream and downstream applications of blockchain and discusses the fundamentals of scalability and interoperability which can benefit many stakeholders in the automotive domain - from the supplier to manufacture and from manufacturer to end-user.

The fourth article is written by *Rear Admiral Dr. S. Kulshrestha (Retd.), Indian Navy*. It's about the current stage of evaluation of the military application of blockchain technologies in areas relating to military logistics, procurement and finance, Internet of Things, and other applications of interest to the military.

The last but not the least, the fifth article by *Dr. Danika Wright* enlighten the readers on how blockchain could transform the way we buy and sell real estate by doing away with the hidden costs and inefficiencies in our existing real-estate markets.

 DOI: 10.5281/zenodo.1202390

Distributed Ledger - Strengths That Warrants Its Adoption

Kannan Subbiah

The *"Blockchain"* is the most talked about technology today that is likely to have a pervasive impact on all industry segments, more specifically in the Banking and Financial Services. Blockchain packs the principles of cryptography, game theory and peer-to-peer networking. Blockchain, once the formal name for the tracking database underlying the crypto-currency bitcoin, is now used broadly to refer to any distributed ledger that uses software algorithms to record transactions with reliability and anonymity. An increasingly interesting aspect of blockchain use is the concept of smart contracts – whereby business rules implied by a contract are embedded in the blockchain and executed with the transaction.

Built on the peer-to-peer technology, blockchain uses advanced encryption to guarantee the provenance of every transaction. The secure and resilient architecture that protects the distributed ledger is on to its key advantage. The other benefits of blockchain include a reduction in cost, complexity and time in addition to offering trusted record keeping and discoverability. Blockchain has the potential to make trading processes more efficient, improve regulatory control and could also displace traditional trusted third-party functions. Blockchain holds the potential for all participants in a business network to share a system of record. This distributed, shared ledger will provide consensus, provenance, immutability, and finality around the transfer of assets within business networks.

The Banking and Financial Services Industries world over are seriously looking at this technology. The Central Banks in many countries including India have formed committees to evaluate the adoption of the blockchain technology, which is expected to address some of the problems that the industry is wanting to overcome over many years. For the financial services sector blockchain offers the opportunity to overhaul existing banking infrastructure, speed settlements and streamline stock exchanges. While many institutions understand its potential,

they are still trying to work out whether blockchain technology offers a cost-cutting opportunity or represents a margin-eroding threat that could put them out of business.

Like the Cloud Computing, there three categories of the blockchain, public, private, and hybrid. A public blockchain is a fully decentralized *"trustless"* system open to everyone and where the ledger is updated by anonymous users. A private blockchain finds its use within a bank or an institution, where the organization controls the entire system. Hybrid is a combination of both public and private implementations, which is open to a controlled group of trusted and vetted users that update, preserve, and maintain the network collectively. Blockchain exploration has propelled banks in multiple directions, from examining fully decentralized systems that embed bitcoin or other virtual tokens to function, to ones where only authorized and vetted users are granted access to a network.

The technology is being commercialized by several industry groups and is coming out with the use cases that this technology will be suitable for across different industry vertical. With the surge in funding for the fintech innovations, the blockchain technology may find its retail and institutional adoption in about 3 to 5 years, while some expect that this will take even longer. Some have invested in in-house development, while others have partnered with others in their pursuit to adopt the blockchain as part of their mainstream business technology.

Listed here are some of the key strengths that drive the adoption of the technology world over.

Trusted

With the frequency at which data breaches are happening, users are seeking to have control over sensitive data. Blockchain by its nature puts users in total control. Applied to payments, blockchain allows users to retain control of their information and enable access to information about only one act of transaction. Participants are able to trust the authenticity of the data on the ledger without recourse to a central body. Transactions are digitally signed; the maintenance and validation of the distributed ledger are performed by a network of communicating nodes running dedicated software which replicate the ledger amongst the participants in a peer-to-peer network, guaranteeing the ledger's integrity. They will also want the ability to roll back transactions in instances of fraud or error – which can be done on blockchain by adding a compensating record,

as long as there are permission mechanisms to allow this – and a framework for dispute resolution.

Traceability

The cryptographic connection between each block and the next consecutive ones forms one link of the chain. This link ensures the maintenance of trace for the information flow across the chain and thus enabling the participants or regulators to trace information flows back through the entire chain. The distributed ledger is immutable as entries can be added to, but not deleted from. This information potentially includes, but is not limited to, ownership, transaction history, and data lineage of information stored on the shared ledger. If provenance is tracked on a blockchain belonging collectively to participants, no individual entity or small group of entities can corrupt the chain of custody, and end users can have more confidence in the answers they receive.

Resiliency

Operates seamlessly and removes the dependency on a central infrastructure for service availability. Distributed processing allows participants to seamlessly operate in case of failure of any participants. Data on the ledger is pervasive and persistent, creating a reliable distributed storage so that transaction data can be recovered from the distributed ledger in case of local system failure, allowing the system to have very strong built-in data resiliency. Distributed ledger-based systems would be more resilient to systematic operational risk because the system as a whole is not dependent on a centralized third party. With many contributors, and thus back-ups, the ledger has multiple copies which should make it more resilient than a centralized database.

Reconciliation

Use cases that center on increasing efficiency by removing the need for reconciliation between parties seem to be particularly attractive. Blockchain provides the benefits of ledgers without suffering from the problem of concentration. Instead, each entity runs a *"node"* holding a copy of the ledger and maintains full control over its own assets. Transactions propagate between nodes in a peer-to-peer fashion, with the blockchain ensuring that consensus is maintained. Reconciling or matching and verifying data points through manual or even electronic means

 | DOI: 10.5281/zenodo.1202390

would be eliminated, or at least reduced because everyone in the network accessing the distributed ledger would be working off the exact same data on the ledger. In the case of syndicated loans, this is more so, since information is mutual and all participants are working from the same data set in a real-time or near-real time.

Distributed

When a blockchain transaction takes place, a number of networked computers, process the algorithm and confirm one another's calculation. The record of such transactions thus continually expands and is shared in real time by thousands of people. Billions of people around the world lack access to banks and currency exchange. Blockchain-based distributed ledgers could change this. Just as the smart phone gave people without telephone lines access to communication, information, and electronic commerce, these technologies can provide a person the legitimacy needed to open a bank account or borrow money — without having to prove ownership of real estate or meeting other qualifications that are challenging in many countries.

Efficiency Gains

Removal of slow, manual and exception steps in existing end-to-end processes will lead to significant efficiency gains. Blockchain also removes the need for a clearinghouse or financial establishment to act as intermediary facilitating quick, secure, and inexpensive value exchanges. Blockchain ensures the most effective alignment between usage and cost due to its transparency, accuracy and the significantly lower cost of the crypto-currency transaction. Distributed ledger technology has the potential to reduce duplication of record keeping, eliminate reconciliation, minimize error rates and facilitate faster settlement. In turn, the faster settlement means less risk in the financial system and lower capital requirements.

About the Author:

Kannan Subbiah is a management professional with 27 years of overall experience in IT Project, Product and Program Management, Enterprise & Solution Architecture and Design & Deployment. One can subscribe to his daily digest at Tech-Bytes by Kannan Subbiah.

© 2018 IndraStra Open Access | DOI: 10.5281/zenodo.1202390

Digital Identity – A Gateway to All Other Use Cases

Dr. Benno Ferrarini, Dr. Julie Maupin, and Marthe Hinojales

Every aspect of human development rests upon the bedrock of trusted identity. Without a verifiable identity of some kind, it is impossible to open a bank account, start a business, conclude a legally binding contract, access essential government services, obtain educational credentials, or conduct just about any other imaginable type of economic or social activity on a broader scale [1]. State authorities attempt to fill this gap by issuing official identities to natural and legal persons falling within their jurisdiction. They do so by issuing written documents such as birth certificates and *citizen identification (ID)* numbers, which can in turn be used to obtain both locally recognized identity-related documents (identity cards, driver's licenses, marriage certificates, tax ID numbers, business licenses, etc.) and globally recognized ones (e.g., passports). This process works better in some states than others. Today, around 1.1 billion people worldwide—particularly in rural Africa and Asia—still lack legal identities (World Bank 2017). It was for this reason that the *United Nations (UN)* in 2015 made the provision of legal identities for all, including birth registrations, an explicit focus of its revised Sustainable Development Goals (UN SDGS 2017).[2]

But even once legal identities have been issued, the question of how to keep official records continuously up-to-date remains problematic. A never-ending string of ordinary events can necessitate the alteration, suspension, or revocation of legal identities and the various entitlements associated with them. Births, deaths, marriages, name changes, declarations of court-determined legal incapacity, bankruptcy or insolvency, and many other events can alter the legal rights and duties attached to a particular identity. Even economically advanced 'good governance' states have long struggled to find ways of making their many disparate recordkeeping systems talk to one another such that all records are kept current.

This lack of inter-registry communication impedes global development efforts by making it extremely expensive and time-consuming for transacting parties to verify one another's legally

recognized identities and entitlements. This is as true of local transactions as it is of global ones. For instance, a simple contract for the sale of a parcel of land by one neighbor to another requires the verification of both parties' identities and their legal capacity to contract, as well as a verification of the seller's current ownership entitlement to the land. To take a cross-border example, a large international financial transfer requires the verification of the sending and receiving parties' identities, a confirmation of the mutual recognition of those identities by the different countries in question, and a confirmation that neither of them is prohibited under any national or international regulation from transferring money internationally (e.g., by reason of being on a terrorism or money laundering watch list). Similarly, in relation to *Digital Ledger Technology (DLT)*-based trade finance further described below, the global diffusion of a company identifier system will facilitate the risk assessment and ownership tracking necessary for smaller companies in developing countries to be granted access to finance and the global economy.

Benefits

Distributed ledger technologies (DLT) offer a technical solution to this complex problem for the first time in history, and on a global scale. Numerous globally focused startups, including Sovrin, Netki, uPort, Civic, and others, are building DLT solutions for real-time self-sovereign digital identity management. The concept of self-sovereign identity could herald radical changes in the global economic organization by turning the data collection practices and revenue models of many existing internet-era businesses on their heads [3]. More importantly, within the international development context, it promises to enable billions of currently excluded persons to integrate into the global finance and commerce systems. As described in the 2016 Caribou Digital/Omidyar paper:

Open, decentralized systems enable individuals to fully own and manage their own identities, leading to the idea of "self-sovereign" identity systems. These systems use combinations of a distributed ledger and encryption technology to create immutable identity records. The individual creates an identity *"container"* that allows them to accept attributes or credentials from any number of organizations, including the state, in a networked ecosystem that is open to any organization to participate (e.g., to issue credentials). Each organization can decide whether to trust credentials in the container based on which organization verified or attested to them; in

other words, a mortgage company may accept a credential issued by a leading global bank, but not one issued by a local bank. Importantly, this model does not require a state-based credential to be initiated (the state credential can be added at a later time, or not at all), which removes a barrier to adoption.

The flexibility and modularity of the self-sovereign identity approach make it ideal for adoption in developing country contexts where there are significant gaps in official state recordkeeping. In fact, those gaps might make it easier for developing countries to adopt such solutions than more developed ones, where large sunk investments in traditional recordkeeping systems often create institutional path-dependencies and high transition costs.

An example of a development-focused start-up using self-sovereign identity as an anchor for its work is Taqanu, which describes itself as *"a bank for refugees and for people without a fixed address."* Taqanu takes advantage of the fact that, while many refugees don't have identity documents, many do have phones. It allows refugees to sign up to have their social media data compiled and analyzed in a way that makes it possible for regulated banks to verify the refugees' identities to a sufficient degree of probability to offer them basic banking services—even if they can't provide a government-issued birth certificate, passport, or other recognized national identity document.

Providing financial system access to excluded populations is one of the most important developmental use cases of DLTs, and further examples are presented in the following sections. For present purposes, the Taqanu example illustrates that the creation of verifiable digital identities is a gateway issue for pretty much every possible DLT use case. Without them, users of DLT solutions could never trust that their counterparties to a transaction: (i) are who they claim to be, and (ii) are entitled to carry out the intended transaction. Digital identity is, therefore, the key to the success of all other DLT use cases. This renders investment in self-sovereign identity infrastructure a necessary prerequisite for every other type of development assistance for which DLT solutions might be explored.

Risks and Implementation Challenges

In order for its benefits to be realized, advocates of self-sovereign identity posit that three core requirements must be met:

(i) Security—the identity information must be kept secure,

(ii) Controllability—the user must be in control of who can see and access their data, and

(iii) Portability—the user must be able to use their identity data wherever they want and not be tied to a single provider (Tobin and Reed 2017)

Many of the leading actors in this space are cooperating under the auspices of the Decentralized Identity Foundation to make this vision a reality.[4] While the broader vision is shared, however, key implementation details have yet to be agreed upon. For example, the security pillar requires the use of cryptographically secure methods of protecting users' data. Most digital identity service providers today use cryptographic functions based on elliptic curves whose security robustness has been thoroughly vetted within the context of contemporary processing environments. But cryptographers warn these functions will most likely prove vulnerable to hacking with the advent of quantum computing, which may no longer be very far away (The Japan Times 2017).

To guard against this risk, all information stored in a user's digital identity wallet should ideally be stored in a quantum-proof way. This is theoretically feasible using known cryptographic techniques [5]. However, building these into a self-sovereign identity wallet in a user-friendly manner—such that the user does not need any technical knowledge to keep his/her data secure—poses nontrivial design challenges. Addressing these will require systematic adherence to user-centered design principles together with comprehensive beta testing of design features in developing country environments in advance of any live deployment of the technology.

The portability pillar also constitutes a risk at present due to the fact that many of the leading firms in the self-sovereign identity race are building their solutions for a specific DLT, e.g. the Bitcoin or Ethereum blockchains. But data portability requires platform neutrality if it is to mean anything in practice. Digital identity solutions that are open source and platform agnostic (capable of being used across multiple distributed ledgers) may be more likely to deliver high performance at lower cost to users in the long run. There is a risk that hype factors associated with the current popularity of particular blockchains may lead development funders to commission digital identity *'proof of concepts'* tied to those specific blockchains, even if the structural design features of the blockchain in question are not well suited to the long-term

success of the project at hand. To mitigate this risk, development funders should adopt a policy of publishing public tenders for all DLT-based proof of concepts—including those whose financial implications would ordinarily place them below the usual budget threshold for a mandatory public tender call. This can help prevent situations that may lead to lock-in effects.

In addition to these technical risks, the mounting evidence makes clear that digital identity efforts can only assist with the achievement of concrete development objectives if properly situated within a broader reform agenda. Past policy interventions were often premised on the assumption that broader access to birth certificates, for example, would lead to human rights protection and a fairer distribution of resources and opportunities. A 2007 Asian Development Bank (ADB) study tested this assumption directly by investigating whether improved access to some form of legal identity improved the livelihoods of the poor by helping them obtain services, benefits, and other rights *(Vandenabeele and Lao 2007).* Based on fieldwork in Bangladesh, Cambodia, and Nepal, it found that the actual benefits from owning a legal identity are limited by the obstacles encountered in individual country circumstances, and more generally by weak institutions and widespread corruption. In other words, the provision of legal identity must be linked to the delivery of essential services relevant to people's livelihoods in order to have a real-world impact.

Selecting which essential services should be linked to a potential self-sovereign digital identity initiative is also an important policy decision. For example, primary education funding in Nepal premised on the introduction of registration laws and legal identity requirements was found to exclude women and minorities most in need of assistance, because these groups faced the highest barriers to obtaining birth certificates in the first place. Program design should, therefore, take into account the risk that introducing a legal identity regime may limit the range of project beneficiaries. For some essential services, superior development outcomes may be reached by providing them to everyone, with or without identity [6].

Last but not least, poor governance, weak institutions, corruption, and resource constraints fundamentally weaken the state's capacity to enforce laws intended to protect citizens' rights. The provision of legal identity makes little difference in such contexts without complementary reforms in these areas. Although self-sovereign identity systems can fill the void left by a weak state in a circumscribed area of application, its benefits cannot expand without an appropriate

enabling environment. Put differently, legal identity and the technologies underlying it are important facilitating tools, but they cannot substitute for development policy as such.

About the Authors:

Dr. Benno Ferrarini is a senior economist at the Economic Research and Regional Cooperation Department (ERCD), Asian Development Bank (ADB).

Dr. Julie Maupin is a senior researcher at the Max-Planck Institute for Comparative Public Law and International Law in Heidelberg, Germany. She is also a senior fellow at the UCL Centre for Blockchain Technologies (London) and the Centre for International Governance Innovation (Waterloo) and is an advisor to the IOTA Foundation (Berlin).

Marthe Hinojales is an economics officer at the ERCD, ADB.

Copyright:

Endnotes:

[1] In traditional systems, identity was a straightforward matter of community recognition. People transacted with those whom they knew and trusted. While such models worked well on a local level, they proved incapable of establishing trust among parties wishing to transact beyond their immediate communities.

[2] In particular, UN Sustainable Development Goal target 16.9 states: "By 2030, provide a legal identity for all, including birth registration."

[3] Companies like Google, Amazon, Facebook, and Apple—whose revenue models depend upon monetizing the large volumes of data collected from their users—will need to find new ways of generating revenue if users become empowered to decide on a granular level which data they share, with whom, and for what specific purposes.

[4] A good source of information on potential partners for building such a solution is the Decentralized Identity Foundation (http://identity.foundation/). Solutions that are open source and platform agnostic (capable of being used across multiple distributed ledgers, as opposed to tied specifically to one particular blockchain) are probably more likely to deliver high performance at low cost to the users in the long run.

[5] For a lay description, see Wikipedia. "Post-quantum Cryptography." https://en.wikipedia.org/wiki/Post-quantum_cryptography.

[6] Prenatal healthcare and childhood vaccination

 | DOI: 10.5281/zenodo.1202390

References:

1. World Bank. 2017. “Identification for Development.” http://www.worldbank.org/en/programs/id4d (accessed 25 October 2017). programs may be examples.

2. United Nations (UN) SDGS. 2017. “Targets and Indicators.” https://sustainabledevelopment. un.org/sdg16(accessed 25 October 2017).

3. Tobin, Andrew, and Drummond Reed. 2017. “The Inevitable Rise of Self-Sovereign Identity.” Sovrin

4. Foundation White Paper. p. 10.https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

5. The Japan Times. 2017. “University of Tokyo Pair Invent Loop-Based Quantum Computing Technique.” Sep 24. https://www.japantimes.co.jp/news/2017/09/24/national/science-health/university-tokyo-pair-invent-loop-based-quantum-computing-technique/#.Wd9ayBOCwdU

6. Vandenabeele, Caroline, and Christine V. Lao, eds. 2007. Legal Identify for Inclusive Development. Manila: Asian Development Bank. https://www.adb.org/sites/default/files/publication/29046/legal-identity.pdf

Blockchain in Automotive Domain

Rahul Guhathakurta

The *"Blockchain"* is a revolutionary database that does away with the weaknesses of traditional solutions for storing big data. It provides a transparent record of the entire business network, allowing buyers and sellers of each vehicle to track where the vehicle is in its lifecycle. The blockchain as a technology is more of a ledger recording *"agreements".* It is a system which contains a continuously growing list of records, called blocks, which are linked and secured using blockchain-based *Public Key Infrastructure (PKI)* encryption. It also provides a complete history of *"deals"* made between two or more parties, in which the record cannot be altered retroactively without the alteration of all subsequent blocks and the collusion of the network.

Upstream Application

The advantages of the blockchain are valuable, to say the least. Automotive manufacturers can partner with a blockchain service provider to create a unique ledger among its network of *original equipment manufacturers (OEMs)* as well. It can help them to address the issues related to parts quality and the cases of fictitious pickups to strengthen its logistics monitoring and control. Like, one can cut tracking time of a particular shipment or series of shipments from several days to seconds. With improved traceability, both automotive manufacturers and OEMs can ensure the authenticity of parts delivery at assembly level milk runs.

Software-based Manufacturing

Software-based manufacturing based on blockchain can easily increase the manufacturing productivity and quality; significantly reduce the expenses for tracking in regards to warranty, maintenance and recycling purposes. Factors related to extra inspections about the product fabrication, version management, and recalls/callbacks would also, be simplified.

For an example, a unique sensor can be added to each and every parts pallet before it is shipped from *original equipment supplier (OES)*-end and tracks its real-time status and location, to

 | DOI: 10.5281/zenodo.1202390

ensure that the shipment complies with the *expected time of arrival (ETA)* at the assembly dock. This entire works in conjunction with the *Internet of Things (IoT)* to form an effective anti-counterfeit strategy by using countermeasure technologies based on blockchain principles, where each supply chain partner proactively takes part in updating the status (attributes) of the item as it traverses from point of sourcing to point of manufacture to point of sale. The whole concept demands an extensive and exhaustive level of cooperation among automotive manufacturers, OEMs, software developers and cyber security firms at a scale that has never been achieved before.

Downstream Application

Vehicular Maintenance

On July 25, 2017, Renault, the French automaker announced a pilot project to digitized its car maintenance program, which uses blockchain as a shared ledger to log all car repair and maintenance history in one place. According to Renault, currently, the information about a vehicle's maintenance history is kept by a range of sources, including repair shops and dealerships, making it harder to keep track of new changes. By contrast, the blockchain-based digital maintenance log prototype puts all of this information in one place. The next pilot, it says, will focus on vehicle-based micro transactions – essential to integrating the IoT with the exchange of value.

Automotive Finance & Vehicle Leasing

Automotive financing varies somewhat by the nature of the transaction, typically it includes a host of verification steps to which blockchain could be applied for efficiency gain over the traditionally cumbersome processes like customer bank validation along multiple phases of transaction set up in compliance with *know your customer (KYC)*, loan approval; review of multiple documents sourced from different locations; scoring and classifying risk; archiving of reviewed documents; etc. A blockchain-enabled smart contracts, which will allow these files to automatically negotiate payment on a new car lease and other terms and conditions with the prospective leaseholder, without the need for a middleman. It will also ensure the execution of secure crypto-payments to the necessary parties.

A dedicated blockchain system can also provide most-needed transparency of information about a vehicle's real wear and tear would help the auto finance provider to more accurately gauge the residual value of the vehicle as the lease approached its end of contract date. For example, an *On-board Diagnostic-II (OBD-II)* device connected vehicle over a defined mobile network, would enable capturing of data like driving behavior events (mileage, hard break threshold exceeded), safety events (airbag deployed, part replacement warning), service events (annual service, part replaced), etc., and get sent to a shared ledger that all parties had access to, including the owner/leaseholder. This, in turn, would enable the auto finance provider to achieve a higher price at subsequent onward sale than would otherwise be possible.

Fleet Tracking

The same fundamental of OBD-II devices can be deployed, riding over a blockchain infrastructure, which, in turn, can enable fleet companies to push & pull OBD-II messages, fetch the gyroscope inclination, along with GPS position of a vehicle or a fleet in real-time. Further, it can be enhanced and integrated with *Electronic Logging Devices (ELD)* in compliance with the *Federal Motor Carrier Safety Administration (FMCSA)* mandate, providing an all-in-one tool that streamlines every facet of a truck driver's job. A cloud-based, blockchain-driven fleet tracking can solve the key issues related to drivers, dispatchers, and fleet owners often face with the best hardware and software available in the market, while also fetching a reasonable rate of *return on investment (ROI)* in near future.

Conclusion: An Integrated Application

Overall, a dedicated multi-tier interconnected blockchain platform based on the fundamentals of scalability and interoperability can benefit many stakeholders, like - a shared ledger - between automotive manufacturers, automotive dealerships, regulators, auto finance-cum-insurance companies, vehicle leasing companies, buyers, sellers and even garages, providing a higher degree transparency and trust in all kind of vehicular transactions, preventing disputes and lowering the overall cost of maintenance and services by tracking ownership, sale, and accident history. And, at the same time, it could significantly streamline processes, especially those that rely on regulatory and compliance approvals. The blockchain is all about bringing in

 | DOI: 10.5281/zenodo.1202390

transparency and efficiency into the existing systems which are running the upstream and downstream supply chains and making them more proactive and predictive.

About the Author:

Rahul Guhathakurta is a Founder/Publisher at IndraStra Global. He is a seasoned retail and supply chain consultant with cross-industry experience spanning across 3 continents.

© 2018 IndraStra Open Access | DOI: 10.5281/zenodo.1202390

Military Applications of Blockchain Technology

RADM Dr. S. Kulshrestha (Retd.), INDIAN NAVY

"Blockchain protocols are a new class of protocols that are extremely resilient to attack – they gain that resiliency by virtue of being decentralized," - Professor Emin Gun Sirer, Cornell University

Blockchain technology is fundamentally a mutually trustable storage facility for information transaction between multiple users. It is a decentralized and secure way to record, share, store, and redistribute information. There is no central authority controlling the Blockchain; it is run, monitored, and owned by everyone. Anyone can download it free and run it or develop it for new applications/types of transactions, just like an open source code. It enables verification of the transactions at any time without impinging upon the privacy of the involved parties. Blockchain technology has the capability to become a disruptive technology during the current decade itself.

"A Blockchain is a magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every pro-gram are always publicly visible, and which carries a very strong crypto-economically secured guarantee that programs running on the chain will continue to execute in exactly the way that the Blockchain protocol specifies." - VitalikButerin of Ethereum

Two main pillars of Blockchain technology are the 'distributed consensus' and 'anonymity' [1]. It has applications in both the financial and the non-financial fields. In the non-financial sector major companies like IBM, Amazon, Samsung etc. are exploring innovative ways in which to use the Blockchain technology. The near-term possibilities include putting 'proof of existence' of health data, legal papers, registry certificates (birth, marriage, death), a digital trail of assets etc in the Blockchain.

IBM and Samsung have developed a system called ADEPT [2] (Autonomous Decentralized Peer To Peer Telemetry) that uses design concepts of Bitcoin to construct a distributed network of an

© 2018 IndraStra Open Access | DOI: 10.5281/zenodo.1202390

Internet of Things. The ADEPT utilizes three protocols-BitTorrent (file sharing), Ethereum (Smart Contracts) and TeleHash (Peer-To-Peer Messaging).

In the financial sectors, big banks find Blockchain a secure and reliable technology and are looking into a host of applications. R3, a financial technology firm is creating a framework for financial applications [3] using Blockchain technology for a consortium of 15 leading banks. R3's Corda distributed ledger platform was used by the banks to design and use self-executing transaction agreements. Two prototypes were created using distributed ledger technology for smart contracts. The consortium included Barclays, BBVA, BNP Paribas, Commonwealth Bank of Australia, Danske Bank, ING Bank, Intesa Sanpaolo, Natixis, Nordea, Scotiabank, UBS, UniCredit, US Bank and Wells Fargo.

Military Applications

The NATO Communications and Information Agency is currently evaluating proposals in areas of application of Blockchain technology relating to military logistics, procurement and finance, Internet of Things, and other applications of interest to the military. The proposals have been submitted as part of the 2016 Innovation Challenge [4] aimed at accelerating transformational, state-of-the-art technology solutions in support of NATO C4ISR and cyber capability requirements.

U.S. Department of Defense (DoD) had raised a critical need for a secure messaging and transaction platform accessible via a web browser or standalone native application. DARPA has therefore sought proposals vide SBIR 20162[v] to *"Create a secure messaging and transaction platform that separates the message creation, from the transfer (transport) and reception of the message using a decentralized messaging backbone to allow anyone anywhere the ability to send a secure message or conduct other transactions across multiple channels traceable in a decentralized ledger."*

*"Whenever weapons are employed … it tends to be a place where data integrity, in general, is incredibly important," …"So nuclear command and control, satellite command and control, information integrity are very important."[*6] - Timothy Booher, Blockchain program manager, DARPA.

 | DOI: 10.5281/zenodo.1202390

Critical Weapon Systems

DARPA has awarded a $1.8 mn contracts [7] to Galois for their Blockchain application Guardtime Keyless Signature Infrastructure KSI, to Verify Integrity Monitoring System for its potential to build a form of unhackable code for an enhanced security in critical weapon systems. KSI can detect advanced persistent threats (APTs) which work to remain hidden in networks. Galois works in the area of formal verification, which is a technique that provides mathematical assurances that a system works only as intended in all cases.

Conclusion

The blockchain is a promising technology. However, as is the case with all new technologies, the following are relevant:

- Users would have to get used to the fact that, under Blockchain technologies, electronic transactions are safe, secure and complete.
- Since it is in its nascent stage, scaling up presents issues which need to be resolved.
- Legal frame work has to be modeled to include Blockchain technology.
- Migration of systems from existing centralized databases and systems could be tedious and expensive.

The fact that modern militaries are focusing on applications of Blockchain technology implies that the day is not far when its applications will percolate down to civil applications and to the common man. Further, possibilities of illegal use of Blockchain technology and hacking distributed networks may be a feasibility at a future date especially when quantum computing matures.

About the Author:

RADM Dr. S. Kulshrestha (Retd.), INDIAN NAVY, holds expertise in quality assurance of naval armament and ammunition. He is an alumnus of the NDC and a Ph.D. from Jawaharlal Nehru University, New Delhi. He superannuated from the post of Director-General, Naval Armament Inspection in 2011. He is unaffiliated and writes in defense journals on issues related to Armament technology and indigenization.

Publication Details:

This article was originally published in a blog maintained by Centre for Land Warfare Studies, New Delhi and it is republished on IndraStra with the permission of Author and the Original Publisher.

References:

1. BlockChain Technology Beyond Bitcoin, Sutardja Center for Entrepreneurship & Technology Technical Report, http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf

2. IBM Reveals Proof of Concept for Blockchain-Powered Internet of Things, http://www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things/

3. Peyton, A., R3 blockchain consortium gets smart on trade finance, http://www.bankingtech.com/551002/r3-blockchain-consortium-gets-smart-on-trade-finance/

4. NCI Agency innovation challenge, https://www.ncia.nato.int/NewsRoom/Pages/160425_Innovation.aspx

5. DoD 2016.2 SBIR Solicitation, http://www.acq.osd.mil/osbp/sbir/solicitations/sbir20162/index.shtml

6. Smart, E., US Pentagon May Use Blockchain Tech For Nuclear Warhead Defense, https://cointelegraph.com/news/us-pentagon-may-use-blockchain-tech-for-nuclear-warhead-defense

7. Ruubel, M., Guardtime Federal and Galois Awarded DARPA Contract to Formally Verify Blockchain-Based Integrity Monitoring System, https://guardtime.com/blog/galois-and-guardtime-federal-awarded-1-8m-darpa-contract-to-formally-verify-blockchain-based-inte

 | DOI: 10.5281/zenodo.1202390

How the Blockchain will Transform Housing Markets

Dr. Danika Wright

An emerging technology, blockchain, could transform the way we buy and sell real estate by doing away with the hidden costs and inefficiencies of our housing markets.

Blockchain is an online ledger that records transactions. It's capable of recording the movement of any kind of asset from one owner to the next.

It's public and isn't owned by any one corporation, there are no charges to record transactions. Its openness ensures the integrity of transactions and ownership, as everyone involved has a stake in keeping it honest.

This means there are fewer intermediaries; less middle-men who increase the costs and time to complete a transaction.

There are risks associated with the system as it's only as strong as the code that supports it, which has come under attack in the past. Despite this, examples from overseas show it is possible to apply this technology successfully to our housing market.

Problems in how the property market is run

For buyers able to find the right property, secure a mortgage and save a deposit, they must also pay for a range of so-called *"hidden costs".* These are additional payments associated with the transaction over the cost of the home itself. Many legal and title-related costs would become near-obsolete in a blockchain system.

The combined costs of title registration, title insurance, and legal fees associated with register the property transfer approach A$1,000 on the average Australian house. Costs continue to rise as the prudent buyer undertakes further due diligence, through building inspection documentation, previous sales records and so forth.

© 2018 IndraStra Open Access | DOI: 10.5281/zenodo.1202390

On top of the financial cost, it then typically takes over a month to settle a real estate transaction in Australia. The blockchain system can speed things up, as currently tedious checks undertaken by hand, move to an automated system overseen and approved by the relevant stakeholders.

There is also the risk that land titles offices with a single database simply get things wrong too. In 2016 it was reported that 300 incorrect certificates had been issued in NSW, with 140 of those being recent property buyers affected by government plans for major motorways in Sydney's west.

There are now concerns that the system's quality could be compromised in several states, including NSW and South Australia, as land titles offices become privatized.

A blockchain real estate market

If blockchain were applied to the property market in Australia, every property would be encoded with a unique identifier. Property IDs already exist in most land registry systems, so these would need to be migrated to a blockchain.

Next, the blockchain ecosystem then needs to have defined who the people behind the transaction are, those stakeholders that include the owner, lender, and government.

Transactions of property are conducted via "smart contracts" – digital rules in the blockchain that process the agreement and any specified conditions. Buying and selling could still take place via agents, or the smart contract can be advanced to incorporate the sale rules and make this decision automatically. The blockchain for each property grows as transactions are added to the ledger.

A housing market without agents, conveyancers and a land-titles office may seem decades away, but a handful of countries have already piloted blockchain land registration system.

In Australia, our current land titles system is among the world's best, but it is not infallible. A range of hidden taxes and transaction costs increase market inefficiencies.

And while the electronic system Property Exchange Australia or PEXA, has brought us to the point of a near paperless property market, it's still an intermediary between the parties and the record of the transfer in the Torrens system - our current land title system.

The added advantage of a blockchain system is in eliminating risks, in particular the risk of records being accessed fraudulently and altered or deleted because it is a permanent and immutable record. This means that a huge amount of computing power would be required, probably along with some collusion, and the alteration is easily detected across the ledger. That's not to say the blockchain system is perfect.

Blockchain's advantage in restricting any changes to historical records becomes a disadvantage when incorrect or fraudulent entries are added. Digital currency managers, Ether and Bitfinex, learned this the hard way through cyber-attacks.

Last year these attacks siphoned off over US$50 million in ether tokens from *"The DAO",* the largest crowd funded venture capital fund. This breach led to a controversial split of Ether into two separate active digital currencies.

Only months later, Hong Kong-based cryto currency trading firm, Bitfinex, had the equivalent of US$68 million stolen by hackers in a security breach reminiscent of the hack that bought down Mt.Gox in 2014. It is little comfort to cautious market regulators that the thieves behind these attacks cannot spend it without revealing their identity on the blockchain.

These hacks demonstrate that blockchain systems are only as secure as the code which supports them. As a nascent technology, its cracks are detected only when they are exposed.

Where blockchain has worked before

Sweden became the first western country to explore the use of blockchain for real estate in July last year. At the time, the Swedish Land Registry partnered with blockchain startup ChromaWay to test how parties to a real estate transaction – the buyer, seller, lender, government – could track the deal's progress on a blockchain.

Other countries at the forefront of blockchain for real estate include The Republic of Georgia, Honduras, and Brazil which announced a pilot program earlier this month. While this might seem like a disparate list, it's in these countries where the long-term potential of a blockchain for real estate are most significant.

 | DOI: 10.5281/zenodo.1202390

Systemic corruption and insecure database management in these countries, and many other emerging economies, is seen as a major constraint on growth and prosperity. Why would you invest in a house, or any other asset, if there is a distinct possibility that the record of your ownership could simply disappear?

With ever increasing demands for improvements to transaction efficiency and local real estate industry giants like CoreLogic appointing research teams dedicated to new technology applications, it might not be long before we see a real estate blockchain system in Australia.

This is an edited version of an article originally printed in The University of Sydney Business School Magazine.

About the Author:

Dr. Danika Wright, Lecturer in Finance, University of Sydney

IndraStra

Global Publishing Solutions

163 W, 71st St., NY-10023

www.indrastra.com | info@indrastra.com