KICS The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express 6 (2020) 43–47

www.elsevier.com/locate/icte

Policy specification and verification for blockchain and smart contracts in 5G networks

Devrim Unal[a,*], Mohammad Hammoudeh[b], Mehmet Sabir Kiraz[c]

[a] *KINDI Center for Computing Research, Qatar University, Doha, Qatar*
[b] *Department of Computing and Mathematics, Manchester Metropolitan University, Manchester, UK*
[c] *Cyber Technology Institute, De Monfort University, Leicester, UK*

Received 30 May 2019; accepted 10 July 2019
Available online 12 July 2019

Abstract

Blockchain offers unprecedented opportunities for innovation in financial transactions. A whole new world of opportunities for banking, lending, insurance, money transfer, investments, and stock markets awaits. However, the potential for wide-scale adoption of blockchain is hindered with cybersecurity and privacy issues. We provide an overview of the risks and security requirements and give an outlook for future research that could be helpful in solving some of the challenges. We also present an approach for policy specification and verification of financial transactions based on smart contracts.

Keywords: Blockchain; Security policy; Smart contract; 5G networks

1. Introduction

Digital transformation is an ongoing trend in all economies and financial systems. According to Huawei & Oxford Economics report, "Digital Spillover: Measuring the true impact of the digital economy" [1], in 2017, 15.5% ($12 trillion) of the global economy was reported as digital and by 2025 this is estimated to be 25% ($23 trillion). Digital economies are expected to be more competitive; with high return on investment, environmentally balanced and socially accessible and inclusive, digital economies are expected to offer new transformative opportunities. The future of digital economy particularly with the intense regional and global competition will depend on their understanding, readiness, and presence of robust infrastructure.

Digital economies comprise of tangible digital assets and non-tangible digital assets and their related infrastructure. The intangible (data, knowledge, software, IPRs, digital coins, and tokens, etc.) investment share in some countries has reached as high as 15% of the GDP and the growth rate of this segment of the digital economy is on the rise [2].

A consensus has emerged among national regulators and global standard setting bodies that blockchain technology brings to the society and economy tremendous new opportunities. However, uncontrolled use of blockchain technology threatens to accelerate socio-economic problems, especially money laundering, fraud, cybercrime, and market instability. Blockchain proposes to utilize the disruptive cryptocurrency application potential to not only neutralize its negative possibilities but also positive potential of these innovations.

Wideband mobile Internet brought by 5G technology needs to be complemented with mobile digital payment solutions. Blockchain is an enabling technology towards closing this gap. Recently, various hardware cryptocurrency wallet providers and smart phone manufacturers have released hardware wallets for mobile phones. This advancement suggests that there will be a significant amount of blockchain transactions conducted over 5G networks. A recent study [3] has surveyed the interplay between blockchain and cyber security and pointed out that the most security-focused blockchain applications are about IoT, data storage and sharing, network security, user privacy and Internet access. All these application areas are also expected to be drivers in the adoption of blockchain technology in 5G networks.

* Corresponding author.
E-mail addresses: dunal@qu.edu.qa (D. Unal), m.hammoudeh@mmu.ac.uk (M. Hammoudeh), mehmet.kiraz@dmu.ac.uk (M.S. Kiraz).

Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

https://doi.org/10.1016/j.icte.2019.07.002

Various security issues for realizing blockchain in 5G networks include, software vulnerabilities [4] of mobile phone applications and operating systems, hacking attacks to hot-wallets to deposit value in the blockchain, and the insufficient enforcement of security policies on the blockchain transactions. Security policy enforcement on the blockchain is particularly challenging in mobile network environments because of the mobility of end user devices and the multiple-domain nature of mobile networks. Additionally, since the public blockchain is a distributed ledger accessible by everyone, access control becomes an important issue in controlling the permissible operations on the blockchain.

Recently, blockchain applications for cyber-security in the mobile edge network have been of interest to researchers. In [5] authors present a blockchain based Mobile Edge Computing (MEC) architecture. In [6] the authors present an IoT framework named "EdgeChain", which is based on blockchain and smart contracts. This line of work is interesting but it is not competing with our presented methodology. Our methodology can be used in such frameworks for the specification and verification of policies for smart contracts. We are not aware of such a previous work in this area.

In this paper, we investigate the security issues of blockchain based transactions in 5G networks, particularly in the mobile edge. We propose a methodology for policy specification and verification of transactions based on smart contracts in next generation mobile networks. Our methodology is different from existing work that it is based on formal logic and supports formal verification of smart contract policies.

The rest of the paper is organized as follows. Section 2 discusses some of the security threats and risks of blockchain. Section 3 discusses compliance to security standards through security policy specification and verification. Section 4 presents the proposed methodology for smart contracts policy specification and verification. Finally, in the conclusion we will analyze the methodology and give further research directions.

2. Security threats and risks for 5G enabled blockchains

Some risks associated with blockchain platforms and technologies include the following:

- Money laundering as a result of the high level of anonymity which makes it difficult for regulators to identify individuals who use the protocol for illicit value transfers. Some cryptocurrencies can be used for money laundering purposes, which pose a challenge to enforce financial sanctions.
- Tax evasion may be a consequent side effect of anonymity. In their effort to deal with the global phenomenon of cryptocurrencies, many countries introduced various taxation schemes for cryptocurrencies.
- Risks for monetary and financial stability, including the potential loss of control of the amount of currency in circulation, which risks inflation — a problem that will intensify with the increase in the size of the cryptocurrency market, as well as with the increase of credit-generation within the economy with the use of cryptocurrencies.
- Growing mistrust in fiat currencies more generally. There are many similarities between fiat currencies and cryptocurrencies. First, crypto currency is a digital representation of value that can be traded online and has at least some of the generally recognized functions of money; it operates as a store of value, a medium of exchange, and as a unit of account, but does not have a legal tender status in any legal order. Accordingly, the widespread use of cryptocurrencies together with the new set of problems associated with them could rebound to upset general confidence in conventional currencies.

The new intermediaries of the cryptocurrency environment pose potentially a great risk for consumers, financial institutions and the government as well. Trading platforms and exchanges of cryptocurrencies to fiat currencies, digital wallet service providers, payment systems and pricing indices, and other clearinghouses for cryptocurrency transactions replace the traditional, very often national, financial intermediaries like central and commercial banks. The new intermediaries are exposed to new problems like for example the risk of hacking.

There are many cyptocurrency hacking incidents as of the time of writing, with the biggest loss of around 500 million USD in a single incident (Coincheck) [7]. The latest hacking incident in 2019 was against Binance, the extent of the loss surpassing 40 million USD in assets, with an additional 4 billion USD loss to the market. These incidents mostly arise from insufficient enforcement of security policies and use of hot wallets (wallets connected to the Internet) to store user crypto assets.

3. Achieving compliance to security standards

3.1. Existing security standards and compliance of security policies

One of the most important areas to explore in the compliance and standards domain is to explore how the security standards in the financial sector can be applied to blockchain based financial transactions in 5G networks. The main goal of these standards is to protect customer data from possible compromise and threats. For example, in the financial sector, any business entity that is involved in accepting, processing, and storing payment card information, is required to comply with Payment Card Industry-Data Security Standard (PCI-DSS). In addition, for general purpose software, organizations can employ the Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC-ISO/IEC 15408) for computer security certification. For policy compliance checking and verification, an approach based on automated tools is valuable to test business blockchain application and cryptocurrency application. It is possible to address this issue within a broad area of formality; from very informal, such as scenario based testing, up to very formal approaches which is based on mathematical approaches to prove the security aspects of software.

In this paper we will present a more formal approach which also supports automation. Additionally, all of these standards

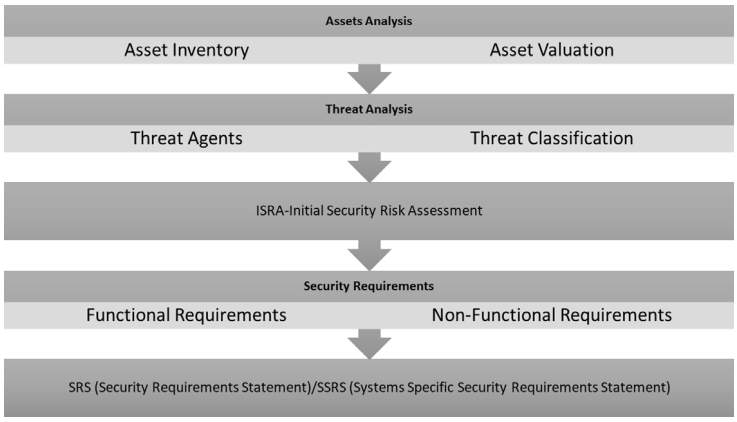

Fig. 1. Security requirements process.

and approaches require structured policy document formats for interoperability and analysis. Therefore, a security policy specification and verification framework for smart contracts, that builds upon structured policy statements and supports formal verification, would be an important enabler for achieving compliance to security standards.

3.2. Security requirements process for smart contracts

Defining security requirements for smart contracts is necessary to address security risks and also an important part of risk resolution. From the standards compliance perspective, security requirements are compulsory in many standards such as ISO 27001 control item 14.1.1 (Information security requirements analysis and specification) [8]. Security policies are also defined within the security requirements process.

In Fig. 1, we provide an overview of the security requirements process. Some assets in the blockchain environment to be considered within the security requirements process are: Distributed ledgers, information assets, business rules, services and functions, source code, intellectual property, encryption keys, information about people and their competencies, account information and funds associated with accounts and transaction logs.

In this regard we identify some examples of critical security requirements for blockchain for financial transactions in 5G networks as follows:
Functional security requirements:
FR-1 Identity management
FR-2 Access control
FR-3 Compliance checking of smart contracts
Non-functional security requirements:
NFR-1 Data protection
NFR-2 Mobility and location based access
NFR-3. Structured policy specification

4. Our methodology: Policy compliance checking and verification for smart contracts

For each transaction conducted by a smart contract, it is necessary to check for consistency analysis for a single policy and between policies through formal analysis. Formal

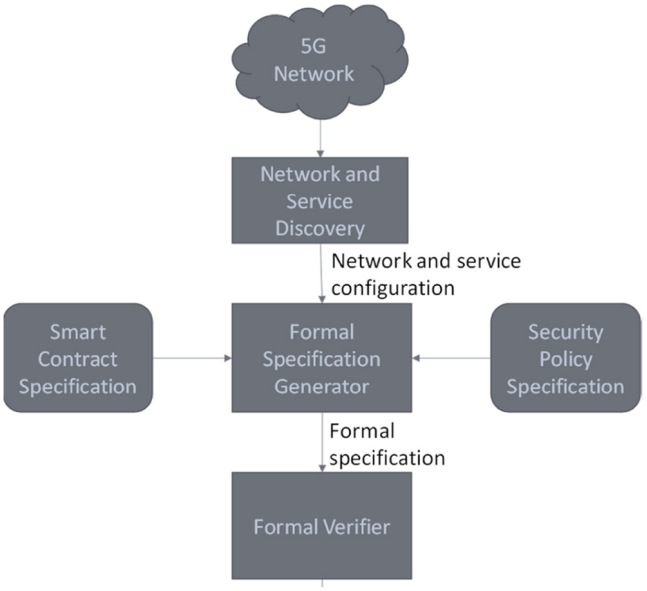

Fig. 2. Overall approach for policy compliance checking and verification for smart contracts in 5G networks.

modeling and analysis of policies for smart contracts, requires a formal model and language for smart contract policies.

A security policy for a smart contract in our context is composed of *agents (users and smart contracts)*, *events* and *objects* of the system; it aims at defining permitted and prohibited *actions*. When defining security policy rules, there are two classes of *constraints*:

1. The constraints that must be satisfied by users and smart contracts when they perform *actions* on *objects*.
2. The constraints that must be satisfied by users and smart contracts when they interact with other users and smart contracts (e.g., responsibility, delegation, hierarchical authority).

The complete proposed flow for the formalization and verification of smart contract policies in the 5G network environment is presented in Fig. 2. In the proposed flow, first the network and service configurations are obtained from the 5G network through network and service discovery. The configuration files, smart contract specification and security

policy specification are input to a formal specification generator, which generates the formal authorization terms and constraints. The formal specification is then input to the formal verifier which generates a policy compliance report.

In the following sub-sections we introduce some example policy statements and explain how these statements can be formally specified and verified for compliance. The formalization and verification approach is based on the FPM-RBAC model [9]. Therefore, we start with a brief reminder of how security policy rules are specified in this model.

4.1. Formal security policy rules in FPM-RBAC

Security policy rules in FPM-RBAC are defined through an authorization term structure, which is the basis of formal specification.

The set of authorization terms in FPM-RBAC is defined as follows: $AT = \{(as, ao, act, co, fo): as \in AS, ao \in AO, act \in ACT, (co, fo) \in C\}$. Here, AS is the set of authorization subjects who may conduct actions on authorization objects. AO is the set of authorization objects, or equivalently, resources that authorization subjects conduct actions upon. A service definition is essentially a subset of resources. ACT denotes the set of actions which may be conducted by a smart contract, such as read, write, deposit or withdraw. A constraint defines the conditions which must be satisfied to execute an action by the smart contract. C defines the set of *constraints* on the execution of the smart contract in the mobile network, where C = {(co, fo): co ∈ PL, fo ∈ AL}. The generic conditions, such as service access, domain and user group membership, mobile network access, are specified in predicate logic (PL). The location and time based policy constraints are defined through the location formula (*fo*) construct which are specified in ambient logic [10] (AL).

4.2. A scenario using smart contracts in 5G networks

We now define a fictitious scenario where a user has access to her crypto-wallet from within multiple wireless networks in her home, in the smart city and at work. This scenario is compliant with the 5G network architecture, where multiple wireless network access technologies will be integrated on a cloud based infrastructure and service based computing.

The user Alice has different requirements for accessing her crypto-wallet from different locations while she is mobile.

- At home she has a 5G mobile network connection. During her time at home, she needs to take care of her elderly mother and small children, therefore she has a shared crypto wallet accessible by the day-caring professional to make necessary spending under her control.
- Around the smart city, she uses her mobile phone to make payments from her daily crypto-wallet for services such as transportation, healthcare and other daily transactions.
- At work she has access to the her investment crypto-wallet where she deposits and sells various crypto-tokens for long term investment and transfers the necessary amount to her other two wallets.

This scenario is built on a multi-domain mobile network architecture, and will be made possible with the seamless connectivity provided by 5G technology. However, the financial transactions on the crypto-assets by smart contracts need to be subject to access control and the operations should be verified in conjunction with a specified policy. Particularly verification is necessary since the transactions on the blockchain are immutable once they are recorded on the blockchain.

4.3. Example security policy statements

For converged network architecture of 5th generation mobile networks, the smart contract structured policy specifications need to support location and time based policies as well as service access policies. Below we present some examples to such policy rules.

R1 (Location based access policy): “Alice is allowed to deposit crypto-assets into the shared crypto-wallet only from Alice’s home network profile”

R2 (Service based access policy) “Daycarer is allowed to spend crypto-assets only on healthcare services for family members”

R3 (Time based access policy): “The withdrawal requests on Alice’s investment wallet may only take place in business days and hours (e.g. Mon–Fri, 08.00–17.00)”

4.4. Formalization of security policy statements

In this section, we present the formalization of mobility, location and time based service access policies presented in the previous section. For the formalization, we use the FPM-RBAC formal authorization terms. The mobility, location and time based constraint formulas in this model are specified through ambient logic, which is a formal modal logic capable of specifying mobility based on locations and time. In this modal logic, three constructs are of particular interest: Parallel (|), Somewhere ($\diamond$), and Sometime ($\diamond$). The parallel construct specifies two entities in the same location. The somewhere construct specifies any entity within a location. The sometime construct specifies the execution of the process to satisfy a temporal constraint during its execution. Together these constructs present a powerful formalism to specify policies for smart contracts executing within various 5G network domains. The formal security policy statements for the policy rules in the previous section are as follows:

R1: (as = Alice, ao = Shared_Wallet, sa = + deposit, co = ActiveDomainUser (as, Home_Profile), fo = Alice_Apartment [as[]] ∧ 5Gmobile_Internet[$\diamond$as []| ao[]])

R2: (as = Daycarer, ao = Shared_Wallet, sa = + withdraw, co = ActiveDomainUser (as, Home_Profile) ∧ ServiceUser (as,Healthcare), UserGroup (user_1, familymember), fo = Alice_Apartment [as[]|user_1[]] ∧ 5Gmobile_Internet[$\diamond$as []| ao[]])

*R3: (as = *, ao = Investment_Wallet, sa = +withdraw, co = ActiveDomainUser (as, Business_Profile), Allowed_Times (Business_Hours), fo = as[]|ao[] ∧ $\diamond$ allowed_times)*

4.5. Verification of security policy statements

In our proposed approach, the verification of security policy statements is achieved through model checking. The formal specification, which is the output of the formal specification generator, consists of a formal process specification and a formal policy specification. The formal process specification represents the state of the network and service configuration and the smart contract specification. The formal policy specification consists of the formalized security policy statements introduced in the previous section.

To check whether a policy statement is satisfied in a given state of the services and network configuration, the satisfaction relation ($\mid =$), which is essentially a structured congruence relation, needs to be computed. This is achieved by the model checker. The model checker checks whether $P \mid = A$ (process P satisfies formula A). The formal process specification is represented as P and the constraints in the formalized policy statements are represented as A. When all policy rules are satisfied within the process specification P, we can conclude that the smart contract execution within a given service and network configuration is compliant with the policy. The model checker has been implemented in Java language. The spatial logic statements are verified inside the Ambient Calculus model checker. The temporal logic statements are converted to NuSMV temporal model checker statements and subsequently verified using the NuSMV model checker.

5. Conclusion

In this paper, we present an approach for policy compliance checking and verification for smart contracts in 5G networks. Our approach builds on formal specification languages and structured policy specifications which are verified through a model checker. Our work complements existing studies in the area of blockchain for 5G networks.

Declaration of competing interest

The authors declare that there is no conflict of interest in this paper.

References

[1] Huawei Inc. and Oxford Economics, Digital Spillover: Measuring the Impact of the Digital Economoy, Sept. 2017. URL: https://www.huawei.com/minisite/gci/en/digital-spillover/index.html. Accessed 30/5/2019.

[2] Jonathan Haskel, Stian Westlake, Capitalism Without Capital: The Rise of the Intangible Economy, Princeton University Press, Princeton, New Jersey, USA, 2018.

[3] Paul J. Taylor, Tooska Dargahi, Ali Dehghantanha, Reza M. Parizi, Kim-Kwang Raymond Choo, A systematic literature review of blockchain cyber security, Digit. Commun. Netw. (2019).

[4] Douglas A. Ashbaugh, Security Software Development Assessing and Managing Security Risks, CRC Press, 2009, (Chapter 2.4).

[5] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, Z. Han, When mobile blockchain meets edge computing, IEEE Commun. Mag. 56 (8) (2018) 33–39.

[6] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu, Y. Zhao, EdgeChain: An Edge-IoT framework and prototype based on blockchain and smart contracts, IEEE Internet Things J. (2019).

[7] How to Steal $500 Million in Cryptocurrency, Fortune Magazine, URL: http://fortune.com/2018/01/31/coincheck-hack-how/. Accessed 30/5/2019.

[8] ISO/IEC, ISO/IEC 27001, ISO/IEC, Switzerland, 2013.

[9] D. Unal, M.U. Çaglayan, FPM-RBAC: A formal role-based access control model for security policies in multi-domain mobile networks, Elsevier Comput. Netw. 57 (1) (2013).

[10] L. Cardelli, A.D. Gordon, Ambient logic, Math. Struct. Comput. Sci. (2006).