uPlexa

Incentivizing the mass compute power of IoT devices to form a means of anonymous, browser-based blockchain payments.

Disclaimer:

You are viewing a version of the whitepaper from 16th September, 2018. Changes to the business, technical and legal models may be made in the future. Check the uPlexa website for the latest version of this whitepaper.

Table of Contents

Introduction & Vision

uPlexa is a p2p electronic payment system focused on harnessing the power of IoT and anonymity. Built on its own blockchain utilizing a modified version of the CryptoNight algorithm, uPlexa was developed in order to interlink the collective power of IoT (internet of things) devices as a whole, while supporting anonymous based payments, particularly for internet & telecom service providers, whilst also supporting anonymous based ecommerce. There are over 9 Billion IoT devices in the world in 2018, with an expectation of 20+ Billion by 2020.

Like Bitcoin, uPlexa is a peer-to-peer (p2p) electronic payment system. However, uPlexa also supports anonymous payments and profitable IoT transaction mining. Not only is uPlexa ASIC resistant, but also aims at being the most profitable coin for users with IoT devices to mine utilizing a specific percentage of unused resources. uPlexa's blockchain will be directly accessible and minable via the web, with absolutely no need to download any external resources. However, downloadable apps will be available, too.

In December of 2017, we saw the largest adoption of any cryptocurrency, Bitcoin. At this time, Bitcoin was not prepared to be adopted by such a grand user base, leading to heavy network congestion, which resulted in slow transaction times and large fees. uPlexa plans ahead by solving these issues by utilizing our Near-Zero Congestion Model (NZCM). The NZCM consists of a powerful hashrate through harnessing the power of IoT devices, while also scaling back micro-payments by having the fee's increase for micro-payments as the network transactions increase. Any payments not considered a micro-payment will always have relatively low fees. NZCM will also use the uPlexa API in-order to utilize off-chain transactions for uPlexa power users. These are only a few straightforward layers of the NZCM. To read more, please read about NZCM on page 6.

Anonymity and privacy are among one of the largest debates within the cryptocurrency field. uPlexa uses the CryptoNight algorithm in order to ensure untraceable private transactions. With uPlexa, our goals are to bring anonymity to internet and telecom service provider payments as well as eCommerce. This will be accomplished by negotiating deals with IT & Telecom providers, as well as launching our own eCommerce platform; supporting anonymous transactions, anonymous store owners, and disapproving the storage and sale of personal information for marketing and all other purposes.

How it Works – IoT Model (Core Functionality)

uPlexa utilizes a modified version of the CryptoNight algorithm in order to provide unquestionable security and anonymous payments. After auditing the default CryptoNight algorithm for our purposes, we soon realized that mining of IoT devices off of the default CryptoNight algorithm is not directly viable nor profitable. The modifications made to the algorithm are to make IoT mining more profitable. Unlike other payment systems, the backbones of our network will be powered by the billions of IoT devices that exist in the world.

Our core objective is to generate a profitable amount of uPlexa to help pay for the electricity in running any given IoT device by mining a proportion of the idle resources on any given IoT device. This may not sound like much in developed countries. However, in developing countries – where most IoT devices are built, they are also more affordable to purchase. For example, individuals in Southeast Asia and other regions have Smart TV's, Smart Refrigerators, Smart Cars, and multiple mobile devices. If they were able to obtain enough profits to at the very least – pay a portion of the cost of running them, they would be in a much better situation, as monthly electricity costs may cost up to as much of 20% of their income.

We plan on supporting most, if not all IoT devices, by developing software specifically for each device to mine uPlexa with a percentage of a devices idle CPU. The amount may be optionally adjusted by the user, and we will have caps in-order to prevent the over-use of a users IoT device. The devices we will be supporting are:

- Desktop & Laptops
- Mobile Phones & Tablets
- Smart TV's
- Smart kitchen appliances (refrigerators, ovens, coffee makers, ranges, etc)
- Smart cars
- Raspberry Pi's
- Servers (Datacenters and server farms)
- Others as IoT continues to develop

How it Works – Fees & Near-Zero Congestion Model (NZCM)

In order to negate heavy network congestion and maintain extremely low fees, we've decided to create a model known as the Near-Zero Congestion Model (NZCM) in-which has several layers:

- Harness the power of mass IoT adoption
- Utilization of the uPlexa NZCM API for off-chain transactions
- Disapproval of extremely small microtransactions
- Scaling fee's at higher rates for microtransactions

With the huge amount of existing IoT devices and the continued adoption of IoT, we have absolutely no doubt that we will obtain a substantial amount of network support to power our blockchain. However, another positive is that for the major use cases of uPlexa, utilizing the NZCM API will result in not having to use the actual blockchain for a large portion of transactions.

The NZCM API will allow webmasters, app developers, and corporations to credit their users in uPlexa while their users choose to mine for that specific service, app, or business. All of which is sent to the individual or business, while the uPlexa is then credited to that individual user on their platform via our API. Thus, when a user spends their mined uPlexa on their platform, a transaction does not need to be put through the blockchain, but is rather processed via their platforms database.

The use-case of uPlexa is mainly for anonymous payments for both internet & telecom providers, as-well as eCommerce. Thus, micro-transactions are not a major priority. We DO wish to focus on a CryptoNight lightning network in the future to support uPlexa and other CryptoNight micro-transactions. However, as uPlexa is not directly supporting micro-transactions, there will be a minimum limit on how much uPlexa can be sent (no less than 1 uPlexa). This amount may be changed at any given time via forking due to the value of uPlexa. For micro-transactions under 5 uPlexa, there will be a scaling fee. Thus, if you're sending less than 5 uPlexa when the network is being flooded with micro-payments, the fee of such micro-transactions will scale up 2x more than any standard payment. The idea behind this, is to negate network attacks and lessen the use of micro-payments with uPlexa. uPlexa is not, yet, a cryptocurrency that focuses on micro-transactions (<$0.15 USD)

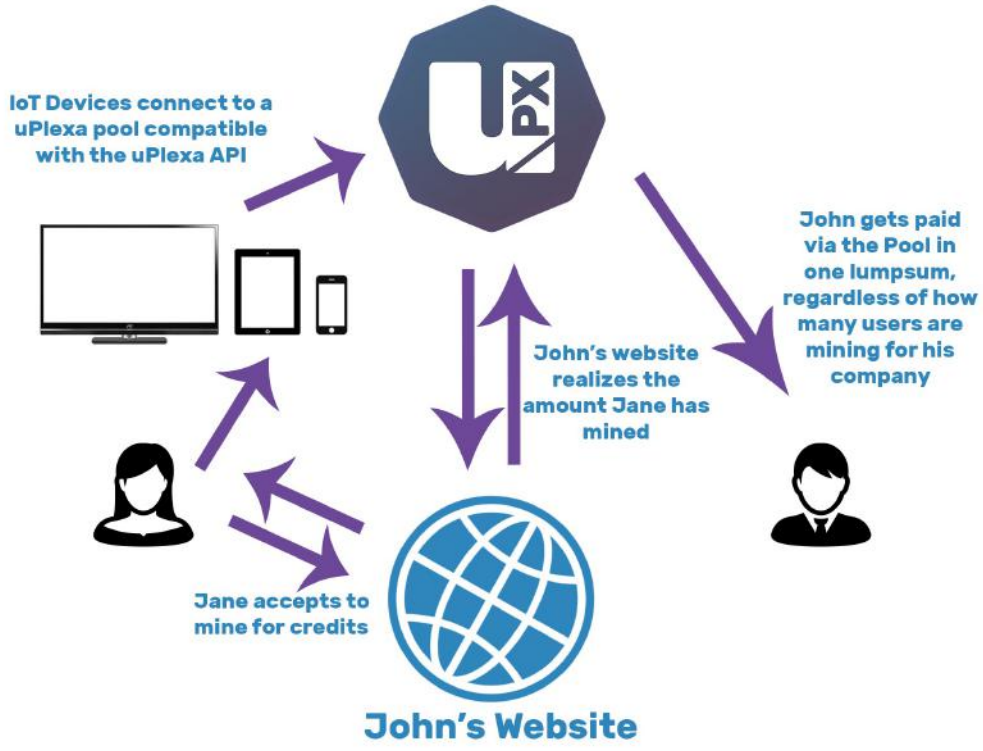
uPlexa NZCM API

The uPlexa API may be used in order to help provide less network congestion by using less on-chain transactions, lessening fees for companies and projects.

How it works

Say, John – the owner of johnswebsite.com wishes to provide a credit system to his users in order for them to purchase goods, services, or make donations. He can ask his users to connect their IoT devices to his online website in order to mine uPlexa coins. In-return, the users will be rewarded with on-site credits utilizing the uPlexa API. Once the users mine enough JohnCredits, the user is than able to make a purchase, or use some of the credits for a discount on John's website.

The mining during this process, is all sent to one wallet, John's wallet. However, each individual user and the amount of hashes they've solved is tracked via the uPlexa API. Thus, when user Jane, wishes to make a purchase; the amount is deducted from the users balance via the API rather than making a separate transaction from her wallet to Johns wallet.



Introducing eCommerce

The eCommerce industry accounts for over $2.3 Trillion dollars of worldwide revenues, with estimates of upwards of $4.88 Trillion dollars by 2021. Source: https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/

The uPlexa team will introduce its very own eCommerce platform based on massively supporting multiple cryptocurrencies, fiat, and also using uPlexa as a private, secure and anonymous gateway for both webmasters and their clients. There will be no KYC for our webmasters, and they will be anonymously paid out via uPlexa. Other things such as developers, plugins, and designs will also be available in the eCommerce marketplace for webmasters to purchase with uPlexa for their own store.

The uPlexa eCommerce system will not charge users until said user is running a profitable store. Meaning, the store is FREE until you start making a minimum of 3x the monthly store fee, which will be around $29 USD/mo for basic stores. Payments will be made daily if you surpass an amount of >$29 USD. Otherwise, payments will be bi-weekly.

Our team has previously worked in the eCommerce industry, everything from BigCommerce, to Wordpress (WooCommerce), and Shopify. We will focus strongly on making a customization and anonymous eCommerce experience to outperform other existing eCommerce systems by listening to customer suggestions and complaints that these companies have forever ignored. We've personally had many conversion boosting ideas for said systems in-which the systems were not capable of without major modifications. Some of which are in-production today for live stores.

With that being said, uPlexa's priority focus regarding eCommerce will be both cryptocurrencies as well as increased conversions for our clients.

Service Payment Anonymity

uPlexa will finally bridge the connection between anonymous payments and service providers. This will be achieved by making multiple partnerships with developing startups that will allow users to pay for their services without KYC and utilizing uPlexa as an optional payment method.

Why Should Service Payments be Anonymous?

- Anonymity provides protection from spy programs with the sole purpose of stealing your private information
- Helps protect you from your data being sold for marketing or other purposes
- Pay for services in other countries when traveling without having to pay “tourist” fees since uPlexa is a global currency, and they don't know who you are
- Avoid other companies from knowing who you're paying, or which company you may be acquiring
- Keep your business suppliers in secret
- Escape government repression and service bans
- Avoid blackmail from ISPs or employees who spy on your data
- Pay for family members services with your own account
- Hackers will be unable to trace a phone number to your name, or hijack your mobile access with your personal details to further obtain access to your online accounts

The anonymous functions of uPlexa go far beyond the codebase, into the realms of large corporations, and policies regarding KYC and anonymity. The most difficult challenges will be finding companies and partners willing to provide a secure and anonymous option to their systems and services. Thus, we will have a strong focus on strategic partnerships, whilst also rewarding bounties to those who help uPlexa achieve its true potential.

IoT Viability and Profitability

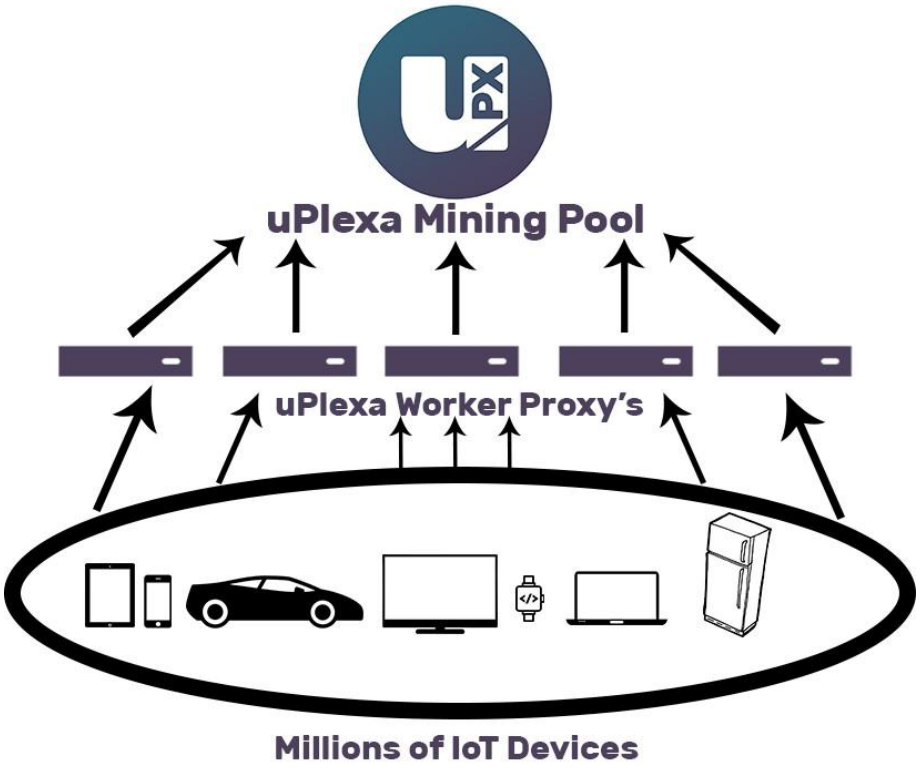
uPlexa will deliver mining to an array of IoT devices, from smartphones and tablets to smart TV's and even smart cars. This is accomplished by running our mining software. uPlexa mining software utilizes a specific set of failsafes in order to prevent said devices from overheating and becoming less responsive by only using a specific portion of the devices idle resources. In our tests, the uPlexa mining software requires less CPU than commonly used applications such as your phones Camera, Facebook, and Netflix.

The Math

Standard smartphone: 28H/s at full bore or 10H/s at 35% CPU Usage
Standard laptop at around 45H/s at full bore or 16H/s at 35% CPU Usage

Utilizing 35% of the CPU provides a median hashrate 13H/s. If Alice has 15 devices; she has 13 * 15 = 195H/s.

The technology making this possible and lightweight is a forked CryptoNight pool combined with an advanced proxy protocol for lessened connections to the pool. With our software, we're able to accept upwards of two million concurrent connections on five Amazon m5.2xlarge instances as proxies, and two Amazon m4.16xlarge instances (one for pool, one for share validation & workload balancing).



Miner Profitability

The profitability involves our modified version of the CryptoNight protocol in-order to provide the most profitable yet anonymous form of IoT mining. The CryptoNight protocol is fairly ASIC resistant. However, future mandatory hardforks that the entire network follows may be required to avoid ASIC mining on our platform. Said hardforks will not be intrusive nor risky.

Our goal with our algorithm is to balance GPU to CPU as close as we can, in terms of cost per dollar for the users mining hardware. The idea behind IoT mining is to have many IoT devices connected across the world will help minimize centralization of mining while maintaining a steady stream of profit for our miners to continually help process transactions on the uPlexa blockchain.

With uPlexa, people are able to use a blockchain that is profitable to mine uPlexa on by connecting directly to one of the uPlexa public pools. They may also choose to connect to a company or website/game pool in order to obtain credits on the said platform.

Technical Explanation – Overview of CryptoNight

CryptoNote Algorithm

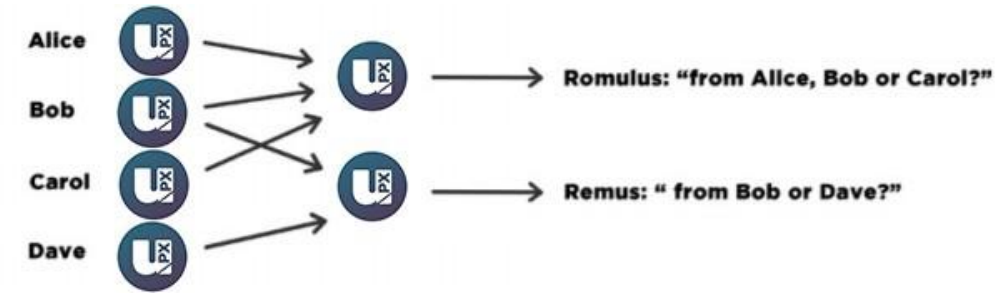
The CryptoNote algorithm is released under an open source license and has been adopted and incorporated into uPlexa as it forms the basis for a solid, well tested cryptocurrency core. It is the same core blockchain technology that is used by both Monero (a top 10 cryptocurrency) and Bytecoin (a top 15 cryptocurrency).

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.

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.

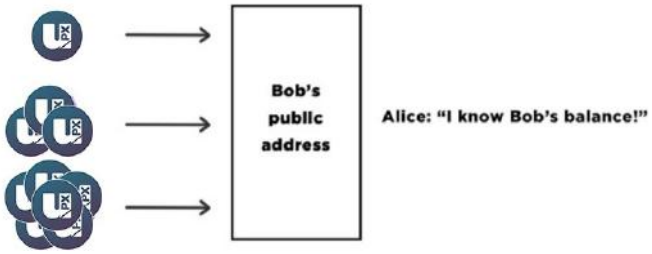


Untraceable transactions

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).

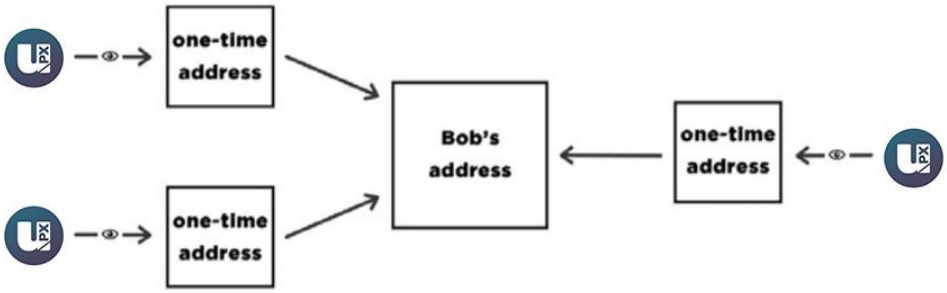
Unlinkable transactions

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.



uPlexa's 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.



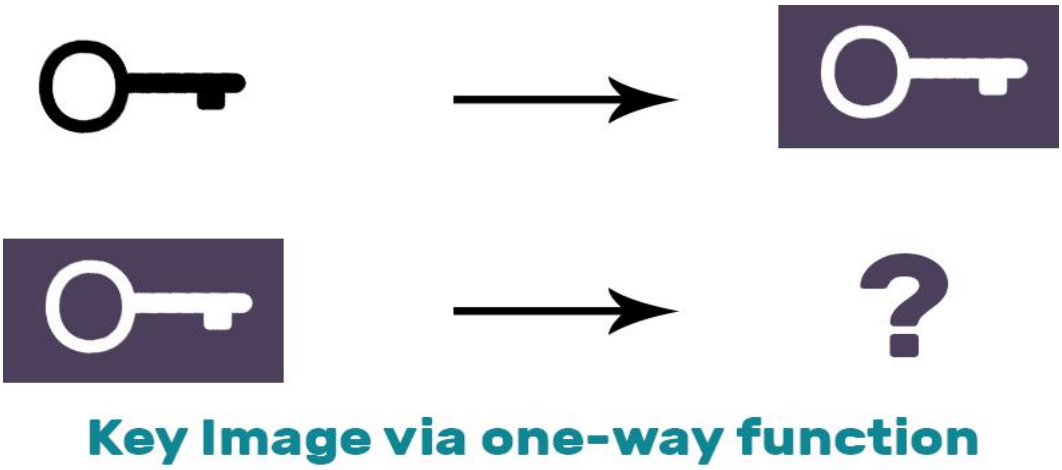
An important part of our protocol is usage of random data by the sender. It always results in a different one-time key even if the sender and the receiver both remain the same for all transactions (that is why the key is called "one-time"). Moreover, even if they are both the same person, all the one-time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

Double-spending proof

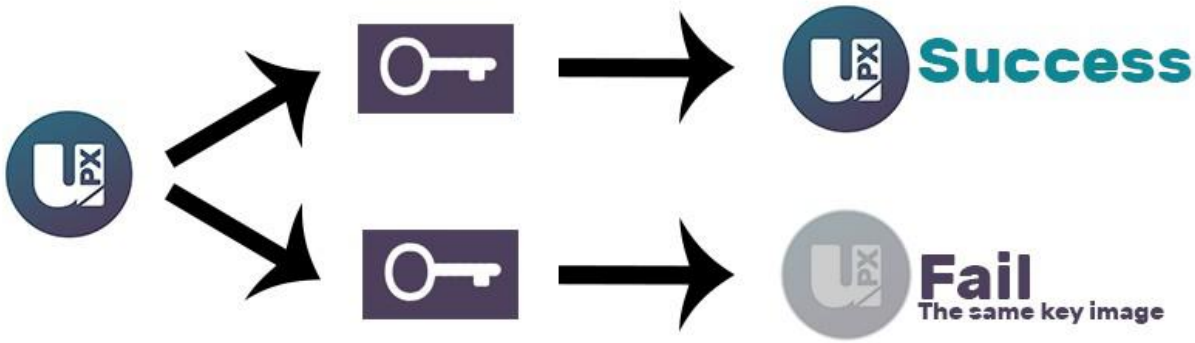
Fully anonymous signatures would allow spending the same funds many times which, of course, is incompatible with any payment system's principles. The problem can be fixed as follows.

A ring signature is actually a class of crypto-algorithms with different features. The one uPlexa's 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, uPlexa's 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.

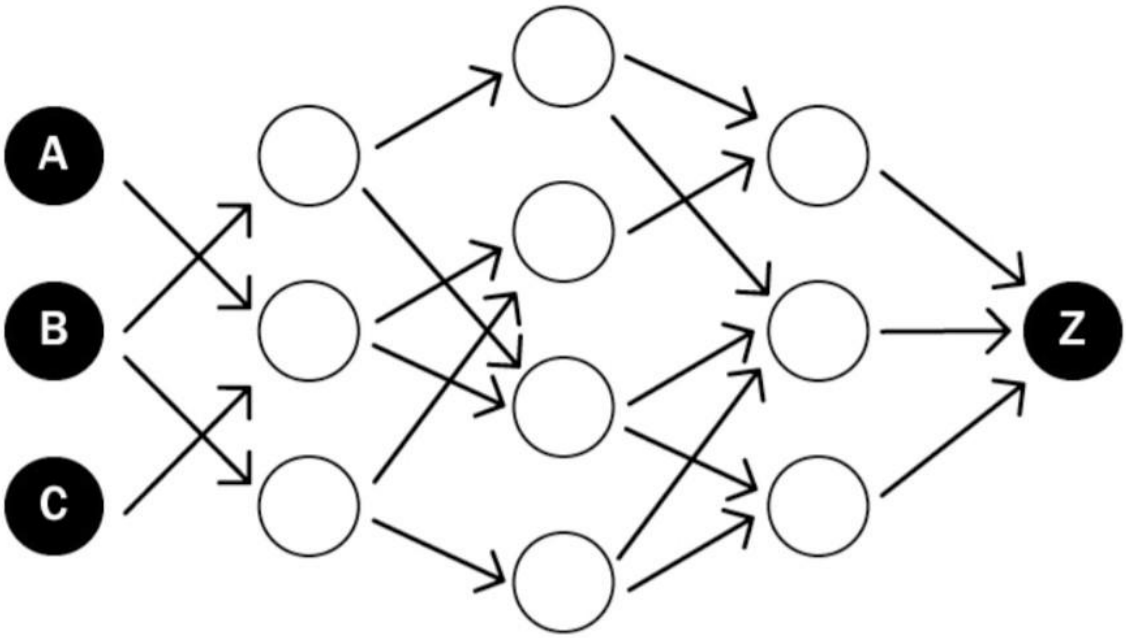


Blockchain analysis resistance

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.

uPlexa’s 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.



Standard CryptoNote transaction

A standard uPlexa CryptoNote transaction is generated by the following sequence covered in this white paper.

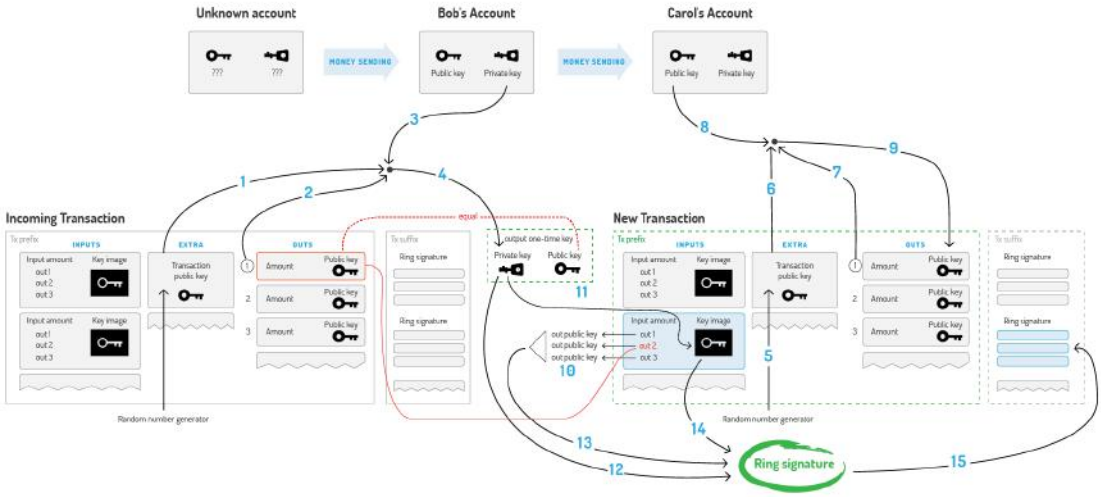
Bob decides to spend an output, which was sent to the one-time public key. He needs Extra (1), TxOutNumber (2), and his Account private key (3) to recover his one-time private key (4).

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.

uPlexa's 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.

Smooth emission

The upper bound for the overall amount of all digital coins is also digital:

MSupply = 264 − 1 atomic units

This is a natural restriction based only on the implementation limits, not on intuition like "N coins ought to be
enough for everybody". To make the emission process smoother uPlexa's CryptoNote uses the following
formula for block rewards:

BaseReward = (MSupply − A) >> 18

Where A is amount of previously generated coins. It gives a predictable growth of the money supply without any
breakpoints.

Conclusion

uPlexa is focused on providing an anonymous coin with complimentary utility with both eCommerce and service provider payments. These utilities will sit on top of the foundational layers of mass IoT hashpower and off-chain transactions.

References

Cryptonote white paper:
https://cryptonote.org/whitepaper.pdf

Cryptonote Inside:
https://cryptonote.org/inside

Bitcoin white paper:
https://bitcoin.org/bitcoin.pdf

Statistica: IoT Connected Devices 2015-2025:
https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

PRISM (surveillance program):
https://en.wikipedia.org/wiki/PRISM_(surveillance_program)

uPLEXA