Chapter 17
Blockchain-Powered Internet of Things, E-Governance and E-Democracy

Renming Qi, Chen Feng, Zheng Liu and Nezih Mrad

Abstract Digital technologies have dramatically changed people's daily life and made our life components much smarter. Nowadays, all users, including both human beings and devices, are connected to centralized servers. These servers act as the authorities, which are trusted by all users, making it possible to exchange critical information and money between untrusted users. However, maintaining large servers is costly and it's not affordable if such digital systems for cities' critical infrastructures are hacked. Blockchain, a technology revolution starting from 2014, offer the potential to solve these problems. It is essentially a tool that records every single transaction and digital event that happen in the virtual world. All the records are open to every user and the information asymmetries between two users are minimized. Thus, it's not possible for one user to cheat or hide information from another user. In other words, two strangers do not need to worry about being cheated by each other. They are allowed, for the first time in history, to do business without a centralized authority. Since a centralized authority is no longer a necessity, these two problems disappear naturally. This survey first explains how blockchain makes this magic happen and then introduces the blockchain's powerful applications in Internet of Things, E-governance, and E-democracy.

Keywords Blockchain · Internet of Things · E-governance · E-democracy

R. Qi
School of Engineering, EME1240-1137 Alumni Ave, Kelowna, BC V1V 1V7, Canada

C. Feng (✉)
School of Engineering, EME4285-1137 Alumni Ave, Kelowna, BC V1V 1V7, Canada
e-mail: chen.feng@ubc.ca

Z. Liu
School of Engineering, EME4205-1137 Alumni Ave, Kelowna, BC V1V 1V7, Canada

N. Mrad
Defence Research and Development Canada (DRDC), Department of National Defence,
National Defence Headquarters, Major-General George R. Pearkes Building, 101 Colonel by
Drive Ottawa, Ottawa, ON K1A 0K2, Canada

T.M. Vinod Kumar (ed.), *E-Democracy for Smart Cities*, Advances in 21st Century
Human Settlements, DOI 10.1007/978-981-10-4035-1_17

17.1 Introduction

Our cities are getting smarter by utilizing digital technologies, such as online video meeting, self-driving cars, online medical insurance payment, and electronic voting etc. The application of digital technologies to smart cities can be, in general, divided into three categories: Internet of Things (IoT), E-governance, and E-democracy. The IoT refers to a network of connected devices (such as smartphones and sensors) where the network connectivity allows these devices to collect relevant information and take corresponding actions. For example, Apple Inc. can help its iPhone users to locate their missing phones by connecting every iPhone to iCloud and collecting GPS information from missing iPhones.

E-governance utilizes digital technologies to provide public services in an efficient and user-satisfactory way. For instance, in- stead of driving to a government building to file their taxes, nowadays citizens can choose to fill in and submit tax forms online, saving hours of unnecessary waiting time. E-democracy leverages digital technologies to facilitate citizens' participation in government's events and decision-making processes, holding political power running in an accountable way. For example, electronic voting provides voters a fast and convenient voting experience, attracting more citizens to vote.

Despite these great benefits, the application of digital technologies to smart cities still suffers from two major issues: high costs and insufficient security. For instance, with respect to IoT, it may incur a huge amount of operational expenditure (Opex) to build and maintain a large-scale *centralized* cloud platform (such as Apple's iCloud) to connect all devices. In addition, current cloud service providers are still not compatible with each other, leading to a high cost of labor to implement an information exchange hub working across different cloud providers. As for security, with an increasing number of connected devices embedded in cities' critical infrastructure (such as railways, tunnels and energy distributions), people cannot afford to under-estimate the risk of a cyber attack to a critical infrastructure that may cause severe damages to city properties and human life. Similarly, there is no proof or protection that our private information, such as bank statements and medical records, collected by E-governance will not be abused by incompetent management (perhaps due to corruption).

In this survey, we investigate a promising solution to all the existing issues: a technology revolution called "blockchain". The blockchain was first introduced by Nakamoto [1] as the ledger of Bitcoin, which is the first widely-deployed digital cash, very similar to the old American "gold-standard" currency. The blockchain can hold a record of every transaction made by Bitcoin users and provides a *decentralized* manner to process these transactions. Unlike traditional financial services hiring a bank to validate each transaction, there is no need for a centralized authority in blockchain. Many participants of blockchain volunteer to verify each transaction, leading to much lower Opex. To ensure the proper performance, these volunteers will be awarded for their correct work on validation and will, sometimes, be penalized for their incorrect work. In this way, blockchain participants only rely on trustable volunteers rather than a centralized authority like banks. On the other hand, if one participant wants to tamper with previous transactions, he has to persuade all the other users agreeing on him to do so, which is proven to be an extremely difficult task. Because of its low cost and high-level security, blockchain has emerged as an ideal technology to store records persistently, including contracts, diplomas, and certificates etc.

The application of blockchain is not limited to financial services. The industry extends the concept of transactions to smart contracts [2]. In order to distinguish blockchain of smart contracts from the previous blockchain of money, we call this stage blockchain 2.0 and the previous stage blockchain 1.0. A smart contract is a contract whose items are self-executing computer programs. Once two willing parties make a smart contract and publish it on blockchain, the associated computer programs will run without any human intervention. Since records in blockchain cannot be altered and the programs will run automatically, both parties have to obey rules in this contract and have no methods to break them. This enables, for the first time in history, untrusted parties to do business with each other without a centralized authority.

Blockchain is envisioned to transform the application of digital technologies to smart cities from two aspects: automation and security. For IoT applications, transactions and coordination between devices can be facilitated by blockchain. Instead of relying on a centralized cloud, devices are empowered to autonomously execute digital contracts, including buying electricity, selling collected information to peer devices and etc. For E-governance applications, the way of enforcing regulations is going to change. Traditionally, regulations are enforced by agencies such as food-safety agency and fiscal agency. With a smart contract in play, regulations can be translated into computer programs, which will be run by blockchain automatically. The human intervention will be taken out of the loop in the entire process, leaving no room for corruption. Security comes directly from the fact that there is no central point in blockchain. Hacking applications on blockchain requires hacking every single user, which is much harder than hacking a single central point. More details of applying blockchain to IoT, E-governance and E-democracy will be discussed in Sects. 17.3, 17.4 and 17.5.

17.2 Blockchain 1.0

Digital cash is infinitely copiable (like copying a file on computer for many times). If someone received a unit of digital cash, he/she can make several copies of it and pass them on to other people, which will definitely disturb the financial system. This problem is called double-spend problem. Previously people hire centralized intermediaries such as banks to solve this problem. When consumers do online payments, the bank will check whether the consumers have enough balance in their accounts and only after confirming that, it will send sellers the money and inform the seller to send consumers the goods. However, blockchain, as a breakthrough in digital cash research, solved the double-spend problem and avoids the centralized third party at the mean time. To explain how blockchain achieves this, we will describe the basic concept of blockchain, including transaction, block and distributed consensus algorithm over the peer-to-peer network.

A transaction in blockchain includes four components: (1) input: spender's address (or user account); (2) output: receiver's address; (3) amount: quantity of units transacted; and (4) metadata: additional information stored with each transaction [3]. Each transaction is signed by its creator with a digital signature, broadcasted to every node in the blockchain network and then recorded in public ledger after validation. Before recording any transaction, the verifying node must ensure two things: (1) the spender owns the money by verifying the digital signatures on the transaction; (2) the spender has enough money on his account by checking every transaction against spender's account in the ledger to make sure he has sufficient balance.

Transactions are passed node by node in the peer-to-peer network, so there is no guarantee that transactions will be received at a certain node or be received in order as they are generated. Here comes the problem of double-spend. Even though malicious user only owns ten dollars, he/she could broadcast two transactions containing 10 dollars to the network simultaneously. Nodes that only receive one transaction judge the received one as verifiable while nodes that receive both only admit the first one. This means that there is demand for a mechanism that enables the whole network to agree on the order of transactions. The mechanism is known as distributed consensus algorithm.

The distributed consensus on blockchain is a two-step process. At first, each node orders the transactions it received by placing them in a linear sequence of blocks. Each block consists of 4 components: (1) transactions collected in a certain period of time; (2) a reference to the block that comes immediately before it; (3) an answer to a hard-to-solve mathematical puzzle. The puzzle is unique for every block and it will be introduced in the following paragraph. The correctness of answer in a block is easy to verify; (4) a timestamp which indicates when the block is built [4]. The transactions in one block are regarded to be created at the same time. Every node can collect unconfirmed transactions into a block and broadcast the block to network as their suggestions on what should be added to the current sequences of blocks. In the second step, blockchain needs to decide which block among these suggestions should really be the next block and make every participant agree with this block. This turns out to be a hard problem since there is no centralized server which is responsible for collecting everyone's suggestions, making the final decision and forcing everyone to agree with the decision.

Blockchain solves this problem elegantly by using a race of solving a hard mathematical puzzle as mentioned above. The first one who solves the puzzle will make the next block. This is also known as "proof of work" [1], because by solving this puzzle, a node can prove that it does use lots of resources to win the race. For example, in Bitcoin, the puzzle is to find a number that makes the hash of the concatenation of this number, transactions contained in this block and the hash of previous block start with a certain number of zeros. The average efforts required to find the answer is exponential with the number of zeros. Bitcoin system will adjust the number of zeros according to the computing power of the network so that average time to find a required number is constant and nearly 10 min [5].

After receiving and verifying the block proposed by the node who first solved the puzzle, other nodes can show their agreement on this block by working on the new puzzle that contains the hash of this block. The block builder is usually called "miner". Miners receive financial awards for spending resources to make a block. In Bitcoin, after building a block, the builder will be awarded a certain number of bitcoins by Bitcoin protocol and each starter of transactions in the block have to leave him a tip. The awards can ensure miners work uprightly since if they conduct malicious behaviors, the blockchain is no longer trustable and then assets of miners on blockchain will become valueless. Besides, the network accepts only the longest sequences. As long as the majority of resources is controlled by miners who don't cooperate to attack blockchain, they will generate the longest sequence and the attacker will be outpaced. As a result, for the first time in history, untrusted parties to do business with each other without a centralized authority.

17.3 Blockchain 2.0

Blockchain 2.0 decentralizes more complicated agreements, i.e. contracts beyond financial systems. Techniques used to decentralize functionality of a ledger in blockchain 1.0 can be adopted to register, confirm and transfer all kinds of contract and assets in blockchain 2.0.

17.3.1 Smart Contract

Simply speaking, smart contracts are published computer programs agreed by both parties on blockchain [6]. A contract in a traditional sense is specific terms between two or more parties in which there is a promise to do something in return for some benefits. Each party must trust the other party to fulfill its obligations. If there is any disputation, they need to resort to courts for resolution. The contract on blockchain is smart in the sense that it allows contractors to solve common problems in a way that minimizes trust. Minimizing trust makes things easier by allowing human intervention to be taken out of the loop, thus allowing complete automation. The automation here means two things. One is after the contract is launched, it will be self-executing and there is no need for contact between contractors. The other is that the contract is able to arrange resources on its own behalf. This ability requires smart property which will be introduced later.

The main difficulty for smart contracts is that computer programs cannot easily and reliably tell what's happening in the physical world or who is telling the truth. Checking whether a financial payment is made is easy for computer programs, but real-world situations like whether one's work achieves the company's standard are hard for computer programs to evaluate. One solution is to use oracles—online service providers who broadcast data which can be used by users as input to smart contracts [7]. A good example is the inheritance gift. An old man leaves an inheritance gift to his grandson and sets the condition that the gift can be received after he passes away. The old man can make the contract and publishes it onto blockchain. An oracle can broadcast new entries in government registry of death. The contract receives this as an input and once the death is confirmed, the gift will be sent automatically.

17.3.2 Smart Property

Smart properties are properties whose ownership are controlled by blockchain using smart contracts [8]. The asset includes physical property (such as a house or a car) and intangible asset (such as votes, ideas, reputation, health data, rights, and shares in a company). The key idea of smart properties is that ownership of these properties is represented by a private key on blockchain. The owner can prove his ownership by showing having access to the certain private key. A good example is buying a car via blockchain. The car's computer requires authentication by using an owner key. Additionally, the car has a token from its manufacturer that has been published on blockchain to prove its existence. This token can also be used to identify its age, mileage and maintenance recording, giving enough information for the buyer to make the decision. In order to buy the car, the buyer makes a smart contract with the original owner with the following item, if the buyer pays the money, the token must be transferred to the buyer's account. The car's computer will be aware of this via blockchain and then the buyer can use its private key to open the car. No third party including government is necessary for this process.

17.4 Blockchain and IoT

Current IoT systems rely on centralized communication models. All devices are identified, authenticated and connected through various cloud servers that support huge processing and storage capacities. However, there is no single unified platform that connects all devices and no guarantee that cloud services offered by different manufacturers are interoperable and compatible. For instance, the field of logistics information support systems is fragmented and diverse. Every logistics company uses their own software products and very few of them can communicate meaningfully with each other. System integrations on any level are almost always built as one-on-one relationship between operational ERPs and their databases and are thus very much costly and tailored work. Human component as the information exchange hub is rather the norm than the exception. Actually, operational information is routinely passed over phone, email and even old-fashioned fax machine by human.

Blockchain works well for this problem. Blockchain achieves trustless connection without sacrificing data integrity, which is what supply chain business is virtually all about. Following this thought, a project named SmartLog is launched [9]. SmartLog is trying to introduce a scenario where all kinds and sizes of logistics companies are able to share and tap into a common blockchain, which will consist of all the relevant information pertaining to the movement of intermodal containers throughout the European Union transport corridors. Information will be gathered from companies' own information management system and then shared among all participants after being anonymized and filtered. There will also be a simple device attached to some of the containers, so companies can validate actual movements of containers in the corridors against the information which they see flowing into the blockchain. The data will serve several different purposes: the participating companies will have immediate access to it and can use it to greatly enhance their operations, resource management, and route optimization planning.

Another downside of current centralized communication model is that costs of installing and maintaining large centralized clouds are high. As the scale of IoT devices tends to grow explosively, these costs will grow substantially and cloud servers will become a bottleneck and a point of failure that can disrupt the entire network. Adopting a standardized peer-to-peer communication model between devices via blockchain will significantly reduce the costs associated with installing and maintaining large centralized data centers. It will also distribute computation and storage needs across the billions of devices from central servers to devices in IoT networks. This will prevent failure in any single node in a network from bringing the entire network to a halting collapse. However, the prospects of the decentralized model are beyond this. Without centralized management, each device manages its own roles and behaviors, resulting in an "Internet of Decentralized, Autonomous Things" [10]. We use the blockchain-powered self-driving car to show this idea. After taking a ride, people can pay directly to the car instead of the driver or the company it belongs to. The car can use these payments to maintain itself and the remaining money becomes the profit of the taxi company. If the car runs out of gas, it drives itself to a nearby gas station and pays the gas dump to get filled. When there are too many passengers for a car, the car can call its peer cars via blockchain to make every passenger served.

Here we present blockchain as "language" used by self-driving cars to communicate with the physical world (passengers) and peer devices (peer cars and the gas dump). We can be more aggressive. Blockchain can be used as general communication tools for artificial intelligence. The artificial intelligence found in Siri and Watson currently is a singular artificial intelligence, which is far from human beings. In contrast, human's society is a form of a multi-agent system, where each agent is independent and intelligent. The society is formed through communication and co-operation between human beings. Blockchain's mechanism of achieving persisting consensus in trustless peer environment makes a multi-agent system of intelligent devices possible. The consensus among devices makes each device get the same sense of a signal as others. These senses act like words in human's language, making device-to-device communication possible. Persistence means that the sense will not diminish with time. For humans, persistence means that we see further by standing on giant's shoulders. There is no necessity to invent calculus again when we use it. For devices, persistence means device-readable knowledge, making devices evolve their functionality automatically. There have already been some primitive discussions in this field, see details in [11, 12].

17.5 Blockchain and E-Governance

A key role of a democratic government is the appropriate distribution of resource among its citizens, both individual and corporate. This goes beyond the distribution of monetary resource and includes social intangibles such as security, the conditions for the maintenance of the rule of law. However, as we have witnessed, governments have become larger, more centralized and more remote from the individual citizens. Centralized model provides poor customer service and is no longer economic. Citizens' queries and needs cannot be responded in time. Governments have started to provide e-governance service, which uses information technology to improve service quality and efficiency. Though a prodigious amount of money has been invested to e-governance to improve service quality and governance efficiency, what is achieved by e-governance is trivial. Blockchain is about to change this by enabling governments to provide service and carry out governance in a detailed way.

A good example is the food safety issue. Consumers surprisingly know little about most of the products they use daily. A complex network of retailers, distributors, transporters, storage facilities and suppliers stand between consumers and the products they use. Governments set up food safety agencies to enforce every component of this chain to comply with standards but the recent Chipotle food contamination crisis [13], Chinese tainted milk scandal [14] show that governments failed.

Blockchain-powered food supply chain management may be a solution. Walmart, IBM and Tsinghua University just started to collaborate together to provide quality assurance for providers and consumers [15]. With blockchain, food products can be digitally tracked from an ecosystem of suppliers to store shelves and ultimately to consumers. Digital product information such as farm origination details, batch numbers, factory and processing data, expiration dates, storage temperatures and shipping detail are digitally connected to food items and the information is entered into blockchain along every step of the process. Governments can use each piece of information to detect critical data points that could potentially reveal food safety issues with the product. Since information on blockchain cannot be altered, this ensures all the information is accurate and that no involver can cheat.

Another example is the regulation in financial systems. Financial institutions need to submit digital reports to regulators to prove that they did not break the regulations. One of the main challenges is that they need to comply with existing regulations: EMIR in EU and Dodd-Frank in US [16]. Due to the myriad of regulatory obligations, the reporting process currently is rather complex. Moreover, regulations in EU and those in the US are not necessarily consistent with each other. This puts a heavy burden on industry and consumes substantial resources. For governments, validating these reports requires much human labor and time. The long delay of this process also enables bank managers to conceal their wrongdoings as they did in the crisis of 2008. And these reports often use different methodologies behind the calculations. This enables companies to take advantage of loopholes to avoid un-profitable regulation and sometimes leads to confusion. Blockchain can benefit both financial institutions and regulators. The regulations in legal files can be translated into smart contracts and then packaged to software. This software defines whether an action is permissible or not so that financial institutions can obey regulations by using API of this software instead of reporting to governments. Since transactions are stored in blockchain, access for regulators to them is easier and faster. Validation can be helped by the consensus mechanism of blockchain: impermissible behaviors cannot be admitted by the network and thus cannot be conducted.

The security of digital resources is also a headache of both governments and citizens. For governments, all information is stored on centralized servers. If one server is attacked, most of the confidential information will be leaked. For users, there is no proof or protection that their privacy collected by governments will not be abused. Even worse, the software used by governments and citizens may be built with backdoors, which can be used to conduct malicious behaviors without being detected. Blockchain provides elegant solutions to these security problems. We first introduce MIT's Enigma, a privacy-preserved blockchain platform [17]. Data is encrypted and stored in distributed nodes. Rather than hacking a centralized server to steal information, hackers need to hack the whole network. Moreover, any smart contract can directly run on encrypted data by using homomorphic encryption [18]. Thus, data on Enigma can be stored, shared and analyzed without revealed to the third party including the government itself, enabling trustless sharing of data and distributed computation without leaking users' privacy. If one wants to use back-doors to conduct malicious behavior, he will not succeed because other users on blockchain will reject his action. Moreover, every action is recorded on blockchain.

Big-data analysis on these records can be adopted to detect abnormal behaviors, prevent new frauds before they happen and even find the source of frauds. Block-Cypher has started to work on this idea [19]. It aims at building a blockchain-based platform on which every action will be given a risk score according to the user's history, behavior pattern, location and etc. The high-scored action which may be a fraud with high possibility will be rejected.

17.6 Blockchain and E-Democracy

Voting is the basic approach to democracy, but current voting system haves been plagued with voting frauds. According to [20], at least 7 billion Americans vote multiple times in federal elections. This duplicity can be used by any special interest groups who seek to gain advantage for the candidates they support. There is also no way for voters to assure that their votes will be accurately recorded and counted. It's not who votes but who counts the votes decides the winner. The voting fraud frustrates people from believing that their votes matter, so most people choose not to vote. In the American federal election of 2012, only 58% of people who are eligible to vote actually voted. Many governments became interested in the electronic voting machine, which could increase the transparency of voting to prevent frauds. However, this interest comes with security warnings. In [21], the authors revealed that one who gained physical access to the Diebold AccuVote-TS voting machine or its removable memory card could install malicious code capable of stealing votes without being detected. Many people will use the same voting machine so this single point failure has enormous impacts on results. Moreover, the voting machine is usually designed, produced and maintained by a single company. There is no proof that this company will not install malicious codes in the machine at the beginning.

Blockchain is an effective solution to problems in the voting system. The blockchain-powered voting runs as follows: (1) Before voting, a user sends his legal Identification and username on blockchain to an identity verifier. After being approved, the user will receive his unique ballot. The verifier is not necessarily the government. The task of verification can be undertaken by miners, who has the incentive to behave uprightly. And by using homomorphic encryption, the verification process can directly run on encrypted data, without leaking the user's identity; (2) During the election, the user completes his ballot and sends it to the blockchain-based ballot box. Each user uses a different device as the entrance point to voting so hacking single device has little effect on the voting results; (3) After the election, each user is allowed to audit the vote results because each user can access the open data on blockchain. In addition, a user's decision will not be known to other voters since users use their pseudo name on blockchain when voting. Many projects of blockchain-based voting have been launched already, such as BitCongress [22], AgoraVoting [23] and FollowMyVote [24].

The other impact of blockchain on democracy is the high-resolution information. Democracy government cannot avoid the wrong choices of public servants. Not every citizen in the city is aware of the city's political, economic and social circumstances. People may vote for a proposal based on other factors rather than its potential effect. IoT devices that are spread all over the city collect unbiased data about every aspect of the city, including the traffic situation, the road status, the water quality and etc. The collected data is published on blockchain and can reveal important factors about the circumstances of the city by adopting big-data analysis tools. When governments want to increase budget, say on municipal construction, citizens have extra facts to judge whether it's reasonable or not. During the election, citizens can turn to the quantized effect of their past work and choose the one with the critical capability, instead of listening to their debates and watching their immoral practices like tarnishing their opponent's reputation on the Internet. The intelligent devices themselves may also have a fair weight in voting. Since they monitor the runtime of city continuously, they are more knowledgeable of the city than citizens. They are also neutral inherently because they are controlled by smart contracts which are feasible only after being agreed by the majority of the network. As a result, their opinion provides great hints for making the right choice. Including them in the democratic system is not impossible in the future. At this point, E-democracy does include e-lives as its name implies.

17.7 Summary

In this survey, we investigate a novel technology named blockchain. We first explain the mechanism of blockchain which enables untrusted parties to do business with each other in a decentralized way. We then use concrete examples to explain the powerful applications of blockchain in Internet of Things, E-governance, and E-democracy. When introducing these examples, we focus on two aspects of blockchain:

1. *Automation*: by using smart contract, devices become self-serving and thus more intelligent. For governments, routine work can also be processed automatically, thus enable governments to provide services more efficiently. Less human intervention in the entire process also lowers the cost.
2. *Security*: one user being hacked is minimized. Besides, every action on blockchain is recorded and transparent to every user. Under such mass surveillance, conducting malicious behaviors without being detected is not possible.

References

1. Nakamoto S (2009) Bitcoin: a peer-to-peer electronic cash system. http://www.bitcoin.org/bitcoin.pdfhttp://www.bitcoin.org/bitcoin.pdf
2. Wood G (2016) Smart contract yellow paper
3. BitcoinWiki (2016) Transaction. https://en.bitcoin.it/wiki/Transaction
4. BitcoinWiki (2016) Block. https://en.bitcoin.it/wiki/Block
5. Croman K, Decker C, Eyal I, Gencer AE (2016) On scaling decentralized blockchains. Bitcoin and Blockchain
6. BitcoinWiki (2016) Contract. https://en.bitcoin.it/wiki/Contract
7. BitcoinWiki (2014) Oracle. https://en.bitcoin.it/wiki/Oracle
8. BitcoinWiki (2016) Property. https://en.bitcoin.it/wiki/Smart Property

9. SmartLog (2016) https://smartlog.kinno.fi/
10. Brody P, Pureswaran V (2014) Device democracy: saving the future of the internet of things. IBM
11. Maxim O (2016) How blockchain relates to artificial intelligence?—BICA Labs. https://medium.com/bica-labs/how-blockchain-relates-to-artificial-intelligence-f0111f39afc9
12. Worner D, Bomhard T (2014) When your sensor earns money: exchanging data for cash with Bitcoin. Exchanging data for cash with Bitcoin, ACM, New York, USA
13. Businessweek B (2016) Inside Chipotle's contamination crisis. http://www.bloomberg.com/features/2015-chipotle-food-safety-crisis/
14. Langman CB (2009) Melamine, powdered milk, and nephrolithiasis in Chinese infants. N Engl J Med 360(11):1139–1141
15. IBM (2016) How blockchain can help bring safer food to China. https://www-03.ibm.com/press/us/en/pressrelease/50816.wss
16. Carlo M (2016) Blockchain, financial regulatory reporting and challenges. https://www.finextra.com/blogposting/13102/blockchain-financial-regulatory-reporting-and-challenges
17. Zyskind G, Nathan O, Pentland A (2015) Enigma: decentralized computation platform with guaranteed privacy. arXiv preprint arXiv:150603471
18. Gentry C (2009) A fully homomorphic encryption scheme. Ph.D. thesis, Stanford University
19. BlockCypher (2016) blockcypher.com. https://www.blockcypher.com/
20. Watchdog (2014) http://watchdog.wpengine.netdna-cdn.com/wp-content/blogs.dir/1/files/2014/06/CrossStateCheckStatistics.pdf
21. Feldman AJ, Halderman JA, Felten EW (2006) Security analysis of the diebold Accuvote-Ts voting machine
22. BitCongress (2016) www.bitcongress.com. http://www.bitcongress.com/
23. AgoraVoting (2016) agoravoting.com. https://agoravoting.com/
24. FollowMyVote (2016) https://followmyvote.com/