KREDIT

WHITEPAPER

Version: v 1.0.1
Author: The Kredit Project
Date: 27-06-2017
www.kreditproject.org

Abstract

This Whitepaper was authored to act as a base document for "Kredit", detailing the features, functionality and research behind the new anonymous Cryptocurrency, as well as providing insight into the Mission, goals, and objectives of the Kredit project. Our Solution is based off of the Monero code base platform, and incorporates multi-signature outputs and encrypted ring signatures.

Table of contents

Introduction

The Kredit Project is an organization founded in late 2016 for the express purpose of the creation, development, and management of the Kredit Cryptocurrency.

Kredit is a digital cryptographic currency, more specificity, a hard fork in the CryptoNote currency. Kredit's technology is based off of Monero's open source technology for Cryptocurrency creation.

The Kredit project concluded in early 2017 that Hard-Forking Monero project was the best course of action for Kredit's creation due to the unique features, adaptable variables, and market scope for anonymous coins.

In this whitepaper we will be covering firstly, Kredit's orientation; what our mission, vision, and core principles are. Secondly the features of Kredit; what sets us apart from the rest. And Thirdly Kredit's technology; a behind the scenes glance at Kredit functionality.

Get ready to explore Kredit – a private, digital, cryptographic currency in the making!

1- Kredit’s Orientation

1.1-1. Mission

The Kredit project’s mission is to develop Kredit into a force unto `itself, much like Bitcoin is currently. We have identified several traits that we believe a Cryptocurrency needs to not only be successful, but to transcend the ordinary.

And they are:

- Privacy
- Fungibility
- Sustainability
- Security
- Feasibility
- User friendliness
- Integration
- Wide-spread adoption
-

Kredit was born to embody all of the above traits while still having the flexibility to improve and adapt to an ever changing Financial and Crypto environment.

Another important aspect of the Kredit mission and a reason for Kredit’s creation is the introduction of Cryptocurrency into the lives of new users. It’s been proven time and time again that Cryptocurrency is a life-changing catalyst of financial freedom and change in people’s lives, and Kredit wants to expose as many people as it can to the benefits of using Cryptocurrency in daily life.

One new user is one step closer to a complete Crypto-world, and at Kredit we believe that we have the potential to add a substantial amount of mileage toward this goal.

1.1.2- Vision

The Kredit project’s ultimate vision is to see Kredit become a Top leading Cryptocurrency in a Crypto-economy that is functional, developed, widely used, driven by it's users, and adapting to their needs comprised of strong, developed Cryptocurrencies.

A decentralized world is a free one, and the completion of Kredit will bring the world ever closer to this ultimate goal.

10 years down the line we see Kredit being an expansive network with users around the globe enjoying the many benefits and features of the Kredit currency and Kredit marking the history books forever as one of the most successful, integrated, and widely used Cryptocurrencies of all time.

But it doesn’t end there! There’s no end in sight for Kredit, the way it was structured and designed it will continue to exist and thrive long after the founder’s mortal bodies have perished. It’s our sincere hope that generations to come will directly benefit from Kredit as a financial structure

1.1-3 Adoption

A concept close to mind when creating Kredit was Adoption. Adoption not only of Kredit but all Cryptocurrencies is important.

The more Cryptocurrencies are directly linked to real-world usability, function, and value, the more they will be adopted further increasing the overall user base.

Although globally Cryptocurrency adoption is on an upward trend, we at Kredit want to make sure that we’re doing the most we can to bolster and nurture user adoption by making Kredit user-friendly on all fronts.

We want to make it simple and easy for everyday users to conduct transactions, and for Businesses to start accepting Kredit as a form of payment.

1.4- Innovation

Another value Kredit believes in strongly is innovation, our team never stops analysing and innovating new applications, uses, and improvements for our currency and network, we’re forever testing the limits of what a Cryptocurrency can be used for.

1.5- Dedication

Above all else the Kredit team is dedicated to what we do. Unlike a Business or organization that's simply going through the motions trying to make a Dollar or two, we're quite literally living our dream as Crypto-pioneers.

The creation and development of Kredit is a personal dream of the founders and as such are devoted fully to getting Kredit airborne and soaring towards success.

1.6- Team

Teamwork is an integral part of any organization, at Kredit we take this a step further. All Kredit team members exhibit a unique blend of passion for Cryptocurrency, Professional work ethic, and raw talent. We’ve built and are continuing to build a team that is able to take Kredit to the place it was meant to be, the top.

2- Kredit Features

2.2.1- Fungibilty

Fungibility is a property that can be defined as “Inter-changable value” for example a dollar is interchangeable with another dollar and therefore is fungible.

Bitcoin and other cryptocurrencies that have transparent blockchains however are not fungible. This is due to the fact that any Coin with enough effort can be traced back to it’s origin and in fact there are many agencies and organizations that primarily do exactly that. Bitcoins are often blacklisted by certain organizations and not accepted as payment due to their previous use in illicit activities among other reasons.

But if you aren’t engaging in illicit activities there’s no need to worry right? Wrong, any coins you receive could have been used in illicit activities further down the blockchain potentially creating complications for you. Imagine you’re at the grocery store and the clerk tells you that you can’t pay for your groceries using your $100 Bill because it was used to buy drugs 3 years ago, doesn’t seem reasonable does it?

That’s why Kredit has concluded that any cryptocurrency with a transparent blockchain is not fungible, due to the long history attached to every coin, one Bitcoin simply does not equal another.

We’ve ensured that every Kredit is totally fungible and free of any influencing factors that could lead to any form of “Blocking”, “Flagging”, or otherwise denial of use.

2.2- Security

Security has been a hot topic of discussion when it comes to Cryptocurrencies for a long time. The security of many Cryptocurrencies is being called into question due to the inherent dangers of the online world such as hacking attacks and data breaches.

At Kredit we've put our minds together and formed a security policy to prevent, deter, and eliminate the threat of external malicious attacks on our system. We're all about dynamic security, there's no such thing as a 100% impenetrable system however we're doing our best to come awfully close with planned regular security updates and enhanced security measures.

Cryptocurrencies as a whole are on the forefront of online security and encryption. Cryptography is quite literally the study of secure communication and encryption.

When it comes to the safety and security of our users we take no short cuts, keeping our user's private information private is one of our top priorities, and we've got the technology to make this possible.

2.3- Privacy

Privacy is without a doubt one of the most important features of any Cryptocurrency. Bitcoin and other Cryptocurrencies with transparent Blockchains claim to be anonymous when in actual fact they are pseudo- anonymous.

We touched on earlier how transparent blockchains detract from the fungible value of a coin, but they also pose a serious privacy risk too. Using a pseudonym to conduct Bitcoin transactions is much like wearing a baraclava in public, while you might be hiding your identity in the short term, anyone following you and seeing what stores you go to, who pays you money, and who you give money to will soon be able to piece together who exactly you are. The only difference here is that using Bitcoin all this information is public and accessible at any time online, no one has to actually follow you around.

When you use Kredit, dynamic ring signatures and our analysis resistant blockchain render you 100% anonymous allowing you to immerse yourself in complete privacy, and you can breathe easy knowing that while conducting your business, your information is inaccessible to prying eyes.

2.4- Feasibility

One of the core elements The Kredit project incorporated in designing Kredit was it’s use as a feasible investment vehicle. We want Kredit to be a beacon of success in the Cryptocurrency world and we’re of the belief that all our users, big and small, are entitled to a share in the prosperity. To make this possible we’ve made sure that using Kredit makes not only practical sense, but Financial sense as well.

2.5- Sustainability

“Slow and steady wins the race” The tortoise said to the hare. Kredit hasn’t strayed far from this ancient proverb.

While Kredit is all about profit we also keep the concept of sustainability close to heart. There can be no shortcuts to getting Kredit to the level we ultimately desire. That’s why Kredit was designed for the long run, incorporating measures to make sure that Kredit can withstand the test of time, and build a large user base with a dynamic network that’s always adapting along with it’s users.

The Crypto-world is rife with Alt-coins and Scam-coins that are either outright dishonest or horribly balanced . We’ve set up Kredit for long-term success by making sure our parameters are well balanced, even in some cases adaptive to user needs. When it comes to long term sustainability Kredit has made no compromise.

2.6- Speed

Speed is an often touched on point by many Cryptocurrencies, and rightfully so, having a fast network works wonders, especially in the complex world of Cryptocurrency.

At Kredit we've devoted a good portion of our time to make sure that our Network is as fast as possible. From transaction speed to Wallet syncing we've optimized every angle to get Kredit running as fast as it should, and it's an ongoing process! We're devising new ways to save our users even more time and add to the convenience factor of Kredit.

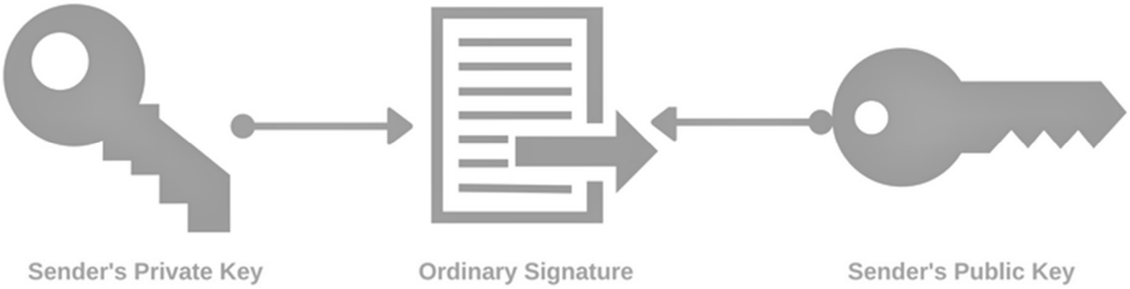
Nothing is more frustrating than waiting hours for a Transaction to be processed or a function to work. To us, speed isn't a luxury, it's a necessity. After all, Time is money!

3- Kredit Technology

3.3.1- Untraceable payments

Generic Cryptocurrency verification processes include using the public key of the transaction signer, this is needed because it proves that the signer is in possession of the private key that matches his public key. However at Kredit we believe that this generic verification process creates a large security gap.

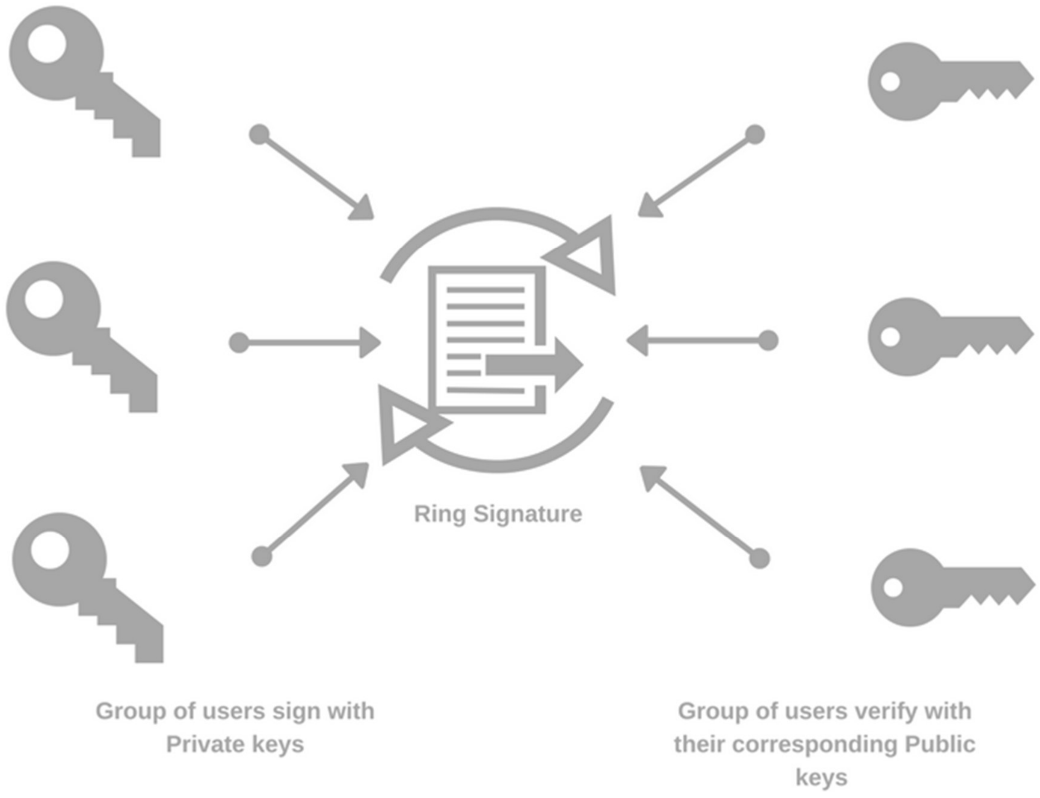
Figure 1: Ordinary Cryptocurrency signature



At Kredit we employ Ring Signature technology. The Ring signature verification method makes use of multiple different public keys during one verification in a group of people, still each with their own public and private keys.

The main difference here being that looking from an external perspective it's impossible to determine who within the group is actually requesting the transaction.

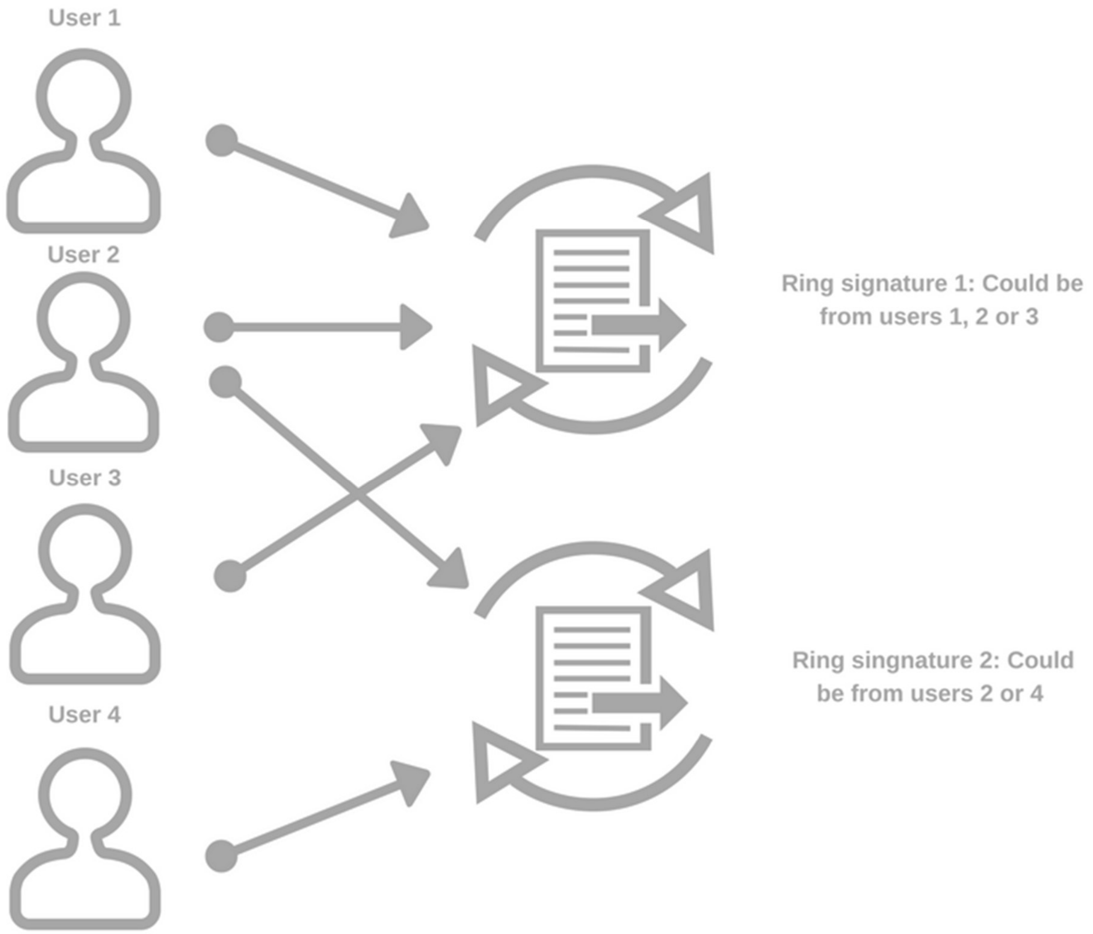
Figure 2: Ring Signature


Ring Signature
Group of users sign with Private keys
Group of users verify with their corresponding Public keys

Using this concept to send Kredit transactions ensures users that: A- Transaction creators are eligible to spend the correct amount and B- Transaction creators' identities are indistinguishable from the other users' public keys used to make the Ring signature.

Kredit Ring signatures combine functionality with privacy seamlessly.

Figure 3: Ring Signature ambiguity


User 1
User 2
User 3
User 4
Ring signature 1: Could be from users 1, 2 or 3
Ring singnature 2: Could be from users 2 or 4

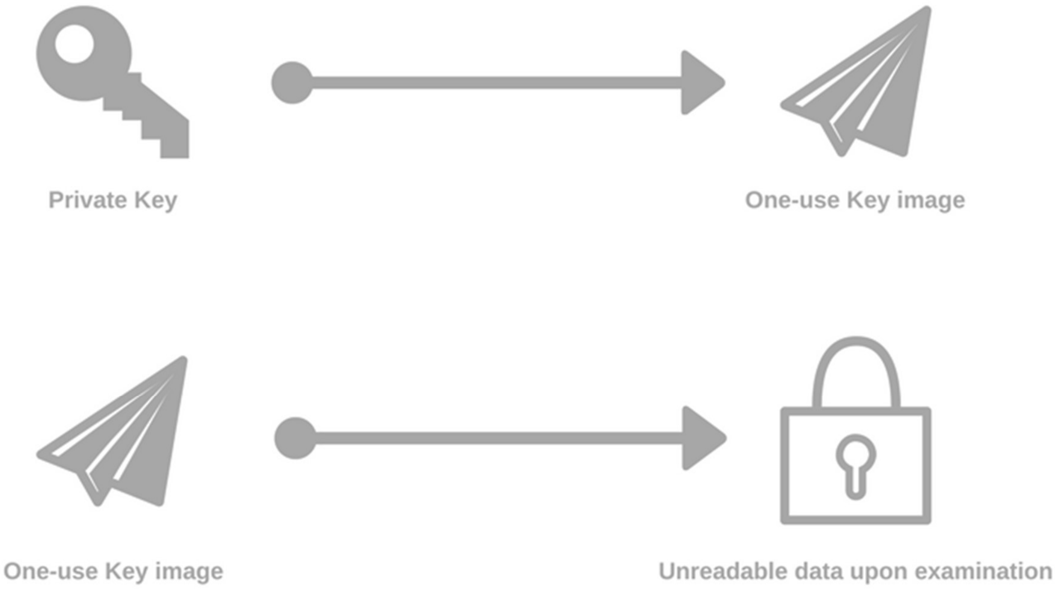
It's worth mentioning that even though your public key will appear in many Ring signatures that you didn't request hiding other users' identity, it will in no way affect you, or your ability to Send/Receive Kredit.

3.3.2- Double spending proof

100% Anonymous Ring signatures would let users spend the same funds over and over again without consequence, logically this can't work with any financial system.

Kredit fixes this problem by employing a modified traceable ring signature system with a built in feature to restrict Double-spend attacks that are common in other Cryptocurrencies. If a malicious user attempts to create more than one ring signature using the same private key, even if the public keys used are different, the signatures are then linked by the system and flagged as a double-spending attempt.

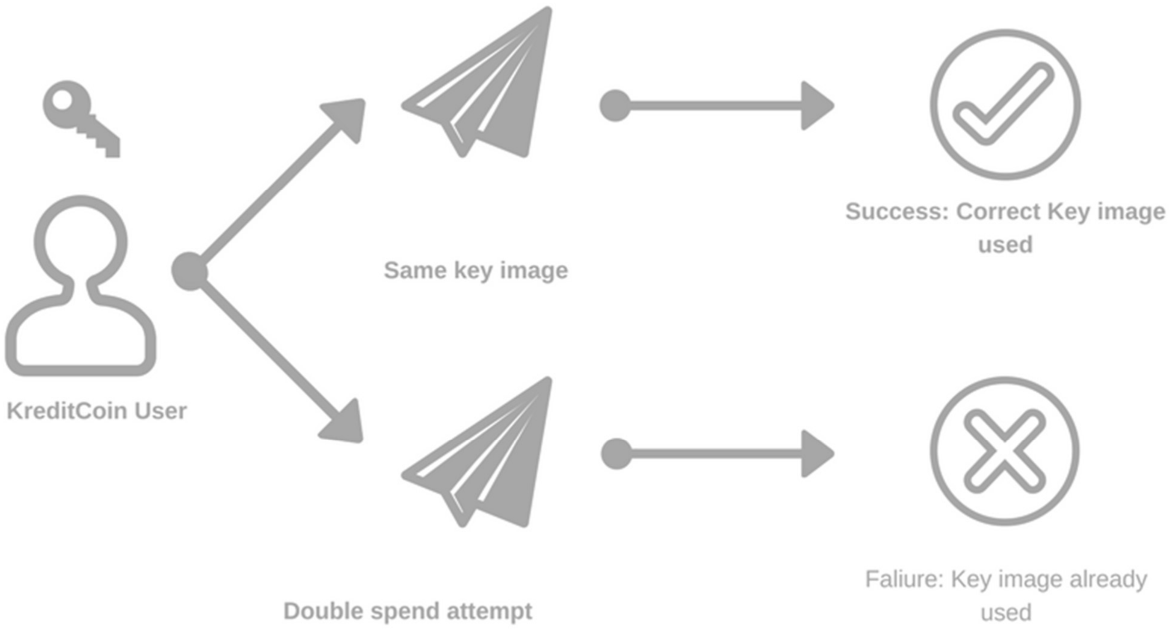
Figure 4: Key images



To do this Kredit uses "Key images", these are one-way cryptographic imprints of private key, No two Key images are

going to be the same, exactly like no two private keys are going to be the same. While key images stand as a measure to prevent double spending, they don't let anyone discover the private key they belong to.

Figure 5: Double-spend Check


Success: Correct Key image used
Same key image
KreditCoin User
Faliure: Key image already used
Double spend attempt

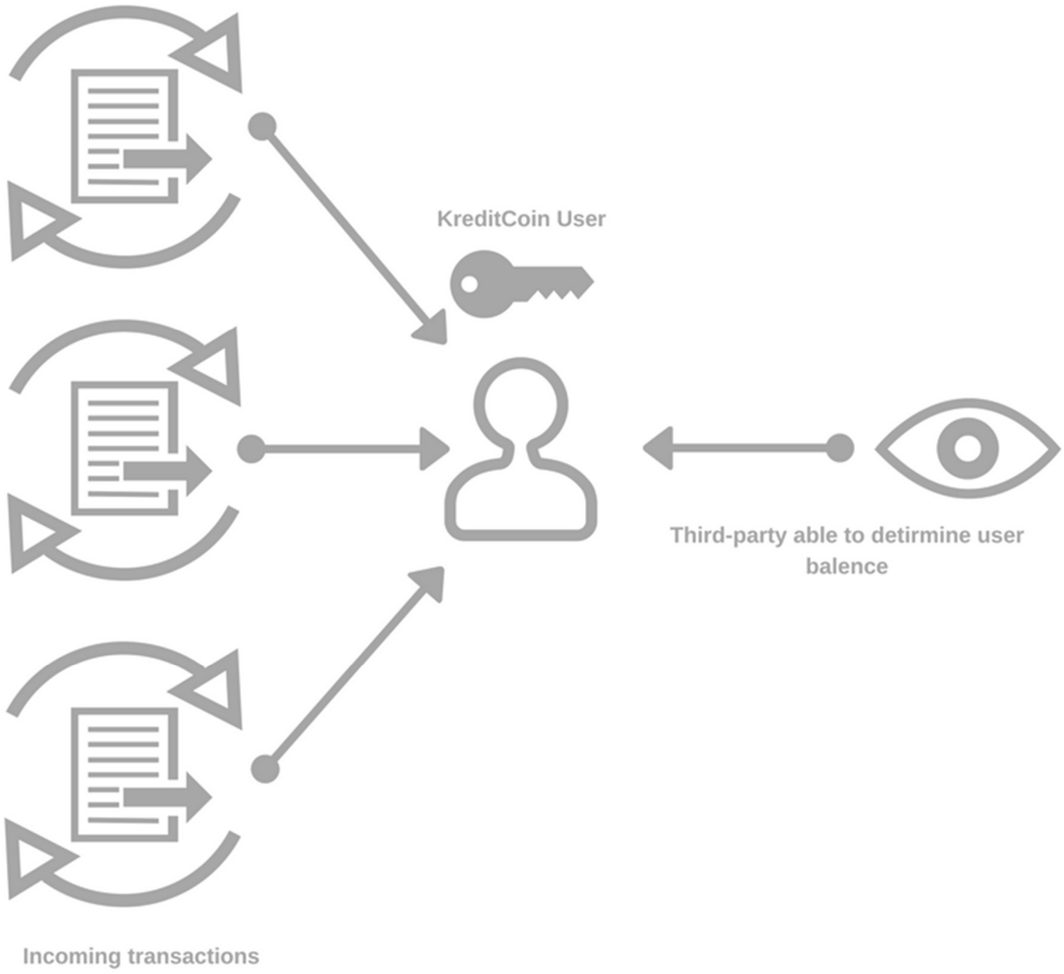
All Kredit users will have installed on their wallets an updated list of all currently used Key images, when you compare the file size to Bitcoin which requires you to download the entire Blockchain (Full record of all transactions), you'll find the Key image database size is much smaller and more convenient. Using Key images is our way of preventing Double-spending, while also keeping our users' identity safe. If you make committing the crime impossible you won't have to punish anyone.

3.3.3- Unlinkable Transactions

When using most Cryptocurrencies, any time you make use of your public address anyone can conduct blockchain analysis to determine your wallet balance by comparing data from your transactions.

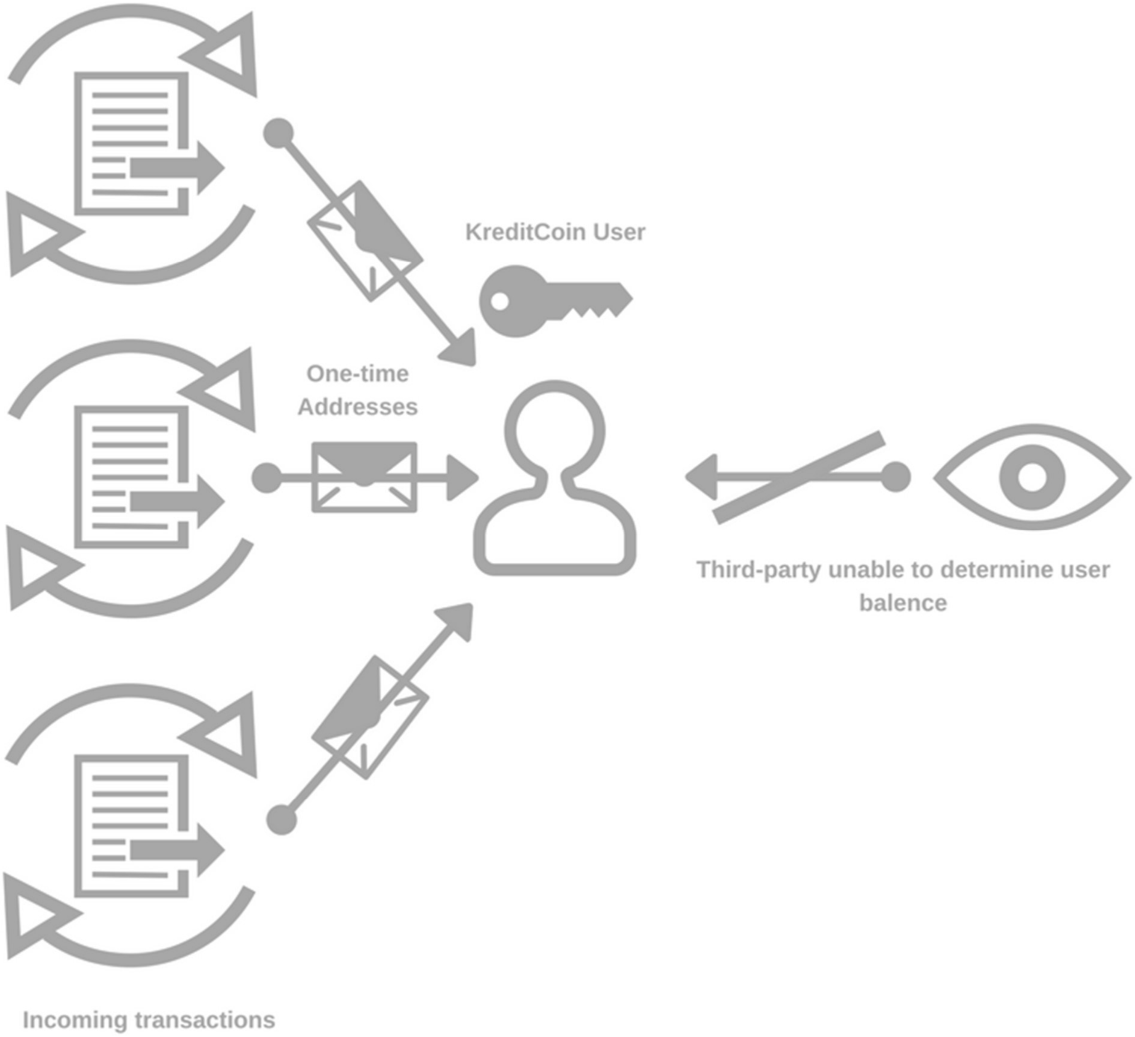
Even when you're protected by Ring signatures your incoming transactions can still be analysed. One can attempt to solve this problem by creating a new public address over and over again with every new transaction, but doing this would soon develop into a chore detracting severely from your convenience factor.

Figure 6: Linkable transactions



Our solution at Kredit is to implement a system in which we automatically create multiple one-time transaction keys derived from your public key for every transaction you conduct. This is possible by modifying the Diffie-Hellman exchange protocol which originally allows two users to produce a mutual secret key which is a derivative from their public keys. We use the receivers public key and random data generated by the sender to generate a unique one-use key to verify the payment.

Figure 7: Unlinkable transactions



Senders can only generate the public part of their keys, while receivers can only read the private part. Therefore third-parties can't possibly analyse transactions as they are a strictly peer-to-peer in the truest sense of the term.

3.3.4- Blockchain analysis resistance

It's possible for anyone, with enough time and resources on their hands, to fully trace any Bitcoin all the way back to when it was mined, finding out the exact path it went along the way, often leading people to conclude who owns what, who sent what, and sometimes who people are.

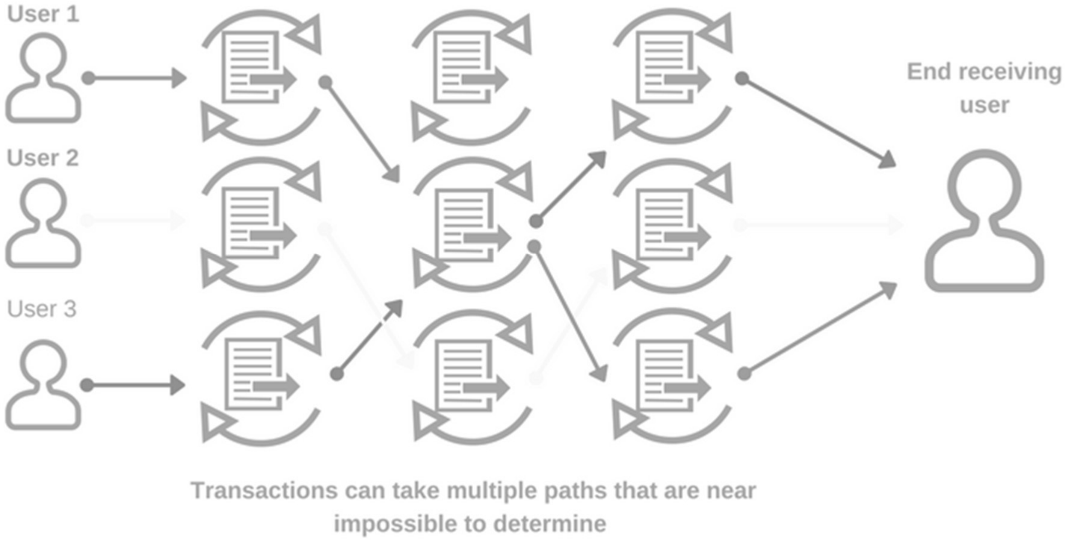
This is attributed to Bitcoin's transparent blockchain, due to it's nature, every transaction has unique variables that are all traceable.

What makes tracing these transactions even easier is users re-using the same addresses multiple times (Even though Satoshi recommended using a different wallet address for each transaction, not that it actually helps much.)

Kredit makes a much different approach, our system is designed to eliminate the risks involved with key re-usage, and traceable variables. We learnt earlier that Ring signatures are derived from a mixture of sender and receiver data, by doing this we provide an anonymous, private, secure platform for our users.

By their very nature Ring signatures are anti-analytical, depending on the size of the signature, the analyst could be trying to determine the original sender in a group of anywhere from 2-1000 people, with every new transaction added to the list making tracking coin paths an increasing impossibility.

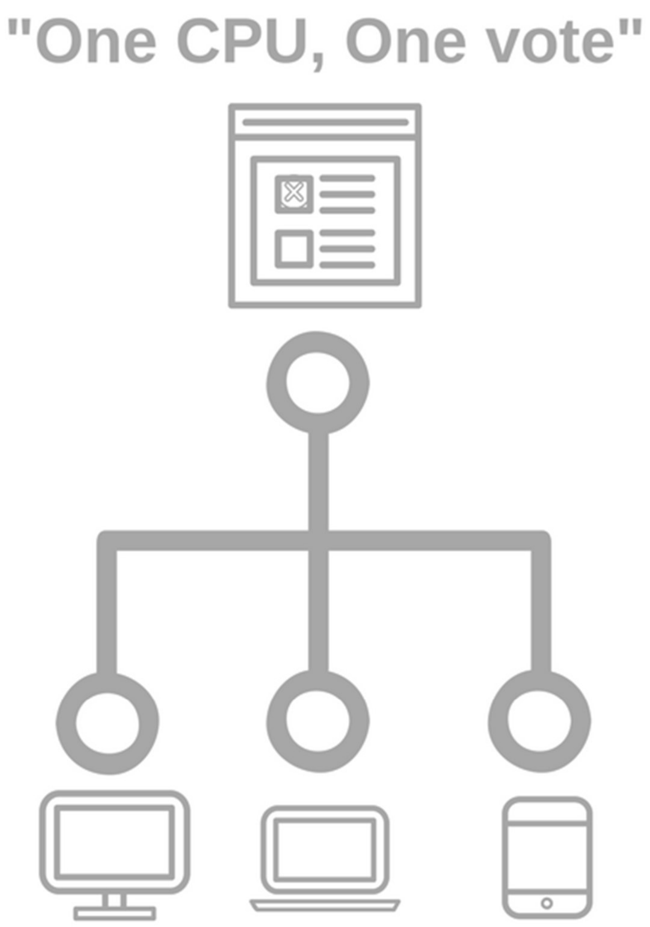
Figure 8: Blockchain ambiguity


User 1
User 2
User 3
End receiving user
Transactions can take multiple paths that are near impossible to determine

3.3.5- Egalitarian proof of work

Kredit's proof of work system is a true rendition of Satoshi's famous phrase "One CPU - One Vote" Our users have the right to vote on New features, transaction order, and supply distribution.

Figure 9: One CPU, One Vote



A Key part of the democratic system is each vote holding the same power. That's why we made sure that all users have equal voting rights.

We employ an Egalitarian proof of work function that is perfectly suited for a multitude of devices. Our scripts are designed to be complex and lightweight, perfect for a CPU to process, but way too

difficult and expensive for advanced mining hardware like ASIC cards and dedicated mining hardware.

Our function depends on a slow stream of memory with an emphasis on latency dependence, every 64 byte long block directly depends on all previous blocks. The resulting effect is an exponential increase in calculation speed.
The algorithm requires only approximately 2 MB per instance, this is because it fits perfectly into the L3 cache present in every core of modern processors, which have been in circulation for many years.

Also a megabyte of internal memory usage will render any ASIC card impractical for use. GPUs and ASICs can run hundreds of instances in parallel but are limited by GDDR5 memory which is infinity slower than an Average CPU's L3 cache.

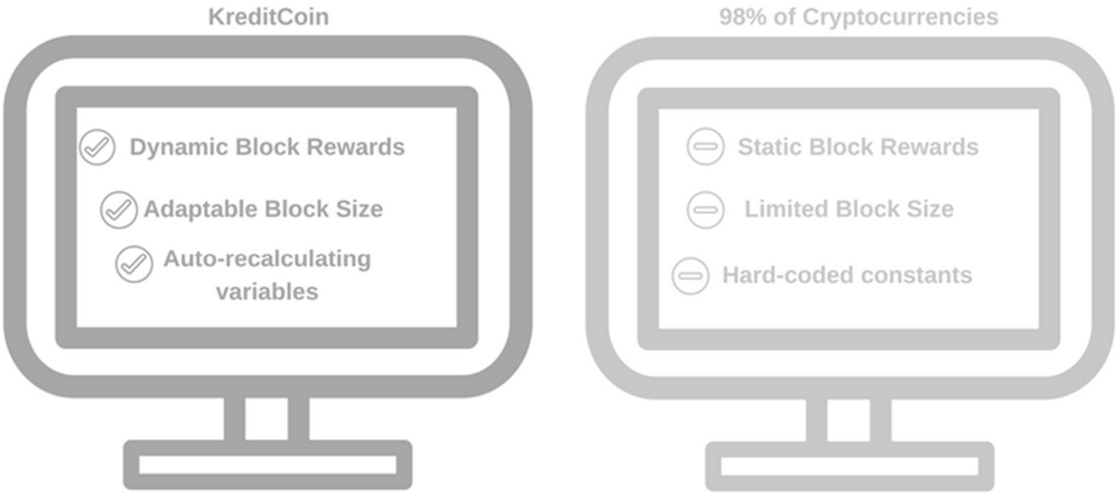
3.3.6- Adaptive parameters

At Kredit we believe that for a currency to be viable, it must not depend on a single person, or a small group of peoples' decision (Someone tell the fiat currencies!).

Bulky Hard-coded constants and magic numbers present in the code of most Cryptocurrencies act as an inhibiting factor for their growth, stability, and overall functionality.

Our solution at Kredit is to incorporate dynamic, auto-recalculating variables in place of these constants to provide a platform for a currency that improves alongside it's users.

Figure 10: Kredit comparison



Almost every crucial limit from Block size to Block Reward is fully adaptive and reactive. Each Kredit Block recalculates difficulty using an algorithm that adds the sum of the work done in the previous 720 blocks and divides it by the amount of time used to solve them, while cutting off 20% of the outliers in the data set. As for our Block size, we employ an algorithm that prevents a bloated inconsistent blockchain, but yet still doesn't apply a "Hard

Limit" onto blocks, allowing for steady growth of blocksize overtime as the network grows and needs to meet the demands of more users.

6. Conclusion

Looking over Kredit as a whole it's plain to see that we're equipped for success. We've got the technology, human resources, and motive to mould Kredit into a Cryptocurrency to rival all others.

We've taken a brief look into Kredit technology, how Ring signatures and an analysis resistant blockchain can maintain user privacy, we've also seen how adaptive parameters can help Kredit evolve to the needs of it's users.

We've explored the founding ideology of Kredit and the beliefs that hold it together at it's core, aside from the programming of course.

We've also looked at what sets Kredit apart from the rest of the pack.

By now I'm sure you agree that Kredit is a genuine recipe for success, in fact we've already started Cooking!

8. Acknowledgements:

Special thanks to the Monero team for making their technology open-source and adaptable to Kredit’s needs. We hope that you continue to grow and prosper.