SpaceKG

Table of content

REVIEW OF CRYPTONOTE

Decentralization and anonymity are important in the financial world because of the inevitable conflicts of interest between any centralization authority and users. The Man needs to be paid, and we need our privacy. It's not a bad thing, it's just how it is, and it can be solved with technology. Bitcoin was the first decentralized, peer-to-peer, pseudonymous attempt at a solution. To this author's knowledge, few other truly unique solutions have been proposed. Overall, the CryptoNote (CN) protocol represents the first new step in the cryptocurrency space since Bitcoin and it's one that deserves as much shoulder space as Bitcoin. It's a heavy hitter, no doubt about that, with quite a few basic improvements over the Bitcoin protocol and a few big improvements. This paper is intended to review the CN white paper, point out at least some of the advantages and disadvantages of the proposed protocol, and illustrate points of possible improvements of the protocol. So how does CN work? Well, just like anything in the cryptography world that works well, it works weirdly. We can imagine the CN protocol as a post-office-box system. Each user has a set of public keys and private keys, just like in the BTC
protocol. Rather than sending CrytpoNote directly to each other's public keys, users execute a Diffie-Hellman exchange and create ring signatures to make a new

Literature Review

Van Saberhagen's history of ring signatures, starting from group signatures, is quite interesting. Group signatures started out as the first way of allowing any public member of a group to anonymously sign a message on behalf of that group, in

which there was a group manager who could, at her own discretion, revoke user's anonymity. The name "group signature" annoyed algebraists, who pretty much invented cryptography, thank you very much.
Ring signatures were developed to remove the centralization point of a group manager. The name also annoyed algebraists. Essentially, if everyone has a public key and a private key pair, all we do is sign our message with our private key like usual, and then publish a set of our friends' public keys together with our own public key, and establish some protocol so that we use the whole public key set to verify the message. Simple! This establishes untraceability.

1. Traceability

Then linkable ring signatures came along, which is confusing because, using our terminology in this paper, it's really not untraceable, or at least scalably traceable. These are ring signatures in which the sender can essentially revoke their own anonymity as desired. Next up came traceable ring signatures, which is also confusing, because it doesn't have to do so much with traceability in our sense. The way traceable ring signatures work is to establish a one-time method of using a ring signature, perhaps in voting schemes. Definitely useful in any token-based system. Finally, we get to ad hoc group signatures in which we just pick our group members on the fly. Using the historical constructions:

- Group signatures
- Untraceable Ring Signatures
- Scalably Traceable Ring Signatures
- One-time-use Scalably Traceable Ring Signatures
- Ad hoc group signatures

Van Saberhagen glued all of that together to get CryptoNote. Pretty clever, really, if you ask me. However, we aren't going to use any of that terminology at all for the rest of the paper. That's just where all of this fits into the "old crypto" context. Which, it turns out, is super important: if you try new crypto, you usually get burned.

2. Improvements over Bitcoin

Little improvements over the Bitcoin protocol abound abound in CryptoNote. Your password is equivalent to your private keys, and each user needs only one address. There is no transaction collisions. You can give away half of your private keys without fear of lost security to, say, a payment processor. Any user can generate an income-auditable address by deterministically generating half of their keys. Transaction scripts are super simple. Global variables like block size and block reward dynamically adjust so we need not worry about network consensus

for infrastructure-like changes to code. Really, most of the nicest benefits are just a bunch of little things.

2.1. Untraceability and Unlinkability. Some bigger stuff makes you just feel good, even if it isn't really a feature: a proof that transactions are unconditionally unlinkable (under the random oracle assumption). According to van Saberhagen, two transactions are unlinkable if we can't prove they went to the same person, and a system is unlinkable if, for any two transactions, they are unlinkable. The random oracle assumes the existence of some perfect hash function, which is somewhat unrealistic but not well approximated by current hash functions. The only better proof would be under the standard model, and almost no cryptographic models are proved under the standard model. No other developers have proven anonymity in their coins. I cannot stress this enough. No other coin has the weight of mathematical proof behind their product. Even Bitcoin only recently has had a rigorous security analysis applied to its methods, and it is known that Bitcoin fails unlinkability and untraceability! This absolutely blows any competing coin out of the water.

The closest contender is Zerocoin/Zerocash. The CryptoNote white paper is wrong in some of their criticism of Zerocash, by the way, since the Zerocash protocol has made a recent breakthrough in their size constraints; however, I quote CN developer Maurice Planck on this one:

[Maurice P]Zerocoin, Zerocash. This is the most advanced technology, I must admit. Yes, the quote above [from the white paper] is from the analysis of the previous version of the protocol.

To my knowledge, its not 288, but 384 bytes, but anyway this is good news [the latest trimming of sizes]. They used a brand new technic [sic] called SNARK, which has certain downsides: for example, large initial database of public parameters required to create a signature (more than 1 GB) and significant time required to create a transaction (more than a minute). Finally, they're using a young crypto, which I've mentioned to be an arguable idea:

https://forum.cryptonote.org/viewtopic.php?f=2&t=19#p55
Now, notice that since we are still pushing information through a function (our random oracle function), and not using a zero-knowledge system, our system is still not fully zero-knowledge anonymous. Andrew Poelstra described a wonderful state-of-the-art on anonymous coins on the CryptoStack Exchange website, including an in-depth discussion about CryptoNote and some proposed tweaks. Transactions are also scalably untraceable. According to van Saberhagen, a transaction is untraceable if all possible senders are equiprobable, meaning a sender chooses a ring signature set of public keys, and from any attacker's point of view, all members of that set are equiprobable as possible senders. Further, this feature is scalable in the sense that you can choose the size of your obfuscating set (ambiguity degree is the number of public keys in your obfuscating set), and even choose your ambiguity degree to be n = 0 if you so desire.

Van Saberhagen, lists two desirable properties of a cryptocurrency: untraceability and unlinkability, and we've mentioned both. Let's say I'm listening in on some cryptocurrency network and I compare two transactions. We can imagine a transaction as being an arrow from one user to another with an amount as it's length. So we have two arrows, of different length. Problem is, we don't know who is sending or receiving, right? At least, ideally, we don't know. So we'll just throw random names on here:

A = Alice 1.101 /Bob = B
C = Charlie 0.0637 /Danielle = D

Van Saberhagen, defines a system to be untraceable if, for each incoming transaction, all possible senders are equiprobable, and unlinkable if, for any two

outgoing transactions, it's impossible to prove they were sent to the same individual. I interpret "impossible" here to mean "of probability that can be made arbitrarily small, if not zero." Let's pause and think about these definitions, because they are great! Notice that the best possible "anonymous" coin would provide no information whatsoever about any given transaction. That is to say, any given sender is as likely as another for any given transaction. So this definition of untraceable is nice and natural.

3. Problems with the Protocol

This is saying a lot: my single biggest question after reading the entire paper sound; who chose the constants? Will there be a plan for choosing new constants in the future if needed? How can I choose other constants if I decide to fork it? Did the NSA come up with CryptoNote and choose these constants so any CryptoNote network has 10% the entropy of any other coin? Who knows. It's probably not a big deal, and every coin has this as a critical point. Indeed, it's a centralization point. If we all go happily forking the CryptoNote code left and right, we are
trusting those developers to have made good decisions on the constants. Next up is the not-so-obvious, already mentioned: this is not a zero-knowledge system, so some information is still preserved after each step. Andrew Poelstra made a wonderful post on CryptoStack Exchange about it: [Andrew Poelstra] This [one-time ring signature scheme] provides good anonymity, but even with the improvements listed presently,
this is not a zero-knowledge scheme. This means that linkability is confounded but an adversary with good analysis tools will certainly be able to glean a non-zero (literally, innity times as much as zero) amount of information.

Andrew is being a bit hyperbolic here. Non-zero simply means "not zero" whereas he's thinking of infinitesimal. Doesn't matter, point is made! The idea is this: a zero-knowledge proof does not use ANY information to construct the proof. Whereas, for example, a random oracle H H(private stuff), a function of the keys. It's "random," it's uniquely identified with the keys in a way that no
outsider can duplicate, and so on, but information is passed through the function. Therefore, if I were the God Almighty on high, if I were the Greek God of Entropy and Statistics, I could peer through this mortal function H and recover your private information.
Anonymity can be violated in a few ways; any time you spend an output and set the ambiguity degree n = 0, you reveal yourself as the spender of that CryptoNote and anyone can go back through the blockchain. Any obfuscating output set with your now-spent output as a member becomes less ambiguous by a degree of 1. Indeed, ambiguity degree becomes monotonically decreasing over time. However, users

never need to set a low ambiguity number since they can prove they made a payment in other ways.

More drawbacks include: keys are twice as large as in the Bitcoin protocol, the CN protocol experiences long-term uncontrolled growth of unspent transaction outputs (UTXO) and a large blockchain. Unfortunately, this seems to simply be ignored by the author, but, honestly, I probably would have ignored it too. You invent something, and it's really heavy. You bring it to the County Fair. Are you going to be like... "hey guys, look at my really heavy thing?" Or are you going to be like... "hey guys, this thing will cut your hair and take your dog for a walk!"
Some jerk may come out of the crowd and may be like "but, dude, that thing weighs like 1000 pounds and it gets heavier every time it sucks up your hair or picks up your dog's doo, which are critical tasks with respect to this creation of yours."
And you just shrug, because you made something, right? Anyway, some other guy may come along and figure out that it needs a hatch so you can lighten it up occasionally. Apparently Andrew Poelstra and G. Maxwell are both working on that now, using Merkle trees and required prefixes for one half of the Cryptonote private keys (the half you would give away to a payment
processor). I am hoping to come up with something.

3.1. New technology. The CN protocol implements a piece of cryptography unseen in cryptocurrencies before, in particular, the idea of using key images to protect against double spending. This is boldly treading on dangerous ground; no matter how deeply I, or any mathematician scrutinizes an algorithm in any white paper,

it's possible some 16 year old in South Africa will figure out a way to crack the encryption. On the other hand, if you throw together some RSA or ECDSA libraries, you know that works. You know that works. This is due to a famous effect in mathematics called "Just because I can't see it doesn't mean it isn't there." I have looked through the CryptoNote white paper and it looks good. This just means I'm not as clever as whoever will eventually break CN and BTC wide open. On the other hand, the number of eyes and brains trying to crack open "old cryptography"
is different by orders of magnitude, with history on its side. However, the only thing for it at this point is to let it stand the test of time.

3.2. New Algorithm. Van Saberhagen makes excellent points that cost of investment should grow faster than linearly with power, and ge describes a perfect algorithm to accomplish the task. But without providing that algorithm, it's just a bunch of snake-oil. I guess the proof is in the code. However, implementing an entirely new Proof-of-Work algorithm could be just as vulnerable to exploitation as implementing any new piece of software. To be frank, without any sort of explicit, clear explanation of how it's been done, it can't necessarily be trusted. With Bit-

coin, the task was clear: find the nonce so that the SHA hash is small. With this algorithm? I have no idea.

Over the past few years, and probably for the next few years, it's been the case that a CPU is better at dealing with stuff that requires lots of random access to memory, whereas GPUs and ASICs have been better at dealing with sequential, iterated data that can be constructed in a lazy way. So, it appears that van Saberhagen has simply taken the Scrypt construction and either iterated it so that each hash depends on all previous states, rather than just the last previous state, or concatenated the input, or something along those lines. This way, all previous states need to be kept in memory and randomly accessed, the process can't be sequentialized easily, and it will be years before ASICs can handle it. However, this is just my best guess. I have no good reason to think this based solely on my reading of the white paper.

What we need is an explicit description of the algorithm, and we need some analysis done on the algorithm.

3.3. Dynamic Variables. Variables adjust dynamically in time. This is, if you recall, a positive from above. It's also a negative. If care is not taken, this can lead to either blow-ups, or wild fishtailing. The CryptoNote authors propose rejecting blocks if they are too large (larger than twice the median). This can, if a longterm attack is executed, lead to an exponential blowup of the blockchain. It's unlikely, and costly, but possible. Furthermore, given the already unwieldy size of the CryptoNote blockchains, doubling the size of the average block even once or
twice could lead to significant problems with the network. A true "blow-up" to infinity is not necessary to cause disruption, and a smaller attack can be avoided mathematically.
To discourage such behavior, a block reward penalty for abnormally sized blocks is introduced; but this may lead to increased fees in times of high economic traffic like Christmas shopping, which would be intolerable to customer acceptance of the coin. This encourages us to find a mathematical solution to block-acceptance rather than to find an economic incentive to users.

4. Deficiencies in the white paper and Further Questions

The white paper is well-organized in terms of sections, for the most part, but extremely poorly written and uses inconsistent terminology. But guys, I'm going to give van Saberhagen a break: there is a LOT of information in a white paper. It can't really be a manual, but in my opinion, there should at least be enough information to re-develop the technology from scratch. Vital information is left out, important

equations are not indexed correctly, and notation is left unexplained. The so-called "standard transaction sequence" in section 4.3 doesn't include any information about where signatures take place. Unfortunately, a lot of this section is... simply hard to read and not well explained. Bad notation is typical; is that the destination key? Or the transaction public key? Which is what? Where is the key image? Where is it even used? Check the diagram! For example, the following two statements should be strung together and followed with an explanatory diagram and a bit of pseudocode.

[Nicolas van Saberhagen] The identity of the signer is indistinguishable from the other users whose public keys are in the set until the owner produces a second signature using the same key pair. [Nicolas van Saberhagen] In case Alice wants to prove she sent a transaction to Bobs address she can either disclose r or use any kind of zero-knowledge protocol to prove she knows r (for example by signing the transaction with r). This aspect of CryptoNote (choosing to violate one's own untraceability to prove payment) is critical for usage as a currency, and hands are waved.

It's absolutely unconscionable to to come up with a new "Proof of Work Algorithm" and then refrain from including any sort of pseudocode to describe that algorithm. Upon which. Your entire. Coin. Is. Based. Ugh.

5. Conclusion

The CryptoNote protocol is absolutely spectacular. It cannot really be compared to Bitcoin because a layer of anonymization takes place between a user's public addresses and their transactions. Further, myriad improved features are scattered throughout. It's a genuinely different way of transferring wealth cryptographically via Blockchain-by-Proof-of-Work, compared to Bitcoin. It cannot be directly said to be a Bitcoin 2.0, but more like a completely different protocol that establishes and obtains different objectives.
There are some critical problems with CryptoNote. The size of the the entire project is just enormous. Key sizes are double the usual size. Unspent transaction output sets and key image sets both grow in an uncontrolled way. Most troubling is the centralization point of allowing an anonymous person on the internet choosing all of our elliptic curve constants without explaining himself.

However, having said all that, CryptoNote is absolutely spectacular. If you have a problem with the constants, and if you can figure out how to generate new ones, I say go for it. The protocol looks secure and tight.

For more info about the Cryptonote please visit
Cryptonote v 2.0

Cryptocurrency Industry Overview

The cryptocurrency, crypto tokens and other digital assets based on blockchain technology are currently experiencing an explosive growth period. Blockchain technology allows the first true internationalisation of a store of value, and recently the adoption rate has meant
explosive growth in both adoption and speculative value. 2017 started with Bitcoin as the number one cryptocurrency with a market capitalization of 12 billion US dollars. Ethereum, a very young upstart of a currency was valued at just 700 million USD. The explosive start to 2017 has seen Bitcoin surge to a market capitalization of over 40 billion USD and Ethereum has caught up at an incredible pace and now has a market capitalization of over 28 billion USD.

The market is excited by the opportunities that blockchain technology and decentralization of currency present. There are over 800 alternative cryptocurrencies trading today, with a new use case for blockchain emerging every week. Investors need to think carefully before choosing a project to ensure the team, the technology and the idea are sound.

What is An Initial Coin Offering?

ICO is the abbreviation of Initial Coin Offering. It means that someone offers investors some units of a new cryptocurrency or crypto-token in exchange against cryptocurrencies like Bitcoin or Ethereum. Since 2013 ICOs are often used to fund the development of new cryptocurrencies. The pre-created token can be easily sold and traded on all cryptocurrency exchanges if there is demand for them.

With the success of Ethereum ICO are more and more used to fund the development of a crypto project by releasing token which is somehow integrated into the project. With this turn, ICO has become a tool that could revolutionize not just currency but the whole financial system. ICO token could become the securities and shares of tomorrow.

Short History of Initial Coin Offering? – ICO

Maybe the first cryptocurrency distributed by an ICO was Ripple. In early 2013 Ripple Labs started to develop the Ripple called payment system and created around 100 billion XRP token. The company sold these token to fund the development of the Ripple platform.

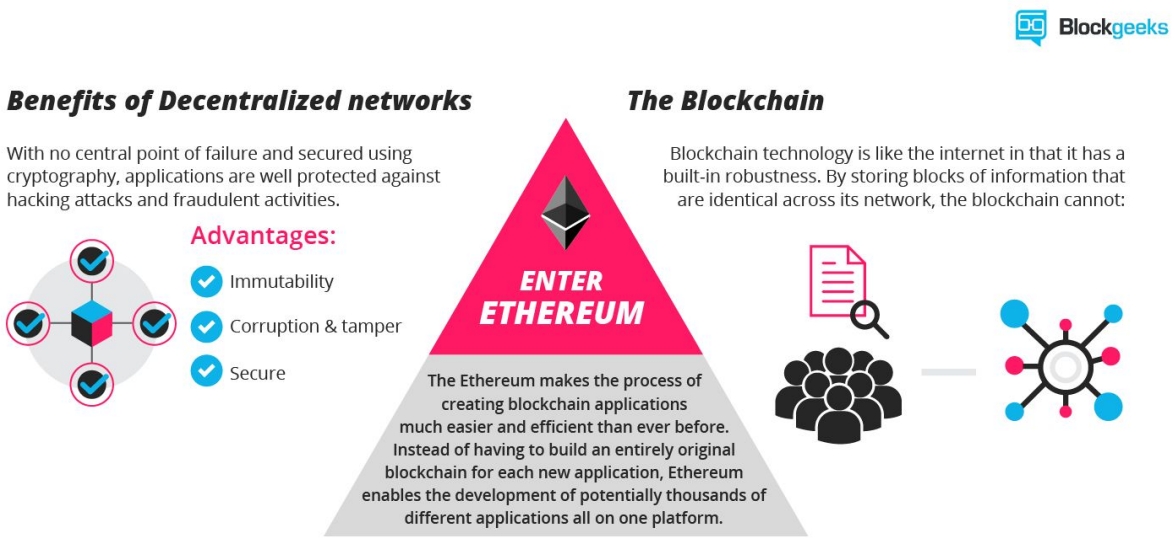
Later in 2013, Mastercoin promised to create a layer on top of Bitcoin to execute smart contracts and tokenize Bitcoin transactions. The developer sold some million Mastercoin token against Bitcoin and received around $1mio.

Several other cryptocurrencies have been funded with ICO, for example, Lisk, which sold its coins for around $5mio in early 2016. Most prominent however is Ethereum. In mid-2014 the Ethereum Foundation sold ETH against 0.0005 Bitcoin each. With this, they receive nearly $20mio, which has become one of the largest crowdfunding ever and serves as the capital base for the development of Ethereum.

As Ethereum itself unleashed the power of smart contracts, it opened the door for a new generation of Initial Coin Offering.

Ethereum – The Initial Coin Offering?- ICO Crowdfunding Machine

One of the easiest application of Ethereum's smart contract system is to create a simple token which can be transacted on the Ethereum blockchain instead of Ether. This kind of contract was standardized with ERC#20. It made Ethereum host of such a wide scope of ICO that you can safely say that Ethereum found its Killer App as a distributed platform for crowdfunding and fundraising.



The most prominent demonstration of the potential of Ethereum's smart contracts has been The DAO. The distributed investment company was fuelled with Ether worth $100m. The investors received in exchange against Ether Dao Token which had their own market price and enabled the holder to participate in the governance of the DAO. After it was hacked, the DAO however failed.

The concept of funding projects with a token on Ethereum became the blueprint for a new and highly successful generation of crowdfunding projects. If you already tried out, you know that investing in token on top of Ethereum is charmingly easy: You transfer ETH, paste the contract in your wallet – and, tata: The token appear in your account and you are free to transfer them as you want.

Examples for successful Initial coin offering on Ethereum are:

- Augur
- Melonport
- Golem
- ICONOMI
- Singular DTV
- First Blood

- Digix DAO.

There are dozens of ICO every month which explore new and creative ways to connect the application with the token and to leverage smart contracts to add more features to these tokens.

The potential of this trend is immense. ICO enables every individual and every company to easily release freely tradable tokens to raise funds. It could be used to completely reconstruct the financial system of shares, securities and so on. It decentralized not just money, but stock creation and trade.

If you want to assess Ethereum's market capitalization you should not only look at the market cap of Ether itself but also on the value of the token, which adds something like $300 Million to Ethereum's $4 Billion market cap.

Legality

The legal state of ICO is mostly undefined. Ideally, the token is sold not as a financial asset but as a digital good like many other things. This is why ICO is often called "crowd sale". In this case, in the most jurisdiction, the funding with an ICO is not regulated, which makes it extremely easy and paperless, given a lawyer experienced with the issue is on board.

However, some jurisdictions seem to be aware of ICO and tend to regulate them similar to the sale of shares and securities. The spectacular implosion of the DAO did a good job in kindle regulators attention. So while ICO currently mostly happen in a gray area, in the future they most likely will be regulated. This could bear some financial and legal risks for investors. Also, the cost and effort to comply with regulation could reduce the advantages of ICO compared with traditional means of funding.

Profit and Loss

Many ICO has been a lucky choice for investors. ETH, for example, was sold at 0.0005 Bitcoin and is worth today 0,05 BTC. Profit: 10,000 percent. Augur token (REP) were sold for around 0,005 each and are now traded at 0,01. The gain in value of 100 to 500 percent in Bitcoin is common for successful ICO.

On the other side, many ICO ends with losses. Cryptocurrencies like Lisk, IOTA-token or Omni did not hold the value in Bitcoin the token has been assessed at the ICO (or struggle to keep it). Often ICO is even used by scammers and semi-scammers: Build a glossy website, write some blocks of bullshit bingo, promise the greatest project/cryptocurrency ever, and be happy if you receive just 50 or 100 Bitcoin. Besides the large and successful ICO, like Lisk, Melonpost, Augur or Iconomi, many small and shady ICO did collect funds and delivered nothing at all.

The ICO market is currently still completely unregulated. Everybody should be aware, that this does imply not only large profits for investors, but also large losses.

The hottest Initial Coin Offering of the past

Let’s have a look what’s going on of the market for ICO. In the past years, there have been a couple of wildly successful ICO.

Hot past Cryptocurrency ICO

Ripple

Ripple Labs created 100 billion XRP-token which serve as an anti-spam mechanism in the payment network Ripple, as you have to pay your network fees in XRP. The XRP are sold by Ripple Labs; their value doesn’t move in a clear direction, while the trend is more downwards. It started with around 5,000 Satoshi, sometimes felt below 1,000 Satoshi, raised above 7,000 and finally fell again to a new low of 600 Satoshi, before again raising on 3,000.

Next

Next was a new gen cryptocurrency made in 2013. For a start, the 1 billion token was sold to early investors. With the ICO the developers only got a double digits amount of Bitcoins. Today the NXT token, however, are worth much more and Next has become a relatively successful and stable cryptocurrency.

Mastercoin

In 2013 Mastercoin announced to build a layer on top of Bitcoin and sold the Mastercoin-token to investors. The developers received around 10,000 Bitcoin,

which has been worth $1mio at this time. Mastercoin token gained value some month later; some investors made huge profits. Later Mastercoin merged with Counterparty and Omni.

Ethereum

The largest ICO by now was made by Ethereum. With a presale of around 60mio ETH, the Ethereum Foundation raised around 31,500 Bitcoin. This event has become one of the biggest crowdfunding ever and the start of a wildly successful cryptocurrency. The investors of the ETH-presale profited massively.

Lisk

Based on BitShares, Lisk is a JavaScript written Blockchain which enables smart contracts on sidechains. Lisk sold the coins for Bitcoins and received around $5mio.

Hot past Ethereum token ICO

While most ICO in the past has been restricted to building a new cryptocurrency, the smart contracts of Ethereum enable startups also to use ICOs to fund development. Most of them are working with Ethereum itself and trick their presold token somehow in the process. Some examples:

Augur

The decentralized prediction market uses so-called REP-token to decide on the outcome of events. 80 percent of these tokens have been sold to fund the development and got the team more than $5m. Today all the token are worth more than $100m.

Golem

The Golem project aims to create a decentralized supercomputer, to which participants can contribute with their own computer and earn money by selling its power. Golem uses the Ethereum blockchain for smart contracts; the GNT token is needed to pay for the services. The ICO was restricted on 820,000,000 tokens, for which the developers received more than 10,000 BTC. Today the market share of Golem is beyond 50,000 BTC.

ICONOMI

Iconomi is a platform for the management of virtual assets. The ICN token is something like shares on the platform and should receive parts of the profits. The developers sold 85,000,000 token and got more than 17,000 BTC for it. Today it has a market capitalization of nearly 40,000 BTC.

First Blood

The Asian platform for decentralized Sportsbet finished the ICO of its token in some seconds. Most of them have been bought by a Chinese exchange.

SingularDTV

SingularDTV wants to merge Ethereum, smart contracts and the production and stream of videos. With the ICO the platform raised more than 12,000 BTC. Today the whole tokens are worth around 40,000 BTC.

SingularDTV wants to merge Ethereum, smart contracts and the production and stream of videos. With the ICO the platform raised more than 12,000 BTC. Today the whole tokens are worth around 40,000 BTC.

The token of above ICO can be bought and traded on exchanges. Some additional ICO has just finish some time ago and prepare to release the newly created token on the Ethereum Blockchain. This are the following projects:

Melonport

Like Iconomi Melonport aims to develop a platform for the management of blockchain assets built upon Ethereum. The MLN token the developers sold will be needed to use the platform and have been sold or more than 2,000 BTC few month ago.

Qtum

This project wants to build a platform for the easy creation and use of blockchain based smart contracts. For this mission, it could raise more than 14,000 Bitcoin in an ICO.

Chrono Bank

The “uber of recruitment” intends to build a platform with its own currency for freelance projects. They sold 710,000 tokens for more than 4,000 Bitcoin.

Dfinity

Similar to Golem, Dfinity wants to build a decentralized platform for cloud computing. In its ICO it raised more than 3,000 Bitcoin.

BlockPay With “only” about 1,000

With “only” about 1,000 Bitcoin the ICO of BlockPay was one of the smaller ICOs. BlockPay is a startup building a payment processor for several cryptocurrencies.

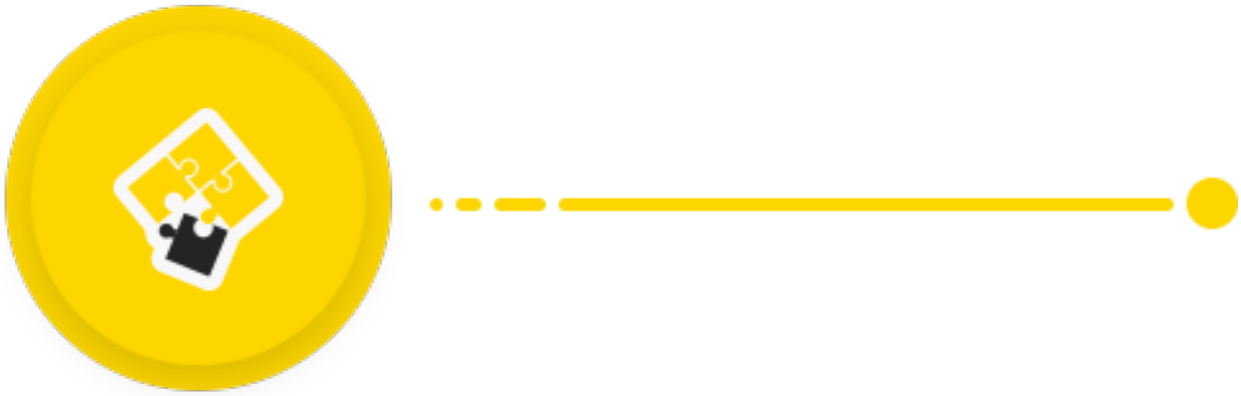
With “only” about 1,000 Bitcoin the ICO of BlockPay was one of the smaller ICOs. BlockPay is a startup building a payment processor for several cryptocurrencies.

This is are just examples. There are hundreds of further more or less successful ICO.

Space KG

ROADMAP

'Hell, there are no rules here - we're trying to accomplish something.' By Thomas Edison



Q1 - Q2 2018

Complete the ICO, based on the resources define a global marketing plan

Q2 - Q3 2018

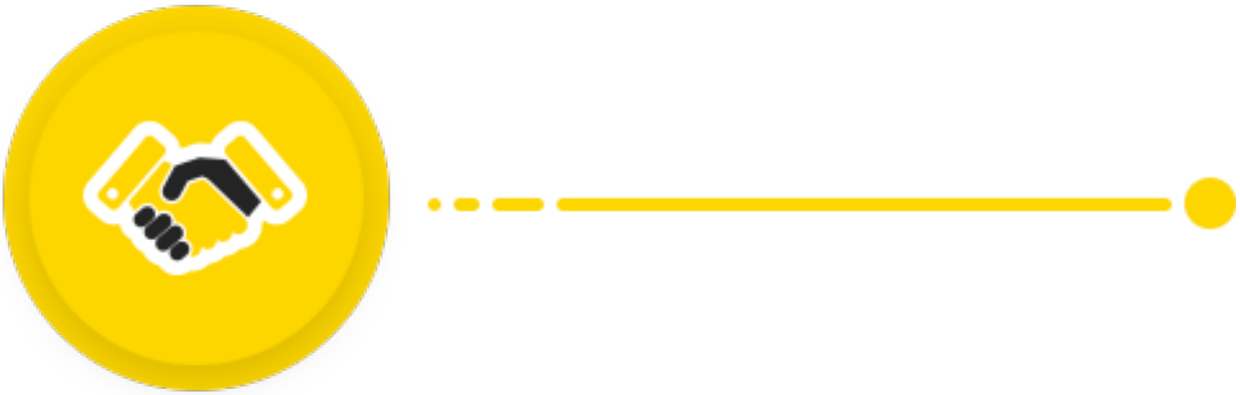
Exchange listing and key scientists recruitment into the project

Q3 - Q4 2018

Launch the first test in a small scale of a carbon nanotubes design that can be later be up-scaled to the real space elevator

Q1 - Q2 2019

Further marketing and involvement of promoters, at this point we could already expect the SKG to start appreciating significantly.



Q3 - Q4 2019

With the huge financial resources available we will attract further brilliant engineers into the project.

We will also be able to negotiate the shipment of the nanotube tether into space

Q1 - Q2 2020

The space elevator construction starts:

- On Earth, probably offshore Equador
- In Space, sending the tether with our contractor space company

At this point we will expect the SKG to be around 100$ – 200$

HOW IT WORKS

1 skg = 1 kg lifted into space via the space elevator, considering current price of sending 1 kg weight into space is around 20000$ using a space elevator the cost will be between 100$ to 200$, this will strongly appreciate the price of the skg in the long term.

ICO details:

Feb 9 – 16 Pre-Ico unsold will go to the next stage

Mar 9 – 16 Stage 1 unsold will go to the next stage

Apr 9 – 16 Stage 2 unsold will go to the next stage

May 9 – 16 Stage 3 unsold will be destroyed

Jun – Jul Exchange listing

Exchange listing:

1 SKG = 0,2 $

1 Eth = 5000 skg

Coin Stages

- PreIco supply 100m – 0.1 Eth = 1000 skg
- Stage 1 supply 100m – 0.1 Eth = 750 skg
- Stage 2 supply 100m – 0.1 eth = 600 skg
- Stage 3 supply 200m – 0.1 eth = 500 skg

Total on sale 500m skg

Total supply 1 billion skg

Why Should I invest in SpaceKG today?

Short-term and long-term benefits

Early investors will benefit from joining the crowdfunding because the skg will double its value towards Ether in 5 months. Once the skg will be on the exchanges, the global interest will further push the value up to unforeseen levels, this will benefit long term investors as well.

The Vision

A space elevator is the only unrivaled way to build spaceships, mine satellites and really access what our universe has to offer. An ICO is a perfect opportunity to start something that will be built in the nearest future, considering the newest material technology breakthroughs, advancements in robotics and the coming fusion nuclear power.

By investing in this project and sharing it, you are:

1. Raising the awareness around private investments in cost effective space exploration.
2. Securing an asset that will be easy tradeable and increasing in value in the future.

Visit our shop now and take part of this revolution!
https://spacekg.net/shop/

Be aware that at the moment it's only possible to buy with Ether, the minimum contribution is the equivalent of 100$.