skeincoin

REBOOT BLUEPAPER 1.14gfx

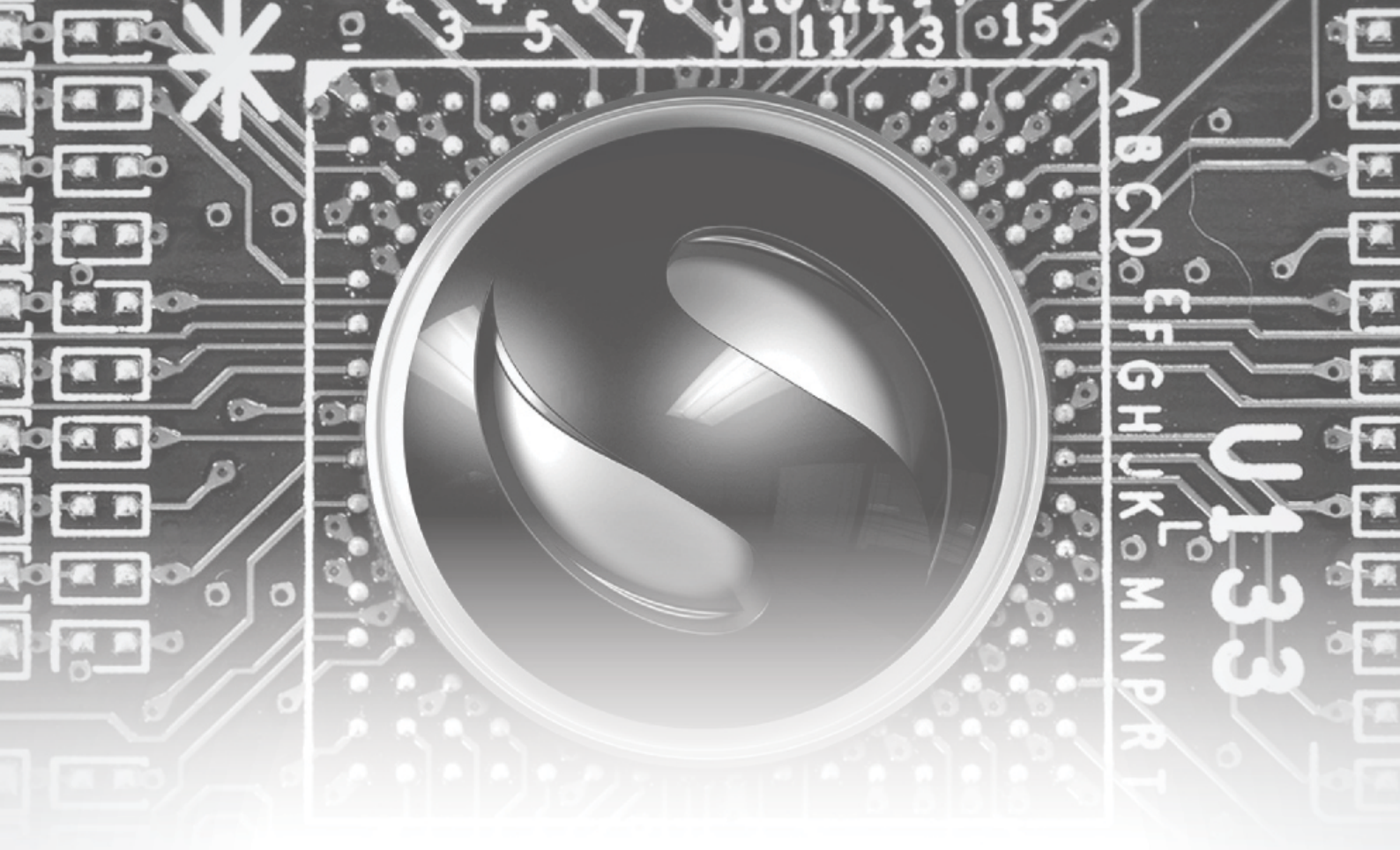
THE SKEINCOIN DEVELOPERS

APRIL 24th, 2018

Abstract

Skeincoin is a peer-to-peer version of digital assets maintaining a consensus mechanism based on the SHA3 hashing candidate Skein. Skeincoin has a fast blocktime, which results in faster transaction time and uses a flexible and energy efficient hashing. By following Bitcoin's development all technical features developed for the Bitcoin network are introduced in the Skeincoin network, resulting in almost instant transactions with ultra low costs. The original team merged with new members to form the Skeincoin foundation and reboot Skeincoin, continue the development and take the next steps to utilize Skeincoin's potential. The Skeincoin foundation is now developing the blockchain ecosystem whilst the newly formed legal entity, Skeincoin Ltd -registered at Belarus' High Tech Crypto Park in Minsk - holds responsibility for business planning and contracts.

Index



1 Technical Overview

Developed in 2013 by Red Kendra, Skeincoin is comparable with Bitcoin and can use all of Bitcoin's developments without going through miner wars and forks. Skeincoin uses a different hashing algorithm for the first hashing round called Skein, which makes it easier to mine and more adaptable to different hardware. Furthermore Skeincoin has a faster blocktarget, resulting in a faster transaction process rate. For the second PoW hashing round Skeincoin uses SHA-256[1]. The blockchain is fast, cost efficient and flexible and thus well suited to be integrated into (micro-)payment applications and markets.

"Skein is fast. Skein-512—our primary proposal—hashes data at 6.1 clock cycles per byte on a 64-bit CPU. This means that on a 3.1 GHz x64 Core 2 Duo CPU, Skein hashes data at 500 MBytes/second per core—almost twice as fast as SHA-512 and three times faster than SHA-256. [...] Skein is efficient on a variety of platforms, both hardware and software. Skein-512 can be implemented in about 200 bytes of state. Small devices, such as 8-bit smart cards, can implement Skein-256 using about 100 bytes of memory."

(Bruce Schneider)[4]

1.1 Skein Hashing

SKEIN is a crypto hash algorithm developed by Bruce Schneier, Niels Ferguson et al[2]. It was one of the finalists in the NIST hashing competition to determine the new SHA-3 secure hashing standard, which is the update to the SHA-2. The winner of the contest for the update was a hash called Keccak. In short: SHA-3 is a standardized version of the Keccak hashing function. The other four final candidates from the new generation of hash functions were: BLAKE, Grøstl, JH - and Skein.

Skein is based on Threefish block cipher, compressing it with a variation of Matyas-Meyer-Oseas hash mode. The name reflects the way Skein alters the plaintext input, using an interwoven form of mixing and permutation, similar to a skein of yarn:

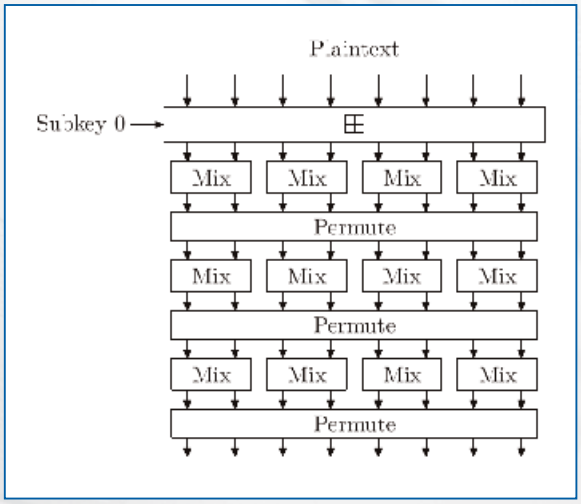


Figure 1: Skein hashing function

Even small alterations to plaintext input, result in an avalanche effect thanks to the interwoven pattern of permutations. Taking the standard text phrase of the “quick brown fox” as an example, just adding a period to the end of the plaintext input changes the result in all parts, making Skein not only fast but also secure:

Skein("The quick brown fox jumps over the lazy dog")
results in:
0xb3250457e05d3060b1a4bbc1428bc75a3f525ca389aeab96cfa34638d96e492a
Skein("The quick brown fox jumps over the lazy dog.")
results in:
0x41e829d7fca71c7d7154ed8fc8a069f274dd664ae0ed29d365d919f4e575eebb

After some partly successful attacks were published, the development team tweaked the hash function further while claiming, that the original would have been able to withstand the attack anyway.[3]

The difference to SHA-2 hashing

Bitcoin is still using the old SHA-2 in the 256bit version (SHA-256). Skein is one of the hash functions from the next generation - 10 years newer than Bitcoin's SHA2 hash. While Bitcoin has to use the limited SHA-256, Skeincoin is using the much more flexible and faster Skein hash.

Skein can further be implemented very efficiently on most hardware (in the order of 6 clock cycles per byte even on older Intel CPUs) as well as into smart cards, which opens up new possibilities for integration.

1.2 Differences to Bitcoin, Litecoin and ERC20 Tokens

While Bitcoin maintains a 10 minute blocktarget (Proof of Work targetspacing), Skeincoin maintains a lower target of 120 seconds. This provides a much higher throughput, while keeping the blocksize equal to Bitcoins. Further there are some small changes in emitionrate: The first 100 blocks of the Skeincoin network rewarded 0.0001 SKC, while the blocks after those rewarded 32 SKC. Like the Bitcoin network, Skeincoin will only have 32 halving events. But in Skeincoin the subsidy halving interval is set to 262800 blocks creating a total coin supply of:

$$\sum_{i=0}^{32} 262800 \left[\frac{32}{2^i} \right] - 100 \times 32 + 0.0001 \times 99 = 16816000.0099 SKC$$

By maintaining only relatively specific codechanges compared to the Bitcoin Core software we were able to take advantage of current Bitcoin developments, such as Lightning or Bulletproofs, creating a solid baselayer for micropayment-integrations both in- and outside the industry.

Similarity to Litecoin?

Litecoin was introduced as an answer to Bitcoin, claiming to be more open to the community, as not only miners with special equipment can contribute to the mining and decision processes within the community. Litecoin approached the hashing with an ASIC hostile algorithm, resulting in the mining by millions of users using their desktop GPU in mining pools instead of expensive ASICs setups available only to a few. Skeincoin opens up the process by allowing all methods of mining due to the high flexibility of the algorithm which results in a support of almost every hardware architecture available.

Is it a Token?

Most ICOs are selling ERC20 Tokens, which are nothing more than a sub-coin of Ethereum. All the advantages and disadvantages of the Ethereum Blockchain are part of these Tokens. When the Ethereum Chain is overcrowded by virtual cat collectors, you can't move any ERC20 Token fast from wallet to wallet and the transaction costs of all ERC20 tokens are always as high as the Ethereum transaction costs. With more and more Tokens flooding the network, they are good for many things, but not for payment systems. Skeincoin is running on it's own blockchain, without any dependency on other chains.

2 Integration of Bitcoin concepts for Skeincoin

Forked from Bitcoin, Skeincoin can adapt all of Bitcoin's features. One of the world fastest progressing open source projects is our development kit. Activation of softforks is easy, as the community is available and strung together. The result is fast progress and the possibility of integrating and adapting concepts, that are developed for Bitcoin but can't be activated on the Bitcoin-Blockchain simple because miners aren't agreeing on the path Bitcoin has to take and on steps that are necessary. Concentrating on the concepts which are important for micro-payments and usability the development will ensure that end-users and companies alike can safely and easily use Skeincoin for their specific needs.

2.1 CSV

With the wallet upgrade to v12.1 Skeincoin already activated the BIP112 CSV softfork. With CSV timelock micro-contracts are activated in the blockchain, supporting important features for micropayments and shop integration[5]. The CSV function allows users e.g. to make timed contracts with 2-out-of-3 signatures. This allows the sending of Skeincoin with an escrow as middleman (which could be a trust-service company for shops). After the contract timed out the receiver has full control over the values, until then the escrow can undo the contract with either of the parties. This is important as it allows secure shop transactions without the need to step in for the trust-service as long as none of the business partners flags an uncooperative behavior. The moment the timer runs out the contract triggers the broadcasting of the transactions and it gets written into the blockchain.

2.2 Atomic Swaps

Atomic swaps open up the possibility to exchange coins and values from one blockchain to another. The result for the users is that they can e.g. exchange Skeincoins to Bitcoins inside their wallet without the need to transfer their coins to an exchange, with all the risks and difficulties. For companies using Skeincoin as micro-payments this cross-chain trading makes it easier to do on the fly transactions outside the Skeincoin blockchain.

The base structure for atomic swaps are smart contracts taking place on two blockchains at once or not at all, which is called atomicity. While user A transfers SKC to user B's wallet this transfer X has a smart contract not broadcasting to the blockchain until another transfer Y on e.g. the Bitcoin blockchain is taking place. This transfer Y is a transfer of B's BTC to A's Bitcoin wallet. The transfer Y also has an underlying smart contract waiting for transfer X. If one of the two transfers aren't completed, the smart contracts won't broadcast the transactions[6].

With Skeincoin following Bitcoin's development, we don't have to solve the atomic swap puzzle alone but will build on the swapping infrastructure developed for Bitcoin.

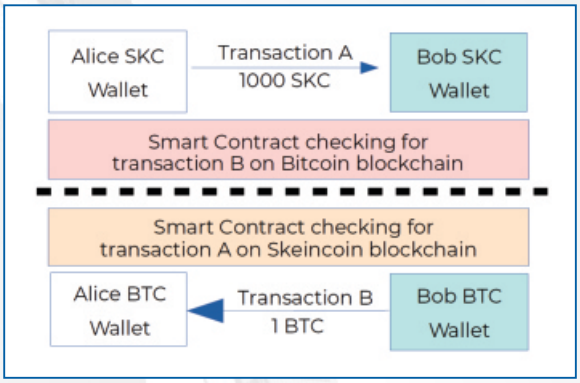


Figure 2: Atomic Swap from Alice to Bob

Atomic Future: P2P Exchange

Once included, Skeincoin will be able to integrate atomic swaps with all other blockchains capable of atomic swaps. These chains will be more or less a grand P2P exchange network, capable of trading all sorts of coins and tokens from blockchain to blockchain without exchanges or fees (apart from the transaction costs) involved. Further new emerging exchanges are trying to act as a graphic user interface for cross-blockchain trading, making P2P trading even easier.

2.3 Lightning Network

Skeincoin doesn't suffer from Bitcoin's high transaction costs, as it isn't used for the thousands of trades that are slowing down the transaction speed while driving up the costs for every transaction. When being integrated into more and more payment systems, Skeincoin could suffer the same issues, but the lightning network is an elegant solution for scaling the blockchain's network to process more movements at lower costs and higher speeds. With an active lightning network micropayments can be signed by a sighash, moving values between untrusted parties by contracts which enforce the payments if one of the contractors is uncooperative or hostile through broadcasting the payment after a series of timelocks[7]. For Skeincoin, even while not needing lightning as urgent as Bitcoin, the effect of implanting it will be thousands of transactions per second with costs as low as 0.0001 $ per transaction. Even nanopayments will be possible without significant transaction costs or the problem that they would slow down the network. As soon as the network is ready, it will be implemented into Skeincoin.

2.4 Privacy features with zkSNARKs / Bulletproofs / Schnorr / CoinJoin

Privacy features for keeping the user or customers transaction data under control are possible for Skeincoin using zkSNARKs/zk-STARKs, Bulletproofs or Schnorr+CoinJoin. Without privacy features Bitcoin and therefore Skeincoin allows everyone to trace back a transaction in both directions, with the account's balances visible as well as all other transactions from and to known accounts:

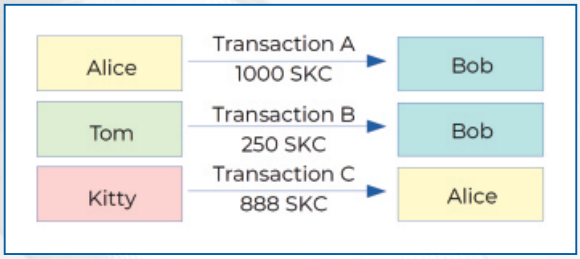


Figure 3: Blockchain transfer without privacy features

zkSNARKs is already being used in ZCASH[8] and thus can be called a working system with some small problems, that zk-STARKs[9] tries to eliminate. With ZCASH being a bitcoin fork, zkSNARKs or its successors could be implemented into Skeincoin as well. This zero knowledge system allows users to send transactions and the network to confirm them, without other users being able to see or find out how much value was transferred by whom to whom. The zkS-protocolls allow confirming if the transaction has taken place without anyone being able to trace back anything from outside[10].

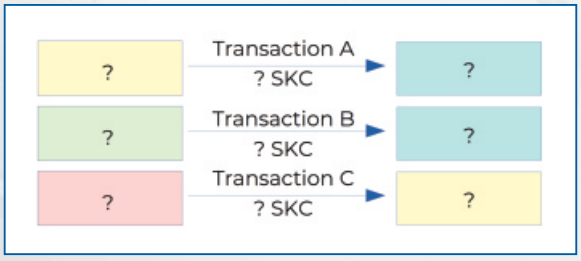


Figure 4: Blockchain transfer with zkSNARKs

Bulletproofs are a new concept developed at Stanford University for keeping the amount within transactions concealed while keeping the traceability of transactions[11]. The main advantages for implementing Bulletproofs are that it's easier to adapt than all other concepts and that the traceability is something that many users like about cryptocoins. Bulletproofs deliver a good balance of anonymity vs trust vs complexity.

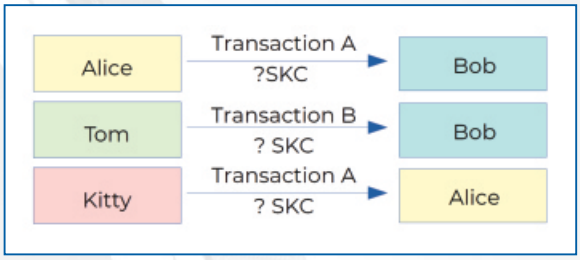


Figure 5: Hidden transaction values with Bulletproofs

Schnorr is building on SegWit and tries to solve a part of the scalability problem in blockchains and has the privacy as a side effect. By mashing up different transactions Schnorr is saving space in the chain blocks and can end up producing transactions with partly concealed values[12]. Privacy isn't a constant effect of Schnorr, so it can't be used alone to produce private transactions. Building on Schnorr CoinJoin mechanisms could be used to mix up two transactions when every a private transaction is asked for, resulting in a privacy-on-demand effect[13].

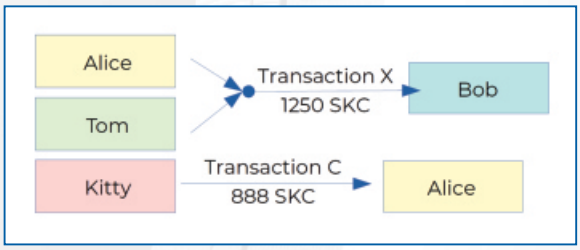


Figure 6: Schnorr transaction with combined transaction to Bob

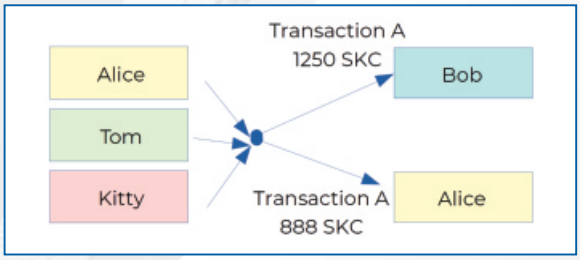


Figure 7: Combined partly-private transactions with CoinJoin

Which feature(s) will be used is up for discussion with the community with usability and reliability as the main arguments apart from the time needed to implement them.

3 The Skeincoin Ltd. Company

The Skeincoin Ltd. Company, registered in the High Technology Park (HTP) in Minsk[14], Belarus, ensures that buying and selling crypto is legal for companies using the Skeincoin blockchain and that the Skeincoin development team can work within legal regulations and without bans.

3.1 Goals

The key function of Skeincoin Ltd. is to act as a legal entity for negotiations for itself and on behalf of the Skeincoin Foundation. Skeincoin Ltd. will act as partner for businesses and as employer. The company will work for its own success while supporting the Skeincoin Foundation in the development of the Skeincoin ecosystem.

3.2 Belarus Crypto Laws

From the end of March 2018, the 'Decree No. 8', signed on December 21th, will change the crypto world. Starting in the High Tech Park in Minsk Belarus will legalize most of the normal crypto-structures and instruments: ICOs, transactions of crypto-coins, mining, exchanges, smart contracts, exchanging crypto into fiat and more[15]. All that tax free for the next five years and supported by an excellent international IT ecosystem in the HTP. In order to make ventures safer for overseas investors, English law will be used for specific activities in the HTP. Whilst some countries consider harsh regulation, others, such as Japan and South Korea, sway between opening and restricting domestic markets. In contrast, Belarus has made significant progress in viable regulation, including the alignment of smart contracts with the local legislative framework - a feat unmatched in any other crypto-progressive nation and seen as a big deal by jurists[16].

3.3 Structure

The Structure of Skeincoin Ltd. is a classic business structure. CEO and COO leading the board, followed by CTO, CFO and various specialized positions working in teams. Andrei Kisarin is the registered CEO in the Minsk HTP and responsible of all local needs for the company. The Skeincoin Foundation is working closely with the company and certain decisions important for both the company and the foundation are made preferably with the highest possible consent from both boards. The members of both organizations come together on a regular schedule to discuss urgent items and the next steps in union.

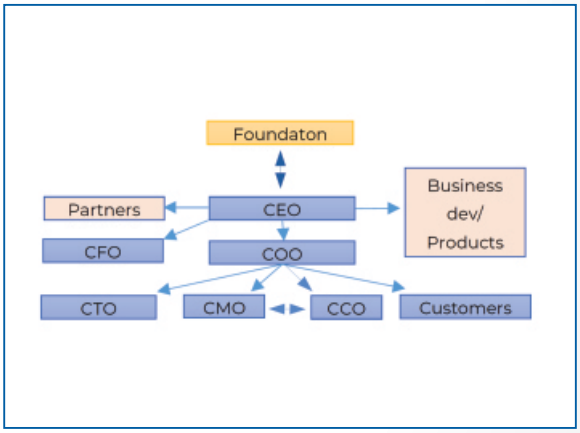


Figure 8: OrgChart of Skeincoin Ltd

3.4 Skeincoin Marketplace

With cryptotrading made legal in Belarus, Skeincoin Ltd can open up a marketplace or other business trading items, coins and other values with Skeincoin on a legal basis. This marketplace can be used as entry point into the global crypto marked. An exchange for other cryptos and alts is possible.

4 Skeincoin Foundation

To complete and amplify the impact of Skeincoin and the Skeincoin company a foundation was set up. The Skeincoin Foundation is responsible for the development, promotion and the community.

4.1 Charter

The Foundation's goal is to develop Skeincoin ecosystem - to improve the coin, its wallet and blockchain, its usability, the payment system, its impact and maintain the community. The funds of the foundation will be used for the payment of developers, community care as well as promotion. The funds are to be used in a way that they can prolong the development for long term and may be frozen partly when needed to strengthen the ecosystem.

4.2 Structure

The Skeincoin Foundation has a flat five member multi-sig structure with an additional two-level security veto branch. Five voting board members are selected to control the foundation's fund spending. Two of these members are part of the company management, three are from development, community and foundation management. Two more board members are security check members without voting but with veto rights. These two are the coin founder and main developer Kendra and the initial financial benefactor of the foundation, Waley. For spending <0,1% of the funds a double agreement without rejection by other board members is sufficient. For <1% a triple agreement without rejection is needed and for big investments >1% <5% four board members have to agree without the fifth disproving. Every rejection needs another member agreeing to overturn the denial. All decisions can be stopped by a veto from one of the two security check members. To overcome the benefactor's veto a consent of all other members is needed. A veto by the developer can't be stopped. To change the charter of the foundation a consent of six members without disagreement is needed.

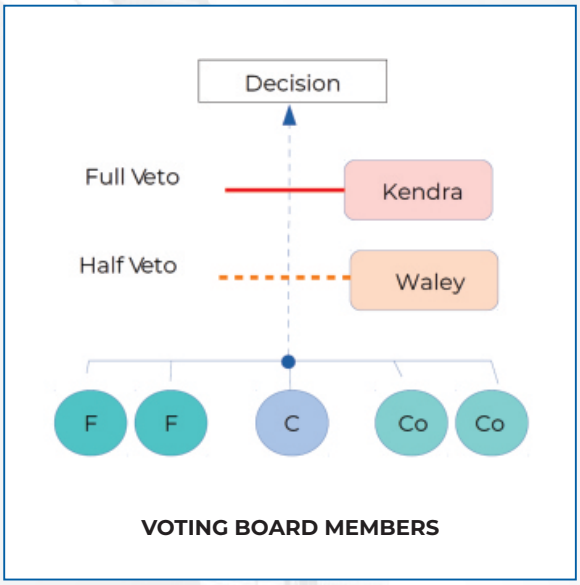


Figure 9: Foundation's decision procedure

4.3 Financial Base

The Skeincoin Foundation has been endowed with a financial base of 500.000 SKC. The companies doing business using Skeincoin are encouraged to consider supporting the foundation to keep the development stable – on a voluntary basis. Moreover, investors, developers and holders can consider contributing to speed up the development of certain aspects (e.g. through bounties) and therefore increasing the coin's ecosystem and its value.

4.4 Media

The Skeincoin Foundation is working with the community using various social media channels. The moderation of these channels is handled by the foundation or one of its board members. The foundation uses the media channels to inform the community, discuss topics, run contests or give advice. The media channels used can change according to the wishes of the community or the usability.

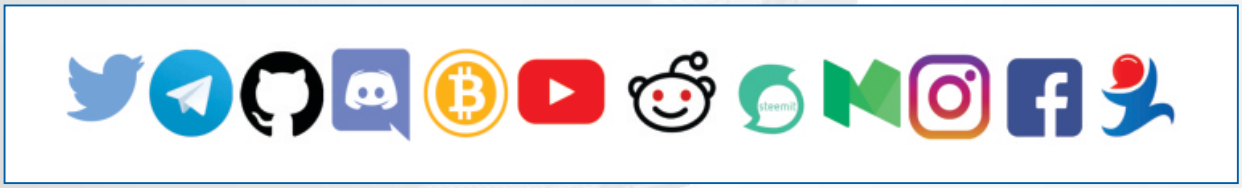


Figure 10: Social media channels used by Skeincoin foundation

5 Moving Values with Skeincoin

We are running transactions fast and with costs as low as 0.0002 SKC per kilobyte which is less than than 0,001% even for small transactions. The speed will go up about ten to hundred times with lightning and the cost will go down even more. Moving values with Skeincoin isn't limited to moving money almost instantly in form of digital assets. Rather the almost instant and ultra-low cost micro-transactions allow the transfer of all kind of values, from trading in-game items to micro-payments for crowdsourced micro-jobs. Users and companies alike will be considered with their different needs, security and usability.

5.1 Multiplatform Lightwallet

A multi-platform lightwallet will ensure that users can send and receive coins without loading a whole blockchain onto their client – the lightwallet connects to nodes instead of loading the chain. Smartphones can use the lightwallet as standalone platform while internet sites as well as games can integrate it into user accounts.

5.2 Skeinpay

Skeinpay is the payment channel for the Skeincoin ecosystem. It will be based on BTCpay, a smart solution for serverbased payment through crypto[17]. Integrating Skeinpay into webshops, apps and games will allow users to pay with Skeincoin within seconds. Skeincoin will function as a full node allowing fast, reliable and easy to connect for businesses and customers alike.

skeinpay®
YOUR CRYPTO PAYMENT SYSTEM

5.3 Skein deBIT

With the Company providing leadership and stability, Skeincoin has a strong legal substructure enabling negotiations in the debit sector to start once the ecosystem has matured. Adding a debit card to the Skeinpay system would make the usability and adoption of Skeinpay more attractive for larger companies. At the moment four players are splitting up the crypto-debit market. With the legal base of Skeincoin Ltd. we are working towards a market share of this sector.

6 The Global Market for SKC

The market and the function within this market for Skeincoin is basically the same as the market and the function for Bitcoin once was - secure, fast and low cost transfers of value via a stable and developing network. While the market for Bitcoin has evolved and resulted in multiple forks with different functions and specializations, the market for Skeincoin hasn't changed. In order to compete with the vast range of coins and tokens that flood the marked Skeincoin is aiming to support selected parts of the online world, starting with micropayments, shop integration and the gaming world. The new Bitcoin functions being introduced into Skeincoin will speed up transactions even more and will allow almost instant transactions at minimal costs. With our experienced team and our loyal community we can directly cooperate with partners. The mission of Skeincoin is to make digital assets available and easy to use for everyone, even for people without technical expertise. Anyone can start a lightwallet on his mobile, add a list of their contacts and transfer values using their names. In-game shopping online and using mobile devices will be easier with the press of one button. At the moment the Skeincoin ltd company, which represents the interests of the community on legal grounds is capable of negotiating with companies, exchanging platforms, making contracts, protocols of intent and signing bilateral agreements on joint activities.

6.1 Cryptoworld, Service, Merch

Early adopters of crypto-payments will comprise mainly of existing cryptocurrency users. Shops integrating Skeincoin first will be the ones selling crypto-service crypto-merchandise, and crypto-tech. The businesses in these sectors are open for cryptopayments, searching for reliable, fast and cost efficient structures. With our team we can help out to integrate the Skeinpay system by solving problems. Instead of having excessive network fees every time some major event disrupts the BTC market, Skeinpay costs will remain at almost zero, permanently. With the legal setup in Belarus, exchanging the coins into fiat is possible and practical.

6.2 Gamers

Apart from shop integration the second largest market for Skeincoin adoption are gaming companies and their customers. More than 600 million gamers are buying or playing online, worldwide. Thousands of games bought online, as well as add-ons and in-game item trading can be seen as open market opportunities with a yearly revenue above 13 billion dollars in 2017[18].

The item trading in MMORPGs and other guild or team based RPGs is often chaotic an unregulated. With in-game trading using blockchain technology there would be an opportunity to solve that problem. The earned coins could be traded in-game for special content sold by the game company as well as being used as entry-fee for contests and competitions. In addition to competition for rank and honor between players, there is the added value of competing for crypto-coins. With microtransactions even an overlay for all in-game activity, purchase via cryptocurrency will be viable through blockchain technologies such as lightening. By doing so the whole nature of in-game competition shifts as players are competing for digital assets with real world applications and value.

7 Past, Present and Future

The Skeincoin blockchain has been running constantly since 2013, which means it can be called one of the mature blockchains in the crypto world. Like most of the mature blockchains Skeincoin's history is full of struggle and surpassing obstacles. With the grown market banks and governments are aware of crypto assets and the struggles will continue. Having overcome many problems in the past years, we are ready for the future.

7.1 History of Development

Skeincoin was developed in late 2013 so it's a working network with an experienced team. The Skeincoin team have overcome many issues and problems over the course of Skeincoin's development. The network proved itself stable but inspite of this, the development was paused after the Mt.Gox crisis[19] as the two exchanges that traded Skeincoin both got hacked (openex[20]/atomictrade) and the whole cryptomarket was facing a steady decline. After years of inactivity the original developers restarted working on the coin. This activity, along with renewed interest in the coin attracted new team members, which brought in both new technical and business skills. With joined forces the two groups started to get the core on track with Bitcoins new features and use the coins potential. At the same time a re-branding started, new concepts emerged and the community started growing. This reboot of Skeincoin started in November 2017.

7.2 Reboot

Since the relaunch, the team has worked hard on all aspects of the Skeinworld at once - re-branding, homepage, community, publicity, development, work groups, exchanges, concepts, company, foundation. 2018 has seen a strong presence on Telegram and increased social media activity on Facebook and Twitter – meeting and informing the community about new developments and structural changes. By doing so the community is growing healthy and the team progresses at a fast pace.

7.3 Future

The relaunch of Skeincoin is still in the early stages. In few months a user base, a foundation and - with Skeincoin Ltd – a basis for legal business and contracts has been registered. Working close with the community and having an experienced, enthusiastic and innovative team we are looking forward to Skeincoin's future. SKC has a bright future and a number of practical applications in payments, micropayments and gaming world especially. We are running transactions fast and with costs as low as it gets, and lightning will make things multiple times faster. That makes SKC an ideal coin for payments. When more new ideas emerge for Bitcoin we are open adopting them and maintaining step with the Bitcoin developers. SKC has all the capabilities and advantages of being an effective, practical, growing and learning system and we are able to move and adapt fast being both practical and innovate.

References

[1] Nakamoto, Satoshi (2008) „Bitcoin: A Peer-to-Peer Electronic Cash System“ https://bitcoin.org/bitcoin.pdf

[2] Schneider, Bruce; Ferguson, Niels, et al (2010). „The Skein Hash Function Family“http://www.skein-hash.info/sites/default/files/skein1.3.pdf

[3] Schneider, Bruce (2010) „The Skein Hash Function Family“ https://www.schneier.com/academic/skein/

[4] Schneider, Bruce (2010) „The Skein Hash Function Family - NIST Round 3 Tweak Description“https://www.schneier.com/academic/paperfiles/skein-1.3-modifications.pdf

[5] https://github.com/bitcoin/bips/blob/master/bip-0112.mediawiki

[6] https://en.bitcoin.it/wiki/Atomic_cross-chain_trading

[7] Poon, Joseph; Dryja, Thaddeus (2016). „The Bitcoin Lightning Network“ http://lightning.network/lightning-network-paper.pdf

[8] Ben-Sasson, Eli; Chiesa, Alessandro; Garman, Christina; Green, Matthew; Miers, Ian; Tromer, Eran; Virza, Madars (18 May 2014). "Zerocash: Decentralized Anonymous Payments from Bitcoin"http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf

[9] Ben-Sasson, Eli; Bentov, Iddo; Horesh, Yinon; Riabzev, Michael (2018). „Scalable, transparent, and post-quantum secure computational integrity“ https://eprint.iacr.org/2018/046.pdf

[10] Reitwießner, Christian (2016). „zkSNARKs in a Nutshell“http://chriseth.github.io/notes/articles/zksnarks/zksnarks.pdf

[11] Bünz, Bendeikt; Bootle, Jonathan, Boneh, Dan et al (2018): „Bulletproofs: Short Proofs for Confidential Transactions and More“ https://eprint.iacr.org/2017/1066.pdf

[12] Maxwell, Gregory; Poelstra, Andrew; Seurin, Yannick, Wuille, Pieter (2018) „Simple Schnorr Multi-Signatures with Applications to Bitcoin“ https://eprint.iacr.org/2018/068.pdf

[13] Ruffling, Tim; Moreno-Sanchez, Pedro; Kate, Aniket (2014) „CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin“ http://crypsys.mmci.uni-saarland.de/projects/CoinShuffle/coinshuffle.pdf

[14] Skeincoin Ltd., Selitskogo, 25A office 22, 220075, Minsk, Belarus

[15] BelTA (2017): http://www.investinbelarus.by/en/press/news/revolution-in-it-what-changes-decree-on-digital-economy-development/

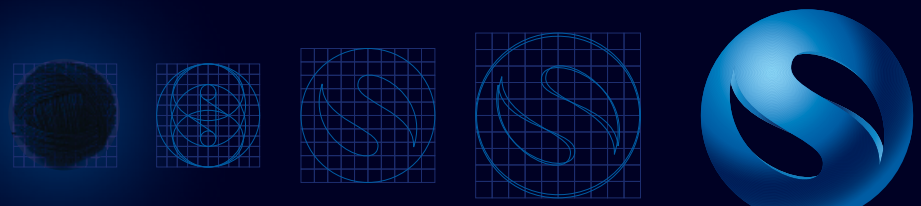
[16] Iryna Chelyshava, Belarus' Cryptocurrency Experiment: Why the World Should Take Notice, JURIST — Academic Commentary, Jan. 10, 2018, http://jurist.org/forum/2018/01/Iryna-Chelyshava-Belarus-cryptocurrency.php

[17] https://github.com/btcpayserver

[18] https://www.statista.com/outlook/212/100/online-games/worldwide#market-revenue

[19] https://blockonomi.com/mt-gox-hack/

[20] https://www.ccn.com/openex-hacked/



skeincoin

Skeincoin Ltd. • Selitskogo, 25A office 22 • 220075, Minsk, Belarus