Absolute Privacy At Your Fingertips

UltraNote.Org

Launch Date 4th November 2017

Updated 28 August 2018

"It is well enough that people of the nation do not understand our banking and monetary system, for if they did, I believe there would be a revolution before tomorrow morning."

Henry Ford (1863-1947)

UltraNote (XUN) White Paper

ABSTRACT

''UltraNote has been designed to solve the core problems inherent to two of the most important aspects of everyone's daily life which are; communication and exchanging money which require both privacy and security. ''

UltraNote is a secure and privacy centred open source digital asset which is accessible to all. With UltraNote you will not only take control over your freedom but also act as your own *''bank''*. You and only you will control and hold responsibility for your funds. Your accounts and transactions are kept private from intrusive eyes through peer to peer encryption technology. UltraNote uses advanced cryptographic techniques, namely zero-knowledge proofs, to guarantee the validity of transactions without revealing sensitive information about them. UltraNote transactions are ***private, untraceable and anonymous.***

The UltraNote Blockchain is a mutually distributed ledger that creates, distributes, facilitates storage and finally executes the exchange of the cryptographic assets (XUN) via its wallets. The UltraNote Blockchain forms the ecosystem of the digital asset, which has been structured to deliver a set of financial and communication solutions. With UltraNote you will get to enjoy; enhanced security, greater utility (Desktop GUI, Online as well as mobile wallet), increased scalability (400+ TPS), wider acceptance, improved efficiency and above all unchallenged privacy. Similar to every blockchain platform, UltraNote payments are stored on the blockchain in order to keep the books balanced but the sender, recipient, and content of each transaction remain anonymous and untraceable. With the Self Destruct message feature you are guaranteed that your message transaction hash is destroyed making it simply inexistent on the blockchain.

At the heart of the system is an optimised version of Bitcoin, offering a fully decentralized open source digital asset which allows enthusiasts to contribute to its development and moreover help bring new ideas to the table on a highly empowering and individual level. With the core principles of the Digital Assets system in mind, the UltraNote platform has been designed to increase global prosperity through improvements in the quality and efficiency of its asset exchange. In addition to the Anonymous and Untraceable Funds Transfer facility, UltraNote wallet offers a P2P Encrypted Messaging with IPFS Encrypted File Transfer Service, Bank like facility such as Deposit for Interest of 3% per year and Integrated CPU Wallet Mining. Within the UltraNote ecosystem; Individuals, Businesses, Cooperatives and Merchants can freely exchange UltraNote coins for payments, Deposit Coins as a Store of Value as well as transfer Confidential Data such as video, voice recordings as well as confidential documents without the involvement of indiscrete 3rd parties like email service providers, banks or governmental institutions.

Furthermore instead of establishing value on UltraNote assets via government backing or declarations from regulating bodies, unlike accustomed commodities like gold or oil, the value of UltraNote is solely based on the quality and soundness of the ecosystem. In a world where governments dictate our financial activities, monitor our communications and data collection institutions stealing our private data from social media and regular service providers; offering an environment of Trust, anonymity and total self-sufficiency is fundamental to UltraNote. Putting the community first, ultimately through mass adoption, a more efficient and better-calibrated system of value will be established to promote prosperity and privacy among a larger and more diverse global population.

KEY DETAILS

Name	UltraNote
Ticker	XUN
Max supply	85 Billion
Decimal Place	6
Block reward	150 Coins
Block target	2 minutes
Maturity Time	10 Blocks
Mining curve	50% over 1st 6 years the remaining mined over 24 Years
Yearly Interest Rate	3% per Year (264,000 Blocks) or 0.25% per Month (22,000 Blocks)
Transactions per Seconds	400+
ICO	No
Blockchain Algo	CryptoNite Lite V1
Mining Specifications	CPU Wallet Integrated Mining & GPU Efficient (ASIC Resistant)
Explorer & APIs	http://explorer.ultranote.org/

Services:

- P2P *Anonymous* & *Untraceable* Fund Transfer
- P2P Encrypted Messaging
- P2P IPFS Encrypted File Transfer
- Bank-like Fixed Deposit 3% Interest per Year
- Wallet Integrated CPU Mining

1.0 INTRODUCTION

Since the introduction of Bitcoin in 2009, right after the world financial crisis of 2008, the rapid adoption of what once was qualified as an unrealistic and impossible project is now taking a real strategic turn to full adoption over the next 10 years. European, Asian and Middle East governments as well as banks are finally recognising the power and competitive threat of digital assets. Either Fed by fear of being left behind or realizing the true power of Blockchain technology they are now also encouraging the introduction of equivalent technology in their core business activities.

While the principal idea behind Bitcoin was to shake down and reshape the way we use and move *money* around the world, as a self regulated ecosystem offering confidential, faster and cheaper facilities as compared to fiat currency, Digital assets are also identified to be capable of empowering global population either in distressed regions as well as 1st world countries to regain power over their wealth. Allowing any Smartphone with an internet connection to turn into a personal and confidential ''*bank''* account, digital assets aim to give citizens of the world indifferent of age, race, location and wealth, the opportunity to store and use their money in a unified and democratic way.

Early adopters and visionaries are already reaping the benefits of their early investments, as the numbers speak for themselves. Bitcoin since 2009 appreciated from $.01 to $10,000 in 2017 scoring an increase of 1,000,000 X over 8 Years and only in 2017 recorded a raise of above 400X. The total digital asset market capitalisation is today in 2017 at $500 Billion from $30Billion over just 9 Months. *Note*: *(This Document is constantly being updated but since market figures are always moving; we are keeping the market reference numbers recorded at the time the first whitepaper was published)*

Technology-based money known as *Digital Assets* or *Cryptocurrency* is now a reality and is poised to develop for generations to come by recruiting more and more adepts as days go by. Bitcoin the pioneer of this emerging asset class has now paved the way and moreover demonstrated how it is possible to establish *Digitalized* and furthermore *Decentralize* ecosystems built on blockchain technology.

Even though Bitcoin and Blockchain technology has a lot to be praised for; the digital asset industry is not yet as glamorous and well-rounded as we may think. For instance **anonymity, price** as well as **scalability/ liquidity** remain major barriers to mass-adoption. Even though Bitcoin, Bitcoin clone coins or Bitcoin like coins allow keeping the names and identifications of users confidential since only the digital (wallet) addresses are used to interact, it is still not as private as ***cash***. Using a mutually distributed transparent ledger, transactions within the Bitcoin or Bitcoin like coins ecosystem can be easily retraced and pointed to specific individuals *(see link below)*. The price of Bitcoin furthermore in regards to mass adoption is not an easy factor to deal with neither. With a low liquidity& limited total supply of 21 Million coins, the price of 1 Bitcoin is now at around $10,000 from an all time high of $19,600. With moreover fees becoming more and more expensive, Bitcoin is now simply unaffordable to nearly 92% of the world's population. Scalability should also be considered as a challenge for Bitcoin and Bitcoin clone coins since being able to handle only 7 Transaction per seconds it is unimaginable to see Bitcoin progress via mass adoption while transactions are being delayed by hours like we witnessed during the end of 2017. Litecoin for instance can handle up to 57 Transactions per Seconds but we are not there yet for a comfortable mass adoption.

https://www.wired.com/2015/01/prosecutors-trace-13-4-million-bitcoins-silk-road-ulbrichts-laptop/

2.0 ULTRANOTE VS. ALTCOINS

Over the past 8 years the huge international success of Bitcoin has of course brought much attention to blockchain technology. Over the years, trying to improve the way people carry business as well as routine daily activities, several developers have also decided to implement their own blockchain start-ups. Today in May 2018, https://www.livecoinwatch.com/ the cryptocurrency reference website in regard to listing and sorting of cryptocurrencies/ Altcoins already has around 2000 listed Digital Assets each of them looking to write their own success story and name on the leader board next to Bitcoin.

Unfortunately this *''Bull Run''* has also brought along several challenges for the digital assets industry actors. Scams as well as *''ridiculous''* projects are surging everywhere like wild mushrooms making some *Altcoins* easy quick money making avenues for several groups of unreliable developers. Mainly running through ICOs their actions are of course hindering trust while promoting greed and creating confusions among interested investors/ users confused about where to put their money. From this perspective it is essential for UltraNote to show that we care about general public education and get them to understand how UltraNote's mission and vision align with the true values of **Decentralisation** and furthermore what UltraNote has to offer within a privacy focused ecosystem.

While majority of Altcoins develop their business model to be a newer or better version of Bitcoin which is at the end of the day only an alternative payment avenue to fiat currencies with some level of confidentiality. UltraNote is bringing to the market real unmatched added value through a range of comprehensive **Communication** and **Financial** services. UltraNote is **Untraceable** & **Anonymous** allowing Private Fund Transfers, P2P Messaging with IPFS Encrypted File Transfers. With the *Bank-Like* Deposit service UltraNote additionally allows users to deposit coins for interest of 3% per year. Positioned to lead mass adoption UltraNote Coin is again ahead of the curve by offering Wallet Integrated CPU Mining which allows anyone with a computer to mine UltraNote coins at minimum costs. Taking full advantage of blockchain technology; UltraNote is the go-to coin for new digital currency adepts as well as avid Cryptocurrency users by setting new standards.

Providing unmatched cutting edge technology such as ***Anonymous*** & ***Untraceable*** Transactions, ***Asset Deposit*** *for* ***Interest, P2P Messaging, IPFS Encrypted File Transfers, Integrated CPU Wallet Mining*** *and* ***400+ TPS*** UltraNote, comfortably confirms its superiority to **Bitcoin** as well as majority of **Altcoins**.

3.0 ULTRANOTE VISION & MISSION

At UltraNote our *Vision* & *Mission* is to establish a truly **Anonymous** as well as **Untraceable** global ***Communication*** and ***Financial*** platform which will unlock unquestionable ***privacy*** for every citizen of the world. Eliminating the drawbacks of traditional communication and financial channels by adapting to the new digital age, UltraNote is now setting grounds to provide a better, safer and egalitarian environment for people to interact and transfer assets. *''Why pay greedy Bankers massive fees to transfer money to a family member or pay your bills when you can pay yourself via mining fees''*

Our focus is set on delivering solutions that improve people's lives and empower citizens of the world to experience ***freedom*** of interaction without concerns about censorship or institutions monitoring their communications or finances. As a result each UltraNote user also becomes hacker worthless. At UltraNote we are highly committed to provide an environment where ***privacy*** and ***anonymity*** is respected and stays unbreakable.

Until today the worldwide power distribution was unfortunately mostly in favour of a handful of individuals known as the *''elites''*, who fed their craving for power through unfair regulations, bans, embargoes, economic sanctions, restrictions, censorship and even great depressions or dictatorship. Although humanity hopes to overcome global crises through education and internationalization, we still fail to take control over our lives and enjoy true freedom. With such a powerful asset as UltraNote it is now time for all of us to regain access to our ***fundamental rights***.

In A World Where Everyone Spies On Each Other, You Have To Be Invisible To Protect Your Privacy!

4.0 ULTRANOTE KEY OBJECTIVES & KEY FEATURES

4.1 Security & Privacy

The core essence of UltraNote is expressed through *Security*, *Trust*, *Peace of Mind*, *Untraceability* and unchallenged *Anonymity*. Build on cryptographic technology to guarantee ***privacy*** UltraNote blockchain offers a cutting edge platform which protects your private life from intrusive eyes while keeping your *communications* as well as *asset transfers* safely executed on the blockchain with the books balanced and tamper proof.

4.2 Liquidity

Liquidity is fundamental for the smooth running of any cutting edge communication as well as payment system. ''*One of the reasons why gold never became as mainstream currency is because of it low level of liquidity*''. Based on an asset exchange platform to perform its operations; a fair amount of assets is necessary to ensure that at any given time enough coins are distributed and made available to secure the transactions. With 85 Billion coins mined over 30 years it has been observed that as time goes by and mass adoption grows, UltraNote will allow for liquidity without disturbing the asset value as well as protect it from hyper inflation which will be in total harmony with the major aim of UltraNote as a digital asset. ''*Empower people by providing affordable access to state of the art communication and Financial technology while being able to self manage their own funds within their own means. Rich or poor we should all have the right to own a few UltraNote coins, Freedom is for everyone*''

4.3 Utility & Usability

As a Privacy Coin: Only the wallet addresses of users are relevant for transactions; No Name, No identity and No IP address will be attached to the wallets. UltraNote has the objective to provide a truly *Anonymous* as well as *Untraceable* communication and financial solution by offering the following Utility applications:

- P2P Private Fund Transfers
- P2P Encrypted Messaging
- P2P IPFS Encrypted File Transfer
- Bank Like Fixed Deposit for Interest 3% per Year
- Wallet Integrated CPU Mining

UltraNote Is Accessible & Fully Operational Via

- Operating system GUI Wallets:
  Available: Windows-Linux-Mac https://ultranote.org/
- Online Wallet https://mywallet.ultranote.org/
- Paper Wallet https://paperwallet.ultranote.org/
- UltraNote Market Place https://market.ultranote.org/
- Open Barzaar https://openbazaar.com/

Strategic Partnerships

- IAME Identity & Payment Solution https://iame.io/
- Check-Coin Online-shopping https://check-coin.com/

Exchanges Listing

- Stocks.Exchange https://stocks.exchange/trade/XUN/BTC/3M
- TradeOgre https://tradeogre.com/exchange/BTC-XUN
- MapleChangehttps://maplechange.com/markets/xunwae?markets=all&column=name&order=asc&unit=volume&pinned=false

Featured Listing Websites

- LiveCoinWatch.com: https://www.livecoinwatch.com/price/UltraNote-XUN
- CoinLib.io: https://coinlib.io/coin/XUN/UltraNote
- CoinCodex: https://coincodex.com/crypto/ultranote/
- WorldCoinIndex.com: https://www.worldcoinindex.com/coin/ultranote
- Blockfolio: https://blockfolio.com/
- Delta: https://getdelta.io/
- Cheddur App: https://www.cheddur.com/
- CryptUnit: https://www.cryptunit.com/
- CoinMarketCap: https://coinmarketcap.com/currencies/ultranote-coin/
- CoinGecko: https://www.coingecko.com/en/coins/ultranote

Upcoming Launch & Release

- Smartphone apps:
  1. Upcoming: IOS- Android Q4 2018 - Q2 2019

IOS and Android Apps for mobile wallets with fully integrated features as well as contact less payments are for UltraNote a fundamental part of its long term growth. In this perspective, mobile wallets will be implemented along the medium term time frame to allow optimised usability together with social integration of UltraNote worldwide.

4.4 Capital Appreciation

With a limited amount of coins mined over a predefined time frame; capital appreciation is simply a by product of demand and supply which directly influence the price of the asset. Adapting to a growing amount of daily transactions and a fixed deposit facility paying annual interest rate, it is inevitable that UltraNote will overtime develop a capital appreciation ecosystem which will allow any stage adopters to be rewarded for believing in the UltraNote project. With an inverted supply curve, it is also expected to witness a more stable price action over the years as compared to other well-known coins jigsaw price pattern. UltraNote supply will match UltraNote demand growth making it always affordable and resilient to hyperinflation. Nevertheless, similar to any traded asset, capital appreciation cannot be guaranteed. *(This section should not be considered as an invitation to buy UltraNote for capital gains. The aim is only to depict the vision of UltraNote)*

4.5 Distribution & Acquisition of UltraNote Coins (XUN)

1st stage UltraNote will only be available via mining which will distribute the coins among miners. It has been identified that in order to make UltraNote available to everyone and encourage an organic growth; No ICO will be implemented on UltraNote which will provide assurance that every interested party/stakeholder gets a fair chance on acquiring UltraNote.

2nd stage UltraNote will be listed on exchanges where miners will be able to cash out (sell) their UltraNote coins at market value. The UltraNote conversion to Bitcoin – Litecoin – Ethereum - Monero & WeyCoins will allow miners and regular users to enjoy their coins as they wish. As stated above UltraNote Development Team together with Community Leaders have already been able to get UltraNote Listed on 4 Exchanges but it does not stop there. We are also in constant negotiation with cryptocurrency exchanges for new listings as well as strategic partners and payments service providers. It is fundamental for the development team to get the best Deal possible for every stakeholder: Miners, Exchanges as well as the UltraNote Community. As time goes by and the UltraNote network grows we will be able to simultaneously expand our partnerships with new merchants along with mainstream service providers.

4.6 Fixed-Limited Supply

A fixed and predefined amount of 85 Billion UltraNote coins will be mined over 30 years. The distribution and mining of UltraNote will still be running for our next generations of users to allow the maximum of people to participate in this new adventure. Although the *Digital Asset* class is still at its infancy stage, we are anticipating a steady expansion of the users' network over the next 10 years. A fair amount of UltraNote coins will not only create an excellent level of liquidity to provide for micro-payments but also stabilize the level of inflation on the asset so as to again allow a wider global participation and organic growth due to its affordable price. Furthermore, with an inverted supply curve we can expect a more stable price action, UltraNote supply will adapt to a growing demand instead of diminishing supply while demands increases. Furthermore the limited supply of 85 Billon coins guarantee the rarity of UltraNote Coins which by default protects the ecosystem from depreciation practices well known from governments when printing new bank notes and making money supply unlimited.

Even if 85 Billion coins can be perceived as enormous; moving the decimal place to 6 instead of 8 or even 12 like other well-known digital assets; the UltraNote *Atomic-Unit* supply aligns perfectly with the major brands supply, thus solving the issue of dividing coins to several decimal places when dealing with micro transactions. Furthermore while keeping the total supply at a fair level for mass adoption, since by 2047 the world population is estimated to be at around 8.4 Billion People, it has been observed that even with a mid-range market penetration there will be enough coins for everyone without facing any oversupply situation.

An example of XUN supply against other Altcoins:

18,446,744.073709551616	-12	(Monero)
21,000,000.00000000	-8	(Bitcoin)
85,000,000,000.000000	-6	(UltraNote)

4.7 Proof of Holding & Deposit for Interest

In order to encourage mass-adoption and offer a fair avenue to people of any background to grown their net worth within a prosperous ecosystem; a ***Bank-Like Fixed Deposit*** facility paying an annual interest rate of 3% is available to UltraNote users. With an annual interest rate comparable to conventional *deposit/saving accounts* at entities like banks or mainstream financial institutions, UltraNote is well positioned to take the lead as a value storage asset too.

4.8 Fully Encrypted-Anonymous & Untraceable Ecosystem

The UltraNote ecosystem is based on the highly encrypted and impenetrable CryptoNote Algorithm and IPFS Protocol allowing complete autonomy, untraceability, anonymity and privacy while transferring funds or communicating within the UltraNote ecosystem. To any entity either within or outside of the UltraNote ecosystem you are simply a ***Ghost***.

4.9 Convertibility

UltraNote coins distributed among community members as stated previously will of course be tradable on relevant recognised cryprocurrency exchanges allowing UltraNote holders to convert their coins to either Bitcoin or other major cryptocurrencies and *Fiat* currency. Merchants' partnerships will in addition contribute to the convertibility options available to UltraNote Holders since they will be able to pay for their bills as well as their goods and services directly with UltraNote Coins from their Wallets. The future implementation of contactless payment via UltraNote mobile wallet on smart phones **IOS** & **Android** will furthermore consolidate the convertibility of UltraNote coins.

5.0 ULTRANOTE TARGET MARKET

As a true ***Anonymous***, ***Untraceable*** and moreover ***Egalitarian*** Digital Asset, UltraNote is designed to appeal to a wide international audience due to its simplicity of utilisation, mining specifications as well as affordability.

Developed to offer a trustworthy and comfortable environment for adults as well as younger people to interact, we believe that regardless of someone's profile everyone can easily benefit from UltraNote. Anyone should be able to privately and safely message a loved one and share holiday pictures away from intrusive eyes. Similarly anyone should be able to transfer funds to a loved one with minimum fees calculated in ***cents*** as compared to mainstream money transfer facilities like *MoneyGram* or *Western Union* charging between *8%* to *10%* of the amount transferred.

As a very safe and affordable cryptocurrency for the mass-market we are expecting parents to feel comfortable enough to make UltraNote their go to digital asset in regard to their children pocket money and financial education. Children as well as adults can feel safe using their UltraNote coins on the relevant platforms while enjoying the freedom of taking care of their own finances and build up their net worth with the fixed deposit service of UltraNote.

6.0 ROAD MAP

- **New Exchange Listings**: Ongoing
- **New Strategic Partnerships**: Ongoing
- **New Mining Pools:** Ongoing
- **Network Reinforcement:** Ongoing
- **Online Wallet Messaging:** Q4 2018-Q2 2019
- **Mobile Wallet App Android & IOS:** Q4 2018 - Q2 2019

7.0 ULTRANOTE MARKETING & COMMUNICATION

Our strategy is to make UltraNote as much accessible as possible which involves a very strong online as well as offline presence managed by a very active marketing and press team.

UltraNote website http://ultranote.org/

UltraNote Official Press Page https://blog.ultranote.org/

Facebook https://www.facebook.com/Ultranotecoin/

Twitter https://twitter.com/Ultranotecoin

YouTube Channel https://www.youtube.com/channel/UCO8vLGEm9zObrKgzMAw-ynA/featured

Reddit https://www.reddit.com/r/UltraNote/

Instagram Ultranote_Official https://www.instagram.com/ultranote_official/

Telegram https://web.telegram.org/#/im?p=g228367263

Discord https://discord.gg/ss2NtaA

Linkedin https://www.linkedin.com/company/ultranote-organisation

Bitcointalk https://bitcointalk.org/index.php?topic=2357930.0

Cheddur https://www.cheddur.com/coins/ultranote

Decentral.News https://en.decentral.news/ultranote-privacy-fingertips/

Other Online platforms are in development and Online/Offline written press as well as Online/Offline mainstream media channels will be implemented in due time as UltraNote gets relevant traction.

8.0 ULTRANOTE TECHNOLOGY

UltraNote is initially build on the Cryptonote Blockchain technology on which is also based Monero as well as Bytecoin our main running mates. Nevertheless even if we share the same technology, our team of developers and analysts have been able to come up with UltraNote with a far better implementation of Cryptonote Technology as developed above. ''***If you like Monero your will love UltraNote''***. Since the launch of UltraNote we have brought much development to the Algo which makes UltraNote a unique project even if sharing the DNA of other CryptoNote Coins.

In order to better understand the technology behind UltraNote; the following ***tech specifications*** have been **directly imported** from ***CryptoNote*** Website. https://cryptonote.org/inside/

CryptoNote Philosophy

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

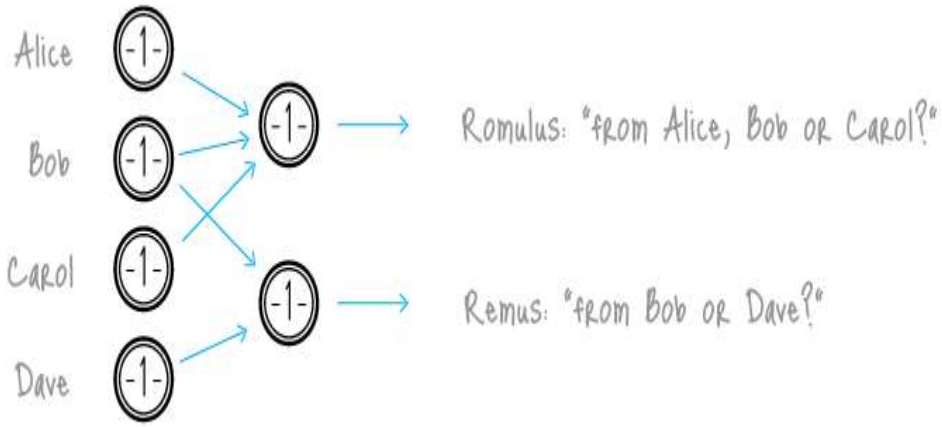
The ordinary digital signature (e.g. (EC)DSA, Schnorr, etc...) verification process involves the public key of the signer. It is a necessary condition, because the signature actually proves that the author possesses the corresponding secret key. But it is not always a sufficient condition.

Ordinary signature

Ring signature [1] 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.

Ring signature

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.



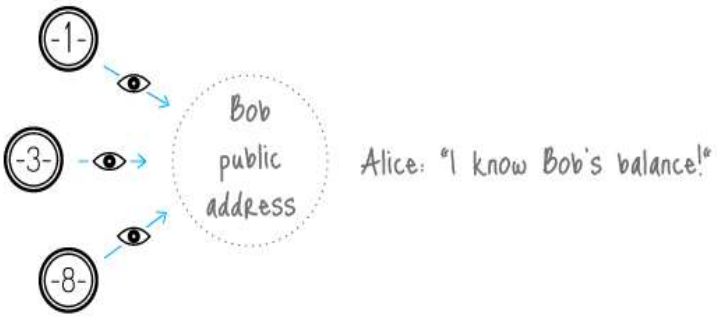
Untraceable transactions

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).

[1] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In ASIACRYPT, pages 552–565, 2001

One-Time Keys: Unlinkable Transactions

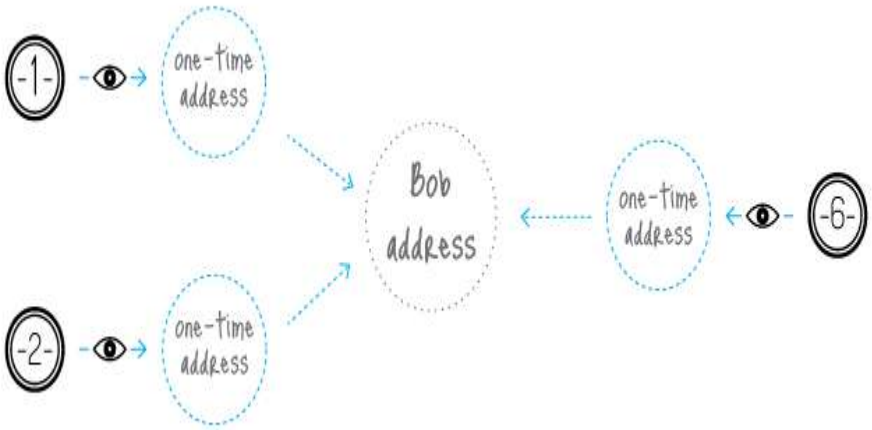
Normally, when you post your public address, anyone can check all your incoming transactions even if they are hidden behind a ring signature. To avoid linking you can create hundreds of keys and send them to your payers privately, but that deprives you of the convenience of having a single public address.



Linkable transactions

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**[1]. 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.

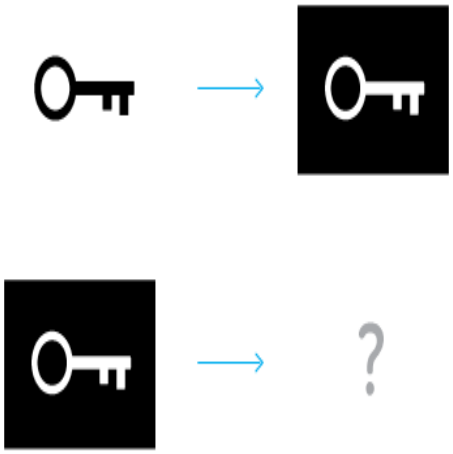


Unlinkable transactions

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.

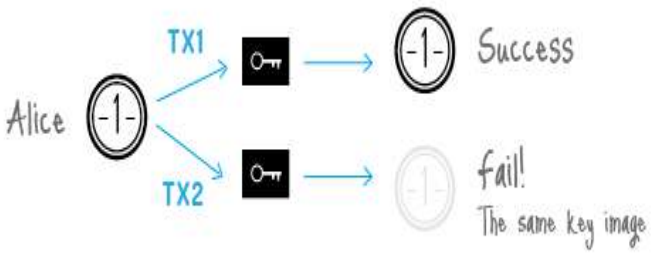
Double-Spending Proof

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**" [1]. 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.



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.



Double-spending check

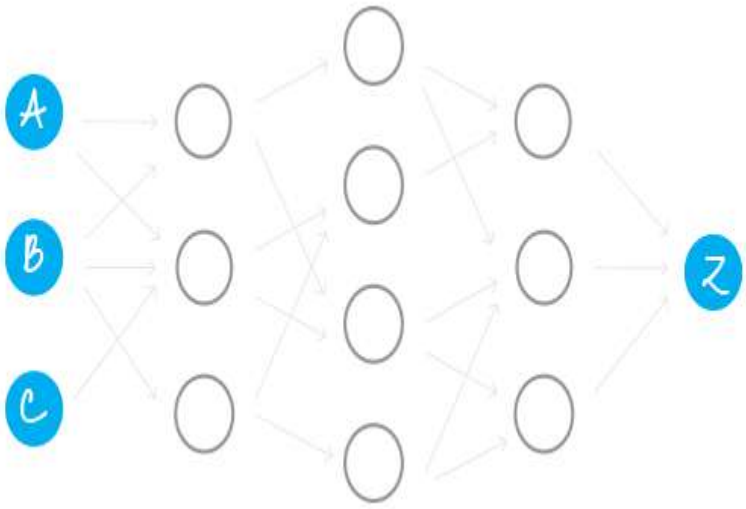
[1] Eiichiro Fujisaki and Koutarou Suzuki. Traceable ring signature. In Public Key Cryptography, pages 181–200, 2007

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?

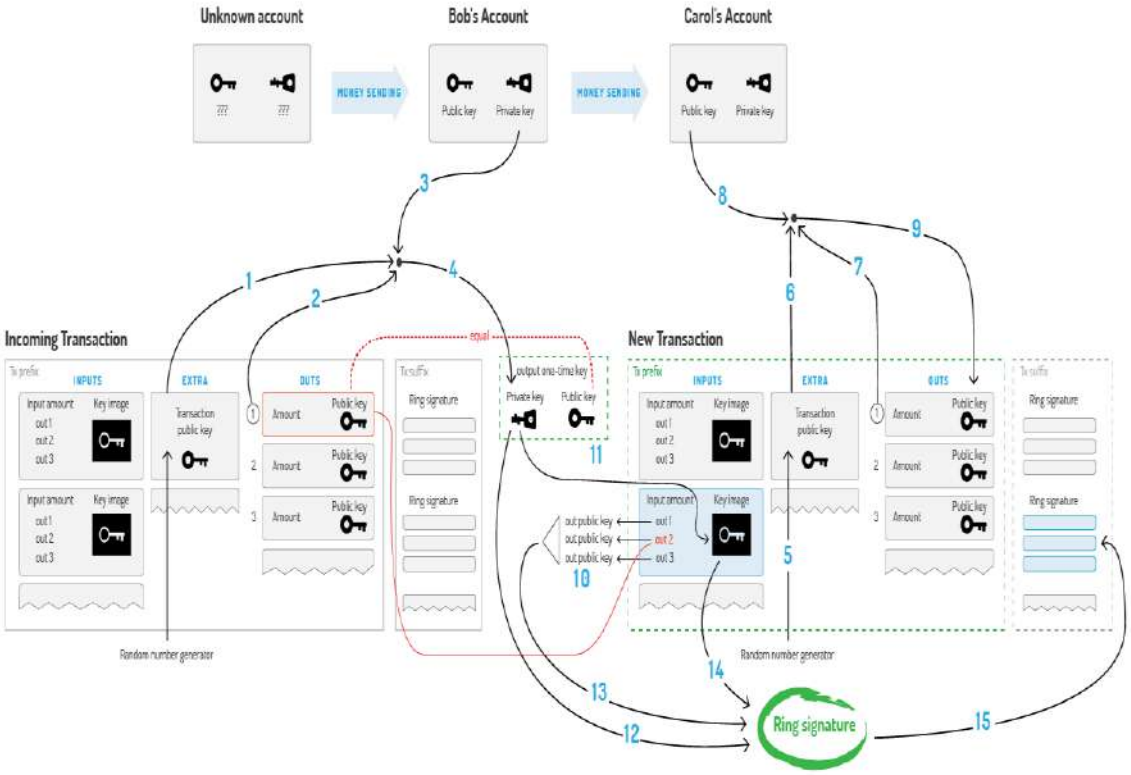
Trying to draw a graph with addresses in the vertices and transactions on the edges, one will get a tree: a graph without any cycles (because no key/address was used twice). Moreover, there are billions of possible graphs, since every ring signature produces ambiguity. Thus, you can't be certain from 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.



Blockchain analysis ambiguity

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).



A standard CryptoNote transaction

9.0 CONCLUSION

Since 2009*, Digital Assets* and *Blockchain Technology* have together certainly received more than enough attention in order to become the hottest subject on the streets. Millions of fiat currencies are being converted into digital assets everyday with a momentum never seen before. Is it the right time to start paying attention? ***Unquestionably yes***! This technology is and will for a long time keep disrupting the way we do business as well as spend money everyday. At the moment the market is certainly very volatile due to several unknown variables that are creating as much hope, excitement, speculation as well as fear. Will digital assets eradicate fiat currency like many people tend to believe? ***Certainly not***! Simply because without Fiat Currency, Digital Assets will have no benchmarking value.

At UltraNote we believe that digital assets as a new asset class has it very own place in an environment where privacy and autonomy is often compromised. As a service provider we expect UltraNote as well as other valuable digital assets to co-exist in harmony within their respective established ecosystem. Similar to any asset class, without fiat currency as a scale of value, an asset is worthless. The key factor is how we use UltraNote to use our fiat currency more efficiently.

Only time will tell how Digital Asset will establish itself but if one thing is certain; it is that cryptocurrency is here to stay and grow. Digital Assets and blockchain technology are still at their infancy state and yet have to achieve mainstream adoption to start expanding further. The internet took almost 2 decades to become what it is today and yet has so much more to offer. Patience will definitely be very generous to anyone who is willing to put a few Dollars or Euros into UltraNote or other solid digital assets as the upcoming 5 years will definitely set solid grounds for what is described as the currency of the new age.

After several years of research and thorough analysis carried out by our expert developers and analysts, we are confident that UltraNote has been executed to be perfectly positioned to record solid organic growth over the next 3-5 years going through mass-adoption, before exploring new horizons such as high profile organisations taking advantage of the cheaper and more cost efficient encrypted communication tools offered by UltraNote. The business applications of UltraNote are furthermore limitless and this is what makes UltraNote a very valuable asset for those who know how to identify long term value propositions.

We humbly invite you to get involved with UltraNote by joining us on our various social media platforms as well as download your wallet on Ultranote.org to start mining with us for a fair chance to prosperity.

Launch is scheduled for the 4th Of November 2017.

Good luck Everyone!

Warmest Wishes,

UltraNote Team