An IoT Electric Business Model Based on the Protocol of Bitcoin

Yu Zhang, Jiangtao Wen
Department of Computer Science and Technology
Tsinghua University, Beijing, China
{yuzhang13, jtwen}@tsinghua.edu.cn

***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.**

***Index Terms*—E-business model, Internet of things, bitcoin**

I. Introduction

INTERNET of things(IoT) is a world wide 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 some of these informations are not for free. 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 and 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 can not give full play to its advantages(e.g. M2M, P2P and M2P). Besides, Bucherer and Uckelmann[4] 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. 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 involves the third party. As a result, the cost has been increased while accompanied with reduced efficiency. Besides the exchange of data, there are many businesses that can be achieved without the involvement of the third party(e.g. rent serves, smart property). The emergence of the bitcoin make it possible to pay or get money through P2P payment without the intervene 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]. People can deal with each other easily, quickly and safely without know whether there is a people or a robot. But neither bitcoin nor other crypto coins are the replacement of the traditional currency, they can not fulfill the payment of the paid information 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 which 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 commodities 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 sensor 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. IoT coin is a new generation crypto coin which is base on the protocol of Bitcoin and Blockchain. People can use keys and scripts which are obtained in them to exchange the paid sensor 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 the third party. Any people who own the IoT coin can also make deal

978-1-4799-1866-9/15/$31.00 ©2015 IEEE

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: The fundamental and operation mode of traditional E-commerce are taken as the reference of IoT E-commerce system, and they 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 the application of IoT.
- High efficiency: Since the transaction removes the involvement of the third party and it 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 through sold 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 paid data and the flow of the currency are basically adjusted by the market, and its pattern completely comply with the market rule.
- Low cost: The new E-commerce system use DACs to manage the exchange and supply of the paid data and services, and using decentered 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 labor has been reduced. What is more, the possibility of intentionally manipulating the currency price, closing the account and counterfeiting have been eliminated.

Since the IoT E-commerce system are based on the mature traditional E-commerce on the Internet, we make a systematic analysis of the conventional electronic business, in order to modify and optimize each part according to features of the IoT on which all devices and physical entities would offer their functionalities and data as web services, and device integration would mean service integration[7] which would help to realize the full potential of the IoT. Besides, we use layered approach to reduce the complexity of the system. The function of each layer is specified while the relationship between adjacent layer is independent from each other so as to be replaced without the interaction. 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 which 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 gives an experiment and section 5 present the conclusion.

II. 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 analyze process[8]. As a series of new technology have been emerged, especially the coming out of the E-business system which was operated on the Internet, they have complete reversed all frameworks and theories of the traditional business model[9]. In the early research, business model was classified and defined in the E-business. [10] suggests that the value creation potential of E-business hinges on four interdependent dimensions(e.g. efficiency, complementaries, lock-in, and novelty). The business model in [11] 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, there are some researches in scientific field that focus on how to innovate on the base of the traditional E-business model. For instance, [12]emphasizes the importance of trial-and-error learning for business model innovation. In [13] the author designs a set of business models that dedicated to media industry. Although these researchs 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[15].

In order to design the IoT E-business model, we need to fully consider architectures and features of existing business models. Besides, complex commercial process of IoT companies can be further abstracted through reducing trivial factors and minor relationships. In [14] 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 interfere of human beings. But he did not mention about the specific method. [16] 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 2009, Osterwalder and Pigneur in [17] proposed a framework which is known as business model canvas, and Bucherer and Uckelmann combined features of IoT based on this framework in [18]. They then analyzed 4 big blocks and 9 small blocks of the business model canvas innovatively 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 which get some achievement on efficiency and rationality. But these studies do not 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 can not be fully reached. Therefore, our work is a worthy exploration.

III. The Architecture of E-Business Model Based on Internet of Things

A. Decentralized Autonomous Corporations

Bucherer and Uckelmann [18] 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. 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 service provide companies like human beings. Based on above analysis, we use modularized method to analyze the IoT E-business model, and propose an 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 they are owned by nobody, and managed all by themselves. They are next generation of corporations and crypto coins(e.g. bitcoin) are the only way to deal with those corporations. Bitcoin is an user autonomous, encrypted electronic digital currency[19]. 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 which is caused by over printed money of the nation. Monitoring by everyone is one of its mechanism which is realized by the Blockchain. All transaction records are encoded in this unique Blockchain. Users would complete the transaction only by accepting it. 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 decentration. But bitcoin is not only just a currency, but also a protocol, a network and a transaction language[19]. Therefore, the theory and technology of the bitcoin is the base of the DACs theory.

B. The Architecture of IoT E-business Model

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 to analyze the IoT E-business. Basic elements of the business process include participate entities, transaction commodities, basic operation modes and transaction modes.

As shown in figure1, there are 4 layers of the IoT E-business model. They are technique basic layer, infrastructure layer, content layer and exchange layer from the bottom up.

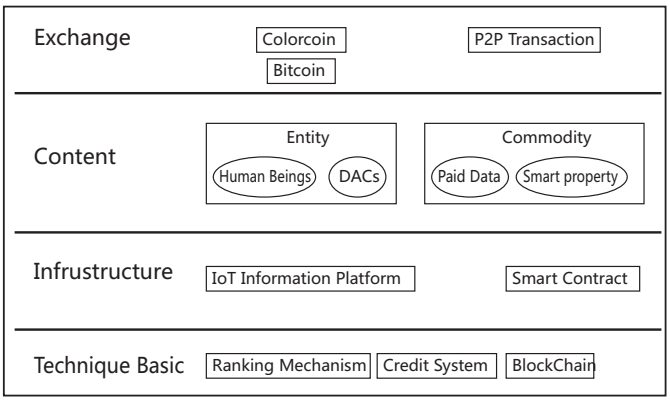


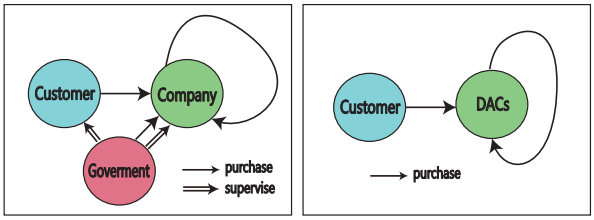
Figure 1. IoT E-business Model

Technical basic layer includes the ranking mechanism module, credit algorithm module and bitcoin Blockchain module. Infrastructure layer contains the information service platform and the smart contract system. Content layer includes two parts: participate entity and IoT commodity. Entity consist of DACs(introduced in III-A) and human beings. Smart properties consist of car, house and parking spaces which can be controlled by electronic locks or access control system. Besides, energy properties(e.g. electricity, water, gas and oil) that can be controlled and quantified by digital devices can also be listed into the field of smart property.

P2P transaction system is on the top of the whole IoT E-business model. It is also 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 IoT coin as the IoT commodity exchange certificates.

2) Entities of the IoT E-business Model: As shown in figure 2a, business entities include customer, company and government in the traditional business model. Customer is known as user who has been the dominant position in business activities. Customer's consumption behaviors consist of demand, purchasable motivation and purchase. The company has many advance features. For example, its organizational structure and customer demand are steady in addition to scientific decision-making system that make it become the most flexible and expandable business entity. The government is the advanced customer who can participate the business activities directly as a customer(i.e. government purchase) in addition to regulate the market.

As shown in figure 2b, however, there are two business activities entities in IoT E-business model: DACs and customer. Every DAC can buy products from other DACs as customer, Meanwhile, everyone can issue their own IoT commodities to become DAC. In other words, there are no essential difference



(a) Traditional E-business entities (b) IoT E-business entities

Figure 2. Business entities

between customer and company. For example, there is a automatic sensor which can send its data to IoT E-business platform, complete the trade and own its own wallet(i.e. the basic unit of DACs). It has to buy power from a power station agent DAC using bitcoins automatically when it is short of power. As a result, any other third parties including the government can not manipulate the market or the DACs. All DACs run automatically without the interfere of human being. Its code and regulation are open sourced 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 because of the modification. Therefore, any malicious modification of the DACs regulation or non-standard DACs are actually invalidate in the IoT E-business model.

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 class 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 device. Besides, there are no traditional stage like storage or logistics, and customers can get their commodities or keys immediately while the deal was closed . Although there are physical entities in smart property and energy property, the shift of the ownership is realized by the token transmission or the digital control.

a) Paid Data: Even if paid data is the main commodity of the IoT E-business model, its value is hard to evaluate or it cannot sold as regular commodities on the IoT. The cost of paid data include in the stage of collection, process, maintenance, hardwares and softwares involved in these stages are easy to calculate. However, the true value of data is hard to evaluate. It is because that the value of the paid data is depend on how much benefits customers could get. In another word, the value of two messages which are processed from the same paid data for two different purposes is totally. Therefore, we need a set of methods to evaluate the value the data so as to make them became commodities in the IoT E-business model. Authors in [20] define seven laws of information, explaining the difference between information commodity and traditional goods.

We can define a systemic and improved price model for the IoT data commodity by these laws, as well as charging standards for different features.

The feature of IoT make it easier to access and issue information. That is to say, we can package different data and messages in a series of modules, then using API to access messages according to our requirement. The 1st rule illustrate that the reasonable charging mode is charging users by number of times they visit the API. The price models for different types of data is to judge whether messages and data are valuable which is equal to the judgment of whether the data related service is worthwhile. The the 2nd rule explain that people are willing to pay more bills for the worthy services. The price models for the same type data contain 3 factors. Firstly, the date is very important to some time-critical data. And they will become valueless if they are out-of-data. As a result, the 3rd rule is about the function between price and valid time. Secondly, the job of sensors are to sample the real world, the price model standard should depend on the authenticity, completeness and coherence of the data. Hence, the 4th rule illustrate the relationship between precision and value. Thirdly, a sole type of data is usually worthless. But their value may multiply by using data analyze method, data mining method and data fusion technique. The 5th rule show that the fusion of information is not a simple addition, but a set of complex interactions. When the amount of data reached a certain degree, they are prone to redundancy which may lead to confusion to human beings and unnecessary processing costs to machines. Therefore, the 6th rule indicate that the less the amount of data, the higher the value that the data should be under the premise of the same effect.

b) 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. shares of the company and access authority of a remote computer) and energies(e.g. power, oil and gas) which can be controlled by digital devices. The benefits of the smart property are that they can minimize fraud and intermediary costs, in addition to complete some transactions which are unlikely to happened in low trust scenarios.

In fact, currently there are 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 adopt the method of user code login to ensure only the right user with 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 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 totally done on the network. In practical, the ownership of the smart property may be reflected in the unlock of the controller(e.g. the door lock, the car lock, the water meter and electric meter). In other words, the owner can control their smart properties by mobile devices equipped with NFC and specified APP.

C. 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 still rely on the third party platform that the potential of the decentered feature can not be fully reached. Since the trade between currency and commodities is real time and automatic in the IoT E-business model, the trade mode 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 paid data and smart property.

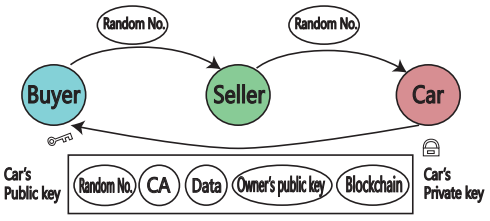
The IoTcoin is a special colorcoin which is a general term of all second generation cryptocoins based on the bitcoin other than a currency. In another word, cryptocoins that are based on the Blockchain and can present virtual goods and smart properties exceed their value can go by the name of colorcoin. Therefore, IoTcoins can be used to present the ownership of many IoT commodities such as smart property, paid data and digital controlled energy.

1) The P2P trade of the IoT E-business model: IoTcoins can trade with bitcoins and other IoTcoins through P2P mode as the voucher of smart property. For instance, a carcoin(i.e. an IoTcoin that present the ownership of a car) can exchange 30 bitcoins or 80000 datacoins(i.e. an IoTcoin that can get access to temperature sensor data for one time). To achieve this, first of all, we assume there are some sorts of communication channel that messages can be posted to. All participating agents receive all messages. And there are two kinds of objects: exchange offer and exchange proposal. The function of Exchange Offer is to post a message like "I'm willing to exchange X coins of color A for Y coins of color B". Exchange Proposal is a proposal to make a transaction. The sequence of the P2P is as follows:

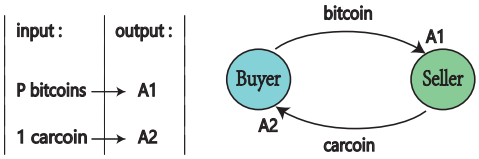
- Alice posts her exchange offer(i.e. exchange 1 carcoin for 30 bitcoins).
- Bob finds Alice's exchange offer and creates exchange proposal. Exchange proposal includes: exchange offer, Bob's txins (i.e. 30 bitcoins that Bob has to send), Bob's txouts (i.e. Bob wants to receive 1 carcoin)
- Alice finds Bob's exchange proposal, she checks if it is screwed up, particularly the included offer is valid. If it is OK, Alice creates her own exchange proposal, it has same offer information. Then Alice composes a transaction which uses both Alice's and Bob's inputs and txouts. However, Alice's txins are signed, but Bob's aren't, so this is an incomplete transaction.
- Bob sees this updated exchange proposal, he checks whether Alice's payment is OK and all his txouts are included, then he signs his inputs.
- Now we have a complete transaction with all inputs signed. It can be submitted on the network. Bob does that, he also sends exchange proposal with a complete transaction.
- Alice sees this complete transaction and now she knows that transfer is complete. All these steps are transparent to users that they just need know how many bitcoins can exchange a carcoin.

2) The transaction of smart property: As introduced in III-B3b, 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 verified by the ownership key which is the private key(KEY-01) of the owner's IoTcoin address. In the first place, there is a public key corresponding to the private key of the car itself when the car leaving the factory. We call it KEY-02. 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 need a digital certificate and the public key of it. The specific transaction processes are shown in figure 3. There are four steps:



(a) step1



(b) step2

Figure 3. Smart property transaction procedure

- The seller has to prove that the car belongs to him. As shown in figure 3a, firstly, the buyer sends the seller a random number, then the seller sends this number to the car. Secondly, the car encrypts a series of data beside this random number and then sends them to the buyer. These data include random number given by the buyer, the public certification of the car, the data of the car(e.g. mileage and the date of purchase), car owner's public key, data format of the carcoin and the Blockchain of the latest transaction. Then the buyer can use KEY-02(i.e. public key of the car) to decrypt the message so as to get these data. As a result, the buyer will confirm the ownership of the car. In addition, the buyer has to import the format template of the carcoin so as to join the P2P trade platform on the IoT and view the trade list.
- The buyer initial a trade after the seller offer a price. As shown in figure 3b, in the first place, the seller has

to price the smart property as P bitcoins and specify a transaction address A1. In the second place, the buyer has to specify a transaction address A2 and start the deal which includes 2 inputs and 2 outputs. The first input is P bitcoins paid by the buyer, the corresponding output is the seller's transaction address A1. The second input is one carcoin paid by the seller which represents the ownership of the car, and the corresponding output is the buyer's address A2. In the third place, if both sides accede this transaction, they will sign their own private key on the contract and broadcast it to the whole network. In the last place, this transaction takes effect and joins up with the main Blockchain. The KEY-03(i.e. private key of A2) substitute KEY-01(i.e. private key of A1) to become the ownership key of the car.

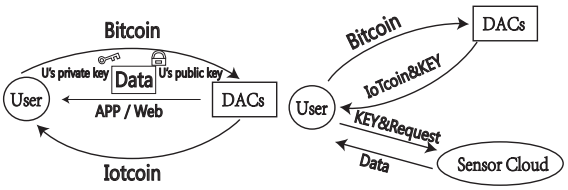
- The update of the car. When the car deems that the ownership has been reallocated and the Blockchain of the new transaction is longer than the old one, in addition to enough tasks stack on the top of the Blockchain to make it inreversible, it will update the ownership data and Blockchain to the latest version. So far, the whole transaction is complete.
- Unlock the car. The new owner of the car can use KEY-03 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 protocal are transparent to the users.

3) The transaction of paid data: Data is a special IoT commodity. It is infinitely replicable and without physical entities. In addition, the processed data are more valuable than the raw data collected by sensors. Therefore, the data provider needs to develop, refine and package these raw data so as to offer product-class data to buyers. The provider can either be human beings or programmable DACs.

There are 2 ways for customers to purchase data on the IoT. One is negative access. As shown in figure 4a, the buyer pays bitcoins to the data provider while the data provider pays IoTcoin which present the access of data to the buyer. The provider will get buyer's public key through this transaction. Then the buyer only need to show his public key to the provider so as to get required data regularly. These data are encrypt by the buyer's public key so that only the buyer can use them. In practical, these operation may complete through a web platform or an APP. The other is positive access. The buyer needs to use the API or SDK offered by the provider to get the required data. As illustrated in figure 4b, the buyer make a P2P deal with the data provider who will send the access key besides IoTcoin. Then the buyer only need to use this key to access the API to get data. The practical realization may with the help of RESTful.

IV. Experiment

In order to construct IoT E-business system, we use an open project "chromawallet"[23] which is based on the concept of colorcoin as the base of the transaction architecture. Besides,



(a) Negative method (b) Positive method

Figure 4. Access methods of data on the IoT

we use IoT cloud platform "Xively"[24] to store and exchange data. The complete transaction process is shown in figure 5.

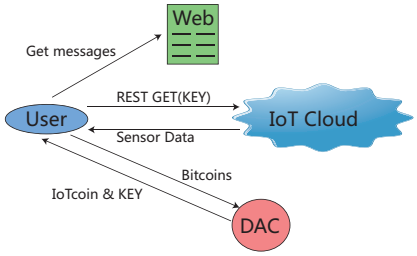
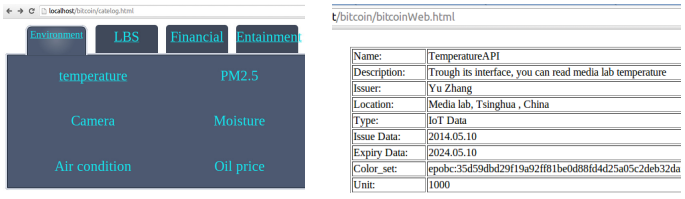


Figure 5. IoT E-business technological process

A. Information Acquisition Session

In this experiment, we assume buyers are human beings. Therefore, they could search for proper commodities through a web shown in figure 6a. After clicking a specific item, the system will enter into the commodity details page shown in figure 6b. This page includes all the details of this commodity such as name, description, issuer, location, information type, issue date, expire date, colorset, unit, URL of the REST, instructions and the format of returned data etc.



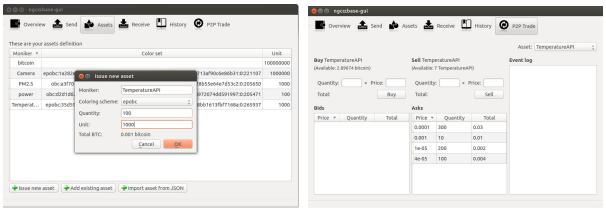
(a) IoT commodity catalog (b) Commodity details

Figure 6. IoT commodity information platform

B. User Client and Communication Session

If the customer has decided which commodity to purchase, as shown in figure 7a, he can import the IoTcoin of this commodity into client by some related messages such as name, colorset and unit.

Then the buyer can recognize all ongoing trade informations of this commodity on the P2P platform. These informations are broadcast by data providers regularly called exchange offer. And there are two kinds of objects: exchange offer and exchange proposal. As shown in figure 7b, clients which are



(a) Import commodity information (b) List of trade information

Figure 7. User client

imported the certain format of the commodity can recognize these informations and show them in list.

- The format of exchange offer send by Alice(i.e. the data provider) is as follows:

```
{ "A":{"color_spec":epobc:35d59dbd29f19a9
       2ff81be0d88fd4d25a05c2deb32daf5be
       c8bb1613fbf7168a:0:265937",
       "value": 200000},
  "msgid": "fb77da0af9b2a097",
  "B": {"color_spec": "", "value": 200000},
  "oid": "400b8dec5200431a"}
```

"color_spec"is the unique identification of this IoTcoin. The former "value"equals the transaction quantity multiply 1000, "msgid"is the ID of this message. "oid"is the ID of this transaction. The latter "value"is the total amount of this transaction. As a result, the price of the IoTcoin equals latter "value" divide the former one and multiply 1000. In this transaction, the price is 1000(i.e. $200000/200000 \times 1000$). The unit is Satoshi(1 Satoshi equal to 10^{-8} bitcoin).

- Once Bob(i.e. the buyer) has decided to choose one transaction from the list, he will create the transaction and send an exchange proposal to Alice. Exchange proposal includes: exchange offer, Bob's txins (i.e. 20000 satoshi), Bob's txouts (i.e. address of IoTcoin). "oid"and "color_spec" must in accordance with Alice's exchange proposal. The format of exchange proposal send by Bob is as follows:

```
{ "A":{"color_spec":"","value":200000},
  "msgid":"a562a2430f921acc",
  "B":{"color_spec":"epobc:35d59dbd29f1
       9a92ff81be0d88fd4d25a05c2deb32da
       f5bec8bb1613fbf7168a:0:265937",
       "value": 200000},
  "oid": "400b8dec5200431a"}
```

- Alice finds Bob's exchange proposal, she checks that it isn't screwed up and included offer is valid. Then Alice creates her own exchange proposal which has the same offer information. Then Alice composes a transaction which uses both Alice's and Bob's inputs and txouts which pay both to Alice and Bob. Alice's signed her txins by her private key, but Bob's aren't, so this transaction is incomplete so far.
- Bob sees this updated exchange proposal, he checks whether Alice's payment is OK and all his txouts are included, then he signs his inputs by his private key.
- Now Bob have a complete transaction with all inputs signed which can be submitted on the network. Besides, he also has to send exchange proposal with a complete transaction.
- Alice sees this complete transaction and now she knows that transfer is complete.

C. Blockchain session

In order to prevent Bob spend one bitcoin twice or Alice cancel the transaction after she got the bitcoin, third parties and a series of related databases are needed to record every transaction. However, there are no third parties in the IoT E-business model. Therefore, we need to public every transaction to the Blockchain which is constructed by the compute power of all clients and monitored by everyone. In another word, everyone is a third party.

In addition to IoTcoin, Alice has to offer the API key to Bob who can use it to access the API of IoT cloud to get required data through other more efficient communication protocols such as TCP/IP.

Validation scripts can choose from a diverse palette of predefined functions. OP_RETURN is one of them. This function accepts a user-defined sequence of up to 40 bytes. When a transaction containing a script with an OP_RETURN function, it will be recorded into a block. The accompanying byte sequences will also enter into the block chain. In this experiment, we transcode these characters of the key into hex format and write them into script.

Messages in the Blockchain is shown as follows:

```
010000000XXXXXXXXXXXXXXXffffffff03XXXXXXXXXXXXXX206a1e582d4170694b65793a20686
d4d4b5432433756706a4c54657a6c66416965XXXXXXXXXXXXXX206a1e582d4170694b65793a20686d4d
4b5432433756706a4c54657a6c66416965XXXXXXXXXXXXXX206a1e582d4170694b65793a20686d4d4b5
432433756706a4c54657a6c6641696500000000
```

Character between "010000000"and "ffffffff" are input relevant data. "03" means there are 3 outputs in this transaction: First output is some bitcoins which are send to Alice. Second output is the change for Bob himself. Third output is the payment for the miner. The role of miner is to package the Blockchain by offering its compute power. "206a1e" is a hexadecimal code. As shown in table I, "20"and "1e" means there are 32 and 30 bytes data afterwards. And "6a" is the code of OP_RETURN in Blockchain. That is to say,"OP_RETURN" account for 2 bytes and data after "1e" account for 30 bytes.

Table I
OP_RETURN HEX DATA FORMAT

20	6a	1e
32	OP_RETURN	30

Strings "582d4170694b65793a20686d4d4b5432433756706a4c54657a6c66416965" are hexadecimal character, and their text format are X-ApiKey: hmMKT2C7VpjLTezlfAie. This is the key that Alice provided to access the API of IoT cloud. There is a website [25] provides the debug tools for OP_RETURN. From the figure 8 we can see there are 3 outputs that carry the API key.

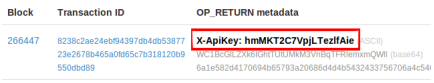


Figure 8. OP_RETURN debug website

In order to get a good experiment effect, we do not encrypt the characters of the key. In practical terms, these characters have to be encrypted by the buyer's public key that only his private key can decrypt them.

D. IoT Cloud API Session

Our experiment is based on Ubuntu13.04 operation system, and using RESTful web services to exchange data. Test tool is cURL and IoT cloud is Xively[24].

The format of request messages are as follows:

```
curl
     --request GET \
     --header "X-ApiKey:hmMKT2C7VpjLT
     ezlfAie" \
     --verbose \
     api.xively.com/v2/feeds/1156420415
     /datastreams/dht_temperature
```

We put the API key into the header and fill the URL with the sensor device ID(i.e. 1156420415) and data channel(i.e. dht_temperature). Then we use the method GET to send the request. After verifying the validity of the API key, the server will return strings in JSON format shown as follows:

```
{ "id":"dht_temperature",
  "current_value":"26.00",
  "at":"2014-06-29T05:45:12.309267Z",
  "tags":["temperature"],
  "unit":{"symbol":"oC","label":"oC"}
```

"Current_value"is the target data in this experiment. So far, we have brought temperature data for 1000 Satoshi.

V. Conclusions and Future Work

In this research, we have proposed a business model for 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 decentration of the IoT E-business model, we propose a P2P transaction mode on the IoT based on the 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 script. At the end, we designed an experiment to verify these theories of the IoT E-business model.

Just as we proposed in III-B3, there are 2 types of commodity in IoT E-business model. One is the smart property, 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 informations 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. The Internet of things: A survey[J]. Computer networks, 2010, 54(15): 2787-2805.

[2] Li H, Tian Y, Liu Y, et al. 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. The internet of things in an enterprise context[M]//Future InternetFIS 2008. Springer Berlin Heidelberg, 2009: 14-28.

[4] Bucherer E, Uckelmann D. Business Models for the Internet of Things[M]//Architecting the Internet of Things. Springer Berlin Heidelberg, 2011: 253-277.

[5] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2008, 1: 2012.

[6] Osterwalder's A. Business model canvas[J]. 2008.

[7] Leminen S, Westerlund M, Rajahonka M, et al. Towards iot ecosystems and business models[M]//Internet of Things, Smart Spaces, and Next Generation Networking. Springer Berlin Heidelberg, 2012: 15-26.

[8] Amit R, Zott C. Value drivers of e-commerce business models[M]. INSEAD, 2000.

[9] Chesbrough H, Rosenbloom R S. The role of the business model in capturing value from innovation: evidence from Xerox Corporation's technology spinoff companies[J]. Industrial and corporate change, 2002, 11(3): 529-555.

[10] Amit R, Zott C. Value creation in ebusiness[J]. Strategic management journal, 2001, 22(67): 493-520.

[11] Osterwalder A, Pigneur Y. An e-business model ontology for modeling e-business[C]//15th Bled electronic commerce conference. Bled, Slovenia, 2002: 17-19.

[12] Tikkanen H, Lamberg J A, Parvinen P, et al. Managerial cognition, action and the business model of the firm[J]. Management Decision, 2005, 43(6): 789-809.

[13] Westerlund M, Rajala R, Leminen S. Insights into the dynamics of business models in the media industry[J]. 2011.

[14] Bohn J, Coroam V, Langheinrich M, et al. Social, economic, and ethical implications of ambient intelligence and ubiquitous computing[M]//Ambient intelligence. Springer Berlin Heidelberg, 2005: 5-29.

[15] Fleisch E. What is the internet of things? An economic perspective[J]. Economics, Management, and Financial Markets, 2010 (2): 125-157.

[16] Palo T, Tähtinen J. A network perspective on business models for emerging technology-based services[J]. Journal of Business & Industrial Marketing, 2011, 26(5): 377-388.

[17] Osterwalder A, Pigneur Y. Business model generation: a handbook for visionaries, game changers, and challengers[M]. John Wiley & Sons, 2010.

[18] Bucherer E, Uckelmann D. Business Models for the Internet of Things[M]//Architecting the Internet of Things. Springer Berlin Heidelberg, 2011: 253-277.

[19] Andreas Antonopoulos, May 29, 2013 It is a protocol, a network, a currency and a transaction language. Most of all, though, it is an application programming interface (API) for money.

[20] Moody D L, Walsh P. Measuring the Value Of Information-An Asset Valuation Approach[C]//ECIS. 1999: 496-512.

[21] https://en.bitcoin.it/wiki/Smart_Property

[22] https://en.bitcoin.it/wiki/Contracts

[23] https://github.com/bitcoinx/ngcccbase

[24] https://xively.com

[25] testnet.coinsecrets.org