Peer-to-Peer Netw. Appl. (2017) 10:983–994
DOI 10.1007/s12083-016-0456-1

The IoT electric business model: Using blockchain technology for the internet of things

Yu Zhang[1] · **Jiangtao Wen**[1]

Received: 21 September 2015 / Accepted: 16 March 2016 / Published online: 13 April 2016

Abstract Nowadays, the development of traditional business models become more and more mature that people use them to guide various kinds of E-business activities. Internet of things (IoT), being an innovative revolution over the Internet, becomes a new platform for E-business. However, old business models could hardly fit for the E-business on the IoT. In this article, we 1) propose an IoT E-business model, which is specially designed for the IoT E-business; 2) redesign many elements in traditional E-business models; 3) realize the transaction of smart property and paid data on the IoT with the help of P2P trade based on the Blockchain and smart contract. We also experiment our design and make a comprehensive discuss.

Keywords Internet of things · Bitcoin · Blockchain · P2P trade

1 Introduction

Internet of things (IoT) is a worldwide network of interconnected objects and human beings, which through unique addressing schemes are able to interact with each other and cooperate with their neighbors to reach common goals [1]. The primary purpose of IoT is to share information of objects, which reflects the manufacture, transportation, consumption and other details of people's life [2]. Using the information in the IoT could make the environment around us better cognitive. But the development of the IoT is still slowly these years. One important reason is that the high costs of the deployment. This paper argues that the connection of devices all over the world and open access to these data can solve this problem. But some of these data are not for free. As a result, people need a convenient, safe and stable transaction system to exchange information and money. Traditional E-business can partly solve this problem. Because E-business development is mature in both theory and implement on the Internet, which is becoming one of the most important E-business models all round the word. But if we duplicate the entire model of E-business of Internet on the IoT, this will lead to many problems. Because IoT is a world where physical objects as well as human beings are seamlessly integrated into the information network, and both human being and physical substances are active participants in E-business process [3]. Since there is a third party in traditional E-business model, IoT cannot give full play to its advantages (e.g. M2M, P2P and M2P). Besides, Bucherer and Uckelmann stress that information exchange between physical entities; human beings and the involvement of all stakeholders in the "win-win" information exchange are the major issue in the designation of the IoT E-business model [4]. Therefore, the traditional cost-centric approach has to be replaced by a value-focused perspective from the view of both business point and giving the full potential of IoT.

Currently, the exchange of paid information can't get rid of the third party. For instance, a developer wants to get the sensor data of a region. First, he needs to buy an account from a company via traditional E-commerce. Then, the sensor data company will send the developer some data or API access authority after they receive the money. Because of the existence of the payment, much labor power has

✉ Yu Zhang
yuzhangiot@gmail.com

Jiangtao Wen
jiangtao.wen@gmail.com

[1] Tsinghua University, Beijing, China

been involved as the third party. As a result, the cost has been increased while accompanied with reduced efficiency. Besides the exchange of data, there are many services that need be achieved without the involvement of the third party (e.g. energy transaction, smart property). The emergence of the bitcoin make it possible to pay or get money through P2P payment without the intervention of the third party. It is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly without a trusted third party [5]. Participates can deal with each other easily, quickly and safely without know whether there is a people or a robot. Since bitcoin is an open-source currency platform and the technological bar is not high, many cryptographic coins are published after bitcoin in order to grab a slice of the crypto currency Market. For example, XRP is a crypto coin that circulates in Ripple (i.e. an open payment network). The biggest advantage of XRP coin is its function to trade with real currency in the world (e.g. U.S. dollar, pound and euro). But neither bitcoin nor other crypto coins are the replacement of the traditional currency. They cannot fulfill the payment of the paid data or smart property in IoT. However, its central message–decentered currency and Blockchain–has important reference value. Colorcoin and mastercoin are the typical second-generation crypto coins that are based on the protocol of the bitcoin and Blockchain. They are both senior intelligence assets protocol architecture that can set up trades designed for stock, futures, virtual currency, third-party custody and smart property and they are completely decentered. Though colorcoin and mastercoin have realized the transaction of smart property and financial products where they have the edge, they do not have the corresponding function and optimization for the trading of paid information in the IoT.

Motivate by such challenges, we propose an E-business architecture designed specifically for IoT, which are base on the protocol of the bitcoin. To begin with, we adopt distributed autonomous corporations (DACs) as the transaction entity to deal with the paid data and smart property. DACs can offer paid services without any human involvement under the control of an incorruptible set of business rules. These rules are implemented as publicly auditable open source software distributed across the computers of their stakeholders. In our E-commerce architecture, people can trade with DACs to obtain IoT coins through P2M. The IoT coin is a new generation crypto coin, which is base on the protocol of Bitcoin and Blockchain. People can use it and smart contract to exchange the paid data or smart property. Through this mechanism, people can buy paid sensor data or smart property rapidly through outright crypto monetary transactions without the involvement of third parties. Any people who owns IoT coins can also make deal with other people through P2P way like DACs. What is more, this E-business architecture is better suited to the IoT because of its following features:

Systematic Fundamental elements and operating modes of the traditional E-commerce are taken as the reference to IoT E-commerce system, which also have been modified and optimized according to the feature of IoT that make them not only possess the integrity of the traditional E-commerce model, but also well suit to the IoT.

High efficiency Since the transaction removes the involvement of the third party and can proceed in Low-trust condition, the amount of time spent is clearly decreased while the efficiency is clear increased.

Flexible In theory, we can deploy a DAC for each device or sensor to trade data or smart property, which enables them to become the provider of IoT commodities. Besides, they could also act as the buyer of the data or smart property that they can buy paid data or smart properties according to their needs. For example, a camera sensor can earn bitcoin by selling its video data, then using these bitcoins to buy power and other required materials to maintain the whole system running effectively and efficiently.

Reasonable Since each DAC can operate independently, the price of commodities is basically adjusted by the market. Besides, its pattern completely complies with market rules.

Low cost The new E-commerce system use DACs to manage the exchange and supply of the paid data and services, and using decentralized IoT coins as the medium of trade which remove the participate of the third party. People can buy paid data from even a single sensor directly. As a result, the high cost of the labour has been reduced. What is more, the possibility of actions such as intentionally manipulating the currency price, closing the account and counterfeiting have been eliminated.

As depicted above, the IoT E-commerce system is built according to the following lines. Firstly, since the IoT E-commerce system is based on the mature traditional E-commerce on the Internet, we have to make a systematic analysis of the conventional electronic business. Secondly, in order to modify and optimize each part according to features of the IoT, all devices and physical entities would offer their functionalities and data as web services, and device integration would mean service integration [6]. Besides, we use layered approach to reduce the complexity of the system. The function of each layer is specified while adjacent layers are independent from each other so that they can be replaced without interactions. In another word, we use modular approach and layer method to manage the data and

service of the new model. Finally, we dissect the protocol of the bitcoin, Blockchain and encryption algorithm that are the basic elements in the prototype of the IoT E-business model. The reminder of this paper is structured as follows. In Section 2, we introduce the background of business models and related work of decentralized company business structure. Section 3 presents the design and implement of IoT-based E-business models with a robust framework. Section 4 presents the conclusion.

2 Previous work

At present, the business model is still a relatively new concept, and it has been predominantly created in market during the last decades of the 20th century. Along with the practical effects become more and more strong, it receives more and more attention from the field of science research. As a result, many business models such as characterization, practical and perspectives are proposed and put into practice. However, there is no unique definition for the business model. For the traditional business system, business model is the substitute or implementation of the traditional business analytical process [7]. As a series of new technology have been emerged, especially the coming out of the E-business system, they have complete reversed all frameworks and theories of the traditional business model [8]. In the early research, business model was classified and defined in the E-business. For example, the author in [10] systematically analyses the traditional business models and constructs a set of business model according to features of Internet to make sure the model is fit for the E-business context. The research focus then moved on to use components method to define each constituent part of the business model. [11] suggests that the value creation potential of E-business hinges on four interdependent dimensions (e.g. efficiency, complementary, lock-in, and novelty). The business model in [12] is composed of four main pillars: they are Product Innovation, Infrastructure Management, Customer Relationship and Financial Aspects. However, with the rise of new technologies and the change of market requires, some researches in scientific field focus on how to innovate on the base of the traditional E-business model. For instance, [13] emphasizes the importance of trial-and-error learning for business model innovation. Zott and Amit in [14] propose a business model that specializes in product market strategy. And in [15] they conceptualize a firm's business model as a system of related activities that transcends the focal firm and spans its boundaries. They also divide all business model elements into two categories: design elements (i.e. content, structure and governance) and design themes (i.e. novelty, lock-in, complementarities and efficiency). In [16] the author designs a set of business models that dedicated to media industry. Although these researches and experiments work well in the Internet Environment, in the IoT and the context of robust and profitable network, the traditional models may no longer be appropriate. Therefore, it is very important to design a more specialized business model [18].

In order to design the IoT E-business model, we have to take account of architectures and features of existing business models. Besides, complex commercial processes of IoT companies can be further abstracted through reducing trivial factors and minor relationships. In [17] the author proposed two important factors in IoT E-business process. They are the track function of real-world entities and the introspection capability. The former opens up all elements in business model being tracked, and latter enables every entity being self-conscious by sensors, actuators and automatic programs. As a result, the transaction can be accomplished rapidly without the interference of human beings. But he did not mention about the specific method. [19] presents a framework describing the core parts of a network business model, which can be applied in developing business model scenarios for technology-based services. In [9] the author proposed a game base services price decision(GSPD) model to depict the progress of price decision between service organizers(SOs) and entities. In 2009, Osterwalder and Pigneur in [20] proposed a framework that is known as "business model canvas", and then Bucherer and Uckelmann combined features of IoT based on this framework in [4]. They then innovatively analyzed the business model canvas by integrating physical entities, IoT devices and big data into 4 big blocks (i.e. infrastructure, value proposition, customer and financial). What's more, they give solutions to each block corresponding to IoT. But they don't propose a new business model.

These studies mentioned above are just baby steps of the combination of the IoT and traditional business model, and they propose some improved models that have some efficiency and rationality. But these studies cannot get rid of the traditional business process. They are just the improvement of the traditional business model. Without the bran-new models designed especially for the condition of the IoT, the potential of the E-business on the IoT cannot be fully reached. Therefore, our work is a worthy exploration.

3 The architecture of e-business model based on internet of things

3.1 Decentralized autonomous corporations

Bucherer and Uckelmann stress that rapid information exchange between participates that all of them can benefit

from this progress are key issues in designing IoT E-business models [4]. Besides, after the IoT has already developed to a mature stage, single function or the combination of functions can integrate into modular services. In another word, physical entities and devices on the IoT can serve as services provide companies like human beings. Based on above analysis, we use modularized method to analyze the IoT E-business model, and propose a new IoT E-business model, which is composed of decentralized autonomous corporations (DACs).

DACs are new breed of corporations that act and behave, for all practical purposes, just like regular corporations. But at first, they are decentralized and owned by nobody. Although people can get profits from DACs, this is only part of its stake mechanisms and has nothing to do with its decentralized nature. The second point is the nature of its automation. The biggest difference between the DAC and the traditional company is that the DAC can make decision itself rather than people.It is also an advantage that we apply the concept of the DAC to the IoT. We can set a serious of basic rules to a device and use machine learning methods to make it automatically in the IoT business. Last but not least, as an independent economy entity, the most distinctive difference between it and the traditional software is that it contains some kind of internal property that is valuable in some way. And its stock mechanism allow sharing its merits to stock owners. DACs are next generation of corporations and crypto coins (e.g. bitcoin) are the only way to deal with those corporations.

Bitcoin is a user autonomous, encrypted electronic digital currency [4]. Since bitcoin is not issued by any nations or organizations, there is no need for bitcoin users to worry about their accounts being closed or the currency depreciation that is caused by over printed money of the nation. Monitoring by everyone is one of its mechanisms that is realized by the Blockchain. All transaction records are encoded in this unique Blockchain. Besides, users all over the Internet have a copy of the Blockchain, you can not falsify transaction records or account balances unless your processing power overtake 51 % of the whole network processing power. The advent of bitcoin creates the era of the decentralization. But bitcoin is not just a currency, but also a protocol, a network and a transaction language [4]. Therefore, the theory and technology of the bitcoin is the base of the DACs theory.

In this paper, we have proposed a new mechanism, which would apply the concept of DACs on the IoT. To be specific, we take a server that have abilities of storage, compute, distribution and a fixed IP address as a DAC. Firstly, owners have to set rules to it. For example, how to purchase data from sensors? What type of data should it buy? How to process the raw data to product? How much is the product? After these settings, this DAC can be fully automated and without any one's interference. Like the BitTorrent and Skype, all DACs in IoT have to follow the same protocol and use bitcoin in the trade. Besides, the transaction is guaranteed by smart contract, which will be illustrated in Section 3.2.4.

3.2 The architecture of IoT E-business model

3.2.1 IoT E-business model

IoT E-business is different from traditional E-business. Most traditional E-business models focus on customer relationship, products innovation, infrastructure management and financial aspects. But the principle and transaction mode of the IoT E-business are completely different from the traditional one. As a result, we have to start with the most basic elements of the business process and construct models in the IoT E-business. As shown in Fig. 1, there are 4 modules of the IoT E-business model. They are entities, commodities, basic Operating modes and transaction modes.

Entities and commodities are the infrastructure of the IoT E-business model. Entities are consisted of DACs (introduced in Section 3.1) and human beings. These IoT entities are not just the provider of the IoT commodity; they also could search and purchase IoT products according to certain conditions automatically. Owing to the difference between traditional E-business modes, IoT products do not include some traditional commodities but sensor data and smart properties. Sensor data also include data processed by human beings or DACs, not just the raw data collected by sensors. Smart properties consist of car, house and parking spaces, which can be controlled by electronic locks or access control systems. Besides, energy properties (e.g. electricity, water, gas and oil) that can be controlled and

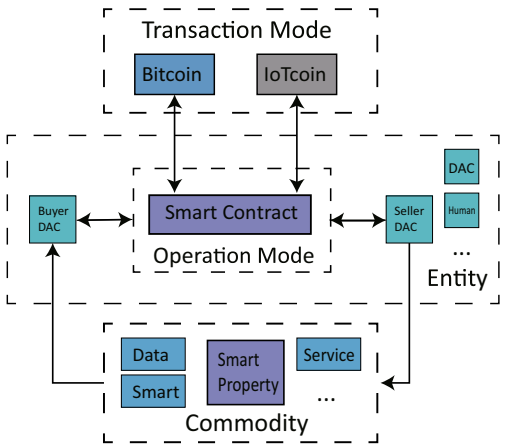

Fig. 1 The architecture of IoT E-business

quantified by digital devices can also be listed into the field of smart property.

Operating mode is the guideline of the IoT E-business process. All stages that from pre-transaction to contract fulfillment have to be redesigned to fit for the new application. What's more, the design and the signature of the smart contract are accomplished in this stage. Smart contract is an important guarantee of the IoT E-business transaction that every trade detail will reflect on it. What's more, signatures, timestamps and series numbers of both sides are recorded on the smart contract. Besides, unilateral entity cannot cancel the transaction after this contract was signed by both sides and broadcast to the entire network. The transfer of the encrypted money and IoT commodities are according to the content of the smart contract.

Transaction modes are the core of the IoT E-business system. The system can complete the P2P deal without the help of any other third party on the IoT. We adopt bitcoin as the currency and IoTcoin as the IoT commodity exchange certificates. Bitcoin is a decentralized crypto currency, which uses the encrypted token to store and transfer itself, the point to point network to carry information, the synchrodata hashing method to prevent double pay, and an powerful script processing system to judge the ownership of the token. The IoT coin is a special crypto coin, in addition to some bitcoin features, it support agent or aggregate point to ensure that its value is irrelevant with bitcoin value. Therefore, it can act as the IoT commodity exchange certificates and exchange by decentralized P2P mode, which is difficult to achieve by traditional financial methods.

We create the IoTcoin is because it is just another medium of payment. Although the decentralization makes a lot of possibilities, they are limited in the process of the payment. When a people use bitcoin to buy some traditional commodities, a third party is ineluctably involved to make sure the money is safe before the commodity is arrive. However, there is no third party in the architecture of the IoT E-business model. Therefore, we need to introduce a P2P transaction mechanism, which is compatible with bitcoin. In this P2P trade, people can get the commodity while pay out the bitcoin.

The primary role of the IoTcoin is act as the title of the smart properties ownership or stakes of a DAC. An example of the formal could be the smart car. The smart car will issue a non-reissuable IoTcoin and publish it into Blockchain, let's call it the carcoin. Then the owner of carcoin is universally regarded as the car owner. In the latter case, IoTcoin is act as the stake of the DAC. Three people (i.e. A, B and C) hold stakes of a DAC, which can sell data to earn money. This DAC will issue some reissuable IoTcoins at its first initialization. Let's call it stakecoin. Like the dividend of the company, A, B and C will get bonuses from this DAC according to their stakecoin's quantity. But this DAC will act automatically to deal with the business in IoT E-business. None of the stockholder can control it unless there is a predefined function that will accept the consensus of stockholders.

Unlike traditional E-business, there is no third party in IoT E-business. Therefore, we need a mechanism to ensure the security and effectiveness of the bitcoin and the IoTcoin. The blockchain can fulfill these requirements, and the mandatory and reliability of this mechanism is list as follows:

- Electronic signature. Since the private key is impossible to fake, the identity of participates can be verified if he signed his private key on the contract.
- Point to point network. Similar to BitTorrent and TCP/IP, IoT E-business network cannot be destroyed because it can operate without the support of a powerful central organization.
- Proof-of-Work. It can prevent users from double-spend. And the effectiveness of the transaction can be verified without a central organization.
- Distributed ledger. Every bitcoin wallet contains the backup of the transaction records of the whole network. Blockchain mechanism means that everyone can examine the existence of a certain transaction and verify the effectiveness of it.
- Hashing algorithm. Every transaction is encrypted by hashing algorithm and adds to the bottom of the latest Blockchain in real time. If a hacker want to cancel or modify a transaction, he need to decrypt the Blockchain to rollback it while the whole network are continually adding new Blockchain. In another word, he must offer more than 51 % computer power of the whole network. It is almost impossible because the bitcoin network has developed to such a large scale.

3.2.2 Entities of the IoT E-business model

As shown in Fig. 2a, traditional business entities include customers, companies and governments. Customers are known as users that are in the dominant position in business activities. Their consumption behaviors consist of demand, purchasable motivation and purchase. Companies have many advance features. For example, their organizational structure, customer demand and scientific decision-making system make them become the most flexible and expandable business entity. In business activities, on the one side, companies are in charge of manufacturing and marketing commodities as manufacturers. On the other side, they have to purchase materials, components, parts and similar goods from other companies as customers. Government's regulation happens in the advanced market economy,

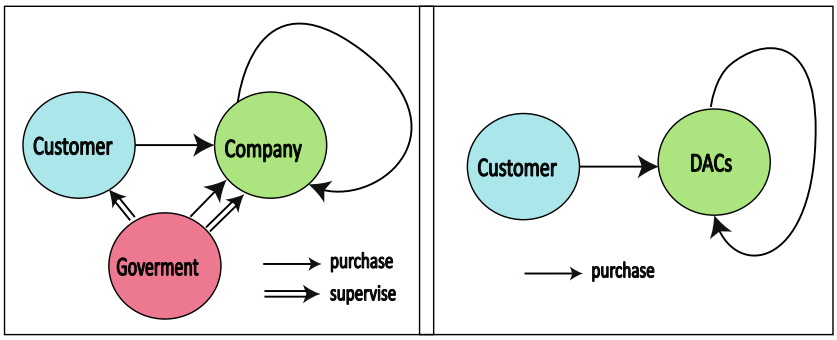

Fig. 2 Business entities. **a** Traditional E-business entities; **b** IoT E-business entities.

especially under the condition of modern market economy. Not only do they have the economy organization and management function but also can participate business activities. Therefore, the government is the senior customer who can participate the business activities directly as a customer (i.e. government purchase) besides the market management function.

As shown in Fig. 2b, there are two business entities in IoT E-business model: DACs and customer. On the one side, DACs can issue IoT data as commodities on the IoT. For instance, a PM2.5 DAC can produce the air quality data and then public the information of these data so as to sell them on the IoT E-business platform. On the other side, DAC have to purchase sensor data or other IoT products to maintain the daily operation. For example, a DAC has to buy power from a power station agent DAC using bitcoins automatically when it is short of power. In the IoT E-business model, any other third parties including the government cannot manipulate the market or DACs. All DACs run automatically without the interference of human being. Its code and regulation are open-source and transparent to everyone. There are no human beings or DACs are willing to make deal with close sourced DACs whose regulations are inconsistent with the standard. Therefore, any malicious modification of the DACs' regulation or non-standard DACs are actually invalidate in the IoT E-business model.

3.2.3 Commodities of the IoT E-business model

There are two classes of the commodities on the IoT: paid data and smart property (Digital controlled energy is also included in the smart property class). They share many common features. For example, they can be transmitted directly on the network or controlled by digital devices. Besides, because there are no traditional stages such as storage or logistics, customers can get their commodities or keys immediately while the deal was complete. Although physical entities are related to smart property and energy property, the shift of the ownership can be realized by the token transmission or the digital control.

Paid data Paid data is the major commodity in the IoT E-business. There are currently some data transactions on the Internet. For instance, some website can provide paid data through their API, which is charged according to access times. However, the type and quantity of this pattern is very limited that the advantage of the IoT's huge number devices connection played no part at all. In this paper, we use DAC as the basic unit to provide paid data. A DAC can be understood as a set of devices, which have enough CPU, memory, storage, bandwidth and at least one static IP address. The owner of it has to set some rules to make it run automatically. These rules include what data it should provide as the commodity? How much it should charge for its commodities? How to buy the raw data and energies to maintain its daily running?

Operating rules of the DAC is completely open and transparent, which means the details of the paid data (i.e. the type of data, sampling rate, accuracy, location and other information), price and buying pattern are open to everyone. Like the vending machine, if the user approves its exchange rules, he will get the commodity after paying the bill. Because owners of the DAC set rules for it, they are in charge of the commodities. But once the rule is set up, the owner's can't modify it.

The value of paid data is hard to evaluate. The cost of paid data comes from the process of collection, storage, distribute etc. Although hardware and software involved in these stages are easy to calculate, the true value of data is hard to evaluate. Because the value of the paid data is depend on how much benefits customers could get. In another word, the values of the information that are processed from the same raw data but two purposes are totally different. As a result, the value of the paid data should be judged by the market discipline.

Smart property The essential of the smart property is using the smart contact to control the ownership of assets on the base of Blockchain. Examples include physical property (e.g. car, parking space and house), non-physical property (e.g. stakes of the DACs) and energies (e.g. power, oil and gas) that can be controlled by digital devices. The

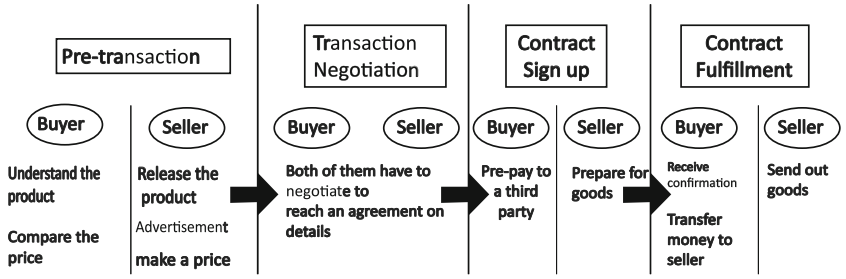

Fig. 3 Operating mode of traditional business

advantage of the smart property is that they can minimize fraud and intermediary costs; in addition to complete some transactions that are unlikely to happened in low trust scenarios.

In fact, there are currently many prototypes of smart property, such as cars with anti theft system that their physical keys are equipped with improved anti theft system to make sure that only the right key can start the engine. Besides, some smart phones use password login system to ensure only the right user with the right key can unlock the device. However, the potential of the smart property are far from being fully developed. In the above example, the private key is usually kept in a physical container (e.g. a car key or a SIM card), which is hard to transfer or control. The Blockchain have changed this situation that the transformation of the smart property ownership can be accomplished on the network.

In practical, the ownership of the smart property may be reflected in the process of unlocking the controller (e.g. the door lock, the car lock, the water meter and electric meter). Traditional keys such as the electric car key or a single RFID/NFC card cannot change the ownership or usage permission in real time. In IoT E-business model, we can use mobile devices equipped with NFC module as the carrier, and use APP based on Blockchain to realize the transfer of ownership or usage permission. Finally, the owner can control smart properties by mobile devices equipped with the NFC module and specified APP.

3.2.4 The operating mode of IoT E-business

As Fig. 3 shows, there are 4 stages in the traditional business operation mode. They are pre-transaction preparation stage, transaction negotiations stage, contract sign up and formalities stage, the fulfillment of the contract and payment stage. In this sub section, we propose the operation mode of IoT E-business after analyzing the traditional one and make a comparison between them.

Pre-transaction preparation stage This stage includes the preparation of all participates in the transaction. In the traditional business, buyers have to prepare money, make plan for purchasing, make market investigation and analysis over and over again, learn different types, quantity, specification, price and transaction modes of commodities. Sellers have to hold news conference of their commodities and advertising them. In addition, they have to conduct a comprehensive market investigation and produce various sales strategies so as to understand the buyer's market. Other participates such as intermediary (e.g. Paypal), bank financial institute, credit card company, customs system, insurance company and transport company also have to get prepared for the corresponding trade.

Since the transaction mode is decentered in IoT E-business model, it doesn't need the participation of bank and financial institute. The pre-transaction preparation stage in IoT E-business only includes preparation works of both buyer and seller. On the one side, the sellers have to advertise their goods. More specifically, they make the specific information, legal provisions, price and type of the commodities (e.g. paid data and smart property) public on the IoT E-business network. On the other side, buyers can search for the commodity on this network and make a comparison to find what they need. Or they can get the certain commodity by inputting filter criteria. Finally, they will find out the needed commodity and start a transaction.

Negotiation stage The negotiation stage starts just after both seller and buyer understand their needed information about commodities. In the traditional E-business, once the seller and the buyer reach an agreement through negotiations and consultations, they use electronic contract to write down detailed instructions such as rights, obligation, commodity's information and claim etc.

Traditional negotiation method is not fit for the IoT E-business model because both buyer and seller could be DACs. As a result, there are 4 situations as shown in Fig. 4.

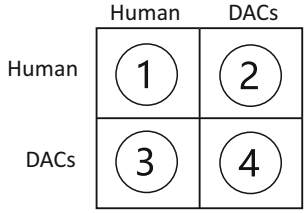

Fig. 4 Negotiation model of IoT E-business

- When both seller and buyer are human beings. The negotiation method is similar to the traditional one. That is to say, all participates of the transaction can communicate on the details of the commodity.
- When the buyer is human being and the seller is DAC. The buyer can get needed commodity through browsing on the IoT or filtering by certain criteria. Then he can find a DAC who will provide him a smart contract. All the details of the commodity and legal provisions are listed on that smart contact. In another word, the buyer cannot communicate with the seller to change the details and price of the commodity. If the buyer do not content with the product, they can change to other DACs.
- When the buyer is DAC and the seller is human being. The buyer will pick up needed commodities on the IoT information platform automatically according to some algorithms and certain criteria. For example, a traffic congestion information provider DAC needs many information sources such as the pressure data of the road, the video from surveillance camera and the speed data from buses and taxis. The DAC will purchase one or more information sources automatically according to the calculation result that take into account of its own product specifications and budget data etc. With these data, the DAC could create the traffic congestion information and issue them to the IoT information platform as an IoT commodity. The seller (i.e. human beings) do not have to communicate with buyer, but to issue the information of their own IoT products on the IoT and sign the smart contract in advance.
- When both buyer and seller are DACs. The situation is very similar to the 3rd one. Both buyer and seller are in accordance with certain rules automatically, and the market mechanism becomes an important way to adjust supply and demand of IoT E-business market. In another word, the more competitive of the commodity, the more demand of the market. Both buyer and seller do not have to waste time and energy to negotiate on details of the product. They just have to sign the smart contract if they come to a consensus.

Contract signing stage Contracts are signed by electronic data interchange (EDI) in traditional E-business, and digital signature is used to guarantee the legal effect. Other insurance measures include negotiation logs and files. This electronic evidence can be used to arbitrate the legal dispute in the transaction. But these evidences have to be kept in a server that is managed by a third party.

Because there is no third party in IoT E-business model, the traditional way wouldn't work. In this paper, we propose a decentralized smart contract to solve the problem. On the one side, the key feature of smart contracts is that it is a decentralized system accessible to anyone, that doesn't require any intermediary party. On the other hand, they are computer programs that can automatically execute the terms of a contract. At core, these automated contracts work like any other computer program's if-then statements. In another word, when a pre-programmed condition is triggered, the smart contract executes the corresponding contractual clause.

In accordance with smart contract, we use the bitcoin as a means of payment. Because it defeats the purpose of smart contracts if a bank still has to manually authorize the release and transfer of money. The bank could control the trade from the source and thereby the execution of the smart contract will become ineffective. Yet bitcoin is itself is a computer program, smart contracts can interact with it. In another word, a computer program can trigger payments.

Because the execution of the smart contract is completely automatically, the terms and conditions in the smart contract must can be triggered. For instance, the condition could be like if the A's data meet the criterion in the smart contract? Or if the ownership of a smart car has been transferred from A to B?

Contract fulfillment stage This stage starts after both the buyer and seller have completed all the procedure of the contract. In the traditional E-business, the seller has to prepare for goods and issues such as customs, insurance, evidence and credit. After that, they deliver their goods to transport company to complete rest tasks such as packing, shipping and transportation. The buyer has to send their money to the seller through banks and other financial institutes after confirming these goods. Or they can notify the third party to send their money to the seller. Then the seller will issue the certifications and tickets after they affirm the money is transferred. After that, the whole transaction is complete.

Traditional contracts have no effect in IoT E-business model. Since DACs is autonomous and there are no specific groups or individual will act as third party. Although the smart contract can trigger events according to certain terms automatically, there are no third party to storage them. Even if these smart contracts are kept by some organizations, there is no guarantee that the content of them will not be modified or delete by someone. Therefore, we need to publish the smart contract into the Blockchain.

As stated in Section 3.2.1, smart contract that based on the Blockchain is verifiable (i.e. Every transaction can be found in the Blockchain), safe storage, impossible to fake and can be used to many aspects in the IoT E-business. Besides, the seller can create a smart contract in advance, which will be published on the Blockchain with a time stamp. As a result, everyone in the network can accept this contract within specified time. If both sides sign the smart

contract with the private key, it will become undeniable. The whole processes are without the involvement of the third party.

As shown in Fig. 5, based on the analysis of traditional business operation mode and differences with IoT E-business, we propose the operation mode of IoT E-business. The 1st stage and the 2nd stage of he traditional business are merged into pre-transaction stage. In this stage, both of the buyer and seller communicate through the IoT information platform, which can analyze, rank and filter IoT commodity information according to certain algorithms and rules. Then it will offer the result to the buyer. The 3rd stage and the 4th stage are merged into transaction stage. In this stage, both sides of the transaction will sign their private key on a smart contract if they come to a consensus. What's more, P2P exchange will complete at the same time. Features of the smart contract guarantee the effectiveness of the transaction.

3.2.5 The transaction mode of IoT E-business

The transaction mode of traditional E-business is the digitization of the financial and monetary to make them circulate on the network. The advantage of IoT E-business model is its decentered feature, which separate it from the control and influence of traditional financial institutes. However, the trade between bitcoin and commodities is currently relying on the third party platform that the potential of the decentered feature cannot be fully reached. Since the trade between currency and commodities is real time and automatic in the IoT E-business model, the it must totally decentered. Therefore, we designed the IoTcoin, which can derive the monetary value from bitcoin network technically so as to achieve P2P trade of the IoT E-business. What's more, IoTcoins are specially designed to fit for the transaction of IoT commodities, especially for DACs and the smart property.

There are two transaction styles in IoT E-business. One is the payment, the other is the exchange. The formal one can be applied to the purchase of the commodities and services on the IoT. For example, one people want to buy commodities from a DAC. He has to sign the smart contract with this DAC and pay bitcoins to it. The latter one can be applied to the transaction of smart property. To take an example, B want to buy a car from A. Firstly, they have to draft a smart contract, which contain the exact terms of the transaction such as how many bitcoins should be paid by B to exchange one IoTcoin. Secondly, both sides confirm this contract and publish it into the Blockchain. At last, the contract will take effect and both sides will get what they need.

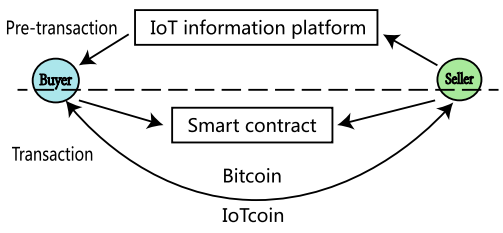

Fig. 5 Operating mode of IoT E-business

3.3 Case study

3.3.1 The workflow of DAC

DAC is the most basic element in the IoT E-business framework. On the one side, it makes deal with sensors and small devices to buy the raw data. On the other side, it processes the raw data into the valuable information and sells them to people and other DACs. And according to the pre-defined rules, some of profits are used to maintain its day-to-day running, others are send to stockholders according to the percentage of the stake. But the stockholder can not affect the behavior of the DAC. They are totally decentralised. The sequence of the DAC workflow is as follows:

- Firstly, the owner of the DAC have to program it through writing code that, at least given predictable environments (e.g. Buy raw data, buy energy, process raw data, sell data etc.), takes a given input and calculates a desired action to take.
- As the framework is decentralized, there is no center server to place the code. And because if the code simply exists as a computer program on some particular machine, the owner of that machine may shut the whole thing down, or even modify its code to make it send all of its money to himself. In order to make the DAC trustable, its code must run complete independently and without any inference. To be specific, we have to split up DAC's code by using an algorithm called Shamir's Secret Sharing, and a piece of the code is given to each participant. In practical, we can put the code and data on the maidsafe, which is a decentralized AWS.
- Once a DAC was started, it has to create a serious of smart contract. In the first place, it has to sign smart contracts with sensors and small devices to buy raw data. Then it processed these raw data according to the preset code and made products for other DACs and people. At last, this DAC can publish the information of these products and signed smart contracts with customers. Contract to the code of the DAC, these smart contract can't put on maidsafe. Because all contents of the contract must be transparent to others. As a result, we use ethereum to realize the smart contract. Codes of major functions are shown in Algorithm 1. First, the smart contract will check whether the DAC has paid

enough money. If the check if pass, these money will be hosted by the smart contract. Second, the smart contract automatically calls a function to fetch the data from sensors. Third, it checks the validity of the data. Only after the checking is passed, the contract will send the data to the DAC and send the hosted money to sensors. If there is no data or the data checking if failed, the contract will send the hosted money and error information back to the DAC.

– Some of the merit will be sent to owners according to the percentage of the stake, others will used to maintain its daily expenses. The operation rules can be modified only if the majority of stockholders reached a consensus.

Algorithm 1 Smart contract: BuyRawData

```
1:  function BuyAll(id)
2:      if msg.value >= 20 then
3:          data = fetchDataFromSensor(dataUrl)
4:      if data exist and data is valid then
5:          send value to seller's wallet
6:          return data
7:      else
8:          send value to buyer's wallet
9:          return "Data is invalid"
10:     end if
11: end if
12: end function
```

3.3.2 The transaction of smart property

As introduced in Section 3.2.3, the prototypes of smart property are currently very common; such as cars which engine can start only by a specified key and mobiles device locked by a pin number. But these private keys usually kept in a physical container (e.g. car keys or SIM cards) that make them difficult to transfer or control. IoT E-business model changes this situation through the transaction of the smart property ownership.

The smart car is an example of such smart properties. The computer of the car can only be unlocked by the owner's private key. In the first place, there is a public key corresponding to the owner's private key that has been stored in the car. In the second place, in order to use the carcoin, which present the ownership of the car in the Blockchain like bitcoin, a little amount of bitcoin (e.g. 0.0001BTC or any bitcoins as long as it is more than the limitation of Blockchain anti-dust rules) was stored in carcoin. In addition, for the sake of offering some car related information (e.g. authenticity, age and mileage), the car needs a digital certificate. The specific transaction processes are shown in Fig. 6. There are four steps:

– The seller has to prove that the car belongs to him. As shown in figure 6a, firstly, the buyer sends a random number to the car. Secondly, the car will encrypt this number by the current owner's public key and send it to the seller. Thirdly, the seller decrypts the message by his private key and sends the random number to the buyer. If it consistent with the original one, then the ownership of the sell has been proven. In addition, the public certification of the car, the data of the car (e.g. mileage and the purchase date), car owner's public key and the latest transaction are recorded in the Blockchain. The buyer can access them freely.
– The buyer initials a trade after he accepts the seller's price. As shown in Fig. 6b, after both side reach an consensus on the deal, they can create an smart contract and publish it into the blockchain. The content of the contract includes: it will determine whether it has received enough bitcoins from the buyer and adequate carcoins from the seller within the allotted time. It these conditions are met, it will send hosted bitcoins to the seller and send hosted carcoins to the buyer. Otherwise, it will send all coins back. This paper implement the prototype of this smart contract on Ethereum, and the main function is shown in Algorithm 2.
– The update of the car. When the car deems that the ownership has been reallocated and the Blockchain of the new transaction is longer than the old one, in addition to enough tasks stack on the top of the Blockchain to make it irreversible, it will update the ownership data and Blockchain to the latest version. So far, the whole transaction is complete.

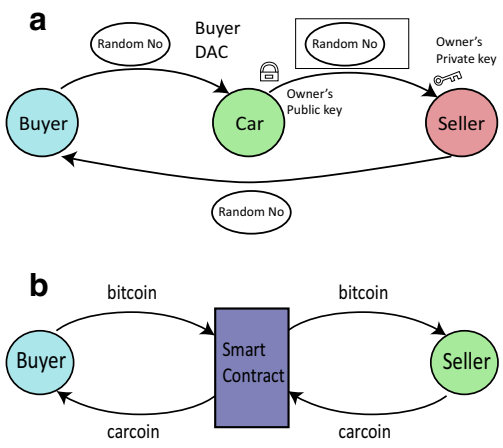

Fig. 6 The transaction of Smart property. **a** Step1; **b** Step2

– Unlock the car. The new owner of the car can use his private key to unlock the car and start the engine. In practical, this process could be designed as a smart engine that can be started by the touch of a smart device equipped with RFID/NFC module, and an APP on this device is used to store and transmit the private key. All the details of the protocol are transparent to the users.

Algorithm 2 Smart contract: CarContract

```
1: function Exchange(id)
2:     if buyer.bitcoin.amount >= 20 and
   seller.carcoin.amount >= 1 and
   (block.timestamp − startTime) < 100 then
3:         send bitcoins to seller's wallet
4:         send carcoins to buyer's wallet
5:     else
6:         send back hosted coin
7:     end if
8: end function
```

In addition to bitcoin, one type of IoTcoins can also trade with other type of IoTcoins through P2P mode. For instance, a carcoin (i.e. an IoTcoin that present the ownership of a car) can exchange 30 bitcoins or 800000 datacoins (i.e. an datacoins that can get access to temperature sensor data for one time).

4 Conclusion and future work

In this research, we have proposed a business model for the IoT. We start with the introduction of DACs and introduce it into the IoT E-business model. We also discuss details of the IoT E-business model from entity, commodity and transaction process, in which we study on the 4 stages of the traditional E-business (i.e. they are Pre-transaction preparation stage, Negotiation stage, Contract signing stage and Contract fulfillment stage.) and redivide them according to the feature of IoT E-business model. In order to achieve the complete decentralization of the IoT E-business model, we propose a P2P transaction mode on the basis Blockchain. In addition, in order to achieve the transaction of smart property and paid data, we designed a method that is base on the smart contract and encrypted coins. At the end, we designed two experiments to verify these theories of the IoT E-business model.

Just as we proposed in Section 3.2.3, there are 2 types of commodity in IoT E-business model. One is the smart property, and the other is the paid data. In the next step, on the smart property, we will develop on smart devices equipped with NFC module and try to work on apps, which can realize the exchange of the ownership and then rewrite information in NFC module so as to achieve the control over the smart property. On paid data, we will try to design the uniform data format and API, and work out the ranking mechanism and credit system. So that we will construct a IoT data exchange platform that people or DACs with sensor data can upload them according to specified format. What's more, people who need data can find required data on the platform and pay for the data provider.

References

1. Atzori L, Iera A, Morabito G (2010) The Internet of things: A survey[J]. Comput Netw 54(15):2787–2805
2. Li H, Tian Y, Liu Y, etal UAI-IOT Framework: A Method Of Uniform Interfaces to Acquire Information from Heterogeneous Enterprise Information Systems[C]//Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing. IEEE, 2013: 724–730
3. Haller S, Karnouskos S, Schroth C (2009) The internet of things in an enterprise context[M]//Future internetFIS 2008. Springer, Berlin, pp 14–28
4. Bucherer E, Uckelmann D (2011) Business models for the internet of Things[M]//Architecting the internet of things. Springer, Berlin, pp 253–277
5. Nakamoto S (2012) Bitcoin: A peer-to-peer electronic cash system[J]. Consulted 2008:1
6. Leminen S, Westerlund M, Rajahonka M, etal (2012) Towards iot ecosystems and business models[M]//Internet of things, smart spaces, and Next Generation Networking. Springer, Berlin, pp 15–26
7. Amit R, Zott C (2000) Value drivers of e-commerce business models[M] INSEAD
8. Chesbrough H, Rosenbloom RS (2002) The role of the business model in capturing value from innovation: evidence rom Xerox Corporation's technology spinoff companies[J]. Ind Corp Chang 11(3):529–555
9. Liu X, Dong M, Ota K, etal (2015) Service pricing decision in cyber-physical systems: insights from game theory. IEEE Transactions on Services Computing. doi:10.1109/TSC.2015.2449314
10. Timmers P (1998) Business models for electronic markets[J]. Electron Mark 8(2):3–8
11. Amit R, Zott C (2001) Value creation in ebusiness[J]. Strateg Manag J 22(6-7):493–520
12. Osterwalder A, Pigneur Y An e-business model ontology for modeling e-business[C]//15th Bled electronic commerce conference. Bled, Slovenia, 2002:17–19
13. Tikkanen H, Lamberg JA, Parvinen P et al. (2005) Managerial cognition, action and the business model of the firm[J]. Manag Decis 43(6):789–809
14. Zott C, Amit R (2008) The fit between product market strategy and business model: implications for firm performance[J]. Strateg Manag J 29(1):1–26
15. Zott C, Amit R (2009) Designing your future business model: An activity system perspective[J]

16. Westerlund M, Rajala R, Leminen S (2011) Insights into the dynamics of business models in the media industry[J]
17. Bohn J, Coroam V, Langheinrich M, etal (2005) Social, economic, and ethical implications of ambient intelligence and ubiquitous computing[M]//Ambient intelligence. Springer, Berlin, pp 5–29
18. Fleisch E What is the internet of things? An economic perspective[J]. Economics, Management, and Financial Markets, 2010 (2): 125-157
19. Palo T, Tahtinen J (2011) A network perspective on business models for emerging technology-based services[J]. J Bus Ind Mark 26(5):377–388
20. Osterwalder A, Pigneur Y (2010) Business model generation: a handbook for visionaries, game changers, and challengers[M] John Wiley Sons

Yu Zhang received the master degree from information and engineering university, Henan, China, in 2011. He is currently working toward the Ph.D degree in the department of computer science and technology, Tsinghua University, Beijing, China. His current research interests include Internet of things, Blockchain, and E-business.