Study on the Computational Trust and Its Model

Qingnian Wang1,2, Wenqian Hong1,* and Chuling Huang2

1School of International Education, South China University of Technology, Guangzhou, 510006, Guangdong, China
2School of Economics and Commerce, South China University of Technology, Guangzhou, 510006, Guangdong, China

*Corresponding author

Abstract. The application of block chain technology has greatly improved our digital ability in work and daily life. By fostering greater trust, blockchain technology has not only increased productivity, but is sure to reshape the relationship between individuals and businesses, leading us toward a true digital economy. For hundreds of millions of people and tens of billions of smart devices, this could mean hundreds of billions of smart contracts running autonomously and significantly enhancing global synergies. This paper aims to explore the computational trust model to demonstrate how the trust be computationalised. By building a global blockchain infrastructure, we are spreading trust, and computational trust will be a ubiquitous part of our society. As more businesses and individuals join in, more people will benefit from this new technology, and the future of human society will become more inclusive, transparent, and trustworthy.

Keywords: Computational trust; Model; Study.

1. Introduction

Social interactions are often guided by trust between the participants, but problems associated with building initial trust are common before relationships are established between social entities. Especially in recent years, when Germany's industry 4.0, China's "made in China 2025", the United States' "industrial Internet" and other new science and technology plans are competing for implementation, profound technological and network environmental changes will continue to affect human society and economic development.

At present, the extremely hot block chain research and application is affecting People's Daily activities and the whole society with a function several times larger than that of the Internet era. A growing body of research suggests that universal trust (known as stranger trust) is good for the economy, while lack of such trust has a negative impact on economic growth. When the exchange of goods and services becomes the focus, trading partners' trust in cooperative behavior can reduce transaction costs. More importantly, blockchain can significantly reduce transaction costs [1,2]. When an economy is made up of companies with lower transaction costs, the economy as a whole has a competitive advantage. Trust is crucial to the organization's internal cooperation and overall effectiveness. It can also reduce organizational complexity. When trust is lacking, information exchange is blocked and the risk of misunderstanding is increased, and poor decision-making becomes a serious problem [3,4]. Similar effects also apply to trust in an organization's internal environment, some of which include successful long-term relationships and reduced transaction costs between enterprises [5].
In multi-disciplinary studies, trust is particularly abundant in the areas of human-computer interaction and e-commerce, mainly in the great difference between computer and information-technology-led communication and face-to-face interaction. Therefore, on the one hand, our lives are increasingly dependent on electronic media, in which a large number of signals are distorted [6]; On the other hand, evolutionary cues of trust provide little support, while reduced information increases uncertainty [7]. An important issue is how to foster trust in the electronic media environment. To interpersonal trust forming process as the foundation, it includes input (signal and symbol), cognitive process, collection and selection of information, the credibility of evaluation, the assessment of the situation, the state of trust, trust decision making, context) and output (trust behavior, interaction, and assessment), and can be applied to the reliability estimate priority model [8]. Any change that affects trust will alter commitments, choices, and the emergence of a new social order, which may lead to serious social disorder. Where is the trust in this case? In the commitment hierarchy, first trust, then credibility, then contracts, fiduciary obligations, and regulations [9].

To sum up, trust will become the cornerstone of human social and economic development, and computational trust is the basis for the operation of interpersonal, human-machine, machine-machine and various trading platforms in the highly developed period of human society. Therefore, how to utilize the online platform and its network environment, especially based on block chain technology, and apply certain methods to expand computational trust, will be a major and arduous task.

2. Literature Review

2.1. Research on Computational Trust

In 1994, Marsh proposed the concept of computational trust table and established a tabulated quantifiable trust model, whose parameters include agent, agent's social environment, situation, knowledge, importance, utility, basic trust, universal trust, situational trust and time [16].

In 1995, Berg et al. devised a trust game to measure trust in the field of experimental economics students. Fukuyama studies cultures through the prism of trust, arguing that economic prosperity and well-being depend largely on trust. Wang and Redmiles took the concept of cheap talk from the economic literature and applied evolutionary game theory to virtual teams to gain insight into the dynamics of interpersonal cooperation. They use this tool to prove quantitatively and qualitatively that cheap words on the Internet do promote the emergence of trust, thus increasing the possibility of cooperation [10]. Morrison analyzes the social order that depends on the ability of individuals to make extended commitments to each other, and points out that any change in influencing factors can change commitments, choices, and the emergence of a new social order, which may lead to serious social disorder.

Sollner et al. provided the answer by focusing on so-called trust networks, which involve entities such as information systems, users, providers, the network user community, and the Internet itself. The main finding IS that user trust in information systems (IS) IS the main driver of user use of IS. As important as trust in information systems is trust in IT service providers [11]. Percy raised the issue of asymmetric trust, pointing out that in traditional finance, participants benefit from asymmetric information. In the blockchain financial system, they benefit from the trust asymmetry. Since the level of trust is calculated from the rate of information flow, the trust asymmetry may be regarded as a special case of information asymmetry, and it is found that there is a "belief consensus", and the trust measure as a possible basic source of the intrinsic value of digital assets [12]. Kun-Tai Chan put forward by the trust of the PGP network and the concept of six degrees of separation theory, establishes a distributed environment based on reputation trust evaluation mechanism, the decentralized environment and application of intelligent contract formula, shows how to use intelligent contract record related information and calculate the trust between the two users value, promote people to the judgment of the reliability of strangers, reduce the risk of being deceived [13].

Jacopo proposed that in the interconnected society, understanding the evolution of trust is the key, especially the impact of recording devices on trust, and proposed digital trust to clarify the impact of digital extended memory on trust, which can be further applied to interpersonal trust supported by social media [14]. Marc proposed the definition and elements of trust, described how to build trust, and
compared the components and similarities and differences of four trust models [15]. Qualitative evaluation dynamics (QAD) is a formal structure evolved from algebraic semigroups introduced about 15 years ago. QAD operators and operands have close language roots. In establishing the trust model, common sense reasoning should be reflected. In QAD, trust is handled in a fairly straightforward way. It can be thought of abstractly as a relationship between a principal (that is, a trusted entity) and a trustee (that is, a trusted entity). This relationship can be represented as a graph of two nodes, the principal and the agent, and the relationship between the two nodes represented by a directed arc. In this way, a society with n agents can use a directed graph with n nodes, called a trust graph. Currently, the blockchain technology that implements modern ledger solutions is also a form of computational trust. Based on bitcoin technology, they leverage so-called proof of work to provide transaction group integrity (and partial authentication).

This work proved to be very difficult to forge as hundreds of thousands of user communities were co-computed and validated by distributed systems. It is calculated for each transaction block, and when a new block is formed, it is cryptographically linked to an existing file and generates a new working proof.

2.2. Research on Computational Trust Based on Intelligent Contract
Due to the development of bitcoin, the emergence of distributed ledger technology has aroused great interest among different communities. Smart contracts, a concept first conceived by Szabo, were not proven until 1995 and are now implemented with the advent of distributed ledgers [17]. Szabo's original definition of smart contracts was: "[s] market contracts […] Facilitate all steps of the signing process "; Search, negotiation, commitment, performance and award are all part of the signing process he refers to [18]. Keren's analysis points out that bitcoin, as a platform, can model and execute smart contracts, but is constrained by its limited scripting language. This limitation and the observation that cryptocurrencies can be seen as "just another smart contract", ultimately led to the development of Ethereum: a smart contract is a decentralized platform for individual applications; Distributed ledgers are equipped with the full programming language of Turing, enabling developers to write "arbitrary" contracts/code [19]. Recently, Braynov developed based on the currency and support platform of Turing complete intelligent contract language (such as Rootstock) [20], maybe even more interesting, also developed with a Turing (Turing) complete language platform for the intelligent contracts, namely the tau - Chain [21]. Satoshi Nakamoto's introduction of bitcoin has excited participants in the financial sector from the start: some are very keen on it, believing it to be the "next big thing", while others are very sceptical [22]. Tschorsch and Scheuermann did an excellent technical survey of distributed ledger technology.

In addition, a quick look at the currently available platforms inspired by bitcoin gives a good picture of the growing popularity of the technology: coinkmertcap.com, for example, which tracks the market capitalization of different cryptocurrencies, lists 719 platforms [23]. Ethereum is proposed as a stand-alone distributed platform - but very similar to bitcoin. To create a distributed, trust-free consensus and solve the dual overhead problem, Ethereum USES workload proof, just like bitcoin, however, it provides an Ethereum virtual machine (EVM) running a turing-based completely stack-based language, opening the door to an assumed unlimited number of applications. Developers do not have to use EVM's opcodes to write smart contracts. In fact, they can use solsen or Serpent, which are high-level programming languages similar to javascript or python, respectively, that can be compiled into EVM byte code [24].

Unlike bitcoin and Ethereum, Nxt, one of the first smart contract platforms, USES equity certificates to reach consensus and address dual spending issues. Furthermore, Nxt does not provide scripting languages for smart contract developers; instead, it provides a RESTFUL API that exposes a set of basic operations that developers can invoke. Unlike Ethereum and Nxt, Rootstock was developed to supplement bitcoin and provide its own Turing complete virtual machine (RVM) to implement smart contracts [25]. The author thinks the Turing tau - Chain platform (Turing) integrity is not required for distributed books, because the Turing brought undecidability (Turing) integrity, namely intelligent contract can enter an infinite loop, the network can never predict the behavior [26]. In fact, Ethereum overcomes its incalculable problems by forcing callers of smart contracts to supply natural gas for transactions (purchased in other currencies, Ethereum's own cryptocurrency); Each instruction on the
EVM consumes a predetermined amount of gas, and they are non-refundable, that is, if the gas is completely consumed and the smart contract is not completed, the gas will never be returned to the caller. Asor proposed to use the ontology of rules and the reasoner to realize the calculation on the network [27]. Authors of smart contracts write them in fully functional programming languages like Idris, which are eventually translated into text. This approach not only makes the computation judgeable, but also allows you to determine the attributes of a smart contract that would not be possible in the Turing complete language, such as whether the contract is connected to the Internet, or whether the contract meets certain interface/requirements, etc. [28].

Hsing-chung Chen studied three trust evaluation equations and proposed to provide solutions through online distributed block chain online authorization through the study of three situations: machine-individual, machine-machine and individual-individual [29]. Michael et al. defined heuristic metrics for control flow invariance, measured the invariance of control flow during deployment of all smart contracts on ethereum, developed a data cleansing method using the call graph, and proposed a measurement no-trust formula [30]. Dominik et al. applied the smart contract trust model to analyze the scale of unreliable trust in ethereum, and finally concluded that the trust model mechanism was applied to the computing algorithm and the ethereum block chain, and the results showed that the algorithm needed six semi-trust validators to find the forged submission [31].

2.3. Research on Computational Trust in Blockchain Environment

In today's network environment, there are many social media platforms, such as Facebook, Google and LinkedIn, which act as identity providers for users and provide social login services. This service is often implemented on the basis of an open ID connection framework and is widely used as a trust anchor when new users register for the online service initially, as well as for subsequent authentication processes. Users will be forced to modify their schedules directly, for example, by canceling some of their events, so that they can limit the type of information they want to release to third parties. More importantly, users do not know how much information is stored or shared by social service providers. In the wake of the Cambridge scandal, Facebook has provided a better understanding of the data they collected, the received and rejected friend requests, the entire conversation or file exchanged through Facebook messenger and the historical calls and messages on the phone. Third party information from social service providers also lacks transparency [32]. Kane et al. applied block chain technology to promote trust among block chain agencies. First, the agent as a node in the block chain has a copy of information; second, the information is saved in the block chain by encryption method to avoid tampering of harmful resources, thus forming a trust building mechanism [33].

Constantin et al. studied online trust under the Bootstrap method, introduced the timeline action proof factor, and built the timeline action proof framework. The model does not rely on any centralized social media platform, and users can fully control the actions they want to use as part of it [34].

Bogdan et al. studied trust layering in cryptographic networks, constructed an example on top of Openchain after analyzing the existing blockchain, and proposed a method to achieve trust by using technologies left in cryptocurrencies [35]. By putting forward the core hypothesis that trust equals risk, Orfeas et al. proposed a distributed financial trust platform by using bitcoin, a decentralized cryptocurrency different from traditional currencies, and conducted a trust flow analysis [36].

As shown above, a more common problem with centralized social services in using timeline actions to promote online trust building is the need to trust social service providers in order to protect the privacy of user actions. A lack of trust naturally leads to the question of whether timeline actions can be fully controlled by the user (independent of any centralized service provider) and serve as an additional trust factor in online interactions.

2.4. (Computational Trust Model and Its Application Case Study

Besfort et al. studied the distributed machine-machine application service of blockchain-based trust community, pointed out the problems in the trust assessment process, and applied it in blockchain M2M [37]. Samuel studied trust among stakeholders in the supply chain, analyzed ongoing intentions driven
by the block chain, and explored data collection and model testing in 344 specialized supply chains in India.

Liu qi et al. studied the cooperative innovation trust mechanism of big data processing based on block chain. Block chain technology is essentially a technical solution to jointly maintain a reliable database in a decentralized and highly trusted way [38]. Leo et al. studied traffic vehicle authorization and trust management based on block chain network and proposed an innovative trust building system based on block chain technology. The system is designed to control application identity, as well as application behavior and network resource allocation and management. In addition, the design of the system using intelligent contract is also introduced [39].

Xu quanqing et al. studied the recognition and trust of decentralized wharf image content based on block chain, discussed the vulnerability of notarization to denial of service (DoS) attacks, and proposed a potential solution: distributed trust based on block chain (DDT). This scheme effectively reduces the risk of denial of service, and at the same time, provides signature confirmation tasks for wharf images [40]. Davide et al. believe that blockchain technology-based (BCT) trustless and trust-based regulatory systems are currently experiencing the greatest hype and are expected to revolutionize the entire field. Tourism products (intangible services) are highly dependent on trust and reputation management [41].

Kristin called for research into blockchain technology, especially smart contracts, to use smart contracts as evidence for legal defense. Because they involve two types of oversight practices. First, the study considers how legal discourse provides (or fails to provide) appropriate oversight for digital contracts. The second is to focus on the investigation and prosecution of criminal activities, as well as the establishment of standards and regulations by the corresponding agencies to force companies to provide records as evidence in these investigations [42]. Blackstad et al. looked at trust solutions in context. Traditional encryption of trust permission data is based on block chain concept and encryption. We see it as a useful tool in the broader toolkit, and it also has the opportunity to provide much better trust for most customer/business interactions. The challenge is to capture the link between protocols, payments and digital assets [43].

Firas et al. argue that trust in smart contracts is a process. It is true that cryptography assurance is an enabler and component of trust in distributed ledger technology, but another kind of trust, the law established by a process involving lawyers, is also needed and a trust mechanism is proposed [44]. Miguel et al. propose applications in the courts that enhance trust and reduce costs. In order to solve the electronic judicial system slow/expensive and inefficient problem, can simplify the production of evidence, to this end, evidence (any type of digital document/file) by all stakeholders (may include a lawyer/client) for digital signatures, and submitted to the online platform, the platform to create evidence that store and manage access to evidence [45].

2.5. Questions that Need Further Study

There are several challenges in the research and extensive application of computational trust: (i) the research on trust is from symbol-based modeling and computing procedures, to the internal trust of people or human agents related to services or technologies, and then to the design of computational trust, but it has not formed an efficient and feasible scheme;

(ii) in the chain of blocks in the computational trust research of intelligent contract, from a number of intelligent platform to establish a contract, the mechanism of the attainment of computational trust connotation of simplification, workload is often to prove (Pow), certificate of action (PoA), certificate of rights (PoS), certificate of rights and interests and active rate (PoSV), certificate of authorization of equity trust (DPoS), and other simple way instead.

(iii) in the application of Bootstrap method to conduct computational trust research, from information tamper proof, to trust flow, and then to online trust research, computational trust research cannot reflect trust flow and its change process due to the lack of a comprehensive model to measure trust;

(iv) in the construction of computational trust model and its application research, the core issue of computational trust flow is related to the application of supply chain, transportation, wharf, tourism, law and other aspects, as well as the trust issue in machine-machine application service. Therefore, it is necessary to explore the computational trust model and its mechanism.
3. Construction of Computational Trust Model

3.1. Computational Trust Expression of Bootstrap Method

According to the Bootstrap method, the computational trust expression is transformed as follows:

Timeline action and timeline action proof (TAP).

The online actions performed by the user are modeled in terms of timeline actions. They are historical evidence of trust and are defined according to the following model:

\[ \langle \text{pk}, \text{atime}, \text{aname}, \text{count}, \text{adata}, (\text{tags}) \rangle \]  \hspace{1cm} (1)

Timeline action proof (TAP) is defined as:

\[ \text{TAP} = ((\text{Setup}, \text{KGenU, SubmitU, IProofU, IProofV})) \]  \hspace{1cm} (2)

The PK, atime, aname, Count, adata, (tags), the Setup (\lambda), KGenU (pp), SubmitU ((pp, sk, (aname, adata, [tags])), IProofU (pp, sk, \Psi), IProofV (pp, PK) respectively is proved that express parameters, such as a series of time, activity.

3.2. Operation Process of Computational Trust Model

Connect timeline actions to distributed ledgers. The abstract ledger is mapped to the information type activity required to store the user and the conditions for defining the validity of the data are specified according to the flow chart for the operation of the computational trust model (figure 1).

The entries in the super ledger contain labels for common information such as users, action types, counters, and ciphertext for active data.

![Figure 1. Flow chart of the operation of the computational trust model.](image)

3.3. Computational Implementation of Trust

According to the dimensions of computational trust structure and combined with the Bootstrap method, this project proposes the implementation plan of computational trust, as shown in figure 2.

3.4. Construction of Computational Trust Model

Start with the standard encryption primitives used as building blocks, and a way to calculate the encryption key to hide the active data. The construction of blocks in this project is as follows:

Our construct relies on the pseudo-random function PRF, and a digital signature scheme DS= (KGen, Sign, Verify) that cannot be forged.

We further rely on the symmetric encryption scheme SE= (KGen, Enc, Dec), which has two security requirements: indiscernability under ind-cpa and error key detection (WKD).
The WKD attribute is not standardized and has been introduced to constrain the probability of successful decryption of a ciphertext by an opponent using two different keys.

4. Conclusion and Discussion
This work will be furthered by strengthening the computational trust mechanism and the model applied in the later research.

Acknowledgements
This work were supported by the Humanity and Social Science Foundation of Guangzhou, China (Grants No.2019GZGJ08) and the Humanity and Social Science Foundation of SCUT.

References
[1] Zak P J , Knack S . Trust and Growth[J]. Economic Journal, 2001, 111(470):295-321.
[2] Arrow K J, Norton. The limits of organization[J]. Journal of Economic Issues, 1974, 9(3).
[3] Häkkinen P. What makes learning and understanding in virtual teams so difficult?[J]. CyberPsychology & Behavior. 2004,7(2):201-206.
[4] F. Hartman, The role of trust in project management, in Managing Business by Projects, ed[M].Finland and Nordnet, Elsinki:Project Management Association,1999.
[5] Koehn D . SHOULD WE TRUST IN TRUST?[J]. American Business Law Journal, 2010, 34(2):183-204.
[6] Kral G. Review Essay: Nicole Döring (2003) Sozialpsychologie des Internet[J]. Historical Social Research, 2004, 29(4(110)):220-226.
[7] Shneiderman B . Designing trust into online experiences[J]. Communications of the Acm, 2000, 43(12):57-59.
[8] Rusman, Ellen, Bruggen V , et al. Fostering trust in virtual project teams: Towards a design framework grounded in a TrustWorthiness ANtecedents (TWAN) schema[J]. International Journal of Human-Computer Studies, 2010, 68(11):834-850.
[9] Morrison A D , Wilhelm W J . Trust, Reputation, and Law: the Evolution of Commitment in Investment Banking[J]. Journal of Legal Analysis, 2013, 7(2):lav007.
[10] Wang Y , Redmiles D . Cheap talk, cooperation, and trust in global software engineering[J]. Empirical Software Engineering, 2015:1-35.
[11] Söllner M, Hoffmann A, Leimeister J M. Why different trust relationships matter for information systems users[J]. European Journal of Information Systems, 2016, 25(3):274-287.

[12] Venegas P. Trust Asymmetry[C]// International Conference on Complex Systems. Springer, Cham, 2018.

[13] Chan K T, Tso R, Chen C M, et al. Reputation-Based Trust Evaluation Mechanism for Decentralized Environments and Its Applications Based on Smart Contracts[J]. Advances in Computer Science and Ubiquitous Computing, 2017, 474: 310-314.

[14] Domenicucci J. Trust, Extended Memories and Social Media[J]. Towards a Philosophy of Digital Media, 2018: 119-142.

[15] Sel M. A Comparison of Trust Models[C]// Springer Vieweg, Wiesbaden, 2015.

[16] Kahneman D, Tversky A. Choices, Values, and Frames[J]. American Psychologist, 2000, 39(4): 341-350.

[17] Inglehart R, Welzel C. Modernization, Cultural Change, and Democracy: The Human Development Sequence[M]. New York: Cambridge University Press, 2005.

[18] Keren A. Trust and belief: a preemptive reasons account[J]. Synthese, 2014, 191(12):2593-2615.

[19] Aquino D, Alves J. The Meaning of Trust for Brazilians with Higher Education[J]. Social Indicators Research, 2017, 130(1): 325-349.

[20] Braynov S. Contracting with Uncertain Level of Trust[C]// Acm Conference on Electronic Commerce. ACM, 1999.

[21] Gefen D. E-commerce: the role of familiarity and trust[J]. Omega, 2000, 28(6): 725-737.

[22] Ke D, Chen A, Su C. Online trust-building mechanisms for existing brands: the moderating role of the e-business platform certification system[J]. Electronic Commerce Research, 2016, 16(2): 189-216.

[23] Aquino D, Alves J. The Meaning of Trust for Brazilians with Higher Education[J]. Social Indicators Research, 2017, 130(1): 325-349.

[24] Braynov S. Contracting with Uncertain Level of Trust[C]// Acm Conference on Electronic Commerce. ACM, 1999.

[25] Bursian D, Weichenrieder A J, Zimmer J. Trust in government and fiscal adjustments[J]. International Tax & Public Finance, 2013, 22(4): 1-20.

[26] Chen H-C. A Trust Evaluation Gateway for Distributed Blockchain IoT Network[C]// International Wireless Internet Conference. Springer, Cham, 2019.

[27] Fröwis M, Böhme R. In Code We Trust? [J]. Data Privacy Management, Cryptocurrencies and Blockchain Technology, 2017: 357-372.

[28] Harz D, Boman M. The Scalability of Trustless Trust[J]. Financial Cryptography and Data Security, 2018: 279-293.

[29] Deutsch M. Trust and Suspicion[J]. Journal of Conflict Resolution, 1958, 2(4): 265-279.

[30] S. Einwiller, When reputation engenders trust: an empirical investigation in business-to-consumer electronic commerce[J]. Electron. Mark, 2003, 13(3): 196–209.

[31] Smith K, Dhillon G. Supply Chain Virtualization: Facilitating Agent Trust Utilizing Blockchain Technology[J]. Revisiting Supply Chain Risk, 2018: 299-311.

[32] Cătălin Drăgan C, Manulis M. Bootstrapping Online Trust: Timeline Activity Proofs[C]// Data Privacy Management, Cryptocurrencies and Blockchain Technology. Springer, Cham, 2018.

[33] Iancu B, Sandu C. A Cryptographic Approach for Implementing Semantic Web’s Trust Layer[M]// Innovative Security Solutions for Information Technology and Communications. Springer International Publishing, 2016.

[34] Litos O S T, Zindros D. Trust Is Risk: A Decentralized Financial Trust Platform[M]// Financial Cryptography and Data Security. Springer, Cham, 2017.

[35] Shala B, Wacht P, Trick U, et al. Trust Integration for Security Optimisation in P2P-Based M2M Applications[C]// 2017 IEEE Trustcom/BigDataSE/ICCESS. IEEE, 2017.

[36] Wamba S F. Continuance Intention in Blockchain-Enabled Supply Chain Applications: Modelling the Moderating Effect of Supply Chain Stakeholders Trust[J]. Information Systems, 2018: 38-43.
[37] Liu Q, Zou X. Research on trust mechanism of cooperation innovation with big data processing based on blockchain[J]. EURASIP Journal on Wireless Communications and Networking, 2019, 2019(1):26.

[38] Léo Mendiboure, Chalouf M A, Krief F. Towards a Blockchain-Based SD-IoV for Applications Authentication and Trust Management[J]. Internet of Vehicles. Technologies and Services Towards Smart City, 2018: 265-277.

[39] Xu Q, Jin C, Rasid M F B M, et al. Blockchain-based decentralized content trust for docker images[J]. Multimedia Tools and Applications, 2017.

[40] Calvaresi D, Leis M, et al. Trust in Tourism via Blockchain Technology: Results from a Systematic Review[C]//Information and Communication Technologies in Tourism 2019. Springer, Cham, 2018.

[41] Cornelius K. Smart Contracts as Evidence: Trust, Records, and the Future of Decentralized Transactions[J]. Second International Handbook of Internet Research, 2018:1-20.

[42] Blakstad S, Allen R. FinTech Revolution // Contextualised Trust Solutions[J]. FinTech Revolution, 2018, 10.1007/978-3-319-76014-8(Chapter 20):319-326.

[43] Khalil F A, Butler T, O’Brien L, et al. Trust in Smart Contracts is a Process, As Well[C]// Workshop on Trusted Smart Contracts in Association with Financial Cryptography. Springer, Cham, 2017.

[44] Matos M, Duque D, Silva J, et al. The Production and Simplification of Evidence - Enhancing Trust and Costs Reduction on Court[C]// Proceedings of the Computational Methods in Systems and Software. Springer, Cham, 2018.

[45] Trˇcek, Denis. An Integrative Architecture for a Sensor-Supported Trust Management System[J]. Sensors, 2012, 12(12):10774-10787.