The Verex Blockchain: A Non-Anonymous Decentralized Ledger with an Assigned-Majority-Validation Consensus Protocol

Working Paper, February 2018

Deane E. Jill

deane.e.jill@gmail.com

Abstract: A useful blockchain should possess the following properties, one or more of which many existing blockchain systems lack: 1) A sound consensus protocol. 2) An efficient transaction-processing system. 3) Immutability of history. 4) Decentralization. 5) An effective avenue for hard-forks and rule changes. We propose a system named the "Verex Blockchain" that will fulfill these requirements. This system employs an "Assigned-Majority-Validation" consensus protocol whereby only nodes within a specialized, designated network may vote on the correct state of the blockchain and add new blocks of transactions without proof of work or stake. New nodes to this network must be approved by existing nodes. These nodes will be controlled by entities with high public visibility such as governments or multinational technology companies, whose identities and actions will be made fully transparent on the blockchain. Transactions will be charged fees in cryptocurrency according to a fixed and known fee schedule, which will be earned by nodes in the designated network. Any user in the world may download the blockchain, receive and verify updates, and submit transactions, but only nodes in the specialized network may write updates to the blockchain.

1. Introduction

Blockchain technology has become extremely prolific over the last few years, and blockchain's ability to offer a widely-accessible decentralized ledger allows for numerous useful applications. However, existing blockchain systems (both those proposed as well as those actually implemented) are lacking in some qualities that are necessary for a blockchain to be stable, secure, and useful. We propose a new blockchain system, which we name the "Verex Blockchain". This paper details the conceptual features of this system, while avoiding the technical details of implementation. We believe that the structure of this system gives it the qualities necessary for a blockchain system to be useful on a truly significant scale. This paper assumes reasonable familiarity with popular existing blockchain systems such as the Bitcoin and Ethereum systems.

2. Properties of a Useful Blockchain

In order for a blockchain system to achieve usefulness on a large scale, it must possess the following properties:

A. Sound Consensus Protocol

The blockchain must have a system whereby consensus on the correct current state of the blockchain may be easily reached. Users must be able to easily obtain a reliable copy of the blockchain, with an accurate history and present state of records. Moreover, users should not have to contend with multiple possible "correct" versions.

In certain existing blockchain systems, there may be multiple acceptable versions of the blockchain in circulation at any one time. In some proof-of-work systems, for instance, there may be multiple chains of equal length (actually, computational complexity), and in such cases, both are potentially legitimate "correct" versions until one grows longer than the other, at which point it usually gains final majority acceptance. This fork, though usually temporary, can cause periods of uncertainty regarding the "correct" version of the blockchain, making this consensus protocol suboptimal.

B. Efficient Processing of Transactions

A useful blockchain must be able to process transactions in a cost-effective manner, confirm them quickly, and write a large number of transactions to the blockchain per period of time. The blockchain's potential use in various economic activities will be limited if the rate of transaction processing is slow, and transaction fees will be high if transactions cannot be processed in a cost-effective way.

Many proof-of-work systems such as the Bitcoin system fail in this regard. They write transactions to the blockchain though a computationally-intensive mining process, which keeps costs high for the transaction processors and results in wasteful energy use. Moreover, in some of such systems, new blocks are discovered infrequently (once every 10 minutes on average in the case of Bitcoin), so confirmations may take a long time (eg. 60 minutes if one waits for 6 Bitcoin blocks to be added on top of the transaction before considering it very unlikely to be reversed). Furthermore, block sizes in such systems may be small, so each block holds a very limited number of transactions. Since new blocks may take several minutes to mine, pending transactions in very large batches may have to wait a long time before being processed.

C. Immutability

The history of transactions on the blockchain should not be easily susceptible to change (except perhaps in extenuating circumstances such as a massive-scale hack that requires a hard-fork to undo). Ideally, when a transaction has been verified and written to a legitimate block on the blockchain, it should have a very small chance of being reversed.

Again, various existing proof-of-work systems are not ideal here. For example, new blocks of transactions mined in the Bitcoin blockchain system may be legitimately added to the blockchain version accepted by most, only to later become discarded when another blockchain version with a longer chain that does not include this block emerges and is quickly accepted instead by the majority. It thus may not be uncommon for recent histories to undergo changes within short periods of time in such systems. This may force users to wait for several blocks to be mined on top of a block before being reasonably confident that the history in the original block will not be changed.

D. Decentralization

One of the touted advantages of the blockchain is that it is decentralized. No one entity can easily manipulate the blockchain, and there is also no single point of failure, since correct copies of the blockchain live on many nodes within a large network.

While many existing blockchain systems claim to be decentralized, there is a danger of centralization in several well-known proof-of-work and proof-of-stake systems. As it becomes more difficult to mine new blocks in proof-of-work systems, computers may pool together to form mining pools, which leads to a concentration of mining power. The mining that secures the blockchain hence becomes more centralized. In proof-of-stake systems where the node holding the most cryptocurrency is most likely to be chosen to forge new blocks on the blockchain and hence earn the transaction fees, this may lead to a rich-get-richer effect, whereby most of the cryptocurrency becomes concentrated in the hands of a few nodes, thus leading to more centralization. The variants of proof-of-stake systems make the rate of wealth growth proportional to the current balance of wealth, potentially resulting in a deep concentration of wealth in steady state.

Related to decentralization, a secure blockchain system must be well-guarded against potential 51% attacks. New users who wish to obtain a copy of a blockchain must usually query existing nodes in the network for this. In proof-of-work systems, they treat the longest chain as the true copy. In proof-of-stake systems, they treat the copy receiving the most votes (where participating parties with larger cryptocurrency balances usually have more voting power) as the true copy. In other systems, a similar concept of a majority-consensus is used to ascertain the true version. A 51% attack may occur if a mining pool controls more than 50% of the mining power, a coordinated group owns more than 50% of the cryptocurrency needed to vote, or more than 50% of the nodes collude respectively. This coordinated party can sabotage the blockchain according to its whims. This seems to be a potential weakness of any blockchain system, though most existing systems are structured such that this attack would require an unrealistically large amount of resources to execute.

E. Avenue for Hard-Forking and Rule Changes

In certain extreme circumstances, a hard-fork on the blockchain or a deployment of a new code base with a new set of blockchain logic may be required. For instance, in the event of massive hacks such as the DAO hack in the case of Ethereum or the Mt. Gox Bitcoin exchange hack, a hard-fork to reverse previous transactions written to the blockchain by hackers may be a prudent (albeit controversial) solution. Furthermore, any blockchain system, no matter how carefully thought out, may suffer from bugs or security flaws only discovered ex-post. In such situations, a new version of code must be adopted by majority of the users in the blockchain network in order for fixes to be implemented.

Thus, a decent blockchain system should have some relatively effective avenue for implementing such changes, though changes will hopefully be infrequent. Unfortunately, in most existing blockchain systems, the avenues for change are cumbersome. The anonymity, vastness, and heterogeneity of the network nodes that make up many prolific blockchain systems today make majority consensus difficult when it comes to agreeing on code changes and hard-forks. For example, Bitcoin saw several spin-offs such as Bitcoin Cash and Bitcoin Gold when a significant subset of the Bitcoin nodes disagreed on certain proposed changes. Such splits add confusion to the system, since they produce multiple blockchains that users may now have to decide between, and are therefore clearly suboptimal.

3. The Verex Blockchain

We propose a novel blockchain system called the "Verex Blockchain" to address the above issues with existing systems. Similar to existing blockchains, the Verex blockchain is a sequence of ordered blocks, with each block containing information such as transaction details.

I. Verex Code

As with many existing blockchain systems, the code that dictates the rules of the Verex blockchain system will be made open-source on a publicly-visible repository, though merges with the master branch may be controlled by an administrator (who will likely be a member of the Verex development team in the initial stages).

II. The Verex Network

The Verex blockchain will be secured by a network of nodes, where each node is a server that will run the Verex code and store a copy of the Verex blockchain.

When initially setting up the Verex blockchain, Verex developers will approach various entities to offer them the opportunity to designate their servers as nodes in the Verex network. An important requirement of the Verex network is that these entities be parties with a visible and reasonably reputable public presence, and access to significant amounts of resources. Examples of suitable candidates for Verex nodes are: large technology companies (eg. Google, IBM), large financial firms (eg. Bank of America, Citigroup), and perhaps even governments of developed countries (eg. branches of the US and UK governments).

When establishing the Verex network, nodes should be chosen such that each unique entity only owns one node, and the entities that own nodes are spread out across various countries. This ensures decentralization of the network. Moreover, the network should be sufficiently large, but not too large such that it renders important processes cumbersome. If there are too many nodes, operations such as obtaining a consensus copy of the current blockchain or broadcasting newly-forged blocks may become time-consuming since the client must query all nodes in the network for this. If there are too few nodes, the network is not secure enough. A network of as few as 21 such nodes should be sufficient to reasonably secure the Verex blockchain initially. Since each node is a high-profile entity with enough resources to fend off most hacker attacks, it will be difficult for an antagonistic external party to take over even a handful of nodes in a coordinated fashion, let alone commandeer majority of the nodes for a 51% attack. Hence, the network need not be very vast.

Whenever a new server becomes a node in the Verex network, it is required to write information related to its identity to a publicly-visible platform. For instance, server address information listed on a publicly-accessible document can be accompanied by the name and point-of-contact details of the associated entity (eg. the official name of a corporation that owns this node and the contact details of a representative of the corporation respectively). In this way, the identities of the operators of each node are transparent to all.

III. Responsibilities of Verex Nodes

Verex nodes secure and maintain the network by fulfilling the following responsibilities:

A. Determining the Current State of the Blockchain

Any user in the world who wishes to obtain the current state of the Verex blockchain can download the Verex code and query the blockchain. During this process, the user client will query each node in the Verex network and receive a version of the blockchain from each node that said node claims to be the most up-to-date version. The blockchain version that majority (> 50%) of nodes agree on is accepted by the client as the "true" version, though the various versions propagated by each individual node remain fully visible to the client. If no consensus is reached, then no "true" copy of the blockchain can be obtained at the moment, and the blockchain is said to be "in limbo". Users may also retrieve and view the batch of all unprocessed transactions pending validation that were sent to the blockchain. Note that simply downloading the Verex code and a copy of the Verex blockchain does not make a user become a Verex node or a part of the Verex network; unlike many other blockchain systems, the general user in the Verex system has read-only access to the blockchain version being propagated by the nodes. Users can submit transactions to the blockchain, but the state of the blockchain can only be altered by the network of nodes. While the identities of network nodes are made public, non-node users remain anonymous.

Verex nodes themselves may also update their local blockchain copies by querying all other nodes and getting the majority-consensus version, which they may wish to do if they have ignored blockchain updates for some time.

B. Accepting New Nodes

In order for a server to become a node in the Verex network, it must be approved by a majority of the existing network nodes. Each node will decide whether to accept a server as a new node or not at its discretion. A potentially viable process of application would be as follows: An entity that owns a server reaches out to a point-of-contact for each network node, using the public information provided on each node's identity. The entity and the network nodes

collectively participate in dialog whereby the entity's identity is verified. The nodes discuss amongst themselves and then elect by majority vote to include the entity's server as a new network node.

In this way, the process for a server to become a network node will be manual and non-systematic, but the exacting nature of this process is a critical element of the Verex blockchain system. Since the Verex nodes decide the true blockchain copy by majority consensus, the network must be careful not to let insidious entities join the network as nodes and wreck future havoc on the blockchain.

C. Expelling Misbehaving Nodes

Just as Verex network nodes must agree to accept new nodes, they may also coordinate to expel existing nodes from the network. They may choose to do so if a node is consistently inefficient at performing its duties, or if it exhibits clear nefarious behavior such as attempts to sabotage the blockchain or relay new blocks that are inconsistent with the agreed-upon rules of the system.

A Verex node may choose to discontinue being a node on the network at any time by relaying this desire to all Verex nodes in the network. A Verex node may also choose to willfully ignore all of its responsibilities, essentially taking itself offline, in the event that, for some reason, other nodes choose not to drop it from the network after its request to resign.

D. Processing Transactions

Every 5 seconds (or some other short period of time), a node in the Verex network is chosen to be the "Designated Processor Node" (DPN). The DPN retains this status for the next 5 seconds, during which it may add a new block to the blockchain. During this time, it can retrieve all unprocessed transactions that have been submitted to the blockchain and process them.

The DPN is selected according to a known, deterministic schedule. According to this schedule, every node in the network takes a turn at being the DPN, and no node goes twice until all others

have gone once. If a node is offline when it is appointed as the DPN, it is skipped, its turn is considered over for this round, and the next online node in line becomes the DPN.

Each transaction that is processed is expected to comply with existing transaction rules (eg. no double-spending of cryptocurrency, required private key signatures on transactions). The DPN will validate transactions according to these rules and add verified transactions to a new block, which it then appends to its copy of the blockchain and relays to all other nodes in the network. No proof of work is required to add a block. The only computations required involve the validating of transactions.

All other nodes continually query the DPN for the latest block. The first block to be received is treated as the only and final block proposed by the DPN for this round. The other nodes then each independently verify the validity of the proposed block. A new proposed block is deemed invalid if its contents do not abide by the rules of the Verex code, if it is submitted by a node that is not the DPN at the time, or if it attempts to alter blockchain history prior to the latest block. If the block is deemed valid, a node will add that block to its blockchain copy. If majority of the nodes add the block to their blockchains, the block becomes part of the consensus blockchain version.

If a DPN discovers a transaction that violates the stated rules, it can reject the transaction, in which case the transaction disappears from the batch of pending transactions and is no longer available for future processing. A list of rejected transactions is also relayed to the rest of the nodes, which similarly independently verify that those rejected transactions are indeed invalid in the presence of the new block, and if so, delete them from the pending transaction queues on their local blockchains so that these do not consume future processing time.

If no new block is submitted by a node during its tenure as the DPN, the blockchain does not grow, the next node in line becomes the new DPN, and the process repeats. If there are pending transactions submitted to the blockchain that were not approved or rejected by the DPN during this round, they remain available for processing by the next DPN.

This system is different from proof-of-work systems in that it does not require any computationally-intensive proof of work to add blocks. This is also different from a proof-of-stake system since servers must be network nodes to validate transactions, but need not have any stake in the form of cryptocurrency in their wallets, and each node always has the same amount of voting power. In fact, this seems to be slightly to significantly different from most existing "proof-of-" systems. Here, blockchain updates require consensual yet independent validation from a designated network of non-anonymous nodes. For lack of a better term, we call this the **"Assigned-Majority-Validation"** consensus protocol.

E. Adopting Hard-Forks and Code Changes

In the event that a hard-fork or a fundamental change to the rules of the Verex blockchain system is required, the nodes in the network can discuss acceptable changes at their discretion, and, with majority consensus, implement such changes. Since the "true" version of the blockchain is the majority-consensus version of these nodes, such changes will come into effect and be present in every copy of the blockchain that users download if more than 50% of the network nodes implement these changes into their local code bases and copies of the blockchain.

The difference between users and network nodes should be re-emphasized. Users may run the Verex code on their machines, query network nodes for the blockchain version and updates to it, and even independently verify that newly-added blocks obey the rules of the code and that rejected transactions are indeed illegitimate. However, when new first-time users wish to obtain a copy of the existing blockchain, as per the Verex code, they will only query the network nodes and not the non-node users for this. Hence, only the network nodes have the bona-fide ability to update the blockchain for the community of users.

IV. Possible Implementation

One possible implementation of the above Verex network node system, albeit perhaps not the most elegant, is to have the server and identity details of each node in the network hardcoded into the Verex code base. Users that pull the latest version of Verex code can query the network nodes by

querying the hardcoded servers should they wish to obtain the network's consensus blockchain version.

If existing Verex nodes decide to induct a new node, they can modify the code base by adding the new node's information to the hardcoded list, collectively agree to adopt the new code base at a designated time, and also notify the community of code upgrades and make the updated code base available for public download. Similarly, Verex nodes can delete a node from the hardcoded list and publish this new code for downloading if they decide to expel a node. Any user that fails to use updated code to pull the latest copy of the Verex blockchain will risk being left with an outdated blockchain (eg. still querying nodes that have been expelled).

If the Verex network nodes are publicly seen as the backbone of the Verex blockchain, and given the fact that they do all of the transaction processing, users are likely to sync their code bases with the version being used by the majority of the nodes.

V. Verex Blocks

Each valid block in the Verex blockchain will hold the following information:

- The set of verified transactions that are included in the block.
- The list of all Verex network nodes and information on the entities that own them at the time when the block was added. While not essential or foolproof, this feature allows one to easily check that the local network list corresponds with the network lists of other blockchain copies.
- The version tag of the Verex code used to generate this block. Again, this is useful for users and nodes to ensure that their code bases are in sync with the consensus code base of the Verex network.

Verex blocks have no specified size limits and can contain an arbitrary number of transactions. However, Verex nodes can always decline a block proposed by the DPN if the block size is unreasonably large, so that the DPN cannot launch a denial-of-service attack by propagating an artificially massive block to the rest of the network. The earliest block in the blockchain, called

the “Base Block”, will hold information on initial asset balances in all wallets on the Verex blockchain instead of transactions.

As more transactions are added and the blockchain grows, it is possible that the blockchain will become too long and excessively large to store efficiently. A solution to this may be to add a feature to the blockchain that frequently collapses all blocks before a certain point (eg. all blocks older than 3 months) into one new base block with the implied asset balances in each wallet, so that the length of the chain is not too unwieldy. This preserves our ability to correctly deduce the current balances in each wallet on the blockchain, but destroys some information on previous older transactions.

Two Verex blockchain versions are considered identical if and only if all information in all of the blocks of the two blockchains match, including historical information.

4. Verex Dollars

A cryptocurrency is necessary to facilitate transactions on the Verex blockchain. To this end, we will create “Verex Dollars”, a cryptocurrency that will transact on the Verex blockchain. The supply will be fixed at 2.1 billion Verex Dollars (or some other set amount), all of which will exist from the outset. The smallest unit of the currency will be the Verex Cent, equal to 0.01 Verex Dollars.

5. Transactions

The Verex blockchain will have wallets belonging to various users. Each wallet will have an address by which others can locate it (to send assets to it, for instance) as well as a private key known only to its owner, which is used to sign various transactions.

A wallet is a virtual container that holds assets. The Verex blockchain can potentially support any number of different types of assets. By default, every Verex wallet will be able to hold the Verex Dollar asset type. External parties can create new asset types and push their code for such asset types to the blockchain as a transaction. Each asset type comes with its own transaction rules,

which will define what makes a transaction involving the asset type valid. Eg. Verex Dollar transactions must be signed with the private key of the payor and the payor account must have sufficient funds for the transaction. The Verex blockchain can potentially record any type of transaction or information, so long as the appropriate asset type is created to support it.

The Verex blockchain may also be used to support smart contracts in the same way that Ethereum does, and pushing code for smart contracts as well as executing them will also be treated as transactions to be processed.

A transaction is only considered successfully sent to the Verex network when it has reached every node in the network (where it will sit on the local blockchain copies, unprocessed and waiting for validation by the next DPN). Every transaction successfully sent will return a transaction receipt to the initiator. Such a receipt can be generated for the user by the local Verex code when the user client receives acknowledgement of the sent transaction from each node in the network. Transactions can be processed in the order in which they were received. If a transaction has been unprocessed for some time, it is automatically canceled (dropped from the transaction queue, never to be processed), and the initiator receives a cancellation notice when all nodes cancel it. Rejected transactions that do not correspond to the Verex system transaction rules for that asset type return a rejection notice when all nodes send out their rejection.

6. Transaction Fees

Each transaction submitted to the blockchain will only be deemed valid if it is accompanied by a mandatory transaction fee that must be paid in Verex Dollars. When a DPN in the Verex network validates transactions, it keeps 50% of all fees associated with these transactions, and distributes the other 50% uniformly among all other online nodes in the network. In this way, a DPN is incentivized to process as many transactions as possible, as it keeps the bulk of the fees. Other nodes are incentivized to accept the proposed new block if valid, since they will also receive a cut of the fees. A server is incentivized to continue acting as a node in the network, since it receives fees so long as it remains an active node.

Each transaction on the Verex blockchain will have a fixed minimum fee of one Verex Cent per transaction. The fee will increase according to a deterministic schedule with the complexity of a transaction. The DPN will continue processing a transaction that is very computationally-intensive for as long as there are sufficient funds made available as part of the transaction to pay for each operation involved in it. If a transaction times-out because it is too computationally-intensive (eg. takes more than 4 seconds to process), or if it reaches a point where there are insufficient funds, or if it is deemed invalid as it violates transaction rules, then all funds made available are kept as a transaction fee and the transaction is rejected. If more than enough funds are made available, the excess is returned to the initiator of the transaction. This is similar to the gas system used by Ethereum, and prevents infinite-loop transactions from bringing down the system. This also discourages the submission of computationally-intensive transactions and invalid transactions. In a similar way, transactions involving the creation of instances of asset types in wallets can also feature an increasing fee scale depending on the size of the asset type object to factor in the costs of having to store it on and propagate it through the blockchain, potentially into perpetuity.

Therefore, one Verex Cent represents the value of a basic transaction on the Verex blockchain. If the market sets the Verex Dollar-to-fiat currency exchange rate at too low a price, many will buy, pushing the price up, since the convenience of a transaction on the blockchain may be worth more to them. For instance, conducting similar transactions using a third-party traditional clearing house may be costlier and take much longer to settle. If the price goes too high, no one will transact on the Verex blockchain as no one can afford to, and they can find cheaper alternatives for transactions such as clearing houses or other blockchains. This renders the Verex blockchain useless, which will also make Verex lose its intrinsic value. Hence, the demand for Verex Dollars will be miniscule at that high price and this should drive prices down. Thus, unlike some existing cryptocurrencies, Verex Dollars have intrinsic value since they are the medium for Verex blockchain transactions, and the market equilibrium price of one Verex Cent represents the worth of one basic Verex transaction to the market. As long as performing some type of transaction on the Verex blockchain is of value to someone, Verex Dollars will retain some amount of intrinsic value.

In very extreme cases, if many parties are held hostage by a high price of Verex Dollars, perhaps by players who have cornered the market, the Verex nodes can also agree to introduce code changes that lower the hard-coded transaction fees so that the fiat currency-equivalent cost of a transaction becomes reasonable. We emphasize that, unlike the gas system in Ethereum, the transaction fee schedule in terms of Verex Dollars should be fixed by the network and not determined by the market.

7. Spin-off Blockchains

Consider the following non-cryptocurrency application of the Verex blockchain: Suppose that U.S.-based banks wish to eschew traditional clearing houses and use the blockchain for their customers' inter-bank transactions instead. A consortium of large banks can band together to create a "U.S. Bank Account" asset type on the Verex blockchain by agreeing on the logic for this asset type and pushing code for creating it to the blockchain as a transaction. Rules for this asset type may be as follows: 1) Every U.S. Bank Account instance must have information regarding the identity of the account holder, the identity of the bank that this account is held at, and the balance of U.S. dollars in the account. 2) A U.S. Bank Account object may be created in a user's wallet only if the object is signed by the private key of the user and the private key of a wallet belonging to a U.S. banking entity that is part of a list of participating banks hardcoded in the code for this asset type. 3) Balances in U.S. Bank Account instances can be altered through blockchain transactions if signed by the private key of the bank at which the account is held. 4) Transactions between U.S. Bank Account objects resulting in changing USD balances in said accounts are valid if signed by the private keys of the related banks and the owner of the wallet holding the payor account. 5) U.S. Bank Account information such as the owner's identity and the balances are encrypted and can only be accessed via the private keys of banks in the hardcoded list, so that such information remains secure from public prying. 6) Basic transaction rules such as the requirement of sufficient balances in payor accounts when making transfers apply.

In this example, users wishing to write their bank account information to the Verex blockchain can contact their banks and work with them to create U.S. Bank Account instances with the appropriate information in their blockchain wallets. The bank may update the account balances accordingly by submitting these as valid transactions (eg. the bank can decrease the balance on the blockchain

when the account holder makes a cash withdrawal at a local branch). Users can transfer USD from their account to the accounts of others by submitting the request to their bank, which then initiates a transaction with the payee bank account, with the acquiescence of the payor's private key. As such a transaction must also be signed by the private keys of the banks of both the payor and the payee accounts, and since these banks have access to owner-identity information in the U.S. Bank Account instances, this system can be made compliant with Know-Your-Customer regulations that U.S. financial institutions must follow.

New banks wishing to join the participating list so that their customers can set up U.S. Bank Account instances on the Verex blockchain as well can contact the banks on the existing hardcoded list. If they are deemed legitimate, the participating banks can push code for a new asset type (eg. "U.S. Bank Account 2.0") as a Verex transaction. The new asset type will follow the logic of the original U.S. Bank Account asset type, but will include the new bank in the list of participating banks. The new code may also include a constructor function for the U.S. Bank Account 2.0 object that allows banks to create new instances of these objects from existing U.S. Bank Account instances. This lets all banks upgrade their U.S. Bank Account instances to U.S. Bank Account 2.0 instances to maintain compatibility going forward. In this way, U.S.-based banks can facilitate and record inter-bank transactions on the blockchain without clearing houses.

Arguably, due to the sensitive nature of such transactions, customers may feel more comfortable if a subset of the banks on the participating list (perhaps the largest, most established ones) acted as nodes in the network instead of the entities on the more heterogenous existing Verex network. To this end, banks can utilize a system structured similarly to the Verex system to form their own spin-off blockchain that will provide such functionalities, either waiving or keeping the transaction fees from this blockchain themselves (perhaps charging transaction fees in USD instead of Verex Dollars since they are not on the Verex blockchain). It would be a simple matter to clone and modify the Verex system code for such a purpose.

Situations such as the above where large institutions within the same industry have a natural incentive to participate in their own blockchain can cause these spin-off blockchains, which will be secured by their own networks of specialized nodes. However, this does not nullify the

usefulness of the original Verex blockchain. There are many applications which no particular industry has a direct incentive to support (or for which the natural industry that should support it does not have the technical resources needed to form a working blockchain network). For instance, a community of users wishing to create their own cryptocurrency disparate from central banks for use in commerce (one of the original proposed uses of Bitcoin) have no natural industry to turn to. They can instead rely on the Verex blockchain secured by the heterogenous network spanning multiple industries to support transactions for such a purpose; incentives related to the accrual of Verex Dollar transaction fees will compensate this network for hosting these applications in the absence of natural incentives.

8. Initial Distribution of Verex Dollars

All or a large portion of the fixed supply of Verex Dollars can be distributed to the public for circulation via an Initial Coin Offering (ICO). This will allow interested parties to purchase Verex Dollars that can then be used to transact on the Verex blockchain. The ICO can be priced at a price below a fair value, where the fair value level is an estimate of the market equilibrium price of a transaction on the Verex blockchain in the future, when the blockchain is assumed to have become very stable and globally prolific.

For instance, suppose that large cash transactions through third-party clearing houses cost an average of US$10 per transaction. If, in the near future, the Verex blockchain becomes well-established enough to handle the same type of transactions at the same volume with equal or better efficiency, then the market should be willing to pay up to $10 per such transaction, or perhaps even more for the added convenience and security of the blockchain. If one Verex Cent is the fixed fee for such a transaction, then it is reasonable to assume that the fair value of one Verex Cent in such a future state of the world is US$10. If we price the ICO at, say, $0.10 per Verex Cent, then the difference between $0.10 and the fair value of $10 would represent the risk premium that those willing to invest in Verex Dollars early would earn from betting that the Verex blockchain will become established and prolific, if their bet indeed comes to fruition. This risk-reward proposition may entice participants to become early adopters of Verex Dollars in the ICO, not just to transact, but to potentially realize capital gains equal to the size of this risk premium.

9. Advantages of the Verex Blockchain

We believe that the characteristics of the Verex blockchain system endow it with the various properties needed to be useful on a significant scale, as detailed below:

A. Sound Consensus Protocol

The "true" copy of the Verex blockchain that users receive when querying the blockchain is the majority-consensus copy of the Verex network nodes. If all nodes are running the same code and hence processing and verifying transactions by the same rules, then they should always agree on the correct version of the blockchain, and a sound consensus is consistently reached. Since only the DPN is allowed to propose a new block at a time, there is no risk of network nodes updating their blockchains differently if they all use the same code.

If a node repeatedly attempts to perform blockchain updates that are not compliant with the rules of the system, it will be easily detected due to the transparency of the system. Any user can query the blockchain version of any node in the network at any time, and thus each node's track record of local copies is fully visible to the world, along with any noncompliant updates. It is a simple matter for all nodes in the network to monitor one another for misbehavior, reject noncompliant updates, and expel the misbehaving node from the network if need be.

The network nodes derive value from being part of the network by earning transaction fees. Since fees are paid in Verex Dollars, the value of their future income is tied to the value of Verex Dollars. Verex Dollars in turn derive intrinsic value from their use as fuel for transactions on the blockchain. Hence, Verex Dollars and the future income of nodes only have value if the Verex blockchain remains useful as a platform for transactions. This incentivizes the nodes to maintain the stability of the blockchain by properly validating all new blocks and consistently monitoring for nefarious behavior by other nodes. The high public visibility of the entities that control the nodes and their actions further incentivizes the nodes to abide by the agreed-upon rules of the system. This should mitigate the nothing-at-stake problem, whereby validator nodes in some systems such as the proof-of-stake system have no disincentive to reject or accept all new blocks without proper independent verification.

B. Efficient Processing of Transactions

New blocks are not too difficult to add to the Verex blockchain as they require no proof-of-work, so all computational resources can be focused on validating transactions. This system is therefore energy-efficient and cost-effective.

New DPNs are chosen every 5 seconds, which means that new blocks are added roughly every 5 seconds. Thus, transactions can be processed and confirmed quickly. Furthermore, since the nodes are owned by high-profile, resource-flushed entities, the servers that act as the nodes should have easy access to the potentially high levels of computational power needed to quickly process large batches of transactions. This allows the blockchain to process and store a large number of transactions per block.

C. Immutability

Since blockchain updates can only be proposed by the DPN, and since the DPN is only allowed to propose one new block at a time, the blockchain history remains immutable when new blocks are added, so long as most network nodes agree on the version of the blockchain before the new block, which will happen if the nodes abide by the same, publicly-known rules. Thus, transactions can be safely considered confirmed when they are added to the newest block, without having to wait for additional new blocks to be forged on top of them. Naturally, blockchain histories can be changed if the majority of nodes conspire to update their blockchains past the most recent block, but this change will be visible to the world, and will tend to reduce confidence in the Verex blockchain. For aforementioned reasons related to public image and the value of transaction fees, Verex network nodes have an incentive to maintain confidence in the system. Hence, network nodes will not collectively violate the established rules unless it is their desire to end the system altogether.

D. Decentralization

Since unique entities are only allowed to operate one node, the Verex network is decentralized. An entity may attempt to operate multiple nodes in the network, but this will only be valid with the consent of majority of the existing nodes, which are unlikely to approve such a change due to the loss of decentralization that it implies.

Moreover, the identities of each node are public, allowing the potentially vast community of users to constantly ensure that the network does not contain a large set of nodes belonging to closely-affiliated entities. The manual vetting of new potential nodes done by the existing network makes identity fabrication difficult for a new node, so new nodes controlled by existing entities cannot infiltrate the network under the guise of separate entities.

It is true that centralization of sorts may occur due to the fact that existing network nodes have a disincentive to add new nodes. As more nodes are added, the transaction fees earned by each node decrease if total transaction fees remain the same. Thus, we may reach a point of saturation whereby the nodes in the network do not wish to include other nodes. However, this point will presumably only be reached when the network is sufficiently large. If the network only consists of a handful of nodes, then the blockchain system is not very secure, and few users will transact on it, hence leading to low levels of income from transaction fees. It therefore benefits existing nodes to include more nodes up to a point. The network may also be willing to include new nodes belonging to reliable, reputable entities for the sake of preserving amicable relations with said entities off the blockchain.

Many of the characteristics of the Verex blockchain system that ensure decentralization also guard against 51% attacks. If majority of the nodes in the network were to collude, they could sabotage the blockchain. However, they have strong disincentives to do so. Colluding to bring down the network or altering balances of assets in their favor will render the blockchain unreliable, and the assets that they gain, all of which only live in virtual space, will hence be worthless. As visible entities, they will also potentially lose the trust of the public permanently.

Nodes may conspire to raise transaction fee levels, but this has a limit as well. If fees are too high, few will transact on the blockchain and fee revenue may decrease. One can argue that the network functions as an oligopoly, and can realize monopolistic power when nodes collude. They will work together to set a transaction fee level that maximizes their profits. Because they are functioning as a monopoly, according to economic theory, this fee level will be higher than the market equilibrium level and the system will realize less benefit than it otherwise would in

a competitive economy. However, there are upper bounds to this level. Set too high a level, and alternative platforms such as competing blockchains and third-party clearing houses will become more attractive. The bounds of this situation should still allow consumers of the blockchain to realize more (or, in the worst case, the same amount of) benefit than in a world without a reliable blockchain. Furthermore, not all nodes may be profit-maximizing entities. Some may belong to governments or non-profit think-tank institutions more concerned with the utility of their constituents than the accumulation of direct income through transaction fees.

In addition, the fact that the nodes are owned by publicly visible, reasonably reputable entities to begin with gives assurance that their intentions are unlikely to be destructive. They are altruistic vanguards of a new-age system at best, and profit-maximizing businessmen at worst, but unlikely to be agents of chaos bent on inflicting instability upon their own revenue-generating system. In any extreme case, the system is still a democracy, given usefulness only by the fact that many users besides network nodes are transacting on the Verex blockchain. A large fraction of the user community can simply decide to adopt a new code base featuring a new list of network nodes while preserving the blockchain history so far if the existing network is colluding to do ill, since every existing user has a copy of the blockchain and the code.

E. Avenue for Hard-Forking and Rule Changes

The relatively small number of entities needed to secure the Verex blockchain and the fact that the entities are easily contactable and publicly known makes it feasible for the node owners to organize effective discussion on fundamental changes to the system such as hard-forks and rule changes should these be needed.

While easy agreement is never guaranteed, there is a higher likelihood of this in the Verex system than in other blockchain systems that feature anonymous nodes, an excessively vast network, or the ability for any arbitrary entity, including possibly the irrational and the ignorant, to act as a validator node.

Some would argue that fundamental changes such as hard-forks completely destroy the purpose of the blockchain, which was originally meant to have a truly immutable history.

However, we strongly believe that any global system that takes on the important responsibility of recording vast amounts of crucial information must have avenues for modification beyond the initially-specified structure. Undoing destructive hacks and fixing critical logical flaws is necessary for a system to have longevity, and blockchain should be no different.

10.Conclusion

Many existing blockchain systems are lacking in one or more qualities that would make such a system useful on a large scale. The Verex blockchain system that we are proposing runs on a non-anonymous network of validator nodes controlled by high-profile, publicly-visible entities, and uses an Assigned-Majority-Validation protocol to verify transactions and reach consensus on the correct current state of the blockchain. Cryptocurrency built on top of the Verex blockchain will incentivize optimal behavior on the part of the network nodes. We believe that the unique features of this blockchain system enable it to offer the various qualities needed for a blockchain to achieve true global scale and utility. We therefore hope that suitable entities will be willing to collaborate to create such a system, and function as the nodes needed for this system's network.