Safex (Blue Paper)

A peer-to-peer marketplace and fungible digital cash system

A guiding document to Safex Developers, Advisors, and Early Adopters

=========

Daniel Dabek, Ivana Todorovic

January 3, 2018

Abstract

A purely peer-to-peer marketplace with an embedded cryptocurrency that is anonymous, has an emission rate based on merit, and is easy to obtain and use by a wide group of people would allow mass adoption of decentralized cryptocurrency. Safex establishes a network where digital currencies are fairly distributed through Proof of Work mining. The emission rate is such that the currency is desirable to earn through productivity and trade. Every action: transfer of currency and trade of goods and services that take place in the ecosystem is via a series of linked transactions that are recorded at regular intervals of blocks. The chaining of transactions of balances forms a blockchain. Security is brought by technologies that enable privacy which allows all participants to enjoy embedded trust and transparency. This provides people with a secure enclave for building digital wealth.

Introduction

While the Safex Blockchain could be a "vanilla" cryptocurrency and blockchain, the further progression of Safex is to establish a decentralized marketplace. Therefore, this document outlines the beta phase of the development cycle. This blue paper outlines the foundation on which the Safex Development team will build upon.
The conversion of Safex Tokens from the Bitcoin Blockchain into the Safex Blockchain will delineate the conclusion of beta, and the start of Safex Cash mining. Future documentation will summarize the innovations that have taken place during the beta development phase and will be published prior to launch. This document is the initial one and there will be more to follow, as development progresses, which will describe in depth each process as it reaches finalization in code.

Token

Safex Tokens provide a means for people to license themselves with the blockchain network. Any activity by users that intends to be lasting, and attached with a form of digital pseudonym, must be established through usage of Safex Tokens. There are 2,147,483,647 Safex Tokens that will ever exist and they serve a number of important utilities for Safex.
At this moment (January 2018) Safex Tokens exist on the Bitcoin Blockchain, but they will be moved to their own blockchain during the launch phase of the Safex Blockchain.

About the Safex Tokens that exist currently on the Bitcoin Blockchain. The origins of the Safex project begin with the token being instantiated and traded on the Bitcoin Blockchain. It adheres to the Omni Protocol, and it is identified by the #56 in the series of assets and its name is Safe Exchange Coin. The initialization of the Safex Blockchain also enables the holders of Safe Exchange Coin, found on the Bitcoin Blockchain

as #56 in the series of Omni Protocol tokens, to convert their Bitcoin based tokens into Safex Blockchain based Safex Tokens. Only the Safex Tokens that have been redeemed on the Safex Blockchain are eligible for the properties for earning incentives and for establishing accounts.

Migration of Safex from Bitcoin Blockchain. The migration of Safex from the Bitcoin Blockchain into the Safex Blockchain marks the start of the Safex Blockchain. All Safex Tokens that are on the Bitcoin Blockchain will be passed through a one way burn function and credited on the Safex Blockchain and will forever only exist on the newly established Safex Blockchain.

Safex Tokens are used to establish Accounts on the Safex Network. Safex Tokens are required to establish a profile on the network that establishes a pseudonym which could be used to create brand recognition and also to maintain a consistent identity. This identity would be valuable for establishing reputation and for making it easy to find a specific user on the network for interaction. A further description of Safex Accounts is found in the subsequent section.

Two types of ways to get incentives. The Safex Blockchain pays incentives to two different forms of Safex Tokens encumbrance. In the first, Safex Tokens are used to make an alias (account) on the network. Payment of incentives are still made to those tokens spent in forming the account. In the second place, someone with Safex Tokens can "lock in" their tokens and begin receiving fees from the marketplace. The second is not permanent, the tokens can be unlocked from the blockchain.

Cost of performing an incentive lock in. Performing a lock in transaction will cost 1 Safex Token which is burned but counts towards the incentives in the lock in. Unlocking the Safex Tokens will cost an additional 1 Safex Token.

Safex Accounts earn incentives. Establishing an account with Safex Tokens requires the user to encumber them in such a way that they can never be removed in the future. The network charges a provision for trading on the marketplace and therefore whoever has established an account receives their share of the provisions based on their holdings relative to the Safex Token supply.
Besides establishing an account and encumbering only the minimal amount of Safex Tokens, individuals can also create an incentive transaction, which enables them to receive incentives on their entire holdings. These special transactions can be unencumbered in the future.

Incentives come from marketplace trades. Incentives are established from charging a 5% marketplace fee, this is a provision on all sales offers of goods and services on the platform. At the conclusion of payment the provision is allocated proportionally to all locked in Safex Tokens.

Dealing with a larger number of incentive distributions. Due to a potentially high volume of incentive distributions, an entire block will be allocated on a regular interval in order to allocate incentives to their respective beneficiaries. The beneficiary will be able to then spend from this block towards other offers in the marketplace or to send to another address.

Cash

Safex Cash is the currency of the Safex Marketplace. Safex Cash is necessary to pay all transaction fees to the network. Every action that takes place on the Blockchain network requires the payment of some network fee. Safex Cash is obtainable through proof of work mining as well as from staking Safex Tokens. Safex Cash is also the principal payment method when fulfilling the purchase of products and services of the marketplace.

Money Supply of Safex Cash. The main function for Safex Cash is to act as an intermediary instrument between parties, that is, to facilitate the business of the market by acting as a common medium of exchange (Mises, 1953). In order to achieve that goal, it should meet the demand for currency so as to enable all transactions on the marketplace. Taking into consideration that Safex Cash should be generated from the start of the Safex Blockchain, the emission of the money supply must adjust according to demand for money supply. Demand for Safex Cash depends on platform growth - growth of new active users (both buyers and sellers) and the number of transactions. Consequently, the emission curve for Safex Cash is designed to follow the rate of marketplace adoption.

Safex marketplace is the innovation - it applies new ideas (encryption, cryptocurrency) and new, more effective technology (blockchain) to e commerce. Therefore, the adequate model that represents future growth of the Safex marketplace is known as "diffusion of innovation". It is a process by which an innovation is communicated internally over time among the members of a social market system (Rogers 1983). The diffusion follows an S-shaped curve which means that the innovation requires a lengthy period from the time it becomes available until mass adoption is achieved. In our case, after the marketplace is released, only a class of innovators are interested in using it (represented with a slow, and deliberate start). As it is communicated in a social system, other groups of consumers begin adopting the marketplace (represented with accelerated growth). In the last phase, growth rate of diffusion decelerates and eventually reaches the saturation level.

The Safex Cash emission curve is going to follow an S shape. There is a limit of 1 billion (1,000,000,000) Safex Cash that will be emitted in the next 20 years (1 minute per block). Half of the coins will be mined in first 7 years, while the other half will be emitted in the following 13 years.

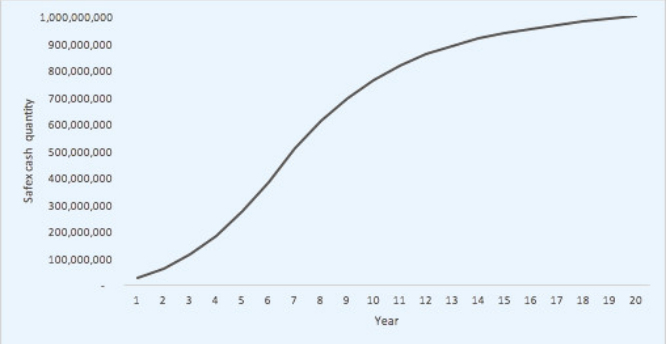

Figure 1: Safex cash emission curve

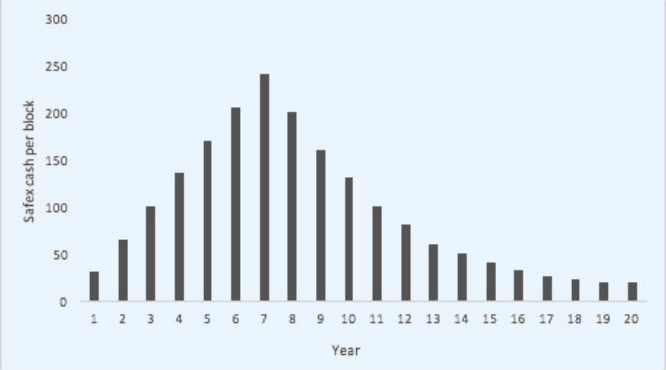

Figure 2: Annual mining reward per block

The purpose of a Safex Cash airdrop. In order to seed the network with activity and be able to cover fees for the initialization of the marketplace, 1 percent of Safex Cash will be airdropped. One half of that amount (0.5% of the money supply or 5 million coins) will be obtainable by the holders of Safex Tokens during the start of the Safex Blockchain. The other 0.5% will be assigned to the Safex development team.

Airdropped coins have a key role in the marketplace operation in the first months of launch, but they will also highly affect the future growth of the Safex platform. An initial condition for using the marketplace is the existence of a certain amount of currency. Without circulation of the currency, operations wouldnt be possible. So, airdropped Safex Cash are literally enabling usage of the platform.

The best way to put money in circulation is to distribute it to those who want to use it. Con-

sequently, coins will be distributed to Safex Token holders and the development team. One smaller amount of the teams currency will be used to cover development costs. The main part will be invested in marketing and promotion in order to increase the number of market participants so as to galvanize trading on the platform. Also, Safex Cash will be used to finance future development of the project using the Safex marketplace mechanisms of service providers. The amount of dividends that Safex holders will earn are directly dependent on the gross merchandise volume. This creates a strong incentive for Safex holders to promote the marketplace and spend (and earn) their Safex Cash from the platform. That is why a significant amount of airdropped Safex Cash will be used for marketing purposes and for buying goods and services.

Safex Cash Divisibility. Safex Cash is divisible to 4 decimal places. 1.0000

Names of divisible quantities:

0.0001 Safex Cash = 1 Dabek
0.001 Safex Cash = 1 Todor
0.01 Safex Cash = 1 Cortez
0.1 Safex Cash = 1 Cabral

Proof of Work Mining. Safex Cash is distributed using an egalitarian proof of work mining algorithm. The algorithm is based on the CryptoNight algorithm (Seigen, 2013). It is unrealistic to think that hardware manufacturers will incorporate more expensive methods to produce application specific machines for mining the coins. Therefore, general purpose computers such as the average home computer and at best graphic card arrays will be efficient at mining Safex Cash. This means that the ability for ordinary people to participate in the support of the network and acquisition of Safex Cash is more evenly distributed. It is for this reason and the Money Supply Distribution that throughout the entire lifetime of the Safex Marketplace and its Blockchain there will be rewards available to those who are adopting the network.
Emission of new coins follows the marketplace adoption model. For example, in years that are expected to have an exponential growth of users and transactions, money supply growth will also be exponential, and vice versa. This means the when there is higher demand for money, mining rewards will be higher. Total supply of Safex Cash is limited to one billion coins and when it reaches the maximum miners will depend on the transaction fees alone which will be ample with widespread usage of the currency.

Table 1: Safex cash mining schedule.

Year	**Block height**	**Mining reward**	**Total supply**
airdrop	0	10	10,000,000
1	525,000	30	25,750,000
2	1,050,000	65	59,875,000
3	1,575,000	100	112,375,000
4	2,100,000	135	183,250,000
5	2,625,000	170	272,500,000
6	3,150,000	205	380,125,000
7	3,675,000	240	506,125,000
8	4,200,000	200	611,125,000
9	4,725,000	160	695,125,000
10	5,250,000	130	763,375,000
11	5,775,000	100	815,875,000
12	6,300,000	80	857,875,000
13	6,825,000	60	889,375,000
14	7,350,000	50	915,625,000
15	7,875,000	40	936,625,000
16	8,400,000	32	953,425,000
17	8,925,000	26	967,075,000
18	9,450,000	22	978,625,000
19	9,975,000	20	989,125,000
20	10,518,750	20	1,000,000,000

Marketplace

The main value proposition of the Safex Blockchain is its embedded marketplace. The world has found that cryptocurrencies are

highly effective for making international payments and purchases (Nakamoto, 2008). However, there are many shortcomings due to offsite clearing of the payments. Safex Blockchain addresses this by providing a fully functional marketplace mechanism where people are capable of offering their goods or services directly on the Blockchain and all payment clearing and processing takes place atomically via blockchain transactions.
There are a number of advantages to such a system:

1. No longer do people need to host complex services to provide purchasing mechanisms for cryptocurrencies.
2. The advancement permits fewer risks in service breach that leads to theft and compromised payment systems involving cryptocurrencies. Safex Marketplace eliminates the web server altogether because all payment and clearing is carried out cryptographically over a decentralized network.
3. Discovery of trading partners becomes more efficient so that you can find products and services readily.

The Safex marketplace is a collection of markets and sale listings. People can interact with the marketplace term agreements. Within a term agreement are the parameters by which a transaction will be fulfilled. Among the attributes include: arbitration, escrow, digital receipts, timestamp proofs, cash on delivery. The possibilities of expanded data structures of a CryptoNote Transaction allows the network to implement various advancements in utility (Werner, 2012).

Void Market (when someone has no category marketplace listing). The Safex marketplace permits any person to pay a listing fee which enables a digital contract to be embedded and executed by the blockchain network. These market listings bare no title, and are free formed with arbitrary parameters.

Title Market (A curated and centrally managed marketplace of vendors and participants). A title market is a listing that is backed by a staked participant. In order to post a listing, such a participant would need to be verified by the Title operator or be the controller of the Title. These listings are enabled to provide an identity; for example the title market for apples could be: apple, and within it are all verified sellers listings of apples, their prices, and terms of redemption.
The curator would then enable settings to provide the proper means for the vendors to fulfill their objectives of trading in their respective markets. The curator can enable or disable anyone from participating in this particular title, for instance, should an apple vendor begin to sell electronics in the market for apples.

Escrow and Arbitration. Curators can also set arbitration rules, and the forms of escrow that are permitted on their market segment. This means that when a merchant decides to offer their product on a specific Title Market, they are enabling all of the rules set forward by the person who established that Title.

Costs of establishing a Title Market. The cost of establishing a Title Market and becoming its curator requires a Basic Account to pay and burn 200 Safex Tokens at the time establishment. The curator of the market can set a fee for utilizing their segment and they will earn the fee from all sellers within their marketplace.

Encrypted Marketplaces. Any user has the ability to fully encrypted their market, and in order to participate in that market, the user must acquire the decryption key.

Finding and Interacting with hosted markets. The transaction hash, is the "web address" in the blockchain where a Title marketplace listing or void market listing can be parsed from.

While the blockchain marketplace cannot be censored in any way, the way people experi-

ence the marketplace can be regulated (voluntarily). Thus, a layer above the blockchain could act as a registry of these transaction hashes that represent the destination to a specific product or service within the Safex marketplace. These addresses can then be filtered and curated on a website or an application.

Accounts

Users of the marketplace can establish a profile via a Safex Account. A Safex Account is able to display its identity and be stored in the blockchain. A basic account consists of a Name, Avatar, Website URL, Unique ID, and an array of PGP Keys. The most important aspect is the fact that a basic account could receive and give reputation.
Effectively, an Account is capable of applying its sell orders to a Title Market or to the Void and represent its wares in that marketplace if approved by the Title Market Curator. A Basic account may not create a Title Market. This type of account can already begin to acquire reputation and give feedback on other transactions.
The cost of a basic account is a burn of 2 Safex Tokens. These tokens are staked and earn residual dividends for the account.

Safex Network fees are paid in Safex Cash. Each action that involves manipulating data related to the marketplace takes the form of a transaction. These transactions bear a network fee that must be paid in Safex Cash.

Each trade enables a feedback event for building reputation. When someone concludes a trade with another party, so long as the trade took place with an account, each person may grant feedback to the other party. Both buyer and seller can award a reputation score between 1-5 as well as a text comment. Part of the provision from a trade is allocated so that people need not worry about additional payments for the data costs when leaving feedback.

Full confidentiality is established by encrypting the marketplace listing. It is also possible that users will want to privately share their marketplace listings. In order to facilitate this, users can encrypt their marketplace listing. Only those characteristics which are required for the Blockchain to process escrow remain visible. The conditions and descriptions of the product or service remain encrypted via PGP.

Treasury

Safex needs a way to finance future development and maintenance. Since safex is a completely decentralized community and software that has been demanded and built by a worldwide collective effort, it also will need to have some form to ensure the maintenance of its future. Other decentralized technology platforms such as Dash (Balazs, 2017) have found great success in proliferating their message and development contributions by offering bounties.
Safex will need to permit for such a provision so that innovation remains on a constant trajectory, and for there to be an unbiased reserve of finance to permit incentives to be made which the community could call on to demand improvements and the development of new features.

Treasury funding comes from trades on the marketplace. A provision on all transactions will be charged from all sales events of 0.02%. This amount will be sent to a repository maintained by the Safex software.

Community appointed Chief Architect. The community could appoint a chief architect who could allocate 50% of the finances based on a monthly balance average without approval from the community. The Chief Architect will submit a key that the blockchain software will recognize for spending funds. All expenses must be a proposal and should be put

towards critical infrastructure bounties to developers, and other necessary expenses for the Safex software.

Nominating a chief architect. Nomination of a chief architect could take place once every 3 months. Also a majority of participating voters will determine the outcome of the vote.

Proposal for spending from the treasury for community initiatives. Anyone with an account could make a proposal and anyone with Safex Tokens before the proposal was formed could cast a vote whether to approve or decline an expense. Majority of participants will determine the outcome of the proposal.

Blockchain

The Safex Blockchain focuses on addressing critical issues related to community adoption and sustainability. This means that people who find themselves using the currency mined on this blockchain must be able to maintain their sovereignty by protecting their balances in such a way that adversaries cannot analyze and make targets of the users. Therefore, the currency must employ anonymizing features to protect the people who use it.
Secondly, users should be able to exercise activities over the blockchain, in this case exposing a marketplace where people can buy and sell the things that they want and need from other people without leaving the confines of the Safex peer to peer network. In addition, the sustainability aspect depends on the blockchain not being constrained and prone to spam attacks due to full blocks as is the case with Bitcoin.

Dynamic block size deals with full blocks. A common flaw and the subject of intense controversy is the capacity of blocks in many blockchain networks, particularly in Bitcoin. The Safex Blockchain employs a dynamically adjusting block size limitation so that as block utilization increases so does the limitation in order to accommodate an ever expanding user base.

Encrypted communication via the blockchain. Anyone can store a PGP key in the Safex Blockchain for a fee. Therefore, messages can be encrypted using the identifier of the PGP key and stored in the blockchain for retrieval in the future by the recipient.

Ring Confidential Transactions ensure fungible currency. A critical element of cryptocurrency is that it must be mutually interchangeable. One unit of Safex Cash must be in the same perception as another Safex Cash unit. This defines the "Cash" term of the Safex Currency. Therefore, the Safex Blockchain employs the use of Ring Confidential Transactions in order to preserve the fungibility of the currency so that each Safex Cash is viewed in the same way. This also means that when spending to a purchase agreement or sending a transaction the recipient has no knowledge of the purchasers other balances and has no knowledge of the purchasers spending habits (Noether, 2015).

RingCT for securing private wealth. Utilizing Ring Confidential Transactions means that only the sender and the receiver know which transaction is correct from the set of inputs used to form a transaction. One the one hand the sender who formed the transaction has information about the real transaction and on the other hand the recipient is able to sign off on a future transaction with their private key. These features are essential to maintain privacy that one should expect with their finances when utilizing a fully transparent and decentralized blockchain.

Conclusion

We have outlined a path that will solve the most important issues that face cryptocurrencies today. Those of fair currency distribution,

a rigorous incentive model for promotion of the ecosystem to more participants, the means to remain secure when spending funds within the digital realm, and finally a mechanism through which people can engage in meaningful trade among each other.

From here the development team is able to produce a minimum viable product that can go to the market and serve the people to conduct crypto commerce. The future will be full of innovations beyond the initial implementation and only because we took the first steps will those enhancements and optimizations be possible. The early adopters are the first to the market and will be veterans of utilizing our novel platform and be leaders in the new economic model that cryptocurrencies have presented to us. We have found the best way to distribute money to support real utilization, while maintaining the incentive for people to participate fairly along the way. This project intends to stand the test of time and should be considered a global infrastructure that is being cultivated for the long term.

References

Balazs, K. (2017.) *Governance and Budget System*, https://dashpay.atlassian.net

Mises L. (1953.) *The Theory of Money and Credit*, Yale University Press, New Haven, CT, USA

Nakamoto, S. (2008.) *Bitcoin: A Peer-to-Peer Electronic Cash System*, bitcoin.org

Noether, S. (2015.) *Ring Confidential Transactions*, https://eprint.iacr.org

Rogers E. (1983.) *Diffusion of innovations (3rd ed.)*. New York: Free Press of Glencoe, USA

Seigen et al. (2013.) *CryptoNight Hash Function*, cryptonote.org

Werner et al. (2012.) *CryptoNote Transaction Extra Field*, cryptonote.org