Miskre – Introduction White Paper

Empowering the Decentralized World

Version 1.0.1

Duy Duong, Hoang Gia, Samson Day

July 09, 2018

Table of Contents

1 Introduction

1.1 Definition of the Problem

1.1.1 Background Information - The Evolution of Money

Throughout the centuries, currency, as a construct, has become more and more abstract.

What exactly is money? Money at its core is a finite expression of value and thus a medium of exchange. It allows for the purchase of products and/or services, in addition it allows the accumulation of value for use at a later time. These basic concepts of money and exchange pre-date even verbal communication. It is an essential mode of human interaction. The modern notion of currency is just a means of facilitating these exchanges in a more sophisticated manner, allowing these finite units of value (a currency note for example) to be portable, traceable, bankable and, ultimately, corruptible.

The utility and philosophical construct of Money are the foundations upon which our modern world was built. But how did money come into existence? It was not the result of a systematized government initiative, it was not mandated by rulers or kings, and it was not developed by the world's great thinkers. Rather, it was an organic result of actions taken in the spirit of self-interest by individuals throughout the world for thousands of years.

1. From as far back as written history provides us insight, people have traded items with practical and finite value such food, decorative items, apparel, tools, and weapons. This system is known as the barter system – and it necessitates that each party must have what the other one wants in order for trade to occur.
2. Indirect exchange using currency began to take shape out of necessity because it's rare to have a coincidence of wants[1].
3. Metal emerged as the standard for currency because of its functional value and scarcity. It could be used to create goods such as jewelry, it was easy to carry and to transfer. It was durable (it did not die like cattle or decay like corn), and it was divisible (it can be split into smaller units if necessary).
4. The next step in the evolution of money was the idea of 'constant unit value' and the standardization of coins. The Coin meant that people did not have to weigh precious metals or estimate the value of the goods and services they were receiving; a kilogram of salt could be worth a fixed number of coins, regardless of what the relative value of the actual metal was to the buyer and the seller. The coin was successful in facilitating faster, easier and more predictable transactions but as the coin's value became further and further removed from the intrinsic value of the metal itself, a pivotal complication arose: the ability to debase the intrinsic value of the coin by diluting its precious metal content without altering its functional value. This was the inception of the modern

[1] The coincidence of wants (often known as double coincidence of wants) is the situation where the supplier of good A wants good B and the supplier of good B wants good A.

notion of money. Once the coin's value was no longer based on the scarcity of the raw material used to create it, we turned to centralized institutions to guarantee the value of our currency.

5. Debasement was one of the leading causes of the downfall of the Roman Empire.[2] Over a period of 200 years, the Roman denarius went from 90%+ silver per coin, to less than 0.5% of silver per coin; causing massive inflation across the empire.
6. Paper money was yet another pivotal leap in the abstraction of currency from the value which it represented; being first introduced in China around the year 600, not emerging in Europe until the early 1600s. British merchants would deposit their gold into secure storage rooms in exchange for a paper receipt, denoting the value of their deposit. As more and more goldsmiths started to issue paper receipts, it became possible to exchange these receipts with any goldsmith and not just the goldsmith who initially issued the receipt.
7. People then began to use these receipts for trade amongst themselves, exchanging them for goods and services. This was the birth of paper money. Paper money eventually became a reliable form of currency. While it did not have intrinsic value in and of itself, it was representative of something that did.
8. Eventually paper money became the standard, and governments started to print it. However, this type of currency was often not backed by a tangible resource, unlike goldsmiths' notes. In the Colonial United States, paper money was printed freely by the federal government, by states, and even by individuals (i.e.: Benjamin Franklin). However, because this paper money wasn't backed by anything of intrinsic value, it was printed in vast excess causing massive inflation and rendering the paper money worthless. After the pitfalls of an unbacked currency controlled by a centralized party were made evident, we reverted to our earlier systems of bartering and trading gold deposit receipts.
9. In the 1860s, the American government started to print paper money again in order to fund the Civil War.[3] However, by the end of the war this printed currency had been

[2] The Roman Empire was one of the largest in history, with contiguous territories throughout Europe, North Africa, and the Middle East. The Latin phrase imperium sine fine ("empire without end") expressed the ideology that neither time nor space limited the Empire. In Vergil's epic poem the Aeneid, limitless empire is said to be granted to the Romans by their supreme deity Jupiter. This claim of universal dominion was renewed and perpetuated when the Empire came under Christian rule in the 4th century. In addition to annexing large regions in their quest for empire-building, the Romans were also very large sculptors of their environment who directly altered their geography. For instance, entire forests were cut down to provide enough wood resources for an expanding empire. In his book Critias, Plato described that deforestation: where there was once "an abundance of wood in the mountains," he could now only see "the mere skeleton of the land."

[3] The American Civil War (also known by other names) was a war fought in the United States from 1861 to 1865. As a result of the long-standing controversy over slavery, war broke out in

debased to the extent that $300 was only really worth around $100. We again lost faith in our government's ability to guarantee the value of our accumulated wealth and subsequently reverted to hoarding precious metals and bartering. By 1880, the United States had remedied this problem by backing their paper money, the Dollar, with gold and allowing people to exchange their paper dollars for their equivalent value in gold.

10. During World War I[4], the United States government again abandoned the gold standard in order to print more money to fund the war. In 1933, it became illegal to own gold with the exception of jewelry and collector's coins. The government reversed this ban in the mid 1970's as the United States Dollar became the default currency for international trade.
11. In the 1950's we saw the advent of the charge card, a deferred payment system that ultimately paved the way for the modern notion of credit and the credit card. The Diners Club Card was released 1950, it allowed its cardholders to dine out and pay at the end of the month for their cumulative spending. The credit card, first introduced by American Express in 1958, and it allowed a cardholder to further defer payment with the condition that they would have to pay interest on their outstanding balance. The credit card allowed the average person to spend beyond their means with seemingly insignificant consequence. Luxuries known only to the upper-class had suddenly become attainable to the masses and the status quo for the middle class had become more than a middle-class income could afford. Here began our true reliance on centralized banks. By the 1970's's there were millions of people spending on credit more than their income could reasonably support and owing the overages to their banks.
12. Electronic money, in the form of online payment processing, online banking, electronic checks and smart cards arose in the 1990's. This demarcated a radical shift in the way in which we interacted with money; not unlike the transition from raw metals to coins.

April 1861, when Confederate forces attacked Fort Sumter in South Carolina, shortly after U.S. President Abraham Lincoln was inaugurated. The nationalists of the Union proclaimed loyalty to the U.S. Constitution. They faced secessionists of the Confederate States, who advocated for states' rights to expand slavery.

[4] World War I (often abbreviated as WWI or WW1), also known as the First World War or the Great War, was a global war originating in Europe that lasted from 28 July 1914 to 11 November 1918. Contemporaneously described as the "War to End All Wars", more than 70 million military personnel, including 60 million Europeans, were mobilised in one of the largest wars in history. Over nine million combatants and seven million civilians died as a result of the war (including the victims of a number of genocides), a casualty rate exacerbated by the belligerents' technological and industrial sophistication, and the tactical stalemate caused by gruelling trench warfare. It was one of the deadliest conflicts in history and precipitated major political change, including the Revolutions of 1917–1923 in many of the nations involved. Unresolved rivalries at the end of the conflict contributed to the start of the Second World War twenty-one years later.

These electronic systems dramatically increased the rate, frequency and diversity of transactions and empowered the small business owner to reliably sell out of state and internationally.

13. Today electronic banking, near-instant transaction processing and deferred payment systems are the cornerstone of our global economy, as is our reliance on the centralized institutions that provide these services.

1.1.2 Centrally Controlled Money

Suppose there are only 10 people in the world, and each has 10 units of the same currency, but there is only one person who can add more money into the system. Let's call this individual 'Person A.'

Now imagine that Person A prints 25 more units of currency (whether through actual printing or typing a number on a screen in the era of electronic banking); inflating the currency by 25%. This will cause all goods and services to go up in price by 25%.

Why is this problematic?

When Person A prints money, this money does not get distributed to everyone equally. Those not on the receiving end of the newly printed money will have to pay a premium for products without any additional currency to pay that premium.

For example, let's say that before inflation you could buy 1 banana for 1 unit of currency. Now with an inflation rate of 25% - 10 units of your currency- which could previously buy 10 bananas – can now only buy you 8 bananas at a rate of 1.25 per banana.

It is important to note that inflation also affect Person A- who will now only be able to buy 28 bananas with their 35 units of currency. However, this is still a significantly more than they could have afforded before (18), and they are much better off than those who were not the beneficiaries of additional currency.

Furthermore- what if Person A did not make known how much additional currency he printed? And before anyone knew there was an influx of new money- he had already used all 35 units of currency and bought 35 bananas. Inflation, especially when opaque, can be very dangerous to an economy.

1.2 Expand on the Problem

1.2.1 Electronic Money vs Cryptocurrencies

1.2.1.1 Electronic Money

Electronic money is a form of fiat money that exists in the digital form. Currently, over 92% of the world's money is digital, while only roughly 8% is in paper form.

What are the advantages of electronic currency:

- Has an existing infrastructure
- Major credit/debit cards are accepted nearly everywhere
- Consumer Protection in case of fraud

Disadvantages:

- Open to manipulation
- Lack of transparency
- High merchant processing fees
- Easier to commit fraud (i.e. reverting a payment when you've actually already received the service/product)

1.2.1.2 Cryptocurrencies

A cryptocurrency is a medium of exchange and has set rules by which it operates. It is considered reliable because it's based on cryptography. No supervisory authority controls all the action on the network. Additionally, it uses blockchain technology to ensure that no information is changed or tampered with by third parties.

Advantages

- Permission-less (ability to move your money anywhere without anyone's permission)
- Trustless (does not need to trust governments or banks, because everything is secured on the blockchain)
- Cheap and fast transactions to anywhere in the world

Disadvantages:

- Currently does not have mass adoption

1.2.2 Problem Context

At this time, banking, credit, and international finance capabilities are for the most part only available to the wealthier echelons of society. This group makes up roughly 13% of the world's population (about 1 billion people). Most of the world actually lives in a cash-based society, and therefore does not receive many of the benefits that electronic currency has to offer.

With the emergence of blockchain technology, we can now create an international peer-to-peer financial system that allows everyone to participate by just downloading a simple application. In this way, cryptocurrency levels the playing field. It is neutral to the sender, the recipient, and the value of transaction; whether you're a farmer living in rural Africa or a large enterprise, you can operate on the same level in the world of cryptocurrency.

Emergence of blockchain technology represents an unprecedented transformation of money and the way we conceptualize it. This radical innovation is disruptive to the current financial system as we know it. An individual will have absolute control over their own finances- which is not true of our current system. With cryptocurrency, it is impossible for anyone to seize,

censor, or freeze your money; no one can tell you what to do or what not to do with your money, and anyone in the world can participate with a device as simple as a smart phone.

Truly disruptive technologies have always encountered obstacles, and cryptocurrency will be no different. Automobiles didn't immediately replace horses; it took decades for the full transition to happen. At first, people ridiculed the early automobiles because they were slower than horses, they broke often, and the gasoline necessary for them to run wasn't always readily available. People also ridiculed the invention of electricity, considering it to be a fad. The infrastructure for natural gas was already in place, providing heating and light, as well as powering machinery. The invention of automobiles, electricity, and the internet all required massive infrastructure inversions to be successful. We aim to be at the forefront of the cryptocurrency revolution, creating the necessary infrastructure to promote innovation and boost adoption rate, so that we can all benefit from a truly global economy that is accessible to all and free from manipulation.

1.2.3 Problems with Governance in Blockchain

1.2.3.1 Distribution

The idea of decentralization has been essential to the cryptocurrency community since its very genesis. However, in practice, most cryptocurrencies delegate the majority stake of the coin to its founding members; thus creating a centralized and exclusionary coin from the start.

1.2.3.2 Democracy

As a result of this schism between the philosophical principles upon which crypto was founded, and the self-interest of many of the founders of the world's most successful coins, we are left with a community that reflects the economic inequality of our mainstream economic system with power in the hands of too few individuals. There is no value in a distributed ledger if the network of people that holds the power to change it is centralized.

Example

The DAO hack: the Ethereum Foundation started an informal vote to determine if there should be a hard fork or not. Only 5.5% of Ethereum holders voted for two reasons: many holders were not aware that there was a poll running and the pole only ran for 24 hours. This created a situation of great inequality- with 25% of yes votes coming from only one wallet. If all ETH holders had voted, the results may have been very different. In this scenario, the Ethereum Foundation had the power to start the vote, choose the time limit, and carry out the act.[i]

1.3 Proposed Solution

Miskre provides a truly decentralized blockchain solution- a standalone community-governed protocol with no central power. This is powerful because it ensures that those *affected* by the rules can participate in *modifying* the rules. Miskre aims to build a global ecosystem that empowers entrepreneurs to bring new technologies to market and bring monetary freedom to

the masses. This will allow everyone- no matter who they are, where they live, or their financial status -to participate in the global economy with full authority and freedom.

Striving to be completely autonomous, Miskre is a standalone blockchain. The Miskre ecosystem will consist of two tokens: MIS and KRE. MIS 20 billion tokens representing rights to the network. KRE 20 billion tokens to be the currency of the network.

End users can use native MIS and KRE tokens to store, receive, transfer, pay for goods and services both online and offline in a fair and trustless system.

Applications/Service Developers/Miskre Core Teams can be incubated by Miskre Labs all over the world to grow their business in the Miskre ecosystem and spread Miskre adoption worldwide.

Blockchain developers can develop and submit protocol updates to receive KRE for their contributions. Anyone can submit a protocol update, change anything in the system, and request a desired amount of KRE for their contribution. If a protocol update is deployed, the system will automatically send the requested reward to the attached wallet/wallets.

2 Miskre Basics

2.1 Introduction

Miskre is a truly decentralized currency based on NEO's source-code[ii] that is being developed into a standalone community-governed protocol with no central power, ensuring that those affected by the rules can participate in their modification.

2.1.1 Why Did Miskre Choose NEO's Source-Code to Build Upon?

Miskre is not an "NEP5-token[5]". Miskre is a standalone blockchain.

NEO is a non-profit community-based blockchain project that utilizes blockchain technology and digital identity to digitize assets, to automate the management of digital assets using smart contracts, and to realize a "smart economy" with a distributed network.

[5] NEP stands for NEO Enhancement Proposal. The NEP5 gives developers a standardized workflow and template to build decentralized applications. All tokens using the NEP5 standard are automatically able to transact with any other token using the NEP5 standard which allows for applications such as decentralized exchanges and other more advanced cross token communication.

Smart Economy = Digital Assets[6] + Digital Identify[7] + Smart Contract[8]

NEO was founded in 2014 and was real-time open source on GitHub in June 2015. NEO was created in attempt to shift our traditional economy into the new era of the "Smart Economy".

NEO's consensus model, speed, and two token system is perfect as a base for what Miskre is trying to achieve. However, due to its centralization and a limited supply of NEO, we chose to build our own chain.

Centralization Explained: Neo Council holds 50% of all NEO, therefore the NEO blockchain is very centralized and is not an ideal chain to build the Miskre model.

Limited Supply: The minimum divisible unit of NEO is 1, however there are only 100 million NEO. This means that the maximum number of people that can have at least 1 NEO is only 100 million, while the world population is nearing 8 billion. This limitation rules out NEO as a good fit for the global ecosystem that Miskre envisions.

Mission

Miskre aims to build a global ecosystem that empowers entrepreneurs to bring new technologies to market and bring monetary freedom to the masses. Allowing everyone; no

[6] Digital Assets are programmable assets that exist in the form of electronic data. With blockchain technology, the digitization of assets can be decentralized, trustful, traceable, highly transparent, and free of intermediaries. On the NEO blockchain, users are able to register, trade, and circulate multiple types of assets. Proving the connection between digital and physical assets is possible through digital identity. Assets registered through a validated digital identity are protected by law.

[7] Digital identity refers to the identity information of individuals, organizations, and other entities that exist in electronic form. The more mature digital identity system is based on the PKI (Public Key Infrastructure) X.509 standard. In NEO, we will implement a set of X.509 compatible digital identity standards. This set of digital identity standards, in addition to a compatible X.509 level certificate issuance model, will also support the Web Of Trust point-to-point certificate issuance model.

[8] The NeoContract smart contract system is the biggest feature of the seamless integration of the existing developer ecosystem. Developers do not need to learn a new programming language, but can use C#, Java and other mainstream programming languages in their familiar IDE environments (Visual Studio, Eclipse, etc.) for smart contract development, debugging and compilation. NEO's Universal Lightweight Virtual Machine, NeoVM, has the advantages of high certainty, high concurrency, and high scalability. The NeoContract smart contract system will allow millions of developers around the world to quickly carry out the development of smart contracts. NeoContract will have a separate white paper describing the implementation details.

matter who they are, where they live, or their financial status to participate in the global economy with full authority and freedom.

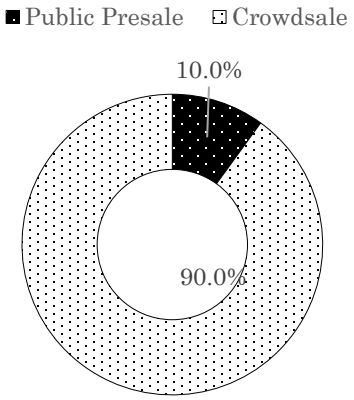
2.1.2 Tokens

Striving to be completely autonomous, Miskre is a standalone blockchain. The Miskre ecosystem will consist of two tokens: MIS and KRE. MIS 20 billion tokens are to represent rights to the network. KRE 20 billion tokens are to be the currency of the network.

2.1.2.1 MIS

20 billion tokens representing rights to the network.

Minimum divisible unit is 1



- 10% MIS Public Presale
- 90% MIS Crowdsale

2.1.2.2 KRE

20 billion tokens to be the currency of the network.

Minimum divisible unit is 0.000001

The initial amount of KRE is 0 and will be generated by MIS.

MIS will continue to generate KRE until the total KRE reach 20 billion; a process that will take 22 years.

The rate of KRE generation will decrease every year;

- 16% of KRE will be generated the first year
- 52% of KRE will be generated in the first four years

80% KRE generated in twelve years

2.1.3 Fair Distribution

In order to create a truly fair and decentralized system, the initial distribution will have to be fair and decentralized. Therefore, our team decided that we will take 0% of the coins unless we participate in the funding rounds ourselves with our own money. If we want to create a protocol that will eventually be the blockchain of the world, taking even just 0.01% of the total coins for ourselves without participating in the funding rounds like everyone else will not only hinder our goal but might make the goal unattainable; it is our belief that users will eventually gravitate towards the most fair and decentralized protocol to use and participate in.

With this fair distribution, Miskre hopes to solve the problem of talented people creating their own projects instead of choosing to work on one protocol.

3 Miskre Blockchain

3.1 Byzantine Fault Tolerance Algorithm for Blockchain

Fully quoted from NEO consensus whitepaper[iii].

Abstract

This article proposes an improved Byzantine Fault Tolerance algorithm, adjusted for a blockchain system. Hypothetically, in this system, messages may subject to loss, damage, latency, and repetition. Also, the sending order may not necessarily be consistent with the receiving order of messages. The activities of nodes could be arbitrary, they may join and quit the network at any time; they may also dump and falsify information or simply stop working. Artificial or non-artificial glitches may occur as well. Our algorithm provides a $f = \lfloor (n-1) / 3 \rfloor$ fault tolerance to a consensus system that comprises n nodes. This tolerance capacity includes security and usability and is suited for any network environment.

Overview

A blockchain is a decentralized distributed ledger system. It could be used for registration and issuance of digitalized assets, property right certificates, credit points and so on. It enables transfer, payment, and transactions in a peer-to-peer way. The blockchain technology was originally proposed by Satoshi Nakamoto in a cryptography mailing list, i.e. the Bitcoin. Since then, numerous applications based on the blockchain emerged, such as e-cash systems, stock equity exchanges and Smart Contract systems.

A blockchain system is advantageous over a traditional centralized ledger system for its full-openness, immutability and anti-multiple-spend characters, and it does not rely on any kind of trusted third-party.

However, like all distributed systems, blockchain systems are challenged with network latency, transmission errors, software bugs, security loopholes and black-hat hacker threats. Moreover,

its decentralized nature suggests that no participant of the system cannot be trusted. Malicious nodes may emerge, so does data difference due to conflicting interests.

To counter these potential errors, a blockchain system is in need of an efficient consensus mechanism to ensure that every node has a copy of a recognized version of the total ledger. Traditional fault tolerance mechanisms concerning certain problems may not be completely capable of tackling the issue that distributed and blockchain systems are faced with. A universal cure-to-all fault tolerance solution is in need.

Proof-of-Work mechanism[iv], employed by the Bitcoin, addresses this issue rather brilliantly. But it comes with an obvious price, i.e. significant electricity cost and energy consumption. Further, with Bitcoin's existence, new blockchains must find different hashing algorithms, so as to prevent computational attacks from it. For example, Litecoin adopts SCRYPT, rather than Bitcoin's SHA256.

Byzantine Fault Tolerance mechanism is a universal solution for distributed systems[v]. Here in this article, based on the Practical Byzantine Fault Tolerance (PBFT[vi]) proposed by Castro and Liskov in 1999, an improved Byzantine Fault Tolerance algorithm is proposed for blockchain systems.

System Model

A blockchain is a distributed ledger system in which participants connect with each other via a peer-to-peer network. All messages within it will be sent by broadcasting. Two types of roles exist: Ordinary nodes and Bookkeeping nodes. Ordinary nodes use the system to transfer and exchange, accepting ledger data; while bookkeeping nodes provide accounting service for the entire network and maintain the ledger.

Hypothetically, in this system, messages may subject to loss, damage, latency and repetition. Also, the sending order may not necessarily be consistent with the receiving order of messages. The activities of nodes could be arbitrary, they may join and quit the network at any time; they may also dump and falsify information or simply stop working. Artificial or non-artificial glitches may occur as well.

Integrity and Authenticity of information transmission are ensured with cryptography while senders must attach signatures to the hash value of the message sent. Here we define $\langle m \rangle \sigma i$ is the message m's digital signature from node i, while D(m) is the hash value of message m. Without special clarification, all signature referred to in this article are signatures to the message hash value.

The Algorithm

Our algorithm ensures security as well as usability. With erroneous nodes in the consensus making no more than $\lfloor (n-1) / 3 \rfloor$, the functionality and stability of the system is guaranteed. In it, $n = |R|$ suggests the total number of nodes joined in the consensus making while R

stands for the set of consensus nodes. Given $f = \lfloor (n-1) / 3 \rfloor$, f stands for the maximum number of erroneous nodes allowed in the system. In fact, the total ledger is maintained by bookkeeping nodes while ordinary nodes do not participate in the consensus making. This is to show the entire consensus making procedures.

All consensus nodes are required to maintain a state table to record current consensus status. The data set used for a consensus from its beginning to its end is called a View. If consensus cannot be reached within the current View, a View Change will be required. We identify each View with a number v, starting from 0 and it may increase till achieving the consensus.

We identify each consensus node with a number, starting from 0, the last node is numbered n − 1. For each round of consensus making, a node will play speaker of the house while other nodes play congressmen. The speaker's number p will be determined by the following algorithm: Hypothetically the current block height is h, then $p = (h - v) \ mod \ n$, p's value range will be $0 \leq p < n$.

A new block will be generated with each round of consensus, with at least $n - f$ signatures from bookkeeping nodes. Upon the generation of a block, a new round of consensus making shall begin, resetting v=0.

General Procedures

Set the time intervals of block generation as t, under normal circumstances, the algorithm executes in the following procedures:

1. A node broadcasts transaction data to the entire network, attached with the sender signature;
2. All bookkeeping nodes monitors transaction data broadcasting independently and stores the data in its memory respectively;
3. After the time t, the speaker sends $\langle PrepareRequest,h,v,p,block,\langle block\rangle\sigma p\rangle$;
4. After receiving the proposal, congressmen i send $\langle PrepareResponse,h,v,i,\langle block\rangle\sigma i\rangle$;
5. Any node, upon receiving at least $n - f$ $\langle block\rangle\sigma i$, reaches a consensus and publishes a full block;
6. Any node, after receiving the full block, deletes the transaction in question from its memory and begins the next round the consensus;

It is required that, for all the consensus nodes, at least $n - f$ nodes are in the same original state. This is to say, for all the nodes i, the block height h and View number v are the same. This is not difficult, consistency of h could be reached by synchronizing the blocks while consistency of v could reached by changing the View. Block synchronizing is not covered in this article. For View change, check next section.

Nodes, after monitoring the broadcasting and receiving the proposal, shall validate the transactions. They cannot write an illegal transaction in the memory once the latter is exposed.

If an illegal transaction is contained in the proposal, this round of consensus will be abandoned and the View change will take place immediately. The validation procedures are as follows:

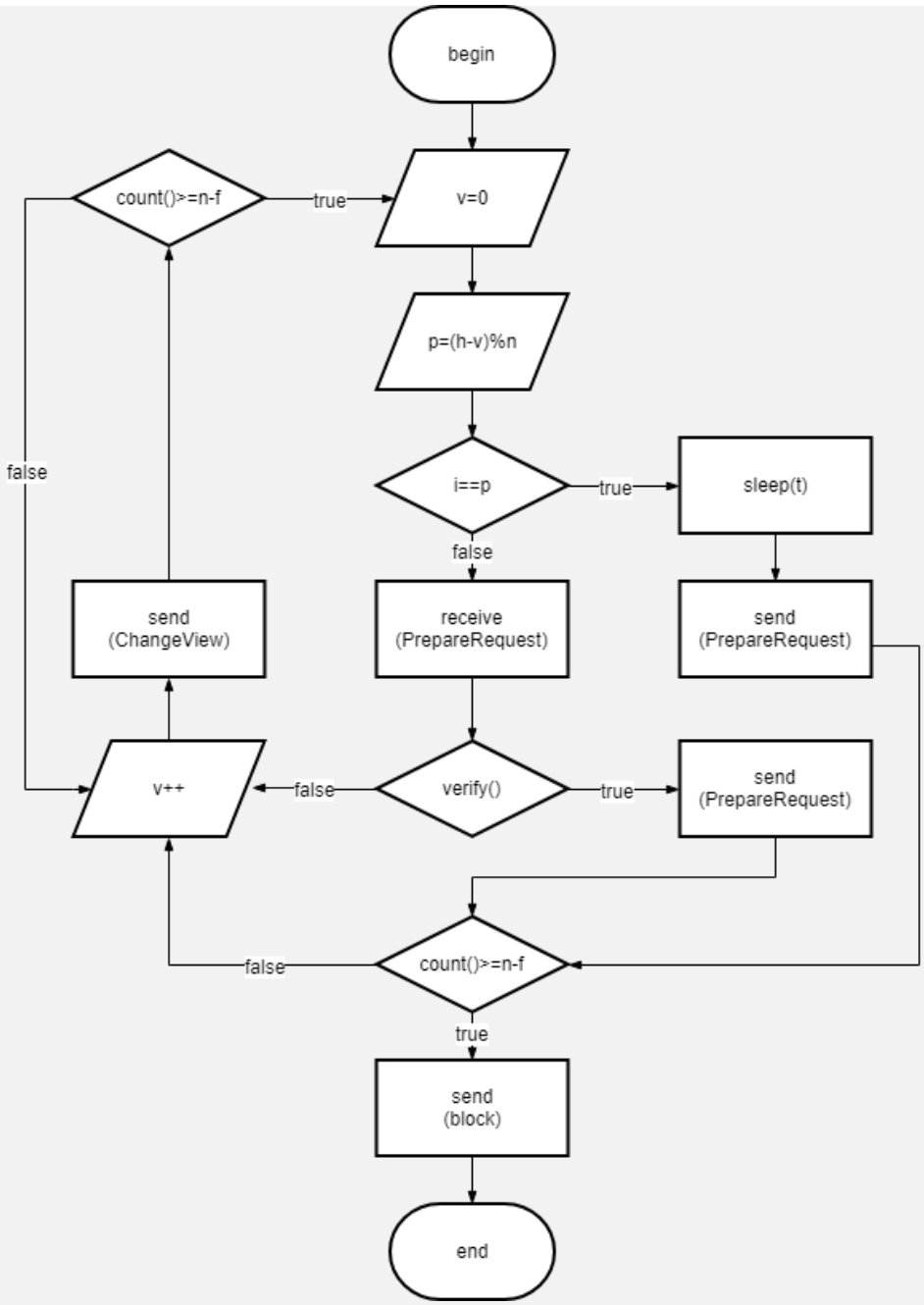
1. Is the data format of the transaction consistent with the system rules? If no, the transaction is ruled illegal;
2. Is the transaction already in the blockchain? If yes, the transaction is ruled illegal;
3. Are all the contract scripts of the transaction correctly executed? If no, the transaction is ruled illegal;
4. Is there multiple-spend in the transaction? If yes, the transaction is ruled illegal;
5. If the transaction had not been ruled illegal in the above procedures, it will be ruled legal;

View Change

If, after $2v+1 \cdot t$ time interval, the nodes i cannot reach a consensus or should they receive proposals that contain illegal transactions, the View Change will take place:

1. Given k=1, $vk = v + k$;
2. Nodes i send View Change request $\langle ChangeView, h, v, i, vk \rangle$;
3. Once any node receives at least $n - f$ same vk from different i, the View Change is completed. Set $v = vk$ and the consensus making begins;
4. If, after $2v+1 \cdot t$ time interval, the View Change is not completed, the k will increase and back to step 2);
   With the k increasing, the overtime waiting time will increase exponentially, so frequent View Change will be avoided and nodes are urged to reach consistency over v. Before the completion of View Change, the original View v is still valid, so unnecessary View Change caused by occasional network latency can be avoided.

Flow Chart



Fault Tolerance Capacity

Our algorithm provides $f = \lfloor (n-1) / 3 \rfloor$ fault tolerance to a consensus system that comprises n nodes. This tolerance capacity includes security and usability and is suite for any network environment.

Request data from nodes contain sender signatures, so malicious bookkeeping nodes cannot falsify requests. Instead, they will try to reverse the system status back to the past, forcing the system to fork.

Hypothetically, in the network environment of the system, consensus nodes are divided into 3 parts: $R = R1 \cup R2 \cup F$, and $R1 \cap R2 = \emptyset$, $R1 \cap F = \emptyset$, $R2 \cap F = \emptyset$. Also hypothetically, both R1 and R2 are honest bookkeeping nodes in an information silo that they can only communicate with nodes in their set; F are all malicious nodes in coordination; moreover, the network condition of F allows them to communicate with any node, including R1 and R2. If F wishes to fork the system, they have to reach consensus with R1 and publish blocks, and then reach a second consensus without informing the R2, revoking the consensus with R1. To reach this, it is necessary that $|R1| + |F| \geq n - f$ and $|R2| + |F| \geq n - f$. In the worst case scenario, $|F| = f$, i.e. the number of malicious nodes is at the maximum that the system could tolerate the aforementioned relation becomes $|R1| \geq n - 2f$ and $|R2| \geq n - 2f$. Added together, $|R1| + |R2| \geq 2n - 4f$, which could be simplified as $n \leq 3f$. Given that $f = \lfloor (n-1) / 3 \rfloor$, which contradicts with the former, it can be proven that the system cannot be forked within the tolerance range.

3.2 Consensus

Miskre implements and improves upon NEO's Delegated Byzantine Fault Tolerance consensus algorithm to allow for an on-chain governance model using ranked choice voting to solve the centralization issue plaguing today's blockchains. Miskre eliminates the need for trusted third parties and puts the power back into the hands of the users of the network, removing the power dynamics and hidden politics in blockchain core development.

For a blockchain to be truly decentralized, we need to incorporate a governance structure that will allow for full visibility and authority for every user on the network, as well as the power to discuss, coordinate, and make decisions as to how the technology should evolve.

"The best "TTP[9]" of all is one that does not exist, but the necessity for which has been eliminated by the protocol design, or which has been automated and distributed amongst the parties to a protocol." – Nick Szabo[vii]

4 True Democracy

In an electoral system consisting of many candidates, candidates are elected to represent the voter's interests. At Miskre, it is essential that we have a fair and democratic voting system to execute the user's wants and needs.

Miskre will introduce a new system of incentivized real-time on-chain governance using a ranked-choice voting system.

[9] Trusted Third Parties

Ranked-choice voting maximizes the effectiveness of every vote to ensure that only the delegates MIS holders truly want are elected. Choice voting is the optimal system for a decentralized system of governance- not only because it minimizes the number of wasted votes, but it also mitigates the impact of tactical voting.

Miskre delegates are chosen from a highly competitive election system, driven by MIS holders. Delegates are responsible for upholding the integrity of the system by verifying transactions and deciding on protocol updates to get rewarded by the system fee that the network receives.

The number of delegates will be determined using the formula: Total delegates = 3n+1, to ensure ⅔ consensus will always be reached. To ensure the sustainable growth of the system, the number of delegates, system fees, and almost everything else can be improved with protocol updates. Miskre's delegate system will allow for the full visibility of decisions of all active delegates, giving MIS holders full control over the network.

The blockchain is transparent. This means that for the first time ever, voters can be sure that the delegates they vote for will do exactly as they said they would. If a delegate changes his vote, MIS holders can always vote for a replacement delegate to enact their desired outcome. MIS holders can also become delegates themselves and vote for protocol updates.

Delegates are allowed to change their vote on protocol updates once every 24 hours.

Users of the system give the power to delegates to decide on protocol updates, a power which they can take back and redistribute however they wish, whenever they wish.

Since Delegates are rewarded with KRE and KRE is only as valuable as the size of the ecosystem, therefore Delegates have incentives to do their job correctly ensuring the grow of the ecosystem.

Delegates can choose to share any percentage of their rewards with MIS holders and the Development Pool.

"Independence and autonomy is the ability to act. If we always need third parties and central organisations to resolve disputes, solve our problems and coordinate us then we are doomed as a species. Central authorities are always a magnet for corruption and that will never change. Learn to be self reliant and make things happen." - Amir Taaki[viii]

4.1 Ranked Choice Voting System

4.1.1 Vote

Under ranked choice voting, voters rank candidates in order of choice. They mark their favorite candidate as first choice and then indicate their second and additional back-up choices in order of preference. Voters may rank as many candidates as they want, as indicating a lower-choice candidate will never affect the chances of their more preferred candidate.

Fully quoted from FairVote – "Multi-Winner Ranked Choice Voting" article[ix].

To find out who wins, votes are counted in a series of rounds to ensure that as few votes as possible are wasted. Each round, one of two things happens: either a winning candidate is identified and elected, in which case the votes they received in excess of what they needed to win transfer to their next choices; or the candidate in last place is eliminated, in which case votes for that candidate transfer to their next choices.

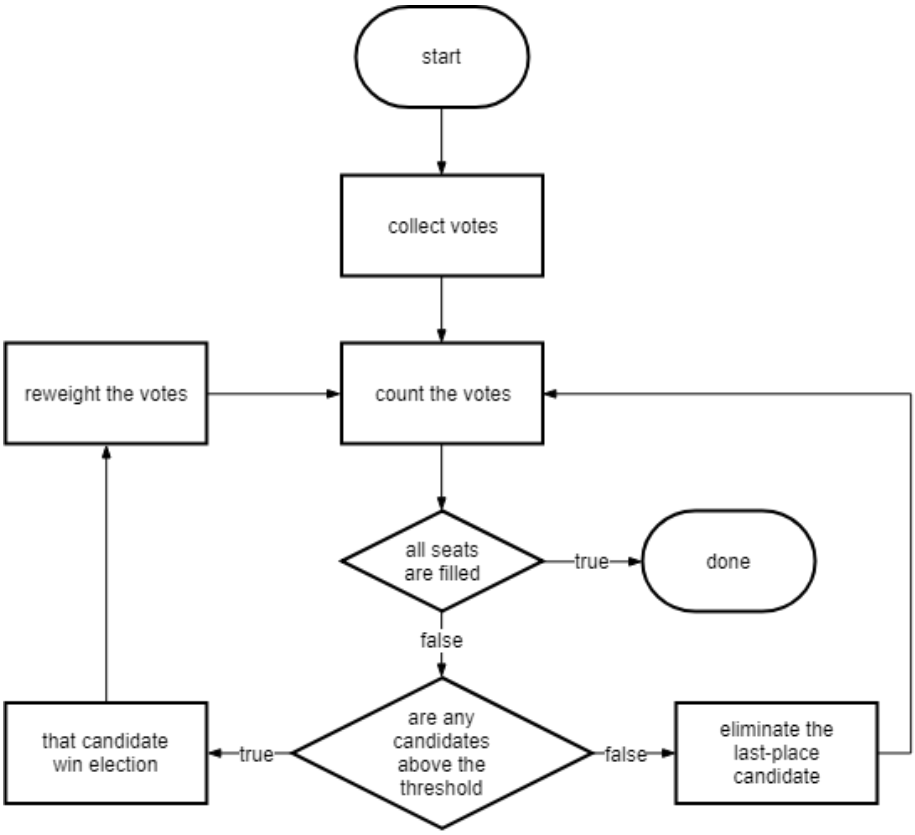
First, we need to know how many votes are enough to guarantee a victory- we will call this the election threshold. The election threshold is the exact number of votes necessary to mathematically guarantee that the candidate cannot lose. For example, if three candidates will be elected, the threshold is 25% of votes (if one candidate has more than 25% of the vote, it is impossible for the three other candidates to get more votes than them because that would add up to more than 100% of votes). If four candidates will be elected, the threshold is 20% of votes. If five candidates will be elected, it is about 17% of votes, and so on and so forth.

Initially, every vote counts towards the voters first choice only. In the case that the votes for the given candidates exceed the threshold to win, and every seat is filled, then vote counting is over. Otherwise, votes are counted in rounds as follows:

If any candidates have more votes than the election threshold, they are elected. The number of votes they received in excess of the threshold are then added to the totals of the continuing candidates. Specifically, a fraction of each vote for the elected candidate will be delegated to the candidate that was ranked next. For example, if a candidate has 10% more votes than the election threshold, every one of their voters will have 10% of their vote count for their next choice. That way, voters can rank a very popular candidate first while still knowing that their vote will make a difference to elect a less popular candidate that they also believe in.

If no candidate has more votes than the election threshold, the candidate with the fewest votes will be eliminated. When a voter's top choice is eliminated, their vote instantly counts for their next choice. This ensures that voters can honestly rank their favorite candidate first, even if that candidate does not stand a real chance of winning.

The cycle of counting surplus votes and eliminating last-place candidates will continue until all seats are filled.



5 On-Chain Proposal Update

Each protocol update requires a ⅔ yes vote from delegates in order to enter the "Pending Deployment" stage. At the "Pending Deployment" stage, if ⅔ of the total delegates vote yes, the protocol update will be automatically executed within 7 days. Delegates can change their vote at any time before the protocol is deployed, and if said delegates change their vote to the extent that the update no longer has 2/3 consensus, it will lose 'Pending Deployment' status until it once again reaches a 2/3 consensus, triggering a new deployment countdown. Additionally, users can vote for new delegates at any time, and replacement delegates can change the previous delegates' votes.

Anyone can submit a protocol update, change anything in the system, and request a desired amount of KRE from the development pool for their contribution. If a protocol update is deployed, the system will automatically send the requested reward to the attached wallet/wallets. A protocol update can attach to an infinite number of wallets. Additionally, it is possible to specify what ratio of the total reward will be received by each wallet.

Our on-chain proposal update system ensures that our blockchain is constantly updated and that talented developers are properly rewarded for their work.

6 Development Pool

The development pool is an autonomous built-in wallet that enables the Miskre blockchain to be self-sustaining. It will work with our delegate feature in order to ensure the continuous development of Miskre's blockchain. Miskre's development pool will incentivize talented developers to create new updates for the Miskre protocol, rather than working on their own projects.

The development pool will source funds through donations from delegates. Specifically, MIS holders who wish to support developers can vote for delegates who will share a significant portion of their rewards with the development pool.

7 Miskre Labs

Miskre labs are strategically placed incubators whose mission is to spread Miskre adoption worldwide. Anyone can apply to build their dreams at Miskre labs locations around the world. We aim to provide everything a startup would need to succeed; finding product market fit, obtaining user validation, sourcing additional funding, etc. Miskre labs are key mechanisms of value creation for the Miskre ecosystem, enabling businesses around the globe to build on the Miskre protocol and providing products and services to the community.

7.1 Where are Miskre Labs Located?

First three labs locations:

1. Bangkok, Thailand
2. Buenos Aires, Argentina
3. Lisbon, Portugal

Next six planned locations:

1. Fukuoka, Japan
2. Cairo, Egypt
3. Cape Town, South Africa
4. Daejeon, South Korea
5. Kiev, Ukraine
6. Minsk, Belarus

Locations are chosen based on but not limited to these criteria:

- Cheap rental: This allows us to set up a large facility. Ideally we would be able to house 20-30 teams consisting of around 2-5 people per team, as well as a Miskre Lab Advisor.
- Startup hubs that will make it possible to identify interesting projects to invest in locally, as well as source additional local talent if necessary.
- Low cost of living allows for more productivity. For example- moving a North American or European team to one of our lab locations will allow them to live and build their

dream project without the constraints of the very high living wage in their home country.
- Nations in which cryptocurrency laws are attractive and the government allows cryptocurrencies to operate freely.
- Low income regions in general. It is here that Miskre can have the most significant impact- helping local entrepreneurs to build technology and initiating development within struggling regions by spreading Miskre adoption to people who otherwise wouldn't have access.

7.2 Miskre Labs Investment

Miskre Labs will invest in early startups by providing them with several important things: guidance and support from our Lab Advisors, a place to work, accommodation, and a basic salary. Anyone can apply to Miskre labs for funding by simply sending in an application online that tells us about their business idea and team.

7.3 Why Get Investment from Miskre Labs Instead of Creating Your Own ICO?

There are several reasons why receiving investment from Miskre labs is more advantageous than creating your own ICO. For example:

- Miskre provides an immediate user base and feedback from the community when released.
- The potential for success from product market fit, instead of the ability to raise tens of millions in an ICO.
- To start an ICO is expensive; requiring costly paperwork and legal fees.

- Most new entrepreneurs don't have the background to secure investment for their ICOs.
- Miskre provides an intense incubation period with full support from industry experts, whom we call Lab Advisors.
- Full access to the resources and connections of Miskre Labs.
- Built on an established and constantly updating protocol.
- Every startup in the ecosystem uses MIS and KRE, which will boost the utilities of the tokens and grow the ecosystem.

8 Conclusion

In an industry obsessed with wealth, we chose trust. Miskre was born to contend with dubious claims of decentralization and enable a like-minded community to affirm both the philosophical and utilitarian potential of blockchain technology. The MIS/KRE token was engineered by our team, but to us, the token is just a key, the world on the other side of the door is what we're interested in. We inhabit the intersection of blockchain technology and libertarian self-governance and truly hope you will join us. Miskre distributes 100% of its tokens to non-affiliated parties, allowing MISKRE to be to be truly decentralized. MISKRE isn't ours, it's yours.

Miskre is the world's first self-sustaining autonomous protocol governed by a fair, democratic system of self-governance. Miskre Labs will be established all over the world to empower entrepreneurs as well as kickstart an international Miskre ecosystem. Miskre funded projects through Miskre Labs will be backed by a payment gateway system that allows online products and services to be easily enabled. Miskre's mission is to allow everyone-no matter who they are, where they live, or their financial status -to participate in the global economy with full autonomy and freedom.

We created Miskre because we truly believe that blockchain will change the world, freeing us from the constraints of our current financial system. However, given the corruption that is beginning to make its way into the crypto-space, we have decided to create a protocol that will protect and encourage the initial free market values with which the cryptocurrency community was initially created.

We believe that the current ICO craze is detrimental to the development of blockchain as a whole, as most of these companies will inevitably fail, causing skepticism in the cryptocurrency community and hampering mass adoption. This is occurring primarily with the rise of crowdfunding. Startups have begun disguising themselves as cryptocurrencies in order to raise significantly more money than they actually need to sustain business. We want to create a coin that acts counter to this corruption – creating a democratic and equitable coin that can be sustained well into the future.

With all of Miskre's components working in unison, we set the framework for a true decentralized protocol. A system where people greater than us can come and receive all they're worth. The Miskre protocol will be the most advanced and best maintained because united, we are stronger.

"Sometimes it is said that man cannot be trusted with the government of himself. Can he, then be trusted with the government of others? Or have we found angels in the form of kings to govern him? Let history answer this question." ~Thomas Jefferson

9 References

[i] Elaine's Idle Mind: Stick a Fork in Ethereum, http://elaineou.com/2016/07/18/stick-a-fork-in-ethereum/

[ii] https://github.com/neo-project/neo

[iii] Erik Zhang, A Byzantine Fault Tolerance Algorithm for Blockchain http://docs.neo.org/en-us/basic/consensus/whitepaper.html

[iv] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. 2008.

[v] 范捷, 易乐天, 舒继武. 拜占庭系统技术研究综述[J]. 软件学报, 2013, 6: 012.

[vi] Castro M, Liskov B. Practical Byzantine fault tolerance[C]//OSDI. 1999, 99: 173 186.

[vii] Nick Szabo: Trusted Third Parties Are Security Holes. 2001. https://nakamotoinstitute.org/trusted-third-parties/

[viii] Amir Taaki: The libbitcoin Manifesto. 2013. https://nakamotoinstitute.org/libbitcoin-manifesto/

[ix] FairVote, Multi-Winner Ranked Choice Voting. http://www.fairvote.org/multi_winner_rcv_example

Others

- https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentralised-infrastructure
- Andreas M. Antonopoulos: The Internet of Money. 2016.
- https://www.businessinsider.com/how-currency-debasement-contributed-to-fall-of-rome-2016-2
- http://www.theorderoftime.com/politics/cemetery/stout/h/pbb-24.htm