Innovation • Compatibility • Success

STANDARDS UNIVERSITY

June 2019 | Volume 9, Issue 1 | Blockchain

IN THIS ISSUE

Blockchain: A Key Enabler for 5G

ABOUT THE IEEE STANDARDS EDUCATION E-ZINE

Technical standards are formal documents that establish uniform engineering or technical criteria, methods, processes and practices developed through an accredited consensus process. The purpose of this publication is to help raise awareness of standards, show the importance of standards, present real-world applications of standards, and demonstrate the role you can play in the standards development process. Knowledge of standards and standards activities can help facilitate your professional engineering practice and improve technological developments to meet the needs and improve the lives of future generations.

Serving the community of students, educators, practitioners, developers and standards users, we are building a community of standards education for the benefit of humanity.

Join us as we explore the dynamic world of standards!

CONTENTS

Letter from the Editor

EMERGING TECHNOLOGY AND ITS APPLICATIONS REQUIRE NEW STANDARDS

Let's put aside the question whether Blockchain is a real technology or a passing fad – a hype. The ups and downs of your fortunes in Bitcoin and similar cryptocurrencies in the last couple of years may have clouded your views. Short-term or long-term success, or failure, of cryptocurrencies may depend on the success, or failure, of Blockchain, but it is important to recognize that Blockchain and the Distributed Ledger Technology (DLT) have far greater uses in wide-ranging applications.

One such use of Blockchain is as a key enabling technology of 5G applications. Prof. Chaudhry and Dr. Asad present their research to propose a Blockchain-based Network Slice and Resource Brokerage system to build an open, transparent, and fair 5G ecosystem. They explain the challenges of addressing the massive cooperation required among 5G devices and potential solutions using Blockchain.

Another application of Blockchain is in creating and maintaining decentralized electric grid (Smart Grid). In his article, Dr. Claudio Lima explains the emergence of, and the importance of, DLT Blockchain for the electric utility industry. He uses Open Blockchain Energy (OBE) Architecture Framework, an emerging standard, and associated reference model to classify and categorize application segments in the energy industry and shows that the concept extends well beyond the Smart Grid to the entire energy sector.

As the world becomes more connected, consumers and industries – and their respective application ecosystems – will inherently require interaction. As these applications create their own DLT blockchains, they will need interoperable solutions. Dr. Claudio Lima, an authority in DLT and Blockchain technology, brings us interesting challenges and the need for global interoperable standards.

Mr. Meloni from University of Cagliari, Italy uses Blockchain and Internet of Things (IoT) to demonstrate the need for consensus algorithms and different ways of achieving the consensus. He then goes on to present the work on the Real-time Onsite Operations Facilitation (ROOF) standard for technical and functional interoperability of federated IoT systems.

Clearly, the need for standards and interoperability in an emerging technology is even greater at this time to ensure smoother deployment and wider adoption in critical applications.

Are you working on building Blockchain applications? What standards do you use? What challenges do you have? Can they be solved by new standards? Would you like to discuss these topics with fellow engineers? Let us know if we can facilitate such discussions. We are all ears!

Happy Reading.
Enjoy!

"Clearly, the need for standards and interoperability in an emerging technology is even greater at this time to ensure smoother deployment and wider adoption in critical applications."

Yatin Trivedi, Editor-in-Chief, is a member of the IEEE Standards Association Board of Governors (BoG) and Standards Education Committee (SEC), and serves as vice-chair for Design Automation Standards Committee (DASC) under Computer Society. Yatin served as the Standards Board representative to IEEE Education Activities Board (EAB) from 2012 until 2017. He also serves as the Chairman on the Board of Directors of the IEEE-ISTO.

Yatin currently serves as Associate Vice President for semiconductor design services at Aricent Inc. Prior to his current assignment, Yatin served as Director of Strategic Marketing at Synopsys where he was responsible for corporate-wide technical standards strategy. In 1992, Yatin co-founded Seva Technologies as one of the early Design Services companies in Silicon Valley. He co-authored the first book on Verilog HDL in 1990 and was the Editor of IEEE Std 1364-1995™ and IEEE Std 1364-2001™. He also started, managed and taught courses in VLSI Design Engineering curriculum at UC Santa Cruz extension (1990-2001). Yatin started his career at AMD and also worked at Sun Microsystems.

Yatin received his B.E. (Hons) EEE from BITS, Pilani and M.S. Computer Engineering from Case Western Reserve University. He is a Senior Member of the IEEE and a member of IEEE-HKN Honor Society.

Blockchain: A Key Enabler for 5G

by Mohammad Asad Rehman Chaudry & Zakia Asad

A Blockchain received public attention with the widespread speculative, monetary gains generated by the cryptographically secure digital currencies, normally called crypto-currencies or digital money. Bitcoin and Ethereum are two of the most commonly used crypto-currencies with a market cap of more than $132 billion [1]. In actuality, crypto-currencies are just a small piece of the blockchain pie. Applications of blockchain vary from cloud computing to food supply chain. For example, Walmart has recently used blockchain to track the origins of fresh foods as a solution to fight food-borne diseases such as E-Coli. Walmart's implementation has illustrated the ability of a blockchain to reduce parsing time for a very large number of supply-chain records from days to seconds [2]. Blockchain can be thought of as a community-driven, real-time database that is fully decentralized and involves a fairly large number of user-nodes to act as data-keepers. The very structure of blockchain has envisioned a new era of data

management systems that is fully reliable, fault tolerant, scam-proof, accurate, authentic, transparent, trustworthy, and above all free from centralized-control. One of the very first footprints of blockchain can be traced back to a time-stamping digital document where the basic idea was to design a system of transactions that could not be altered and helped to settle transactions in a fair fashion [3]. Curiously, the following prose from Shakespeare summarizes the notion behind blockchain:

Time's glory is to calm contending kings,

To unmask falsehood and bring truth to light,
To stamp the seal of time in aged things,
To wake the morn and sentinel the night,
To wrong the wronger till he renders right

Blockchain, in its simplest form, is a chain of blocks where each block contains some verifiable record(s), and all the blocks are linked through their crypto-hashes. New records are registered (created) by appending new blocks along with their timestamps to the existing chain of blocks.

Blockchain is predicted to be a key player in reaping real benefits from 5G Networks. Its applications range from providing an autonomous platform for resource sharing, enabling ubiquitous edge computing, to content-based-storage; all of which are significantly different than contemporary scenarios associated with 4G [4]. 5G is all about connecting heterogeneous devices and complex networks with a network of more than 50 billion devices[5]. On one hand, millimeter waves and small cells are a critical building block of 5G, and enable high data rates and low latencies in addition to many other benefits. On the other hand, millimeter waves and small cells give rise to several challenges for example low transmission radiis, and interoperability among complex sub-networks. To overcome many of these challenges, 5G devices are expected to perform several collaborative tasks from routing and relaying to computing. For example, 5G can enable holographic communication within short distances without need of any cooperation among devices, but when this distance is large (or network is not homogeneous) the data transfer speed as well as the viability of the service drops significantly. This shortcoming is not limited to holographic communications, but many other realistic applications—ranging from e-health, M2M communications and factories of the future to the real-time analytics—suffer the same fate. In short, cooperation among 5G devices is necessary for its transformative success. Blockchain can enable such sort of massive cooperation as shown in Figure 1. This collaboration is necessary for many crucial scenarios such as network slice brokerage, mobile wallets, edge computing, M2M, healthcare, IoT, mobility management, smart roaming, and spectrum sharing.

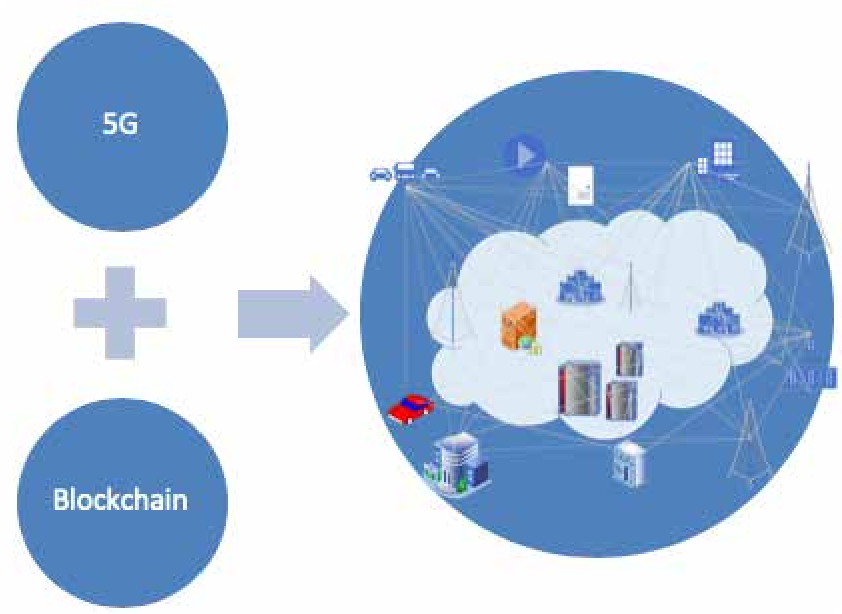
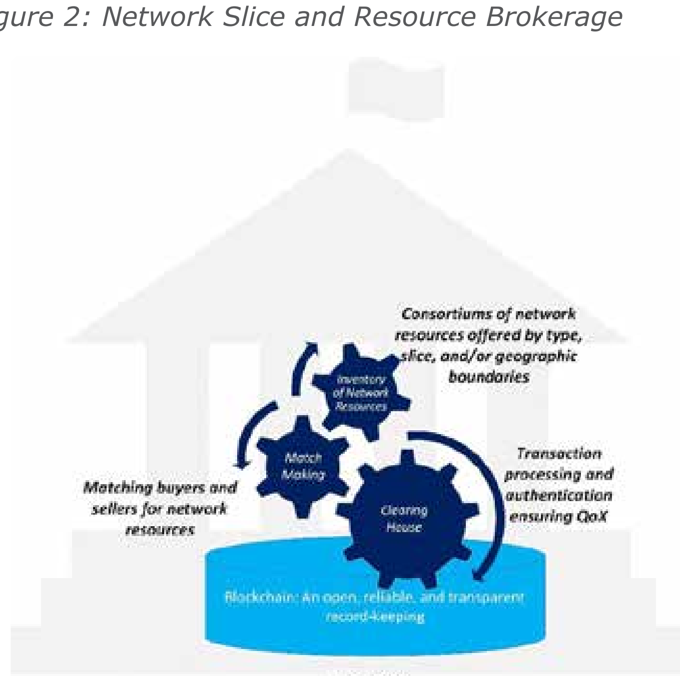


Figure 1: 5G and Blockchain

Network slice and resource brokerage are key enablers to extend the reach of 5G to non- traditional venues. Blockchain can be a key element for successful realization of such ecosystems. Specifically, these ecosystems have a diverse set of requirements from frequent relaying to time-sensitiveness. Ensuring a wide range of requirements over existing infrastructure is a challenge that calls for innovative solutions such as network slicing. Network slicing ensures that a network is tailored to application requirements in an end-to-end fashion. For instance, a network—offered and maintained by several operators—can be partitioned into different slices like a mobile broadband slice, an IoT slice, and a mission-critical slice, to name a few. Resource sharing among end users and devices is going to play a vital role in the success of a network slicing mechanism , e.g., by performing relaying and edge computing. The resource sharing can either be voluntary or associated with some reward. For example, a cell phone user can be offered a reward in terms of an offset in their monthly bills.

A big challenge for network slice and resource brokerage is the need to maintain an open, transparent, and fair system within the extraordinary number of resources and several shady players. Blockchain is a natural choice for such a scenario. Figure 2 presents such a network slice and resource brokerage system developed by us. It consists of the following three major components: 1. Inventory of network resources, which represents a collection of network resources offered by type, slice, and/or geographic boundaries. 2. Match making, which matches buyers and sellers for network resources. 3. Clearing house, which deals with the transaction processing and authentication while ensuring QoX. Here "X" stands for the performance parameter as per a buyer's requirements., e.g., QoS, QoE, etc. Figure 3 depicts a realization of our proposed system, with the focus on blockchain dynamics, for a specific transaction where a user "A" requests a network resource from user "B".

Figure 2: Network Slice and Resource Brokerage



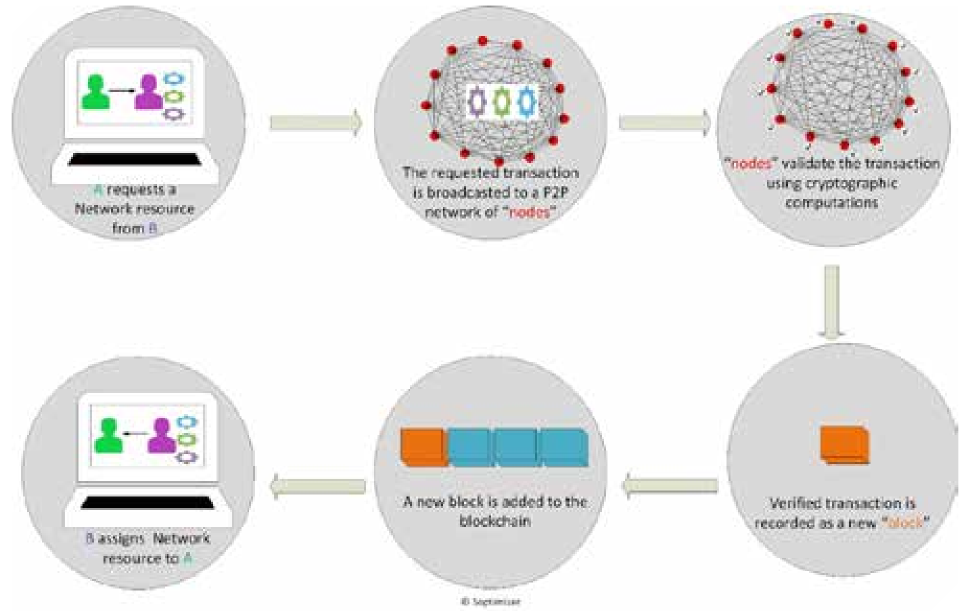


Figure 3: Resource Brokerage: Blockchain Dynamics

References:

1. "CoinMarketCap Cryptocurrency Market Capitalizations," Nov, 2018. https://coinmarketcap.com/
2. K. Nash, "Walmart-Led Blockchain Effort Seeks Farm-to-Grocery-Aisle View of Food Supply Chain," The Wall Street Journal, Jun 25, 2018.
3. S. Haber, W. Stornetta, "How to time-stamp a digital document." In Conference on the Theory and Application of Cryptography, pp. 437-455. Springer, Berlin, Heidelberg, 1990.
4. M.A.R. Chaudhry, " Joint IEEE Spectrum and ComSoc Talk, Test and Measurement Virtualization and Blockchain: Enablers for 5G Networks," Nov 13, 2018. https://bit.ly/2Qefaor
5. D. West, "How 5G technology enables the health internet of things." Brookings Center for Technology Innovation 3 (2016).

Mohammad Asad Rehman Chaudhry
is a seasoned professional, innovator, and thought- leader with extensive experience in multi-disciplinary projects in Information and Communication Technologies. Dr. Chaudhry received a PhD in electrical and computer engineering from Texas A&M University. He currently spearheads projects in Blockchain, Software Defined Ecosystems, Big Data Systems, Next Generation Networks, and System Optimization. He is the Chair for The Institute of Electrical and Electronics Engineers Standards for Software Defined and Virtualized Ecosystems (SDN/NFV Performance). He is also Co-Founder and the Executive Director with Soptimizer, a Canadian start-up providing services and solutions to disruptive technologies.

Some of his previous roles include High Performance and Exascale Systems Team with IBM Research, a Research Fellow with Hamilton Institute, University of Toronto, a Network Scientist with RCUH for DARPA System F6, an Assistant Director of Huawei-UET Technology Joint Telecom Center, as well as a Faculty Member of the Electrical Engineering with the University of Calgary, and the University of Engineering and Technology. He is a recipient of the Fulbright Fellowship, the Presidential Scholarship, the Texas A&M Class Star Award, and Ontario Graduate Scholarship. He is an Ambassador, and a Diversity Champion for Rotman School of Management at the University of Toronto, Canada.

Zakia Asad
received a PhD in electrical and computer engineering from the University of Toronto, Toronto, Canada. She is the CTO with Soptimizer, Canada. She possesses extensive experience of both academia and industry, and has successfully led several projects ground-up.

Dr. Asad received the Schlumberger Fellowship, Edward S. Rogers Sr. Scholarship, Texas A&M ECE Scholarship, a PITB Fellowship, and Prof. KU Medal.

Key Benefits of Blockchain on Education and Science

by Paolo Tasca

I. Introduction

New technologies are impacting and changing both traditional and modern industries alike. No sector is exempt from this revolution, and that includes education. Indeed, the education sector has already begun transforming, as seen in the digital shifts that are increasingly necessary to improve the experience of students and youngsters alike and to prepare them for the jobs of the future which at this moment are still unimaginable (Schwartzbeck and Wolf, 2012). The education system has the essential social task of developing minds that will be able to mix past disciplines with new fields of discovery. This is one of the most important functions of government and is vital not only for individuals but for society as a whole. Universities and institutions can take advantage of key developments like cloud storage, big data, and blockchain solutions to improve learning experiences and offer better services to students.

II. Problems

The educational, cultural and knowledge system as a whole has always faced risks and problems with difficult solutions. First of all, most academic and professional institutions issue certificates and credentials that are difficult to verify. Employers and third parties seeking to verify a single resume are often required to use inefficient and expensive procedures to test the authenticity of all aspects of the applicant's experience. As expected, companies rarely have the time and resources required for those procedures and therefore they don't even verify the content. In addition, many diplomas are not digitally verifiable. It seems that only a few institutions release free and online certifications. In the case of qualifications obtained in the past, the situation is even more complicated. To give a sense of the scale of the problem, the UK Higher Education Degree Datacheck (Hedd) surveys students and graduates about degree fraud every year. The results are pretty alarming – about a third of people embellish or exaggerate their academic qualifications when applying for jobs (The Guardian, 2014).

> "Old-fashioned organizational paradigms and a conservative attitude toward innovation have prevented the widespread institutional adoption of new technologies in general."

Secondly, in recent years there has been a surge in the number of unverified degrees issued by legitimate-sounding institutions. These organizations often advertise themselves as official institutions with names that closely resemble those of famous academies, such that the distinction between them is not immediately apparent. This problem is aggravated by increased counterfeiting of diplomas and certificates. The proliferation of institutions raises an important question as to the quality of educational systems and universities, which is difficult to evaluate in a quantitative way. Institutions very often issue diplomas or certificates with scant or absent details as to the course of study pursued and the student's achievements. Employers, evaluators, and recruiters thus find themselves in the difficult position of having to consider documents of doubtful provenance, which are not standardized, and with possibly low image quality. These and similar problems might find solutions in blockchain technology.

III. Blockchain

Initially introduced as a technology to support the functioning of a decentralized payment system outside the brokering circuit of central banks, distributed-ledger technologies have evolved from both a quantitative and a qualitative perspective. In addition to the Bitcoin network, many other distinct blockchain systems have been developed and go beyond the simple transfers of funds, by implementing different and/or supplementary functions (Tasca & Widmann 2018). Currently, there are thousands of blockchain systems worldwide, some running on forks of successful technologies such as Bitcoin or Ethereum, while others propose completely new functionalities and architectures. For this reason, instead of 'blockchain', we can refer to blockchains or blockchain technologies in order to encompass all the possible architectural configurations and also, for the sake of simplicity, the larger family of distributed ledger technologies, i.e., community consensus-based distributed ledgers where the storage of data is not based on chains of blocks (Tasca & Tessone 2019).

Despite the technical rivalry and variation, the underlying philosophy still remains substantially unchanged: blockchains enable new forms of distributed software architecture where agreement as to the shared state of decentralized and transactional data can be established in a network of peers (network nodes), which may be untrusted and anonymous (and potentially dangerous). The distributed nature of the blockchain networks requires participants to reach a consensus on transaction data under a predefined set of rules that govern the update of a shared register (ledger). The data of past transactions are ordered in the ledger and cannot be altered except by agreement of the majority of peers. Two core cryptographic technologies ensure and authenticity of each transaction: (i) public-private key infrastructure used to store and spend money; and (ii) cryptographic validation of transactions (Böhme et al., 2015). Cryptographic technologies can thus create a "trustless" infrastructure to enable transactions: the trust is directly guaranteed by the blockchain system without the need of third parties (De Filippi and Wright, 2018). There is no integration point or central authority required to approve transactions and set rules. No single point of trust, no single point of failure.

Until recently, high schools and universities have not thought of using blockchain technologies to solve or mitigate the problems set out above. Old-fashioned organizational paradigms and a conservative attitude toward innovation have prevented the widespread institutional adoption of new technologies in general. This is partly due to the fact that the benefits of new technology are typically undermined by the high costs of training people in its use. With blockchain, however, the benefits of this trade-off weigh decisively in favor of technological adoption. In fact, the fundamental characteristics of a blockchain address each of the key administrative challenges facing high schools and universities: data transparency, auditability, availability, immutability, and efficiency. In other words, it makes all the internal processes more efficient.

The benefits of blockchain apply primarily to data collection, processing, and sharing. The main beneficiaries are:

Students. Blockchain could provide higher security and robustness to their data: the use of high-security cryptographic techniques ensure that personal information will never be manipulated or subject to malicious data leaks or (unauthorized) commercial surveillance. Students could also benefit by using self-sovereign identity solutions to certify their identity without needing to share the underlying data that make up that identity. Indeed, access to educational services pass through a robust ID system that allows uncontroversial identification; however, according to the World Bank, only about one-third of the global population currently holds a national ID that enables access to the education system (USAID, 2017).

Universities and other institutes of education. Fully automated data processing benefits high school, colleges and university registrars who handle (typically, manually) sensitive and confidential student records. These records include but are not limited to attendance records, immunization records, grades, transfer information, transcript requests, etc. University registrars could be removed from the verification process altogether. As a result, considerably fewer resources would be devoted to qualification verifications and more time can be spent on higher priority tasks, such as verifying the school qualifications of prospective students.

Employment agencies and Job Seekers. Employers might, in fact, avoid the expensive, complicated and lengthy processes involved in background checks and evaluations of job applicants; agencies might speed up the job seeking process by easily proving the authenticity of applicants' academic qualifications.

In terms of areas, blockchain can be applied to:

Transcripts. Academic credentials must be universally recognized and verifiable. At the moment, verifying academic credentials remains largely a manual and expensive process (heavy on paper documentation and case-by-case checking). Blockchain solutions could streamline verification procedures and reduce fraudulent claims to unearned credentials.

Students records and certificates. Students' records and any other type of accreditation can be stored in a blockchain. Digital records and certificates hold many advantages over paper records and certificates: they require far fewer resources to issue, maintain and use. The veracity of any record can be verified automatically, without human intervention. The security of the records derives from the security of cryptographic protocols, which ensure that any extract or certificate is cheap to produce but extremely expensive to reproduce by anyone other than the issuer. Finally, any issuer-fraud, such as changing the timestamp or changing a certificate serial, is not possible in a blockchain environment.

CV. Blockchain can enhance fraud detection and prevention. This would free up administrative resources by reducing the amount of work needed to process credential verification requests. In addition, blockchain is useful in this way not only for academic institutions but also for employers and third parties, such as job seekers. The former might avoid the expensive, complicated and lengthy processes involved in background checks and evaluations of job applicants; the latter might speed up the job seeking process by more easily proving the authenticity of their academic qualifications.

Libraries. Blockchain could help libraries expand their services by building an enhanced metadata archive, developing protocols to support community-based collections, and facilitating more effective management of digital rights.

Peer reviews and scoring. Thanks to blockchain, the review process could be open to any peer in a given community in a transparent way. Authors could be scored/rated automatically by the nodes in the blockchain network as opposed to by a handful of peer reviewers.

IP rights. Currently, tracking intellectual property is a costly endeavor run by specialized, usually when there is a significant business incentive to do so. Time-stamping scientific discoveries protects against the misuse of intellectual property. Blockchain could also enable a model of open innovation and open educational resources whereby we would eliminate intermediaries such as fee-based journals, thus allowing anyone to publish openly, accurately keeping track of re-use without putting limitations on the source material. Each contributor would be directly rewarded based on the level of actual use and re-use of their educational materials, similar to how researchers would be rewarded based on citations to their papers.

Publishing. Blockchain could have multiple applications in the publishing industry, from securing new talent to rights management, and anti-piracy efforts. This is true not only for the scholarly publishing community, but also for journals, magazines, and any other kind of content publishing. New platforms are emerging to level the playing field for writers and encourage collaboration among authors, editors, translators, and publishers. Smart contracts on top of the blockchain can streamline sharing, licensing, and usage of digital rights.

However, all that glitters is not gold. A problem that is worth highlighting is the complex relationship between blockchain and well-established regulations, among which a particular challenge is data protection. With the recent enactment of the General Data Protection Regulation (GDPR), data need to be exchanged in accordance with definitive standards, and subject to certain essential rights. Some of these (the right to be forgotten and data reduction, for instance) are not easily enforceable when it comes to blockchain and DLT. Blockchain architectures will, for instance, either need to store raw personal data off-chain or provide some mechanism for the deletion of private keys where these give access to an individual's data. Whether regulators would find such implementations compliant with GDPR remains to be seen. Thus, the path to widespread adoption of the technology in the education sector is still long, and many challenges remain.

References
The Guardian, (2014) 'Degree deceit: does it pay to lie on your CV?', https://www.theguardian.com/careers/careers-blog/lie-degree-cv-jobseekers-graduate

Böhme, R. et al. (2015) 'Bitcoin: Economics, Technology, and Governance', 29(2), pp. 213–238. doi: 10.1257/jep.29.2.213.
De Filippi, P. and Wright, A. (2018) Blockchain and the Law. Harvard University Press.

USAID, 2017, 'Identity in a Digital Age. Infrastructure for Inclusive Development'. Technical Report, https://www.usaid.gov/digital-development/digital-id/report

Schwartzbeck, T. D. and Wolf, M. A. (2012) The Digital Learning Imperative: How Technology and Teaching Meet Today's Education Challenges. Digital Learning Series.

Scott, P. (2000) 'Globalisation and Higher Education: Challenges for the 21st Century', Journal of Studies in International Education. doi: 10.1177/102831530000400102.

Tasca, P., & Widmann, S. (2017). The challenges faced by blockchain technologies–Part 1. Journal of Digital Banking, 2(2), 132-147.

Tasca P, Tessone CJ. 'A Taxonomy of Blockchain Technologies: Principles of Identification and Classification'. Ledger. 2019 Feb 15;4.

Paolo Tasca
Executive Director, UCL-CBT
Mentor of the Supercharger Program

Paolo Tasca is a Digital economist specialising in P2P financial systems. An advisor on blockchain technologies for different international organisations including the EU Parliament and the United Nations. Paolo is founder and Executive Director of the Centre for Blockchain Technologies (UCL CBT) at University College London. Prior to this, he was Lead Economist on digital currencies and P2P financial systems at Deutsche Bundesbank, Frankfurt working on digital currencies and P2P lending.

Paolo is the co-author of the bestseller FINTECH Book and the co-editor of the book Banking Beyond Banks and Money. In addition, he is author of various scientific papers about blockchain, which have been published by prestigious international scientific journals, such as the Harvard Business Review. As Executive Director of the UCL CBT, Paolo is also directly involved in various research projects concerning different application fields of blockchain technologies. Among them, the BARAC Project (Blockchain Technology for Algorithmic Regulation and Compliance) supported by EPSRC, and the P2P-IoET Project (The Internet of Energy Things: Supporting peer-to-peer energy trading and demand side management through blockchains) supported by Lloyds Register Foundation.

Dr Tasca holds an M.A in Politics and Economics (summa cum laude) from the University of Padua and a M.Sc. in Economics and Finance from Ca' Foscari, Venice. He did his PhD studies in Business between Ca' Foscari Venice and ETH, Zürich. His doctoral dissertation on systemic risk in financial markets was subsidized by the Swiss National Science Foundation with more than 500.000 €.

Other current appointments are: Permanent Member of ISO TC 307 committee on standardisation of blockchain systems at the International Organization for Standardization (ISO); Member of the DLT/1 technical committee at the British Standards Institution (BSI); Honorary Research Associate at Univeristy of Cape Town Financial Innovation Lab; Honorary Research Associate of CFS at Goethe University; Research Associate at the Systemic Risk Centre of the London School of Economics; Research Associate of the Institut de Recherche Interdisciplinaire Internet et Société; Senior Advisor of the Beihang Blockchain & Digital Society Laboratory in Beijing; Board member of the Cyprus Blockchain Innovation Centre.

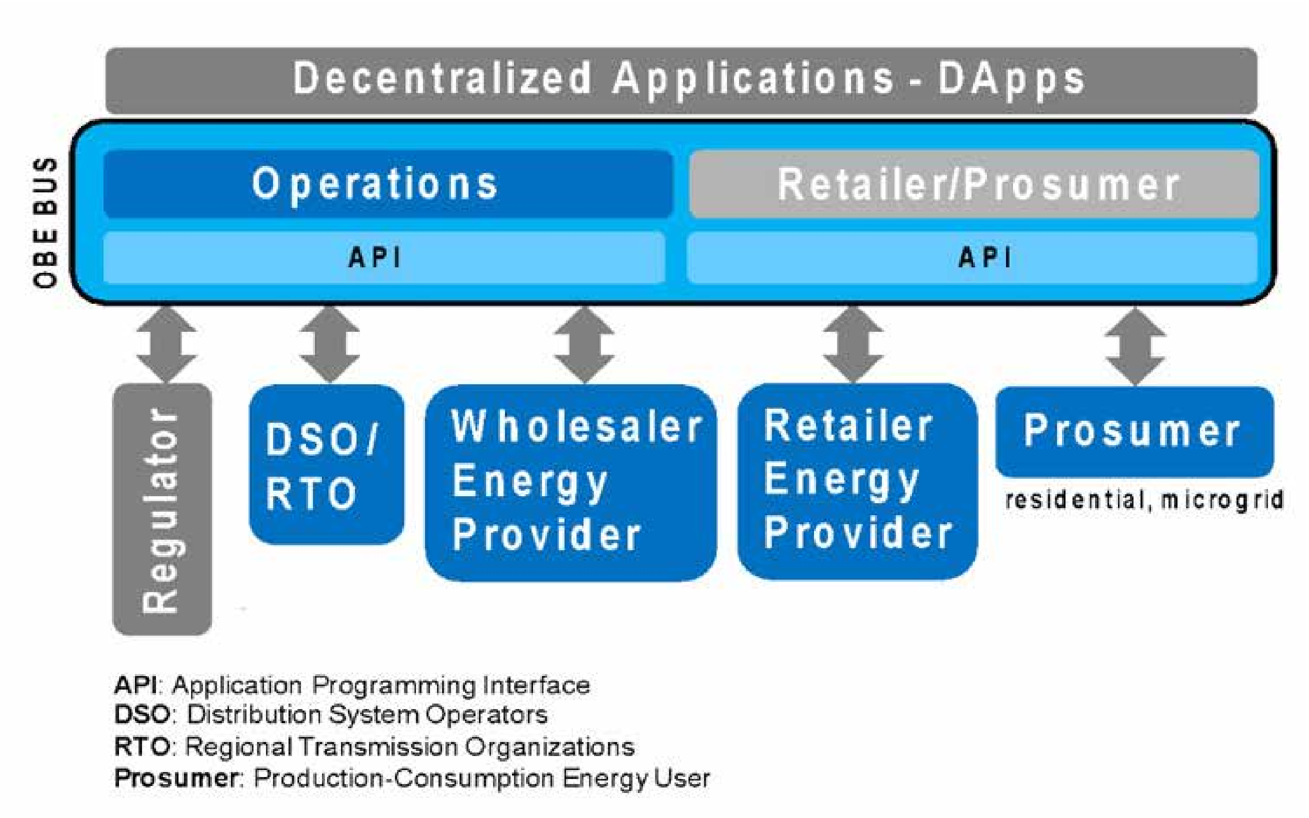
Towards an Open DLT Blockchain Energy Standard for Decentralized Grid Applications

by Dr. Claudio Lima, Ph. D.

Introduction

Blockchain is defined as a distributed ledger technology (DLT) that is becoming the underlying layer of the future of the Internet. It is creating a new wave of decentralized services applications, called "DApps," that will be introduced to replace most of today's centralized, cloud-based Internet applications. Permissioned, enterprise, and consortium-based DLT Blockchain has been considered as a new enabling technology layer of information technology (IT) enterprise systems and processes, used in industry vertical markets to improve IT operations, security and process efficiency [1,2].

DLT Blockchain is being introduced in the energy vertical, particularly in the utility grid sector, to reduce costs, improve security, disintermediate processes, speed transactions, register and authenticate grid assets and data and improve all smart grid operations [3]. On the other hand, new Blockchain-enabled transactive energy models have been defined and introduced at the consumer and edge side of the grid, which may reshape traditional grid business models, enabling a new wave of decentralized services. Utilities will experience a new level of digital transformation by adopting DLT Blockchain technologies, which can be considered as an evolution towards grid modernization.



Open Blockchain Energy (OBE) Framework

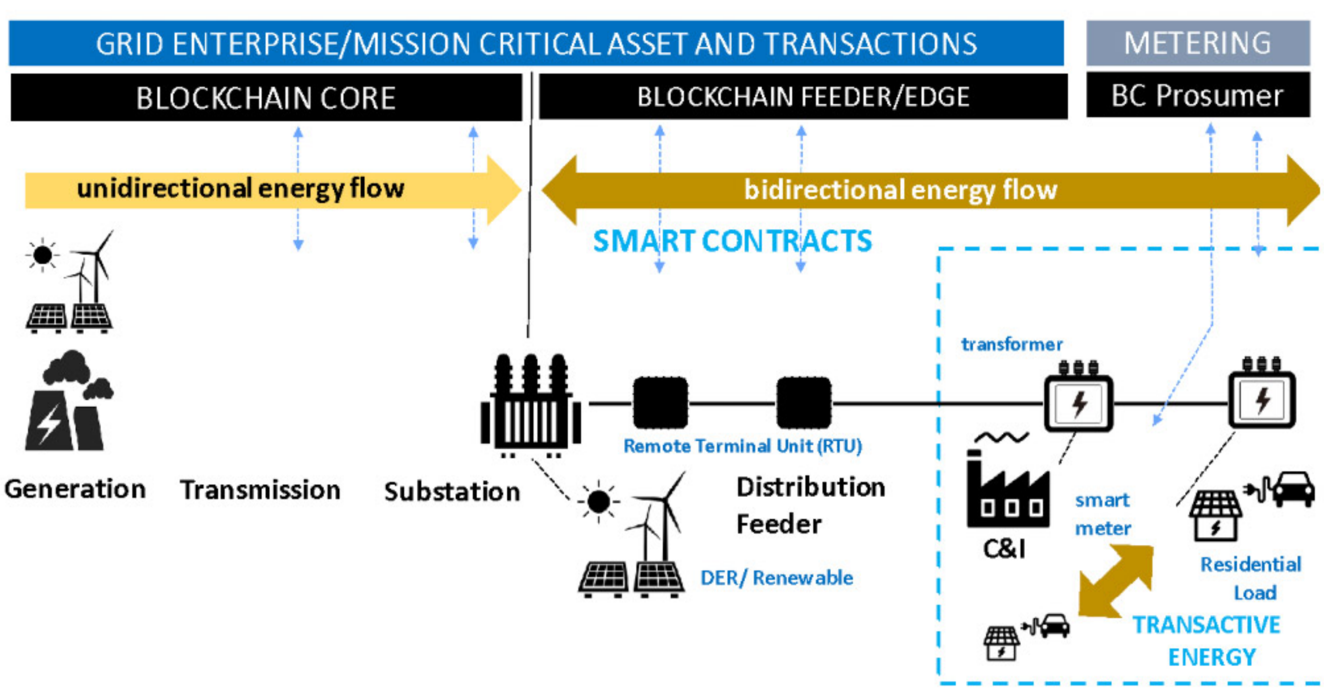
Before DLT Blockchain is considered in the energy sector, it is important to understand, classify and categorize all its applications segments, and define key concepts and frameworks. For this reason, a new Open Blockchain Energy (OBE) Architecture Framework is proposed and under consideration by the IEEE Standards Association, to create the first concepts on how to segment the DLT Blockchain processes, functionalities, applications, and use cases in the energy grid, which can be harmonized to enhance existing smart grid standards [4].

The distributed ledger OBE BUS contains two main segments. One related to mission critical, secure, and scalable grid operations (Blockchain core and edge); the other on the prosumer (producer and consumer of energy) or customer-facing side (Blockchain prosumer). Both will have DLT Blockchain segment-specific open application programming interfaces (APIs) to support multiple Blockchain grid applications segmentation. The operations segment can support high performance, high security, and mission-critical industrial grid Blockchain operations, where distribution system operators (DSOs) and regional transmission organizations (RTOs) work as participants in the process, as well as wholesaler energy providers, such as independent power producers (IPPs). On the consumer-facing side of the grid, a multitude of new Blockchain applications can be developed, where retailer energy providers, residential and microgrid prosumers can be connected to OBE open APIs. For each grid segment, a set of distinguished Blockchain decentralized applications (DApps) can be developed. This framework can be further evolved and detailed to accommodate more specific grid domains and applications in the near future. An Open Blockchain Energy reference model is needed to drive new grid services, improve and optimize the existing ones and eventually introduce new Blockchain-enabled transactive energy regulation in the energy sector. Figure 1 shows the preliminary concepts of the OBE framework

Fig. 1 – Open Blockchain Energy (OBE) Framework (source: Blockchain Engineering Council-BEC IEEE standards contribution)

End-to-End DLT Blockchain Grid Segmentation

In the energy grid industry vertical, there is no one-size-fits-all DLT Blockchain solution. There are distinct processes, type of assets, and functional requirements that distinguish a typical grid electricity end-to-end solution. For instance, from the generation all the way to the distribution substation, there is a need to control and secure mission-critical assets that are isolated from most of the grid-edge and enterprise processes. This core grid segment, particularly at the transmission and distribution (T&D), substation, and grid edger (feeder side) are currently run by synchrophasor network, supervisory control and data acquisition (SCADA), and DNP3 protocols, evolving towards the IEC 61850 object-oriented protocol. The last mile segment is the prosumer customer-facing side, which includes all customer loads, electric vehicle charging stations, residential and commercial roof-top solar and batteries, with lots of renewable energy penetration at the edge and consumer side.



Based on these definitions, the DLT Blockchain energy grid solutions can be further classified into three main segments—Blockchain core, Blockchain edge/feeder, and prosumer. Each segment has their own grid devices and equipment, which are an essential part of the modern grid. From the T&D side, there are bulk renewable and fossil fuel generation, transmission lines, and substations. From the grid edger/distribution feeder-side, there are important grid elements, called remote terminal units (RTUs), such as capacitor banks, reclosers, voltage regulators, volt-var, transformers, etc. From the consumer-generation side (prosumer), there are smart meters, roof-top solar with connected electrical vehicle charging stations and energy storage systems. Each grid element can be a source/sink that generates its own "smart contract," which is a Blockchain "what..if" embedded software logics. The enterprise and mission-critical permissioned Blockchain platforms can connect to existing grid enterprise/SCADA management system, such as energy management systems (EMS), distributed energy resources management systems (DERMS), and also to enterprise advanced metering infrastructure (AMI) solutions, using grid device smart contract logics that can contain important grid events, transactions, and asset identification that need to be registered and authenticated in the DLT Blockchain shared database. This shows the importance of identifying the critical assets and transactions and defining the levels of security and performance for each Blockchain grid segment. It is very important to create these isolated and federated Blockchain segments to improve grid security, scalability and performance, addressed by the 2P2S (performance, privacy, security, scalability) design principles [1]. Figure 2 shows the end-to-end DLT Blockchain framework with three distinct segmentations of the grid.

Fig. 2 – End-to-End Grid DLT Blockchain Framework Segmentation (source: Blockchain Engineering Council-BEC IEEE standards contribution)

Key Takeaways

Currently, there is a lot of of misconception in understanding that Blockchain technology can be applied beyond bitcoin or cryptocurrency applications and therefore can provide tremendous value to the utility of the future. The vast majority of the energy/utility regulatory commissioners are still trying to understand how Blockchain can be used in regulated and unregulated energy markets and how it can play in distributed transactive energy services that may disrupt traditional grid-centric generation models. In most cases, however, Blockchain is associated with high energy consumption scenarios due to the bitcoin mining proof-or-work (PoW) consensus algorithm, which is creating a new and unexpected distributed load to be managed by utilities. However, it is just a matter of time before more deployments are validated and the Blockchain value proposition is realized by grid-energy operators and consumers.

In parallel, there is a strong need to create standards in the DLT Blockchain Energy vertical. With this proposition, the IEEE Standards Association (SA) established in September 2018 the IEEE P2418.5 DLT Blockchain in Energy Standards Working Group [5], which is charged with developing the first global standards to address DLT Blockchain reference architecture, end-to-end framework design, interoperability requirements, and use cases to drive technology adoption.

In summary, DLT Blockchain technologies will be a critical enabling technology for grid modernization, introducing new decentralized services, operational, and cybersecurity models for energy/utilities.

References

[1] C. Lima, "Blockchain Architectures and Framework – System-of-System Approach", IEEE NIST Blockchain Global Summit 2018, NIST, Sep 2018. [2] C.Lima, "Developing Open and Interoperable Distributed Ledger Technology (DLT)/ Blockchain Standard, IEEE computer society, December 2018

[3] C. Lima, "Digital Enabled Blockchain Energy in Grid Modernization", special issue of European Union Parliament Magazine on Blockchain, November 5th, 2018.

[4] C. Lima, Smart Grid IEEE 2030, ETSI, April 2011. [5] IEEE P2418.5 Blockchain in Energy Standards WG, https://standards.ieee.org/project/2418_5.html.

Dr. Claudio Lima, Ph.D. Blockchain Engineering Council, BEC Co-Founder IEEE Blockchain Standards Working Group Vice-Chair Dr. Claudio Lima is a seasoned technology executive and thought leader in Advanced Blockchain, IoT and AI technologies with expertise in energy (utilities, oil and gas), smart city and telecom/IT digital transformation. He has a Ph.D. in Electronic Engineering at the UKC (England). Previously he was the Global Smart Grid CTO of Huawei Technologies in Europe-Asia-Pacific and a Distinguished Member of Technical Staff (DMTS) at Sprint Advanced Technology Labs (Sprint ATL), in Silicon Valley-CA. Dr. Lima currently leads the IEEE Blockchain Standards development as Chair and Vice-Chair of IoT and Energy Working Groups. He also serves as the Blockchain Cybersecurity Industry Advisory Board Member of the Department of Energy (DOE)/PNNL.

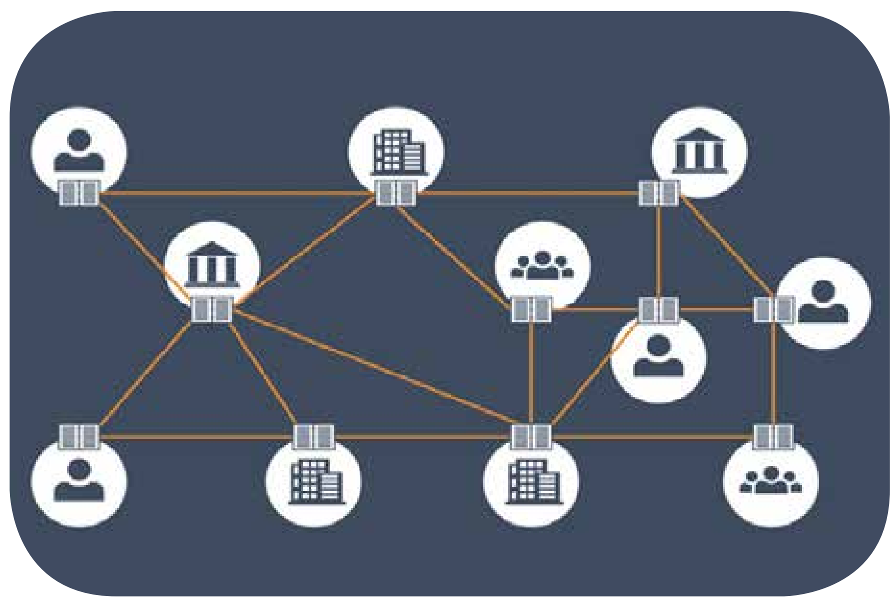
Distributed Ledger Technology (DLT) Blockchain Interoperability Standards

by Dr. Claudio Lima, Ph. D.

Introduction

Distributed Ledger Technology (DLT)/ Blockchain is being introduced as the new Internet layer of value, adding the "trinity of Ts" [1]—trustability, transparency, and traceability—to any asset class transaction (information/ data and physical goods) in the Internet that can be authenticated, validated, traced and registered in a distributed, peer-to-peer (P2P) digital ledger system [2], also addressing data privacy and security [3]. Blockchain is also part of a broader scope of Distributed Ledger Technology (DLT) that is becoming the underlying layer of the future of the Internet, creating a new wave of Decentralized Applications, called "DApps," that will be introduced to replace most of today's centralized, cloud-based Internet applications. With Blockchain, businesses will experience a complete transformation of their current models by removing intermediaries, reducing costs, and improving the trustability of the Internet—and, therefore, enabling a new wave of decentralized services.

DLT is an enabling technology of the new information technology (IT) enterprise system and processes, with substantial work developed on the permissioned, enterprise- and consortium-based Blockchain side, addressing real IT problems and vertical-market solutions. Hybrid public-enterprise-consortium DLT Blockchain architecture frameworks are expected for future use case applications that create an inter-working and interoperable Interchain solution, similarly to what happened with Intranet and Internet networking in the early 80s.



Fragmented Industry and the Need for Interoperable Standards

Currently, the Blockchain industry is completely fragmented with different alternatives, such as, open and proprietary platforms that support permissioned or permissionless, public, enterprise or consortium-based solutions. In addition, there is no relevant consistent standardization across different technologies and platforms to address the issues of interoperability or interworking.. Therefore, interoperability is becoming an important topic that needs to be addressed if the DLT Blockchain industry ecosystem wants to survive in the near future [4], where today, standards for global mass Blockchain adoption are still lacking.

DLT Blockchain Interoperability: The New Standards Frontier

Most of today's Blockchain standards activities are focused on specifying and developing generic frameworks, interfaces, and technology modules that work in self-contained or specific platform environments, or industry vertical market [4,5]. Once more complex uses of DLT Blockchain are required across multiple enterprise segments, between enterprise or consortium-based and public (permissionless), or between multiple enterprises to run more complex use cases, requirements, and implementations, then there will be a strong need for an end-to-end DLT Blockchain interoperability standards [4]. A typical set of DLT Blockchain

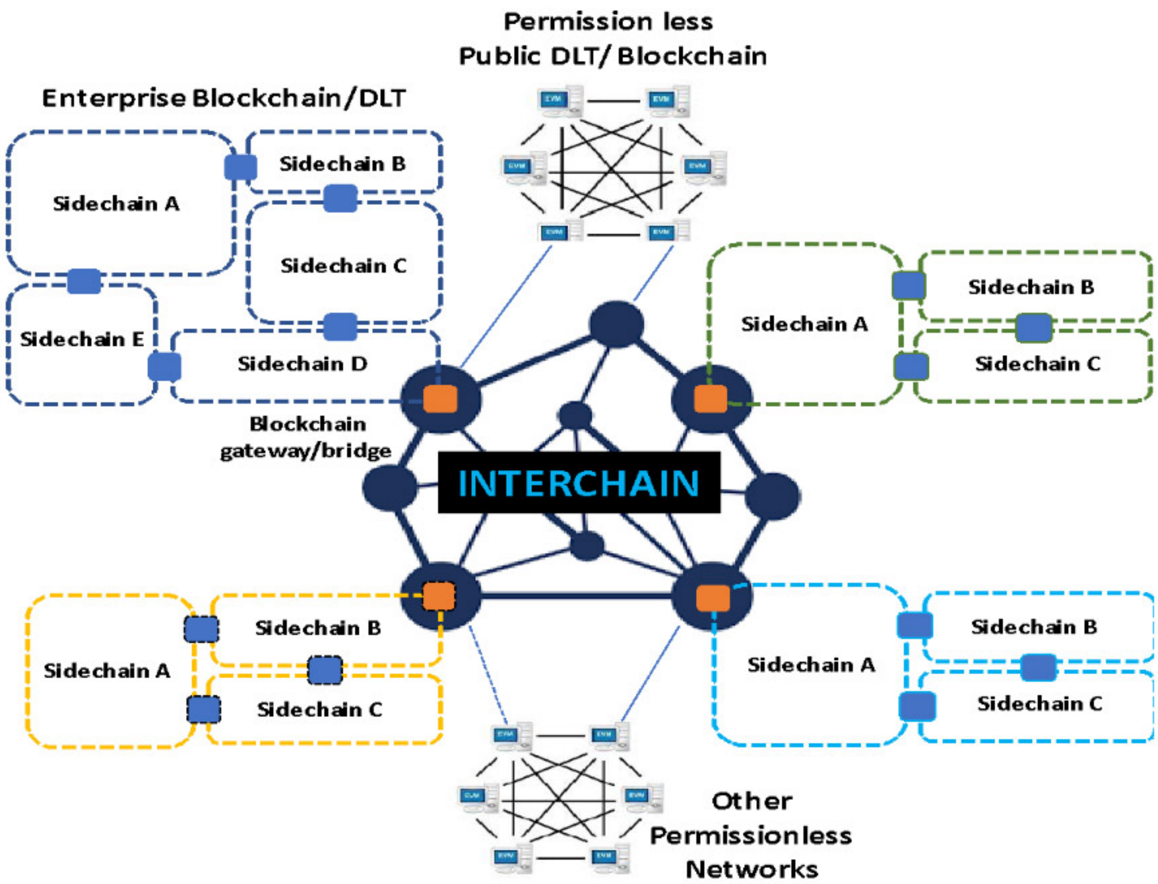


Figure. 2 – DLT Blockchain interoperability between permissioned and permissionless networks. source: Blockchain Engineering Council-BEC

standards with focus on interoperability and scalability are among several industry Blockchain requirements that are essential for the survival and mass adoption of Blockchain as an enabler of the decentralized Web 3.0 Internet.

In particular, the IEEE Blockchain in Energy WG global standards [5] is currently working to address the need for DLT Blockchain open and interoperable standards for the energy industry, which is considered to be a complex multi-segment, multi-domain vertical market requiring multiple DLT Blockchain solutions that are open and interoperable, where the concept of "one size fits all" does not apply. In this new standards proposal, the end-to-end energy grid segmentation, with different types of DLT Blockchain frameworks are used to address a particular set of use case applications. Each segment will have its own DLT solution, that at some point, may need to interoperate with other segments to transfer value, assets, and tokens between these multiple platforms. This is just one application of a particular industry vertical. Similar concepts can be extended to other industry segments.

Cross-Chain Interoperability for Decentralized Applications (DApps) and Inter and Intra-token Transactions
It is expected that within the next few years, there will be a strong need for cross-chain interoperability between different enterprise-grade (permissioned) and public (permissionless) DLT systems, where different platforms will interact with one another to make the development of unified or multi-wallet DApps with inter- and intra-token transactions between different Blockchain platforms much easier, efficient, scalable, and pervasive. Multiple sidechains (a special class of Blockchain) will be required, each performing a specific DLT function, and interoperability between these multiple network segments shall be defined using a common-ground protocol, or some bridge/gateway artifact. This will be the ultimate requirement for the creation, consolidation, and interconnection of multi-DLT Blockchain technologies, as the future of decentralized networks and services (also called Interchain)

Key Takeaways
Creating open and interoperable DLT Blockchain standards is an important step to connect multiple open source and proprietary technology platforms that are geographically dispersed, and serve different industry verticals and use cases. This is an important step for the evolution of Blockchain as an enabler of the Internet of Trust and the new enterprise IT layer. Global standards, such as the IEEE Blockchain standards series, are addressing these generic and interoperable frameworks.

References

[1] C.Lima, "Blockchain Is The New Internet— The Trinity Of Ts," https://goo.gl/hq7ACy

[2] C.Lima, DLT/Blockchain Architecture and Reference Frameworks, 2018 IEEE NIST Global Blockchain Summit, NIST, Maryland, Sep. 17th, 2018.

[3] C.Lima, "Adapting Blockchain for GDPR Compliance", InformationWeek, https://goo.gl/QmBHgE

[4] C.Lima, "Developing Open and Interoperable Distributed Ledger Technology (DLT)/ Blockchain
Standard, IEEE computer society, December 2018 (upcoming).

[5] IEEE P2418.5 Blockchain in Energy Standards WG, https://standards.ieee.org/project/2418_5.html.

Dr. Claudio Lima
(lima@blockchain-eng.org) Dr. Claudio Lima is a seasoned technology executive and thought leader in Advanced Blockchain, Internet of Things (IoT) and AI technologies with expertise in energy (utilities, oil and gas), smart city and telecom/IT digital transformation. He has a Ph.D. in Electronic Engineering from the University of Kent -UKC (England). Previously he was the Global Smart Grid CTO of Huawei Technologies in Europe-Asia-Pacific and a Distinguished Member of Technical Staff (DMTS) at Sprint Advanced Technology Labs (Sprint ATL), in Silicon Valley-CA. Dr. Lima is co-Founder of the Blockchain Engineering Council (BEC), and leads the IEEE Blockchain Standards development as Chair and Vice-Chair of IEEE Energy and IoT Standards Working Groups, respectively. He also serves as the Blockchain Cybersecurity Industry Advisory Board Member of the US DOE/PNNL.

Blockchain Consensus for the Internet of Things

by Dr. Alessio Meloni

Blockchain-based IOT solutions are well suited for simplifying business processes while reducing overall costs and security threats. As an example, IoT can exploit blockchain technology to build trust among untrusted devices or federated IoT areas, reduce infrastructure costs, and accelerate data exchanges.

Currently, connections among non-trusted devices pass through remote nodes (e.g., cloud systems) even if IoT devices are within a few meters from each other. This brings a number of significant disadvantages such as high maintenance costs, weakness for supporting time-critical IoT applications [1], security and trust issues.

Adopting a standardized blockchain model among the billions of devices envisioned in the IoT domain [2] would significantly reduce the costs associated with centralized and remote data and computation centers. While the literature offers some examples of blockchain deployment in IoT [3], up to now there is no de facto standard solution. Due to the massive number of devices and resource constraints, deploying blockchain in IoT while maintaining a good balance of the triad performance-scalability-reliabilty is particularly challenging. The optimal blockchain architecture has to scale to many IoT devices and it should be able to process a high throughput of transactions.

To this, consensus algorithms assume a central role since they are the groundbase of any existing Blockchain and define how transactions are validated. While the initial rationale behind Blockchain was its capability to ensure consensus among untrusted parties in a public and freely accessible network, further developments have broadened the plethora of transaction validation as well as the means of access restriction and blockchain node organization (private, federated, distributed, or public) in order to shape the triad performance-scalability-reliability according to the particular needs of a certain domain. IoT is not an exception. In the following paragraphs, the current state of the art in blockchain consensus is presented before discussing ongoing standardization efforts related to blockchain deployment in IoT federated networks.

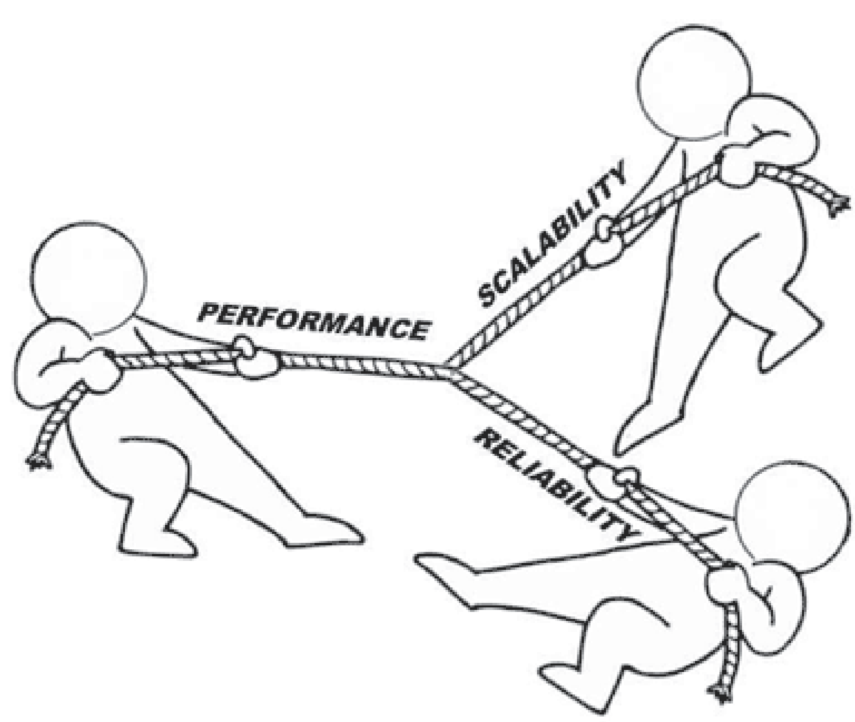


Figure 1: Every Blockchain solution is a tradeoff of performance, scalability and reliability

The father of consensus: Proof of Work (PoW)
The most classic consensus mechanism, which is also the one implemented by the most popular and oldest digital currency (Bitcoin) is the Proof of Work (PoW). In PoW, nodes willing to participate in the creation of new blocks of transactions for the chain (namely miners) solve computationally hard problems in order to be granted such permission. Since various miners (honest or not) might attempt to add blocks to the chain, PoW relies on the concept of the longest chain as the most trustworthy.

This poses the following problems:

- Computational power means powerful calculators consuming energy but having just one miner per block being successful
- Block generation time is a tradeoff between speed and security
- The added blocks have to be validated by the entire blockchain network, resulting in small throughput

Last but not least, PoW is a game of brute force without any binding rules, which we could compare, in history, to those times when the strongest army would win. This means that the rationale of a decentralized system is not necessarily true. The recent hashwar that brought to the hard fork of Bitcoin Cash (BCH) into BCH ABC and BCH SV has revived this point of discussion showing the inherent lack of democracy that PoW has.

A greener alternative: Proof-of-Stake (PoS)
In PoS, blocks to be added to the blockchain are selected by a voting procedure involving all blockchain nodes that

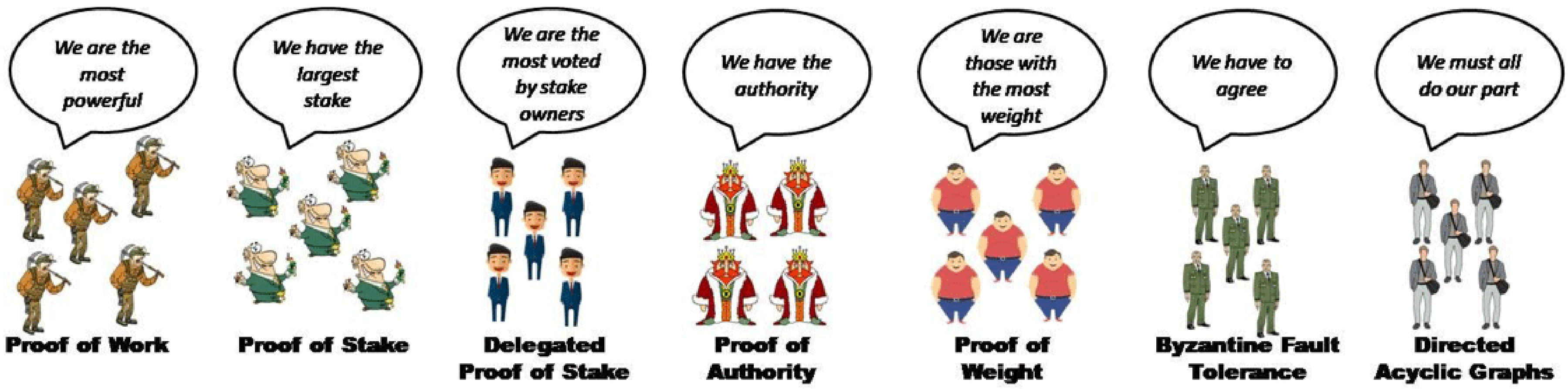


Figure 2: Consensus algorithms for the Blockchain

have a stake.Their voting power is related to their stake. This means that no energy is wasted in a computational task ending in itself. In case of a fork, nodes decide which fork to support. Due to this last point, a well-known problem of this consensus mechanism is the so called "Nothing at Stake," where nodes can vote for both sides of every fork that happens without any computational effort required, thus mining the credibility of the blockchain.

Concerning PoS democracy, while a stake of more than 50% would allow control of the blockchain, it is believed that such a big stake amount is hard (yet not impossible) to own. Nevertheless, voting power modifications of PoS are considered, where weighting the stake by other properties, such as the time a certain stake has been owned, is used. While all these countermeasures might improve security, they are strictly related to the domain of interest and the way stakes are used by blockchain nodes.

Representative democracy:
Delegated Proof-of-Stake (DPoS)
In DPoS, token owners vote to elect delegates to validate blocks on their behalf. The voting power is dependent on the number of tokens and the votes can be redirected at any time. The number of delegates depends on the blockchain but are usually in the range of dozens. As an example, EOS Blockchain has 21 delegates also called block producers. Blocks are delivered by block producers in a shuffled order. By apriori selecting block producers, the blockchain can be designed to run more efficiently and with higher throughput and lower block production times (in the fraction of seconds) without the drawbacks found in PoW and PoS. Indeed, in DPoS block producers collaborate to make blocks instead of competing like in PoW and PoS. In addition, the EOS Blockchain does not charge nodes for transactions, but rather considers their stakes as determining the amount of network, cpu, and RAM power that nodes can use.

Centralized by design: Proof-of-Authority (PoA)
In PoA, transactions are validated by approved accounts (the authorities). This allows high throughput (as in the case of DPoS) but with an oligarchic rather than democratic approach. For this reason, PoA finds its best application in private blockchains where apriori trusted nodes are used because of the scalability and performance benefits, despite the lack of decentralization.

Generalizing PoS: Proof-of-Weight
Proof-of-Weight is a general term used to refer to consensus algorithms leveraging on some kind of node property that determines their power in the consensus procedure. It can thus be considered as a further generalization of PoS and PoW. Indeed the weight could be the stake or the computational power, but also something different that is related to the specific application domain of the blockchain. As an example, the concept of trustworthiness in the Social Internet of Things [4] could be used.

Byzantine Fault Tolerance (BFT)
BFT consensus algorithms apply solutions derived from the Byzantine generals problem to the Blockchain. In the Byzantine generals problem, a certain number of generals are separated by distance and have to pass messages through the enemy zone in order to communicate and converge to an agreement on whether to attack the enemy or not. A partial agreement would result in a defeat (namely a fault). Some of the consensus algorithms found in the literature derive from BFT. As an example, in Practical Byzantine Fault Tolerance (PBFT), groups of nodes share a leader who is elected using an election algorithm. If the leader fails, a new leader will be elected and a new group is created. This consensus mechanism typically requires multiple rounds among nodes to reach an agreement, which leads to huge communication overhead and limits scalability and its use in a public Blockchain in which the choice of leaders could be problematic.

Participatory Democracy:
Directed Acyclic Graphs (DAGs)
DAGs use a form of consensus that handles transactions asynchronously and in which every node willing to make transactions can do so by validating previous transactions. This theoretically opens up to a number of transactions per second, which is not upper-bounded. The most well-known consensus algorithm in DAG is the Tangle, which is used in the IOTA implementation. In the Tangle, in order to send a transaction, two previous transactions that have been received need to be validated. This policy strengthens the validity of transactions as more transactions are added to the Tangle. However, if not many transactions are made and a single node can generate one third of the total transactions, it could take over which validations are labeled as true. For this reason, IOTA uses the concept of a "coordinator" that checks the validity of transactions in the booting phase during which not many nodes participate. The good thing about Tangle is that it is designed with IoT micro-transactions in mind. However, it does not provide an architecture or data structure to decentralize IoT and it is not Turing complete, meaning that scripts and smart contracts are not allowed.

Standardization of Blockchain consensus for the IoT
The IEEE 1931.1 Working Group is currently working on

the definition of an Internet standard for technical and functional interoperability of federated IoT systems for Real-Time Onsite Operations Facilitation (ROOF) that operate and function in a secure, semi-autonomous, and decentralized manner. Blockchain technology can play a key role in accomplishing this goal and is thus being investigated by the Working Group [5].

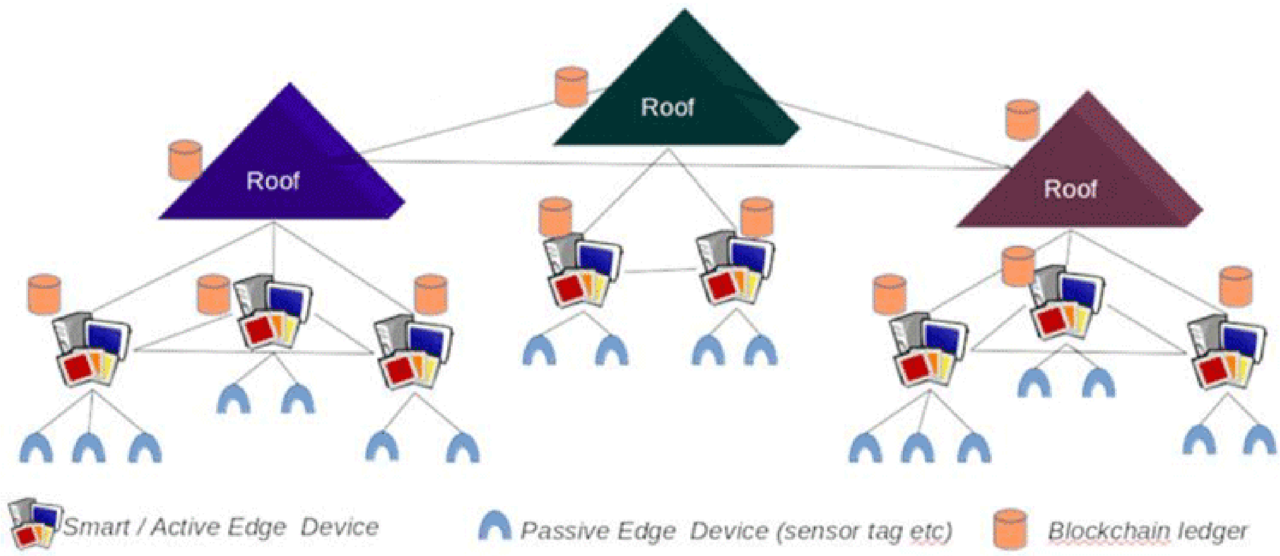


Figure 3: Blockchain architecture in the ROOF context [5]

From ROOF's perspective, the Things in an IoT application should be able to operate and cooperate within the context of a local environment in a secure and independent manner. In other words, each local IoT network deployment should be able to act autonomously and connect to other federated networks when needed or for added value. Blockchain fits perfectly in this context.

Each federated network should respond to their specific requirements. Some federated networks could be more or less restricted in terms of access and data retrieval from the outside; some could even decide to use consensus algorithms suitable for realtime applications or for IoT devices with constrained computational capabilities such as PoA or DPoS, which would leave the role of interfacing with the "public blockchain" and the other federated networks to one or a set of trusted nodes. Other federated networks in which IoT entities are untrusted and dynamically join and leave the network would be more likely to leverage on other consensus mechanisms, such as a Proof-of-Weight, based on the trustworthiness of devices or on how long that device has been part of the federated network.

Yet, the problem of connecting all these federated networks with different blockchain requirements (i.e., blockchain interoperability) remains. One area that is showing promise in this sense is the use of sidechains [6]. Sidechains allow for a specific use case to be addressed, while still being able to interoperate with the outside blockchain world by creating ways in which one blockchain or sidechain can successfully communicate with another blockchain or sidechain in a "workflow" configuration. The main threat regarding this point and thus a key point to tackle in order to advance the state of the art, is that the amount of work it requires to achieve interoperability between an ever-growing number of federated chains as use cases and applications in the IoT domain grow.

Conclusions

Computationally complex consensus mechanisms are not suitable for IoT scenarios and the resources needed to reach consensus must be wisely allocated. A federated network made of different interoperable blockchains responding to the specific domain requirement and interacting by means of gateways or sidechains to the public blockchain network is more likely to become the standard for blockchain deployment in the IoT. Although DPoS currently looks like the most promising for transactions in a public federated blockchain, none of the current consensus algorithms are yet to be deployed in IoT as a standard adoption and the characteristics of each consensus algorithm need to be further evaluated and optimized in order to fit the IoT application domain.

References

[1] A. Meloni, P.A. Pegoraro, L. Atzori, A. Benigni, S. Sulis, Cloud-based IoT solution for state estimation in smart grids: Exploiting virtualization and edge-intelligence technologies, Computer Networks, vol. 130, 2018, pp. 156-165.

[2] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[3] S. Huh et al., "Managing iot devices using blockchain platform," in Advanced Communication Technology (ICACT), 2017 19th International Conference on. IEEE, 2017, pp. 464–467.

[4] M. Nitti, R. Girau and L. Atzori, "Trustworthiness Management in the Social Internet of Things," in IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 5, pp. 1253-1266, May 2014.

[5] A. Meloni et al., "Exploiting the IoT Potential of Blockchain in the IEEE P1931.1 ROOF Standard," in IEEE Communications Standards Magazine, vol. 2, no. 3, pp. 38-44, September 2018.

[6] A. Back et al., "Enabling Blockchain Innovations with Pegged Sidechains", https://blockstream.com/sidechains.pdf.

Alessio Meloni (meloni@ieee.org) is with the Department of Electrical and Electronic Engineering at the University of Cagliari, Italy. His research interests include the Internet of Things, Smart Grids, Blockchains, and embedded systems for the IoT. He is a member of IEEE P1931.1 WG.

Funny Pages

Blockchain

by Marketoonist.com