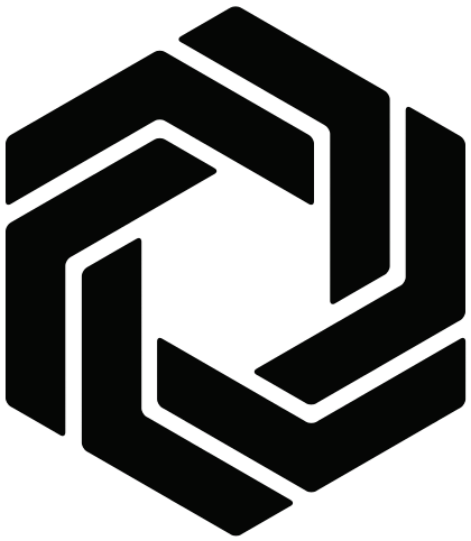

HEXXCOIN

WHITEPAPER v1.1

Published April 15, 2018

Index

Welcome to the future: Introducing Cryptocurrencies

Since the internet boom of the mid 90s, an ever-growing number of people have taken to the internet to do their shopping. Emerging online retail companies have tempted consumers with a variety of products that virtually no physical stores could rival. Cutting middle-men has allowed nascent companies like eBay and Amazon to offer a spectacular range of products for bargain prices and survive the dot-com bubble to become household names today.

Pioneer companies like PayPal tried to offer an alternative payment option to debit cards and were largely successful. Technically, their transactions are *central*, meaning that they are all stored in one central database at the headquarters. If a transaction is verified by that one database, it is genuine, otherwise, it is not.

As time progressed, this model of payment was heavily questioned. Did there really have to be a central database to the transactions? Why couldn't people simply send each other money without the need for a single authoritative party to verify all transactions?

For a long time the idea of a system that allows monetary transactions to proceed without a central authority was the holy grail of free banking and a mere dream in the minds of nerds and computer geeks. Everybody wished for it to happen and almost everybody thought it was impossible.

Until one mysterious Satoshi Nakamoto entered the stage…

Nobody knows who he is, where he is from, whether he is still alive or not or if he is a single person or a group of people. Yet everybody knows what he has done.

Satoshi invented an ingenious system where a network of users, none of them acting as a centre of authority, could verify transactions with each other. How did he do the unthinkable? Well, the basic concept behind his invention is rather simple; remember the old days when teens downloaded pirated mp3s using Napster? Well, Satoshi's invention works pretty much the same, except that the users are sharing records of monetary transactions instead of Hit me baby one more time!

The blockchain works on a network of computers that share records of transactions. In return for using their internet bandwidth, time, effort, and electricity, these computers receive rewards in the same currency. Those who run those computers are called **miners**. Back in 2010 the average Joe could mine bitcoins on his Pentium desktop, but nowadays mining has become so difficult that only mining farms utilizing specific hardware (ASIC) can get any serious reward out of it.

Since its early days, bitcoin and its underlying blockchain technology were regarded with much apprehension and scepticism. In late 2011 WIRED magazine published an obituary article (https://www.wired.com/2011/11/mf_bitcoin/) wailing the presumed "demise" of the currency, which at the time was down to $2.4 from its June high of $28.9. A laughing stock today, a lot of people took it seriously at the time. After all, bitcoin was 83% down in merely five months.

Today, longer transaction times and higher transaction costs make a lot of people doubt the future of bitcoin as a currency, yet no matter what happens to bitcoin, the blockchain technology will ultimately triumph, above all because it *employs technology towards freedom and liberation*. We might regress for a moment to discuss this last motif.

Since its publication almost 70 years ago, George Orwell's 1984 has become a beloved classic, even resurging to the ranks of bestsellers in 2017. The novel, as it is well-know, revolves around the "big brother" of the government using technology to spy on and control his loyal subjects. It is a terrifying vision and one that has a wide audience who take it for granted, yet there are those who realize that the opposite is actually true. In his book *Our Posthuman Future*, Francis Fukuyama, a prominent political scientist, discussed how technology was actually turned against the big brother, allowing laymen to watch their governments.

> "The political predictions of … 1984 were entirely wrong. The year 1984 came and went, with the United States still locked in a Cold War struggle with the Soviet Union. That year saw the introduction of a new model of the IBM personal computer and the beginning of what became the PC revolution … the personal computer, linked to the Internet, was in fact the realization of Orwell's telescreen. But instead of becoming an instrument of centralization and tyranny, it led to just the opposite: the democratization of access to information and the decentralization of politics. Instead of the Big Brother watching everyone, people could use the PC and Internet to watch Big Brother."

Francis Fukuyama, *Our Posthuman Future*, page 4

Fukuyama's vision is made more meaningful today after various protests in the world, particularly the revolutions of the Arab spring of 2011, were first ignited by guerrilla activists who used mobile cameras and social networks to document and expose regime brutality in ways that were entirely impossible a mere couple of decades earlier. A simple research on the limitations imposed on communication in totalitarian countries clearly proves Fukuyama's point; technology wasn't the ally of the big brother after all.

If we are to apply this to the blockchain technology, we will realize that it ultimately derives its power from its ability to fit perfectly in the zeitgeist of the moment: the greater movement to employ technology towards freedom and decentralization. This is why cryptocurrencies have returned stronger time after time, regardless of how fiercely they were sabotaged by governments or bankers, and this is precisely why they will ultimately triumph.

Obviously, a major component to freedom is anonymity, and Bitcoin does indeed deliver some pseudoanonymous features; funds are not tied to individuals but rather to addresses on the blockchain and users are allowed to create as many of these as they wish to further obfuscate their transactions.

Alas, all user activity is available on the blockchain for public access. By analysing where transactions originate from and where they are destined, along with the transaction amounts, any individual with access to the blockchain records can trace all bitcoin transactions…
Bitcoin had done the unthinkable in terms of decentralizing payments and disrupting traditional banking, yet it fell short of delivering the ultimate goal for which it was created. It offered very little privacy.

Perfecting the awesome: Addressing privacy issues

Over the few years since the advent of bitcoin (which is still an eternity in the turbulent timescale of cryptocurrency) various approaches were developed to address the privacy issue, each more refined and sophisticated than its predecessor. We are here to offer a very basic outline of these approaches along with their strengths and shortcomings.

Transaction mixers

Imagine John wants to pay Michael $100 but doesn't want anybody to know about it. So he gives the money to a third person, Sam, and asks him to send the money to Michael. You can't trace this, because Sam is doing this for everybody. So all day long he is collecting payments and sending payments and you don't know who is paying who. Transaction mixers work in exactly in this way. They act as add-ons to bitcoin (coinmixer.se/en/)

Shortcomings:

- One way to expose transaction mixers is to trace the transaction through the amount. If John paid Sam $328 then you can trace who received $328 from Sam and realize this is the person receiving John's payment.
- Another issue is that you must rely on the mixer to deliver your payment. In other words, the mixer can receive the payment and give nothing back. The payment simply gets stolen.
- An even bigger concern is if the mixer is maliciously keeping records of the transactions, with the intention of releasing the information to third parties.
- If the mixer has a low volume of transactions, a network graph analysis can still expose transactions.

Ring signatures (ex. Monero)

Another improvement on transaction mixers is using decoy (fake) transactions alongside with real transaction inputs. This further complicates things and makes it difficult for a third party to differentiate real inputs from decoy ones. A further elaboration on this technique is to hide the amount of money sent as well as using decoy inputs. This technique is called Ring confidential signatures.

Shortcomings:

- All the decoy inputs are encrypted in the same way as real inputs, thus resulting in more power use, more processing load on the hardware, and too much unnecessary data. All this leads to the bloating of the blockchain and to increasing the fees of transactions.

- These transactions can still be exposed by analysing the time when the transaction is submitted and thus link it to the identities of the sender and the recipient.

ZK-Snarks (ex. Zcash)

This technology allows private transactions to be optional, thus preventing a lot of the disadvantages discussed above. All private transactions get into a private transaction set, and in order to spend a transaction from this set, the sender should provide a cryptographical proof that his transaction does indeed exist in the set (but without revealing which one.) This makes it impossible to know which transaction of the various transactions in the set is the one being sent, and thus it becomes impossible to track it.

Those interested in knowing more technical details about ZK-snarks can benefit from revising the *Zcash Protocol Specification Paper* (https://raw.githubusercontent.com/zcash/zips/master/protocol/protocol.pdf)

Shortcomings:

- At its core, this protocol relies on a trusted setup to choose the initial protocol parameters, and any individual who possesses these parameters can view all private transactions and, more catastrophically, can counterfeit as many coins as they wish without outsider observers noticing the least suspicious of activities. In other words, the ZK-snarks system is entirely built upon trusting the developers and if one of these turns out to be a betraying Judas, then the currency will catastrophically fail.

Zerocoin protocol (ex. HEXX)

This protocol was first proposed by Dr. Matthew Green et al with the intention of creating cryptocurrencies with true cryptographic anonymity. It functions in a similar way to the ZK-snarks protocol: private transactions are optional to prevent bloating of the blockchain and there is also a private transaction set where private transactions are accumulated. The major difference is that, instead of relying on a trusted setup of parameters known to a number of people (who can later ruin things if they are not trustworthy), the Zerocoin protocol uses parameters from the RSA factoring challenge (RSA-2048 in the case of HEXX). Back in March 1991, two big prime numbers were chosen at random, multiplied together, and then destroyed. The participants of the challenge were then asked to retrieve the original prime numbers for a reward. Not only did the participants fail in their quest, but nobody has figured what these numbers were till this very day! So unless some quantum computer can somehow factor these numbers, your zerocoin transactions are perfectly anonymous.
Note: The HEXXCOIN team is aware of the zerobug which has affected various Zerocoin currencies. We would like to emphasise that the team is currently in possession of a solution to this bug and that we have the technology that allows HEXX's transactions to be anonymous while fully functional.

Reading material on Zerocoin protocol:
http://spar.isi.jhu.edu/~mgreen/ZerocoinOakland.pdf
https://en.wikipedia.org/wiki/RSA_Factoring_Challenge

HEXXCOIN: From a bumpy start to a promising future

HEXXCOIN started in early 2015 as a fork from another coin, Crave. The project was short lived, with the original developer at that time quickly abandoning the project. Two years later, a new developer decided to revive the coin and issued a swap where HEXXCOIN was updated to a Zcoin fork. Alas, this initiative was also short lived, with the developer abandoning the project few months after the swap.

Finally, around January 2018, the current team was formed and took HEXXCOIN over. Ever since, the team has expanded and HEXXCOIN has reached new heights not remotely rivalled at any earlier stage of its existence.

So despite its painful labour, HEXXCOIN is well on its way to become the next breakthrough in privacy coins. Surprisingly, this bumpy start has led to a very pleasant consequence; two cycles of revival and abandonment have resulted in tens of thousands of coins becoming permanently inactive and probably forever lost – together, they make a very large proportion of a coin whose current circulating supply is merely over one and a half million coins. Remember all those stories of people trashing hard drives containing thousands of bitcoins back when it was worth 30 cents? Well, this was the case with HEXX, except that it happened on a much larger scale!

This can be easily verified by visiting the rich list on the HEXXCOIN blockchain explorer (https://chainz.cryptoid.info/hxx/#!rich) and checking the tens of thousands of coins that were not touched in over a year. It's important to notice that HEXX was trading for roughly 1-2% of its current price when these addresses were last accessed, which makes it extremely unlikely someone is resisting even a partial sale at this insane profit.

The nerdy stuff: HEXXCOIN in technical details

Name: HEXXCOIN (HEXX)
Symbol: HXX
Algorithm: Lyra2z330 (POW – ASIC/GPU resistant)
LYRA2(BEGIN(thash),32,BEGIN(nVersion),80, BEGIN(nVersion),80,2,330,256)
Block time: 2.5 minutes (four times faster than Bitcoin)
Block size: 4mb
Difficulty retarget function: BRNDF
HEXXCOIN uses a faster block time than Bitcoin. On average there are only 2.5 minutes between blocks. This means faster confirmation time for your transactions, and also 4 times higher network transaction capacity. As a result, no more insane transaction fees or long wait times for your payments.

HEXXCOIN is exclusively mineable on CPU to to allow for a fair mining opportunity to everyone and not only to professional miners who possess expensive GPU and ASIC hardware. Difficulty

retarget occurs every block which makes the network stable by preventing any sudden fluctuations of the network hashing speed.

The current circulating supply at the moment (April 2018) slightly above 1,580,000 coins and the maximum supply is 9,999,999 HEXXCOINS. HEXXCOIN has a very small inflation rate, at which the maximum supply will be reached in about twenty years.

Every block (2.5 mintues), two HEXXCOINS are issued and are distributed in the following fashion:

- 0.7 HEXXCOIN is distributed amongst miners
- 0.7 HEXXCOIN is distributed amongst Xnode owners
- 0.6 HEXXCOIN for community funds and nodes. These funds are reserved for development, exchange listings and marketing. They are only accessed after the democratic voting of members. As the value of HEXXCOIN grows, the fouds will become more significant and will allow more significant marketing action and exchange listings.

Note: In about two years, the block reward for community fee will be removed and instead awarded for stacking. In other words, in two years HEXXCOIN will have mining, Xnodes and stacking all in the same time.

The community also allows holders of HEXXCOIN to setup **Xnodes** which add transparency, security and speed to the HEXXCOIN network. In return for their efforts, Xnode owners generate passive income in the form of HEXX rewards. Currently, an Xnode can be setup for 2000 HEXX. All Xnodes combined generate 403.2 HXX per day which are distributed equally amongst Xnodes. Thus the number of HXX rewards per node depends on the number of Xnodes in the network. Technical assistance and elaborate guides to create Xnodes can be found in our discord page.

The way ahead: Our roadmap

Q1 2018

- Community takeover ✓
- New team extended by accepting new members ✓
- Core update ✓ (Hard fork successfully took place on 1st of March 2018)
- Establishing a network of Xnodes ✓ (Established and currently running)
- Coin funding system ✓ (Established)

Q2 2018

- New exchange listings ✓ (listed on CryptoBridge, more exchanges to come)
- Cloud CPU mining
- Cloud Xnode services
- Mobile Wallet
- GUI update

Q3 2018

- Core update 16.x
- Lite Wallet
- POS hybrid implement starts
- **Fork with Bitcoin to produce BitcoinZeroX (see below)**

Q4 2018

- Xnode code update

Q1 2019

- Improved budget system
- Using supernodes community integration (voting system)

Bitcoin on anonymity steroids: Enter BitcoinZeroX (BZX)

As mentioned in the roadmap, the community is glad to announce that HEXXCOIN will be used to extend the functionality of bitcoin by offering it Zerocoin anonymity. The fork between HEXXCOIN and Bitcoin will occur in Q3 2018 to result in the unique coin BitcoinZeroX (BZX)

BitcoinZeroX will be awarded to Bitcoin and HEXXCOIN holders at a ratio of 1:1. i.e you get 1 BZX for every HEXX or for every BTC that you own. BitcoinZeroX will be superior to Bitcoin private in terms of anonymity because it is based on the zerocoin protocol and not the ZK-snarks protocol as explained above.

BitcoinZeroX will also have masternodes and will be a project of its own with its own Whitepaper that will be released in due time. We are aware of the way similar forks have proceeded and of the sharp decline of the price of other coins following such forks. The HEXXCOIN community would like to assure you that the development of HEXX will continue with all due care after the

fork has proceeded and that we have prepared a number of measures to limit any major sell-offs of HEXX after the fork. (Passing hint: Bitcoin is not the only currency that can benefit from a zerocoin security fork!)

The geeks behind the coin: meet our team

HEXXCOIN is a community project run by a team of developers and enthusiasts using a democratic voting system. We believe that cryptocurrencies as a decentralized form of currency should not be managed by a monolithic organization. We are NOT a company!

[Dev007] began the revival of the Hexx Project in January 2018, after it was abandoned by previous developers. He is now the lead developer and applies the experience he has gained and adopted from other successful crypto projects to persist with improving the anonymity and development of Hexxcoin for the foreseeable future.

Albin D. [Shiki0] is a Slovenian core team developer, IoT enthusiast and CPU miner with schooling background of computer electrician and informatics engineering. A typical geek, he can't resist the urge to tinker with anything electronic and see how stuff works. He listens to trance music, enjoys hiking and mountain climbing, and loves to watch the reactions of his Croatian Shepard Gara when they sit together to watch horror movies!

Felix Brucker is a German developer who holds a bachelor in computer science from Hochschule Darmstadt and is currently preparing for his master's degree. He bought his first HEXXCOINS during the April 2017 swap and has HODL'd his coins for over eight months of inactivity (we're talking Warren Buffet patience here!) Ever since the community takeover, he has joined the new team and has made his presence noticed on Github. He is a cat lover who is yet to own one. He likes listening to electronic music and watching sci-fi movies.

Ron W. [DevCon] is a Dutch developer based in Amsterdam (legal weed!) who specializes in web and application development, internet security and work on blockchain technology on a daily basis. He likes to listen to techno and enjoys Japanese food when he takes a break from coding in python, javascript, React and CSS3/SASS. He has been involved in HEXXCOIN since February 2018 and can be easily recognized by the massive spider tattoo on his neck.

[nwo99] is an Australian citizen of middle eastern background. An amateur writer, he contributes guides and written material to the HEXX community. He also likes to show off his Arabic and Italian skills in the international Discord support pages. When he is not moderating forums and debating trolls, he listens to metal and watches vintage wrestling (hence his handle).

[IndominusHexxx] currently has 5 years' experience with a Fortune 500 company, 12 years total experience in Marketing and is studying for a Master's Degree in Business/Marketing. When he has time left over in the day before the evening mea he can be found battling in the trenches of crypto economies, although he has long ago given up explaining what "a bitcoin" is at the dinner

table. He is a frequent international flyer and enjoys people watching and finding time for happiness in his life.

[josephx] is an Australian cryptocurrency enthusiast, privacy advocate and Brand Designer for creative and emerging technologies and has worked across multiple cryptocurrency projects to translate complex concepts to a broad audience. JosephX also develops cryptocurrency Bounty systems to encourage community growth and team participation. When not kerning fonts or handling arc tools, JosephX can be found at local meetups or reading Antonopoulos old- school; like in a “book”.

Kirk Y. Oropel [Azul] is a crypto-trader and experienced Marketer, specialising in privacy and VPN applications and working in Distribution for the past 4 years. Azul joined Hexx in February 2018 and has been a strategist for community growth through Social Media Marketing. When he isn’t expanding markets, you can find him helping run the Iloilo Crypto Community in the Philippines.