Decentralized Monetary Policy for Cryptocurrencies

Alon Shtaierman
Decentralized Monetary Policy for Cryptocurrencies

Research Thesis

Submitted in partial fulfillment of the requirements for the degree of Master of Science in Computer Science

Alon Shtaierman

Submitted to the Senate of the Technion — Israel Institute of Technology
Nisan 5779 Haifa April 2019
This research was carried out under the supervision of Prof. Eli Ben-Sasson and Prof. Yuval Ishai, in the Faculty of Computer Science.

The contents of this thesis were presented at CESC2018

Acknowledgements

I would like to thank my advisors, Prof. Eli Ben-Sasson and Prof. Yuval Ishai, for their professional and personal guidance, for sharing their vast knowledge, and for their unyielding support.
And I would like to thank my parents; for sacrificing so much so that I could achieve my goals in life, and for making me the man I am today.

The generous financial help of the Technion is gratefully acknowledged.
Contents

List of Figures

Abstract 1

1 Introduction 3

2 Inflation and Deflation 7

3 Economic Systems 9
  3.1 Goods and Services 9
  3.2 Money Supply 10
  3.3 Agents 10
  3.4 Purchasing Power 11
  3.5 Proof of Claim 12

4 Spring Cleaning 13
  4.1 Redistribution Scheme 13
  4.2 Incentive Compatibility 14
  4.3 Miner Compensation 15
  4.4 Spring-Cleaning Frequency and Termination 19
  4.5 Error Margin 20

5 Stablecoins 21
  5.1 Off-Chain Collateralized 22
  5.2 On-Chain Collateralized 22
  5.3 Seigniorage Shares 23

6 Related Work 25

7 Conclusions 29

Hebrew Abstract i
List of Figures

4.1 Miner’s Dilemma .................................................. 15
4.2 Extended Miner’s Dilemma ............................... 16
4.3 Possible Relation of $t \cdot \frac{x_a}{M - l - t}$ for a given Miner .......... 17
4.4 Perceived Lost Coins Over Time .............................. 19
Abstract

The rapid increase in the popularity of cryptocurrencies brought with it not only questions regarding the quality of the technology itself, but also the economic phenomena surrounding them. Bitcoin in particular has proven itself to be a very volatile commodity [Baek and Elbeck, Applied Economics 2015], and a poor currency, according to the definition of money [Kocherlakota, Journal of Economic Theory]. This has given rise to numerous alternative cryptocurrency models, which set about to improve upon their roles as a currency. One inherent problem presented by fixed-capped cryptocurrencies, such as Bitcoin, is that of lost-coins. Lacking a private-key restoration scheme, it is impossible to transfer funds out of an electronic wallet upon losing its private key. Since fixed-capped cryptocurrencies impose a strict monetary policy, by which the ultimate amount of coins in circulation is preset at a constant value, the phenomenon of lost coins has a debilitating effect on the system, effectively reducing the number of actual coins in circulation over time. In this paper, we introduce the problem and possible solutions that allow lost coins to be recirculated into the system, in a way that doesn’t violate its security.
Chapter 1

Introduction

Many crypto-currencies enforce a rather strict monetary policy; setting a predetermined fixed cap on the total amount of coins that will enter circulation. This is usually done in order to maintain artificial scarcity, so the coin’s value does not depreciate. Bitcoin, in particular, is set to cap at 21,000,000 coins. From an economic standpoint this poses an interesting question regarding the future of fixed-capped crypto-currencies such as Bitcoin. Kinesian economists would argue that such currencies have a deflationary nature because they are incapable of adjusting to surges of demand [SS17], while advocates would argue that deflation is good; since when the coin appreciates in value everyone becomes richer.

Stability is important because of the three functions that are a necessary prerequisite for any coin to be accepted as a currency: store-of-value, medium-of-exchange, and unit-of-account.

Store-of-value refers to the currency’s ability to retain its value over time. It is important to note that while most fiat currencies that exists nowadays normally suffer from some loss of value due to targeted inflation they do not violate this function due to the fact that the rate of inflation is controlled by the centralized governing entity, and is transparent to all participants within the system. Thus when all the participants are aware of the inflation and its rate they can account for the value-loss over time, and pseudo-stability is maintained. Medium-of-exchange measures how widely accepted a given currency is as a buffer between exchanges. Ideally currencies should be non-consumable, long-lived, fungible and devoid of intrinsic utility. Thus any interest to hold onto a coin should be solely for the purpose of future trade. It is important to note that as such, without maintaining store-of-value, a given coin wouldn’t maintain its status as a medium-of-exchange for very long. Unit-of-account refers to the ability to measure the value of goods and services with units of the given currency. As before, if store-of-value is violated then unit-of-account cannot be upheld, as the coin’s volatility would make it impossible to reliably measure value.

Generally, most modern central authorities who issue fiat currencies as legal-tender devise a dynamic strategy in order to maintain these functions, since fiat currency has no
inherent value or utility. This strategy is commonly referred to as a monetary-policy. While monetary policy can defer from one country to another, there usually are many similarities in regards to the thresholds which prompt a change in policy, and the possible actions the central authority can then take to react. Often the central authorities attempt to evaluate the rate in which their currency appreciates or depreciates in value against the available goods and services, this is referred to as inflation or deflation.

In a given economy, inflation represents a decrease in the purchasing power of the currency, due to an increase in the money-to-goods ratio. Conversely, deflation is an increase in the purchasing power of the local currency, due to a decrease in that ratio.

The challenge of devising a contemporary monetary policy for crypto-currencies has been gradually gaining more attention over the past few years. In particular, we are interested in researching decentralized monetary policies. Such mechanisms should achieve the goal of coin stability for a crypto-currency, without jeopardizing its the trust-less security guarantees. Decentralization means that agents within the system must come to a consensus regarding the current value of the crypto-currency, and the appropriate steps that must be taken accordingly. This becomes tricky when considering that many agents may have incentives to spread misinformation in the system for personal gain. If the truth about the coin’s value cannot be reliably ascertained, then the monetary policy will inevitably fail to maintain stability. Thus, we consider incentive-compatible mechanisms as a crucial backbone of such systems. Incentive-compatible mechanisms ensure that it is in every agent’s best self-interest to align themselves with the suggested protocol, thus acting as a counterpart to regulation in centralized systems.

As an interesting case study into one facet of decentralized macro-economic mechanisms we chose to explore the problem of lost crypto-currency. Currency which is lost or destroyed is a deflationary factor - as it poses an effective decrease of the overall money in circulation. For example; governments often approximate how much paper money was lost per year in order to decide how much more money to reprint.

In crypto-currencies such as Bitcoin, lost coins are represented by the sum total of balances held by wallets whose private keys are no longer attainable by any user within the system. This can occur whenever a user loses a private key linked to one of their wallets, either intentionally or unintentionally [You18], and it is important to note that such a user is thereafter indistinguishable from one which never owned the wallet to begin with. The end result is that, in fixed-cap crypto-currencies, the total amount of coins in circulation will often be effectively lower than the intended cap [Han13]. Without restoration schemes, one can argue that at $t = \infty$ the real amount of coins in circulation can effectively aspire to 0.

Schemes that revolve around private-key restoration exist but they always introduce the risk of theft, and usually involve the use of a third party which somewhat defeats the purpose of a trust-less distributed payment system. In this paper we address the problem of lost coins in a crypto-currency-based economy similar to Bitcoin, and propose a distributed mechanism to reintroduce lost coins into circulation without the
need for key-restoration. As a consequence of this usually the original owners of the lost currency are not fully-reimbursed, if at all, and we strive to explain how the coin reenters circulation in a way which does not incentivize exploitation. In order to support the proper incentives, we propose that the system periodically runs spring-cleaning cycles, during which all agents are required to provide proof that they have access to their accounts. Thus, by process of elimination, lost coins are gradually revealed to the system. At the end of this phase, all coins which were not claimed are considered lost, and are then redistributed proportionally among the agents.

A similar idea was proposed by Gjermundrød and Dionysiou[GD14], but their system sought to redistribute lost coins among the miners alone. This redistribution scheme would not suffice to our end, since it would wrongly incentivize a rational miner to censor an agent’s attempt to prove claim over their funds for the promise of greater redistribution rewards. We show that by proportional redistribution, agents are properly encouraged to provide proof for their claims (whenever possible), while miners are incentivized to include these proofs in the public ledger.

Our main contribution is an incentive-compatible solution to the problem of lost cryptocurrency recirculation.

In chapter 2 we begin by outlining a motivation into the nature of the problem of lost crypto-currencies, and why it is important.

In chapter 3 we define a formal framework which simplifies the structure of economic systems, which we later use to prove some attributes of our suggested mechanism.

In chapter 4 we present our mechanism, along with its two primary components proof-of-claim, which is the way by which agents in the system indirectly reveal lost currency, and spring-cleaning, which describes when actions must be taken in order to restore lost coins into the system, and how.

In chapter 5 we return to the more general problem of decentralized monetary-policy by exploring the proposed mechanisms of crypto-currencies which attempted to tackle this issue, dubbed collectively as Stablecoins.

Our results show that a feasible solution to the problem of lost crypto-currency exists, achieving a decentralized solution which we prove is incentive-compatible.
Chapter 2

Inflation and Deflation

Inflation is a macro-economic phenomenon which describes a rising change in prices for most goods and services in an economy. When this happens, standards of living decline. That’s because each coin buys less, so any agent has to spend more money for the same amount of goods and services that coin used to purchase. Economists theorize that, if inflation is mild, it can actually spur further economic growth. If prices rise slowly and gradually, it can encourage people to buy now and avoid future price increases. This increases demand, driving further economic growth. Thus, many countries aim for a low inflation rate.

Contrary to this, deflation is the negative change in prices for goods and services in the economy. When this happens, prices of goods and services decline, meaning each coin can purchase more than it used to. This can lead to an increase in living standards when the deflation rate is mild, and economists are split on whether this is good for an economy. As inflation can motivate people to spend more at present, deflation motivates hoarding: Why spend a coin now when you can hold onto it for a while and see it appreciate in value? This leads some economists to theorize that higher rates of deflation can lead to deflationary-spirals and recessions [SS17].

Be that as it may, uncertainty about the money base, which is a situation in which two or more agents are split in their opinion about the amount of currency in circulation, is detrimental to the stability of the system, as it violates the currency’s usage as a medium of exchange. In large economic systems, such as countries, this certainty comes from trust in the central authority, and there are many cases in which violations of said trust lead to catastrophic economic crises. In decentralized systems such as Bitcoin, it might seem natural to believe that such certainty is guaranteed by the protocol, since the entire information is transparent on the ledger. However, there is no way for the average user to know exactly how many Bitcoins are effectively lost to the system, therefore, the amount of actual coins in circulation remains a matter of speculation, as prices drop and soar by hundreds of percents every month.
Chapter 3

Economic Systems

In order to explain concepts such as purchasing power, transactions and exploitation, which are necessary to argue the importance of a coin-restoration mechanism, we propose a simplistic and rational model which encompasses the primary factors of an economic system, such as goods and services, money supply, agents, etc.

The economic system is defined by the many components which compose it, and is designed as a "game" in which each participant’s goal is to maximize their own assets, either by owning more goods and services, or increasing their purchasing-power (defined below).

For simplicity we assume all participants are rational agents, but their knowledge of the system itself isn’t perfect. The asymmetry in knowledge is imperative to argue the negative effects of deflation in such an economic system, and thus emphasize the need for a coin-restoration mechanism.

The economic system is comprised of goods and services, money supply, agents and associated functions, all of which are explained in this section.

3.1 Goods and Services

Broadly speaking, goods and services represent the aggregation of all the available resources in the economic system. Goods can be material or otherwise, such as land, food, or intellectual properties. Services generally refer to manpower, in the form of the available work for hire. As such the total available goods and services in an economic system can be denoted as a set $T$.

Another important distinction is that goods and services have value projected by their utility. This is unlike money, which ideally has no utility (beyond the marginal utility of its usage as a store-of-value and a medium-of-exchange). This is why it is prudent to discuss the game in terms of purchasing-power, as the agents’ only incentive to hold money over goods and services is derived from their ability to use that money as a non-consumable, non-decaying way to acquire goods and services at a future time.

For simplicity we assume there is a known and measured correlation between the value
and utility of a given good or service, and therefore in order to simplify the discussion of purchasing power we assign each good or service value using a function $v : T \rightarrow R^+$. In order to describe the total value of the entire set of goods and services, we expand the function to apply for sets of goods and services as well, such that for a given subset $T' \subseteq T$:

$$v(T') \triangleq \sum_{t \in T'} v(t) \quad (3.1)$$

### 3.2 Money Supply

The money-supply, denoted as $M$, represents the sum total of all currency in the economic system. At a point in time, given a set of goods and services, the value of the entire money supply should be equal (proportionally) to the available amount of goods and services. As such a change in the money supply does not generate additional wealth - but rather dilutes the value of a single unit of currency in the system such that if the sum total of all goods and services is represented by $T$ then a single unit should be proportionally worth $c = \frac{v(T)}{M}$. If the money supply is changed by $\epsilon$ units of currency, then each individual unit’s value should change accordingly:

$$c' = \frac{v(T)}{M + \epsilon} \quad (3.2)$$

This equation represents both the decrease in the coin’s value (or purchasing-power) if $\epsilon$ is positive ($c' < c$), and an increase in the coin’s value vice-versa ($c' > c$).

### 3.3 Agents

Agents represent the entities participating in the economic system. Every agent controls an amount of currency out of the money supply (between 0 and $M$), and a certain amount of goods and services which they bring to the table. We denote an individual agent as $a$ or $a_i$, and the amount of currency they control respectively as $x_a$ or $x_{a_i}$ (We call this agent a’s account). We represent the entire set of agents in our system as $A = \{a_1, ..., a_N\}$. For simplicity we assume that the number of agents $N$ is fixed and finite.

The economic system should maintain:

$$\sum_{i=1}^{N} x_{a_i} = M \quad (3.3)$$

Similarly, every agent also exerts control over some goods they own and services they provide to the economic system, denoted $t_{a_i}$. For simplicity we assume the goods and services are partitioned among the agents, such that every good and service is owned by one agent, and one alone. As such, the available goods and services in the economic
system are directly influenced by the participating agents, each bringing to the system the goods they own and the services they can provide. As such the economic system should also maintain:

\[ \bigcup_{i=1}^{N} t_{a_i} = T \]  

(3.4)

To maintain the economic system, an increase in the money supply has to be reflected by a change in the agents’ accounts. This increase can be represented by a subset of agents receiving newly minted coins. Alternatively a decrease can represent a subset of agents which lose a sum of their currency. In either case a change in the money supply represents a change in the equilibrium of the system. for simplicity we’ll assume new money must always enter/leave circulation via an existing subset of the set of all agents \( A \).

Thus, we denote the subset of agents through which the change in the money supply was introduced as \( A' \subseteq A \), where the complement set is \( A' = A \setminus A' \). If the money supply was changed by \( \epsilon \) then we denote each agent’s \( a \)’s individual change by \( \epsilon_a \) s.t. \( \sum_{a \in A'} \epsilon_a = \epsilon \).

### 3.4 Purchasing Power

Purchasing power is generally defined as the financial ability to buy goods and services. This means that the purchasing power of the entire money-supply should be proportional to the sum total of goods and services. We denote purchasing power of a given agent \( a \) as a function \( P_p(a) \). In a given state (of money supply \( M \) vs a constant supply of goods and services \( T \)) \( P_p(a) \) should maintain:

\[ P_p(a) = x_a \cdot c = x_a \cdot \frac{v(T)}{M} \]  

(3.5)

Given the entire set of agents in our economic-system \( A = \{a_1, ..., a_N\} \) then \( P_p \) should maintain:

\[ P_p(A) = \sum_{i=1}^{N} P_p(a_i) = \sum_{i=1}^{N} x_{a_i} \cdot c = \sum_{i=1}^{N} x_{a_i} \cdot \frac{v(T)}{M} = \frac{v(T) \cdot \sum_{i=1}^{N} x_{a_i}}{M} = \frac{v(T) \cdot M}{M} = v(T) \]  

(3.6)

In other words, when considering the collective purchasing power of all agents within the system, it should amount in value to that of all goods and services. In essence an agent’s purchasing power can be thought to represent their respected share of the ”pie” of wealth, represented by their share of the money-supply. We assume that, rationally, an agent’s primary incentive is always to maximize their purchasing power. When the money-supply is constant, this incentive is directly translated to a desire to increase the amount of currency the agent controls. The important distinction is that when the money supply changes these desires aren’t necessarily aligned. We also note that as the
supply of goods and services changes this also globally affects each agent’s purchasing power (this is where inflation/deflation comes into play).

We note that if in a given moment in time the money-supply changes by $\epsilon$ then each agent’s purchasing power changes accordingly:

$$P_p(a) = x_{a_i} \cdot \frac{v(T)}{M}$$  \hspace{1cm} (3.7)

$$\hat{P}_p(a) = \begin{cases} 
(x_a + \epsilon_a) \cdot \frac{v(T)}{M + \epsilon} & \text{if } a \in A' \\
x_a \cdot \frac{v(T)}{M + \epsilon} & \text{if } a \in \hat{A}' 
\end{cases}$$  \hspace{1cm} (3.8)

### 3.5 Proof of Claim

Since the difference between an agent who lost access to their wallet and an agent that never owned the wallet to begin with is practically non-existent, the only reasonable alternative is to identify lost coins by process of elimination. As mentioned, it can be difficult to distinguish between coins which are being hoarded by a certain agent, and those which are lost to the system, since neither are included in any transaction for a prolonged period of time. The main difference lies in the agent’s ability to create a valid transaction from a given wallet, by use of its associated private-key. As such, any valid transaction serves as an implicit proof of claim for the contents of the given wallet, as it shows without a doubt that the instigating agent hasn’t lost his private key up to that moment.

By regularly and correctly encouraging agents to generate transactions in the system, if only for the sake of proving that they are able to, the coins which are not claimed after enough time can be considered lost to the system, and promptly redistributed accordingly. We call this concept *Proof of Claim* or *PoC*, and a transaction which is only generated for the sake of *Proof of Claim* a *PoC transaction*. A *PoC transaction* is similar to a regular transaction, but enables a given agent to play both the sender and the receiver of the funds within. Its sole purpose is to serve as proof that the agent is capable of producing a valid private key to sign a transaction from the wallet, and thus that they have claim on the funds within. Fees are still imposed on the transaction, necessary to assure its inclusion in the public ledger, and in the next section we argue that a rational agent will always opt to produce a valid *PoC transaction*, as the alternative would be to forfeit the associated coins.
Chapter 4

Spring Cleaning

Generally speaking, there is no reason for agents to provide PoC for their funds (other than those which occur naturally as a result of an actual transaction within the system). Therefore sufficient incentive must be given to agents to produce PoC for their funds in order to recognize lost coins within the system.

In order to enforce such incentive, we propose that every set amount of time the system will run a spring-cleaning phase, during which all agents are required to provide PoC for their wallets. At the end of this phase, all coins held by unclaimed wallets are considered lost to the system, and are then redistributed proportionally among the agents.

A similar idea was proposed by Gjermundrød and Dionysiou [GD14], but their system sought to redistribute lost coins among the miners alone. This redistribution scheme would not suffice to our end, since it would wrongly incentivize a rational miner to censor any agent’s PoC transaction for the promise of greater rewards via redistribution. In our solution we show that redistributing lost coins proportionally to each agent’s account provides sufficient incentive for them to produce PoC for their wallets.

4.1 Redistribution Scheme

Considering every agent’s primary goal is to maximize their purchasing power, we propose that at the end of the spring-cleaning phase the total amount of coins which are perceived as lost (denoted $\epsilon_P$) will be redistributed among the agents proportional to their claimed funds. So, if agent $a$ produced PoC for $x_a$ currency, they should receive

$$\frac{x_a}{M - \epsilon_P} \cdot \epsilon_P$$

coins from the redistribution.

Thus, if agent $a$ had a purchasing power of $P_p(a) = \frac{x_a \cdot V(T)}{M}$ prior to the spring-cleaning, then after the lost coins are redistributed their new purchasing power holds:

$$\hat{P}_p(a) = (x_a + \frac{x_a}{M - \epsilon_P} \cdot \epsilon_P) \cdot \frac{V(T)}{M}$$  \hspace{1cm} (4.1)
Assuming coins which are proclaimed as lost after the spring-cleaning is over are no longer usable, this means the money supply in the system will never exceed the $M$ value. Furthermore, since the amount of money an agent is liable to get via redistribution depends on the amount of coins they have provided with PoC during the spring-cleaning phase, and any coins which the agent doesn’t claim are considered lost and redistributed, constituting a loss for an agent who was their last owner, this should incentivize most agents to provide valid PoC for their coins in the spring-cleaning phase.

### 4.2 Incentive Compatibility

An economic system which is incentive compatible is such that every agent achieves the best outcome for themselves simply by acting according to the desired protocol. As established, assuming every rational agent seeks to maximize their purchasing power, we seek to show that it is in each agent’s best interest to provide PoC for all their transaction.

In order to prove this, consider an agent $a$ owning $x_a$ coins. During the spring-cleaning phase they can choose $\delta \in [0, 1]$ fraction of their coins to declare. As any coins which are not declared are then lost to the agent and redistributed, they stands to lose $(1 - \delta)x_a$ coins. We denote any other lost coins in the system as $l$, such that if the total amount of coins which is regarded as lost at the end of the spring-cleaning period is $\epsilon_P$ then $\epsilon_P = l + (1 - \delta)x_a$.

Thus we come by the following theorem:

**Theorem 4.1.** The strategy which maximizes agent $a$’s purchasing power after spring cleaning is declaring $\delta = 1$ factor of their account $x_a$

**Proof.** The agent’s new purchasing power after spring-cleaning is described by the following equation:

$$
\hat{P}_p(a) = c \cdot \left( \delta \cdot x_a + \frac{\delta \cdot x_a}{M - l - (1 - \delta)x_a} \cdot (l + (1 - \delta)x_a) \right) \tag{4.2}
$$

$$
= c \cdot \left( \frac{\delta \cdot x_a}{M - l - (1 - \delta)x_a} \cdot (M - l - (1 - \delta)x_a) \cdot (l + (1 - \delta)x_a) \right) \tag{4.3}
$$

$$
= c \cdot \left( \frac{\delta \cdot x_a \cdot (M - l - (1 - \delta)x_a + l + (1 - \delta)x_a)}{M - l - (1 - \delta)x_a} \right) \tag{4.4}
$$

$$
= c \cdot \left( \frac{\delta \cdot x_a \cdot M}{M - l - (1 - \delta)x_a} \right) \tag{4.5}
$$

We want to show that the best possible result for $a$ (i.e. - maximum purchasing power) is achieved by choosing $\delta = 1$, so we derive the purchasing power function by $\delta$:.
\[
\frac{d}{d\delta} P^p(a) = c \cdot \left( \frac{(x_a \cdot M (M - l - (1 - \delta)x_a) - \delta x_a \cdot M \cdot x_a)}{(M - l - (1 - \delta)x_a)^2} \right)
\]
\[
= c \cdot \left( \frac{(x_a \cdot M^2 - x_a \cdot M \cdot l - x_a^2 \cdot M + \delta x_a^2 \cdot M - \delta x_a^2 \cdot M)}{(M - l - (1 - \delta)x_a)^2} \right)
\]
\[
= c \cdot \left( \frac{x_a \cdot M \cdot (M - l - x_a))}{(M - l - (1 - \delta)x_a)^2} \right)
\]

Since \( M > l + x_a \geq 0 \) the derivative of the purchasing power is a monotonically increasing function of \( \delta \in [0, 1] \), and thus the maximum value is attained by choosing \( \delta = 1 \). Therefore, it is in each rational agent’s best interest to claim the maximum coins he is able to during the spring-cleaning phase.

4.3 Miner Compensation

Since the spring-cleaning phase still requires the use of the public ledger to document the PoC transactions, the miners are required to include these transactions in the public ledger during this time period. As such, transaction fees still need to apply to PoC transactions, in order to provide adequate compensation for miners to include them in the blockchain.

For simplicity we assume some constant value \( f \) denotes the standard fee for a given transaction. Thus any miner \( a \) which records a PoC transaction for \( t \) funds is faced with the decision to either include it in their block and reap the reward from its associated fee, or censor it, in the hopes of receiving more coins via redistribution when the spring-cleaning phase ends.

<table>
<thead>
<tr>
<th>Decision</th>
<th>Include</th>
<th>Censor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reward</td>
<td>( f )</td>
<td>( t \cdot \frac{x_a}{M - l - t} )</td>
</tr>
</tbody>
</table>

Figure 4.1: Miner’s Dilemma

Where \( M \) is the money supply and \( l \) is the true amount of lost coin (or the amount of lost coin which the miner perceives). We note that since the amount of effective money in circulation is \( M - l \) then no transaction can prove claim for more than that
amount, thus: \( t < M - l \). Therefore, to we observe that:

\[
\begin{align*}
t \cdot \frac{x_a}{M - l - t} & > f \\
\Downarrow & \\
t \cdot x_a & > M \cdot f - l \cdot f - t \cdot f \\
\Downarrow & \\
t \cdot (x_a + f) & > (M - l) \cdot f \\
\Downarrow & \\
t & > (M - l) \cdot \frac{f}{x_a + f}
\end{align*}
\]

By this comparison it would seem that any PoC transaction which provides claim for more than \((M - l) \cdot \frac{f}{x_a + f}\) coins would be censored by any rational miner. However, if we consider all other miners as an opposing player, we come to this extended table which is similar to the prisoner dilemma (where \(p\) is the proportion of mining power of miner \(a\)):

<table>
<thead>
<tr>
<th>Opponents</th>
<th>Include (f \cdot p)</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include</td>
<td>(f)</td>
<td>(t \cdot \frac{x_a}{M - l - t})</td>
</tr>
</tbody>
</table>

**Figure 4.2:** Extended Miner’s Dilemma

We attempt to prove that any rational miner should always opt to include a given transaction rather than censoring it, thus maintaining incentive compatibility within the system. We present this in a similar way to the standard prisoner dilemma, showing that some miner’s have a Nash-equilibrium, where their decision is independent of their opponents’, and always results in inclusion being preferable to censorship. Then we show that for miner’s who have an in-equilibrium, the existence of the former agents also compels them to opt to include. One key observation is that miners who have smaller accounts have less interest to censor, since their expected reward from redistribution is proportional to the PoC they can produce for their own account.

Thus, we had to make some working assumptions in order to come by a reasonable proof, as presented by the following theorem:

**Theorem 4.2.** Assuming accounts are anonymous and independent of potential mining power, every miner has some mining power, but no miner has absolute power, and the spring-cleaning phase runs long enough such that every miner has a high probability of including at least one block during that time period, then every rational miner’s most lucrative strategy is to include every given transaction.
Proof. As presented by the table, any miner who attempts to censor a transaction runs the risk of receiving no reward, if any other miner has included in their stead. Since every miner has some mining power, but no miner has absolute power, it follows that $0 < p < 1$, and so $f > f \cdot p > 0$.

Since the potential reward for censoring a PoC transaction is dependent on the amount of funds $t$ and the miner’s own account $x_a$, each miner might perceive a different equilibrium: Either $f > f \cdot p \geq t \cdot x_a M - l - t \geq 0$, or $f \cdot x_a M - l - t \geq f \cdot p > 0$, or $t \cdot x_a M - l - t \geq f > f \cdot p > 0$. We illustrate these scenarios in the following graph:

![Figure 4.3: Possible Relation of $t \cdot \frac{x_a}{M - l - t}$ for a given Miner](image)

Particularly, we separate these into two distinct scenarios depending on a given miner’s view of the value of $t \cdot \frac{x_a}{M - l - t}$: If $t \cdot \frac{x_a}{M - l - t} > f$ we denote this as Scenario I and in all other cases we denote this as Scenario II.

In order to analyze the miner’s optimal strategy we look at the expected rewards based on their decision against the opponent miners. We present the miner’s strategy as a random variable $X \in \{0, 1\}$, where 1 represents the decision to include the PoC transaction, and 0 represents the decision to censor. Similarly, we present the opponents’ strategy as a random variable $Y \in \{0, 1\}$. We denote the miner’s expected reward as $z$, such that:

$$z = f \cdot P(X = 1, Y = 0) + (f \cdot p) \cdot P(X = 1, Y = 1) + 0 \cdot P(X = 0, Y = 1) + ... + (t \cdot \frac{x_a}{M - l - t}) \cdot P(X = 0, Y = 0)$$

For simplicity we denote the rewards for different strategy combinations as $A = f$, $B = t \cdot \frac{x_a}{M - l - t}$, $C = f \cdot p$, $D = 0$ and so:

$$z = A \cdot P(X = 1, Y = 0) + C \cdot P(X = 1, Y = 1) + B \cdot P(X = 0, Y = 0) + D \cdot P(X = 0, Y = 1)$$

From the miner’s perspective, inclusion (or $X = 1$) is only preferable if the expected rewards are higher than the alternative. The strategy formula is then:

$$A \cdot P(Y = 0) + C \cdot P(Y = 1) > B \cdot P(Y = 0) + D \cdot P(Y = 1)$$
Since each side of the inequality presents a given strategy for $X$, we simplify the probability function $P$ by only referring to the rival strategy $Y$.

In order to examine what effect the rival’s strategy has over the miner, we denote $\rho = P(Y = 1)$ (and so $1 - \rho = P(Y = 0)$), and isolate it in the inequality:

$$A \cdot (1 - \rho) + C \cdot \rho > B \cdot (1 - \rho) + D \cdot \rho$$

$$\downarrow$$

$$(A - B) \cdot (1 - \rho) > (D - C) \cdot \rho$$

$$\downarrow$$

$$(A - B) - (A - B) \cdot \rho > (D - C) \cdot \rho$$

$$\downarrow$$

$$A - B > (A - B + D - C) \cdot \rho$$

The final result depends on the value of $A - B + D - C$:

$$\begin{cases} 
\frac{A - B}{A - B + D - C} > \rho, & \text{if } A - B + D - C > 0 \\
\frac{A - B}{A - B + D - C} < \rho, & \text{if } A - B + D - C < 0 
\end{cases}$$

In Scenario II, where $f > t \cdot \frac{x_a}{M - I - t}$ (or in other words, $A > B$) it is easy to see that the miner’s best interest is always to include the transaction, since no matter the value of $0 \leq \rho \leq 1$ the rewards for inclusion far exceed it, meaning their decision is independent of any opponent. We call these Nash miners, appropriately.

Miners who perceive Scenario I, however, find themselves in a Nash in-equilibrium since $t \cdot \frac{x_a}{M - I - t} > f$. Thus, they must rationally consider every opponent’s decision when formulating their own, therefore the value of $\rho$ can no longer be neglected as with Scenario II. For these miners the solution to the strategy equation is always

$$\frac{A - B}{A - B + D - C} < \rho$$

since $A - B + D - C < 0$ (This is because in Scenario I it holds that $B > A > C > D$). Therefore, these miners should rationally only consider opting to censor if $\frac{A - B}{A - B + D - C} > \rho$.

Assuming the miner’s accounts are anonymous means that a given miner cannot know the sizes of accounts the opponent miners hold and thus how honest they are inclined to be (since the account size directly influences the size of the censor reward $B$). Furthermore, since we assume the sizes of accounts are independent of the miner’s potential mining power, this means that miners cannot predict the power Nash miners have in the system, and therefore how likely they are to produce blocks. Further assuming
that the spring-cleaning phase lasts long enough so that even small miners have a good chance to include a block means that \( \rho \approx 1 \), and therefore even miners who are not Nash miners are inclined to choose to include transactions, since the risk the Nash miners pose is too great.

\[ \blacksquare \]

### 4.4 Spring-Cleaning Frequency and Termination

Spring cleaning can either be put to a majority vote within the system, or, more simply, have it occur at regular intervals (i.e. - every set amount of blocks).

As for the question of termination. The naive solution would be to hold the spring-cleaning phase for a set amount of time (or, more accurately, a set amount of blocks). Alternatively, the spring-cleaning phase can end when no new PoC transactions are recorded for a set amount of time.

As the spring-cleaning phase progresses, more and more coins are expected to be claimed by one agent or another via PoC transactions. The result is that if the true amount of lost coins within the system is \( \epsilon_T \), then as the spring-cleaning phase unfolds the amount of perceived lost coins \( \epsilon_P \) should aspire to the true amount. We note a number of factors which might cause the perceived amount to defer from the truth, but in no way is it possible for \( \epsilon_P < \epsilon_T \) to hold at any point (due to the nature of PoC).

![Figure 4.4: Perceived Lost Coins Over Time](chart)

Figure 4.4: Perceived Lost Coins Over Time
4.5 Error Margin

We denote $\epsilon_P - \epsilon_T$ as the error margin of lost coins within the system. Whenever the error is greater than 0 this indicates that prior to the spring-cleaning phase there were coins which were not technically lost (meaning at least one agent was able to use them), but the owning agent made no claim for them during the spring-cleaning phase (deliberately or otherwise), and are thus lost to him after spring-cleaning has terminated.

An example of this would be if the agent in question owned less coins in a given wallet than the fee $f$ which is required for a PoC transaction for that wallet to be included in the blockchain by any miner.
Chapter 5

Stablecoins

In previous chapters we have shown that incentive compatibility for a decentralized monetary system is tantamount to regulation in the centralized counterparts: Both serve to encourage agents to conduct themselves honestly. Similarly, incentive compatibility might be the key to design dynamic, decentralized monetary policy mechanisms for cryptocurrencies in the future. Certainly the problem of monetary stability has been one of considerable debate, often used to debunk the credibility of the most popular cryptocurrencies\cite{Nak08}.

With that in mind, there exist some cryptocurrencies that chose to tackle this very issue. These are collectively referred to as Stablecoins, and we discuss them further in this chapter as work related to decentralized monetary policy.

Stablecoins are digital tokens which are intended to provide measurable stability and security. In other words, their value remains constant and stable over time.

There are various types of stablecoins, some differing slightly from one another in the way they are implemented, and some vastly different in their approach to monetary stability. Be that as it may, there are a couple of concepts that are common to all kinds of stablecoins. these are pegging and the use of collateral.

Pegging refers to the practice of maintaining a fixed exchange rate between a given currency to the value of another item - be it another currency or some other measure of material value. Two kinds of pegging exists: hard-pegging, where a rigid 1 : 1 exchange rate is enforced. An example of this is the old gold-standard, where the US government pegged the US dollar to the value of gold. The second type is soft-pegging, in which the exchange rate isn’t strictly enforced but is rather regulated by the governing entities to aspire as closely as possible to the targeted exchange rate. Most national currencies nowadays are softly pegged to the value of goods and services in the economic system by a metric known as the CPI (Consumer Price Index).

Collateral refers to any item of value to an agent which is accepted as a pledge to repay a loan. In case the agent in question defaults on their debts, their collateral is then forfeit. Most stablecoins rely on some form of collateral to peg their value, and to create individual stake for agents within the system. However, there exist an interesting
case study for stablecoins which do not rely on collateral as an integral part of their design.

Currently stablecoins can be separated into three types:

- Off-Chain Collateralized
- On-Chain Collateralized
- Seigniorage Shares

5.1 Off-Chain Collateralized

Off-Chain Collateralized currencies are the easiest to understand of the three. These currencies are characterized by a hard peg against some fiat currency or good which is also used as collateral by the users of the system.

An example of an off-chain collateralized currency is Tether, which happens to be the most widely used stablecoin at present. While tether itself isn’t technically a cryptocurrency, it still serves as an example of what off-chain collateralization is: using something outside of the economic system as collateral within it. Tether pegs its value to the US dollar at a 1:1 exchange rate, where users of tether are expected to deposit a certain amount of dollars at the company’s banks in order to receive a comparable amount of tether in return. It is easy to see how their dollars are then held as collateral for the exchange, as the only way for a given user to reclaim his deposit is to repay the appropriate amount of tether in return.

The advantages of off-chain collateralized currencies are that they are very easy to understand and implement. The pegged exchange rate is easily maintained in the system by simple incentive: Why bother selling tether for more than a dollar when the company’s banks can issue as many tethers as there are dollars for cheaper? Alternatively, attempting to sell tether for less than a dollar wouldn’t be lucrative at all, given that these tether can be sold back to the banks for a higher value.

However, off-chain collateralized currencies suffer a crucial flaw: while pegging them to some fiat currency guarantees an easy-to-maintain ad-hoc monetary policy, it also means that they are subjected to the same fluctuations as the collateral. Thus the entire system’s stability hinges on the stability of the chosen collateral, meaning trust is still an integral part of such systems.

5.2 On-Chain Collateralized

On-Chain Collateralized currencies are simple, in principle, to their off-chain counterparts. However where the off-chain collateralized currencies relied on some outside source of collateral which needs to be further tracked in some ledger, on-chain collateralized currencies rely solely on information which can be contained within the
blockchain itself. As such, these currencies generally accept some kind of preexisting
cryptocurrency as collateral for their own.

So then, if these stablecoins rely on other non-stable cryptocurrencies as collateral,
how can they possibly achieve the stability they promise? The answer lies in two
common practices of such currencies.

The first is over-collateralization; by which the stablecoin’s exchange rate against
the collateral cryptocurrency is often held at a larger ratio than a simple 1:1 exchange
rate. This in turn allows for flexibility when the collateral itself is volatile, so that users
are discouraged to attempt short-sales within the system.

Secondly, since the collateral is expected to be volatile, and tracked solely on the
blockchain itself, there is a need for the system to be able to evaluate the stablecoin’s
value occasionally. Thus many such stablecoins, such as Dai, employ a group of external
Oracles, which are used to value the stablecoin against some external factor (in the case
of Dai, oracle value it against the US dollar).

It is important to note that while Dai itself has shown remarkable stability over
the course of its lifespan, the system itself hinges on the honesty and neutrality of the
oracles themselves. If the oracles have an incentive to harm the system they can do
so simply by relaying false information regarding the stablecoin’s value. In Dai such a
scenario is addressed, and the suggested solution in such a case is to shut the system
down and allow users to withdraw their collateral at some fixed rate. This is a crude
solution which is meant to keep the oracles in check: as any attempt to attack the
system won’t yield many returns before it ”self-destructs”[Nak08].

5.3 Seigniorage Shares

Seigniorage shares was a stablecoin concept suggested in a paper by Robert Sams in
2014 [Nak08]. In the paper Sams describes stablecoins with a dynamically changing
money supply, which are governed by a decentralized algorithm that is responsible to
buy and sell the stablecoin’s tokens in order to maintain the token price near some
intended peg. While stablecoins of this type are effectively untested in practice, their
promise has aroused considerable interest, as they suggest both a solution to the trust
problem of off-chain collateralized currencies like Tether, and the reliance on outside
oracles required of on-chain collateralized currencies such as Dai.

In essence the paper suggests the usage of a two-currency economy: coins and
shares. Coins are used for everyday transactions just like any other cryptocurrency,
while shares cannot be transacted between agents, but instead promise the prospect
of future returns as they can be traded for more coins in the future. The idea is that
agents can dynamically choose to convert their shares to coins at any time, and vice-
versa. Thus when the value of the coin is low (meaning the coin is diluted), agents are
organically encouraged to begin converting their coins to shares, as they can purchase
them at a reduced priced (since the coins value is lower than it used to be) and then
sell them back when the price rises. The process of exchanging coins for shares via the algorithm dynamically raises the value of the coin, as the process removes coins from circulation, and thus counters the inflation. Alternatively, if the coin becomes deflated, meaning it grows in value, then shareholders are encouraged to sell some (or all) of their shares and enjoy an increased return in revenue, thus increasing the amount of coin in circulation and diluting its value.

This process is similar to the way some central governments choose to employ their monetary policy: In the USA for example, the central bank issues treasury-bonds which it can sell freely on the market. Treasury bonds promise a small but guaranteed return on investment, and so many groups have interest to purchase them in bulk at times. Similarly, when the US government is interested in decreasing the amount of dollars in circulation, new treasury bonds are sold at a discounted price to remove some coin from circulation. Alternatively, when the money supply is low, treasury bonds can be purchased back by the central back with additional premiums in order to pump more cash back into circulation.
Chapter 6

Related Work

In this chapter we revisit the previous work done by Gjermundrød and Dionysiou [GD14] regarding lost coin recirculation. In their paper they’ve also addressed the problem of lost coin as a deflationary factor for a crypto currency system.

Similarly they recognized the challenge of identifying coins which are actually lost within the system, and also proposed that it is necessary for users to prove ownership over wallets in order to reveal the lost currency by process of elimination.

While this work suggested a spring-cleaning mechanism as a way of periodically correcting the system, Gjermundrød and Dionysiou compared their own solution to a type of distributed garbage collection, where user wallets which don’t transact for a given amount of time eventually expire, allowing the coins within to be recirculated.

The key difference between their work and this one is in the redistribution scheme. Gjermundrød and Dionysiou suggested that lost coins collected by their algorithm should then be distributed by way of future block rewards. The implication of this design choice is that recirculated currency is awarded solely to miners, in contrast to our solution, which proportionally redistributed the currency to all users in the system.

In order to illustrate the problem with Gjermundrød and Dionysiou’s redistribution scheme we revisit the miner’s dilemma as introduced in chapter 4: Table 6 illustrates the problem which arises by redistributing lost currency exclusively to miners. Since any coins which are deemed lost are gradually redistributed in future block rewards, for any account which holds $t$ funds and attempts to prove claim for them during its legitimate lease period, a prospective miner can either choose to include the transaction in a block, receiving and expected reward of $f \cdot p$, or choose to censor the transaction by

<table>
<thead>
<tr>
<th>Opponents</th>
<th>Include</th>
<th>Censor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include</td>
<td>$f \cdot p$</td>
<td>0</td>
</tr>
<tr>
<td>Censor</td>
<td>$f$</td>
<td>$t \cdot p$</td>
</tr>
</tbody>
</table>

Table 6.1: Gjermundrød and Dionysiou’s Miners’ Dilemma

...
not including it in any future block. Should all miners collude on this, and censor the account, the miner’s expected reward from redistribution is \( t \cdot p \). Thus, for any rational miner, the trade off between including or censoring an account is \( f \cdot p > t \cdot p \Rightarrow f > t \). Accordingly, the only way a user can guarantee the inclusion of their proof-of-claim on the chain is by setting a transaction fee equal to the entire contents of their account.

We note that the unwanted equilibrium is broken if for at least one miner, denoted \( m_0 \), with mining power \( p_0 \), the sum total of fees for all PoC transactions is higher than the prospective rewards for censoring, or in total: \( \sum_{i=1}^{w} f = w \cdot f > \sum_{i=1}^{w} c_i \cdot p_0 \). Where \( w \) is the sum total of wallets in the system, and \( c_i \) is the \( i \)th account.

However, this adds considerations for the protocol designer. Assuming the goal of the protocol designer is to guarantee the correct execution of the suggested protocol (in this case, the reveal of any valid PoC that was transmitted in the system) then they must assure that spring cleaning runs long enough so that even if only a single miner is incentivized to include all PoC-transactions, the spring-cleaning runs long enough for them to do so. To illustrate this we consider the following parameters:

- \( c_i \) - the \( i \)th account
- \( f \) - transaction fee (fixed)
- \( p_0 \) - minimal targeted mining power (or safety parameter)
- \( T_h \) - average block time
- \( w \) - number of generated PoCs
- \( k \) - number of transactions per block
- \( L \) - length of spring-cleaning (in blocks)

Thus, the minimal number of blocks needed for \( m_0 \) to successfully complete spring-cleaning on their own is \( \frac{w}{k} \). Considering that statistically \( m_0 \) owns a portion of \( p_0 \) out of any interval on the blockchain, this means that the expected length of spring cleaning to allow for at least \( \frac{w}{k} \) is:

\[
L \cdot p_0 \geq \frac{w}{k} \Rightarrow p_0 \geq \frac{w}{kL} \tag{6.1}
\]

Therefore, depending on the designer’s preferred safety parameter \( p_0 \), the length of spring cleaning varies, we note that there is another constraint applied to \( p_0 \) when considering the incentive formula:

\[
w \cdot f > \sum_{i=1}^{w} c_i \cdot p_0 \Rightarrow \frac{w \cdot f}{\sum_{i=1}^{w} c_i} > p_0 \geq \frac{w}{kL} \tag{6.2}
\]

Note that this relationship between \( p_0 \) and \( f \) represents the value \( p_0 \) must maintain to support any targeted transaction fees. We illustrate this by example:
Example 6.0.1. We apply reasonable values to the aforementioned parameters:

- \( k = 1000 \)
- \( w = 10000000 \)
- \( \sum_{i=1}^{w} c_i \approx 20000000 \)
- \( f = 0.001 \)
- \( T_h = 10 \) (minutes)

Then:

\[
\frac{10000000 \cdot 0.001}{20000000} = 0.002 = p_0 \geq \frac{10000000}{1000 \cdot L} = \frac{10000}{L} \quad (6.3)
\]

Therefore, the length of spring cleaning must be at least:

\[
L = 5000000 \quad (6.4)
\]

Consider an average block creation time of 10 minutes, this translates to over 95 years of spring-cleaning to assure correctness.

When compared to our own suggested protocol we note that the same notion applies to the length of spring-cleaning depending on the chosen security parameter, however, since our redistribution scheme isn’t factored by mining power, the security parameter isn’t upper bound by the targeted transaction fees:

\[
\frac{w \cdot f}{\sum_{i=1}^{w} c_i} > p_0 \geq \frac{w}{kL} \Rightarrow f k L > \sum_{i=1}^{w} c_i \quad (6.5)
\]
Chapter 7

Conclusions

Bitcoin showed for the first time that a societal function which was believed to require a central authority to manage (banking) could be achieved in a decentralized manner. This raises the question: What other decentralized solutions can we find to other centralized problems.

As crypto-currencies become more widely accepted as an alternative form of payment, so the demand for better models increases, to replace the obsolete schemes. Many alternative models seek to improve upon the technological limitations of Nakamoto’s original whitepaper, addressing problems of security, anonymity [ca16], and scalability [SLZ17]. While others, inevitably, attempt to improve upon crypto-currencies usage as actual money.

While the problem of lost coins can be detrimental to crypto-currencies employing a fixed-capped monetary policy, we’ve shown a possible solution that maintains the distributed nature of the system, where the best course of action for each participant is achieved by following the desired protocol.

We view this work as a tentative step forward in the world of crypto-currency macroeconomics. In particular, it would be interesting to see if a crypto-currency employing a decentralized and dynamic monetary policy emerges in the future. One which is able to combat and mitigate the otherwise volatile nature other crypto-currencies have become notorious for.
Bibliography


תקציר
בשנים האחרונות חלה עלייה חדות בпитופיות של המטבעות הקRIPTוגרף. בכל ש الْיוזמות
ומתווך הסעם, כל צוות אשלוט להשקיח באשר לסכמות של תכניות נושאי, ובראשו
להתפוך מלאכת השמתה בקביעת ביטוי. בתוכן, מתכובע הקRIPTוגרף мнיר하며 למון, כי
ויהי עוד בתכונת האלת, השיגה הואכי לכל מהאייזן בים. פ聯רב התמורות, והיינו, כי
מסקט אל היום, ולפי החזרה התכונת של כיס - כלומר, אורח של אפקט, או מודר ממדית.
ולunbind את ביניים של הודעה מנדרים, דלק, חלק אפקט, מפרטים. הקבוצה, הלא
אלטרנטיביים, הquier להتعاמע את התוכן של הביקור, אל פתר: ביצוע של סקציבור,(sr
אותיה, באפיזות, י윤ה בבית, בתוכנית, ובתוכנה, אטס, מודירים.
וייושב השיבו, וכק גם בירוק של יעקוב התכונה.
ובכחלק התכונות ייצבות תכונת התכונת על ידי סכום יררכיה - בדור של החוב passphraseית,.toJSONStringי,
המחלש המגנון המבוך ביש סכום תכונות (蟆ים תרגום). מודיריםergency מודר לא
וכלל תכונות לדוח ממוצע, המגנון קצונת בודק בהכובע הקretweeted, בהלס, מקימי, ובלוס
ידי ישוניות הדרכים למסים הבסיס התכונת (כלומר, הביבית, בוחן המזומן או האסאיה והEventListener(לאחר למשלון).)
וכל תכון הקرياضים, כי יש מודר סכום סכום, ממונותר על פי הפרטים, ומודר
במסתע בחרות למוש. بما הביבית, בתוכן, очередה מתוכנות, וממשות מודר תכונת, מודר
חברת לע הכובע התכונת, שאו פסג מעורר, ואילו במעבדה אצוריים ממעסית את קס על
תקרה על הכובע התכונת, שאו פסג מעורר, ואילו במעבדה אצוריים ממעסית את קס על
כיום התכונת או שאוי ממעסית אצוריים.
בכיסי התכון, ואילו ממעסית אצוריים.
בשל העובדות שנובえば תכונת הקرياضים המבໂלוג בוור או סכום יררכיהemic
במסתע בחרות,🛍 יענהรถไฟ המגנון של אוכלי מסתע בחרות, אולק שמשי התוכנה אחר התוכנה, מבית
לאוToyota ידישוניות הביבית, בחרות, בחרות花纹רטונב, או שמתוכנות מודר מתוכנות, או שמתוכנות
בלשון עד כי או מסתע בחרות אוכלי ממעסית פריטים.
ושובו זה כמותי ביבית או ביבית פריטים, מに対וניות מתוכנות, שמתוכנות للمהרי
הכיסי והתוכנה של התוכנה או שמתוכנות מודר מתוכנות, או שמתוכנות
הכיסי התוכנה וביבית ממעסית, או שמתוכנות, או שמתוכנות
הכיסי התוכנה וביבית ממעסית, או שמתוכנות, או שמתוכנות
הכיסי התוכנה וביבית ממעסית, או שמתוכנות, או שמתוכנות
המחקר בוצע בתנאיות של הפרופסורים של ברכ-שושן ויובל יהודי, בפקולטה למופת המרכז.

CESC2018.

הכין עבדו הוזמן בכנס תודות בדרכו לפרסומת שprofession של פרופסורים של ברכ-שושן ויובל יהודי, בעלת מחקרי המערכות, שיתוף הידע והتعاون המוחלטים במושград שלמה.

הכין עבדו הוזמן בכנס תודות בדרכו לפרסומת שprofession של פרופסורים של ברכ-שושן ויובל יהודי, בעלת מחקרי המערכות, שיתוף הידע והتعاون המוחלטים במושград שלמה.

בattività לפרסומת בכנס תודות בדרכו לפרסומת שprofession של פרופסורים של ברכ-שושן ויובל יהודי, בעלת מחקרי המערכות, שיתוף הידע והتعاون המוחלטים במושград שלמה.

על השפעת אבדות ל القادم שלאי חום.

הכインターハ הומד מוסרה לشعبניה על מים מחקר אז.
מדעיה מחשב

אלון שטיירמן

הוגש לכתל הפקודים של המכון לכתלקנות גיסắm

2019 - אפריל - תשמ"טי

 записות ק年之 ע"י מספר ת"ל: 2019 - 04 - 16
مدיניות מנכורות מבורות עבר מסעート

קריפטוגרפיה

אלון שטיירמן