- 1

BITSOAR

SoarSmartBridge

Feb. 2018

Contents

Blockchain in the Fourth Industrial Revolution

The basis for creating the cryptocurrency, called Bitcoin, is the Blockchain. The infrastructure, utilizing the encryption technology and distributed network technology, has meanwhile proven the fact that the 'safe and transparent online trading book can actually be operated.'

In addition, many experts have predicted that the Blockchain would be a destructive technology which could shake the global market. Just as the Internet has emerged, the businesses, like Netscape and Yahoo, have come out, and then, the services, like search engines, e-commerce, e-mail and the like, have appeared.

On whether the data sent by other people is trustworthy, all participant taking part in a distributed network, called the Blockchain, authenticate this transactional information. Accordingly, there is little possibility of forgery and falsification, and transaction details can be shared transparently. In addition to it, it is useful in that it may utilize much less computing resources, compared to the existing cases. At the moment that AI and IoT are connected to the actual business, when a variety of information is exchanged between objects or when payment is made automatically, the infrastructure of block-chain is expected to play the most key role.

Status of Blockchain Technology

The Blockchain technology was originally designed as a Public Blockchain or Public Distributed Ledger in which anyone could join the network. However, as Bitcoin may prove, the Public Distributed Ledger has several technical and empirical problems. Especially, there are various shortcomings: that it is necessary to put a lot of resources to maintain and manage the network in which a

number of unspecified people participate; that the internal information related to the transfer is transparently disclosed; that it has a very slow processing speed; anonymity of trader; etc.

For this reason, the Private Blockchain technology, through which the distributed network is composed of only the limited number of participants centered on the global financial industry, is standing out. It is because that even through it does not have to consume huge computing power like the Bitcoin, the strength of Blockchain network could be utilized which ensures network stability, while automatically handling the transaction and settlement in real-time. The Private Blockchain, also referred to as the licensed distributed ledger, seems to enable more efficient operation, while simultaneously solving a variety of problems that the existing Public Blockchain has.

Outline of BITSOAR

BITSOAR will be composed to be used in the encrypted settlement structure for payment and settlement that integrated the service area for all payments into one application and in the logistics platform for stamps on the distribution and commodities. It is a global mobile solution, based on the geographic location, payment and settlement module gateways, and the synergy effect of Blockchain.

(+ Smart contract technology)

BITSOAR is ready for the explosive growth in the global scale and market share. (+ Smart contract technology + payment + product certification)

The service will be expanded to the whole world, and firstly, the off-line store has already been successfully launched in Ho Chi Minh City, Vietnam.

BITSOAR has offices in ZUG (Switzerland), Singapore (Singapore), Vietnam (Ho Chi Minh), Indonesia (Jakarta), and Hong Kong (China), and we have organized a team of outstanding professionals who are developing the businesses globally.

Bitcoin has given us the Blockchain, Ethereum a smart contract, and Altcoins its own unique characteristics. Here, it is necessary for us to discuss the services for general investors, not as speculating tools of traders.

We all know that wonderful and brilliant Blockchain technology would bring us great wealth. However, BITSOAR does not think of such technologies as the "everything in cryptocurrency" or the "cryptocurrency designed for investors for just one purpose".

The current highly exaggerated cryptography capabilities have no profit potential in the future. Instead of relying on cryptography capabilities, the BITSOARs are developing the best Blockchain technology in order to extend the range of services that SSB's structure (SmartBridge) can provide, After implementing it on the SSB core via the SoarSmartBridge, we may use these connections and multipurpose data fields to configure new features, providing important services to consumers.

The examples of technologies that the SoarSmartBridge integrates into the SSB core include the selective private transaction, such as InterPlanetary File System (IPFS), InterPlanetary Database(IPDB - if available), and InterPlanetary Linked Data (IPLD); and the additional technologies which could appear potentially, such as web torrent without a server, like potentially additional technologies [1a], Tendermint verification of Practical Byzantine Fault Tolerance (PBFT)[1b], or Web2web [1c]. Along with additional technical information, SoarSmartBridge may provide the additional white papers for general upgrades over the SSB platform.

The main purpose of BITSOAR is simple. It is to increase the consumer selection by focusing on two key areas: rapid security core technology and practical services for real users.

- Initial generation of Bitcoin: Jan. 3, 2009 (Reward of 50 BTC)

- First half-life: Nov. 28, 2012 (Reward of 25 BTC)

- Second half-life: Jul. 10, 2016 (Reward of 12.5 BTC)

- Third half-life: Expected on Jul., 2020 (Reward of 6.25 BTC)

And the Bitcoin has another feature that it is being operated very transparently to the extent to be second to none of any other financial system in the world, rather than anonymously, by introducing the decentralized system, called a distributed ledger. In other words, anyone can view details of transactions not only of mine but also of others through the distributed ledger.

Necessity for BITSOAR

Bitcoin is an innovative cryptocurrency based on the Blockchain, but it biggest disadvantage is that it has less stability in that there is no actual trading, legal device, and control subject. Especially, in the general public, it is very complicated and difficult to safely store and use the cryptocurrency .

BITSOAR is an advanced cryptocurrency that is newly created in order to resolve the disadvantage of the low level stability and complicated and difficult currency usage of Bitcoin. Through this, BITSOAR will further improve the technical and monetary value of Bitcoin. ARK is not just a simple cryptocurrency. It is an ecosystem for the mass adoption of cryptocurrency.

By building the SSB platform on top of a highly secure core Blockchain, integrating key distribution technologies, and developing a use case to surely spread the capabilities of the SSB network, the BITSOAR's employees will provide an overall user-friendly platform that increases user adoption of Blockchain technology. Utilizing and integrating these technologies, the BITSOAR's ecosystem will adapt to all new challenges.

Through the integration of use cases, BITSOAR will bring consumers to block-chain technology, and will be able to develop successful consumer websites, products, and logistics networks, to improve general knowledge on the cryptocurrency industry.

Development Policy of BITSOAR

BITSOAR is a cryptocurrency developed by inheriting as it is the structural features of an incredibly perfect and stable Bitcoin. And in order to make BITSOAR used safely and conveniently, the BITSOAR platform will be additionally developed.

The total amount of BITSOAR to be issued is 3,980,000,000 BSR.

Since the issued amount of BITSOAR is predetermined, there is hardly the cases that the price value would decline after the inflation ends and the peak moment passes.

BITSOAR's participants are foundations, operators, miners, and users.

• The foundation is responsible for establishing and disseminating BITSOAR's development and operational policies. Here, the goal of the policy is to make a set of rules that can stimulate the value increase of BITSOAR and activate the transaction.

• Operators are responsible for monitoring and identifying whether they comply with BITSOAR's development and operational policies. In particular, it also plays a role of listening to customer complaints, handling inquiries, and creating and publishing reports on them.

• The miner plays a role in maintaining the BITSOAR system and receives a coin as a reward for this.

• The user is a person who actually uses the BITSOAR system. The user can purchase a coin, and send or receive coins, through the BITSOAR system.

BITSOAR's Specification

• Coin name: BITSOAR COIN

• Coin symbol (unit): BSR

• Total: 3,980,000,000 units (pre-mining of 3.68 billion units)

• Mining type: 300 million

• Coin type: PoW

• Hashing algorithm: X11

• Transaction rate: 10 TPS (600 TX per minute)

• Block size: variable (1MB - 4MB)

• Block time: 600 seconds (10 minutes)

• Number of block rewards: 50 units

• Number of blocks: 144 units

• Half-life: 1 year

- Community: including pool stack and web developers, network engineers, hardware specialists, financial managers, musicians, traders, social media promoters, and business owners, a diverse group of people and technology groups cooperate to realize the visions shared by BITSOAR's participants.

- Basic Token: It is protected by the cryptographic Blockchain network similar to Lisk and Crypti, which run on the Delegated Proof of Stake (DPoS) Consensus Algorithm. BITSOAR DPoS provides a newly adopted voting system, incorporating more improvements than the previous implementation for DPoS.

- Blockchain set connected via SoarSmartBridge: In order to improve the capabilities of the SSB platform, BITSOAR uses the SoarSmartBridge to connect useful and exclusive Blockchains. This SoarSmartBridge will support the communication between verified bridge Blockchains which can perform tasks and advanced functions. BITSOAR will use the SoarSmartBridge to connect many popular Blockchains and finally, can create an integrated bond among the various ecosystems. For example, the first Blockchain to which BITSOAR will connect is as follows:

There are Bitcoin, Ethereum, Lisk, integration of other companies' anonymous networks, one or more exclusive game economy tokens (codename: S***** [Ticker: AR ***]), and a number of bridges that link existing Blockchains with future new Blockchains.

- Security: As understanding that the security is an important concern to everyone, we ensure a core of security that the encryption and security principles are integrated throughout the life cycle of the overall development and they surely meet users' needs and expectations. Through the continuous risk analysis and recurrence penetration testing of internal problems, a system will be provided that meets the high standards required in this type of environment.

- Privacy Protection Policy: The anonymous network integration of SSB will provide SSB users with optional personal information when sending SSB transactions to all services developed for the SSB platform. The anonymization service may potentially be provided by other company's technology integration partnerships.

- Self-supporting environment: BITSOAR has a mission to make consumers aware of the points they are using but are not aware of, and to have the Blockchain technology easily used by consumers. We not only develop tools to connect virtual reality with the reality, but also provide unique services that consumers want to purchase by using SSB. BITSOAR develops additional platforms and services that benefit from SSB technology to provide online and offline revenue

streams for the SSB platform, to encourage consumer participation and at the same time, educate the block-chain technology, and to add value to SSB cryptocurrency by researching and developing new and exciting ways. BITSOAR grows by integrating the sales flow into our project, and can provide more special services than those for users' selection.

Additional information is provided in the Appendix section at the end of this white paper. And

(Appendix 1: SSB is … (content.))

(Appendix 1.1 Use cases)

(Appendix 2: Core of SSB Card Sales Network)

BITSOAR Hashing Algorithm

The hashing algorithm for BITSOAR is X11. X11 is a much more sophisticated algorithm than SHA256, preventing the concentration of hashing power by dedicated diggers. X11 is a revolving-type hashing algorithm, materialized by sequentially applying 11 different hashing algorithms. The 11 algorithms involved in this are blake, bmw, groestl, jh, keccak, skein, luffa, cubehash, shavite, simd, and echo.

Typical coins using X11 are as follows:

BITSOAR : Technical Details

This section briefly outlines the technical aspects of the BITSOAR Blockchain.

BITSOAR is a blockchain of cryptocurrency derived from Lisk, Crypto, and BitShares, which has unique differences and improvements in the DPoS consensus algorithm. This code association will provide the future simplified interactions between other block-chaining systems that use BITSOAR and DPoS as a consensus. This homogeneous code base can provide service connections in the form of Lisk blockchain applications, and can also offer other additional systems supplied by the block-chain manager.

Delegated Prood of Stake(DPoS)[2]

BITSOAR uses the DPoS consensus system, which was first introduced in Bitshares.

This consensus algorithm was designed to eliminate the problems associated with Proof of Work (PoW), that is, the centralization of computation power and the real world energy waste which is exponentially growing. It is not fully distributed because it relies on the consensus by a fixed number of elected representatives, but ensures better distribution than Bitcoin. The realization of consensus algorithms will have been improved over time and to develop into an optimal consensus system.

The technical description of the BITSOAR Blockchain is as follows:

- DPoS(Delegated Prood of Stake)

- BITSOAR active forging delegates.

- The representative (witness) elected by the voting mechanism built in DPoS

Inflation rate over time (ETH and LISK for comparison)

- 8 second block time

- Reducing the block time through future core upgrades.

- 25 transactions per block

- Increased through soft forks as needed.

- Routing table

- SmartBrige data fields for customized use and bridging Blockchains

BITSOAR network use will be extended to main credit card networks through major core upgrades, For example:

- Increasing the number of active forging delegates (witnesses)

- Increasing the block size to include more transactions

- Materializing the testnet of prior-approved PBFT block concept [codename: TwinChain]

- Routing table that minimizes hops (skips) between nodes when the block is broadcasted

- Mining including BITSOAR Uncles

* Uncles are stale blocks, ie with parent that are ancestors (max 6 blocks back) of the including block.

(Source: https://github.com/ethereum/wiki/wiki/Mining#mining-rewards)

Two versions of the node software are used to run the SSB core.

- Relay node: It is a node with full API functions that serves as a feature-rich light client backend. In the relay node, the transaction fees are not charged and it can not forge ARK blocks.

- Mining node: It is a node with the reduced API functions, which can reduce the potential exposure to potential DDoS attacks which can occur on SSB platforms. The forging node can forge BITSOAR and receive transaction fees.

Including desktop clients (Windows, MacOS, and Linux) and mobile clients (Android and iOS), an official light client is provided for network access just before the main net starts. The network itself does not use the graphical user interface by default. All SSB accounts can be created offline and managed free of charge on a single device (computer, mobile phone, embedded ARM, and IoT).

BITSOAR transaction

In the BITSOAR system, all transactions contain a digital signature per transaction, also including a public key for verifying this digital signature. The following figure illustrates how to use digital signatures in BITSOAR transactions.
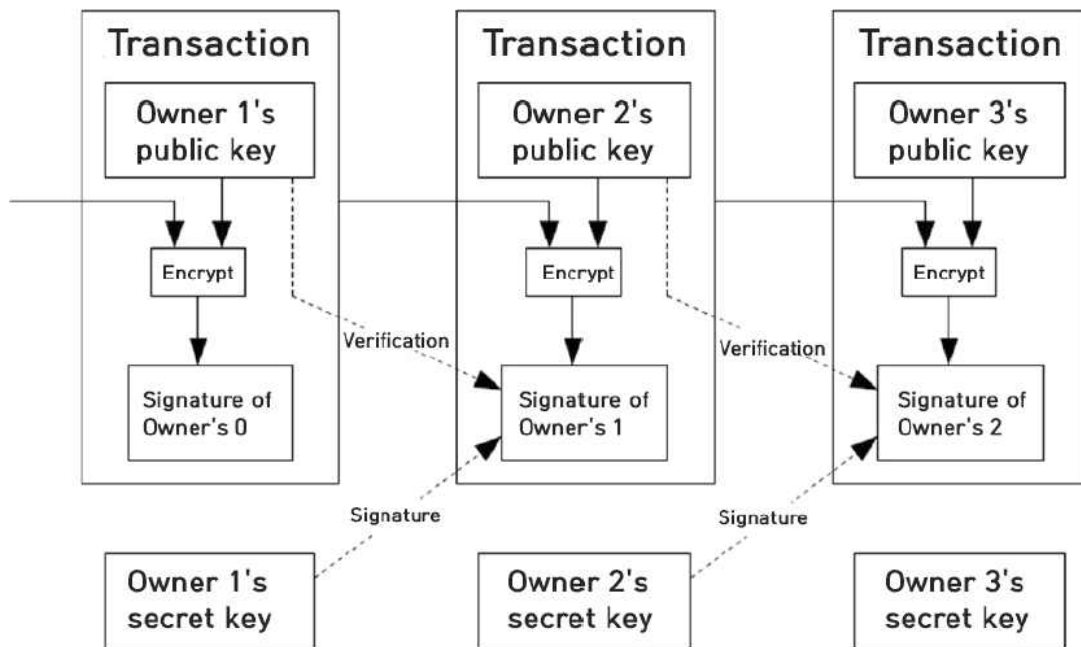
In the Blockchain in the BITSOAR system, all transactions issued are stored, and each transaction contains a set of digital signature and public key. Thus, all participants in the BITSOAR system can sequentially verify all transactions performed on the Blockchain in the past. If you verify the digital signature of a transaction, you can see the followings:

- Whether a third party has forged or tampered with transaction contents

- Whether a third party has performed the transaction through the ways, such as stealing and the like

- Whether the legitimate owner of the coin has performed the transaction properly

To issue a transaction, you will need a key pair of public and private keys. To create a key pair of BITSOAR, the key length should be 256 bits or more using an algorithm called Elliptic Curve Cryptosystem (ECDSA). The advantages acquired by using the Elliptic Curve Cryptosystem are that the same degree of encryption strength as other methods, such as RSA, ElGamel code or the like can be realized by using shorter keys, and as a result, it can make the processing performance

improved.

Time Stamp Server

The BITSOAR system starts from a time stamp server. The time stamp server works in the way to have a hash for the block of each item that should be time-stamped and then to publish the hash to the other nodes. It's like a newspaper or Usenet Post. The time stamp proves that the data that entered the hash clearly existed at that time. Each time stamp has a hash including the previous time stamps, and creates chains, thereby enhancing the safety of previous time stamps.
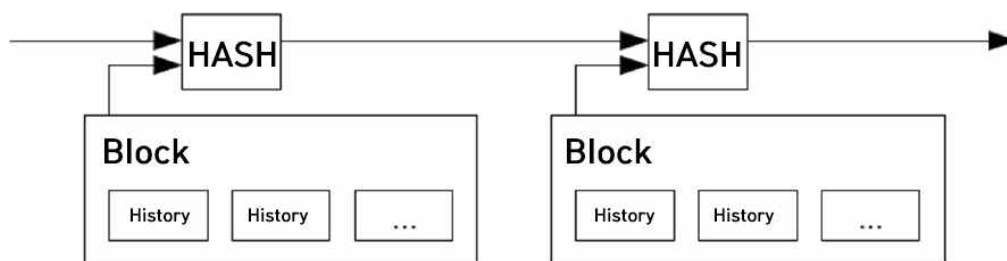
Proof of Work

In order to materialize a distributed time stamp server based on P2P, the BITSOAR system will require a work proof system similar to Adam Back's Hashcash, rather than the methods, such as a newspaper or Usenet post. The proof-of-work acts a behavior detecting whether the bit value of hash starts with zero, when it had been hashed in the same way as SHA-256. On average, the tasks grow exponentially depending on the number of 0 bits, and the verification can be done easily by performing a single hash.

To configure the time stamp network, the BITSOAR system implements a proof-of-task that increases the temporary token (nonce) in the block until it finds a value that can generate a hash containing 0 bits. Once you have done the proof-of-work by utilizing the CPU's resources, the block has no way to change anything, other than to perform the proof of work again. The blocks created subsequently are connected, in the form of chains, to the previous block, and then, you will have to work again on all the connected blocks which has been subsequently created, in order to change one block.
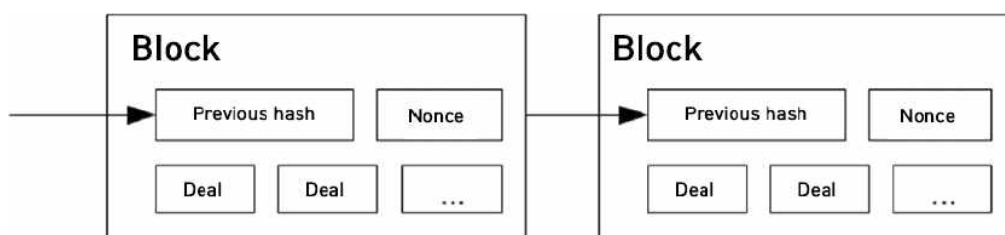
The proof-of-work can also solve the question of "how do you know which chain is the chain in which many nodes have judged to be correct?" If that multiple judgments are based on one vote cast per IP, it can be overturned by someone who has been assigned many IPs. Thus, the proof of work is inevitably progressed in a way of a single vote per CPU. Multiple judgments are represented by the longest chain in which the greatest effort of work proof was put.

If multiple CPU resources are controlled by honest nodes, the chains controlled by those honest nodes will become longer at the faster rate than any other competitor. To modify the past block, you need to perform a proof-of-work again on that block and all blocks that follow it, which must exceed the length of the longest node. We will show the probability that a slow attacker trying to catch up with a longer chain is exponentially weakened as the block is added in a later chapter.

Over time, the hardware speeds up, and to cope with the growing number of nodes participating in the network, the difficulty of the proof of work is

determined by the moving average according to the average number of blocks generated per hour. The faster the block creation speed, the more the difficulty increases.

SoarSmartBridges

The SSB platform does not directly support Sidechains or Decentralized Apps (dapp) databases. Instead, the mechanism for connecting the Blockchains is provided through the connecting fiunction built-in to the SSB core. This Blockchain can send and receive trigger function notifications and information data via the basic SSB network through the SmartBridge(s) and coded readers developed as the customized forms. SmartBridges may also be used to connect the "centralized" services. For example, all users can listen to the SSB network for specific triggers within the SmartBridge via Encoded Listeners, making the developed autonomous system enabled to work on its behalf. Encoded listeners are developed by the connection Blockchain manager, but BITSOAR provides a Rapid Deployment Engine that helps generate these encoded listeners.

Through the bridge Blockchain, BITSOAR can create a bridge Blockchain system, like a microloan connected to a Blockchain. In this Blockchain, those who need microloans can be connected with those who can help.

The worldwide lending, payment and transfer processing for BITSOAR is handled simply by combining the online/offline transmission hardware with the services that allow reimbursement from many Altcoins. BITSOAR may connect via SmartBridge. The profiles and service classes are stored and processed using IPDB (future integrated) with a software platform for discovery.

What is SmartBridge?

Let's imagine SmartBridge as a transactional unit. This information can be transferred in a transaction to another Blockchain or service, which can be directly

noticed from another Blockchain or service (via the secondary listener).

For example:

- Server A sends the SmartBridge fields and SSB transactions filled with commands, '2 Ethereums will be sent to an account of 12341234'.

- Server B receives these transactions, reads the SmartBridge field, confirms the amount transferred, and if it is correct, it generates a transaction and sends it 2 Ethereum accounts of 12341234.

Reward Tiers for SSB Token Transaction Participation

- If the token transaction successfully reaches at least 2.000 BTC, ARK Crews would like to congratulate all token traders of 10 BTC or higher by offering NFC rings (selectable in sizes and colors) which could be paid, with a BITSOAR trademark for limited edition. Participants with 20 BTC or more transactions will receive 3 limited edition BITSOAR rings for their families.

- Participants who have traded more than 50 BTC will be entitled to order an additional plastic smart card and station battery charger in addition to the rewards for participants more than 20 BTC. For the pre-orders, a benefit, called a free lifetime service, will be given through The Plastic Company. In addition, the purchase price will be charged after the Plastic pre-ordering step is completed. All deliveries of plastic or NFC rings will be handled by the relevant company.

The delivery date may change depending on the situation.

- Participants trading for more than 100 BTC will be VIPs who can have a lifetime access to the private ARK developing Slack, through which they can get additional information on new projects and updates, in addition to 50 BTC rewards. While VIPs are progressing the ARK service in which the alpha/beta testings are scheduled, they can discuss, interact, and comment on their experience with other VIP participants or developers. VIPs are VIP advisors to ARK

crews and do not receive any additional monetary rewards.

* Slack: It is a tool to improve productivity by providing concise but essential functions for those who need for collaboration. It is easy to simply understand it as a messenger (SNS).

(Source: http://nopdin.tistory.com/1849 [sentimentalist])

- Participants who contribute 420 BTC or more until the end of the token transaction will be entitled to receive the rewards of Accolades, Rare GM VIP Capabilities, all the benefits listed on other benefits (non-monetary), and lifetime access right to the Game Master VIP CARD, in addition to the rewards which those who have done the transaction of more than 100 BTC will receive.

Launching Test Net

The test net is open to the public during the token trading period. Furthermore, an initial test version for the Light Client (desktop and mobile) is also released for testing.

BITSOAR MASTER CARD

- Integration and testing of InterPlanetary File System [6] (IPFS)

- Preparing for the future integration of InterPlanetary DataBase[7](IPDB)

- Developing the smart bridge core code

- Blockchain penetration (Hacking) testing, debugging, and optimization

- Smart bridge and initially optimized block time test

- Removed by Lisk ports having application and API.

- 2017/01/31: Ark founders run all 51 nodes.

- 2017/02/01: The full node software is released and distribution, for light clients:

- Desktop: Windows, Mac OS, and Linux

- Mobile: Android and iOS

- 2017/02/06: The major Bounties start distributing to Bounty participants.

- The usage of ARK forging becomes available

- Official conversations with exchanges for adding ARK tokens.

- Releasing (withdrawing) residual funding funds of cryptocurrency traded at escrow

- Business Registration. We are currently speaking with lawyers from countries in the priority list.

- Ordering for NFC rings and Plastic Smart Card rewards.

- Official card design and hardware design for P2P transactions.

- Delivering NFC rings to eligible participants (March / April).

- Delivering the plastic smart cards to eligible participants (March / April).

- Integrating ARK anonymous network providing arbitrary anonymous transactions (March - May)

- Employing ARK developers for ARK core and service department.

- Building communities

BITSOAR - P2P Card network

This schedule will not change if at least 10,000 BTC is collected during BITSOAR-TEC period. Otherwise, it will be developed within a reduced scope. The BITSOAR card network will be designed and released for general usage (availability) in or before the fourth quarter of 2018. It is composed as follows:

- Researching, sourcing, and developing various smart cards / NFC materials

- Partnerships with manufacturers for NFC / wearable non-contact chips

- Designing, studying, and prototyping modular POS hardwares / softwares that can run on ARM systems.

- Sales and distribution of NFC wearable devices (2nd - 3rd quarter in 2019)

- Materializing pre-approved PBFT blocks for fork removal

- Implementation of SSB Forging Uncle to reduce latency and block time

- Code development for easily encrypted encoding audiences

- Research and development of new tools, systems, and services to expand the adoption of various programs (ASCH, IPLD, Web2Web, and others)

Network

The steps for operating the network are as follows:

1) New transactions are delivered to all nodes.
2) Each node aggregates new transactions to blocks.
3) Each node performs a work proof task to generate a block.
4) When a node finds a solution to the proof of work, the block is forwarded to all nodes.
5) Nodes accept a block if the transaction information on the block for which the proof of work was ended is valid and not redundantly used.
6) By connecting the accepted blocks to the chain and then, performing the task of creating the next block, the nodes implicitly express that they normally accepted blocks.

The following figure illustrates the two-separated Blockchain, which is automatically organized into a single Blockchain by the consensus algorithm.

Separated Blockchain (https://mastanbtc.github.io/blockchainnotes/consensustypes)
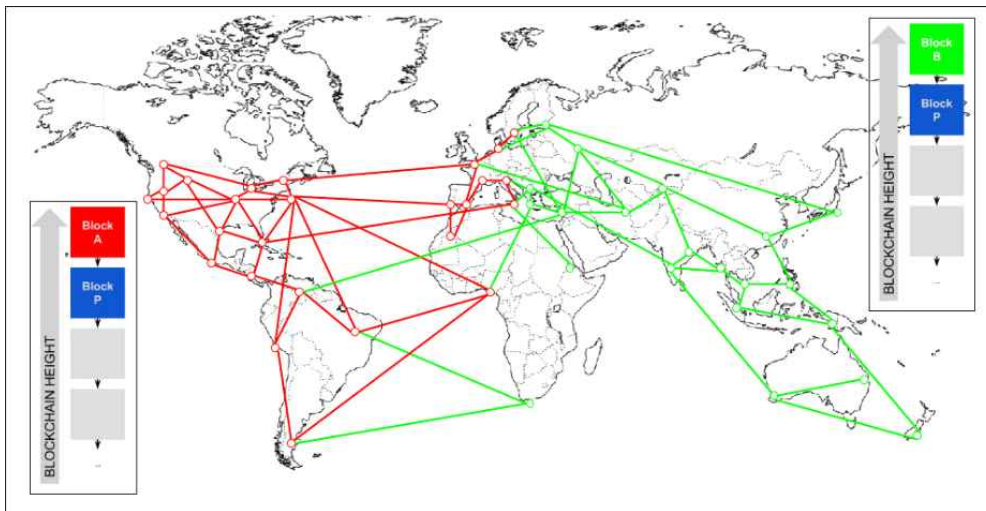
Nodes always think of the longest chain as the right chain, and work to expand the longest chain. If the two nodes find the answer to the proof of work at the same time and deliver the two blocks to all other nodes, nodes will receive one of them first, and the block which each node will first receive may be different. In this case, the nodes will accept the firstly received node as the longest chain and work on that, keeping the other block in case that it becomes longer. In this bifurcated chain, the length of one branch becomes longer as the next work proof is found. Then, the nodes that were working on the other node change their chain which they are going to work into the longer chain.

A new transaction does not surely have to be delivered to all nodes. As long as a new transaction is forwarded to more nodes, it will be put in a block before it gets longer. That is, it can be seen that this block transmission method is strong against message loss. If the node does not receive the block, when it receives the next block, the relevant node will recognize that the previous block has been lost and will request a block that has not been received.

Rewards

Conventionally, the initial transaction of a block is a special transaction that may launch a new coin owned by the creator of the block. Since there is no central institute issuing coins, this transaction adds an incentive for the nodes that support the network, and also provides a way to divide and distribute coins initially. Adding continuously constant amounts of new coins is similar to gold miners who spend money to add gold to the circulation.

In the BITSOAR system, it is CPU time and electricity that are consumed. The incentive can also be covered by transaction costs. If the output value of a transaction is less than the input value, the difference in value, then, is the transaction cost added to the incentive value of the block containing the transaction. Once the pre-determined coin number begins to circulate, the incentive is entirely converted to transaction costs, and the incentive is nothing to do with inflation.

The incentive can encourage the nodes to stay honestly. If a greedy attacker could utilize more CPU power than that of the entire honest nodes, the attacker is trying to steal people by stealing them, the attacker will have to choose one of two, whether to use that CPU power to steal people by stealing their payment costs or to utilize it to create a new coin. System attackers would have to find that it would be much more profitable to operate the system in accordance with these rules preferring themselves having more new coins than combining all the other coins.

Increasing Disk Storage

Once the most recent transaction of the coin is stored in a sufficient-sized block, the transactions consumed prior to that block may be discarded to save disk

storage space. In order to save this disk storage space without destroying the block hash, a transaction that only includes the root block in the block hash can be made into the MerkleTree. For the MerkleTree, the process of making two lower hashes into one repeats, finally creating one hash.
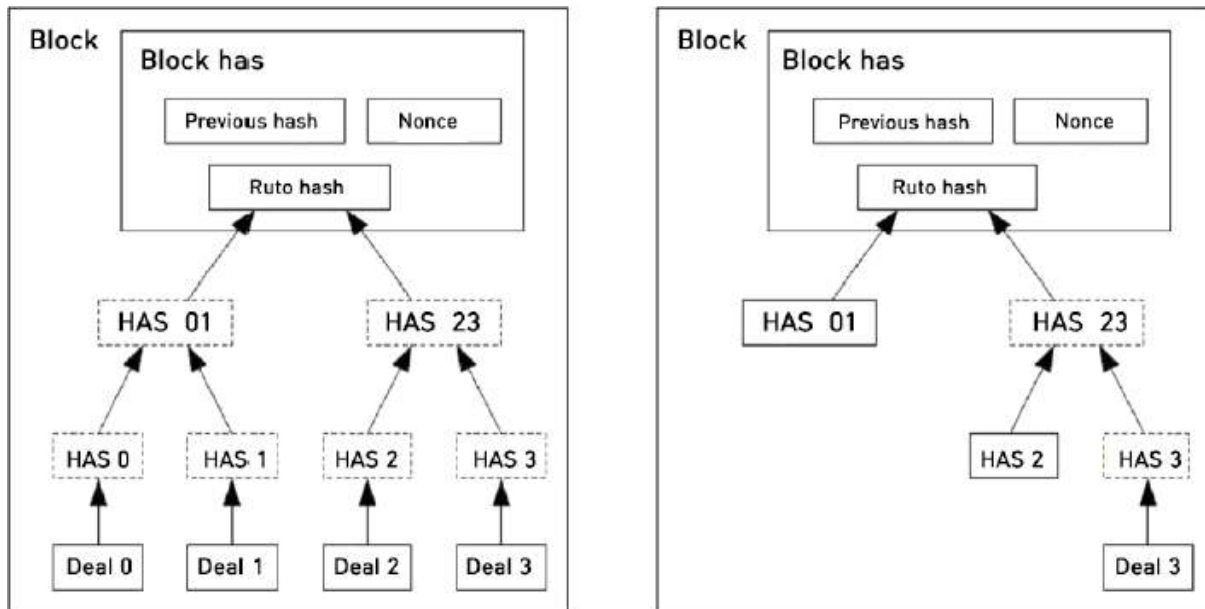
Simplified Payment Proof

It is possible to prove the payment without using the entire network node. All that the user has to do is to have a copy of the header block of the longest chain. The copy of the header block is obtained by querying other nodes until it is convinced that it has the longest chain and obtain the branches of the Merkletree connected with the block containing the desired transaction. Users cannot directly identify transactions themselves, but by placing the block containing the relevant transaction in the longest chain, it can be indirectly identified that the block has been received in the longest chain, followed by other blocks.

Longest Proof-of-Work Chain
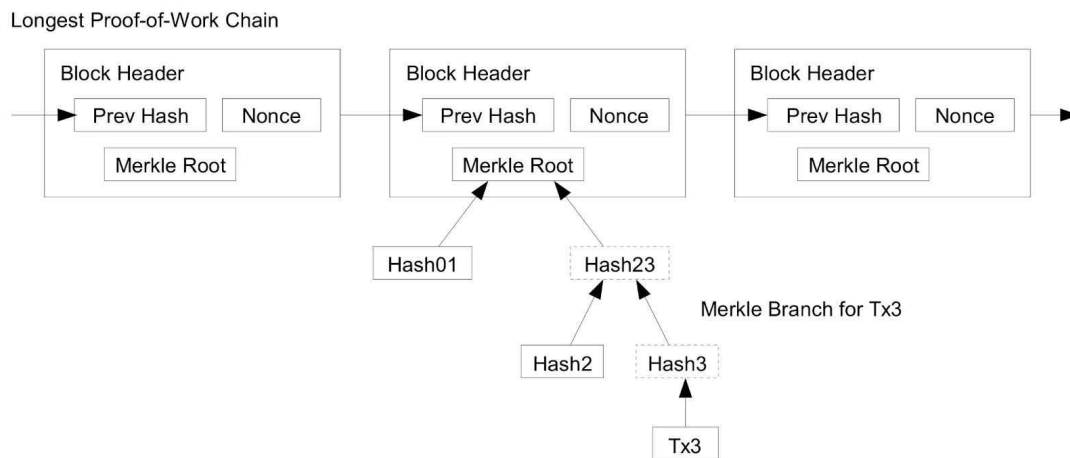
This proving method is reliable if the network is controlled by honest nodes, but if attackers have more dominant resources than honest nodes in the network, it is more vulnerable one. This simplified method is likely to allow nodes in the network to prove transactions for themselves, while having enough possibility to be deceived by transactions created by attackers if the attacker has the dominant resources over all other honest nodes in the network. One strategy for protecting the system from this problem is receiving warnings from them when the nodes detect an abnormal block, allowing the user's software to identify the abnormal part after receiving the entire blocks and the warned transactions. The business operators receiving frequent payments may still want to be more independent, and to run their own nodes for security and faster certification.

Combination and Splitting Value

Even though it is possible to treat a coin personally, it would be cumbersome to split the fund into cent units in a certain transaction, making them into separate transactions. In order to separate and combine values, a transaction will become to contain multiple inputs and outputs. Typically, there will be a single input by the previous large transaction, multiple inputs combined by small amounts of money, and a maximum of two outputs. Of these two outputs, one is payment, and the other, if any, would be the amount of money that is returned to the sender.
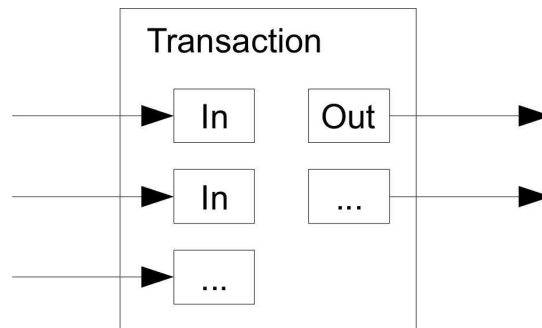
If a single transaction is subordinated to multiple transactions or their transactions are subordinated to much more transactions, the Fan-out of splitting and spreading them out is not a problem here. It is not necessary at all to extract a copy for a complete self-execution on the transaction history.

Privacy

The traditional bank model achieves a privacy rating by restricting access to relevant parties and trusted third party information. This model is excluded because of the need to publicly announce all transactions, but the privacy can still be maintained by blocking the information flow in other places. This is enabled by keeping the public key anonymous.

The general public can tell that someone is sending some money to other else, but there is no information on whom the transaction links. This is similar to the information rating published by the stock exchange, and in the stock exchange, the tape is recorded that records the time and size of individual transactions, but it does not tell who the parties interested are.
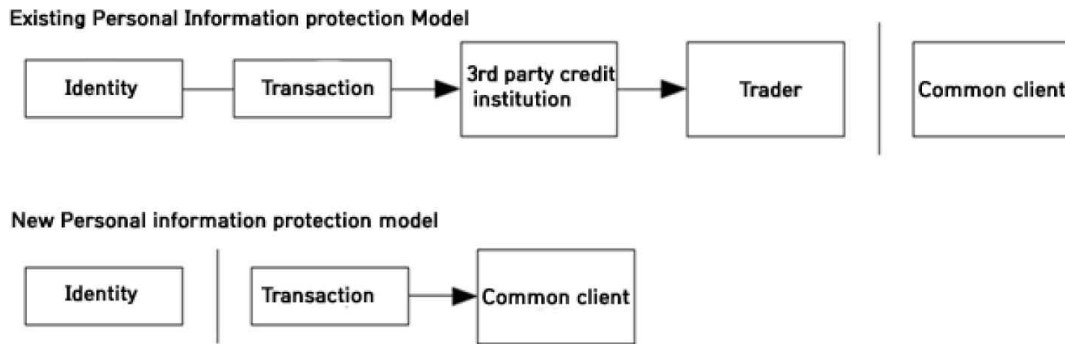
As an additional firewall, to prevent those parties from linking with the general owner, a new secret key pair must be used for each transaction. In multi-input transactions, some links are still inevitable, which inevitably represents the fact that their inputs are owned by the same person. If the owner of the key becomes known, there may be a risk that the links will make other transactions belonging to the same owner known.

Calculation

Let's consider the scenario of an attacker trying to create an alternate chain that is faster than the host chain. Even if this is the case, the BITSOAR system is also safe from any arbitrary changes, such as illegal coin creation or coin swindling. Nodes will not admit payments for invalid transactions, and in addition, honest nodes will never acknowledge the blocks containing them.

An attacker may attempt to change one of his own transactions in order to get the money back he recently spent. The competition between the honest chains and the attacker chains can be characterized by the Binomial Random Walk. A successful event is an honest chain that can be extended by one block by increasing the lead by +1, and the failure event also means a chain of attackers that can be extended by one block by decreasing the gap by -1.

The probability of catching up with an attacker from any particular deficit is

similar to the Gambler's Ruin problem. Let's assume that the Gamblers with infinite credit start from the state of deficit and maybe try the infinite challenges in order to reach Breakeven. We can calculate the probability that an attacker reaches a breakeven point, or that an attacker catches up with an honest chain, as follows:

$$q_z = \begin{cases} 1 & if\ p \le q \\ (q/p)^z & if\ p > q \end{cases}$$

In the formula above, 'p' is an honest node, 'q' is an attacker node, and 'q_z' is the probability to be found by an honest node. If an Assumption of p> q is given, the probability decreases exponentially in the block numbers the attacker has to catch up with. On the contrary possibility, if the attacker does not have a good fortune early on the possibility, the chance of the attacker becomes small enough to disappear because he drags further behind.

Now, let's discuss how lond the recipient of new transactions needs to wait until we are fully confident that the sender will not be able to change the deal. We assume that the attacker is the sender who wants the recipient to believe that the attacker has paid himself for a while, and then, he return the payment to himself after some time has elapsed. When this happens, the recipient will receive a warning, but the sender expects such event will happen very late.

The recipient creates a new secret key pair, and also sends the public key to the sender just before his signing. Until an attacker is lucky enough to have a chain much ahead of sender and executes the deal at that moment having the chain, this prevents the sender from preparing a chain of blocks before continuously doing such an operation. Once a transaction is dispatched, the dishonest sender will secretly begin the computation task in a parallelled chain containing an alternate version of his own transaction.

The recipient waits until the transaction is added to the block and the z blocks are linked to the block thereafter. He does not know the exact quantity the attacker has progressed. However, assuming that honest blocks take an average estimated time per block, the potential regression curve of the attacker would be the Poisson Distribution with the Expected Value as follows:

$$\lambda = z \frac{q}{p}$$

Now, to calculate the probability that the attacker is still catching up, we multiply the Poisson Density function by the amount of progress that can be made by the probability that the attacker can catch up from that point.

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \left\{ \begin{array}{ll} (q/p)^{(z-k)} & \textit{if } k \leq z \\ 1 & \textit{if } k > z \end{array} \right\}$$

The formula for preventing the formula from being counted as infinite is as follows:

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)} \right)$$

This part is materialized in C language, which is as follows:

```
1
2    #include <math.h>
3
4    double AttackerSuccessProbability(double q, int z)
5    {
6      double p = 1.0 - q;
7      double lambda = z * (q / p);
8      double sum = 1.0;
9      int i, k;
10     for (k = 0; k <= z; k++)
11     {
12            double poisson = exp(-lambda);
13       for (i = 1; i <= k; i++)
14       poisson *= lambda / i;
15       sum -= poisson * (1 - pow(q / p, z - k));
16     }
17   return sum;
18   }
19
```

If executing some results, we can see that the probability decreases exponentially in z.

Value Rising Strategy BITSOAR

The BITSOAR Foundation should announce and implement strategies to support or stabilize the value of BITSOAR, or prevent further declines in it.

First, BITSOAR's stabilization/smoothing strategy is as follows:

- Acquiring some part of BITSOAR by the foundation
- Strengthening the positive (+) announcement activities for stabilization

Second, BITSOAR's Boosting strategy is as follows:

- Conducting paid-in capital increase and capital increase without compensation
- Strengthening positive (+) announcement activities for boosting

Third, BITSOAR's investment strategy is as follows:

- Investing in coin development
- Investing in public interest and social welfare organizations
- Investing in opening branches and franchising
- Investing in coin activation

The BITSOAR Foundation will continuously strive to increase the value of coin and conduct our expanding strategy.

Expanding Strategy of BITSOAR

BITSOAR is a coin designed to fit the digital industrial revolution, in which the 21st century fusion and compond businesses, represented by artificial intelligence, big data, Internet of things, shared economy, etc., can be actively incorporated. This platform advantage of BITSOAR will further maximize the value of BITSOAR. The followings are the APIs provided to support the IT business by BITSOAR.

- Providing 'coin API' to convert points to BITSOAR
- Providing 'DB interlocking API' that can be linked with various DBs
- Providing 'Exchange API' for operating our own exchange
- Providing 'Operational management API' supporting independent operation
- Providing 'Wallet API' for development of wallet app
- Providing 'test server' for the purpose of testing

BITSOAR is designed based on a flexible and strong architecture basis, and at the same time, it is implemented in modern languages, having very outstanding expandability. This feature is useful to easily integrating BITSOAR into various fields, which would lead the coin business successfully in the end.

BITSOAR Roadmap

The BITSOAR team was founded on October 15, 2015 and is a strong team that has led several projects.

| I. Establishment of coin team	II. Definition of coin specification
- Composing coin members - Conducting coin market research - Hosting the coin seminar - Drafting the white paper of coin	- Coin definition - Coin logo - Coin design - Blockchain design
III. Coin engine research	IV. ICO preparation and progress
- Coin mining module research - Coin transmission module research - Coin wallet module research - Coin certification module research - Coin management module research	- Creating ICO roadmap - Reviewing legally ICO - Preparing ICO presentation - Developing ICO token issuing system - Developing ICO login system
V. Developing coin engine - II	VI. Developing coin platform
- Coin mining module development - Coin transmission module development - Coin wallet module development - Coin certification module development - Coin management module development	- Transaction server development - Blockchain server development - Coin wallet development - Mining system development - Application system development
VII. Registration of coin exchange	VIII. Establishment of coin foundation
- Registration of GitHub source - Registration of mining service - Registration of Blockchain search service - Registration of API service	- Purpose of the foundation - Definition of main activities - Drafting budget - Preparation of policies

Establishment of BITSOAR Foundation

The BITSOAR Foundation is a non-profit organization that manages all information related to BITSOAR. The BITSOAR Foundation follows the following

procedure:

① Member recruitment ② Names and position ③ Representative information ④ Digital currency and bond/share issue information ⑤ Policies and regulations ⑥ Council meetings and guidelines ⑦ Board members and policies ⑧ Funds and accounting, ⑨ Supplementary regulations
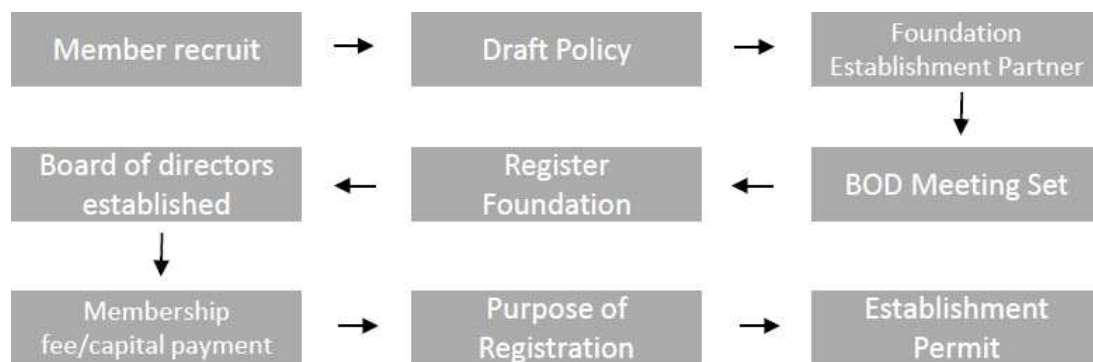
BITSOAR Foundation's mission

The BITSOAR Foundation intends to establish a systematic strategy to increase the intrinsic value of coins. Specifically, it is as follows:

- Establishing BITSOAR's Ho Chi Minh branchs in Vietnam

- Realizing rapid listing on the International Exchange

- Listing on various international exchanges

- Launching the global mobile wallet (supporting multi-languages)

- Establishing the global infrastructure (Russia, UK, Japan, China, Vietnam, Brazil, Mongolia, Paraguay, and Thailand)

- Releasing a VISA card available for global payment

- Opening 1,000 branches in China and Vietnam

- Scheduled to install ATM in China and Vietnam

BITSOAR Team

The members who plan and promote BITSOAR are as follows:

	Sangdong Kim, CEO : Majored in Computer Science in Inha Univ., Korea. He has served as a representative of leading IT companies so far, and awarded the Minister prizes from the Minister of Information and Communication and the Ministry of Science, ICT and Future Planning.
	Attila Ferencz, Rumania, CIO : After his doctoral degree in computer science in Cluj-Napoca Univ., Rumania, he served as a professor for many years. Since 1999, he has been working as a senior researcher at Samsung Electronics R&D Center and KT Research Center, and he is currently working as a cryptocurrency expert.
	Sergei Kuratov, Russia, CTO : He is an IT professional with 20 year career, currently working as an expert on hardware and software architecture for large-scaled web services in USA, Israel, Japan, Korea, China, Spain and others.

Conclusion

BITSOAR can be used completely for business purposes, as well as exchanged domestically and internationally. Also, when registered in the cryptocurrency exchange, the general users can actively buy and sell the coins. It provides a chance to synchronize with various businesses, so can bring reasonable benefits.

In addition, the BITSOAR Foundation and its member companies will do their best to help investors gain substantial and stable returns.

References

01. Alt chains and atomic transfers:
    https://bitcointalk.org/index.php?topic=193281.msg2224949#msg2224949
02. B-money: http://www.weidai.com/bmoney.txt
03. Bitcoin, A Peer-to-peer Electronic Cash System: https://bitcoin.org/bitcoin.pdf
04. Colored coins whitepaper: https://tinyurl.com/coloredcoin-whitepaper
05. Decentralized autonomous corporations, Bitcoin Magazine:
    https://tinyurl.com/Bootstrapping-DACs
06. Ethereum: https://ethereum.org.
07. Ethereum Merkle Patricia trees:
    https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-Patricia-Tree
08. Ethereum RLP: https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-RLP
09. GHOST: http://www.cs.huji.ac.il/~avivz/pubs/13/btc_scalability_full.pdf
10. Intrinsic value: https://tinyurl.com/BitcoinMag-IntrinsicValue
11. Jae Kwon. Cosmos, A Network of Distributed Ledgers:
    https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md
12. Joseph Poon and Tadge Dryja, Lightning Network:
    https://lightning.network/lightning-network-paper.pdf
13. Mastercoin whitepaper: https://github.com/mastercoin-MSC/spec
14. Merkle trees: http://en.wikipedia.org/wiki/Merkle_tree
15. Mike Hearn on Smart Property at Turing Festival:
    http://www.youtube.com/watch?v=Pu4PAMFPo5Y
16. Namecoin: https://namecoin.org/
17. Patricia trees: http://en.wikipedia.org/wiki/Patricia_tree

18. Paul Sztorc. Drivechain - The Simple Two Way Peg: http://www.truthcoin.info/blog/drivechain/

19. Peter Todd. Tree Chains: https://github.com/petertodd/tree-chains-paper

20. Peter Todd on Merkle sum trees: http://sourceforge.net/p/bitcoin/mailman/message/31709140/

21. Raiden. Raiden Network: https://raiden.network/

22. Reusable proofs of work: http://www.finney.org/~hal/rpow/

23. Secure property titles with owner authority: http://szabo.best.vwh.net/securetitle.html

24. Golden Master and Branch whitepaper: http:/www.gmbcoin.org/gmb-whitepaper.pdf/

25. Simplified payment verification:
    https://en.bitcoin.it/wiki/Scalability#Simplifiedpaymentverification

26. Smart contracts: https://en.bitcoin.it/wiki/Contracts

27. Smart property: https://en.bitcoin.it/wiki/Smart_Property

28. StorJ and Autonomous Agents, Jeff Garzik: https://tinyurl.com/storj-agents

29. The Bitcoin Model for Crowdfunding:
    https://startupboy.com/2014/03/09/the-bitcoin-model-for-crowdfunding/

30. Vitalik Buterin. Ethereum Sharding FAQ: https://github.com/ethereum/wiki/wiki/Sharding-FAQ

31. Zooko's triangle: http://en.wikipedia.org/wiki/Zooko's_triangle