Trivechain 2.0 (TRVC)

Ji Sheng Tan, Yee Chin Ang, Arpita Chopra and Kah Wai Chooi

Abstract— **The evolution of value transfer has gone from the basics of value transfer to smart contract. Trivechain is a public blockchain managed by Decentralized autonomous organization (DAO) with focus on bridging businesses to enter the new era digital age with implementation of blockchain-based technology and DApps (decentralized applications) with the help of (i) Direct Send, instantaneous transactions; (ii) Exclusive Send, privacy protection payment system; (iii) Trive-Governance, the decentralized autonomous organization that will shape and decide the future development of Trivechain; (iv) TriveStamp, a trust-less time-stamping proof of existence service; (v) TriveApp, applications can be built and transacted on the TRVC network ensuring that the application exist on a server-less state; (vi) TriveAsset, a platform for asset issuance with options to include metadata for the need of business logics;**

Proof-of-Work (PoW) and Proof-of-Stake (PoS) are two common validation method used in blockchain technology. Leveraging on the pro of both validation method, Trivechain is utlizing both PoW and PoS based validation method in a hybrid fashion to increase security and sustainability in blockchain. Block rewards are given to both PoW Miners and PoS owners through the Trive Masternode Network (TMN).

I. INTRODUCTION

Prior to year 2008, commerce on the Internet rely heavily on a financial institution, as there are no method yet existed which could render the requirement of trust obsolete. In turn, financial institutions then imposed transactions fees for its services as a mediator.These fees coupled with the fact that transactions are always reversible, causes small casual transactions to be impossible.

In year 2008, Satoshi Nakamoto proposed a peer to peer electronic cash system, namely Bitcoin making value transferring transaction possible [1]. The introduction of cryptocurrencies causes the role of financial institutions as a mediator in online transactions less significant. Blockchain technology along with the inception of Bitcoin is revolutionizing the way transactions are performed on the Internet. Bitcoin provides pseudonymous transactions in a public ledger, with a one-to-one relationship between sender and receiver. This provides a permanent record of all transactions that have ever taken place on the network [2]. Bitcoin is widely known in academic circles to provide a low level of privacy, although with this limitation many people still entrust their financial history to its blockchain.

The concept of proof-of-work in Bitcoin allowed decentralized consensus on a large scale network with no central authority achieving a total peer-to-peer transactions. However, due to the very nature of decentralization, the blockchain is inherently not private. This has obvious implications for users' personal privacy, as all transactions are traceable in the block chain. So, Duffield, E., & Hagan, K. [3] proposed the DarkSend protocol in the year 2014 that provides extensions to merge transactions together into larger anonymous transactions. Using regular nodes and elects a masternode among them to create the transaction in a decentralized fashion. In the year 2015, Darkcoin renamed and is now commonly known as Dash, Digital Cash.

Being able to transfer value by trusting entirely on a network of peers is becoming acceptable and started getting attentions. Dr Gawin Wood [4] began documenting his new concept of transaction based state machine known as Ethereum. Introducing the ability to execute codes that could change a state within the blockchain and fee calculation using gas instead of purely the size of the Input and Output UTXOs used by the Bitcoin. Ethereum begin with a genesis state and incrementally execute transactions to morph it into some final state. It is this final state which we accept as the canonical version of the world of Ethereum. The state can include such information as account balances, reputations, trust arrangements, data pertaining to information of the physical world; in short, anything that can currently be represented by a computer is admissible. Through the Ethereum protocol the reader may implement a node on the Ethereum network and join others in a decentralised secure social operating system. Smart contracts may be authored in order to algorithmically specify and autonomously enforce rules of interaction.

In this paper, we propose a series of improvements to Bitcoin, Dash and Ethereum resulting in a decentralized, efficient, flexible, scalable, strongly anonymous cryptocurrency, with tamper-proof direct sending of transactions and the ability to execute smart contracts with load distribution to on-duty masternodes. So, the load are equally distributed between the miners and the masternodes.

II. HYBRID VALIDATION METHOD

A. The Best of PoW and PoS

Trivechain is a hybrid system encompassing both concepts of Proof-of-Work and Proof-of-Stake to solve inherent issues pertaining to security and decentralization with sustainability and scalability in mind. In its initial stages, Trivechain will be a PoW centric coin where network circulation is increased through traditional mining and miners are rewarded with block rewards. A proven method for exponential growth in infancy stages where hashing difficulty levels are low and reward-to-work ratio is high.

As Trivechains value, network circulation and hashing difficulty increases, users are rewarded with coins through the PoS algorithm. Therefore, as traditional mining becomes less rewarding over time, a progression into PoS increases

sustainability as energy requirements of the network are significantly reduced.

Furthermore, this increases security against the vulnerabilities surrounding Bitcoin and PoW based cryptocurrency which is controlling more than 51% of the mining power in the network, known as the 51% attack [5]. As it becomes significantly more difficult to acquire 51% of all TMN and 51% of all mining power at the same time. as opposed to 51% of all mining power and exponentially more difficult as the value and circulation of TRVC increases.

B. X16R Proof-of-Work

Proof-of-Work is a concept in which a system which requires a feasible amount of work in order to deter malicious uses of computing power such as launching denial-of-service (DoS) attacks or sending spam mails [6]. Although it had already existed before Bitcoin, the coin became the first actualization of this concept on a large commercial scale.

Trivechain utilizes a digital distributed ledger technology known as a blockchain which serves as the foundation. The blockchain contains a record of all Trivechain transactions, assets transaction and other meta data which are arranged in sequential blocks, preventing any users from spending their holdings twice. In order to circumvent tampering or alterations, the ledger is publicly accessible and shared by all users, so a modified version would be easily detectable and rejected by other users.

Tampering with the ledger is detected through hashes, long strings of numbers that also serve as proof of work. Place a given set of data through a hash function (such as X16R), and it will only generate one hash. Due to the cascading effect, however, even a small change to any portion of the original data will result in a totally unrecognizable hash. Also, whatever the size of the original data set, the hash generated by a chosen function will always be the same length. The hash is a one-way function; it cannot reverse engineered to obtain the original data. It can only be checked to determine whether the data that generated the hash matches the original data.

The proof-of-work also solves the dispute of determining fair representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of- work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. The probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added. To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour.If they're generated too fast, the difficulty increases.

Every proof-of-work algorithm with the aim of preventing the existence of ASIC will fail because there is no absolute way of preventing it but there are ways to slow down the existence by making it harder to create such as using different types of algorithm.

The x11 is a common hashing algorithm that utilizes an unconventional approach also recognized as algorithm chaning. X11 contains all of 11 SHA3 candidates algorithm, where in the chain, the calculation of each hash is submitted to the very next algorithm. By adapting multiple algorithms, the chances of an ASIC being created for the currency is small.

Despite the complex chaining of hash algorithms, the D3 ASIC miner from Bitmain has made X11 mining with GPU and CPU not profitable. So, we will be using another type of hashing algorithm in Trivechain 2.0. To ensure that the hobbyists are able to mine the TRVC with Central Processing Unit (CPUs) and Graphics Processing Units (GPUs). Trivechain will continue to make changes to the hash algorithm as soon as the existence of ASIC for X16R.

C. Trive Masternode Network Proof-of-Stake

Proof-of-Stake (PoS) was a concept actualized to solve problems or shortcomings of the PoW method. The first of these problems is the energy expended for mining. The computing power required to carry out the cryptographic calculations only ever increases as the difficulty increases, thus consuming greater amounts of electricity. In the long run, this would be counterproductive to the health of a cryptocurrency as miners would have to sell substantial portions of their coins for fiat currency to foot the electricity bill, devaluing the price of the cryptocurrency.

The Proof of Stake addresses this issue by instead awarding mining power proportional to the number of coins held by a miner. Therefore, a PoS miner is limited to mining a percentage of transactions that is reflective of his/her ownership stake, unlike a PoW miner who utilizes raw energy (electricity). For example, a minor who owns 1% of a coin, will only be able to mine a maximum of 1% of all available blocks. This also greatly reduces the energy requirements of the network.

Another potential problem with the PoW system in the long run, is the potential for mining power monopoly. As the mining difficulty increases and block reward decreases, the amount of miners will undoubtedly decreases which then makes the network susceptible to a 51% attack. A 51% attack is when a miner or mining pool controls 51% of all the computational power of the network, and creates fraudulent blocks of transactions and validates them himself [5]. This effectively enables him/her to siphon large quantities of the coin from the network for himself.

However, with a PoS system, an attacker looking to gain monopoly of the network would have to own 51% of the cryptocurrency which only gets more difficult and expensive as the coin appreciates in value. Additionally, the greatest deterrent against such an attack is that a miner with a 51% stake in the coin would not have it in his best interest to

attack a network which he/she holds a majority share. Such an attack, would immediately devalue the currency and as such, he/she would be more incentivized to maintain a secure network.

1) Trive Masternode Network Operation: Only two types of messages are utilized for the activation of the Masternodes in the network- Masternodes information message and Masternode network message. Apart from these two, there are other messages for running ExclusiveSend and DirectSend. Masternodes are formed by depositing 10,000 TRVC to a wallet which will lead to the activation of the nodes, thus allowing it to multiply all across the network. A secondary backup key is then generated for signing all further messages. This key will lock the wallet while working on a standalone condition.

By using the secondary backup key, a cold mode is available on two different machines. The primary hot client submits 10,000 TRVC with the secondary backup key into the message. When the cold detects a message and the secondary backup key, the Masternode is activated. This will then deactivate the hot client and the 10,000 TRVC in the Masternode stands zero chances of getting attacked after activation. In the beginning, a Masternode sends a Masternode Information message across the network, stating:

- 10,000 TRVC Collateral
- Public IP Address
- Masternode Signature (secondary public key)

A network message will be sent every 15 minutes to prove that the node remains activated. Once the time-to-live gets out to date, the network eliminates the inactive node from the system, stopping clients from using nodes. Network can also be pinged by the nodes, however if the ports are closed, it will be marked as inactive and not be compensated

2) Trive Masternode Network Incentive Program: These Masternodes enhance the existing architecture of full nodes which are commonly used in the Bitcoin network, by providing an incentive to owners; therein ensuring consistent cost-to-benefit ratios. This is important because the upkeep of traditional full nodes rise exponentially as the network expands and owners often resort to measures that cause the quality of service and speed of transactions to decrease.

The node must store a minimum of 10,000 TRVC for the Masternode to get started. Once activated, clients on the network will receive services from the nodes and get an incentive bonus. These payments for Masternodes are taken from the same block reward that are shared among the governance, PoW and the masternodes, with an estimate of 28% of total block reward being assigned to Trive Masternode Incentive Program. Masternodes incentive tends to differ according to the current total activated Masternodes, mainly because the incentive program has a fixed amount of percentage whilst Masternodes network fluctuates.

III. Decentralized Autonomous Organization

One of the major highlight of blockchain technology is that they are decentralized. This means they are not controlled by a single institution like a government or central bank, but instead are divided among a variety of computers, networks, and nodes. In many cases, blockchain projects make use of this decentralized status in order to attain levels of privacy and security that are typically unavailable to standard fiat currencies and their transactions.

The Decentralized Autonomous Organization also known as DAO is an organization that was designed to be automated and decentralized. The DAO was unaffiliated with any particular nation state, particular company or a particular group of personel. DAO is an automated system and a crowdsourced process having decision-making power to manipulate funds eliminate human error.

In Trivechain, the DAO is fueled by TRVC and facilitate with group of Masternodes owner, the DAO is designed in such a way that allow anybody in the community to place a certain amount of TRVC to create a proposal and allow the community to vote on the proposal. Every masternode can vote either agree or disagree on a proposal during the voting period. If the voting is passed through with majority of them voting agree, the TRVC is distributed to the person that proposed the idea. The proposal can be to run a marketing campaign, to operate a mining pool, build a website containing information and even building new innovation on top of the current core. The DAO was designed to allow masternodes to vote for the development direction of the public chain.

IV. Block Reward and Supply

Instead of constantly halving the reward given to the miners and masternode operators like many other public blockchain protocol that creates an exponential decay in the block reward. Trivechain will be introducing a 25% inflation reduction of block reward every 525,600 blocks after the first 226,630 blocks which is the fork to TRVC 2.0. The block reward will start with 25 TRVC per block.

The block reward will be distribute 30% to TriveGovernance, 42% to PoW Miner and 28% Trive Masternode Network.

V. Use Cases

A. Direct Send (DS)

Trivechain also introduces a new concept called DirectSend (transaction locking and masternode consensus). This technology will allow for cryptocurrencies such as Trivechain to compete with nearly instantaneous transaction systems such as credit cards for point-of-sale situations while not relying on a centralized authority. Through the use of a consensus between Masternodes, the signals of a transaction are locked and only spendable in a specific instant transaction. Widespread vendor acceptance of Trivechain and DS could revolutionize cryptocurrency by shortening the delay in confirmation of transactions from as long as an hour (withBitcoin) to as little as a few seconds.

B. Exclusive Send (ES)

ExclusiveSend grants users absolute confidentiality by masking the origin of their financial assets. Each Trivechain

in a wallet is composed of different"signals", and so can be thought of as individual coins independent of each other.

ExclusiveSend utilizes this feature along with an ingenious mechanism to scramble the signals of person A with the signals of persons B and C, without requiring any movement of coins. Therefore, users are in full control of their assets at all times. ExclusiveSend is a unique scrambler which is not only decentralized but works to constantly remove all traceability for each Trivechain in circulation. The central principle behind this feature is fungibility, in economics, a term used to express an assets interchangeability with other assets of the same type. In short, this ensures that there is no difference between any two Trivechains in the network. This is important because coins accumulate history due to associations.

with prior transactions, which could result in price discrepancies between coins with little history and coins with a lot of history. without having a difference in price in the form of a premium for coins with less or no history. Furthermore, without this feature, some coins may lose their value entirely if they are blacklisted after being traced back to transactions which are associated with illegal or criminal activities. However, with ExclusiveSend, all Trivechains in circulation with have zero traceability and thus unassociated with any previous transactions, guaranteeing absolute fungibility.

In order to prevent mass conversion of Trivechain into fiat currency in a single transaction, like in the case of an attack, ExclusiveSend is limited to 500 TRVC per session. To further facilitate user experience as well as deter against attacks, ExclusiveSend runs in a static state. At predetermined intervals, a users client will request to join other clients via a Masternode. Upon access into the Masternode, a queue object is transmitted throughout the network describing the denominations the user is looking to make confidential, without revealing any information that can be used to find the identity of the user.

Every ExclusiveSend round is an independent event, which increases confidentiality and a minimum of three users are required for each transaction. With this setup, the theoretical greatest chance that an attacker follows a transaction is 1 out of 3, but this is further improved by linking transactions through several Masternodes to further increase confidentiality.

To further increase the confidentiality of a users identify, Trivechain utilizes Masternode Clouding in addition to the Static Confidentiality. This works by clouding Masternodes so that they are unable to identify which signals belongs to which users, through the use of a relay system.

Instead of a user submitting the signals directly into the pool, a random Masternode is assigned from the network and requested to relay the signals to the intended Masternode. With this approach, a Masternode only receives and knows the number of signals but cannot trace which signals belong to which users.

C. Trive Governance

In Trivechain, it can run a system adequately by its own, just need to set or pre-programed rules. DAO holds its members funds and use the fund at definite purpose. To create a proposal in DAO there are 5 parameters to specify Recipient, Amount, Proposal details, Voting duration, Deposit. Recipient will create a proposal and define the amount for proposed transaction, Curator has to define voting duration. Minimum duration can be 1 week, Longer duration will be beneficiary. Curator has to deposit some amount of TRVC for proposal creation. If there is any false information in parameters then transaction will be fail.

Set of rules for DAOs governance - 1. For each proposal there should be high members of participation for vote and each member will be rewarded for there participation. 2. A member can delegate proxy vote and also can receive reward for it but proxy can be abolish anytime. 3. Rewards will split between number of members, Rather than number of tokens.

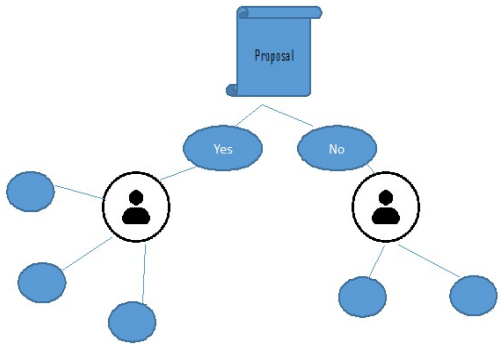

Fig. 1. Proxy Voting

D. Trive Stamp

Trive Stamp is a stamp in blockchain created after hashing a file or document. What is hashing?Why we do hashing? Hashing is a function designed for any arbitrary input to get a fixed-length of output. Hashing will return hash values and hash code. Trive Stamp is combination of meta data(file size, file type) and hash code. Hashing is important for data security. If anyone want to decrypt the data using hash code wont be able to do that.

Input	Hash code
Welcome	548aed7438aadb5934ffdb7d79cb47c2cadb 5934ffdb7d79cb63acef80125da0

TABLE I
HASHCODE MAPPING

There are some quality constraints for hash code

- Hash code should be different for each input.
- Should be impossible to decrypt.
- For same input hash code should be same.
- After any alteration in document hash code should be totally different

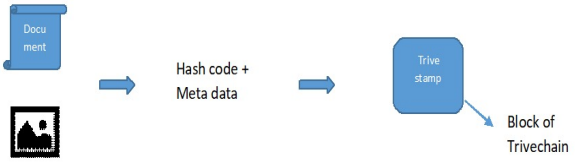

Fig. 2. Trive Stamping

E. TriveApp

There are various sectors where blockchain technology can be implemented to, and its not restricted only to the realm of financial sector. For instance, retail and e-commerce services, healthcare services, financial services and real estate industries. TriveApp is a solution and an opportunity for all sectors to tap into the blockchain market, enabling them to customize their application system on top of Trivechains platform. By utilizing simple programming language, new businesses will only need to pay a small amount of fees in Trivechain to integrate their application.

TriveApp could potentially eliminate communication issues between various parties. Take healthcare industries for example - one of the general application in this industry could be signing off the medical record. Healthcare could adapt multi-signatures (a method in which transactions only happens when a certain amount of authorized parties have approved or signed off) to give permission to other parties to fully or partially access to the medical record. In addition to that, the implementation can also verify that a major or minor procedure has taken place. The usage of blockchain makes sure that the information is encrypted and accessible only to those who have the authority to open it.

Nowadays, mobile applications are being acquired from centralized organizations, meaning that app developers would need to pay a registration fees to be listed on these platforms, and, on top of that pay commission of as high as 30% per sale.

F. Trivechain Wallet

Trivechain Wallet is a cryptocurrency wallet that allows you to store multiple cryptocurrency including TRVC, Tokens and Assets that are tokenized using TriveAsset in just one and only wallet. Trivechain Wallet is design in such a way that they are a wallet where you are able to pay in a cryptocurrency that you do not have by converting other cryptocurrencies that you have. There is no need to create another wallet and download additional wallet allowing you to send one type of cryptocurrency and the receiver receiving the type of cryptocurrency he preferred.

The merchant can select the type of cryptocurrencies they preferred and the system will do the conversion giving the payer the options to choose between a wide range of cryptocurrencies available in the market.

VI. CONCLUSIONS

Through the utilization of Trivechain technology including TriveGovernance, TriveAsset, TriveApp and TriveStamp. Trivechain aims to be a decentralized platform with a core focus on improving the expansion of existing business into blockchain technology as well as serving as a solid foundation for startups. Moreover, with the use of both Proof-of-Work and Proof-of-Stake algorithms combined with the Trive Masternode Network, Trivechain aims to be a self-sustaining ecosystem where long term sustainability as well as scalability are strong focuses. The double-tiered network also serves as a highly configurable platform that can easily house additional features and improvements at a later stage, thereby essentially ensuring the Trivechain project is an ever evolving entity.

In addition to businesses, the public users also benefit from features such as ExclusiveSend and DirectSend which serve to enhance user accessibility, privacy and provide for a secure, intuitive transaction system for a wide range of personal and business activities.

Additionally, Trivechain also aims to be a platform that can be easily integrated into existing e-commerce solutions, financial institutions as well as social media. This is realized through the use of a seamless abstraction layer which then allows existing commercial, financial and social media platforms to utilize features such as the DirectSend without having to heavily restructure their infrastructure. As such, we strongly believe that Trivechain, with its open-ended design, is highly adapted to serve as a strong foundational layer for a large number of financial and commercial protocols in the future.

REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
[2] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013, October). A fistful of bitcoins: characterizing payments among men with no names. In Proceedings of the 2013 conference on Internet measurement conference (pp. 127-140). ACM.
[3] Duffield, E., & Hagan, K. (2014). Darkcoin: PeertoPeer CryptoCurrency with Anonymous Blockchain Transactions and an Improved ProofofWork System. bitpaper. info.
[4] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151, 1-32.
[5] Bradbury, D. (2013). The problem with Bitcoin. Computer Fraud & Security, 2013(11), 5-8.
[6] Back, A. (2002). Hashcash-a denial of service counter-measure.