TRIVECOIN (TRVC)

Ji Sheng Tan and Terrence Chooi

Abstract— **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, trivecoin 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 VIP Masternode Network (TVIP).**

The evolution of value transfer has gone from the basics of value transfer to smart contract. Trivechain as a core protocol is in the path of 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) BizContract, a trustee service; (iv) BizApp, a hybrid of centralized and decentralized application; (v) BizFactory, token issuance; (vi) cWallet, wallet for multiple cryptocurrency. (vii) cPay, payment gateway accepting cryptocurrencies with close to instant exchange.

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 achiving 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 perating 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, effecient, 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

TriveCoin 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, TriveCoin 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 TriveCoins 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 TVIP Masternode 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 TriveCoin increases.

B. X11 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.

TriveCoin, much like several other cryptocurrencies, utilizes a digital distributed ledger known as a blockchain which serves as the foundation. The blockchain contains a record of all TriveCoin transactions 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 X11), 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.

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 until a later component of its life cycle In a Bitcoins life cycle, hobbyists started to mine currency with Central Processing Unit (CPUs), followed by Graphics Processing Units (GPUs) soon after it was produced to easily take over CPUs Due to the die size and complexity needed to form an ASIC for mining x11, it is expected to take a longer period of time than it did with Bitcoin. The more powerful CPU gives the same average amount of returns as compared to GPUs. GPUs have also been said to be more energy efficient compared to Scrypt algorithm, which runs 30 - 50% cooler.

C. TVIP Masternode 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) TVIP Masternode 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 1000 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 1000 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 1000 TRVC in the Masternode stands zero chances of gettingattacked after activation. In the beginning, a Masternode sends a Masternode Information message across the network, stating:

- 1000 TRVC Submission
- Obtainable IP Address
- Signature (secondary backup key)
- Stamp Time
- 1000 TRVC Public Key
- Secondary Backup Public Key
- Charity Public Key
- Charity Proportion

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) TVIP Masternode 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 1000 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 stash of fundings, with an estimate of 40% of total block reward being assigned to TVIP 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. Block Reward and Supply

Instead of constantly halving the reward given to the miners and masternode operators like many other coins that creates an exponential decay in the block reward. Trivecoin will be introducing a 10% inflation reduction of block reward every 200,000 blocks after the first 200,000 blocks.

The genesis block of the Trivechain consist of 33,600,000 TRVC for the early adopter that bought the coin through an Initial Coin Offering (ICO) with a small portion reserved for the Trivechain Foundation to fund the research and development of Trivechain for the next 60 years.

To encourage miners and masternode to start mining Trivechain and setting up masternode, the initial block reward is set to 50 TRVC per block with a exponential decay. Upon reaching block height of 24000, the block reward is halved; and upon reaching the 100,000 mark, the block is halved leaving the block reward at 12.5 TRVC per block.

Exponential decay of block reward is good for investors of the coin to have exponential grow in their net worth of portfolio, Trivechain position ourselves as a coin that is relatively stable and made for daily trading. So, we kept the reward constant with no inflation from 2,600,000 blocks onward until the reach of the maximum supply which is 84,000,000 TRVC or block height of 12,115,999 after which the block reward will be based purely on the transaction fee of transactions made within the block.

IV. Use Cases

A. Direct Send (DS)

TriveCoin also introduces a new concept called DirectSend (transaction locking and masternode consensus). This technology will allow for cryptocurrencies such as Trivecoin 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 Trivecoin 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 TriveCoin 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 Trivecoin 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 TriveCoins 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 TriveCoins in circulation with have zero traceability and thus unassociated with any previous transactions, guaranteeing absolute fungibility.

In order to prevent mass conversion of TriveCoin 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, TriveCoin utilizes Masternode Clouding in addition to the Static Confidentiality (section 6.2.). 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. BizContract

BizContract is a unique solution to the problems currently plaguing implementation of smart contracts. Traditional smart contracts while in theory have a broad application, are often not implementable in the real world due to several factors such as difficulty of integration into existing systems, high implementation costs, multiple abstraction layers and lack of autonomy. The goal of the BizContract is to systematically address these areas where the smart contract has fallen short while also expanding on its true potential.

Firstly, the BizContract will be developed as an isolated component of TriveCoin and this way, it can be developed to be either centralized (so as to greatly ease integration with existing systems) or decentralized (highest level of anonymity). This flexibility in the design of BizContract will simplify integrationand reduce costs.

Secondly, the introduction of a seamless abstraction layer to access storage of all ledgers instead of separate abstraction layers for respective ledgers.This coupled with the DirectSend feature will allow for nearly instantaneous transactions times with minimal use of network traffic and computational power. Also, a seamless abstraction layer will greatly ease integration into already established financial management systems. In addition to addressing pre-existing problems with smart contract systems, the two-tier system also provides a greater array of functionality. BizContract, while serving as a trusted medium between business and customer, will also function as an escrow service which guarantees the right amount to be paid for an agreed upon product or service.

Furthermore, BizContract can retrospectively function as a trustee service very much like financial institutions, in that the contract is either immediately enforced should the conditions be met or vice versa. With this in mind, BizContract will also pursue a novel feature whereby the traditional property investment is combined with crowdsourcing, enabling a shared purchased of properties with significant value. This unique feature will bring about a fresh and exciting investment opportunity to the general public looking to invest in real estate but do not have the individual capital to do so.

D. BizApp

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. BizApp 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 TriveCoin to integratetheir application.

BizApp 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 multisignatures (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.

E. BizStore

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.

Though these well-known platforms do provide their services pretty well, BizStore strives to make a 100% user-friendly decentralized application store, by providing a system where consumers and app developers have first-hand interaction.

With TriveCoins decentralized BizStore, app developers would only need to pay a small amount of fees with TriveCoin to be listed on BizStore, andenjoy maximum profit

without having to reimburse a hefty amount of salescommission.

F. BizFactory

Many upcoming new businesses are not familiar with programming new tokens, or are struggling financially to hire a software engineer in the early phase of their expansion. Though there are increase in demand for new businesses to venture into blockchain technology, the aforementioned problems are impeding new ventures to participate.

BizFactorys platform makes it easily accessible, simple and straight forward for new businesses to venture into blockchain. BizFactory allows them to create their own tokens without needing to have knowledge of coding or programming skills. This unique platform will ease the new business to rapidly evolve into a conventional mechanism for todays business, without having to drain their initial capital. In order to issue a token on TriveChain, new businesses only need to fill up the basic information with the following information:

- Contracts address
- Maximum supply of tokens
- Name of token
- Tokens abbreviation
- Tokens logo
- Number of decimals

G. cWallet

Cwallet is a cryptocurrency wallet that allows you to store multiple cryptocurrency in just one and only wallet. Cwallet 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.

H. cPay

CPay is a service design to be the crossover central settlement payment gateway for merchant to receive cryptocurrencies. 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.

V. CONCLUSIONS

Through the utilization of TriveChain, TriveChain Standard and BizContract, TriveCoin 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 and ICOs. Moreover, with the use of both Proof-of-Work and Proof-of-Stake algorithms combined with the Trive VIP Masternode Network, TriveCoin 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 TriveCoin project is an ever evolving entity.

In addition to businesses, the private users also benefit from features such as ExclusiveSend, DirectSend and BizContract which serve to enhance user accessibility, privacy and provide for a secure, intuitive transaction system for a wide range of personal and business activities. Escrows which typically require a financial institution as a mediator can now instead be executed through a peer-to-peer interface with the BizContract automatically enforcing the escrow once all conditions have been met. This not only reduces the overall transaction cost by removing the need for a mediator, but also potential makes the whole process nearly instantaneous.

Additionally, TriveCoin 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 a seamless abstraction layer which then allows existing commercial, financial and social media platforms to utilize features such as the BizContract and DirectSend without having to heavily restructure their infrastructure. As such, we strongly believe that TriveCoin, 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.