Best of IEEE Blockchain Technical Briefs 2018

Best of IEEE Blockchain Technical Briefs 2018

In This Issue:

Best of IEEE Blockchain Technical Briefs

Chonggang Wang, Editor-in-Chief, IEEE Blockchain Technical Briefs

In this special edition of the IEEE Blockchain Technical Briefs, we are highlighting the top articles of 2018. Sponsored by the IEEE Blockchain Initiative, Technical Briefs feature brief technical articles to inform and advance blockchain and related technologies.

Since launching in July 2018, the IEEE Blockchain Technical Briefs continue to explore new blockchain designs, challenges, applications and standards. If you haven't had a chance to read through our past issues, this special edition is a great place to start. Here you will find the most popular Technical Brief articles from 2018!

1. *Secure and Privacy-preserving Smart Contract-based Solution for Access Control in IoT*
2. *MedRec: Patient Control of Medial Record Distribution*
3. *Auto-translation of Regulatory Documents into Smart Contracts*
4. *A Pentagon of Considerations Towards More Secure Blockchains*
5. *Enabling Multilevel Data Sharing Based on Blockchain and Smart Contract*

If you are working in the blockchain space, we are always looking for new contributors. Look over our editorial guidelines and contact the Managing Editor at blk-editor@ieee.org for more information.

Chonggang Wang received his Ph.D. degree from Beijing University of Posts and Telecommunications (BUPT) in 2002. He is currently a Member Technical Staff with InterDigital Communications. His current research interests include decentralized IoT, semantic computing and services for IoT, fog computing for IoT, IoT data analytics, and advanced IoT services. He also has abundant IoT standardization experience including oneM2M, IETF, IEEE, and ETSI TC M2M. He was the co-founder (2011-2013) and the founding Editor-in-Chief (EiC) of IEEE Internet of Things Journal (2014-2016). He is currently the Associate EiC of IEEE Transactions on Big Data and the EiC of IEEE Blockchain Technical Briefs. He is an IEEE Fellow for his contributions to IoT enabling technologies (2017).

Secure and Privacy-preserving Smart Contract-based Solution for Access Control in IoT

Chao Lin, Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan, China; **Debiao He**[*], Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan, China; **Xinyi Huang**, School of Mathematics and Computer Science, Fujian Normal University, China; and **Kim-Kwang Raymond Choo**, Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, USA

[*]Debiao He is the corresponding author.

IEEE Blockchain Technical Briefs, July 2018

Internet of Things is, as the name suggests, a network of Internet-enabled objects (e.g. sensors and smart devices) with applications in smart homes, smart cities (e.g. medical and health-care settings, and intelligent transportation) [1]. The interconnection of physical objects provides efficient data collection and sharing in IoT applications, although there are also underpinning security concerns (e.g. potential data or privacy leakage). Hence, one particular area of focus it to design an effective and (provably) secure access control scheme to protect related resources (e.g. the collected or processed data) against unauthorized access (or modification).

Conventional access control systems are generally centralized (in the sense of having the same trust domain), which are known to suffer from the following limitations: a single point of failure and lack of support for dynamicity (i.e. the need to be mobile and belong to different management communities) and polycentricity (i.e. the capability to be managed by several managers) in IoT devices. Thus, there has been interest in researching on the role of blockchain in IoT access control (e.g. transaction-based [2][3] and smart contract-based [4][5][6]). Blockchain is a distributed and chronological ledger commonly maintained by public / private / permissioned nodes (corresponding to the three types of blockchain), according to a consensus mechanism such as Proof-of-Work (PoW), Proof-of-Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT) [6]. In other words, blockchain can provide decentralization, verifiability and immutability to enhance security (in conjunction with other cryptographic tools), service availability (avoiding the single point of failure), system scalability (e.g. due to programmable smart contracts), and potentially other features / properties. Despite the potential of blockchain in IoT access control, a number of limitations need to be addressed, and these are as follows:

Pseudonym. The claimed anonymity is mainly guaranteed by allocating some addresses generated from a one-time public key (e.g. Ethereum address) to IoT devices, and clearly it will be challenging to identify a specific IoT device in a large real-world infrastructure such as a smart city (or even a smart campus or university system, such as the University of Texas system that spans 14 institutions). It is also known that there are several ways (e.g. transaction graph analysis [7] and quantitative analysis [8]) to find the connection between an address and it’s concrete entity. Once an adversary can link the allocated address to a specific device, all of the device’s request / management access records will be disclosed; hence, compromising the device’s identity and location privacy.

Non-lightweight. Some blockchain designs use transactions to publish or update access control policy (into the chain directly or via a smart contract). However, this requires the IoT devices to be capable of publishing transactions. However, transactions in some current pervasive blockchain systems (e.g. Bitcoin and Ethereum) are constructed based on the Elliptic Curve Digital Signature Algorithm (ECDSA). This cryptographic primitive may not be able to be deployed directly on IoT systems, particularly resource-constrained IoT devices as these devices generally have limited memory space that cannot support the computational and storage costs required of the ECDSA algorithm.

Policy-public. Blockchain-based solutions generally require the submission of access control policies directly into the blockchain (note that even in smart contract-based approaches, smart contracts' data will be eventually chained into the blockchain) to ensure verifiable-consistency, immutability and hence traceability. Unfortunately, this will also reveal all the access control policies to the public, meaning that anyone can learn the required policies to access IoT devices' resources even when they are not authorized. This will further leak IoT devices' sensitive information beyond the inferred metadata from accessible data.

Insufficiency. From the view of smart contract-based solutions, the proposals do not take secure design of smart contract into account. Smart contracts deployed and executed in practice may contain design flaws and security vulnerabilities, which can be exploited to facilitate attacks such as tokens-stolen, and deadlocked-state [9]. More seriously, once a contract is deployed in the blockchain, it will be immutable; namely, its functionality cannot be modified anymore. Hence, it is important to ensure the security of smart contracts before deploying it in the blockchain.

To solve these issues in existing blockchain-based solutions for access control in IoT, we propose a new smart contract-based solution, combining two cryptographic primitives (i.e. Group Signature, Public Key Encryption) and *FsolidM* [9]. Our proposal comprises the following entities: *owner* (maintaining the access control policy of its IoT devices), *gateway* (publishing the transaction for IoT devices), *IoT devices* (collecting data for owner), and *permissioned nodes* (maintaining the blockchain ledger and serving as a group manager for executing the group signature scheme). We will also briefly introduce the core designs as follows.

- A permissioned blockchain is more appropriate in our context, where hundreds of thousands transactions are conducted within seconds. The use of the permissioned blockchain also offers advantages such as increased privacy control and the ability to modify the cost requirement. Here, we propose adopting *JUICE*[1] (an open service platform) to realize our architecture, because it can support *Solidity* (a programming language designed for writing contracts such as Ethereum). We can also build a user-friendly graphical interface using *Java* and *JavaScript*, and *JUICE* provides a rich set of cryptographic API calls (e.g. homomorphic encryption, group signature, and zero-knowledge proof) for privacy-preserving applications.
- We suggest replacing ECDSA with a group signature scheme (e.g. [10]) in the transaction to achieve conditional anonymity. That is, no one but the group manager (i.e. permissioned nodes) can trace and reveal the group member identity of a signer. Note that resource-constrained IoT devices generally cannot support the computations of a group signature scheme, and hence we use the *gateway* to publish transactions for the devices. Generally, these IoT devices connect to an external environment via a physical connected gateway (with certain computational capacities).
- In order to protect the confidentiality of access control policies recorded in the blockchain, the *owner* needs to encrypt the access control policies using the gateway's public key via some public key encryption scheme first. Then, the *owner* uploads the encrypted polices into the smart contract and only the corresponding *gateway* with the secret key can decrypt and obtain the policies.

- Considering the possible security vulnerabilities from smart contracts, we propose using *FsolidM* to design and deploy our secure smart contract for access control in IoT. As discussed in [9], *FsolidM* provides a user-friendly graphical editor that enables developers to design smart contracts as fnite-state machine (FSM) and a corresponding tool for translating FSM into *Solidity* code.

Due to the integration of group signature schemes and a simple public key encryption in smart contract, our proposal can efficiently mitigate two conflicting requirements, namely: anonymity versus accountability, and transparency versus confidentiality, as well as addressing the deficiencies of conventional centralized or even existing blockchain-based systems. Hopefully, our proposal can inspire other secure blockchain-based applications in IoT such as data sharing, authentication, communication, and so forth.

[1] https://www.juzhen.io/

Acknowledgement

1. The work was supported in part by the National Key Research and Development Program of China under Grant 2017YFB0802500.
2. The work was supported in part by the National Natural Science Foundation of China under Grant 61501333, Grant 61572379, Grant 61472287, and Grant 61772377.
3. The work was supported in part by the Natural Science Foundation of Hubei Province of China under Grant 2017CFA007 and Grant 2015CFA068.
4. The work was supported in part by the Cloud Technology Endowed Professorship.

References

[1] I. Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, A. Gani, M. Imran, and M. Guizani, "Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges," IEEE Wireless Communication, vol. 24, no. 3, pp. 10 - 16, 2017.

[2] G. Zyskind, O. Nathan, A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," IEEE Symposium on Security and Privacy Workshops, pp. 180 - 184, 2015.

[3] A. Ouaddah, A.A.E. Kalam, A.A. Ouahman, "FairAccess: a new Blockchain-based access control framework for the Internet of Things," Hindawi Security and Communication Networks, vol. 9, no. 18, pp. 5943 -5964, 2016.

[4] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, J. Wan, "Smart Contract-Based Access Control for the Internet of Things," CoRR abs/1802.04410, 2018 (https://arxiv.org/abs/1802.04410).

[5] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184 - 1195, 2018.

[6] C. Lin, D. He, X. Huang, K.-K. R. Choo, A. V. Vasilakos, "Bsein: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," Elsevier Journal of Network and Computer Applications, vol. 116, pp. 42-52, 2018.

[7] M. Ober, S. Katzenbeisser, K. Hamacher, "Structure and Anonymity of the Bitcoin Transaction Graph," MDPI Future Internet, vol. 5, no. 2, pp. 237 - 250, 2013.

[8] D. Ron, A. Shamir, “Quantitative Analysis of the Full Bitcoin Transaction Graph,” Financial Cryptography, pp. 6 - 24, 2013.

[9] A. Mavridou, A. Laszka, “Designing Secure Ethereum Smart Contracts: A Finite State Machine Based Approach,” CoRR abs/1711.09327, 2017 (https://arxiv.org/abs/1711.09327).

[10] T. Ho, L. Yen, C. Tseng, “Simple-Yet-Efficient Construction and Revocation of Group Signatures,” International Journal of Foundations of Computer Science, vol. 26, no. 5, pp. 611 - 624, 2015.

Chao Lin received his Bachelor and Master degrees from the School of Mathematics and Computer Science, Fujian Normal University in 2013 and 2017, respectively. Currently, he is pursuing his Ph.D. degree in the School of Cyber Science and Engineering, Wuhan University. His research interests mainly include authentication of graph data and blockchain security.

Debiao He received his Ph.D. degree in applied mathematics from School of Mathematics and Statistics, Wuhan University in 2009. He is currently a Professor of the School of Cyber Science and Engineering, Wuhan University. His main research interests include cryptography and information security, in particular, cryptographic protocols.

Xinyi Huang received the Ph.D. degree from the University of Wollongong, Australia. He is currently a Professor with the School of Mathematics and Computer Science, Fujian Normal University, China, and the Co-Director of Fujian Provincial Key Laboratory of Network Security and Cryptology. He is an Associate Editor for the IEEE Transactions on Dependable and Secure Computing. He serves on the Editorial Board of International Journal of Information Security (IJIS, Springer), and has served as the Program/General Chair or Program Committee Member in over 80 international conferences. His research interests include applied cryptography and network security.

Kim-Kwang Raymond Choo (SM'15) received his Ph.D. in Information Security in 2006 from Queensland University of Technology, Australia. He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA). In 2016, he was named the Cybersecurity Educator of the Year - APAC (Cybersecurity Excellence Awards are produced in cooperation with the Information Security Community on LinkedIn), and in 2015 he and his team won the Digital Forensics Research Challenge organized by Germany's University of Erlangen-Nuremberg. He is the recipient of 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, ESORICS 2015 Best Paper Award, 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and British Computer Society's Wilkes Award in 2008. He is also a Fellow of the Australian Computer Society.

Editor:

Zheng Yan is currently a full professor at the Xidian University, China and a visiting professor and Finnish academy research fellow at the Aalto University, Finland. She received the Doctor of Science in Technology from the Helsinki University of Technology, Finland. She authored and co-authored about 200 peer-reviewed articles, 8 conference proceedings and solely authored two books. She is an inventor of 60+ granted patents and PCT patents, all of them were adopted or purchased by industry. Some of her granted patents are applied in international standards. She has given 20 keynotes and invited talks in international conferences and universities. Her research interests are in trust, security and privacy; data mining; mobile applications and services; social networking and cloud computing. Prof. Yan serves as an organizational and technical committee member for more than 80 international conferences and workshops. She is an associate editor of IEEE IoT Journal, Information Fusion, Information Sciences, IEEE Access, JNCA, Soft Computing, IEEE Blockchain Technical Briefs, Security and Communication Networks, etc. and a special issue leading guest editor of ACM TOMM, Future Generation Computer Systems, Computers & Security, IJCS, MONET, IEEE Systems Journal, etc. She is a founder steering committee co-chair of IEEE Blockchain conference. She is organizing and has organized 10+ conferences, such as IEEE Blockchain 2018, NSS/ICA3PP/IEEE CIT2017, IEEE TrustCom/BigDataSE/ISPA-2015, IEEE CIT2014, etc. Her recent awards include a number of Outstanding Leadership Awards for IEEE conference organization; the 2017 IEEE ComSoc TCBD Best Journal Paper Award; Outstanding Associate Editor of 2017 for IEEE Access; EU Eureka Excellence Award (2017); Best Individual of Shaanxi Province from Abroad (2014), “100 Expert Plan” winner of Shaanxi Province, China (2011); Sisu Award of Nokia Research Center (2010); EU ITEA Bronze Achievement Award (2008). She is a senior member of IEEE.

MedRec: Patient Control of Medical Record Distribution

Andrew Lippman, MIT; **Nchinda Nchinda**, Candidate for MS in Computer Science at MIT; **Kallirroi Retzepi**, Graduate Student, Viral Communications group at MIT; and **Agnes Cameron**, Master's Student, Viral Communications group at MIT

IEEE Blockchain Technical Briefs, July 2018

Introduction

Increasingly, people in the United States are required to manage their own healthcare and associated information. The days of the lifetime family doctor are over. At the same time, healthcare providers have to make that data available. This circumstance opens the door for innovative approaches to patient management. One obvious solution is a "Swiss bank" for healthcare records. This offloads engaged patient management to a cross-provider intermediary. In return for that convenience, we risk the addition of new data silos and commercial control points.

As an alternative, we can use a non-commercial, distributed system that allows patients to control who can access their records and thereby create a network solution where providers join that network and make data available on-demand at the behest of patients. MedRec is a *network* rather than a *service.* The advantage of this is that we can provide a cross-provider, patient-oriented interface and interaction mechanism. We constructed it using an Ethereum blockchain and we have tested it with diverse data bases provided by our research partner, the Massachusetts-based Beth Israel Deaconess Medical Center. Further development will be done by a new, non-profit research endeavor called the Health Technology Innovation Center operated at BIDMC with continued participation by a team at the MIT Media Lab[1].

We note three features of the system that are potentially significant. First, the system is designed to accommodate access to data for clinical researchers and serve as a point of entry for socially valuable epidemiological research for example to understand the propagation of disease and epidemics. MedRec is about more than patients or doctors, it is a component of a general healthcare environment.

Second, the architecture of MedRec is general. There is little that is health specific. We envision that it can be a model for the management of individual identity and permissions in many circumstances where end-user control of identity and personal information *across applications* is important. This can be a basis for social networks and as a convenience for individuals who want to simplify who knows what about them. There is no coinage or transaction inherent in MedRec; it is designed to be free and open.

Third, in keeping with the design ethos of the Viral Communications Research Group at the MIT Media Lab, the system can be adopted incrementally, organization-by-organization. It is useful for internal management of records by hospital networks that consist of many independent providers and it scales to multiple, large-scale healthcare organizations.

MedRec was inspired by original work by Ariel Ekblaw and Asaf Azaria[2]. The current version, which is a new architecture, is supported by a grant from the Robert Wood Johnson Foundation. We use a blockchain that is maintained by medical providers who originate records to archive "smart contracts" that define access rights. Other information is also stored on chain. The goal of the program is to create a disinterested, non-profit, university-based system for patient control.

Design

The architecture of MedRec is easily understood by analogy to the World Wide Web. The web consists of three elements: An HTTP server that provides access to local data, the HTML protocol by which access is obtained and web elements are defined, and a browser that forms the interface. Ideally, anyone and everyone could be a server and web browsers can draw from multiple ones to create a presentation. The World Wide Web is by design a network rather than a client-server architecture even though in practice there are dominant servers.

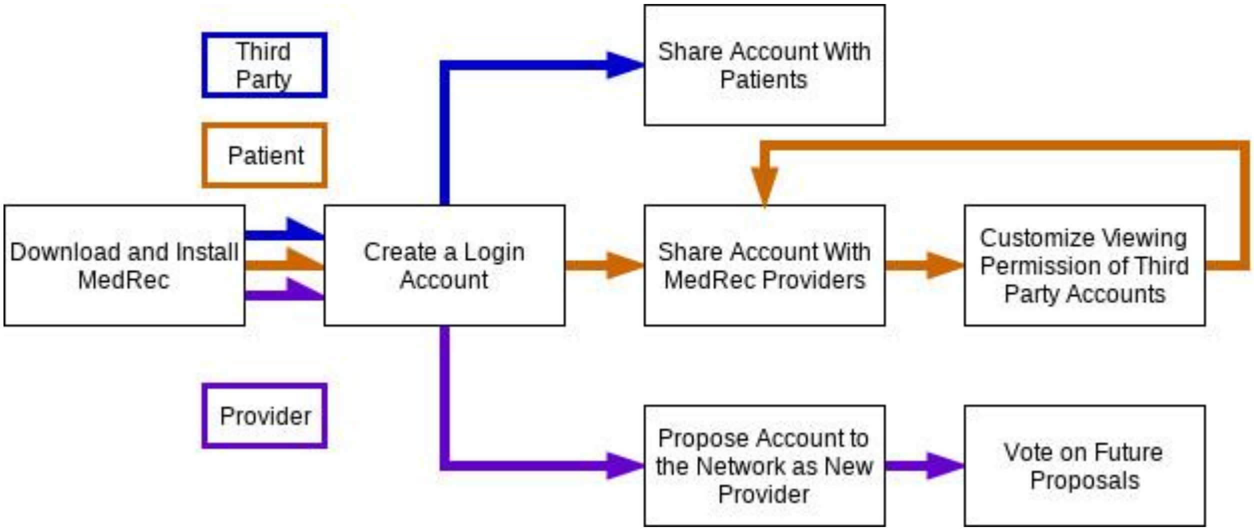
In MedRec, the language is a set of contracts initiated by patients that define what entities or parties can access which records[3]. There are currently three types of contracts and more can be created. The simplest is one that asserts that entity *B* can access the records of patient *A.* More complicated ones allow for intermediary healthcare proxies, or allow a pharmacy to access all prescription records for patient *A* from *any* healthcare provider.

We call the server equivalent a "full node." Full nodes are administrative members of the network. They can append blocks to the chain, admit new administrative members, and distribute notifications submitted to or originated by them. Examples include requests for participation in a clinical or epidemiological study or record changes. We use proof of authority to append blocks and the addresses of holders of that authority are also stored on chain[4]. New members with those rights are voted in by a majority of existing members. This facility is part of the Ethereum Blockchain[5].

The interface is a local app run on a PC or phone[6]. It allows generation of contracts and polls providers for notifications. There is an interface for a provider and one for a patient. Patient interfaces are light nodes and may or may not contain a copy of the blockchain. Third parties can also run an equivalent light node. That may include research organizations, pharmacists, patients' relatives, etc.

Operation

In this section, we show the work flow for three potential network constituents: healthcare providers, patients, and third parties such as pharmacies and research organizations.


Third Party
Patient
Provider
Download and Install MedRec
Create a Login Account
Share Account With Patients
Share Account With MedRec Providers
Customize Viewing Permission of Third Party Accounts
Propose Account to the Network as New Provider
Vote on Future Proposals

Every user in the MedRec network installs the software and creates a login account. New providers make proposals to a special smart contract that orchestrates the addition and removal of providers to the network. Existing providers vote on whether to accept these proposals. Patients form relationships by sharing their account ID (an Ethereum address) with medical providers. Once a relationship with a provider is formed, patients can enable other accounts with the power to view portions of the medical data stored by that provider.

Caveats, Assessment, and Future Work

There are several elements to adoption of a MedRec network that are subjects of further work and development.

Most important is the means by which providers adopt and interface to the system. A provider, as operator of a full node, commits to run a program that grants access to their databases under the rules of MedRec contracts. This entails an interfacing investment that can be significant. For large providers who already use an existing patient management application, this need be done once for that system and others can then use it. For smaller providers such as group practices, one must build an interface for each system that is in use.

As with any blockchain implementation, important questions include who maintains the blockchain, what the trust model is, what threats are to be defended, and what consensus scheme is to be used. In this case, the network is semi-public. Anyone can join as a light node and be the predicate in a contract. But only providers can authorize contracts and append to the blockchain. Providers are trusted entities but we immunize the system against intrusions of their internal systems by requiring majority voting.

We argue that Ethereum-supported proof of authority mechanism is a robust solution. The overhead of running a full node is small both in terms of management and allocation of resources. Conversely, the advantages are large. The open-source model allows us to evolve with needs and community desires. These issues are assertions that will be tested at scale in real use.

A second issue is the nature of the patient interface. We suspect that individual management of personal data is a chore akin to management of a retirement plan. They are similar in that when we are young and healthy, we likely dedicate little energy to either retirement or healthcare. It has been amply demonstrated that people devalue long term or low probability events. A good interface may ameliorate this. To date, the interface we have implemented is optimized to be simple and encouraging. It allows for contract creation and deployment, visualization of the user's network and the ability to fetch and view data from the remote database. As we add features that are common in commercial healthcare interfaces, we have to ensure that the system does not become a chore to use. This will evolve in time.

Conclusion

We have created a blockchain-based system that serves a societal need without the intrusion of visible transactions or an application-specific coinage. We substitute a network for a service and use the blockchain to manage that service. There is no implicit economic associated with the work, nor any view of how society is organized. The general nature of the solution is amenable to other cases where an open-source, distributed model is useful. We hope that the system will evolve to serve the needs of medical community and societal health. The code is accessible at https://github.com/mitmedialab/medrec

[1] https://www.bidmc.org/about-bidmc/news/2018/05/bidmc-launches-htech

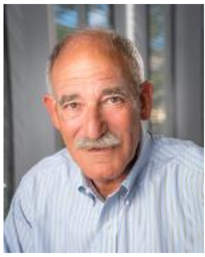
[2] Azaria, Asaph, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. "MedRec: Using Blockchain for Medical Data Access and Permission Management." In *Open and Big Data (OBD), International Conference on*, pp. 25-30. IEEE, 2016

[3] http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

[4] De Angelis et al. PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain,
ceur-ws.org/Vol-2058/paper-06.pdf

[5] https://github.com/ethereum/wiki/wiki/White-Paper

[6] This give the app the appearance of a web-app and runs on diverse devices: https://electronjs.org/



Andy Lippman is a Senior Scientist at MIT and founding associate director of the MIT Media Lab. He got his BS and MS at MIT, and PhD at EPFL, Lausanne. He has worked for 45 years on personal computing, networking and interactive systems. In the 1980s he directed the “Movie-Map” project that presaged Google's streetview. He helped pioneer visual computing and communications systems such as MPEG and digital HDTV. His current research group addresses Viral Communications, systems that are often peer-to-peer and can grow organically through adoption rather than a priori agreement. He has studied blockchains and digital currency for six years. Some recent work involves developing personal networks for social action and a blockchain-based identity control system for medical records.

Nchinda Nchinda is a Candidate for MS in Computer Science at the Massachusetts Institute of Technology. His work has covered on cybersecurity and distributed systems, focusing on blockchain technology. He is a fan of real time multiplayer strategy games and an avid, albeit unskilled Dota2 player. Nchinda is high functioning introvert with a well-developed imagination.

Kallirroi Retzepi is a graduate student at the Viral Communications group at the MIT Media Lab. She has a background in engineering, neuroscience and design. She is interested in the decentralized Web, online interfaces, user behaviors and how to change them.

Agnes Cameron is a master's student in the Viral Communications group. This year she has been part of the MedRec team, and she is more generally interested in decentralised and self-organising network systems. Originally from the UK, she holds an MEng in Information and Computer Engineering from the University of Cambridge, specialising in self-organising systems and holography.

Editor:

Weisong Shi is a Charles H. Gershenson Distinguished Faculty Fellow and a Professor of Computer Science at Wayne State University where he directs the Mobile and Internet Systems Laboratory, the Connected and Autonomous Driving Laboratory, and Wayne State Wireless Health Initiative. He is also the Program Director of the Cyber-Physical Systems (CPS) program at Wayne State. He is an IEEE Fellow and an ACM Distinguished Scientist.

Dr. Shi received his B. E. from Xidian University in 1995, and Ph.D. degree from the Chinese Academy of Sciences in 2000, both in Computer Engineering. He authored one book, edited one book, published over 180 publications cited by 5000+ times (H-index: 38), received research support from and consulted for a variety of governmental and industrial organizations, such as National Science Foundation, Department of Veteran Affairs, Air Force Research Laboratory, Gates Foundation, Swedish Research Council, Michigan Life Science Corridor, Facebook, Intel, Chrysler and so on. He is the inaugural Editor-in-Chief of Smart Health Journal, the Associate Editor-in-Chief of IEEE Internet Computing Magazine. He had served as the chair of the IEEE Computer Society Technical Committee on the Internet (TCI) during 2012-2016, and serves on the editorial board of IEEE Transactions on Services Computing, ACM Transactions on Internet of Things, IEEE Internet Computing, Elsevier Sustainable Computing, and so on.

Dr. Shi is a recipient of the National Outstanding Ph.D. dissertation award of China (2002), the NSF CAREER award (2007), Wayne State University Career Development Chair award (2009), Charles H. Gershenson Distinguished Faculty Fellow (2015), College of Engineering Faculty Research Excellence Award (2016), the Best Paper award of ICWE'04, IEEE IPDPS'05, HPCChina'12 and IEEE IISWC'12, the Best Paper Nominee award of ACM UbiComp'14, the Best Student Paper Award of IEEE HealthCom'15, the Best Paper Award from IEEE eHealth in 2017. This month, he received the Most Downloaded Publication Award for his paper “The Promise of Edge Computing” published on IEEE Computer Magazine.

Auto-translation of Regulatory Documents into Smart Contracts

Olivia Choudhury; **Murtaza Dhuliawala**; **Nicholas Fay**; **Nolan Rudolph**; **Issa Sylla**; **Noor Fairoza**; **Daniel Gruen**; and **Amar Das**, IBM Research, Cambridge, MA

IEEE Blockchain Technical Briefs, September 2018

Introduction

The evolution of Blockchain 2.0 expanded the scope of this emerging technology beyond cryptocurrency by introducing *smart contracts*. Although the notion of smart contract was conceived by Nick Szabo twenty years ago [1], it was first implemented on the Ethereum blockchain in 2014 [2]. Smart contracts are self-executing computer programs that implement a set of functionalities, based on business rules, to validate transactions in a blockchain network. Such rules are found in contractual agreements, and include, but are not limited to, defining and enforcing the terms of a contract between parties, keeping a strict and cohesive schedule of deadlines, and allowing change to the original rules, given the consent of the parties involved. Smart contracts can automate such complex business logic by embedding, verifying, and enforcing the contractual clauses of an agreement without intermediaries. However, the translation of business rules written for regulatory purposes to a smart contract specifying a blockchain transaction can be challenging and time consuming. Moreover, business rules are often re-used among different contracts, and redundant effort is needed to generate similar smart contracts.

To address the above-mentioned challenges, we have developed a framework that automatically generates smart contracts from domain-specific business rules in regulatory documents. Such an infrastructure can not only reduce the level of expertise required for and the time and cost incurred in specifying smart contracts, but also support reproducibility. Our framework comprises two parts: (a) extraction of business rules from documents using machine learning and natural language processing techniques, and (b) conversion of extracted rules to smart contract functionalities using domain knowledge, formally represented as ontologies and semantic rules.

To demonstrate our framework, we consider the use case of clinical trials, that involve complex, multi-party interactions. A clinical trial protocol, equivalent to a business agreement, defines a list of pre-approved activities and required actions that must be satisfied by intended stakeholders. One of the major requirements of a protocol is the schedule of activities (SOA), a tabular representation of activities that must be accomplished at each study visit or within an allowable window. We show how our framework extracts SOA rules from a protocol and embeds them into a smart contract for subsequent enforcement and validation.

System Design

Extracting business rules from agreements

As the first step, we employ machine learning and natural language processing (NLP) techniques to extract relevant information that could potentially become rules or constraints for the smart contract. We leverage IBM Watson's suite of cognitive services for entity extraction and map them to rules that apply to them. In some cases, we also need specialized modules for extracting time information to ensure that constraints are time bound when they need to be. We utilize optical character recognition (OCR) and other computer vision techniques to extract SOA tables from PDFs of clinical trial protocols. This information is then processed using NLP in order to gain semantic meaning of the extracted information, which focus on the activities that need to be accomplished on a certain visit and when the visits occur. Through a human-in-the-loop visual interface, we verify the semantics extracted from the table, such as, when visits should occur, which lab tests and procedures must be conducted on those visits, and modifications to a visit. This verified information is then abstracted and passed along to the next step of the framework, as shown in Figure 1. Further details of the extraction of business rules from documents can be found in [3].

Embedding business rules into smart contract

We use standardized knowledge representation, such as ontologies and semantic rules, to model the information extracted in the previous step. An ontology conceptualizes the knowledge of a domain as classes (concepts in a domain), individuals (instances of a class), properties (common characteristics of instances), and relationships (between classes). We design a clinical trial ontology using the popular Web Ontology Language (OWL) [4]. We then follow the Semantic Web Rule Language (SWRL) [5] to express the extracted rules or constraints. SWRL allows writing Horn-like semantic rules [6], containing at most one positive literal, that are built on OWL concepts. The clinical trial ontology and associated semantic rules provide a knowledge base that can be further exploited for reasoning or drawing inference.

The constraints expressed as semantic rules must be incorporated into and enforced by the smart contract. To achieve this, we devise a context-free grammar to parse the required constraints from the rules. For a given domain, such as clinical trial, we create a smart contract template to stipulate the functionalities, based on rules derived from the ontology and protocol. This serves as the skeleton for generating the final smart contract to be used in the blockchain network. We represent the source code of this template in a hierarchical tree structure, called an abstract syntax tree (AST). The AST can be traversed in a depth-first search manner and manipulated to add the parsed constraints procured from the semantic rules. Once updated, we convert the AST into a new smart contract containing the embedded constraints parsed from the rules. This is illustrated in Figure 1. Details of this procedure can be found in [7].

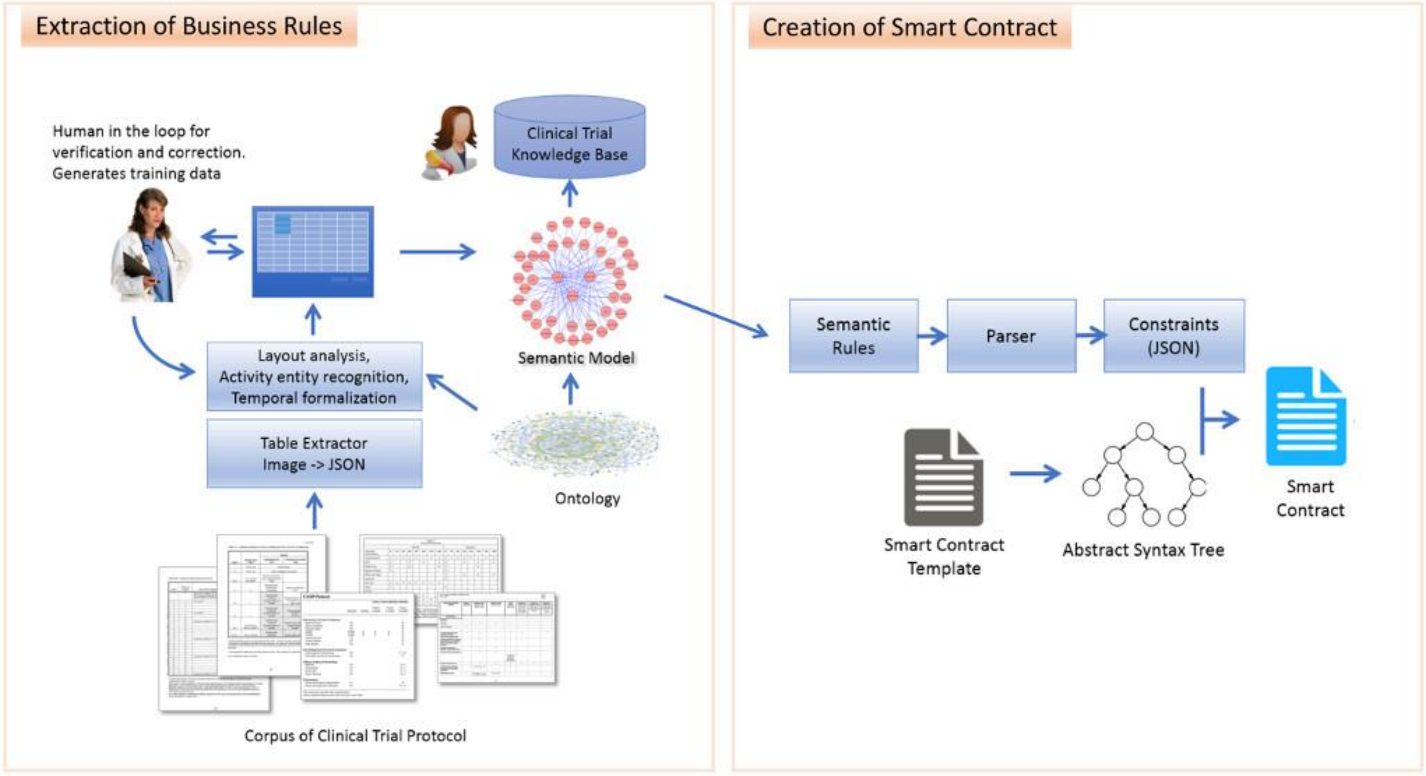

Extraction of Business Rules
Creation of Smart Contract
Human in the loop for verification and correction. Generates training data
Clinical Trial Knowledge Base
Semantic Model
Layout analysis, Activity entity recognition, Temporal formalization
Table Extractor Image -> JSON
Ontology
Corpus of Clinical Trial Protocol
Semantic Rules
Parser
Constraints (JSON)
Smart Contract Template
Abstract Syntax Tree
Smart Contract

Figure 1: System design of the framework for auto-generating a smart contract from domain-specific business rules.

Discussion and Future Work

Due to limited availability of labeled data, our current method of constraint extraction relies on hand-crafted features and rules. As shown in [3], although we achieve a precision of 0.95 across 20 training and test protocols, we can further improve the predictive capability by creating and leveraging a larger set of training data with annotations. Such a dataset will also help in deriving data-driven rules, thereby making the system more robust and capable of capturing complex rules and relationships. In order to avoid the need for domain expertise in designing ontologies and semantic rules, we will also develop an automated approach of building domain-specific knowledge base. For the purpose of demonstration, we have considered clinical trials and Go language as the use case and programming language, respectively. However, our framework can be easily applied to other use cases and programming languages.

Current efforts in generating a smart contract involve significant technical expertise,time, and cost. They also do not support reproducibility for a given application domain. Our novel framework, based on machine learning formalism, NLP, ontologies, semantic rules, and AST, can extract business rules from regulatory documents and incorporate these constraints into a smart contract. Such automation will reduce the level of inherent complexity associated with blockchain and smart contracts and encourage their adoption across different applications.

References

[1] N. Szabo, “The idea of smart contracts,” *Nick Szabo's Papers and Concise Tutorials*, vol. 6, 1997.

[2] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” *Ethereum Project Yellow Paper*, vol. 151, pp. 1{32}, 2014.

[3] M. Dhuliawala, N. Fay, D. Gruen, and A. Das, “What Happens When? Interpreting Schedule of Activity Tables in Clinical Trial Documents,” *ACM-BCB’18: 9th ACM International Conference on Bioinformatics, Computational Biology and Health Informatics (In Press)*, 2018.

[4] D. L. McGuinness, F. Van Harmelen, “OWL web ontology language overview,” *W3C recommendation*, vol. 10, no. 10, p. 2004, 2004.

[5] I. Horrocks, P. F. Patel-Schneider, H. Boley, S. Tabet, B. Grosof, M. Dean, “SWRL: A semantic web rule language combining OWL and RuleML,” *W3C Member submission*, vol. 21, p. 79, 2004.

[6] A. Horn, “On sentences which are true of direct unions of algebras,” *The Journal of Symboic Logic*, 16(1), 14-21, 1951.

[7] O. Choudhury, N. Rudolph, I. Sylla, N. Fairoza, and A. Das, “Auto-Generation of Smart Contracts from Domain-specific Ontologies and Semantic Rules,” *IEEE Blockchain Conference*, 2018. http://cse.stfx.ca/~cybermatics/2018/Proceedings/pdfs/iThings!GreenCom!CPSCom!SmartData!Blockchain!CIT!Cybermatics2018-1Q1rrimpxFNyCxx89cHrQN/2ovSxOqBeseB6dSnHGs2qJ/5LlYvOqaMAJCLsiA32X9C5.pdf

Olivia Choudhury is a postdoctoral researcher at IBM Research, Cambridge, MA, USA. She received her PhD degree in Computer Science and Engineering from University of Notre Dame, USA. Her research interests include blockchain technology, federated learning, healthcare informatics, genomics, and distributed computing.

Murtaza Dhuliawala is a research software engineer at IBM Research, Cambridge, MA, USA. He received his Masters in Computer Science with specialization in Artificial Intelligence and Machine Learning from Georgia Institute of Technology, USA. His research and past experience span the areas of machine learning, deep learning, NLP, interactive storytelling, healthcare research, blockchain, finance applications, and developing cognitive, AI applications.

Nicholas Fay is a healthcare data scientist at IBM Research, Cambridge, MA, USA. He received his Masters in Computer Science from Rensselaer Polytechnic Institute, USA. His previous research focused on network science and social media analytics. His current research interest includes application of machine learning, NLP, and wearables in the healthcare space. He is also interested in blockchain, IoT, and application platforms surrounding them.

Nolan Rudolph is a software engineer. He received his Bachelors of Science in Computer Science and Engineering from Ohio State University, USA. While at IBM Research, he explored the applicability of blockchain technology in healthcare. He now applies data science and programmatic decisioning in the adtech industry through his work at Dataxu.

Issa Sylla is a research software engineer at IBM Research, Cambridge, MA, USA. He received his Bachelors of Arts in Middle Eastern Studies from Dartmouth College, USA. His research spans geographic disparities in clinical trials, application of blockchain technology within healthcare, and machine learning.

Noor Fairoza is a DevOps Engineer at IBM Research, Cambridge, MA, USA. She received her Masters in Telecommunication Systems and Management from Northeastern University, USA. Her research interests include application of blockchain technology in healthcare, network engineering, and application of DevOps-Agile in research.

Daniel Gruen is a Research Staff Member at IBM Research, Cambridge, MA, USA. He received his PhD in Cognitive Science from UCSD, USA. He works on the design of AI-based tools that let practitioners and strategic decision-makers seamlessly incorporate insights from big-data, analytics, visualization, and cognitive systems. His current work focuses on health-related applications, including automatic video understanding and summarization.

Amar Das is the Director of IBM's Learning Health Systems team. He received his MD and PhD in Biomedical Informatics from Stanford University. His research focuses on developing new statistical, computational, organizational, and regulatory approaches to the assessment, deployment, and adoption of healthcare solutions. Prior to joining IBM Research, he was a faculty member at Stanford University Medical School and the Geisel School of Medicine at Dartmouth.

Editor:

Claire-Isabelle Carlier is an Enterprise Architect at Brookfield Renewable Partners, where she advises various operating businesses across the globe on their strategic technology planning. Her role involves supporting IT-OT convergence and adoption of new technologies. She became interested in blockchain back in 2015 shortly after the Ethereum platform was launched and the ideas of decentralized applications and smart contracts started spreading. Since joining Brookfield in 2017, she has been following closely the evolution of use cases for the energy sector and asset management, and the related market landscape of vendors and products. As member of IEEE Smart Cities Technical Committee, she has also been researching how blockchain could contribute to making cities smarter for citizens, organizations and municipalities.

A Pentagon of Considerations Towards More Secure Blockchains

Qi Zhang, IBM Thomas J. Watson Research, Yorktown Heights, NY, USA; **Reza M. Parizi**, Department of Software Engineering and Game Development, Kennesaw State University, GA, USA; and **Kim Kwang Raymond Choo**, Department of Information Systems and Cyber Security, University of Texas at San Antonio, Texas, USA

IEEE Blockchain Technical Briefs, September 2018

With the rapid growing interest in cryptocurrencies such as Bitcoin and Ethereum, their underlying technology, blockchain, is catching huge amount of attentions from both academia and industries. More than a distributed database, blockchain is able to establish trust among multiple untrusted participants. This is achieved by using cryptographic techniques such as hash pointer [4], and consensus algorithms such as Proof of Work (PoW) [5].

As a trusted platform, blockchain finds itself a good fit in many use cases, especially when multiple untrusted participants need to be involved. For example, Walmart is collaborating with IBM to use the blockchain (Hyperledger Fabric) to enable the safety, transparency, and efficiency of their food supply chain, in which the farmers, distributors, wholesalers, and etc. are involved. Also, many financial institutes are sitting together to actively explore using blockchain to facilitate the process of onboarding customers and to build faster inter-bank payment systems. In these cases, the use of the blockchain reduces the cost of having a third party to validate all the transactions, improves the traceability and auditability of the recorded data, thus makes the whole process more efficient.

Although the blockchain platform is described as tamper-proof, it is not impossible to be tampered with. The security of the platform and the privacy of the data stored in the blockchain ledger are still the top concerns of the practitioners. Therefore, it is extremely important to understand how reliable the existing blockchain technology is and what are the efforts to make it more secure and provide better data privacy.

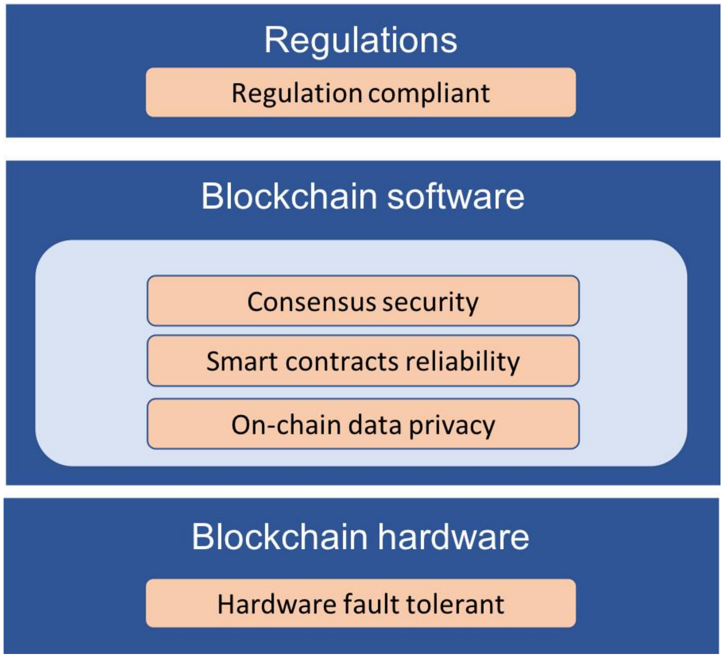


Figure 1. Blockchain Security Considerations.

This paper investigates five critical factors that need to be considered towards building more secure blockchains – consensus security, smart contracts reliability, on-chain data privacy, hardware fault tolerant, and regulation compliant. As shown in Figure 1, these factors spam across the blockchain hardware, software, as well as its related regulations. For each factor, this paper discusses its importance and explores both the state-of-the-art solutions and the future opportunities.

Consensus security

Blockchain platforms rely on the consensus algorithms to ensure that it is extremely difficult for some malicious users to subvert the whole network. As an example, Proof of Work is one of the consensus algorithms that is Byzantine fault tolerant, in which miners compete with each other to publish blocks via solving a cryptographic puzzle. In order to successfully commit a malicious transaction (e.g. a double spend transaction) into the ledger, an attacker needs to have more than half of the whole computing power of the network. This supposed to be almost impossible given the large number of the participants in the network. However, with the appearance of powerful mining pools, the blockchain could be subverted if multiple large mining pools decide to join and hack the network together. Other than Proof of Work, many other consensus algorithms, such as Proof of Stake [11] and Proof of Elapsed Time [12], are also proposed. Some analysis has been made regarding to the security of different consensus algorithms [2]. The better we understand their vulnerabilities, the more secure the blockchain platform can achieve.

Smart contracts reliability

Smart contract is the key of blockchain-based applications, turning the blockchain into a decentralized computing platform. It executes the logic of the transactions on the blockchain and the results of the successfully executed smart contracts are recorded in the blockchain ledger. Even with a secure consensus algorithm, the vulnerability of the smart contract is also detrimental. Due to a bug in the smart contract, the famous DAO hack [6] managed to steal more than $60 million worth of ether by carrying out a reentrancy attack [7]. Such attacks have raised developers' awareness of creating highly secure smart contract. Given the smart contracts can be written in many different languages, such as Solidity in Ethereum, Go and Java in Hyperledger Fabric, exploring the vulnerabilities of such programming languages and understanding how to prevent them in a blockchain environment is very necessary. For the developers, it is essential to thoroughly validate the security of their smart contracts before deploying them on the blockchain.

On-chain data privacy

In blockchain, transaction data are shared by all the participants, this could be problematic for data privacy, especially if some of these transactions are confidential. This could also be a significant obstacle for blockchain to be widely accepted. Efforts have been made to preserve the on-chain data privacy. For cryptocurrency blockchains, instead of having real user name or ID in each transaction, a user on a blockchain is represented by a key, which is a string of characters that has nothing to do with the user's real-world identity. Also, a user on the blockchain can be represented by multiple keys instead of one, which further reduces the probability of identifying a user by such keys. However, anonymizing the user ID is not entirely privacy-preserving. Given the transactions on the blockchain as well as the advanced data analytics techniques, private information can still be inferred by combining the transaction data with various real-world hints [1]. Zcash [8] is the first attempt to use zero-knowledge cryptography to fully encrypt the transactions on the blockchain while such transactions can still be validated. In Hyperledger Fabric, data privacy is achieved by having different channels on the same blockchain platform. Each participant can join different channels, and transaction data in one channel cannot be seen by other channels. In short, how to achieve data privacy is an important consideration before moving to blockchain, and solutions that can share the data in a privacy preserved manner will be helpful.

Hardware fault tolerant

While paying attention to the security of the blockchain software, we should not ignore the fact that the blockchain network is running on multiple normal computers. These computers, especially when running in a less secure environment, can fail due to many reasons, either being hacked by a malicious user or crashing due to software/hardware errors. For example, Ethereum platform users have reported corrupted data files due to false positives of antivirus software, and some Bitcoin users also experienced block checksum mismatch [9]. These users have to re-download all the blockchain transactions in order to recover. This is quite cumbersome and time consuming, especially for a long running blockchain with large amount of data. Therefore, tools are needed to help user effectively validate the integrity of their blockchain nodes, and also quickly recover from the failure.

Regulation compliant

Blockchain also needs to be compliant with the regulations that protect user data privacy. One of the recently activated regulations is GDPR (General Data Protection Regulation) [3]. An important aspect of GDPR is it requires the personal data can be forgotten. In other words, the users have the rights to erase their personal data. Such regulation does provide stronger and more unified personal data protection for Europe Union citizens, but it seems to be contradicted with the design of the blockchain, which guarantees immutable records. Designing regulation-compliant blockchain solutions is becoming appealing but also challenging. One of the solutions is to put the hash of the personal information on the blockchain, while keeping the raw information in an off-chain storage, thus the information can be deleted when necessary. In this case, the hash on the blockchain can be used to validate whether the raw information in off-chain storage is authentic or not. As an alternative, an editable blockchain proposed by Accenture [10] can also be helpful in this case. While preserving the tamper-proof characteristics, such blockchain can be edited by designated authorities, which makes it possible to erase the personal information stored on the chain.

As Vitalik Buterin [13], the co-founder and inventor of Ethereum [14], mentioned: “The main advantage of blockchain technology is supposed to be that it’s more secure, but new technologies are generally hard for people to trust”. Therefore, what we envision is a more secure, privacy-preserving, and regulation-compliant blockchain technology.

References

[1] https://arxiv.org/pdf/1502.01657.pdf

[2] https://arxiv.org/pdf/1805.03490.pdf

[3] https://www.eugdpr.org/

[4] https://www.deltadeltaandmoredeltas.com/hash-pointers/

[5] https://en.bitcoin.it/wiki/Proof_of_work

[6] https://ieeexplore.ieee.org/abstract/document/8248566/

[7] https://pdfs.semanticscholar.org/66cc/6e3f36c4282a189249523a5e88577739b736.pdf

[8] https://z.cash/technology/index.html#how-it-works

[9] https://arxiv.org/pdf/1805.01081.pdf

[10] https://link.springer.com/chapter/10.1007/978-3-319-94478-4_18#citeas

[11] https://courses.cs.ut.ee/MTAT.07.022/2017_fall/uploads/Main/janno-report-f17.pdf

[12] https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp

[13] https://en.wikipedia.org/wiki/Vitalik_Buterin

[14] https://www.ethereum.org/

Qi Zhang received a Ph.D. degree in computer science from Georgia Institute of Technology, Atlanta, USA, in 2017. He is currently a Research Staff Member in IBM Thomas J. Watson Research Center. His research interests include cloud computing, big data processing, distributed systems, and Blockchain systems. He published research articles in referred journals and conference proceedings such as IEEE TC, IEEE TSC, ACM CSUR, VLDB, SC, HPDC, IEEE ICDCS, IEEE ICWS, IEEE CLOUD. Dr. Zhang received the top 5 picks award in IEEE ICWS 2017. He served as a program committee member for IEEE Blockchain 2018. He is also a frequent reviewer for international research journals such as IEEE TSC, IEEE TCC, and international conferences such as ICDCS, SIGMOD, and Middleware.

Reza M. Parizi is a Software Engineering faculty in the Department of Software Engineering and Game Development at Kennesaw State University, GA, USA. He is a consummate technologist and software engineering researcher with an entrepreneurial spirit at KSU. He is the member of Cyber Scientist- A community of cybersecurity researchers, as well as IEEE, IEEE Blockchain Community, IEEE Computer Society and ACM. Prior to joining KSU, he was an Associate Professor at New York Institute of Technology. He has applied his insights and expertise to a host of innovative and technology driven projects across start-ups, security, software, and education industries. He received a Ph.D. in Software Engineering in 2012 and M.Sc. and B.Sc. degrees in Software Engineering and Computer Science respectively in 2008 and 2005. He has more than 8 years of working experience in industrial software development and project managing. His interests are R&D in Blockchain, smart contract programming, emerging issues in software engineering, and the practice of secure software-run world applications. He has published several research papers in top reputable scientific and international conferences and also has two copyrights to his credit.

Kim-Kwang Raymond Choo received a Ph.D. in Information Security in 2006 from Queensland University of Technology, Australia. He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA). In 2016, he was named the Cybersecurity Educator of the Year - APAC (Cybersecurity Excellence Awards are produced in cooperation with the Information Security Community on LinkedIn), and in 2015 he and his team won the Digital Forensics Research Challenge organized by Germany's University of Erlangen-Nuremberg. He is the recipient of the 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, IEEE TrustCom 2018 Best Paper Award, ESORICS 2015 Best Research Paper Award, 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and British Computer Society's Wilkes Award in 2008. He is also a Fellow of the Australian Computer Society, an IEEE Senior Member, and an Honorary Commander of the 502nd Air Base Wing, Joint Base San Antonio-Fort Sam Houston.

Editor:

Dr. Shucheng Yu is an Associate Professor of Electrical and Computer Engineering at Stevens Institute of Technology. Before he joined Stevens, Dr. Yu was an associate professor of Computer Science at the University of Arkansas at Little Rock, where he also served as the chair of the Computer Science department and the director of the Computational Research Center of the university. He received his PhD in Electrical and Computer Engineering from Worcester Polytechnic Institute in 2010. His research interest is on cybersecurity in general, with recent focuses on security and privacy for data analytics, security & privacy in smart systems, wireless systems and security. He has published over sixty impactful research articles in academic journals and conference proceedings which have received numerous citations. He has been the editor or guest editor for four international journals, and at the organizing committee for over ten international conferences including IEEE Infocom and IEEE Globecom. He serves the board of trustee for Wireless and Optical Communication Conference (WOCC) and is a member of IEEE and ACM.

Enabling Multilevel Data Sharing Based on Blockchain and Smart Contract

Chunming Rong, University of Stavanger; and **Antorweep Chakravorty**, University of Stavanger

IEEE Blockchain Technical Briefs, July 2018

Data sharing has become a popular daily life activity all around the world. Data driven value creation has foreseen potential in many sectors, for example energy, health, banking, insurance and transportation. However, violations of user privacy and digital rights management (DRM) in form of unintended data use, corporate applications and security breaches are being widely reported across multiple sources [1,2,3]. This is further highlighted with growing public concerns about their online behavior and the enforcement of regulations such as EU General Data Protection Regulation (GDPR) [4]. A major impediment in delivering privacy is the lack of frameworks that provide accountability and transparency for distributed IT services; hence it becomes difficult for users to understand, influence and determine how their service providers honor their obligations. Therefore, it demands a shift in the data management paradigm which needs to put the user in the center of all operations performed on their data.

Blockchain [5, 6] is an innovation for creating distributed trust between users facilitating exchange of value over a network. It can be seen as a decentralised read only database operated collectively by participants in the network. Participants in the network are entities that support, maintain and facilitate a blockchain. These participants could be anonymous individuals banding together to provide computational capacity to support a public network or different organizations that provide computing infrastructure to support an enterprise blockchain application through a permissioned consortium network. In case of public networks, anonymous miners across geographical boundaries cohesively work together to validate and confirm transactions and in permissioned networks a consortium of distinct organizations needs to maintain consensus on each transaction that gets committed to the blockchain. Each participant locally maintains the same version of this ledger in their own environment and agrees upon any updates or changes to its state. This enables trust to be distributed throughout the network, without the need for a central intermediary. The decentralisation of trust allows the blockchain technology to be transparent, secure, auditable, redundant and immutable. Since each participant maintains the same version of the truth, it removes the potential of conflict and risk of single point of failure. Additionally, it also enhances the trust of end users using applications hosted on such blockchain networks as they are able to get confirmation about operations on their data from multiple distinct entities rather than a single centralized party.

Blockchain and other distributed ledger technologies (DLTs), through recent development, enables not only transactions, but also smart contracts [7, 8, 9] allowing complex computation on a network, where in transactions are enveloped in a computer code that emulate the logic of contractual clauses. Smart contracts can exchange money, property, data, shares or anything of value in a transparent and conflict free way without the need of a middleman, government agency, bank, lawyer or a notary. Participants responsible for maintaining a blockchain processes transactions only after successful verification of a smart contract. This allows enforcement by the community, of terms and conditions around an agreement in similar fashion to that of traditional contracts. Smart contracts would allow definition of criterias based on which two parties can agree to exchange, operate and retract information.

Harnessing such developments on blockchain and smart contracts, has led to the potential of disruptive decentralized applications that aim to provide end users the ability to trace, retract, revoke and limit sharing of content. It would give the digital right and sharing control power back to the data creator, which is often considered as lost once it is shared today. Innovative business models across various sectors could be developed from data management, social networks, supply chain, energy to smart cities.

- New data management platforms could facilitate a sharing economy [14, 15] where in, enterprises would get access to authentic prospect data and their customers would be rewarded for sharing data. A blockchain would record data/value exchange from an owner to receiver. It would validate transactions through smart contract based criterias on purpose of use, availability and contract nullification conditions that an owner and receiver agree.
- User centric social networks [10, 11] could allow users to share content as transactions on a It would enable them to have lineage and traceability on their content and the ability to enforce conditions through smart contracts on any operations on their data.
- Interactive applications for smart energy ecosystems could also be supported on a blockchain for peer to peer and community level energy trading [12, 13]. User transactions on energy prosumption could be recorded in the blockchain to facilitate trading of their excess energy with their neighbourhood and the grid. Custom business centric tokens on the blockchain as a payment option would allow users to earn such rewards for trading and use them for payment of services within the ecosystem.
- Efficiency in global supply chains would be improved using blockchain for trust and security in digities document workflow allowing a tamper proof repository for documents and shipping events reducing barriers, delays and frauds [16].
- The use of blockchain technology in smart cities is multifaceted. Along with providing city utility providers and communities opportunities to develop new business models, it would also allow citizens to control what information they share with their cities. In this case, the user owns their data, not the owner of the application. Users can choose how much data they are willing to share. Furthermore, the cities can use the analytics generated by the user data to make informed decisions on future urban developments by participating in a smart contract that would defined the rules of engagement.

Multilevel data sharing based on Blockchain and Smart Contract allows building of trust between enterprises and customers by providing the necessary tools and services for the data owner to be in the driver's seat of their data. It further cultivates ample opportunities for new disruptive business applications across various sectors by bringing trust to internet services. The research, innovation and adaptation of decentralized blockchain applications would lead to revolutionizing of the current information and data service industry within this decade.

References

[1] V. Goel. Facebook tinkers with users' emotions in news feed experiment, stirring outcry. The New York Times, 2014.

[2] J. Ball. Nsas prism surveillance program: how it works and what it can do. The Guardian, 8, 2013

[3] Cadwalladr, Carole, and Emma Graham-Harrison. "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach." The Guardian 17 (2018).

[4] EU GDPR Portal. (2018). EU GDPR Information Portal. [online] Available at: https://www.eugdpr.org

[5] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[6] A. Hayes. Evidence for bitcoin. Altcoin Price Efficiency: Miners' Arbitrage in Cryptocurrency Markets, 2014.

[7] V. Buterin. A next-generation smart contract and decentralized application platform. white paper, 2014

[8] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg. Proofs of ownership in remote storage systems. In Proceedings of the 18th ACM conference on Computer and communications security, pages 491–500. ACM, 2011

[9] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. University of Maryland and Cornell University, 2015.

[10] Chakravorty, A., & Rong, C. (2017, January). Ushare: user controlled social media based on blockchain. In Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication (p. 99). ACM.

[11] D. Konforty, Y. Adam, D. Estrada, and L. G. Meredith. Synereo: The decentralized and distributed social network. 2015.

[12] Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L., & Weinhardt, C. (2018). Designing microgrid energy markets: A case study: The Brooklyn Microgrid. Applied Energy, 210, 870-880.

[13] Aitzhan, N. Z., & Svetinovic, D. (2016). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Transactions on Dependable and Secure Computing.

[14] Chohan, U. W. (2018). The Concept and Criticisms of Steemit. SSRN.

[15] IOTA. (2018). IOTA Data Marketplace – IOTA. [online] Available at: https://blog.iota.org/iota-data-marketplace-cb6be463ac7f?gi=c036fb543344

[16] Nash, K. S. (2016). IBM pushes blockchain into the supply chain. The Wall Street Journal. Available online:https://www.wsj.com/articles/ibm-pushes-blockchain-into-the-supplychain-1468528824

Professor Chunming Rong is the head of the Center for IP-based Service Innovation (CIPSI) at the University of Stavanger (UiS), Norway and adjunct Chief Scientist leading Big-Data Initiative at IRIS. His research work focuses on Cloud Computing, Daya Science, Energy Informatics, Security and Privacy. He is an IEEE senior member and is honored as member of the Norwegian Academy of Technological Sciences (NTVA) since 2011. He has extensive contact network and projects in both the industry and academic. He is steering member of IEEE Cloud Computing and Steering Chair of IEEE CloudCom conference and workshop series. He is the co-Editors-inChief of the Journal of Cloud Computing (ISSN: 2192-113X) by Springer and associate editor of the IEEE Transactions on Cloud Computing (TCC). Professor Rong is also a keynote speaker on "Service Security in Cloud" at IEEE CloudNet conference in Luzembourg, 2014. Professor Rong has extensive experience in managing large-scale R&D projects funded by both industry and funding agencies, both in Norway and EU. Chunming will be the Chief Technology Officer (CTO).

Dr. Antorweep Chakravorty is an Associate Professor at the University of Stavanger, Norway. His current research and development work is in the field of applied Blockchains, Big Data, Large Scale Machine Learning, and Data Privacy. He has an interest in real-world problems, especially development of privacy enabled data-driven services in smart energy, healthcare, and smart city domains. Antorweep completed his PhD. in 2015 with a thesis on *Privacy Preserving Big Data Analytics* at the University of Stavanger, Norway. Along with having a background in applied research in data-driven solutions, he is also involved in mentoring, teaching and supervision. He spent 6 months on a research exchange program at IBM Thomas J. Watson Research Center, New York, USA.

Editor:

Dr. Qinghua Lu is a senior research scientist at CSIRO, Australia. Before she joined CSIRO, she was an associate professor at China University of Petroleum. She formerly worked as a researcher at NICTA (National ICT Australia). She received her PhD from University of New South Wales in 2013. Her research interest includes architecture design of blockchain applications, blockchain as a service, model-driven development of blockchain applications, reliability of cloud computing, and service engineering. She has published more than 70 peer-reviewed academic papers in international journals and conferences. She is an IEEE member and serves on the Program Committees of a number of international conferences in blockchain, cloud computing, big data and software engineering community.

IEEE Blockchain Technical Briefs Editorial Board

- Chonggang Wang, Editor-in-Chief, IEEE Fellow, InterDigital Communications
- Olivia Choudhury, Managing Editor, IBM Research, USA
- Mohammed Atiquzzaman, Edith Kinney Gaylord Presidential Professor, School of Computer Science, University of Oklahoma, USA
- Nathan Ming Kun Aw, Blockchain & Microservices Engineer, OCBC Bank
- Claire-Isabelle Carlier, Enterprise Architecture Business Analyst, Brookfield Renewable Partners, Canada
- Kim-Kwang Raymond Choo, Cloud Technology Endowed Professorship, University of Texas at San Antonio, Senior IEEE Member, USA
- Francisco Curbera, Director, Blockchain and Consumer Health Development, IBM Watson Health, USA
- Mahmoud Daneshmand, Industry Professor, Stevens Institute of Technology, IEEE Life Member, USA
- Andy Lippman, Senior Research Scientist, Massachusetts Institute of Technology (MIT), USA
- Chengnian Long, Professor, Shanghai Jiaotong University, China
- Qinghua Lu, Senior Research Scientist, Data 61, CSIRO, Australia
- Ammar Rayes, Distinguished Engineer, Technology Director, Cisco Systems, USA
- Khaled Salah, Professor at the Department of Electrical and Computer Engineering, Khalifa University, Abu Dhabi, UAE, IEEE Senior Member
- Weisong Shi, Professor, Wayne State University; IEEE Fellow, USA
- Hong Wan, Associate Professor, School of Industrial Engineering, Purdue University, USA
- Honggang Wang, Associate Professor, University of Massachusetts (UMass) Dartmouth, USA
- Jiang Xiao, Associate Professor, Huazhong University of Science and Technology, China
- Zheng Yan, Professor, Xidian University; IEEE Senior Member, China
- Shucheng Yu, Associate Professor, Electrical and Computer Engineering, Stevens Institute of Technology, USA
- Yan Zhang, Professor, Department of Informatics, University of Oslo; IEEE Senior Member, Norway