



Samsung Wallet

WhitePaper v.1.1
03.06.2019

SWCoin.site

Table of contents

Table of contents	2
Abstract	3
Crypto market challenges	3
Custody risk	3
Regulation	5
Possible falsification and distortion of market data	5
Samsung Wallet product	6
Asset management	6
Distributed Orderbook (DOB)	6
Samsung Orderbook implementation	7
Order acceptance to the DOB mempool	8
DOB anti spam and fraud protection	9
Trades history blockchain storage	9
Samsung Swaps	11
Samsung Swap technology	11
Samsung Wallet Swap implementation	12
Samsung SDK	14
Additional functionality	15
Immutability and decentralization	15
Samsung Wallet ecosystem	16
Platforms	17
Competitive analysis	17
UI Preview	18
Roadmap	22
Current stage	22
SWC Coin	23
Team	24
Glossary	26

Abstract

A brief glance at the emerging market of crypto projects is sufficient to understand the potential of the blockchain as a powerful, advanced technology of the future. Yet, despite its vast prospects, a major part of blockchain-based systems still remains at an entry-level, far from being qualified for a general user. Today, the developers' community is facing a number of unresolved issues preventing a full-scale implementation of the blockchain technology in a vast variety of industries, where it could potentially be applied at a great profit.

Crypto market challenges

Blockchain-powered technology is intent on leading the future of financial markets. Today, however, we still observe extensive obstacles for the development of blockchain-based markets. One of the greatest market challenges is the remaining necessity of trust towards centralized financial services in an otherwise decentralized environment. Third party custody risks affect ecosystem sustainability, bringing vulnerability to manipulative and regulative actions.

Samsung Wallet radically solves problems described above by introducing a fundamentally new platform for custody-free, transparent, immutable cryptocurrency trading. Our platform is the simplest way to connect buyers and sellers within a decentralized framework. Samsung Wallet is a new type of decentralized cross-blockchain exchange.

Custody risk

Satoshi Nakamoto, the creator of the Bitcoin, has presented the world with a revolutionary technology thereby offering significant advantages to any projects which would incorporate it. These advantages, namely, transparency, openness, and independence from trust-based mechanisms, have been explored and utilized over the years by those involved in the field.

Since the early days of Bitcoin, cryptocurrency market has evolved into a sophisticated multi-blockchain phenomenon. According to coinmarketcap.com statistics, cryptocurrency market contains over 1,5K different currencies with exchange turnover of over 14 bln in dollar equivalent daily. In addition to coinmarketcap statistics, we should consider the volumes of intransparent and unregulated peer to peer exchange market (a.k.a. *Over The Counter*) as well.

However, present-day exchange providers managing huge exchange volumes inherit custody risks, which counterposes the ideas of transparency, openness, and independence from trust-based mechanisms.

More than once have major exchanges experienced security breaches. One of the most disruptive failures was the Mt. Gox exchange collapse. It took the market up to a year to recover after the disaster. The list of the publicly known biggest failures for custodian-based centralized crypto exchanges would impress an unprepared spectator:

Date	Amount lost	Exchange
February, 2014	650,000 BTC (\$368M)	Mt.Gox
March, 2014	150 BTC (\$101k)	bitCoin
March, 2014	896 BTC (\$572k)	Flexcoin
July, 2014	3,700 BTC (\$2M)	Mintpal
July, 2014	5000 BTC (\$1.8M)	Bitpay
January, 2015	7,170 BTC (\$1.82M)	BTer.com
January, 2015	3,000 BTC (\$777k)	Kipcoin
January, 2015	18,866 BTC (\$4.3M)	Bitstamp
March, 2015	150 BTC (\$3.2k)	Coinapult
May, 2015	1,500 BTC (\$350k)	Bitfinex
January, 2016	13,000 BTC, 3,000,000 Litecoin (\$5.8M)	Cryptsy
March, 2016	469 BTC, 5,800 ETH 1,900 Litecoins (\$230k)	ShapeShift
May, 2016	250 BTC, 185,000 ETH, 1,900 Litecoin (\$2.14M)	Gatecoin
August, 2016	119,756 BTC (\$65M)	Bitfinex
October, 2016	2,300 BTC (\$2.6M)	Bitcurex
July, 2017	37,000 ETH (\$7M)	COINDASH
July, 2017	5,300 ETH (\$1M)	Bithumb
August, 2017	1,500 BTC (\$500k)	Enigma

On a good note, along the process of evolution, each new failure leads to new knowledge, a portion of which crypto professionals comprehend and evangelise in public nowadays in the following way: *if one doesn't have the keys to his/her crypto assets, they can be gone at any moment and this will be irreversible.*

Regulation

Cryptocurrency market draws attention of customers, media, business, hedge funds and even filmmakers. Unfortunately, regulators do not stay aside and give a lot of their attention to the blockchain market as well.

The fundamental idea behind Bitcoin is a censorship-free currency without a central bank, the immutability of which is to be empowered by the financial incentivisation of the stakeholders. Egalitarian permissionless approach showcased by this cryptocurrency contradicts the regulation created for fiat money markets and so is a subject to scrutiny by the officials.

However, while being at the early stage of the development, it is essential to preserve this approach for the further market development and expansion. For the only way of keeping the promise of the Bitcoin manifest is to carry on developing decentralized immutable solutions.

Possible falsification and distortion of market data

In most mechanisms employed by centralized exchanges, the actual market data is unverifiable and suffers from lack of trust. Traders can be misled by false data, intentionally or unintentionally distributed by centralized operators. In a current market state, manipulation and failure to deliver actual trading data can devolve into severe losses for the investors.

Besides the current real-time market data, the history of trades and orders can be substituted, wiped off or distorted in a similar fashion.

Proper end customer and average investor protection from aforementioned risks appears to be a vital step for further successful market development.

Samsung Wallet product

The aforesaid problems are what the blockchain industry is currently faced with and yet fails to solve. Being on the way to achieving its mass adoption, the industry is expected to solve these issues only with a fundamentally new approach based on the idea of decentralization of digital assets exchange. As a reaction to the current challenges of the industry, Samsung project was created - a convenient and versatile decentralized solution for the custody-free cryptocurrency trading.

Samsung Wallet platform is based on a unique, proprietary engine, specially designed to solve its specific tasks. Therefore, this White Paper contains a large number of technical terms describing certain elements of the platform. Each original term is highlighted in ***bold and italic*** when first encountered in the text: for instance, Samsung Swap. At the end of the paper, a glossary with detailed explanations of the terms is available.

Asset management

Samsung Wallet provides a powerful, in-demand service that allows users to reduce efforts spent on managing ***crypto assets*** and renders it transparent and trustless. To make our platform even more convenient and beneficial for users, the Samsung Wallet team utilizes best UI and security practices thus facilitating use of our platform's functionality to the full range. Essential operations one would like to do with his/her cryptocurrency are:

1. Receive crypto assets to the generated wallet
2. Import assets to the wallet using ***private keys*** of various formats
3. Store private keys in a securely encrypted environment
4. Send assets to other ***addresses***
5. Select ***cryptocurrency node*** to use
6. Select ***blockchain explorer*** to use

Aforesaid wallet functionality will be built on the ***SPV (Simplified Payment Verification)*** technology. This allows customers to avoid prolonged blockchain synchronization while preserving the security of so-called ***'full node wallets'***.

The keys are stored in an encrypted manner on the end-user device or a hardware wallet (eg. Ledger, Trezor, etc.) Keys can be backed up with the passphrase for all the listed currencies or with a string format key for each currency.

Distributed Orderbook (DOB)

An ***Orderbook*** is an electronic list of buy-and-sell orders of specific security or financial instruments, organized by price level. The Orderbook lists the number of asset units being bid or offered at each price point, or market depth. It also identifies the market participants behind the buy-and-sell orders, although some might choose to remain anonymous. The Orderbook is dynamic and constantly updating in real time throughout the day.

The approach to the construction of the blockchain exchanges (e.g. Binance, Mt. Gox, Bitfinex etc.) has been copied from fiat operators, like NASDAQ, NYSE, LSE, ending up with failures happening one after another.

Besides the well-known custody-centric fails, market manipulation through falsification and distortion of market data, unfortunately, happens as well. However, blockchain establishes new forms of financial products. Adopting new opportunities this technology brings is the most guaranteed way for promising and smart projects to skyrocket. One of the undervalued possibilities is the creation of a completely decentralized and transparent Orderbook.

Samsung Orderbook implementation

Distributed Orderbook (DOB) is a way to represent market offers in a decentralized manner, in accordance with the spirit of blockchain industry.

Samsung DOB is based on a *BitTorrent protocol*. BitTorrent is a communication protocol for peer-to-peer file sharing ("P2P") which is used to distribute data and electronic files over the Internet.

BitTorrent is one of the most common protocols for transferring large files, such as digital video files containing TV shows or video clips or digital audio files containing songs. Peer-to-peer networks have been estimated to collectively account for approximately 43% to 70% of all Internet traffic (depending on location) as of February 2009. In November 2004, BitTorrent was responsible for 25% of all Internet traffic. As of February 2013, BitTorrent was responsible for 3.35% of all worldwide bandwidth, more than half of the 6% of total bandwidth dedicated to file sharing.

To anticipate a better understanding of how Samsung Swaps will work within the Samsung Wallet we should reveal major principles of the Distributed Orderbook and order matching. In terms of Samsung Wallet Orderbook an order possesses following characteristics:

1. **An order is an offer, not a commitment.** By creating an order, customer posts an ad for a future *trade*. When the time of the trade comes, the customer can avoid processing the transaction if he/she desires so. Maker faces a moderate decrease of his/her current rating in case of rejecting to trade against his/her own orders.
2. **Order placement doesn't block customers' funds.** Unless the orders have matched between two traders, funds are not being moved. Only after two traders confirm a trade the funds actually move from their wallets.
3. **An order can be executed with multiple trades.** An order can be filled with several trades with an unbounded range of traders (*takers*). Until the order is canceled it stays active in the orderbook and available for trade.
4. **Offline traders cannot trade.** Samsung Swaps require both customer and wallet to be online in order to be processed. In case a customer gets off the Internet or closes wallet application the order becomes invisible for other traders. After the connection is established back the order automatically gets back to demonstration at the orderbook. *In future the protocol will allow offline trading but this function is out of scope for current document.*
5. **Execution is a manual operation.** Samsung Swap technology is known to be the best among others because even within the exchange customer retains control over the private keys. *In*

future the protocol will allow offline trading but this function is out of scope for current document.

6. **Maker is free to reject execution.** Before the start of the swap, maker can change his/her mind for various reasons, such as the amount of trade being less/more than desired or the rating of the counterparty being below the *maker's* expectation. The only shortcoming that maker faces is a moderate decrease of his/her current rating.

Order acceptance to the DOB mempool

Samsung DOB is an immutable and decentralized solution created to transmit information about the exchange orders among Samsung wallet users.

DOB is maintained by the Samsung Wallet clients serving as nodes in the distributed network. When an order is transmitted to the network it first gets verified by all of the Samsung Wallet clients available.

All the clients validate following information before submitting it to the *mempool*:

1. **Data consistency.** All the data should be submitted to the mempool in pre-described by the orderbook protocol format and shouldn't contain *injections* nor interfere the dependencies in the orderbook that can appear.
2. **Order Legitimacy.** Active nodes from the network analyse the following parameters:
 - a. Accordance of the Order *digital signature* to the Makers public address in the blockchain appointed in the order
 - b. Availability of the amount on the wallet address appointed in the order. Maker cannot stake more than he/she has on the wallet
 - c. Absence of the conflict between newly created order and the previously created orders with the same signature
3. **Blacklist screening.** The absence of the orders address in the blacklist of spamming or rarely finishing trades actors.

After necessary checks are processed Samsung Wallet adds Order to the DOB and starts *seeding* it with the neighbouring Samsung Wallets.

When an Samsung Wallet receives a new valid block (see [Trades history blockchain storage](#)), it removes all the orders executed within the previous time and contained in this block from the mempool.

DOB anti spam and fraud protection

In many ways DOB mempool works as the widely known and high-load production verified Bitcoin Mempool and has a very similar realisation. This ensures us in a high level of attack resistance of the solution and a very unlikely possibility of spam and fraud within the network.

However for the first period of operation Samsung Wallet team leaves itself the right to blacklist fraudulent and spamming actors from the network by blacklisting addresses or public keys by signatures. Centralized nature of such verification should not and will not last for a long time. The complete decentralization of the DOB blacklisting will be finished with the release of decentralized ratings system planned in the Roadmap.

Trades history blockchain storage

Samsung Wallet will use a custom-built *Byzantine consensus* algorithm that keeps DOB historical data safe without needing to “mine” blocks, even in the case of a situation where your nodes malfunction or become susceptible to the actions of bad actors. This feature also makes it near impossible for a bad actor to add incorrect data or change the history in Samsung Wallet Blockchain. In case of many compromised nodes, Samsung Blockchain still maintains its fundamental security properties, protecting data. Samsung Wallet Blockchain will update immediately with the addition of every new block.

Samsung Wallet will gather successful and unsuccessful trades into blocks; the whole block is approved Samsungally. Each trade is executed separately from the Samsung Wallet Blockchain. Samsung Wallet Blockchain will be used only in the purpose of storing historical data.

As every block includes the hash of the previous block, it is impossible to change one block without the appropriate changes to each of the following blocks. This ensures immutability of the trade log; once a trade is committed, it cannot be retroactively modified or evicted from the log. Similarly, it is impossible to insert a trade in the middle of the log

Samsung Wallet uses a custom modification of Byzantine fault tolerant consensus to guarantee that in any time there is one agreed version of the blockchain. It is assumed that the environment is decentralized, i.e., any node is allowed to fail or be compromised. Consensus is *authenticated*; consensus validators are identified with the help of public-key cryptography.

To generate a new block and vote upon it, a 3-phase approach is used.

- The consensus algorithm is divided into rounds, the beginning of which is determined by each *validator* based on its local clock. For every round, there is a predefined leader validator, which is determined based on the round number, blockchain height and other information from the blockchain state. The leader creates a block proposal and sends it to other validators
- Other validators check the proposal, and if it is correct, vote for it by broadcasting prevote messages to the validators
- If a validator collects prevote messages for the same proposal from a supermajority of validators, it executes transactions in the proposal, creates a precommit message with the resulting data storage state and broadcasts it to the validators
- Finally, if a validator receives precommits from a supermajority of validators for the same proposal, the proposal becomes a new block and is committed to the local storage of the validator

Historical data from the blockchain will be used in the purpose of public actors rating system. Public actor rating will be counted on the basis of the number of successfully finished exchanges. Data is collected with the help of *blockchain oracles* from the networks where Samsung Swaps are processed.

Samsung Swaps

A cross-chain is an exchange of cryptocurrencies between users. Basically, party A sends Coin A to party B's Coin B address via blockchain, while party B does the same with Coin B. These actions happen independently on parallel blockchains, in a one-way fashion. Such setup raises the possibility of either of the parties never honoring his/her end of an agreement. One of the ways to solve this issue is involvement of a trusted third party. An Samsung cross-chain swap, on the other hand, solves this problem without the need for a third party.

Samsung swaps require each party to arrange a transaction contract. The contracts contain an *output* spendable by the the opposite party, but the rules required to collect is are different for each party involved.

Samsung Swap technology

The first party (called the initiator) wishes to trade Coin B for Coin A with the other party (called the participant). The initiator allocates the intended amount of Coin B to a contract and generates a "secret". The secret will later allow the participant to collect the contract output. Until he/she learns the secret, the participant is unable to spend from the initiator's Coin B contract.

The participant creates a contract on the Coin A blockchain in a similar to the initiator fashion. To create the contract, the participant requires a cryptographic hash of the initiator's secret. The initiator could not access this contract without revealing the secret to the participant.

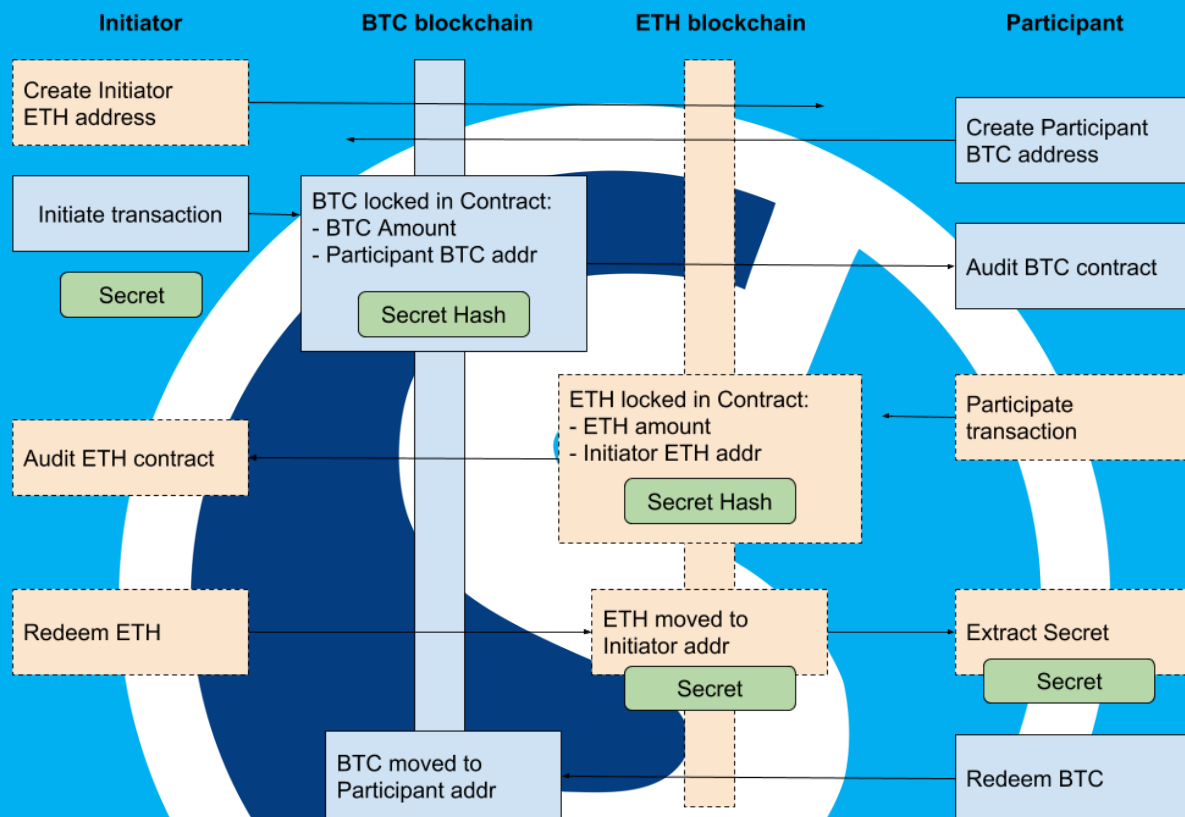
After both parties created their contract, neither of them can collect their coins back until the allotted time expires. The initiator redeems the participant's contract, thereby revealing the secret to the participant. The latter redeems the former's contract using the secret extracted from him/her.

When a certain period of time (typically 1 hour) expires and the participant did not redeem the contract output, it is refunded back to the initiator's wallet. The participant's contract can also be refunded back to the participant, but only after half the period of time that the initiator is required to wait before their contract can be refunded (typically 2 hours).

The initiator can also trade Coin A for Coin B and the procedure will be the same, but with each step performed in the opposite direction on another blockchain.

This procedure is considered Samsung (i.e. with a timeout) since it gives each party at least 24 hours to redeem the coins from the opposite blockchain before a refund can be performed.

The image below provides a visual of the steps each party performs and the transfer of data between each party:



Samsung Wallet Swap implementation

Samsung Wallet has implemented the best solution on the market for both Samsung Swaps and Distributed Orderbook. The process of an order creation and execution is designed as follows:

1. Customer A creates an order for the trade and signs it with the private key. The order inherits following parameters:
 - Currency pair.** The currency desired to receive and the currency desired to be sold.
 - Size.** Order size is not to be limited by trading lots but will have a minimum value that will cover current *network commissions* for processing a swap.
 - Price.** The price that is desired to process the trade with.
 - Price type.** Price can be of a fixed (set in stone) or float type (following the current market rate).

Price margin (optional). This specification is used for the float type prices. A margin is the amount to be put above or below the *market price*.

Minimal amount (optional). The standard number of units in a trading security. Minimal amount represents the minimal quantity of a blockchain asset as set out by the maker. Minimal amounts are designed to help crypto users with large sums, do so by refraining from performing many small trades within one order.

Wallet address. Public address of the cryptocurrency corresponding to the blockchain asset to be sold. Wallet should contain no less than the amount of the active orders created by this customer.

Signature. To demonstrate the authenticity of digital messages sent to the Samsung Wallet environment (Orderbook and Following order execution), Samsung Wallet uses digital signatures. A valid digital signature gives a recipient a reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message, and that the message was not altered in transit. The Samsung mnemonic seed is used as the private key for signing the messages. With Samsung Wallet signature customers can be identified and rated as more/less efficient partners for Swaps without limiting their privacy and anonymity.

2. The order is sent to all Samsung Wallet users via the proposal of an update to the file distributed and synced among all users.
3. One of the Verification nodes checks the order for legitimacy in terms of Samsung Wallet environment. Verification node creates an updated version of the DOB file wiping off the closed orders and adding new ones.
4. The new version of the DOB file is synchronized along the network once in a minute.
5. Customer B picks the order from the orderbook and decides to trade against it. Customer B indicates the amount he would like to exchange.
6. Customer B's Samsung Wallet sends a request to the Customer A's Samsung Wallet. The request for exchange contains the following parameters:

Amount. The sum desired for a trade.

Wallet address. The public address in blockchain B which Customer B possesses within the Samsung Wallet.

Signature. Keys signed by the Customer B.

7. Customer A's Samsung Wallet confirms the trade after processing several checks:
 - a. Sufficiency of the funds on the Customer B's wallet
 - b. Accordance of the amount desired to trade with the order
8. Customer A confirms the trade with the password
9. Customer B's wallet commences the swap process

...

A detailed description of Samsung Swap process can be found at [Samsung Swaps](#) paragraph.

...

10. Customers receive funds to the corresponding addresses.

The implementation of both Samsung Wallet orderbook and the matching procedure requires no blockchain consensus algorithm since the DOB and matching are not built as smart-contracts or onchain solutions. DOB is a distributed file and matching happens on a peer-to-peer basis.

Samsung SDK

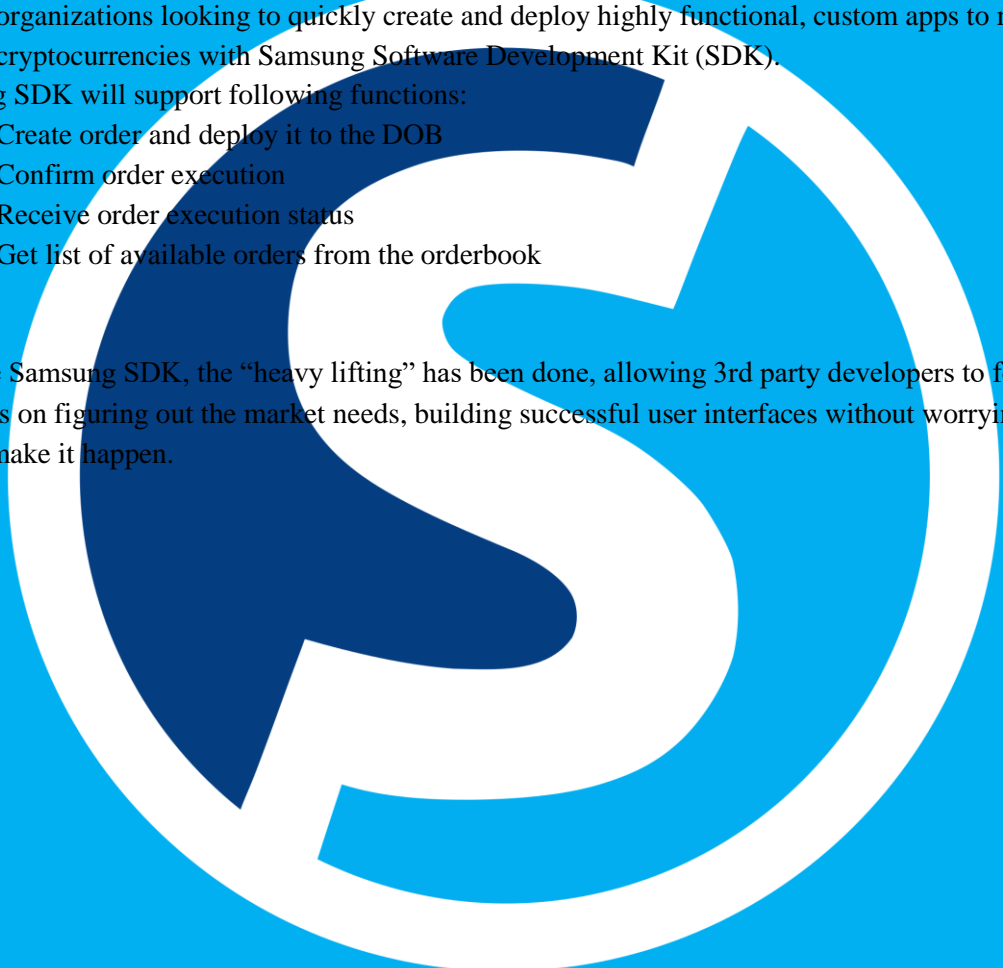
Developing even simple applications working with blockchains takes time and money. Creating complex, highly-functional distributed blockchain apps can take a number of highly skilled blockchain developers, thousands of hours for RnD which comes out in millions of USD costs. Following the promise of building a completely decentralized solution Samsung Wallet team will provide the following:

1. Availability to develop applications working with Samsung Wallet DOB and Samsung Swaps code. The protocols will be open and available for integration.
2. Developers SDK to smoothly integrate Samsung Wallet exchange functionality without having to mess with complicated protocols. Samsung Wallet will provide a solution to organizations looking to quickly create and deploy highly functional, custom apps to manage cryptocurrencies with Samsung Software Development Kit (SDK).

Samsung SDK will support following functions:

1. Create order and deploy it to the DOB
2. Confirm order execution
3. Receive order execution status
4. Get list of available orders from the orderbook

With the Samsung SDK, the “heavy lifting” has been done, allowing 3rd party developers to focus resources on figuring out the market needs, building successful user interfaces without worrying about how to make it happen.



Additional functionality

Samsung Wallet adopts various means of exchange. For some occasions, customers might be willing to use non-Samsung exchange functionality. Being a custody-free solution, Samsung Wallet implements only instant exchange options. For the convenience of Samsung Wallet users, two instant exchange options are implemented:

1. **Shapeshift.** ShapeShift is the fastest, most private, and most convenient way to swap digital currencies, with the exchange rate always remaining competitive. Following the Samsung Wallet community vote, ShapeShift was selected as a default option for instant exchanges.
2. **Changelly.** Popular cryptocurrency exchange providing the ability to instantly and seamlessly exchange over 90 altcoins at the best market rate or to buy them using a bank card. Operating since 2015, Changelly has attracted over 1.5M registered users from around the world. Currently, the service processes more than 15K transactions daily with a monthly turnover of around 60K BTC.
3. **Fiat options.** Fiat options to be provided to the customers in cooperation with partner services. Integration will be carried in a seamless smooth manner. Samsung will not process fiat operations himself following “do not touch fiat” policy. Early commitments from the partners already received and will be unveiled prior to the public crowdsale. Following options are planned for the implementation: payment cards acceptance, bank wires acceptance, bank wire withdrawals.

Immutability and decentralization

Blockchains are designed to be immutable and decentralized. Samsung Wallet team believes products designed for cryptocurrency assets should be immutable and decentralized as well. That is why it's important for Samsung Wallet to be a serverless, immutable solution in all the aspects. All parts of the system operate in a decentralized manner and are not controlled by any company or party:

1. **Samsung Wallet Distribution.** Application is distributed over the BitTorrent network and is supported by the customers.
2. **Asset Management.** Cryptocurrency private keys are stored on the customer side and are not transferred to the server.
3. **Transaction creation.** Transaction is created on the customer-side. The client application handles all the necessary cryptography and transmits it to the node. Customer can appoint any node with open RPC API.
4. **Transaction History.** Transaction history is retrieved from blockchain explorers over the commonly used API requests. Customer can point the block explorer he/she trusts most or deploy own one and use it as source of transaction history.
5. **Orderbook.** Samsung Wallet utilizes own Distributed Orderbook technology. Samsung DOB is based on a BitTorrent protocol and cannot be seized or stopped. DOB is distributed among all the online wallets.
6. **Order execution.** Order execution is processed peer-to-peer and blockchain based. No third party is involved in the transaction processing. The transaction is custody and possible intervention free.

Samsung Wallet ecosystem

The success of the Samsung Wallet is contingent on the participation of a variety of different users. We will briefly give an overview of the key roles that participants can play in the Samsung ecosystem.

1. **Traders.** End-users that hold, convert and transfer blockchain assets.
2. **Blockchain Assets Issuers.** People, companies, communities, organizations or foundations that issue new Smart Coins, configuring the initial supply, price, CW, and managing the initial issuance of Coins. This also includes creators of Relay Coins, which can connect any existing *ERC20 Coins* to the network.
3. **Cryptowhales.** Traders with the amounts of assets too big to be normally adopted by openmarkets and willing to perform personalized or non-personalized risk-free *OTC deals*.
4. **Arbitrageurs.** Traders that monitor the Decentralized Orderbook for prices that are inconsistent with an external exchange, and then restore price consistency through arbitrage. Arbitrageurs are organically incentivized to keep prices consistent and hence are important participants in the Samsung ecosystem.
5. **3rd party developers.** Companies or individuals creating services utilizing Samsung Wallet DOB and Samsung Swap code. Developers can build specialized Samsung Wallets, exchange Relays, Decentralized OTC platforms or implement part of the Samsung functionality in their existing services.



Platforms

Samsung Wallet team is focused on bringing truly decentralized experience to all the customers on all the platforms. Samsung Wallet technology is created with the idea of omni-channel product which customer can access from any device he/she has.

Samsung Wallet supports the following platforms at the moment:

- Microsoft Windows
- MacOS
- Ubuntu
- Debian
- Fedora

Within the development further platforms are to be supported as well:

Web

- Javascript web based application

Mobile

- iOS
- Android

Browser plugin

- Chrome
- FireFox

Competitive analysis

Feature	Bitfinex	0x	Etherdelta	Exodus	Altcoin.io	Airswap.io	BarterDEX	Samsung
Exchange assets	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Immutable solution	No	No	No	Yes	No	No	?	Yes
Private key on device	No	Yes	No	Yes	?	Yes	Yes	Yes
Cross chain Samsung swap	No	No	No	No	Yes	No	Yes	Yes
Decentralised orderbook	No	No	Yes	No	Yes	No	Yes	Yes
User friendly interface	Yes	No	Yes	Yes	Yes	Yes	No	Yes
Banking card acceptance	No	No	No	No	No	No	No	Yes
Instant centralized exchange	Yes	No	No	Yes	No	No	No	Yes

UI Preview

Samsung Wallet is created to make day-to-day cryptocurrency usage more secure while bringing the best customer experience to our clients. Following are the example screenshots from the interface of the Samsung Wallet Alfa Version.

Current stage

As of now, Samsung Wallet is a functioning ecosystem. Company is profitable. Desktop application supporting:

1. Asset management for BTC, ETH, DCR, LTC and 200+ ERC20 Coins
2. Main net Samsung swap [exchange](#)
3. Exchange assets via instant exchange services (Changelly, ShapeShift)
4. Backup with 12 words passphrase

The product is available for download at www.SWCcoin.site.



SWC Coin

Samsung Wallet will issue own Coin, called the SWC (Samsung Wallet Coin). A strict limit of 100M SWC will be created, never to be increased. SWC will run natively on the Ethereum blockchain with ERC20.

1. Around 5.500.000 SWC are currently distributed among retail investors, advisors and airdrop/bounty hunters. 70% of these Coins belong to over 30.000 small holders.
2. No more than 4.500.000 SWC will be distributed during the next 12 months for Airdrop, Affiliate rewards and Market Making.
3. 25% of funds will remain in lockup until there's a professional investor demand. In case there's none, the funds will be released after 5 years.
4. 5.000.000 SWC (BEP2) + 5.000.000 SWC (ERC20) are reserved liquidity for BEP2 <> ERC20 swapping tool.

Samsung Wallet gives utility value for holders:

- Discount on exchange services.
- Discount on buying crypto with bank card.
- Extra features for trading desk service.
- Dedicated support managers.
- Payment for coins listing.
- Affiliate and bounty rewards.
- Stacking rewards for holders.

Glossary

Crypto asset - a digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets.

Private keys - a private key in the context of Blockchain is a secret number that allows crypto assets to be spent. Every Crypto asset wallet contains one or more private keys, which are saved in the wallet file. The private keys are mathematically related to all Crypto asset addresses generated for the wallet.

Addresses - an identifier of alphanumeric characters, that represents a possible destination for a Crypto asset payment. Addresses can be generated at no cost by any user of Crypto asset.

Cryptocurrency node, Full node wallet - any computer that connects to the Blockchain network is called a node. Nodes that fully verify all of the rules of Bitcoin are called full nodes. Full nodes download every block and transaction and check them against Blockchain consensus rules.

Blockchain explorer - a block chain browser (also called "block explorer") is a program or web site that lets users search and navigate a blockchain. Uses include: checking address balances, tracking coin transfer histories, watching for transaction acceptance, monitoring the network hash rate and other statistics.

SPV (Simplified Payment Verification) - a method for verifying if particular transactions are included in a block without downloading the entire block. The method is used by some lightweight Blockchain clients. Thin clients don't verify the preceding blocks, they use the number of confirmations (whether they are valid or not) as a measure of the likelihood of a block chain reorganization producing a new longer fork which excludes the transaction.

Full node wallet - a full node is a program that fully validates transactions and blocks. Almost all full nodes also help the network by accepting transactions and blocks from other full nodes, validating those transactions and blocks, and then relaying them to further full nodes. It's possible and safe to run a full node wallet to support the network and use its wallet to store your Crypto assets, but one must take the same precautions you would when using any Crypto asset wallet.

Orderbook - an order book is an electronic list of buy and sell orders for a specific security or financial instrument, organized by price level. An order book lists the number of assets being bid or offered at each price point, or market depth. It also identifies the market participants behind the buy and sell orders, although in some cases participants choose to remain anonymous (most likely for crypto markets).

BitTorrent protocol - a communication protocol for peer-to-peer file sharing ("P2P") which is used to distribute data and electronic files over the Internet.

Order - in means of the current document an order is an investor's declaration of willing to purchase or sell a crypto asset. Orders are typically placed over the phone or online. Orders fall into different available types which allow investors to place restrictions on their orders affecting the price and time at which the order can be executed.

Trade - trade is a basic economic concept involving the buying and selling of goods and services, with compensation paid by a buyer to a seller, or the exchange of goods or services between parties.

Taker - a taker is an individual or company that must accept prices in a market and takes liquidity from the makers. A Taker hits previously created order from the orderbook.

Injections - an exploitation of a computer bug that is caused by processing invalid data. Injection is used by an attacker to introduce (or "inject") code into a vulnerable computer program and change the course of execution. The result of successful code injection can be disastrous, for example by allowing computer worms to propagate.

Signature - a mathematical scheme for demonstrating the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity).

Seeding - an uploading of already downloaded content for others to download from. A peer, a computer that is connected to the network, becomes a seed when having acquired the entire set of data it tries to download. This data consists out of small parts so that seeds can effectively share their content with other peers, handing out the missing pieces. A peer deliberately chooses to become a seed by leaving the upload task active when content is downloaded.

Byzantine consensus - a dependability of a fault-tolerant computer system, particularly distributed computing systems, where components may fail and there is imperfect information on whether a component is failed. In a "Byzantine failure", a component such as a server can inconsistently appear both failed and functioning to failure-detection systems, presenting different symptoms to different observers.

Validator - a special role for active consensus participants maintaining consensus in Byzantine networks. While not all the nodes in the blockchain network may be actively involved in the consensus algorithm Validator nodes do.

Blockchain oracles - an application for a delivery of data to the blockchain and delivery of the data itself.

Market price - current price at which an asset or service can be bought or sold. The economic theory contends that the market price converges at a point where the forces of supply and demand meet.

Network commissions - a fee that spenders may include in any Blockchain transaction. The fee may be collected by the miner who includes the transaction in a block.

ERC20 (223) Coins - a technical standard used for smart contracts on the Ethereum blockchain for implementing Coins. It defines a common list of rules that an Ethereum Coin has to implement, giving developers the ability to program how new Coins will function within the Ethereum ecosystem.

OTC deals - crypto assets traded in some context other than on a formal exchange such as the Poloniex, Binance, Kraken. The phrase "over-the-counter" can be used to refer to Crypto assets that trade via a dealer network as opposed to on a centralized exchange.

Smart contract - a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible.

KYC procedure - the Know Your Client form is a standard form in the investment industry that ensures investment advisors know detailed information about their clients' risk tolerance, investment knowledge and financial position.

KYC forms protect both clients and investment advisors. Clients are protected by having their investment advisor know what investments best suit their personal situations. Investment advisors are protected by knowing what they can and cannot include in their client's portfolio.

