uPlexa

Incentivizing the mass compute power of IoT devices to form a means of private blockchain payments & privacy infrastructure for software(s)

Disclaimer:

You are viewing a version of the whitepaper from 6th July, 2021. 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 privacy. Built on its own blockchain, utilizing a modified version of the Cryptonote algorithm, uPlexa was developed to interlink the collective power of IoT (internet of things) devices as a whole. All the while, supporting privacy-based payments, and ultimately, ecommerce and privacy-based software(s). ***Note***: There are over 31 billion IoT devices in the world in 2021, with an expectation of 125+ Billion by 2030.

Like Bitcoin, uPlexa is a peer-to-peer (p2p) electronic payment system. However, uPlexa also supports private payments and profitable IoT transaction mining. uPlexa is ASIC resistant, and also aims at being the most profitable coin for users with IoT devices to mine by utilizing a specific percentage of unused resources. By targeting low-power architecture, uPlexa becomes one of the few cryptocurrencies that can be considered eco-friendly. uPlexa's blockchain is directly accessible and minable via the web, with absolutely no need to download any external resources. However, downloadable apps are 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. Not only is uPlexa much more private, with a PoW algorithm that is not only more eco-friendly but has the potential to be one of the most decentralized PoW algorithms that aslo accounts for such congestion via dynamic block sizes.

With so much government regulation, electronic fraud and compromised data, privacy is once again coming to the fore and is now among one of the largest debates within the cryptocurrency field. With this in mind, uPlexa uses the **CryptoNote** algorithm to ensure completely private transactions to ensure that user’s data is consistently secure. With uPlexa, our goals are to bring privacy to the world, in both transactional and in everyday software(s). On top of the blockchain itself, the uPlexa Foundation is also working on building a high-speed decentralized VPN on top of the uPlexa network.

How it Works – IoT Model (Core Functionality)

uPlexa utilizes a modified version of the Cryptonote algorithm to provide unquestionable security and 100% private payments. After auditing the default CryptoNight (the PoW of Cryptonote) algorithm for our purposes, we soon realized that mining of IoT devices off 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 today.

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 a whole lot 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 user’s 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 – PoW/PoS Split

In 2021, the uPlexa project will release "***Steadfast Storm***™ ". The Steadfast Storm will fork away from a soul Proof-of-work (PoW) algorithm to a split of 80/20 PoW/PoS. This means, 80% of all block rewards will be allocated to PoW based miners, and 20% will be awarded to Proof-of-stake (PoS) based utility nodes.

What is a Utility Node?
A utility node (an improved upon version of a master node) is a node that will help enable instant transactions, DVPNs, and UNapps on the uPlexa network. Utility Nodes will receive 20% of all block rewards and will help eliminate the chance of a 51% PoW based attack. Utility nodes will require 2,000,000 UPX to stake to become a part of the network and are paid dividends on the uPlexa network to incentivize the community to operate said nodes. The 2,000,000 UPX requirement will decrease much like our current block rewards. To read more about our block rewards and emissions, please scroll to page 21. Users with less UPX capital may choose to become a part of a Utility Node pool to stake a lesser amount and still receive dividends.

Near-Instant Transactions via Utility Nodes

Utility nodes (UN's) will help us enable instant transactions in the future for uPlexa, without compromising privacy. UN's will also eliminate the chance of any 51% PoW based attack on the uPlexa network. This is due to UN's being able to help verify blocks at a faster rate than PoW, whilst still allowing PoW to confirm that the chain is aligned properly and that no fork has occurred. Later, it will only require 1-2 PoW based block confirmations to securely confirm a transaction. At said time, block times will likely be decreased from two minutes to 15-30 seconds depending on our purging technology at this time.

DVPNs (Decentralized VPNs) via Utility Nodes

Utility nodes will allow a deep web type service to run off the uPlexa blockchain. Users may connect to said network and allow their wallets to act as a VPN in order to surf the web privately. This will be done by implementing a layer 2 onion routing protocol to the uPlexa network and having Utility Nodes act as exit relays for users to connect to. Currently, we wish to serve our dVPN as a free and unlimited-use service. However, we will also have a hardfork “hot and ready” in the chance that abuse, or scalability issues occur within the uPlexa network. To provide a counter to any potential network congestion, we may implement a spending utility for the uPlexa network in which will decrease network abuse without the requirement of throttling user’s data on the dVPN. This could be implemented by charging a fee of $0.01-0.05 USD per 1GB of network data depending on priority. Charging such fees will provide more spending utility for the network, limit abuse, and advise a larger audience on how to use privacy-based cryptocurrencies such as uPlexa.

Mixnet via Utility Nodes

As previously mentioned, utility nodes will power the dVPN on Plexanet. The dVPN, in reality, is more of a mixnet. A mixnet is a network in which create near-untraceable communications via chaining proxies together (known as mixes). The data packets are taken from multiple outputs (senders), shuffles them around, and sends the data back out in random order to the next destination (which would then be the next hop, and there’s a minimum of three hops!). With said mixnet, there will be hidden services. Hidden services are websites or services in which use Plexanet technology to stay private and secure – whilst also providing user anonymity. Hidden services are untrackable and censorship-resistant. The Plexanet mixnet could be thought of as a private, yet decentralized internet built on top of the existing internet. Plexanet URL’s will look something like: https://006c742296ba7d1139561af7719288f1.upx

Of course, there will be ways to acquire .upx domains on the network, providing a more user friendly domain name. The exit-node capabilities of the mixnet will be the major component of what we refer to as the “dVPN”.

UNApps (Utility Node Apps)

Utility Node Apps (UNapps) are private and decentralized apps hosted on the uPlexa network. UNApps will provide private and decentralized infrastructure for software developers who wish to create privacy based applications without the requirement of infrastructure capital, and without needing to find and manage for-privacy, anti-censorship hosting providers. UNApps will bring forward an entire new platform when it comes to obtaining software for users. There will be a subset of rules when it comes to UNApps, preventing the storage of user data by any UNApp developers, whilst providing the utmost highest privacy to all users and developers.

Commerce & Integrations

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/

For commerce, you have a wide variety of options. Brick and mortar businesses, online brands, and social commerce. It is one of uPlexa's core goals to support commerce and businesses of all size. In order to achieve this, uPlexa has released integration libraries for NodeJS, PHP, and Python alongside direct plugins for WooCommerce, Magento, Prestashop, Opencart, and WHMCS.

On top of the integrations released by the uPlexa team, uPlexa has also partnered with CryptoCurrencyCheckout.com while additionally supporting Shopify, WCMarketPlace, Crypto Invoice, Twitch, Youtube, Twitter, Facebook, Instagram, Streamlabs, and Website Donations.

Private Payments

Among uPlexa's core consensus, is privacy. Payments should be private, and not open to the prying eye of the general public and data mining corporations. Uplexa is what we would think of as a GDPR compliant cryptocurrency.

Why Should Payments be Private?

- Privacy 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.
- Less likely to be blackmailed, kidnapped, or extorted from the milk man knowing how much money you have.
- Avoid other companies from knowing who you are paying, or which company you may be acquiring.
- Protect your business supplier's data.
- Escape government repression and service bans.
- Avoid blackmail from ISPs or employees who spy on your data.
- Pay for family member's 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 privacy functions of uPlexa go far beyond the codebase, into the realms of large corporations, and policies regarding KYC and privacy. The most difficult challenges will be finding companies and partners willing to provide a secure and private 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.

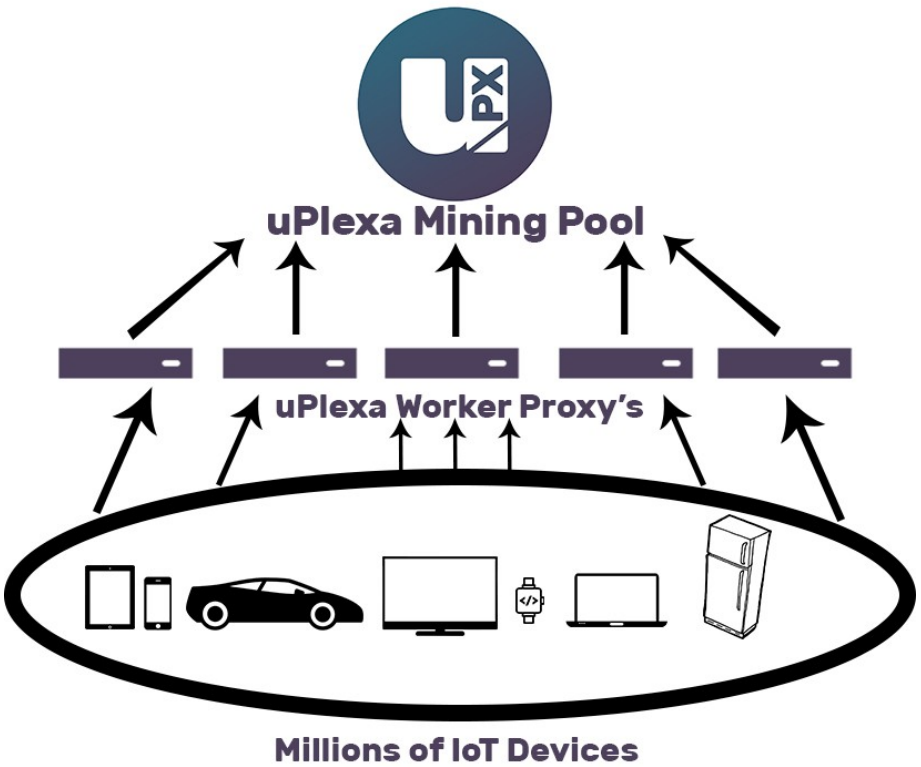
IoT Viability and Profitability

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 fail-safes 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 can 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 stems from our modified version of the CryptoNight protocol which provides the most profitable yet private 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 that 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 CryptoNote

CryptoNote Algorithm

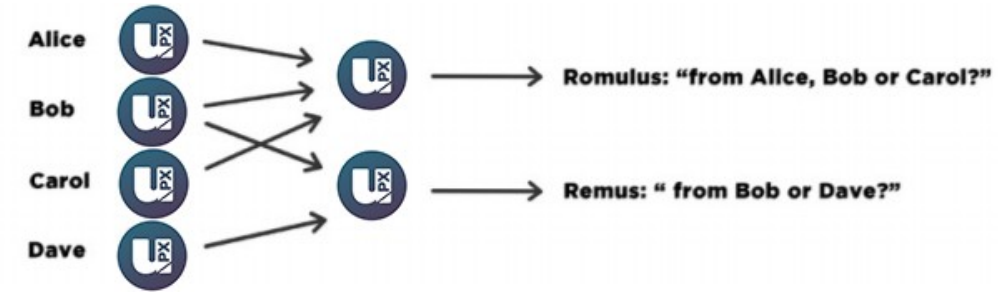
The CryptoNote algorithm is released under an open-source license and has been adopted and incorporated into uPlexa as it forms the basis for a solid, well tested cryptocurrency core. It is the same core blockchain technology that is used by both Monero (a top 10 cryptocurrency) and Bytecoin (a top 15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

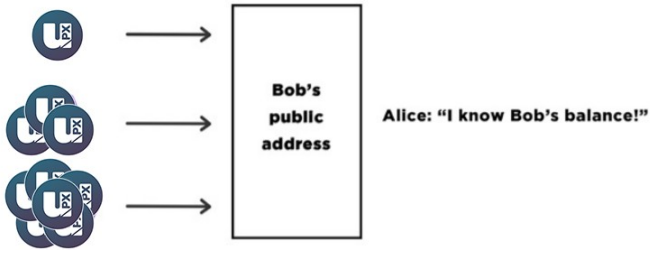


Untraceable Transactions

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).

Unlink-able Transactions

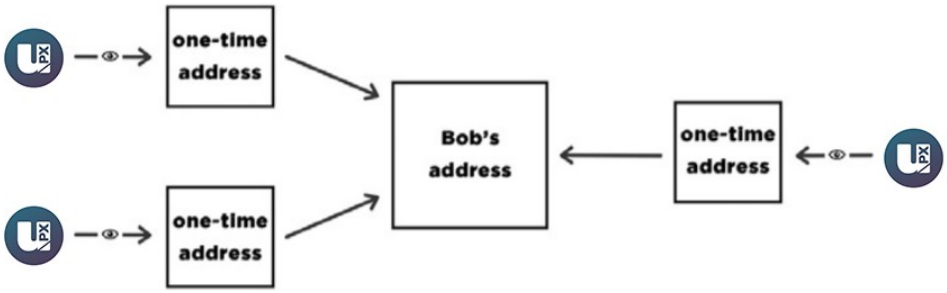
Normally, when you post your public address, anyone can check all your incoming transactions even if they are hidden behind a ring signature. To avoid linking, you can create hundreds of keys and send them to your payers privately, but that deprives you of the convenience of having a single public address.



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 transaction 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.



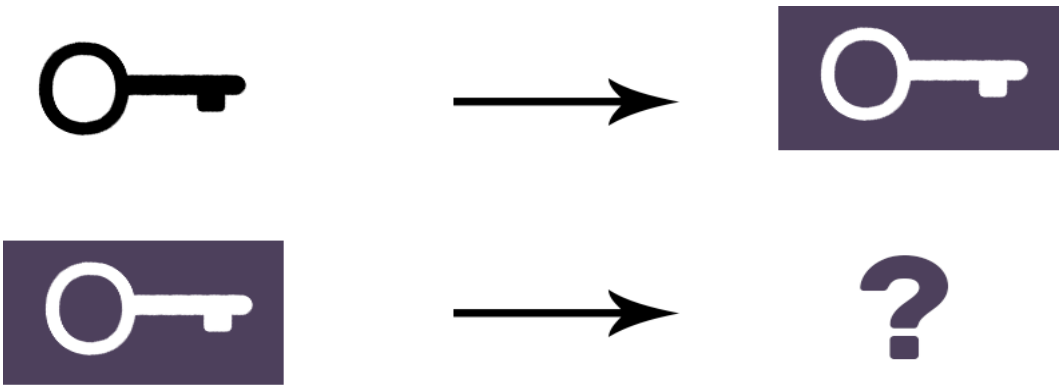
An important part of our protocol is the usage of random data by the sender. It always results in a different one-time key even if the sender and the receiver both remain the same for all transactions (that is why the key is called "one-time"). Moreover, even if they are both the same person, all the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

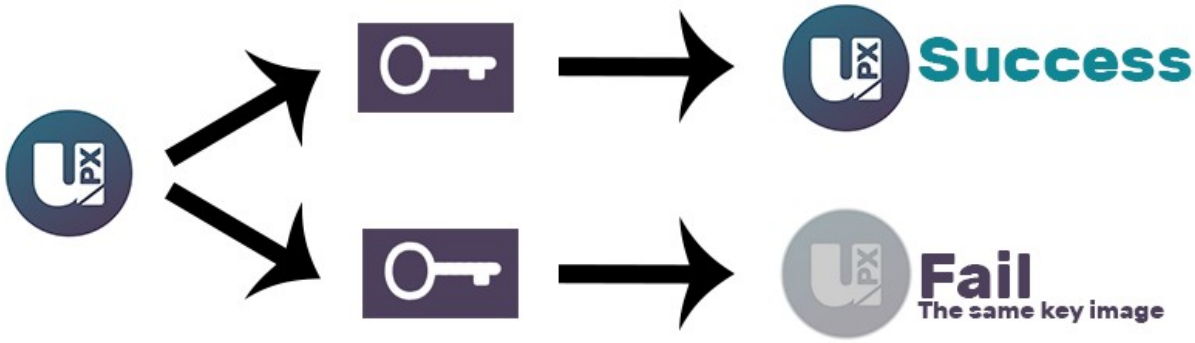
A ring signature is actually a class of crypto algorithms with different features. The one uPlexa's CryptoNote uses is the modified version of the "Traceable ring signature". In fact, we transformed traceability into linkability. This property restricts a signer's anonymity as follows: if he creates 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 an image of this key. The one-way functionality 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.



Key Image via one-way function

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.



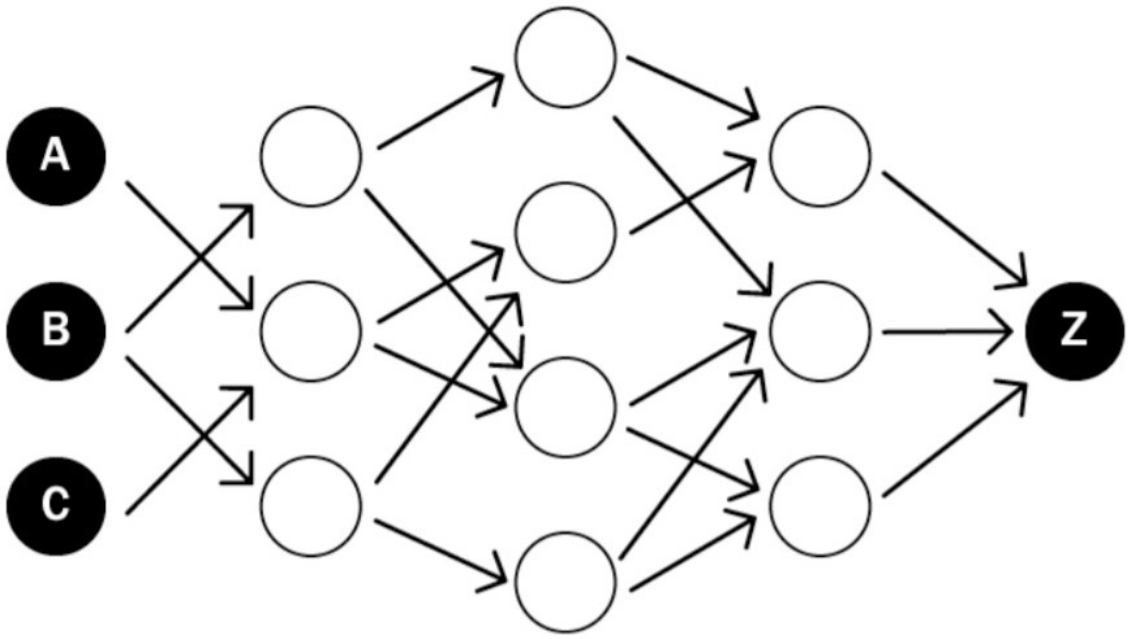
Blockchain analysis resistance

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 because all the transfers between addresses are transparent in that 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. For example, if you have a public address (such as 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 cannot be certain from which possible sender the transaction-edge comes to the address-vertices. 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.

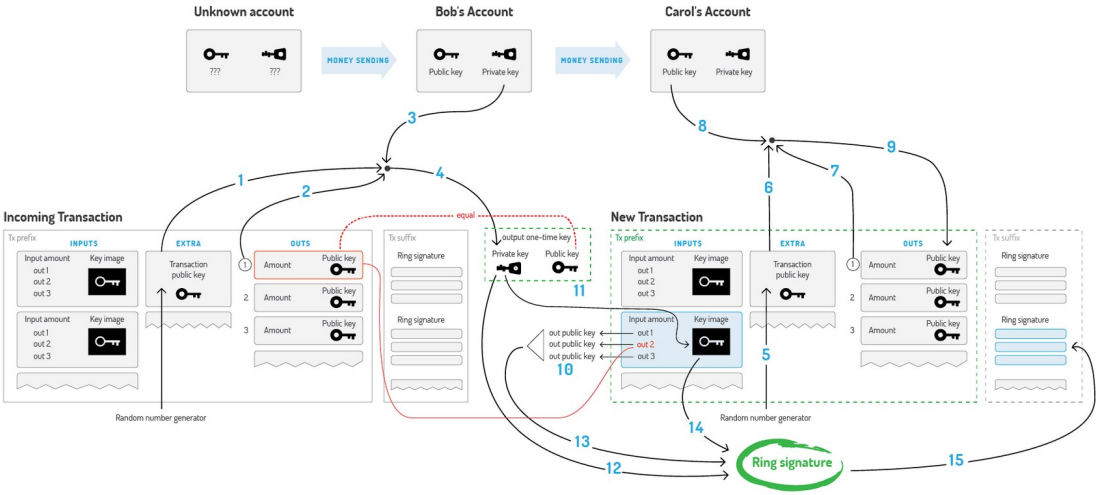
Bob decides to spend an output, which was sent to the one-time public key. He needs Extra (1), TxOutNumber (2), and his Account private key (3) to recover his one-time private key (4).

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 its 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) >> 21

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 a privacy-based asset with complimentary utility for both commerce and software(s). These utilities will sit on top of the foundational layers of mass IoT hash power and utility nodes.

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)

IoT Connections to Reach 83 Billion by 2024:

https://www.juniperresearch.com/press/iot-connections-to-reach-83-bn-by-2024