Semester Report

Haoqian Zhang
Supervisor: Prof. Bryan Ford
DEDIS Lab

January 2020

1 Introduction

The financial crisis that happened in 2008 is considered by many economists to have been the worse financial crisis since the Great Depression[6]. In the same year, the Bitcoin white paper was published by Satoshi Nakamoto[9]. The coincidence seems to reveal that Bitcoin, or its underlying technology named blockchain, would change our financial system.

Twelve years have passed now. Bitcoin has gained a huge success and blockchain has become the focus not only in industry but also in academia. And yet, our monetary system remains fundamentally unchanged, with the possibility that the next financial crisis is coming within the next few years.

In this report, I first introduce how money is created in our current monetary system, revealing the fact that money can not be created without creating debt. Besides, the phenomenon of asset price inflation in recent decades could be related to our monetary policies that primarily focus on the general price of goods and services and pay little attention to asset price.

Cryptocurrency, on the other hand, could be issued in a debt-free manner. Cryptocurrency issuance mechanisms are predefined in codes and verifiable on the blockchain, and therefore cryptocurrency provides higher transparency than our current monetary system. However, how to design a monetary policy for cryptocurrency that could be used in daily life is still unclear.

In this semester, I first developed a toolkit for cryptocurrency. It aims to help economists to design better issuance mechanisms for cryptocurrencies. It consists of a currency issuance language and a simulation framework. The currency issuance language describes the issuance mechanism formally, and the simulation framework provides useful information, such as money supply and inflation rates, for the monetary design.

Next, I extend the currency issuance language, so that it can also describe the monetary policy of community cryptocurrencies. Community

cryptocurrency is a type of cryptocurrency with identity control and a type of community currency with blockchain implementation. The monetary policy of community cryptocurrency contains three dimensions: currency issuance, transaction, and demurrage. In the end, three examples of applications utilizing community cryptocurrency is given.

2 Current Monetary System

I introduce a simplified monetary system representing reality. Central banks control the base money through open market operations, and commercial banks create the majority of money in the fractional reserve banking system. Through this simplified model, you would see that creating money is associated with creating debt. An economy based on debt means that economic growth is necessary to repay the debts. If the growth rate slows down, massive default could happen, leading to a serious financial crisis. Also, only a few vital players in the monetary policy committee of central banks control our monetary system. The process is not democratic and transparent, though it greatly affects individual behavior and decisions.

2.1 Base Money

The base money, also monetary base, represents the notes and coins circulating in the economy, including currency held in public and commercial banks and reserves of commercial banks held in their central bank. Base money is directly managed by the central bank, which could expand or contract the base money. The base money, however, is just a small part of the total money that we use every day. The majority of the money is created by commercial banks through the fractional reserve banking system.

2.2 Fractional Reserve Banking System

The fractional reserve banking system is the most common banking practices throughout the world. Traditionally, it is described as follows: a bank takes in customer deposits as cash, and then the bank can lend out a portion of the money, keeping only a fraction of it as a reserve. It is based on the expectation of banks that only a portion of customers would seek to withdraw their deposits at one time, and therefore, the banks do not need to keep all the money. They can only keep a fraction of it to satisfy the withdrawal requests and lend out the rest to gain interest.

This process has effects on the money supply. Let us imagine a simplified economic world. Assuming bank A initially has 100$ cash and the reserve ratio is 10%, meaning bank A will be able to lend out 90% of its money, that

is 90$. bank A decides to lend out the 90$ to its customer Alice who is creditworthy. Then, Alice uses that money to buy some goods from Bob. After receiving the money, Bob decides to deposit that money to his bank, bank B, rather than keep it under his mattress. Now the bank B has 90$ deposit and it can lend out 81$, keeping 9$ as a reserve. After some transactions, bank C will have 81$ deposit that is from bank B, and it will be able to lend out 72.9$, keeping 8.1$ as a reserve. You can see that this process can go on and go on. In the end, our simple economic world will have up to 1000$. Among those money, the initial 100$ is called base money created by the central bank, and the rest 900$ is called commercial bank money created by commercial banks.

The example above, which describes a situation where multiple banks collectively create money with multiple loans, however, does not accurately describe the actual process in modern times, although it is still written in many textbooks and taught in many places. The major difference is that when a bank makes a loan, it generally does not give cash, but simply adding a number to your account. The electronic money works differently than cash. If the reserve ratio is 10% and a bank has 100$ of cash, in the example above the bank can lend out 90$ in cash and keep 10$ for as a reserve to satisfy the reserve requirement. Or, in modern times, 100$ can satisfy the reserve requirement of 1000$ deposit. Therefore, the bank has a room of 900$ in deposits to still be within the reserve requirement. The bank could create those deposits by making loans. Now the bank can lend out 900$ in a single loan, rather than 90$ in the previous example. When the bank lends out 900$ to Carol, instead of giving Carol cash, the banks add 900$ to Carol's account. It is possible because nowadays we do not rely on cash for all transactions, we greatly rely on electronic money. All electronic money is created by commercial banks.

A single bank can create money out of nothing, but it can not create money infinitely. Many factors, such as behavior of the money holders, influence the money creation by commercial banks[8]. The reserve requirement set by the central bank provides an ultimate upper bound of how much money the commercial banks can create. If the reserve ratio is RR and total amount of base money is B, the maximum amount of commercial bank money M that can be created follows the equation:

$$M <= B \times (1/RR - 1) \tag{1}$$

To summarize this section, most of the money is created by commercial banks, rather than the central bank. Money is created out of nothing whenever a bank gives out a loan.

2.3 Open Market Operation

Although the majority of the money is created by commercial banks, the central bank can control the money supply through open market operations by manipulating the short-term interest rate and the supply of base money. The central bank can either buy or sell the government bonds in the open market or lend money to the commercial banks for a defined period. When the central bank buys governments bonds from banks, new base money is created by the central bank out of nothing, while when the central bank sells the governments bonds, the base money used to buy those government bonds by banks is returned to the central bank, and therefore the base money supply is contracted. Similarly, when the central bank gives a loan to a commercial bank, new base money is created, while when the commercial bank repays the loan, the base money is destroyed.

2.4 Debt-Based Economy

In our current monetary system, the amount of money that is created when a loan is issued by banks equals to the principal of the loan, but the money for the interest of the loan is not created. As a consequence, whenever money is created, our monetary system creates more debt than money.

Banks are not the only entities that can lend money. Non-bank entities can also lend money. Since banks are the only entities that can create money when lending, other lending must be done with the money that was already created by banks. When a loan is issued by a non-bank entity, more debt is created but money is not, resulting in more debt than money.

We are in a situation where money can not be created without creating debt, but we can create debt without creating money. As a result, the total amount of debt is larger than the total amount of money.

2.5 Asset Price Inflation

In today's world, central banks have not paid much attention to control asset prices. The primary goal for most of the central banks in today's world is to provide their countries' currencies with stable prices by controlling inflation. The Bank of England, for instance, is trying to keep the inflation rate at around 2% [1]. The meaning of the inflation here only refers to the price rise of consumer goods and services purchased by households, measured by the Consumer Prices Index (CPI). However, CPI does not account for rising asset prices.

This hypothesis seems to indicate what is happening now in our world. With a belief that asset prices would continue to go up, more money is used for purchasing assets, causing the rise of asset prices. In the meantime, less money is used for consumer goods and services purchasing. To avoid our

economy falls into a zero inflation or even deflation situation measured by CPI, the central bank has to inject more money into the market. However, the newly injected money is also likely to be used for assets purchasing, resulting in the rise of asset prices even more. Then the belief is intensified and a positive feedback loop is formed. The correlation between money growth and asset price inflation in the short, medium and long run [3] supports this hypothesis.

3 Toolkit for Cryptocurrency

Bitcoin caught everyone's attention when it appeared in a white paper in 2008; various cryptocurrencies based on blockchain have emerged since then. Blockchain technology provides an approach to build the next or alternative monetary system, improving transparency and reforming the method of currency issuance.

Cryptocurrency could be debt-free money. In our current monetary system, money is created with debt. Cryptocurrency, however, could be created without debt. For example, creating a Bitcoin does not increase someone's debt level (assuming miners do not borrow money to buy hardware to mine bitcoin).

Transparency is naturally provided by blockchain. The currency issuance mechanism is written in the software in every node participating in the consensus and therefore is available to every consensus node. The issuance mechanism is unchangeable unless every node agrees to change. In an open blockchain system, all the contents in the blockchain are available to read, allowing everyone to audit all the transactions, including those coinbase transactions which create new coins.

However, what is the optimal monetary policy for cryptocurrency is still not clear. Bitcoin is designed with extreme deflationary characteristics, which could lead to severe deflationary spiral[4]. Although other cryptocurrencies are designed in different ways, the general principle of how to design the monetary policy for the cryptocurrency that we could use in daily life is still unknown.

Our toolkit for cryptocurrency, consisting of a currency issuance language and a simulation framework, helps in designing monetary policy aspects. The monetary policy is formally written in the currency issuance language and the simulation framework processes it automatically. The critical information regarding monetary, such as money supply and inflation rate, is in the simulation framework.

3.1 Currency Issuance Language

Although the issuance mechanism of a cryptocurrency is transparent and available in its source code, it is difficult to understand for most people and economists who do not have a programming background. Instead, the currency issuance language is designed in a way that is easy to understand for everyone and focuses only on the cryptocurrency issuance mechanism.

The currency issuance language is represented in JSON format. Below is a simple example of describing the bitcoin issuance mechanism:

```
{
  "base": "block",
  "period": 1,
  "update": [
    {
      "formula": "50 / (2 ** (Height / 210000))",
      "target": "BlockMiner"
    }
  ]
}
```

The *base* field represents the base unit of the currency issuance, while the *period* field describes the interval in terms of the base unit between two currency issuance events. In the above example, Bitcoins are created each time when a new block is discovered. The base field could be any string, but should have a symbolic meaning that everyone agrees on. In a blockchain-based cryptocurrency system, block is a common concept that every node knows. Other potential bases could be a unit of time, such as day, month or year.

The *update* field contains an array that describes the detailed currency issuance procedure. Each element in the array elaborates on one type of currency issuance. One element could contain up to four fields, namely *condition*, *times*, *formula* and *target*. The condition field is a boolean expression, representing the condition of the issuance, with *True* to be the default setting. The *times* field is an integer expression whose value is no less than 1, representing the times that issuance would be executed, with 1 to be the default setting. The *formula* field is an expression that returns an integer number, describing how many coins would be issued. The *target* field is used to describe who would receive the newly created coins.

In the *update* field, external variables and functions could be imported and called. A word starting with a capital letter in value fields indicates that it is an external variable. In Bitcoin example above, *Height* and *BlockMiner* are two external variables. *Height* is the block height of the current block, and *BlockMiner* is the address of the block miner who found the cur-

rent block. Having the symbolic meaning of variables would be helpful to understand the behavior of the issuance, and therefore is recommended. Variables that are imported could be arbitrarily complex objects. Below is a more complex example used to describe the ethereum issuance mechanism:

```
{
  "base": "block",
  "period": 1,
  "update": [
    {
      "formula": "BaseReward",
      "target": "BlockMiner"
    },
    {
      "times": "len(UncleBlocks)",
      "formula": "BaseReward*(9-UncleBlocks[i].k)/8",
      "target": "UncleBlocks[i].Miner"
    },
    {
      "condition": "len(UncleBlocks)>0",
      "formula": "len(UncleBlocks)*BaseReward/32",
      "target": "BlockMiner"
    }
  ]
}
```

In this example, *BaseReward*, *BlockMiner*, *BaseReward* and *UncleBlocks* are external variables. The *UncleBlocks* is an array, in which each element is a object. The *len(array)* is a external function, returning the length of its input.

The interpreter of the currency issuance language is written in the Go language. It uses the **expr** library[2] to evaluate the expressions and output the corresponding values, therefore the *condition*, *formula* and *times* fields support arbitrary expressions in the Go language.

3.2 Application

3.2.1 Issuance Standard

Description text and programming code are two common methods used to describe the currency issuance mechanism, but they both have pros and cons. Humans can easily understand description text, but the program is not able to process it automatically. The issuance mechanism written in code can be directly executed, but provides poor readability to humans. The

currency issuance language could become a standard way of describing currency issuance. The currency issuance language combines two advantages. The JSON file could be read and understood by humans relative easily and could be processed by programs automatically.

The language is independent of the underlying architecture, therefore the JSON file could be plugged into different platforms. It can be inserted into a blockchain or non-blockchain based cryptocurrency system as a configuration file of its monetary policy.

3.2.2 Simulation

The currency issuance language is a perfect tool for simulation, as it eliminates the complex features of blockchain systems, focusing only on the monetary policy. Two levels of simulation are supported, namely micro-level and macro-level. The micro-level simulation is based on accounts. Whenever new coins are generated, a specific account who receives those coins would be indicated in the JSON file. With the assumption of how transactions have happened between each account, the simulation would be able to provide the distribution of balances. The macro-level simulation is based on the aggregated information. All coins are counted in an aggregated account, or a few aggregated accounts, indicating the total supply. To speed up the simulation, the base could be changed to a larger scale, such as year, depending on the accuracy needs. For example, it is reasonable to assume that, in Bitcoin, 52560 blocks would be generated in a year based on the assumption that a new block will be generated every 10 minutes on average. Although it does not accurately reflect the reality, it is good enough for simulation with the unit of a year. Figure 1 shows the predicted Ether supply and inflation rate by the macro-level simulation, assuming that the Ethereum monetary policy would not be changed in the future years. The parameters are calculated based on the historical data of Ethereum since the last upgrade in March 2019.

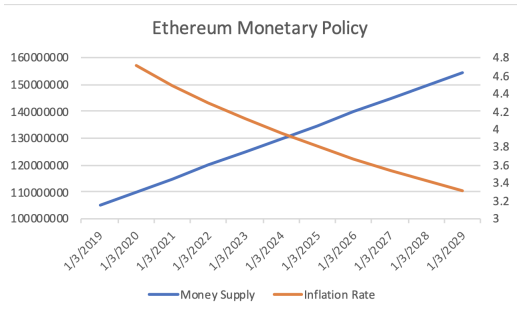

Figure 1: Ether supply and inflation rate predicted by the simulation

3.3 Limitation

The language has certain limitations. The assumption and mechanism of blockchain can not be separated clearly, requiring that the users who would like to understand it to have background knowledge in blockchain, increasing the threshold of the understanding. Another limitation is that not all issuance mechanisms of cryptocurrencies can be modeled into this framework. Some issuance mechanisms are complex, such as stable coins which often rely on two separate coins to control the money supply, making it inappropriate to model them into a simple JSON file.

4 Community Cryptocurrency

In previous sections, we introduced two types of issuing money. The first one is by issuing debts, as it is used in our current monetary system. The second one is by providing resources, as it is used in cryptocurrencies. Community currency offers an alternative method by directly issuing money to its members. It is possible because, within a community, Sybil attacks could be prevented by implementing identity control.

Various forms could be used as support media for a community currency. Blockchain, as a new technology, provides certain advantages: Blockchain ensures that there is no single point of failure, increasing the availability and reliability of the system. Blockchain provides transparency, allowing every user to audit all transactions recorded in the blockchain. Monetary policy is formally written in a smart contract and blockchain ensures it executed correctly. In this report, we define that community cryptocurrency is a type of community currency with blockchain implementation.

4.1 Identity Control

Identity control prevents Sybil attacks. With identity control, we assume that one physical person can only have at most one virtual identity in a community cryptocurrency. The identity control could be achieved by the following methods:

- Community-based Identity Management: Any person who wants to join a community must go through a centralized registration process. Communities can rely on existing national identity documents(e.g. Passport, Driving license) to verify the uniqueness of a person.
- Proof-of-Personhood: a decentralized mechanism that binds physical entities to virtual identities in a way that enables accountability while preserving anonymity[5].

After identity control, each member will receive a public/private key pair. The public key is the virtual identity of the member, while the private key is used to sign transactions.

4.2 Monetary Policy

The monetary policy of a community cryptocurrency is described in a smart contract. A community can launch a new community cryptocurrency by deploying the smart contract into the blockchain. The community needs to establish the monetary policy before deployment, although the monetary policy can be updated in a later stage. Monetary policy can be established from the following three aspects: currency issuance, transaction, and demurrage.

Currency could be issued in two phases. When the smart contract is initialized, the constructor can contain the code for coin distribution. Coins can be equally distributed to every account in the community or can be distributed according to a map indicating the initial balance of each account. After initialization, coins can be issued in two methods. First, coins can be created according to periodic events, such as every hour, or a new block being created. Second, coins can be generated when a new member joins into the community.

The transaction fee can guide the behavior of the community members. Different transactions could have different transaction fee rates. It is expected that high transaction fee discourages transactions while low or zero transaction fee encourages transactions. Regulating the transaction fee is a method to reduce speculation transactions. We propose that, if a transaction is labeled as speculation, a higher transaction fee is charged. Or, the other way around, if a transaction is marked as non-speculation, zero or even lower transaction fee is charged.

Demurrage in community currency is the action of reducing the value of currency in proportion to the time that it is held. Demurrage encourages people to keep circulating currency so as to avoid the loss of value[12]. The most famous example of implementing demurrage-charged community currency took place in the Austrian town Wörgl between 1932 and 1934, resulting that the unemployment rate diminished drastically [11].

4.3 Monetary Policy Language

The monetary policy language is an extended version of the currency issuance language. It could describe not only the currency issuance but also the transaction and demurrage fee. The demurrage feature can be implemented by adding an external function *balance(account)* to get the balance of the account and paying the demurrage fee from the balance accordingly. To include transaction fees, the process of transfer needs to be formalized

in the language. Below is an example of utilizing monetary policy language to describe issuance and transfer in Bitcoin.

```
{
    "events": [{
      "base": "block",
      "period": 1,
      "update": [
        {
          "formula": "50 / (2 ** (Height / 210000))",
          "target": "BlockMiner"
        }
      ]
    }],
    "transfer": {
      "condition": "Value>0 && TransactionFee>0 &&
          balance(Sender)>=Value+TransactionFee",
      "update": [
        {
          "formula": "-Value",
          "target": "Sender"
        },
        {
          "formula": "Value",
          "target": "Receiver"
        },
        {
          "formula": "TransactionFee",
          "target": "BlockMiner"
        }
      ]
    }
}
```

The *transfer* field describes the condition upon which a transfer transaction happens and the balance changes after a transfer transaction. *Height, BlockMiner, Value, TransactionFee, Sender, Receiver* are the variables which need to be provided from the block and the transactions in the block.

4.4 Community Council

A community council is a group of people who have the authority to update the monetary policy and allow new members to join the community. To

reduce the trust to have in a single individual, the system can utilize secret sharing[10]. Each member of the community council receives a share of the private key for updating the smart contract. Any group of t members (out of n) in the community council will be able to do updates and any group of less than t members will not be able to do so.

4.5 Demurrage Implementation

For a currency with paper as its support media, demurrage could be implemented by requiring paying a stamp periodically by the currency holder. With blockchain, the demurrage fee could be charged automatically.

One naive approach to implement the demurrage fee is to update each account's balance periodically. If we set that demurrage fee to be 1% of the total value per month, after one month, each account's value should be reduced by 1%. However, this approach has a high operation cost at the end of each month, possibly causing the blockchain system temporarily unable to respond to other requests.

In a cryptocurrency with the UTXO model, an account's balance is calculated by adding all the UTXOs linked to that account. The demurrage fee could be implicitly charged by reducing the real value of UTXOs. For example, an account has a UTXO with a value of 100 coins. In the first month, it can spend all 100 coins in the UTXO, while in the second month, it can only spend 99 coins in the UTXO. The rest 1 coin is to be the demurrage fee. The value of the UTXO is never changed, but its real value is reduced implicitly. A client software can calculate the real balance of an account by combining the information of UTXOs and current time, without modifying UTXOs explicitly.

Bitcoin can implement a demurrage feature with a hard fork. The demurrage period can depend on the blocks generation. Roughly 4320 blocks represent a one-month interval, with the assumption that on average every 10 minutes a new block will be found. As the security of Bitcoin depends on the financial gains of the miners, when the block reward of bitcoin becomes too small in the future, it might influence the security of bitcoin as a whole. Demurrage can help this situation. Collected demurrage fees could be used as a source for future block rewards so that Bitcoin can be secured without creating new coins.

Another common model in cryptocurrency is the global balance model. In this model, each address is associated with a value representing the balance of this account in a database. The naive approach in which the software updates each account's balance at the end of each month requires O(N) time for charging demurrage fees and O(1) time for updating balances after a transaction. The similar trick in the UTXO model can also apply here to improve efficiency. At the end of each month, the real balance of every account is reduced for the demurrage fee, while the value of balance in

the database remains unchanged. The value of an account's balance in the database is updated to represent the real balance only when this account receives or spends coins. An account's real balance can be calculated from the value of the balance in the database and the last-updating timestamp of this value.

4.6 Application

4.6.1 Universal Base Income

Universal base income could be implemented by utilizing a community currency. Two basic problems are needed to be solved. In order to maintain a fair system, preventing Sybil attacks is important. This can be solved by deploying identity control. Another issue is the source of funding for the universal base income. Demurrage could help with providing funding by taxing all coins holders. The following JSON code describes a simple universal base income scheme:

```
{
  "base": "month",
  "period": 1,
  "update": [
    {
        "times": "len(Members)",
        "formula": "-balance(Members[i])*0.01+1000",
        "target": "Members[i]"
    }
  ]
}
```

In this community currency, every member of the community would receive 1000 coins as monthly base income. At the same time, a monthly 1% demurrage fee is charged for every account (*balance(account)* is a function that returns the balance of the account). Therefore, in each month, 1% of the total currency supply is paid for the demurrage fee. Initially, the demurrage fees partially fund the base income payments, and when the total currency supply reaches 100*1000*len(Members), all the base income payments are funded by the demurrage fees.

Apart from funding the base income payments, demurrage here can help to reduce the gap between the rich and the poor. Although it is the same demurrage rate for every member, rich people would pay more for the demurrage fee. Also, those who care about the demurrage, which usually are poor people, have the incentive to use their coins before the demurrage

deadline to avoid demurrage fee. Both can relieve the inequality problem within the community.

4.6.2 Mutual Credit

In a mutual credit system, the currency is issued by a simultaneous debit and credit between participants in a transaction[7]. Any debt is the income of other members in the system, and therefore the total sum of all balance is zero. Similar in the universal base income system, identity control is vital in the mutual credit system. Only members of the community are allowed to have credit balance and to trade with other members. The community council is responsible to set the limits (positive and negative), and any member whose balance exceeds the limits is obliged to move his balance back towards zero by spending or earning. A mutual credit system can be described by a simple JSON file with restrictions on transfer transactions:

```
{
    "condition": "Value>0 && balance(Sender)-Value>=
        negative_limit(Sender) && balance(Receiver)+Value<=
        positive_limit(Receiver)",
    "update": [{
            "formula": "-Value",
            "target": "Sender"
        },
        {
            "formula": "Value",
            "target": "Receiver"
        }
    ]
}
```

The *condition* field describes the condition in which a transfer transaction is allowed to make sure that both balances of the sender and receiver do not exceed the limits set by the community council. *negative_limit(account)* and *positive_limit(account)* are two functions that return the negative and positive limit separately. The *update* field describes the changes in the balances after the transaction.

4.6.3 Information Sharing

The idea of community currency can also apply to non-currency applications. In information sharing platforms, if Sybil attacks are not prevented, bots can automatically create countless accounts and spams. Below is an example of using the community currency to prevent spamming.

```
{
    "transfer": {
        "condition": "Value>=1 && balance(Sender)>=Value",
        "update": [{
            "formula": "-Value",
            "target": "Sender"
        }]
    },
    "events": [{
        "base": "day",
        "period": 1,
        "update": [{
            "times": "len(Members)",
            "formula": "-balance(Members[i])+10",
            "target": "Members[i]"
        }]
    }]
}
```

The purpose of coins here is to have an upper limit of posts that each member can publish. A member has to use at least one coin when he wants to publish a post. If he decides to use more than one coin to publish a post, the number of coins associated with the post could indicate its priority. Each day, the 100% demurrage fee is applied to each account and 10 coins are given equally to every account, meaning that each member can at most publish 10 posts per day. When a member wants to publish a post, she needs to inserts the hash of the post into the transaction as proof, and at least burn one coin in that transaction.

5 Conclusion

Our monetary system is not perfect. The increasing debts and rising asset prices are risk factors for a financial crisis, even though now we have the most advanced technology and economic theory in human history.

Cryptocurrency offers new hope, allowing us to build a monetary system from button up in a decentralized, transparent and democratic way. However, we are still in a very early stage. With the currency issuance language and the simulation framework, the monetary policy is formally described and simulated, helping economists to better understand and analyze the monetary policy. Community cryptocurrency provides a method of issuing currency based on physical persons. It can be used to implement universal

base income, mutual credit system, and even in non-currency domain like spamming prevention system.

References

[1] https://www.bankofengland.co.uk/monetary-policy/inflation.

[2] https://github.com/antonmedv/expr.

[3] Fredrik NG Andersson et al. Monetary policy, asset price inflation and consumer price inflation. *Economics Bulletin*, 31(1):759–770, 2011.

[4] Simon Barber, Xavier Boyen, Elaine Shi, and Ersin Uzun. Bitter to better—how to make bitcoin a better currency. In *International Conference on Financial Cryptography and Data Security*, pages 399–414. Springer, 2012.

[5] Maria Borge, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, and Bryan Ford. Proof-of-personhood: Redemocratizing permissionless cryptocurrencies. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 23–26. IEEE, 2017.

[6] Jon Hilsenrath, Serena Ng, and Damian Paletta. Worst crisis since '30s, with no end yet in sight. *The Wall Street Journal*, 18, 2008.

[7] Bernard Lietaer and Gwendolyn Hallsmith. Community currency guide. *Global Community Initiatives*, pages 1–32, 2006.

[8] Michael McLeay, Amar Radia, and Ryland Thomas. Money creation in the modern economy. *Bank of England Quarterly Bulletin*, page Q1, 2014.

[9] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot, 2019.

[10] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[11] Christian Thiel. Complementary currencies in germany. *International journal of community currency research [Special Issue]*, pages 17–21, 2011.

[12] David Vandervort, Dale Gaucas, and Robert St Jacques. Issues in designing a bitcoin-like community currency. In *International Conference on Financial Cryptography and Data Security*, pages 78–91. Springer, 2015.