Fruo Whitepaper

v1.0.3 - 12.01.2018

Ciciru Network Limited

Index

Summary

We live in exciting times. Thanks to different technologies, our lives are made easy and convenient. The Internet seems like the best invention ever made. We only think about the endless possibilities, what we can do online. We don't think that thanks to this technology, our personal information is easily accessible to anyone. You would be really amazed if you'd know how much information different companies and authorities know about you.

Different cryptocurrencies try to solve our privacy concerns by using blockchain technology in many different products. Fruo is dedicated to the privacy of the payments. With Fruo's features, you can receive, send and spend your money without anyone knowing anything about it. There's no possible way to find out if you are using Fruo features, although all these features are based on internet. This means it is possible to stay anonymous, online.

Fruo's main feature is FruoCoin, which is totally untraceable cryptocurrency with many privacy features. It uses latest CryptoNote's technology to achieve private blockchain. FruoCoin sends all payments thru disposable addresses, to ensure there's no way to find out who the payment sender was. More than 99% of all cryptocurrencies are traceable thanks to the public blockchains. But FruoCoin is blockchain analysis resistant - Nobody except the wallet owner can see their wallet balance and transactions history.

Every connection between clients and any Fruo platform is made thru TOR network, which hides clients IP addresses. Without TOR network, it would be possible to find out the cryptocoin users location very easily. Each network device has its own IP address, which is linked to your name and address.

In this whitepaper, we describe specifically how this all works.

The Problem

For over 150 years, there has been a notoriously vague trend in the finance industry. This reality stems from the fact that, there has to be a trusted third party (middleman) for anyone to be involved in money transfer transactions. These third parties (middlemen) include; a central bank, government, or credit card companies. However, these middlemen lack the ability to provide real-time, precise traceability of monetary transactions.

The first point of entry in a formal financial system is a bank account. Be that as it may, about two billion individuals around the world still remain unbanked. The other three billion adults have revealed all their personal information to the banks.

Banks know everything - where from money came and where did you spend it. If they don't like something, they can decline any payment. We may think, banks keep our information safely and securely, without revealing it to someone, but we are wrong. Banks share your statements with different authorities and even with private companies.

Solution to these problems should be Bitcoin. Bitcoin is a virtual currency or cryptocurrency, that's controlled by a decentralized network of users and isn't directly subject to the whims of central banking authorities or national governments. Bitcoin is transparent payment network, where every transaction made is publically visible. This gives us the knowledge, that there are no hidden fees while transferring money in Bitcoin network.

Bitcoin and 99% of all the cryptocurrencies won't provide us privacy, what we need. Although, there's no names or real addresses linked to any cryptocoin address, it's still possible to find out who was the payment sender. Most of the cryptocurrencies use wallets, which know your IP address. Because of that, every transfer you make is linked to your IP address. IP addresses are unique and connected to real persons name and address.

Cryptocurrencies are mostly made for online payments, although most of the payments we make every day is in real life in real places. There's a way to put the amazing blockchain technology to work in our real lives in our everyday payments.

Solution

One former Bitcoin developer says, 2018 may be the year when privacy coins take over the market dominance. “With recent news of net neutrality repeal, people are starting to look for new ways to still remain private online and also in real world.” Bitcoin was created to have transparency in payments and be independent of banks. But bitcoin, with most of the other cryptocurrencies, is too transparent. “It’s a good idea to publically show all the transfers and addresses in the blockchain, this lets us know there are no hidden fees and it shows us exactly when the receiver gets their funds.” Bitcoin shows us that blockchain technology works, and we can achieve the independence of banks and governments “Blockchain works, and now it’s time to add privacy to this amazing technology. We don’t want everybody to know where from we got our money and where did we spend it.” Although, crypto addresses aren’t connected to specific persons, publically, it’s still possible to find out who owns which wallet. And with complete transparency, it’s also possible to track all the spendings.

FruoCoin is decentralized cryptocurrency built on CryptoNote protocol. FruoCoin automatically mixes addresses when sending and receiving coins. This way even the payment receiver won’t know who sent them these coins. FruoCoin is also blockchain analysis resistant, it means no information about payments is publically available. In FruoCoin’s blockchain, nobody can see payment sender, receiver addresses, or even the amount transferred. The only information available in blockchain is that at some time, some payment took place.

For extra privacy, all Fruo’s platforms connect to client thru TOR network, which hides the users IP address. This way, it’s not even possible to find out if someone is using FruoCoin.

Use Fruo Wallet to store all your cryptocurrencies privately.
Use Fruo Exchange to trade all your cryptocurrencies privately.
Use Fruo Pay to pay everywhere in the world privately.
Use Local Fruo to buy FruoCoins privately.

Privacy does matter and Fruo will give you ultimate privacy.

Main Features

FruoCoin - Untraceable transactions, with fast confirmation time and at low cost. This is FruoCoin, which is main Fruo feature. FruoCoin uses the best privacy concerned cryptocurrency protocol called CryptoNote. Every transaction made is sent thru multiple disposable addresses, to make every transaction untraceable. Unlike more than 99% of cryptocurrencies, FruoCoin is blockchain analysis resistant. There's no public information available of any wallet. Only the wallet owner can see their balance and transactions.
Fruo Wallet - Cryptocurrencies are online technologies, it means devices communicate each other to send and receive coins. While communicating, your device sends out your IP address. The IP address is linked to your name and address. To protect yourself and to use cryptocurrencies anonymously, we made Fruo Wallet, which hides your IP address. When starting the wallet, the program automatically connects to TOR network. All the communications between the wallet and others are made thru secure TOR network. Without using Fruo wallet, you cannot be 100% anonymous.
Fruo Pay - Pay with FruoCoins everywhere in the world. With Fruo's prepaid Mastercard, you can pay at every shop, which accepts debit cards, around the world. With Fruo's mobile application, you could pay everywhere in the world which accepts contactless (NFC) payments. While making payment, Fruo automatically exchanges your coins to fiat currency at the current exchange rate.
Fruo Exchange - To get private coins without revealing your identity, or to change your fruocoins to any other currency, use Fruo Exchange. Fruo exchange is decentralized digital currency market which connects thru TOR network. Every trade you make is anonymous. In Fruo exchange, there are no identities connected to your trading account and there are no trading limits.
Local Fruo - People around you are willing to exchange their coins for cash or for any other local payment method. There are no questions asked, just fiat currency for exchange of FruoCoins. All exchanges go thru Escrow to protect users. There are no personal details needed while making the exchange. Another way to get FruoCoins locally is to use special Fruo ATM machines, which accepts your local currency for exchange of FruoCoins.

Timeline

2017

Q1
Dutch Blockchain Hackathon
Through Market Research

Q2
Consulting With Advisors & Experts
New Features & Ideas

Q3
New Team Formation
Partnership with Ciciru Network

Q4
Complete Branding & Design
First Working Prototypes
Community Giveaway
Pre-ICO For First Investors

2018

Q1
Public ICO
Prototype Testing
FruoCoin Launch
Beta Wallet & Exchange
FruoCoin Distribution
FruoCoin Listing On Exchanges
Wallet Anonymisation
Beta Mobile Application

Q2
Merchant Solutions
Payment Gateways
Gold Wallet Release
Contracts With Mastercard
Gold Mobile Application
Mastercard Pre-Orders

Q3
Gold Exchange Platform
Exchange Mobile Integration
Beta Local Fruo
Mastercard distribution

Q4
Online Marketplace
Forex Trading Platform
Gold Local Fruo

* Beta is first working release, without all the final product functionality. Beta release may contain bugs and performance issues.
** Gold is the final release of working product. The gold release has all the final functionality and has no performance issues.

FruoCoin

To provide anonymous payments, we need a working payment system. We cannot use any fiat currency for this system because these are controlled by governments and banks. The best solution is to use blockchain technology and cryptocurrencies. Best anonymous cryptocurrency system is CryptoNote. CryptoNote is the technology that allows the creation of completely anonymous egalitarian cryptocurrencies. There are also already known cryptocurrencies, which uses CryptoNote technology like Monero and Bytecoin.
Although CryptoNote has really good features and makes transactions untraceable, it doesn't have some good features, which another privacy concerned cryptocurrency called Verge has. Verge uses multiple anonymity-centric networks such as Tor and I2P. The IP addresses of the users are obfuscated and the transactions are completely untraceable.

FruoCoin connects amazing CryptoNote functions with Verge's IP hiding technology. FruoCoin is the ultimate combination of anonymous cryptocurrencies. There's no possible way to trace any payment or any wallet owners.

CryptoNote + Verge = FruoCoin

FruoCoin features
Blockchain analysis resistant
No public information about wallet addresses
Payments sent thru one-time disposable addresses
Payment source IP address hidden with TOR network

FruoCoin specifications
Currency symbol: FRU
PoW algorithm: CryptoNight
Total supply: 30’000’000 FRU
Block reward: Smoothly varying
Block time: 60 seconds
Difficulty: Retargets at every block

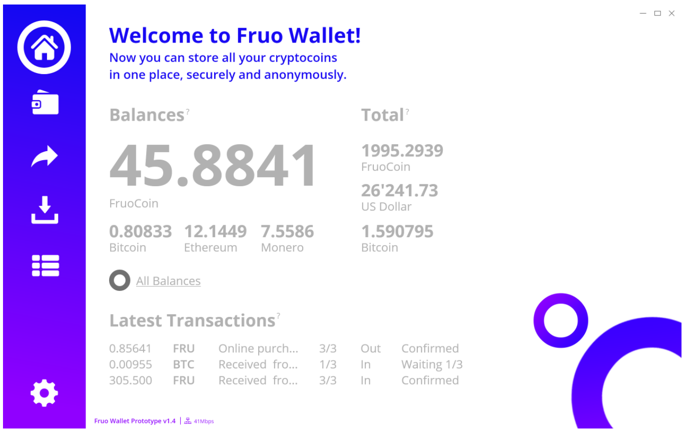
To fund Fruo projects, FruoCoins are for sale in public ICO.
FruoCoins are distributed to ICO and giveaway participators.

Fruo Wallet

You can store your cryptocurrencies in many different ways. Most reliable is to store your coins in the official wallet. There's also a possibility to store your coins offline, in a paper wallet.

Most cryptocoin wallets don't use any privacy techniques and your wallet is connected to your IP address. In public blockchain, there are written only addresses, but it's possible to find out who is the owner of any wallet.

To solve this huge privacy issue with cryptocurrencies, we have made an anonymous wallet, which can store all your most popular currencies. Fruo wallet hides users IP address with TOR network. Every time you start the application, it automatically connects to the blockchain thru multiple TOR nodes. For extra security, Fruo wallet generates new disposable addresses for every transaction made.



Welcome to Fruo Wallet!

Now you can store all your cryptocoins in one place, securely and anonymously.

Balances?

45.8841
FruoCoin

0.80833 Bitcoin · 12.1449 Ethereum · 7.5586 Monero

All Balances

Total?

1995.2939
FruoCoin

26'241.73
US Dollar

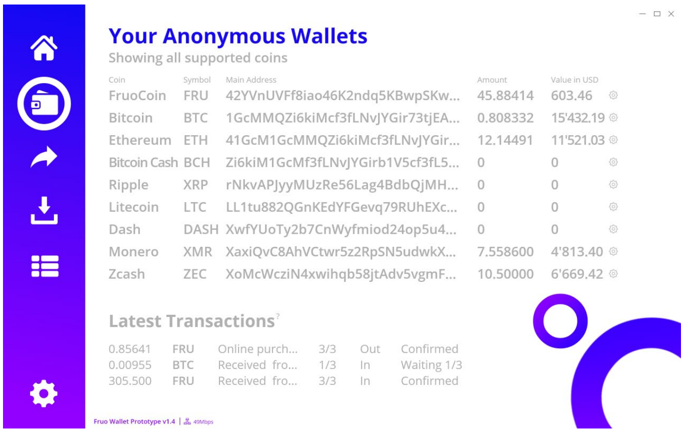
1.590795
Bitcoin

Latest Transactions?

0.85641	FRU	Online purch...	3/3	Out	Confirmed
0.00955	BTC	Received fro...	1/3	In	Waiting 1/3
305.500	FRU	Received fro...	3/3	In	Confirmed

Fruo Wallet Prototype v1.4 | 41Mbps

Fruo wallet home screen, showing most used coins balances, all wallet balances total worth with current exchange rates in different assets, and last 3 transactions made thru the wallet.



Your Anonymous Wallets

Showing all supported coins

Coin	Symbol	Main Address	Amount	Value in USD
FruoCoin	FRU	42YVnUVFf8iao46K2ndq5KBwpSKw...	45.88414	603.46
Bitcoin	BTC	1GcMMQZi6kiMcf3fLNvJYGir73tjEA...	0.808332	15'432.19
Ethereum	ETH	41GcM1GcMMQZi6kiMcf3fLNvJYGir...	12.14491	11'521.03
Bitcoin Cash	BCH	Zi6kiM1GcMf3fLNvJYGirb1V5cf3fL5...	0	0
Ripple	XRP	rNkvAPJyyMUzRe56Lag4BdbQjMH...	0	0
Litecoin	LTC	LL1tu882QGnKEdYFGevq79RUhEXc...	0	0
Dash	DASH	XwfYUoTy2b7CnWyfmiod24op5u4...	0	0
Monero	XMR	XaxiQvC8AhVCtwr5z2RpSN5udwkX...	7.558600	4'813.40
Zcash	ZEC	XoMcWcziN4xwihqb58jtAdv5vgmF...	10.50000	6'669.42

Latest Transactions?

0.85641	FRU	Online purch...	3/3	Out	Confirmed
0.00955	BTC	Received fro...	1/3	In	Waiting 1/3
305.500	FRU	Received fro...	3/3	In	Confirmed

Fruo Wallet Prototype v1.4 | 49Mbps

Fruo wallet wallets screen, showing all available cryptocurrencies and their default addresses with current balances and estimate value in fiat currency. In the bottom, showing last 3 transactions.

Fruo wallet will be available also for mobile devices with slightly different functions. The mobile wallet will also feature Fruo Exchange, Local Fruo, and Fruo Pay functionality.

*Provided screenshots are taken from the first version of Fruo wallet prototype. The real application may differ in design and features.

Fruo Pay

Cryptocurrencies are mainly made for online use. The system is too complex for newbies and nontechies. Places which accepts cryptocurrencies uses mainly scanning QR-code function and then sending payments manually. Using this outdated method may be really problematic because most commonly know cryptocurrency confirmation times are up to 10 hours. Merchants give away products without waiting for the confirmations. Payments may not get the confirmations at all, or by the time payment is confirmed, the coin is worth much less. This leaves merchants to loss, and they don't want to accept innovative payments anymore.

To solve the real-life payment problem, we made Fruo Pay. Fruo Pay has 2 different functionality features - Fruo Mobile application and Fruo Pre-Paid Mastercard.

In the app, Fruo Pay uses NFC or WiFi direct function to connect with Merchant device. The merchant receives paid FruoCoins instantly, and they can spend them or exchange for fiat currency immediately. The program is totally safe and protected by latest 256-bit SSL encryption. This way, merchants have no need to wait for the confirmations, and the client can spend only the coins available in his wallet.

Fruo Pre-Paid Mastercard is an option, which enables to spend FruoCoins in everywhere in the world which accepts regular card payments. Fruo Mastercard has also contactless tap to pay function, to make paying easier than ever. Fruo Mastercard is connected to users mobile application. While paying, Fruo card automatically exchanges FruoCoins into local fiat currency with the current exchange rate. Merchants receive payment in their currency, like with any other card payment made.

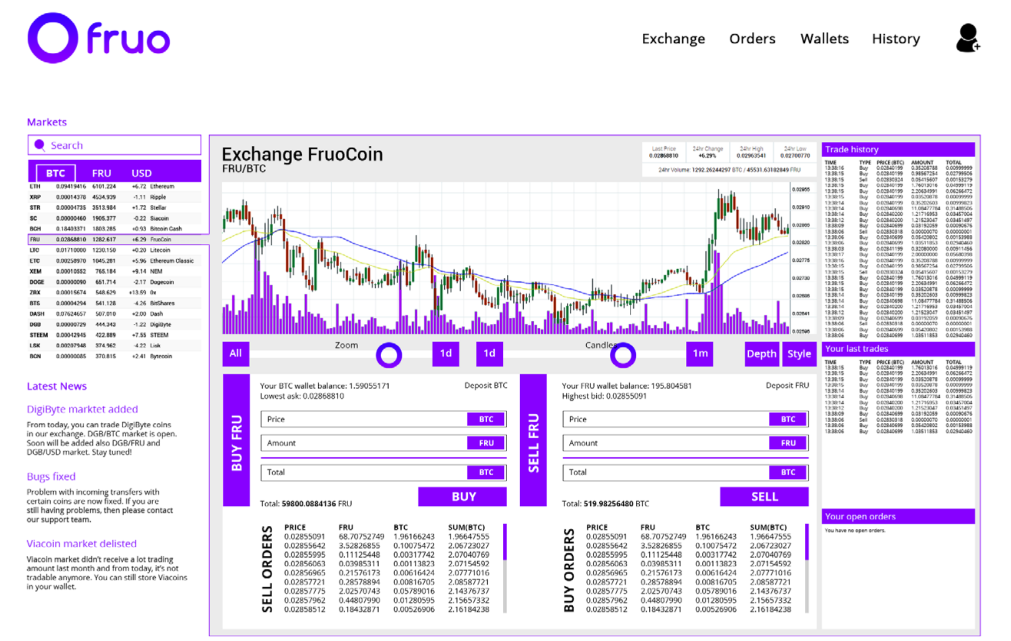
Fruo Pre-Paid Mastercard Prototype

Fruo Exchange

There are really many exchanges out there, for really much cryptocoins. At the beginning of 2018, there is total of 1400 cryptocurrencies and 8000 different currency pairs tradable. About 170 exchange platforms allow you to trade different cryptocurrencies. It's really hard to choose the most reliable trading platform, where to play with your cryptos. There's no exchange platform out there, where are no problems and bad reviews. Each exchange has different requirements for their clients and different limits. And there is no exchange, where you can trade all your favorite cryptocurrencies in one place. At the end you have accounts in 10 different exchange, each with different login details and each has your documents. Holding coins in such exchanges may be a bad idea because the coins are actually in exchanges wallet, not in yours. Exchanges are like banks, they know all your personal information and they control your money. They also set limits to your funds.

Fruo Exchange is decentralized exchange platform with no trading limits. User accounts are wallet based, not persons based. Fruo exchange won't ask any personal details about you, even not your email address. While registering you will get a FruoCoin address with the public and private key. And you need to choose the password. You can log in with your username and password, to restore your password you need to know your public and private address.
Fruo Exchange is not connected to your device directly, because it may reveal your IP address. While accessing Fruo Exchange, your device automatically connects to exchange thru TOR network. This way, nobody can ever know that you are using Fruo's Exchange platform to trade your coins.

Screenshot of Fruo Exchange Platform Alpha Version



Markets

ETH	0.09419416	6101.224	+6.72	Ethereum
XRP	0.00014378	4534.939	-1.11	Ripple
STR	0.00004735	3513.984	+1.72	Stellar
SC	0.00000460	1905.377	-0.22	Siacoin
BCH	0.18403371	1803.285	+0.93	Bitcoin Cash
FRU	0.02868810	1282.617	+6.29	FruoCoin
LTC	0.01710000	1230.150	+0.20	Litecoin
ETC	0.00258970	1045.281	+5.96	Ethereum Classic
XEM	0.00010552	765.184	+9.14	NEM
DOGE	0.00000090	651.714	-2.17	Dogecoin
ZRX	0.00015674	548.629	+13.59	0x
BTS	0.00004294	541.128	-4.26	BitShares
DASH	0.07624657	507.010	+2.00	Dash
DGB	0.00000729	444.343	-1.22	DigiByte
STEEM	0.00042945	422.889	+7.55	STEEM
LSK	0.00207948	374.962	-4.22	Lisk
BCN	0.00000085	370.815	+2.41	Bytecoin

Latest News

DigiByte marktet added

From today, you can trade DigiByte coins in our exchange. DGB/BTC market is open. Soon will be added also DGB/FRU and DGB/USD market. Stay tuned!

Bugs fixed

Problem with incoming transfers with certain coins are now fixed. If you are still having problems, then please contact our support team.

Viacoin market delisted

Viacoin market didn't receive a lot trading amount last month and from today, it's not tradable anymore. You can still store Viacoins in your wallet.

Exchange FruoCoin
FRU/BTC

Last Price	24hr Change	24hr High	24hr Low
0.02868810	+6.29%	0.02963541	0.02700770

24hr Volume: 1292.26244297 BTC / 45531.63182849 FRU

Your BTC wallet balance: 1.59055171 Deposit BTC
Lowest ask: 0.02868810

Price BTC
Amount FRU
Total BTC

Total: **59800.0884136** FRU

SELL ORDERS

PRICE	FRU	BTC	SUM(BTC)
0.02855091	68.70752749	1.96166243	1.96647555
0.02855642	3.52826855	0.10075472	2.06723027
0.02855995	0.11125448	0.00317742	2.07040769
0.02856063	0.03985311	0.00113823	2.07154592
0.02856965	0.21576173	0.00616424	2.07771016
0.02857721	0.28578894	0.00816705	2.08587721
0.02857775	2.02570743	0.05789016	2.14376737
0.02857962	0.44807990	0.01280595	2.15657332
0.02858512	0.18432871	0.00526906	2.16184238

Your FRU wallet balance: 195.804581 Deposit FRU
Highest bid: 0.02855091

Price BTC
Amount FRU
Total BTC

Total: **519.98256480** BTC

BUY ORDERS

PRICE	FRU	BTC	SUM(BTC)
0.02855091	68.70752749	1.96166243	1.96647555
0.02855642	3.52826855	0.10075472	2.06723027
0.02855995	0.11125448	0.00317742	2.07040769
0.02856063	0.03985311	0.00113823	2.07154592
0.02856965	0.21576173	0.00616424	2.07771016
0.02857721	0.28578894	0.00816705	2.08587721
0.02857775	2.02570743	0.05789016	2.14376737
0.02857962	0.44807990	0.01280595	2.15657332
0.02858512	0.18432871	0.00526906	2.16184238

Trade history

TIME	TYPE	PRICE (BTC)	AMOUNT	TOTAL
13:38:16	Buy	0.02840199	0.35208788	0.00999999
13:38:15	Buy	0.02840199	0.98567254	0.02799506
13:38:15	Sell	0.02830324	0.05415607	0.00153279
13:38:15	Buy	0.02840199	1.76013016	0.04999119
13:38:15	Buy	0.02840199	2.20634991	0.06266472
13:38:15	Buy	0.02840199	0.03520878	0.00099999
13:38:14	Buy	0.02840199	0.35202603	0.00999823
13:38:14	Buy	0.02840698	11.08477784	0.31488506
13:38:14	Buy	0.02840200	1.21716953	0.03457004
13:38:12	Buy	0.02840200	1.21523047	0.03451497
13:38:09	Buy	0.02840699	0.03192059	0.00090676
13:38:06	Sell	0.02830318	0.00000070	0.00000001
13:38:06	Buy	0.02840699	0.05420802	0.00153988
13:38:06	Buy	0.02840699	1.03511853	0.02940460
13:38:03	Buy	0.02841199	0.32080000	0.00911456
13:38:17	Buy	0.02840199	2.00000000	0.05680398
13:38:16	Buy	0.02840199	0.35208788	0.00999999
13:38:15	Buy	0.02840199	0.98567254	0.02799506
13:38:15	Sell	0.02830324	0.05415607	0.00153279
13:38:15	Buy	0.02840199	1.76013016	0.04999119
13:38:15	Buy	0.02840199	2.20634991	0.06266472
13:38:15	Buy	0.02840199	0.03520878	0.00099999
13:38:14	Buy	0.02840199	0.35202603	0.00999823
13:38:14	Buy	0.02840698	11.08477784	0.31488506
13:38:14	Buy	0.02840200	1.21716953	0.03457004
13:38:12	Buy	0.02840200	1.21523047	0.03451497
13:38:09	Buy	0.02840699	0.03192059	0.00090676
13:38:06	Sell	0.02830818	0.00000070	0.00000001
13:38:06	Buy	0.02840699	0.05420802	0.00153988
13:38:06	Buy	0.02840699	1.03511853	0.02940460

Your last trades

TIME	TYPE	PRICE (BTC)	AMOUNT	TOTAL
13:38:15	Buy	0.02840199	1.76013016	0.04999119
13:38:15	Buy	0.02840199	2.20634991	0.06266472
13:38:15	Buy	0.02840199	0.03520878	0.00099999
13:38:15	Buy	0.02840199	0.03520878	0.00099999
13:38:14	Buy	0.02840199	0.35202603	0.00999823
13:38:14	Buy	0.02840698	11.08477784	0.31488506
13:38:14	Buy	0.02840200	1.21716953	0.03457004
13:38:12	Buy	0.02840200	1.21523047	0.03451497
13:38:09	Buy	0.02840699	0.03192059	0.00090676
13:38:06	Sell	0.02830318	0.00000070	0.00000001
13:38:06	Buy	0.02840699	0.05420802	0.00153988
13:38:06	Buy	0.02840699	1.03511853	0.02940460

Your open orders

You have no open orders.

Local Fruo

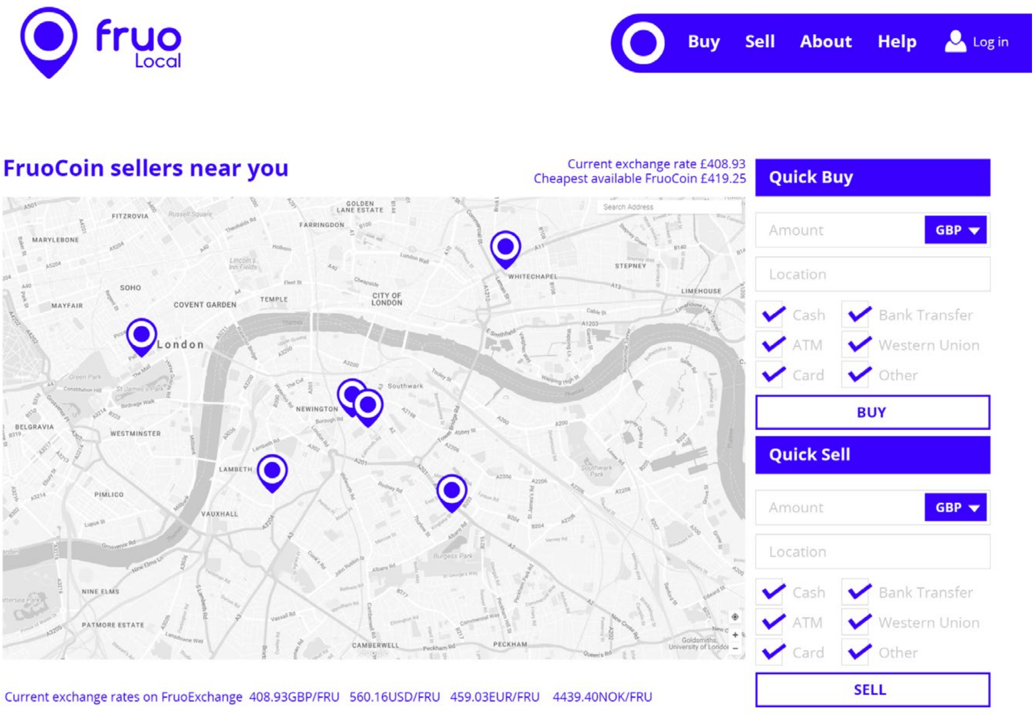
Buying cryptocurrencies with fiat currency may be complicated and will take a lot of time. The first time, exchanges ask really much information about you and they need to prove your identity. This may take weeks. If you need cryptocurrencies faster, then the ideal solution is to buy them from people around you.

Local Fruo is a decentralized platform, which connects buyers and sellers. At Local Fruo, people can post their selling and buy ads for free. People choose their own requirements for the trade and payment methods. People can even choose their own pricing if they don't want to sell at the current market rate.

Local Fruo won't ask any personal details from seller or buyers. To sell FruoCoins, users have to transfer their coins into the Local Fruo wallet. Buyers will receive their coins into their own FruoCoin address. Coins won't be released before both buyer and seller confirms, everything is OK.

Other Local Fruo feature will be local ATM machines, which accept cash for an exchange of FruoCoins. Also, it's possible to sell your FruoCoins to ATM machine and receive cash for return.

To make the trade private and anonymous, using Local Fruo platform, your device automatically connects thru TOR network. This way, you can buy FruoCoins with your local payment method or cash, and remain 100% anonymous.



FruoCoin sellers near you

Current exchange rate £408.93
Cheapest available FruoCoin £419.25

Current exchange rates on FruoExchange 408.93GBP/FRU 560.16USD/FRU 459.03EUR/FRU 4439.40NOK/FRU

Screenshot of Local Fruo web platform prototype

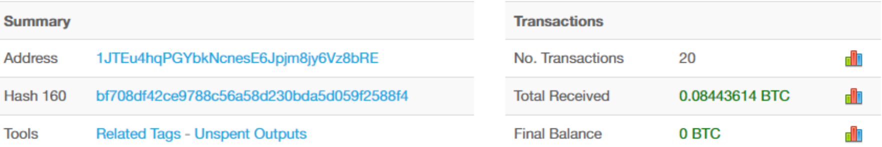
Bitcoin problems

Bitcoin is a virtual currency or cryptocurrency, that's controlled by a decentralized network of users and isn't directly subject to the whims of central banking authorities or national governments. Bitcoin is by far the most popular and widely used cryptocurrency. All other cryptocurrencies are called altcoins. Bitcoin is not perfect, that's why we need alternative cryptocurrencies (altcoins). Altcoins are made to improve Bitcoin functionality and to use Bitcoin's blockchain technology in various projects.

FruoCoin solves most of Bitcoin problems. These are the biggest problems with Bitcoin.

1. Traceability of transactions
Privacy and anonymity are the most important aspects of electronic cash. Peer-to-peer payments seek to be concealed from third party's view, a distinct difference when compared with traditional banking. In particular, T. Okamoto and K. Ohta described six criteria of ideal electronic cash, which included "privacy: relationship between the user and his purchases must be untraceable by anyone. From their description, we derived two properties which a fully anonymous electronic cash model must satisfy in order to comply with the requirements outlined by Okamoto and Ohta:
Untraceability: for each incoming transaction all possible senders are equiprobable.
Unlinkability: for any two outgoing transactions it is impossible to prove they were sent to the same person.
Unfortunately, Bitcoin does not satisfy the untraceability requirement. Since all the transactions that take place between the network's participants are public, any transaction can be unambiguously traced to a unique origin and final recipient. Even if two participants exchange funds in an indirect way, a properly engineered path-finding method will reveal the origin and final recipient. It is also suspected that Bitcoin does not satisfy the second property. Some researchers stated that a careful blockchain analysis may reveal a connection between the users of the Bitcoin network and their transactions. Although a number of methods are disputed, it is suspected that a lot of hidden personal information can be extracted from the public database. Bitcoin's failure to satisfy the two properties outlined above leads us to conclude that it is not an anonymous but a pseudo-anonymous electronic cash system. Users were quick to develop solu-

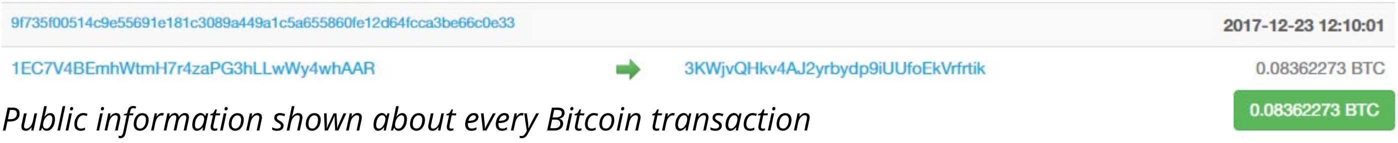
tions to circumvent this shortcoming. Two direct solutions were “laundering services” and the development of distributed methods. Both solutions are based on the idea of mixing several public transactions and sending them through some intermediary address; which in turn suffers the drawback of requiring a trusted third party. Recently, a more creative scheme was proposed by I. Miers et al. “Zerocoin”. Zerocoin utilizes a cryptographic one-way accumulators and zero-knoweldge proofs which permit users to “convert” bitcoins to zerocoins and spend them using anonymous proof of ownership instead of explicit public-key based digital signatures. However, such knowledge proofs have a constant but inconvenient size - about 30kb (based on today’s Bitcoin limits), which makes the proposal impractical. Authors admit that the protocol is unlikely to ever be accepted by the majority of Bitcoin users.



Summary	
Address	1JTEu4hqPGYbkNcnesE6Jpjm8jy6Vz8bRE
Hash 160	bf708df42ce9788c56a58d230bda5d059f2588f4
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	20
Total Received	0.08443614 BTC
Final Balance	0 BTC

Public information shown about every Bitcoin wallet address



9f735f00514c9e55691e181c3089a449a1c5a655860fe12d64fcca3be66c0e33			2017-12-23 12:10:01
1EC7V4BEmhWtmH7r4zaPG3hLLwWy4whAAR	→	3KWjvQHkv4AJ2yrbydp9iUUfoEkVrfrtik	0.08362273 BTC
			0.08362273 BTC

Public information shown about every Bitcoin transaction

2. The proof-of-work function

Bitcoin creator Satoshi Nakamoto described the majority decision making algorithm as “oneCPU-one-vote” and used a CPU-bound pricing function (double SHA-256) for his proof-of-work scheme. Since users vote for the single history of transactions order, the reasonableness and consistency of this process are critical conditions for the whole system. The security of this model suffers from two drawbacks. First, it requires 51% of the network’s mining power to be under the control of honest users. Secondly, the system’s progress (bug fixes, security fixes, etc...) require the overwhelming majority of users to support and agree to the changes (this occurs when the users update their wallet software). Finally this same voting mechanism is also used for collective polls about implementation of some features. This permits us to conjecture the properties that must be satisfied by the proof-of-work pricing function. Such function must not enable a network participant to have a significant advantage over another participant; it

Bitcoin problems

requires a parity between common hardware and high cost of custom devices. From recent examples, we can see that the SHA-256 function used in the Bitcoin architecture does not posses this property as mining becomes more efficient on GPUs and ASIC devices when compared to high-end CPUs. Therefore, Bitcoin creates favourable conditions for a large gap between the voting power of participants as it violates the “one-CPU-one-vote” principle since GPU and ASIC owners posses a much larger voting power when compared with CPU owners. It is a classical example of the Pareto principle where 20% of a system’s participants control more than 80% of the votes. One could argue that such inequality is not relevant to the network’s security since it is not the small number of participants controlling the majority of the votes but the honesty of these participants that matters. However, such argument is somewhat flawed since it is rather the possibility of cheap specialized hardware appearing rather than the participants’ honesty which poses a threat. To demonstrate this, let us take the following example. Suppose a malevolent individual gains significant mining power by creating his own mining farm through the cheap hardware described previously. Suppose that the global hashrate decreases significantly, even for a moment, he can now use his mining power to fork the chain and double-spend. As we shall see later in this article, it is not unlikely for the previously described event to take place.

3. Irregular emission

Bitcoin has a predetermined emission rate: each solved block produces a fixed amount of coins. Approximately every four years this reward is halved. The original intention was to create a limited smooth emission with exponential decay, but in fact we have a piecewise linear emission function whose breakpoints may cause problems to the Bitcoin infrastructure. When the breakpoint occurs, miners start to receive only half of the value of their previous reward. The absolute difference between 12.5 and 6.25 BTC (projected for the year 2020) may seem tolerable. However, when examining the 50 to 25 BTC drop that took place on November 28 2012, felt inappropriate for a significant number of members of the mining community. Figure 1 shows a dramatic decrease in the network’s hashrate in the end of November, exactly when the halving took place. This event could have been the perfect moment for the malevolent individual described in the proof-of-work function section to carry-out a double spending attack.

Bitcoin problems

4. Hardcoded constants
Bitcoin has many hard-coded limits, where some are natural elements of the original design (e.g. block frequency, maximum amount of money supply, number of confirmations) whereas other seem to be artificial constraints. It is not so much the limits, as the inability of quickly changing them if necessary that causes the main drawbacks. Unfortunately, it is hard to predict when the constants may need to be changed and replacing them may lead to terrible consequences. A good example of a hardcoded limit change leading to disastrous consequences is the block size limit set to 250kb1. This limit was sufficient to hold about 10000 standard transactions. In early 2013, this limit had almost been reached and an agreement was reached to increase the limit. The change was implemented in wallet version 0.8 and ended with a 24-blocks chain split and a successful double-spend attack [9]. While the bug was not in the Bitcoin protocol, but rather in the database engine it could have been easily caught by a simple stress test if there was no artificially introduced block size limit. Constants also act as a form of centralization point. Despite the peer-to-peer nature of Bitcoin, an overwhelming majority of nodes use the official reference client developed by a small group of people. This group makes the decision to implement changes to the protocol and most people accept these changes irrespective of their "correctness". Some decisions caused heated discussions and even calls for boycott, which indicates that the community and the developers may disagree on some important points. It therefore seems logical to have a protocol with user-configurable and self-adjusting variables as a possible way to avoid these problems.

5. Bulky scripts
The scripting system in Bitcoin is a heavy and complex feature. It potentially allows one to create sophisticated transactions, but some of its features are disabled due to security concerns and some have never even been used. The script (including both senders' and receivers' parts) for the most popular transaction in Bitcoin looks like this:
<sig> <pubKey> OP DUP OP HASH160 <pubKeyHash> OP EQUALVERIFY OPCHECKSIG.
The script is 164 bytes long whereas its only purpose is to check if the receiver possess the secret key required to verify his signature.

Bitcoin problems

There are also smaller problems, not related to the code, which FruoCoin solves.

1. Bitcoins Are Not Widely Accepted
Bitcoins are still only accepted by a very small group of online merchants. This makes it unfeasible to completely rely on Bitcoins as a currency. There is also a possibility that governments might force merchants to not use Bitcoins to ensure that users' transactions can be tracked more easily.
Solution - Fruo has features, which can be used worldwide. Fruo's prepaid Mastercard is a card, which enables you to pay everywhere in the world. It means all places which accept debit card payments, accept FruoCoin payments.

2. Wallets Can Be Lost
If a hard drive crash or a virus corrupts data, and the wallet file is corrupted, Bitcoins have essentially been "lost". There is nothing that can be done to recover it. These coins will be forever orphaned in the system. This can bankrupt a wealthy Bitcoin investor within seconds with no way form of recovery. The coins the investor-owned will also be permanently orphaned.
Solution - Fruo wallet force you to write down your private key for recovery.You can print out the paper wallet or just write down the private key.

3. You cannot buy Bitcoin without revealing your identity
You can exchange real money for Bitcoins on many sites. The problem is, they want you to confirm your identity and address, even if you want to buy a very small amount of Bitcoins.
Solution - Fruo has ATM machines, which accept cash and you can get FruoCoins as the return. There's also a Local FruoCoins platform, where real people exchange real money for coins without asking anything about you.

Specificied solution

Untraceable Transactions

In this section we propose a scheme of fully anonymous transactions satisfying both untraceability and unlinkability conditions. An important feature of our solution is its autonomy: the sender is not required to cooperate with other users or a trusted third party to make his transactions; hence each participant produces a cover traffic independently.

1. Literature review

Our scheme relies on the cryptographic primitive called a group signature. First presented by D. Chaum and E. van Heyst, it allows a user to sign his message on behalf of the group. After signing the message the user provides (for verification purposes) not his own single public 1This is so-called "soft limit" — the reference client restriction for creating new blocks. Hard maximum of possible blocksize was 1 MB key, but the keys of all the users of his group. A verifier is convinced that the real signer is a member of the group, but cannot exclusively identify the signer. The original protocol required a trusted third party (called the Group Manager), and he was the only one who could trace the signer. The next version called a ring signature, introduced by Rivest, was an autonomous scheme without Group Manager and anonymity revocation. Various modifications of this scheme appeared later: linkable ring signature allowed to determine if two signatures were produced by the same group member, traceable ring signature limited excessive anonymity by providing possibility to trace the signer of two messages with respect to the same metainformation. A similar cryptographic construction is also known as a ad-hoc group signature. It emphasizes the arbitrary group formation, whereas group/ring signature schemes rather imply a fixed set of members. For the most part, our solution is based on the work "Traceable ring signature" by E. Fujisaki and K. Suzuki. In order to distinguish the original algorithm and our modification we will call the latter a one-time ring signature, stressing the user's capability to produce only one valid signature under his private key. We weakened the traceability property and kept the linkability only to provide one-timeness: the public key may appear in many foreign verifying sets and the private key can be used for generating a unique anonymous signature. In case of a double spend attempt these two signatures will be linked together, but revealing the signer is not necessary for our purposes.

Specificied solution

2. Definitions

2.1 Elliptic curve parameters

As our base signature algorithm we chose to use the fast scheme EdDSA, which is developed and implemented by D.J. Bernstein. Like Bitcoin's ECDSA it is based on the elliptic curve discrete logarithm problem, so our scheme could also be applied to Bitcoin in future.

Common parameters are:

q: a prime number; $q = 2^{255} - 19$;
d: an element of Fq; $d = -121665/121666$;
E: an elliptic curve equation; $-x^2 + y^2 = 1 + dx^2y^2$;
G: a base point; $G = (x, -4/5)$;
l: a prime order of the base point; $l = 2^{252} + 27742317777372353535851937790883648493$;
Hs: a cryptographic hash function $\{0, 1\}^* \Rightarrow F_q$;
Hp: a deterministic hash function $E(F_q) \Rightarrow E(F_q)$.

2.2 Terminology

Enhanced privacy requires a new terminology which should not be confused with Bitcoin entities.

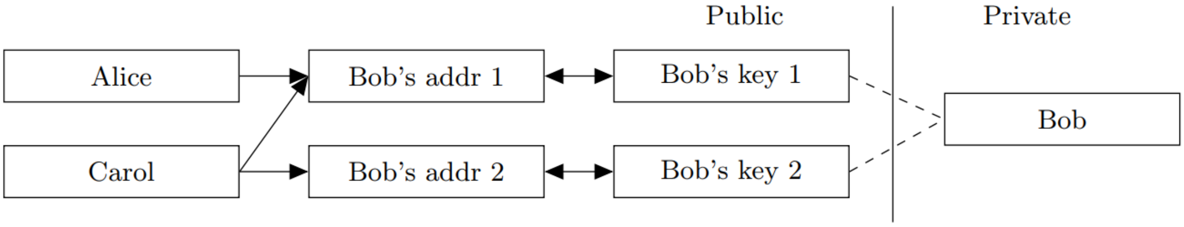
private ec-key is a standard elliptic curve private key: a number a *E* $[1, l - 1]$;
public ec-key is a standard elliptic curve public key: a point $A = aG$;
one-time keypair is a pair of private and public ec-keys;
private user key is a pair (a, b) of two different private ec-keys;
tracking key is a pair (a, B) of private and public ec-key (where $B = bG$ and $a \neq b$);
public user key is a pair (A, B) of two public ec-keys derived from (a, b);
standard address is a representation of a public user key given into human friendly string with error correction;
truncated address is a representation of the second half *(point B)* of a public user key given into human friendly string with error correction.

The transaction structure remains similar to the structure in Bitcoin: every user can choose several independent incoming payments (transactions outputs), sign them with the corresponding private keys and send them to different destinations. Contrary to Bitcoin's model, where a user possesses unique private and public key, in the proposed model a sender generates a one-time public key based on the recipient's address and some random data. In this sense, an incoming transaction for the same recipient is sent to a one-time public key (not directly to a unique address) and only the recipient can recover the corresponding private part to redeem his funds (using his unique private key). The recipient can spend the funds using a ring signature, keeping his ownership and actual spending anonymous.

Specificied solution

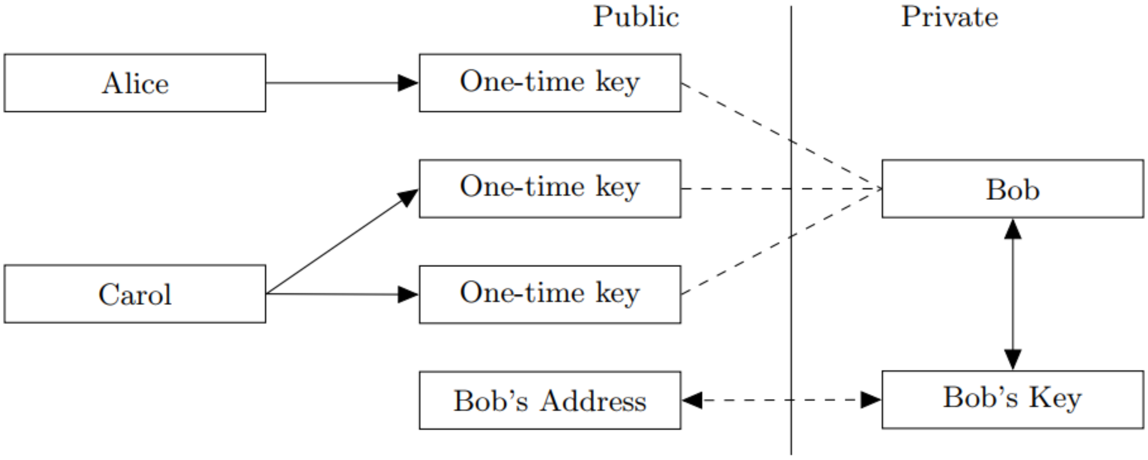
3. Unlinkable payments

Classic Bitcoin addresses, once being published, become unambiguous identifier for incoming payments, linking them together and tying to the recipient's pseudonyms. If someone wants to receive an "untied" transaction, he should convey his address to the sender by a private channel. If he wants to receive different transactions which cannot be proven to belong to the same owner he should generate all the different addresses and never publish them in his own pseudonym.



Traditional Bitcoin keys/transactions model.

We propose a solution allowing a user to publish a single address and receive unconditional unlinkable payments. The destination of each CryptoNote output (by default) is a public key, derived from recipient's address and sender's random data. The main advantage against Bitcoin is that every destination key is unique by default (unless the sender uses the same data for each of his transactions to the same recipient). Hence, there is no such issue as "address reuse" by design and no observer can determine if any transactions were sent to a specific address or link two addresses together.



CryptoNote keys/transactions model.

Specificied solution

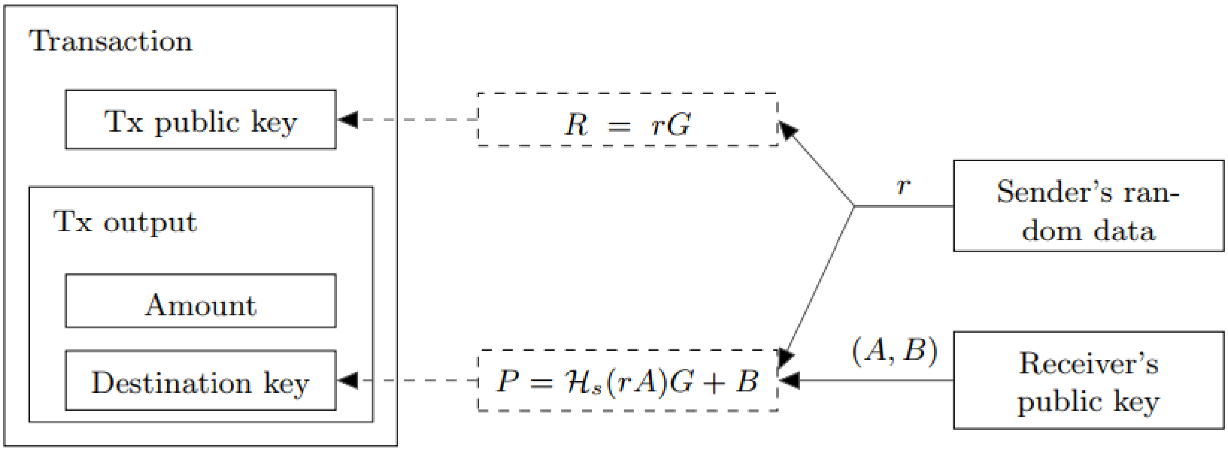
First, the sender performs a Diffie-Hellman exchange to get a shared secret from his data and half of the recipient's address. Then he computes a one-time destination key, using the shared secret and the second half of the address. Two different ec-keys are required from the recipient for these two steps, so a standard CryptoNote address is nearly twice as large as a Bitcoin wallet address. The receiver also performs a Diffie-Hellman exchange to recover the corresponding secret key.

A standard transaction sequence goes as follows:

1. Alice wants to send a payment to Bob, who has published his standard address. She unpacks the address and gets Bob's public key (A, B).

2. Alice generates a random r E [1, l−1] and computes a one-time public key P = H_s(rA)G+B.

3. Alice uses P as a destination key for the output and also packs value R = rG (as a part of the Diffie-Hellman exchange) somewhere into the transaction. Note that she can create other outputs with unique public keys: different recipients' keys (A_i, B_i) imply different P_i even with the same r.

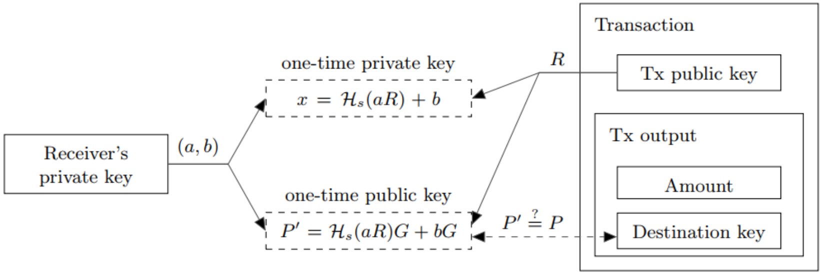


Standard transaction structure.

4. Alice sends the transaction.

5. Bob checks every passing transaction with his private key (a, b), and computes P' = H_s(aR)G + B. If Alice's transaction for with Bob as the recipient was among them, then aR = arG = rA and P' = P.

6. Bob can recover the corresponding one-time private key: x = H_s(aR) + b, so as P = xG.
He can spend this output at any time by signing a transaction with x.



Incoming transaction check.

As a result Bob gets incoming payments, associated with one-time public keys which are unlinkable for a spectator. Some additional notes:

• When Bob "recognizes" his transactions (see step 5) he practically uses only half of his private information: *(a, B)*. This pair, also known as the tracking key, can be passed to a third party (Carol). Bob can delegate her the processing of new transactions. Bob doesn't need to explicitly trust Carol, because she can't recover the one-time secret key p without Bob's full private key (a, b). This approach is useful when Bob lacks bandwidth or computation power (smartphones, hardware wallets etc.).

• In case Alice wants to prove she sent a transaction to Bob's address she can either disclose r or use any kind of zero-knowledge protocol to prove she knows r (for example by signing the transaction with r).

• If Bob wants to have an audit compatible address where all incoming transaction are linkable, he can either publish his tracking key or use a truncated address. That address represent only one public ec-key B, and the remaining part required by the protocol is derived from it as follows: a = H_s(B) and A = H_s(B)G. In both cases every person is able to "recognize" all of Bob's incoming transaction, but, of course, none can spend the funds enclosed within them without the secret key *b*.

4. One-time ring signatures

A protocol based on one-time ring signatures allows users to achieve unconditional unlinkability. Unfortunately, ordinary types of cryptographic signatures permit to trace transactions to their respective senders and receivers. Our solution to this deficiency lies in using a different signature type than those currently used in electronic cash systems. We will first provide a general description of our algorithm with no explicit reference to electronic cash.

A one-time ring signature contains four algorithms: (**GEN, SIG, VER, LNK**):

GEN: takes public parameters and outputs an ec-pair (P, x) and a public key I.

SIG: takes a message m, a set S' of public keys $\{P_i\}_{i}\neq_{s}$, a pair (P_s, x_s) and outputs a signature σ and a set S = S' U {P_s}.

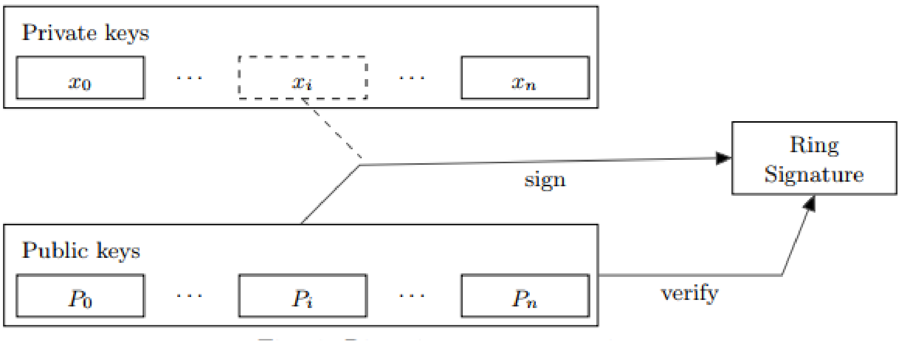
VER: takes a message m, a set S, a signature σ and outputs "true" or "false".

LNK: takes a set I = {I_i}, a signature σ and outputs "linked" or "indep".

The idea behind the protocol is fairly simple: a user produces a signature which can be checked by a set of public keys rather than a unique public key. The identity of the signer is indistinguishable from the other users whose public keys are

Specificied solution

in the set until the owner produces a second signature using the same keypair.



Ring signature anonymity.

GEN: The signer picks a random secret key x E [1, l − 1] and computes the corresponding public key P = xG. Additionally he computes another public key I = xH$_p$(P) which we will call the “key image”.

SIG: The signer generates a one-time ring signature with a non-interactive zero-knowledge

proof using the techniques from. He selects a random subset S’ of n from the other users’ public keys P$_i$, his own keypair (x, P) and key image I. Let *0 ≤ s ≤ n* be signer’s secret index in S (so that his public key is P$_s$).

He picks a random {qi | i = 0 . . . n} and {wi | i = 0 . . . n, i ≠ s} from (1 . . . l) and applies the following transformations:

$$L_i = \begin{cases} q_i G, & \text{if } i = s \\ q_i G + w_i P_i, & \text{if } i \neq s \end{cases}$$

$$R_i = \begin{cases} q_i \mathcal{H}_p(P_i), & \text{if } i = s \\ q_i \mathcal{H}_p(P_i) + w_i I, & \text{if } i \neq s \end{cases}$$

The next step is getting the non-interactive challenge:

$$c = \mathcal{H}_s(m, L_1, \dots, L_n, R_1, \dots, R_n)$$

Finally the signer computes the response:

$$c_i = \begin{cases} w_i, & \text{if } i \neq s \\ c - \sum_{i=0}^{n} c_i \mod l, & \text{if } i = s \end{cases}$$

$$r_i = \begin{cases} q_i, & \text{if } i \neq s \\ q_s - c_s x \mod l, & \text{if } i = s \end{cases}$$

The resulting signature is *σ = (I, c_1, . . . , c_n, r_1, . . . , r_n).*

VER: The verifier checks the signature by applying the inverse transformations:

Specificied solution

$$\begin{cases} L_i' = r_i G + c_i P_i \\ R_i' = r_i \mathcal{H}_p(P_i) + c_i I \end{cases}$$

Finally, the verifier checks if $\sum_{i=0}^{n} c_i \overset{?}{=} \mathcal{H}_s(m, L_0', \ldots, L_n', R_0', \ldots, R_n') \mod l$

If this equality is correct, the verifier runs the algorithm **LNK**. Otherwise the verifier rejects the signature.

LNK: The verifier checks if I has been used in past signatures (these values are stored in the set I). Multiple uses imply that two signatures were produced under the same secret key. The meaning of the protocol: by applying L-transformations the signer proves that he knows such x that at least one $P_i = xG$. To make this proof non-repeatable we introduce the key image as $I = xHp(P)$. The signer uses the same coefficients (r_i, c_i) to prove almost the same statement: he knows such x that at least one $H_p(P_i) = I \cdot x^{-1}$.

If the mapping $x \Rightarrow I$ is an injection:

1. Nobody can recover the public key from the key image and identify the signer;
2. The signer cannot make two signatures with different I's and the same x.

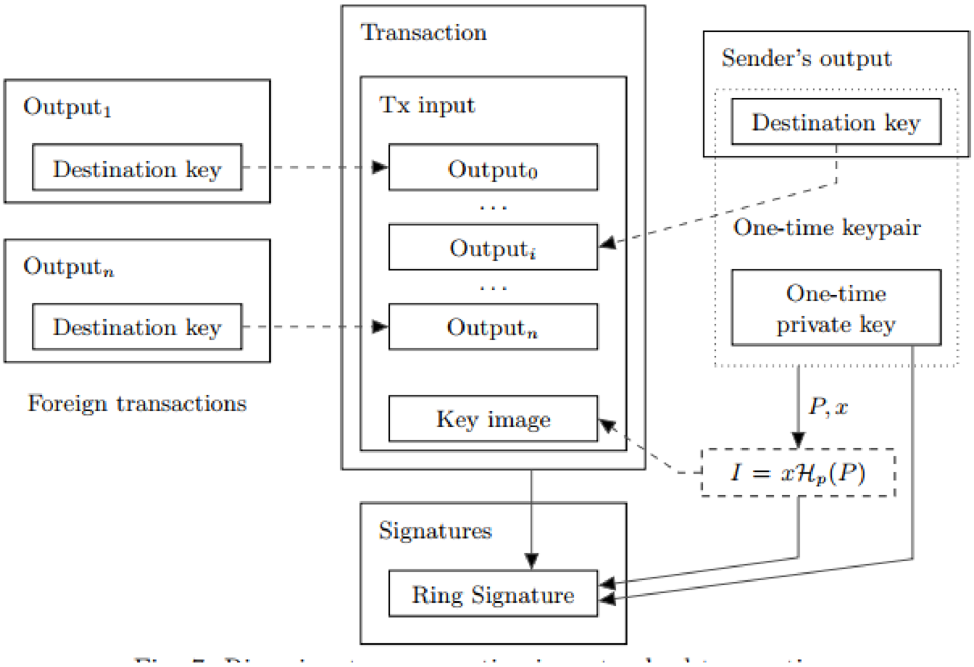
A full security analysis is provided in Appendix A.

5. Standard CryptoNote transaction

By combining both methods (unlinkable public keys and untraceable ring signature) Bob achieves new level of privacy in comparison with the original Bitcoin scheme. It requires him to store only one private key *(a, b)* and publish *(A, B)* to start receiving and sending anonymous transactions. While validating each transaction Bob additionally performs only two elliptic curve multiplications and one addition per output to check if a transaction belongs to him. For his every output Bob recovers a one-time keypair (p_i, P_i) and stores it in his wallet. Any inputs can be circumstantially proved to have the same owner only if they appear in a single transaction. In fact this relationship is much harder to establish due to the one-time ring signature. With a ring signature Bob can effectively hide every input among somebody else's; all possible spenders will be equiprobable, even the previous owner (Alice) has no more information than any observer. When signing his transaction Bob specifies n foreign outputs with the same amount as his output, mixing all of them without the participation of other users. Bob himself (as well as anybody else) does not know if any of these payments have been spent: an output can be used in thousands of signatures as an

Specificied solution

ambiguity factor and never as a target of hiding. The double spend check occurs in the **LNK** phase when checking against the used key images set. Bob can choose the ambiguity degree on his own: n = 1 means that the probability he has spent the output is 50% probability, n = 99 gives 1%. The size of the resulting signature increases linearly as *O(n+ 1)*, so the improved anonymity costs to Bob extra transaction fees. He also can set *n = 0* and make his ring signature to consist of only one element, however this will instantly reveal him as a spender.



Ring signature generation in a standard transaction.

CryptoNote

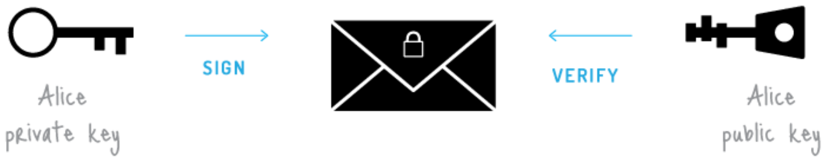
CryptoNote Phylosophy
CryptoNote is the technology that allows the creation of completely anonymous egalitarian cryptocurrencies. A number of our community members have been focused on research and development for more than a decade. We aim to promote the derived principles to influence the contemporary economic paradigm.

The current power distribution on our planet is the legacy of the world where the economy is controlled by the few. The status quo was shaped throughout centuries, making human beings engage in rat races, detrimental rivalry, and bloodshed. In spite of humanity's hope to overcome local crises through education and internationalization, we still fail to have full control over our lives.

However, state-of-the-art advancements in technology, mathematics, and cryptography may become the key to subvert this paradigm. The advent of cryptocurrencies is the first sign that the new world is coming. It is marked with a hope that the economy will interlace with the technology, that communities will set new transparent principles, and impartial cryptographic algorithms will control its implementation.

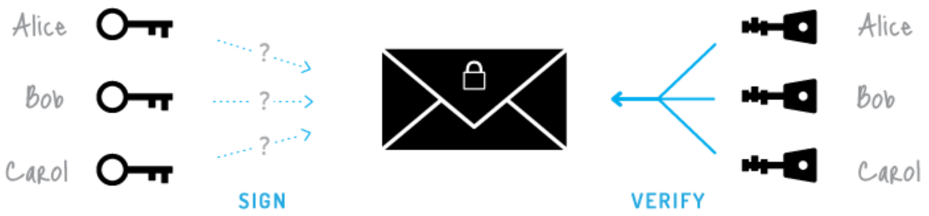
It is in our philosophy to encourage enlightenment through breakthrough innovations. Emancipation begins with laymen getting access to financial resources that will give the oppressed the hope for quality education, drinking water, and a better life. CryptoNote is not about creating yet another digital currency. It is the mindset and concepts that represent the first small step to regain the power over ourselves in order to live peacefully and prosper.

Ring signatures: Untraceable payments
The ordinary digital signature (e.g. (EC)DSA, Schnorr, etc...) verification process involves the public key of the signer. It is a necessary condition, because the signature actually proves that the author possesses the corresponding secret key. But it is not always a sufficient condition.

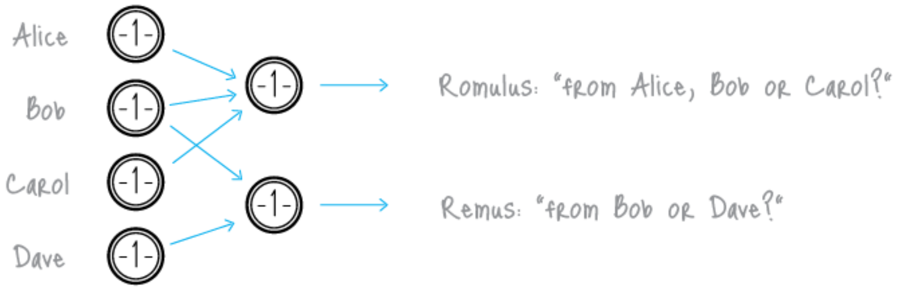


CryptoNote

Ring signature is a more sophisticated scheme, which in fact may demand several different public keys for verification. In the case of ring signature, we have a group of individuals, each with their own secret and public key. The statement proved by ring signatures is that the signer of a given message is a member of the group. The main distinction with the ordinary digital signature schemes is that the signer needs a single secret key, but a verifier cannot establish the exact identity of the signer. Therefore, if you encounter a ring signature with the public keys of Alice, Bob and Carol, you can only claim that one of these individuals was the signer but you will not be able to pinpoint him or her.

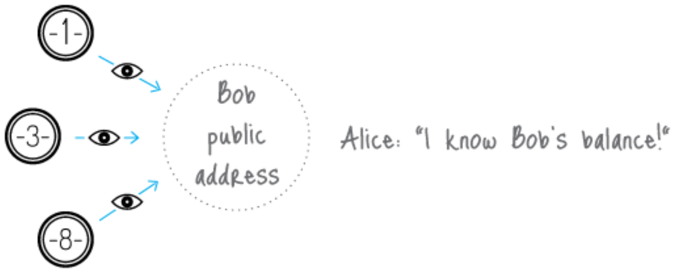


This concept can be used to make digital transactions sent to the network untraceable by using the public keys of other members in the ring signature one will apply to the transaction. This approach proves that the creator of the transaction is eligible to spend the amount specified in the transaction but his identity will be indistinguishable from the users whose public keys he used in his ring signatures.

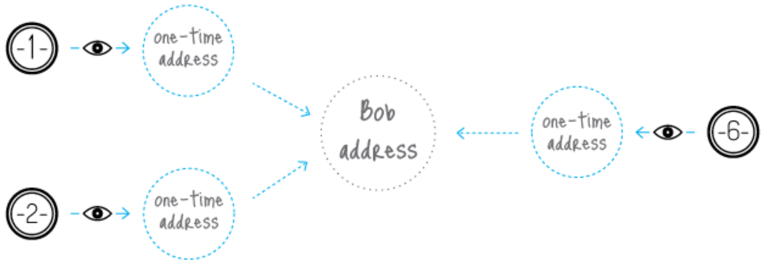

Alice
Bob
Carol
Dave
-1-
-1-
-1-
-1-
-1-
-1-
Romulus: "from Alice, Bob or Carol?"
Remus: "from Bob or Dave?"

It should be noted that foreign transactions do not restrict you from spending your own money. Your public key may appear in dozens of others' ring signatures but only as a muddling factor (even if you already used the corresponding secret key for signing your own transaction). Moreover, if two users create ring signatures with the same set of public keys, the signatures will be different (unless they use the same private key).

One-time keys: Unlinkable transactions
Normally, when you post your public address, anyone can check all your incoming transactions even if they are hidden behind a ring signature. To avoid linking you can create hundreds of keys and send them to your payers privately, but that deprives you of the convenience of having a single public address.



CryptoNote solves this dilemma by an automatic creation of multiple unique one-time keys, derived from the single public key, for each p2p payment. The solution lies in a clever modification of the Diffie-Hellman exchange protocol. Originally it allows two parties to produce a common secret key derived from their public keys. In our version the sender uses the receiver's public address and his own random data to compute a one-time key for the payment.
The sender can produce only the public part of the key, whereas only the receiver can compute the private part; hence the receiver is the only one who can release the funds after the transaction is committed. He only needs to perform a single-formula check on each transactions to establish if it belongs to him. This process involves his private key, therefore no third party can perform this check and discover the link between the one-time key generated by the sender and the receiver's unique public address.



An important part of our protocol is usage of random data by the sender. It always results in a different one-time key even if the sender and the receiver both remain the same for all transactions (that is why the key is called “one-time”). Moreover, even if they are both the same person, all the one-time keys will also be absolutely unique.

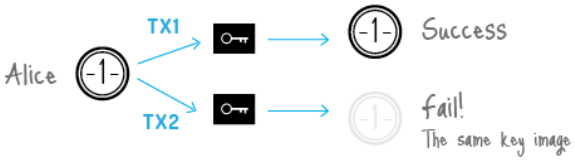
Double-spending proof

Fully anonymous signatures would allow spending the same funds many times which, of course, is incompatible with any payment system’s principles. The problem can be fixed as follows.

A ring signature is actually a class of crypto-algorithms with different features. The one CryptoNote uses is the modified version of the “Traceable ring signature”. In fact we transformed traceability into linkability. This property restricts a signer’s anonymity as follows: if he creates more than one ring signature using the same private key (the set of foreign public keys is irrelevant), these signatures will be linked together which indicates a double-spending attempt.

To support linkability CryptoNote introduced a special marker being created by a user while signing, which we called a key image. It is the value of a cryptographic one-way function of the secret key, so in math terms it is actually an image of this key. One-wayness means that given only the key image it is impossible to recover the private key. On the other hand, it is computationally impossible to find a collision (two different private keys, which have the same image). Using any formula, except for the specified one, will result in an unverifiable signature. All things considered, the key image is unavoidable, unambiguous and yet an anonymous marker of the private key.

All users keep the list of the used key images (compared with the history of all valid transactions it requires an insignificant amount of storage) and immediately reject any new ring signature with a duplicate key image. It will not identify the misbehaving user, but it does prevent any double-spending attempts, caused by malicious intentions or software errors.

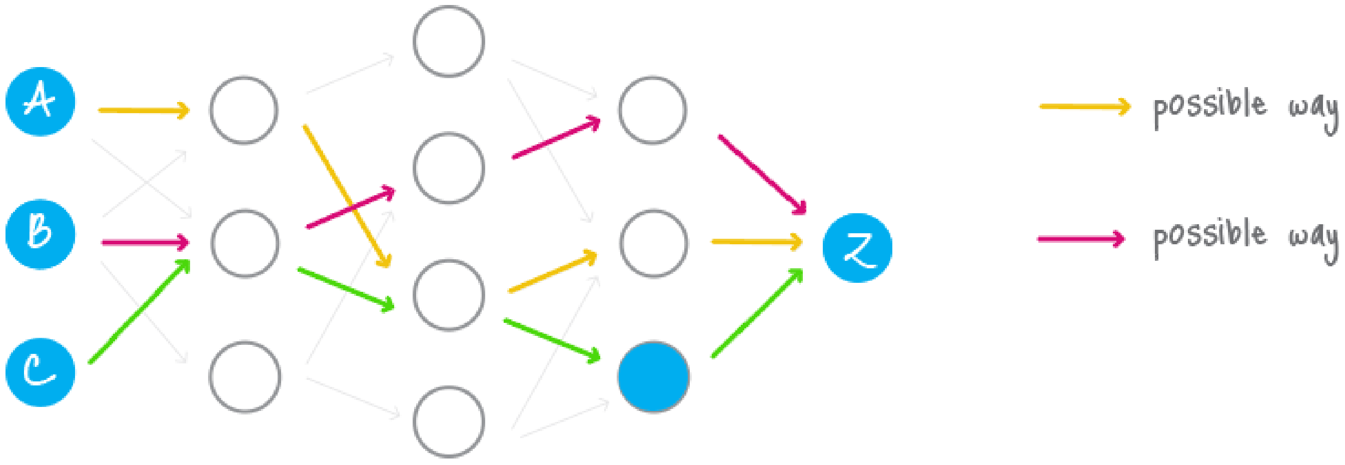


CryptoNote blockchain analysis resistance

There are many academic papers dedicated to the analysis of the Bitcoin's blockchain. Their authors trace the money flow, identify the owners of coins, determine wallet balances and so on. The ability to make such analysis is due to the fact that all the transfers between addresses are transparent: every input in a transaction refers to a unique output. Moreover, users often re-use their old addresses, receiving and sending coins from them many times, which simplifies the analyst's work. It happens unintentionally: if you have a public address (for example, for donations), you are sure to use this address in many inputs and transactions.

CryptoNote is designed to mitigate the risks associated with key re-usage and one-input-to-one-output tracing. Every address for a payment is a unique one-time key, derived from both the sender's and the recipient's data. It can appear twice with a probability of a 256-bit hash collision. As soon as you use a ring signature in your input, it entails the uncertainty: which output has just been spent?

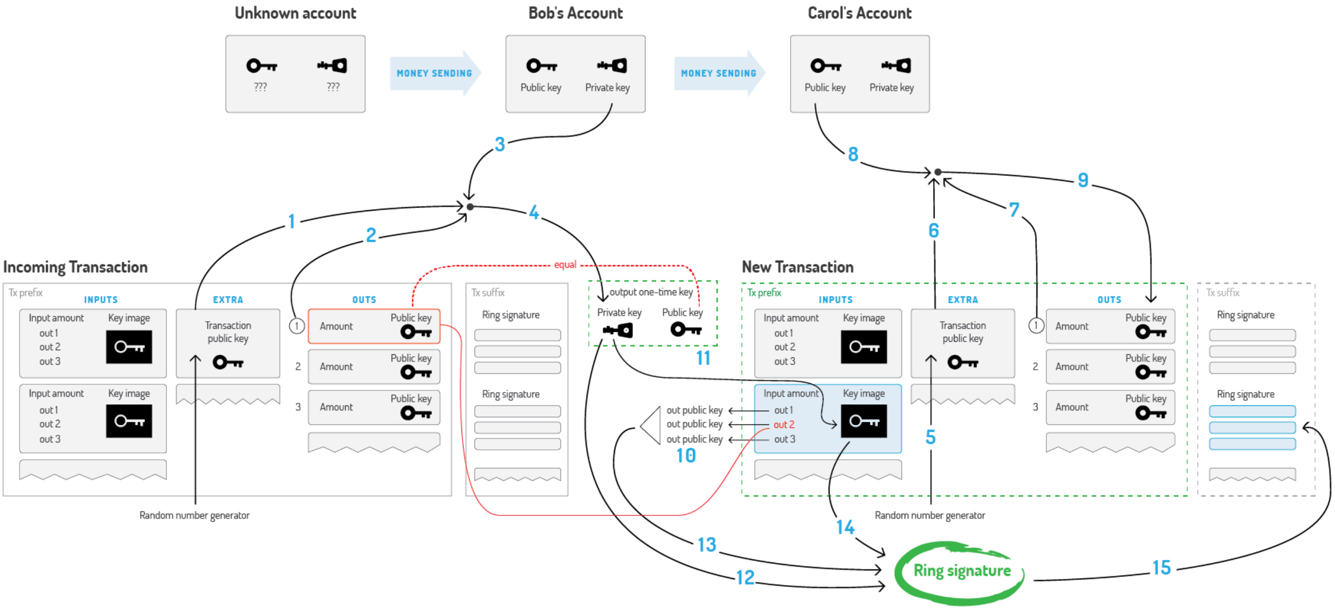
Trying to draw a graph with addresses in the vertices and transactions on the edges, one will get a tree: a graph without any cycles (because no key/address was used twice). Moreover, there are billions of possible graphs, since every ring signature produces ambiguity. Thus, you can't be certain from which possible sender the transaction-edge comes to the address-vertice. Depending on the size of the ring you will guess from "one out of two" to "one out of a thousand". Every next transaction increases the entropy and creates additional obstacles for an analyst.



CryptoNote

Standard CryptoNote transaction

A standard CryptoNote transaction is generated by the following sequence covered in the white paper.
Bob decides to spend an output, which was sent to the one-time public key. He needs Extra (1), TxOutNumber (2), and his Account private key (3) to recover his one-time private key (4).
When sending a transaction to Carol, Bob generates its Extra value by random (5). He uses Extra (6), TxOutNumber (7) and Carol's Account public key (8) to get her Output public key (9).
In the input Bob hides the link to his output among the foreign keys (10). To prevent double-spending he also packs the Key image, derived from his One-time private key (11).
Finally, Bob signs the transaction, using his One-time private key (12), all the public keys (13) and Key Image (14). He appends the resulting Ring Signature to the end of the transaction (15).



Adaptive limits

A decentralized payment system must not depend on a single person's decisions, even if this person is a core developer. Hard constants and magic numbers in the code deter the system's evolution and therefore should be eliminated (or at least be cut down to the minimum). Every crucial limit (like max block size or min fee amount) should be re-calculated based on the system's previous state. Therefore, it always changes adaptively and independently, allowing the

network to develop on it’s own.
CryptoNote has the following parameters which adjust automatically for each new block:
1) Difficulty. The general idea of our algorithm is to sum all the work that nodes have performed during the last 720 blocks and divide it by the time they have spent to accomplish it. The measure of the work is the corresponding difficulty value for each of the blocks. The time is calculated as follows: sort all the 720 timestamps and cut-off 20% of the outliers. The range of the rest 600 values is the time which was spent for 80% of the corresponding blocks.
2) Max block size. Let MN be the median value of the last N blocks sizes. Then the “hard-limit” for the size of accepting blocks is 2*MN. It averts blockchain bloating but still allows the limit to slowly grow with the time if necessary. Transaction size does not need to be limited explicitly. It is bounded by the size of the block.

Egalitarian proof of work
The proof of work mechanism is actually a voting system. Users vote for the right order of the transactions, for enabling new features in the protocol and for the honest money supply distribution. Therefore, it is important that during the voting process all participant have equal voting rights. CryptoNote brings the equality with an egalitarian proof-of-work pricing function, which is perfectly suitable for ordinary PCs. It utilizes built-in CPU instructions, which are very hard and too expensive to implement in special purpose devices or fast memory-on-chip devices with low latency.
We propose a new memory-bound algorithm for the proof-of-work pricing function. It relies on random access to a slow memory and emphasizes latency dependence. As opposed to scrypt, every new block (64 bytes in length) depends on all the previous blocks. As a result a hypothetical “memory-saver” should increase his calculation speed exponentially.
Our algorithm requires about 2 Mb per instance for the following reasons:
1. It fits in the L3 cache (per core) of modern processors, which should become mainstream in a few years;
2. A megabyte of internal memory is an almost unacceptable size for a modern ASIC pipeline;
3. GPUs may run hundreds of concurrent instances, but they are limited in other ways: GDDR5 memory is slower than the CPU L3 cache and remarkable for its

bandwidth, not random access speed.
4. Significant expansion of the scratchpad would require an increase in iterations, which in turn implies an overall time increase. “Heavy” calls in a trust-less p2p network may lead to serious vulnerabilities, because nodes are obliged to check every new block’s proof-of-work. If a node spends a considerable amount of time on each hash evaluation, it can be easily DDoSed by a flood of fake objects with arbitrary work data (nonce values).
One of the proof-of-work algorithms that is in line with our propositions is CryptoNight, created by Bytecoin developers in a cooperation with our team. It is designed to make CPU and GPU mining roughly equally efficient and restrict ASIC mining.

FruoCoin + Fruo Wallet
FruoCoin works on CryptoNote technology, which hides all payments and makes them untraceable. This is the perfect solution to have private payments. Although, if you don’t protect yourself, then it’s possible to find out that you are using FruoCoin. Everything you make online is connected to your device and your device has IP address, which reveals your identity online. To protect your identity, use Fruo wallet. By using Fruo wallet, your IP will be hidden via TOR network.

With FruoCoin and Fruo Wallet combination, nobody could ever know that you are using FruoCoin. This is 100% privacy, which only we can offer.

TOR

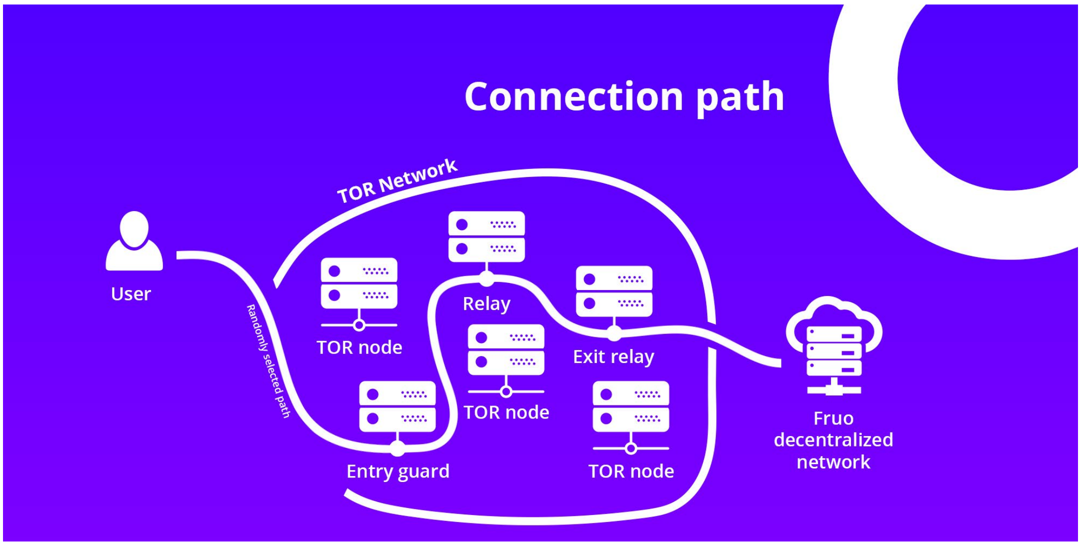
All Fruo features use TOR nodes to connect to the internet. This hides user IP address, and like this, it provides anonymity for users.

Tor, derived from an acronym for the original software project name “The Onion Router” is an IP obfuscation service which enables anonymous communication across a layered circuit-based network. Tor directs internet traffic through a free worldwide volunteer overlay network consisting of more than seven thousand relays to conceal a user’s location and usage from anyone conducting network surveillance or traffic analysis. The layers of encrypted address information used to anonymize data packets sent through Tor are reminiscent of an onion, hence the name. That way, a data packet’s path through the Tor network cannot be fully traced. Tor’s use is intended to protect the personal privacy of users as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored.

Onion routing is implemented by encryption in the application layer of a communication protocol stack, nested like the layers of an onion. Tor encrypts the data, including the next node destination IP, multiple times and sends it through a virtual circuit comprising successive, randomly selected Tor relays. Each relay decrypts only enough of the data packet wrapper to know which relay the data came from, and which relay to send it to next. The relay then rewraps the package in a new wrapper and sends it on. The Final relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing, or even knowing, the source IP address.

Because the routing of communication is partly concealed at every hop in the Tor circuit, this method eliminates any single point at which the communicating peers can be determined through network surveillance that relies upon knowing its source and destination.

Connection path between user and Fruo network



Conclusion

In today’s digital world, remaining anonymous is really hard. Blockchain technology is here to solve this problem. Not fully, but it can help us in many different areas. Usually, blockchain technology comes with cryptocurrencies, which are digital assets with value. Cryptocurrencies are mostly meant for online payments, but most of the payments we make every day is in the real world in real places. FruoCoin is new cryptocurrency, which focuses on privacy and in real life payments. If the blockchain technology reaches in masses, we might see our world change.

More information about Fruo project can be found on the website.
www.fruo.co

For the question, please ask for the community or Fruo support.
Forum1 - https://forum.fruo.co/
Forum2 - https://www.reddit.com/r/FruoCoin/
Community chat - https://t.me/fruocoin

Fruo support - support@fruo.co

Fruo’s project is made possible thanks to Ciciru Network.

CICIRU NETWORK LIMITED
Registration number: 167303
Address: 24.5 Old Northern Highway, Boston Village,
Belize District, Belize

Thank you!

This whitepaper uses references from the following websites.
The referred content is not owned by Ciciru Network.

https://fmella.com/
https://www.investopedia.com/
https://cryptonote.org/
https://blockchain.info/
https://coinmarketcap.com/
https://vergecurrency.com/
https://medium.com/
https://en.wikipedia.org/