# Global Digital Currency System Analysis and Research

Xinyue Du[1], Xiangyang Li[2], Qian Zhong[3], Xiufen Wang[3*]
[1]School of Food Science and Bioengineering, Tianjin Agricultural University, Tianjin, 300384, China
[2]School of Engineering and Technology, Tianjin Agricultural University, Tianjin, 300384, China
[3]School of Computer and Information Engineering, Tianjin Agricultural University, Tianjin, 300384, China
*Corresponding author

**Abstract:** In recent years, with the rapid development of cryptography technology and Internet technology, digital currency has exploded in popularity in various parts of the world. Our team's objective is to find a model to analyze the global digital currency system, and then use our models and research to create a strategy for the development of global economy. Firstly, we consult the relevant data and information. Then we construct two representative ECC models of digital currency, as well as UTXO model and Account model. And it turns out that the digital currency has higher safety factor, lower cost and convenience. Secondly, based on our models, we analyze the development of digital currency at the individual, national and global levels. We find that there has been a large fluctuation in the recent years. Thus, we further study this issue and the results show that the lack of effective supervision is one of the main causes of fluctuation. Then, we conclude that more and more countries would pay more attention to block-chain technology and related regulatory mechanisms. Thirdly, aiming at further analysis of the digital currency market of different countries, we choose America and China in our further investigation. We get that most countries expect better development of the digital financial system and greater rapport in international relations. However, at present these countries don't modify their current banking and monetary models. Finally, we perform a sensitivity test to verify the stability of our model and conclude the strengths and weakness of our model. The result demonstrates that our models can help us to deeply understand the development of digital currency in a certain extent.

**Keywords:** Digital currency; Block-chain technology; Supervision mechanism

## 1. Introduction

### 1.1. Modeling assumption

With the rapid development of economic, digital currency, as a new type of currency, is rising rapidly. Digital currency market has a certain impact on many countries. The emergence and use of digital currency have contributed greatly to the circulation of the global economy. However, there are still some issues in the use of digital currency. Its price fluctuation is fierce. And it's lack of supervision subject. These issues have also caused a certain impact on financial stability. It has aroused the strong concern of the people and the government [1].

Digital currency is a new digital method of financial transactions, so there are concerns about its security.

At the G20 Summit, countries expressed their attitudes towards digital currencies. In general, most countries believed that digital money can be an advantage of the financial system. But during the development of digital currency, countries need to strengthen the protection of investors [2].

Digital currency has some benefits to financial services users and governments. However, some issues still exist. If these issues could be addressed, digital currency could work better for individuals, businesses and governments. The geographical distribution of digital currency use in the world is shown in Figure 1. The representative countries are Europe, the United States, Japan, China and Canada.

### 1.2. Our work

Firstly, we analyze the viability and effects of a global decentralized digital financial market, then establish the reasonable mathematical model.

Secondly, we study the different needs of countries and analyze their willingness to work with this new financial marketplace. Then we study countries weather modify their current banking and monetary models.

Thirdly, we discuss the strategy for adoption and expound the rationality of this strategy. According to the different national conditions, we put forward the corresponding implementation.

Fourthly, based on a representative financial system model, this article includes the mechanisms for oversight of such a global digital currency. And it extends the analysis to consider the long-term effects of such a system on

the current banking industry, global economy and international relations between countries.

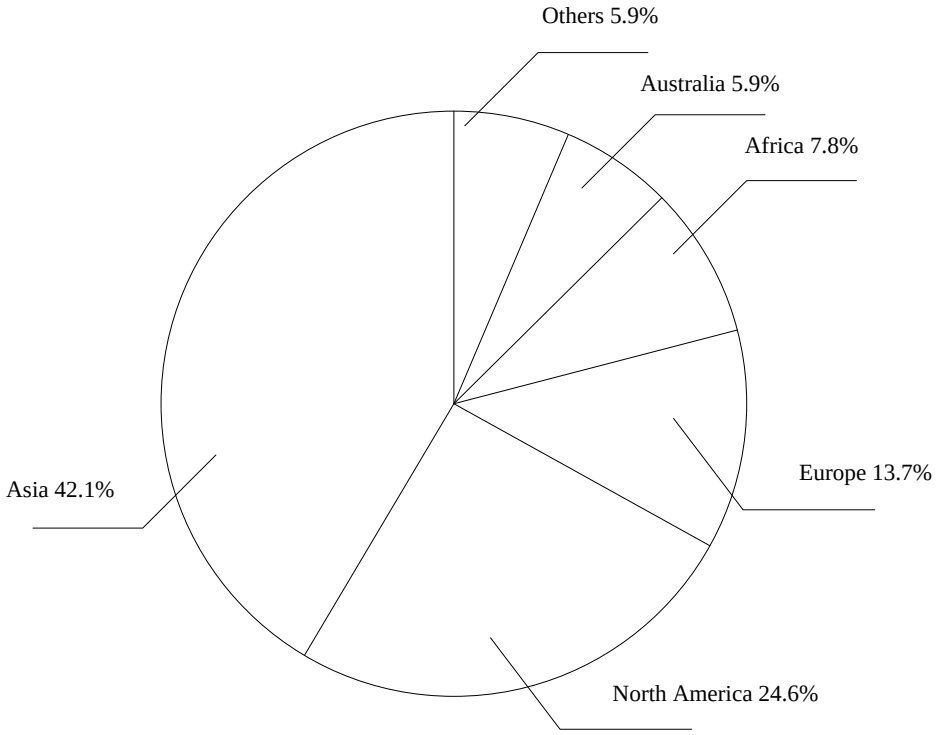


**Figure 1. The geographical distribution of digital currency**

Finally, we provide policy recommendation for national leaders, who hold mixed opinions about this effort. And this policy recommendation offers rationale for the parameters and dynamics included in our model.

## 2. Assumption

Assumption 1. Assume that culture, population and technology have no greater impact on national economy when analyzing the impact of models on the economy.

Assumption 2. In calculating the safety factor of the digital currency, profits from illegal transactions are not taken into consideration.

Assumption 3. The data consulted have authenticity and accuracy to a certain degree.

## 3. Notation of Parameters

We start the analysis by giving a list of parameters involved in the model as shown this Table 1. Other symbols that are used only once will be described later.

**Table 1. A list of parameters involved in the model**

| Number | Symbol | Definition |
|---|---|---|
| 1 | K1 | Random integer of Communication A |
| 2 | K2 | Random integer of Communication B |
| 3 | G | The basic point |
| 4 | Fp | Finite domain |
| 5 | n1 | The order of the basic point of BTC |
| 6 | r | The order of the elliptic curve |
| 7 | n2 | The large prime factor of r |
| 8 | P | Random point on elliptic curve |
| 9 | λ | A random parameter |
| 10 | Pt | The price of the digital currency |
| 11 | Qt | The Profit of the digital currency |
| 12 | Ut | Invisible Fundamentals |
| 13 | rf | Risk-free interest rates |
| 14 | Bt | Foam Ingredients |

# 4. Application of Our Model

## 4.1. Data source

The selection of data is of vital significance to the model. The authenticity and extensiveness of the data make the model more practical. After repeated search, we find the real data involved in the Shao's article [3]. Although the authority of these data is beyond doubt, due to the variety of variables will be used in different areas in the process of model building. So, these data must be varied. We look for an alternative method that uses some of the data that is already in "Comparison of UTXO and Account models" [4]. Then we use computer simulation part of the data that modeling need according to objective laws.

## 4.2. Decentralized digital financial model

First of all, we analyze BTC.

Encryption of BTC: We use the rational points on the elliptic curve to make it difficult to calculate the elliptic discrete logarithm on the Abel addition group. ECDH and ECMQV are the implementations of the Diffie-Hellman and MQV key negotiation protocols on ECC. The model scheme for establishing key negotiation is as follows: Elliptic curve parameter equation:

$$Y^2=X^3+aX^2+b$$

Related factors:

$$h=r/n$$

The keys of Communicator A and Communicator B are (SK1, PK1) and (SK2, PK2). And the public keys are PK1 and PK2.They place on a trusty third-party authentication center. The negotiation and sharing of the temporary key process is shown in this figure.

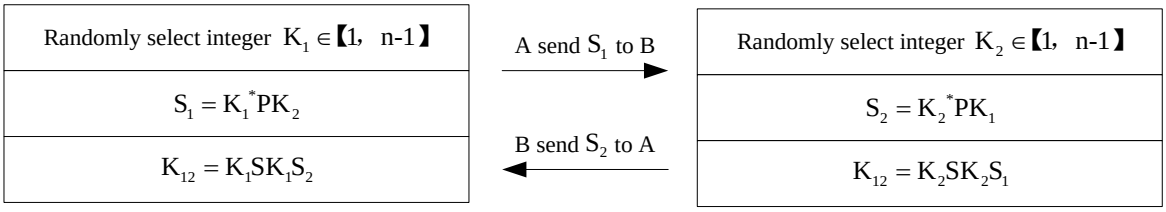


**Figure 2. Encryption process**

Communicator A obtains the shared key is $K_{12}$:

$$K_{12}=K_1S_2SK_1^{-1}=K_1K_2G$$

Communicator B obtains the shared key is $K_{21}$:

$$K_{21}=K_2S_1SK_1^{-1}=K_2K_1G$$

So $K_{12}=K_{21}=K_1K_2G$, and $K_{12}$ equals $K_{21}$. Ensure that both parties can get the same key. Therefore, BTC has multiple security attributes, and it can resist a variety of attacks.

Trading of BTC: The trading model of BTC is the UTXO model. In the model, the transaction represents a change in the UTXO collection, and the account and balance are higher abstractions on the UTXO collection and exist in the wallet.

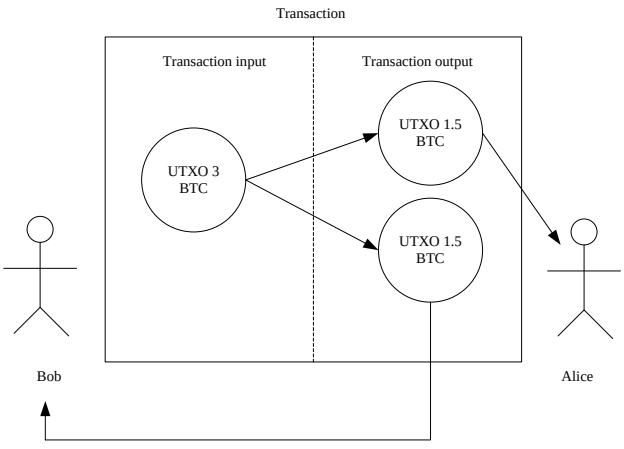


**Figure 3. The model of UTXO**

Analyzing this model, we could obtain the advantages of the UTXO model.

The calculation takes place in the chain. And the transaction itself is the result and proof. The burden of calculating the transaction is borne entirely by the wallet. It re-

duces the burden of the chain; The sequence and dependence of transactions are easy to verify, and it is easy to prove whether a transaction is consumed or not; The UTXO model is stateless and easier to handle concurrently; It's very private.

However, this model also has some drawbacks:

It is difficult to achieve some complex logic, and its space utilization is a little low; It is difficult to implement some complex logic, and its space utilization is low; Its signature consumes more CPU and storage space.

Next, we analyze ETH.

Encryption of ETH: The encryption of ETH uses Elliptic Curve Digital Encryption Algorithm (ECDSA), which is based on Elliptic Curve Cryptography (ECC). And the theoretical basis of ECC is the dot-multiplication formula. The multiplication of elliptic curve points:

$$z = nQ$$

Geometric equations of elliptic curves:

$$Y_2 = X_3 + aX_2 + b$$

The addition of elliptic curve points:

$$Q + P = Z$$

$$(xq, yq) + (xq, yq) = (xz, yz)$$

Flip the elliptic curve point:

$$xz = \lambda_2 - xp - xq$$

$$yz = \lambda(xq - xz) - yp$$

$$\lambda = \frac{(y_p - y_q)}{(x_p - x_q)} \Rightarrow \lambda = \frac{(3x_q^2 + a)}{2y_q}$$

ECC requires only a shorter public key when providing the same level of security.

Trading of ETH: The trading model of ETH is the account model. It preserves the state of the world, and the state of the chain. They generally behave in the form of State Root and Receipt Root in the block. Trading is only the event itself without results, and the consensus of the transaction and the consensus of the state can essentially be isolated.

By analyzing this model, we could obtain the advantages of the Account model; Contracts are saved as code, and the Account model is better programmable; The Account model can greatly reduce costs through contractual method.

The disadvantage of this model is that there is no dependence between Account model trading. And we need solve the replay problem. The state migration from the child-chain to the main-chain requires a more complex protocol.

We compare the operational strategies of these two typical digital currencies, and draw the following conclusions: The development of digital currency in the early stage is relatively stable, and the use of the last two years has reached a peak. However, with the development of digital cryptographic currency, there is a downward trend. For example, BTC and ETH reached a peak in 2017. Then, in 2018, BTC fell by about 70%, and ETH fell by about 90% [5].

Some digital currency Block-chain networks have the defect of insufficient extensibility. Some digital currencies emphasize the application of Block-chain technology. In addition to having the characteristics of digital currency, there is also the possibility of the writing applications with contract functions. So this digital currency has a better space for development.

With the innovation and development of Block-chain technology, more and more people pay more attention to the security of Block-chain. Besides, government departments also need to strengthen the study of Block-chain security issue and establish relevant safety standards to promote the healthy development of Block-chain.

### 4.3. Analysis of digital financial market

In this part, we study decentralized digital financial model and analyze digital financial market. We identify key factors that would limit or facilitate its growth, access, security, and stability at all the individual, national, and global levels.

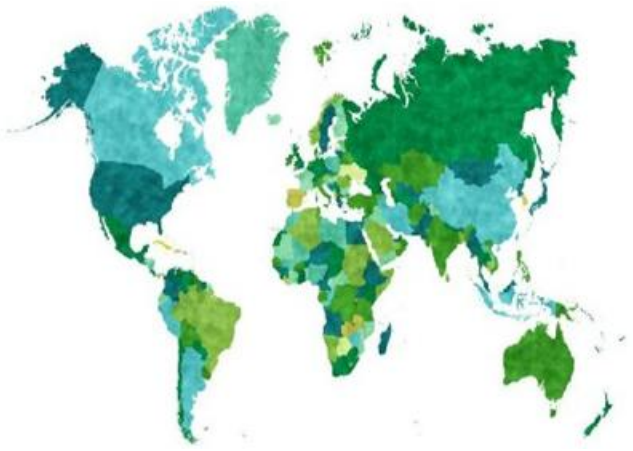

**Figure 4(a). The use of digital currency in some countries**

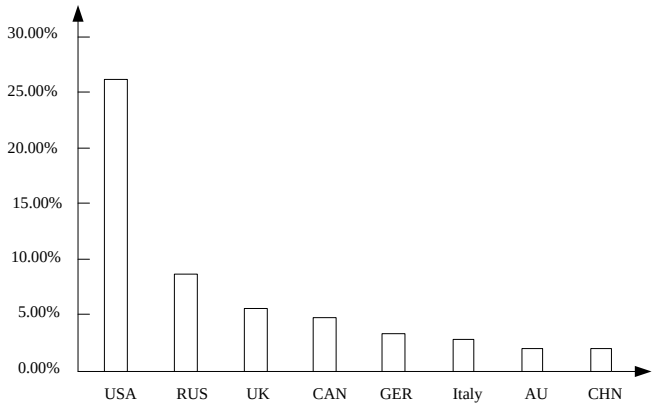


**Figure 4(b). The use of digital currency in some countries**

This figure represents the annual use of digital currency in every country in the world. It can be seen from this figure that different countries have different uses of digital currencies, according to their respective development conditions. Some countries use more digital currency, others use less.

Then, we get the following conclusions:

Many digital currencies use the Block-chain technology, but there are some differences. Some digital currencies are "complete node de-centric, power-centric and development-centric". And some digital currencies are "completely central". According to the calculation results of our model, the development of the above first digital currency is more stable.

Models of different digital currencies are varied. The UTXO model has unique and creative advantages in simple business and cross-chain. The Account model has advantages in programmability and flexibility.

In terms of individuals, countries and society, digital currency has generally grown steadily. But it has fluctuated considerably over the past year. And this fluctuation had a certain impact on the global digital financial system. It caused many citizens in the world to pay keen attention to the digital currency.

According to the different economic development conditions of various countries, different countries have different attitudes towards the new financial markets. Developed countries, represented by the United States, Germany and Japan, and developing countries represented by China are willing to cooperate with new financial markets. And they will not modify the current banking and monetary model for the time being in accordance with national conditions. At the same time, every country expects better development of the digital financial system.

### 4.4. Strategy of digital currency

We strictly calculate the security of digital currency. Through the model of encryption and trading in two representative digital currencies, it shows that the use of digital currencies at the individual, national and global level can achieve a higher level of security if better safety codes are followed. To achieve this goal, government need provide more improved oversight mechanisms. Therefore, we provide a more perfect management mechanism than the traditional supervision mechanism.

Develop more complete the management of Block-chain technology. Strengthen the development of technical reserves, parameters and digital currency rules. Accelerate the construction of network infrastructure to provide a solid material foundation for the distribution of digital currency. Do a good job before the transformation of the business model management system. Establish a trust system based on big data.

### 4.5. Assessment from different perspectives

The long-term impact of digital currency on banking [6].

On the one hand, its beneficial effects are that the use of digital currency reduces information asymmetries between banks and customers. And it reduces bank compliance costs and management costs, and it avoids cumbersome data maintenance by banks. In addition, digital currency effectively improves the efficiency of bank business processing.

On the other hand, its adverse effects are that digital currency compress the traditional bank business income and affect the liquidity of banks.

The long-term impact of digital currencies on local, regional and world economies.

Its advantages are that digital currency is an important tool for the total amount of economic adjustment. It can greatly enhance the adjustment of currency price instruments. Its adverse effects are that enterprises at the end of

the payment channel will be greatly impacted, and the digital currency may affect the current deposit reserve system. In addition, the emergence of new currencies to market macro-control increases its difficulty.

The long-term impact of digital currency on international relations.

For one thing, its beneficial impacts are that the development of new currencies could promote the coordination and cooperation among countries, increase friendly trade between the international and promote the development of national economies.

For another, its adverse impacts are that the use of digital currency and regulatory regimes in each country are different. It results in a phenomenon of fluid flow in the international circulation of digital currency.

## 5. Testing the Mode

In this part, we test our model by comparing the benefits of different policies. It shows that our model is generalized and performs stably under different conditions. We convince that our model is able to solve the problem successfully.

We use "foam test model" [7] to test the result of our model. Establish the following model:

$$P_t = \sum_{i=0}^{\infty} (\frac{1}{1+r_f})^i E_t(D_{t+i} + U_{t+i}) + B_t$$

Through the above test model, it shows that our model result error is small. In the future market, digital currency sharp fluctuation probability is relatively high. The price of digital currency may include foam. So, we need more perfect regulatory system.

According to the test results and empirical evidence, the development trend of digital currency market is shown in Figure 5. This is in line with the normal market development trend.

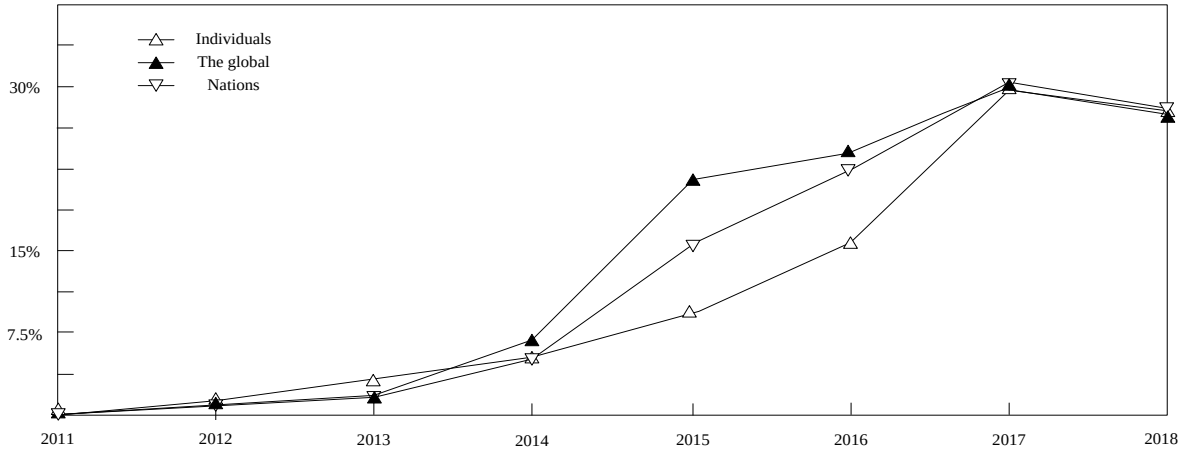


**Figure 5. Digital finance development trend chart**

## 6. Conclusion

### 6.1. Strengths

Our model considers plenty of the influencing factors. We identify the most important feature accurately in the model and take the influence of other significant factors into account.

The data in our model consist of parts of the data in literature and simulation data imitated by computer, which improves the science and accuracy of our model.

### 6.2. Weakness

In the process of analyzing the problem, a small amount of data is missing, so there are some effects on the accuracy of the model.

One limitation of our current approach is not to bring our policies into line with the circumstances of all countries.

### 6.3. Future work

In future work, our goal is to provide a better solution. This solution could both increase the countries' benefits and promote more stable development of the country's economy.

## 7. Acknowledgment

Tianjin Agricultural University student innovation and entrepreneurship training project (201910061006).

## References

[1] Li M.G., Lin M., Cai W.D., Huang S., Wu J.Y. Practical experience and thinking of implementing digital money at home and abroad based on the perspective of financial stability. Fujian Finance. 2017, 03, 45-49.

[2] The attitude of countries towards digital currency at the-G20-summit. 2018, 03, 31.

[3] Shao X.B. Research on the improvement of key negotiation scheme in elliptic curve cryptography system. Computer Security. 2010, 02, 23-25

[4] Comparison of UTXO and accountmodels. Nervos Network.

[5] The difference between Bitcoin and Etheric Square and the pros and cons which is better-blockchain. http://m.qukuaiwang.com.cn/news/14165.html

[6] FanY.H., Li Y.X. Taking Bitcoin as an example to discuss the legal supervision of digital currency. Applicable by Law. 2014, 07, 48-52.

[7] Shi W.R., Wang W.T., Meng H.Y. General situation, influence and prospect of digital money development. Financial Aspect. 2016, 07, 25-32.