Geeq

**John P. Conley**
August 2018

# The Geeq Project White Paper

Version 2.0

# The Geeq Project White Paper


## John P. Conley[1]


### Version 2.0

**August 2018**


## Abstract

GeeqChain is a new approach to distributed ledger technology that uses a proprietary validation protocol called Proof of Honesty (PoH).[2] PoH empowers users who hold tokens on any GeeqChain to determine for themselves whether the network of validating nodes is behaving honestly. This allows GeeqChain to provide 99% Byzantine Fault Tolerance (BFT) while delivering rapid transaction finality at extremely low transactions cost. An additional protocol based on economic mechanism design gives GeeqChain Strategically Provable Security (SPS). GeeqChain's architecture allows for the creation of an ecosystem of federated chains that can safely share GeeqCoins and other native tokens as well as support many different types of internal business logic. This makes GeeqChain suitable for a wide variety of use cases, allows for upgrades and bug fixes without breaking protocol or instituting hard forks, and offers a flexible and more secure alternative to Ethereum's ERC20 standard for startups wishing to create new platforms to take advantage of blockchain's potential. GeeqCoin itself is supported by an algorithmic monetary policy to reduce price volatility. Our new approach to a stabilized-token makes GeeqCoin a less risky store of value and a more attractive medium of exchange.



1 I would like to thank Stephanie So of Vanderbilt University for her contributions in developing the ideas in this white paper, Ric Asselstine of Terepac Corporation for his vision and work to bring these ideas into reality, and Yorke Rhodes of Microsoft for turning my attention to blockchain and cryptocurrencies in the first place.

# Table of Contents

# 1. Introduction

Traditional databases are maintained on private servers by central authorities who control access, grant permission to alter, update and delete records, and who are ultimately responsible for the accuracy of the data. Trusting such data is equivalent to trusting in both the honesty and the security competence of the central authority.

Blockchains are append-only, distributed ledgers. No central authority owns or controls the data. Users send requests to write new records to a set of decentralized, often anonymous, nodes[3] who must come to a consensus on their validity. Once a record is written to a block and committed to the chain, it becomes both immutable and nonrefutable. Cryptographic signatures and recursive hashing of blocks make it computationally impractical to delete, alter, or claim that one never agreed to the contents of a record. If a blockchain is public and transactions are written in cleartext (as they are in Bitcoin), records in the chain can be independently verified by any user who wishes to do so. If copies of the chain are stored in many places, it becomes almost impossible to censor or prevent access to the data it contains.

Blockchains allow agents to cooperate without the need to trust in the honesty or good behavior of one another or any third party. For example, Bitcoin's transaction protocol ensures that a sender has enough tokens in his account to cover a transfer and, once the transfer is made, the receiver can be secure in the knowledge that it cannot be reversed. Ethereum's smart contracts permit even more sophisticated interactions between users without the need for mutual trust.[4]

Unfortunately, the promise that blockchain holds for creating decentralized and trustless ways to transact, share information, and improve distributed business processes is limited by several factors. Most importantly, existing protocols offer relatively weak security guarantees. Most approaches are subject to 51% attacks, have relatively centralized or small validator/delegate pools, have high transactions cost, and/or have difficulty scaling up to handle large numbers of transactions.

GeeqChain addresses these problems using a new proprietary protocol for validating blockchain transactions called Proof of Honesty (PoH). PoH empowers users who hold tokens on any GeeqChain to determine for themselves whether the network of validating nodes is behaving

3 Nodes are computers on a network that participate in validating transactions and writing blocks of transactions to the chain. Depending on the blockchain and approach to validation, nodes are called miners, stakeholders, delegates, or voters, among other terms. Humans (who we call agents) own these computers and make them available to the network. One agent may be the owner of several nodes, or may simply be a user who makes transactions on the blockchain but does not provide validation services.

4 It should be noted, however, that the Ethereum smart contracts have also led to a number of significant security issues. For example, on June 17, 2016, a coding error in the smart contract supporting the DAO resulted in a theft of 3.4M ETH worth $53M. More recently (November 6, 2017), another coding error in the Ethereum smart contract supporting Parity's multi-signature cryptocurrency wallets locked up accounts holding over 500k ETH worth over $150M. More generally, theft of tokens is a significant issue. For example, on January 26, 2018, $534M worth of NEM coin were stolen from Coincheck, the largest Japanese cryptocurrency exchange. According CNBC, $1.1B in cryptotokens were stolen in the first half of 2018. https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html

honestly. This allows GeeqChain to provide 99% Byzantine Fault Tolerance (BFT)[5] while delivering rapid transaction finality at extremely low transactions cost. Blocks or chains with false transactions are easily identified and orphaned, while dishonest validators are automatically ejected from the system. Additional protocol elements based on economic mechanism design bring GeeqChain up to 100% BFT.

The GeeqChain ecosystem (the Geeqosystem) is built on a foundation of federated and interoperable instances[6], each supported by a hub and spoke network of anonymous and decentralized nodes. A single instance of GeeqChain is able to validate 40 transactions per second using standard residential broadband connections. If volume increases, the GeeqChain protocol automatically splits the chain in two and places half of the accounts and nodes on each new ledger. Since a chain can be split as many times as needed to meet transactions demand, GeeqChains are infinitely scalable.

GeeqChains have separate validation and application layers, each with their own blockchains and ledger states. The validation layer contains only GeeqCoin accounts for users and nodes and allows only simple accounting transactions. This minimizes potential attack surfaces and protects GeeqChains from contamination by dangerous smart contract code or having slanderous, racist, or copyrighted material written immutably into the ledger. The main purpose of the validation layer is to make payments to nodes for the validation and virtual machine services they provide to the application layer. GeeqCoin itself is a utility token that can be moved across all instances of GeeqChain and lubricates the transaction validation engine that is the foundation of the Geeqosystem.

The GeeqChain application layer is designed to give developers a flexible, secure, and efficient platform upon which to build out their visions. Applications can be written in a variety of programming languages and can include native tokens, arbitrary data objects, smart contracts, and any sort of business logic a use case requires. Applications can be configured to interoperate with one another or to firewall themselves off from the rest of the Geeqosystem. Each application runs on its own instance (or instances) of GeeqChain. This means that applications do not compete with one another for the computational resources provided by the validating node network.

---

5 BFT comes from Lamport, Shostak, and Pease (1982) in which they describe "The Byzantine Generals Problem". To understand the idea, suppose that ten generals of the Byzantine empire are surrounding a city, some of whom have been bribed not to attack. Suppose the participation of at least seven is required in order to conquer the city. Otherwise, the attack fails. Such a battle plan is said to be 30% BFT. Most blockchain protocols have BFT of 50% or less. More generally, BFT is a measure of how tolerant a system is to faulty components. Unfortunately, characterizing robustness in this way tends to make protocol designers think of nodes as parts of a system that either work as expected, or fail, instead of as rational agents with preferences who are capable of doing either depending upon the circumstances. GeeqChain's security model is based on game theory and economic mechanism design. Honest validation by all nodes is the only coalition-proof equilibrium of GeeqChain's protocol. This provides Strategically Provable Security which is an even stronger security guarantee than 100% BFT. See the companion technical paper "Proof of Honesty: Coalition-Proof Blockchain Validation without Proof of Work or Stake" for more details and a proof of this claim.

6 An "instance" of a GeeqChain is a complete and independent blockchain that uses the GeeqChain protocols and architecture. Each instance has its own set of validating nodes, its own set of GeeqCoin accounts that are recorded in the validation layer blockchain of the instance, and its own application code that governs how native tokens and data-objects are transacted in the application layer blockchain of the instance. Thousands of instances of GeeqChain may exist that can communicate, exchange native tokens, and write GeeqCoin balances to the accounts on one another's ledgers.

On GeeqChain, “code is law.” GeeqChain's users need not worry about arbitrary hard forks that may be imposed on platforms validated by Proof of Work or Proof of Stake, nor about the uncertainty that may arise from the actions of a centralized or voter-determined governance structures. However, bugs, hacks, upgrades, new functionalities, the advent of quantum computing, and so on, all make it desirable to enable applications to evolve and change over time. GeeqChain’s solution is to create new genesis blocks for applications and give users and validators the option to vote with their feet and migrate to the new instance voluntarily. Users and validators who wish to stay and use the original protocols may do so. Code is law and GeeqChain never imposes new law on unwilling users.

GeeqChain also employs a novel algorithmic monetary policy that stabilizes GeeqCoin value. At the highest level, this involves keeping a fraction of the fiat currency made from token sales in escrow to be used to smooth out exchange rate volatility and maintain user confidence in the GeeqChain platform. GeeqCorp will sell tokens as the GeeqCoin fiat price on exchanges goes up to fund and replenish a Fiat Stabilization Reserve (FSR) account. In turn, the FSR will be used to buy back and remove GeeqCoins from circulation (putting them in a Token Stabilization Reserve (TSR) account on the chain) if the GeeqCoin fiat price moves down. In effect, GeeqCorp creates additional demand in down-cycles, and additional supply in up-cycles.

# 2. Problems with Existing Blockchains

Blockchain has the potential to profoundly transform the way we work, transact, and share information. As a technology, however, blockchain is an immature technology and several significant problems need to be solved before this potential can be achieved.

## 2.1 Security

All the advantages that blockchain offer depend on honest transaction verification and block-writing. Bitcoin uses Satoshi’s Proof of Work (PoW) protocol, while Ethereum (the second largest cryptocurrency) and many other “alt-coins” use a variant. PoW protocols have in common that they are susceptible to 51% attacks. That is, if more than 50% of the nodes/miners are dishonest, then they can take over the chain and write any transactions they please. If 50% or more are honest and follow protocol, an authoritative fork will exist on which all transactions are correct.[7] As a result, Bitcoin and similar protocols are said to have a Byzantine Fault Tolerance (BFT) of 50%. We discuss the value of BFT as a measure of security in more detail below.

In PoW protocols, nodes are generally run by anonymous agents. The principle of one CPU, one vote, applies. Any agent who is willing to bear the computational cost of trying to mine a block can join the validation network anonymously and as an equal. The hope is that this cost deters Sybil attacks in which many “fake” identities are created in order to gain majority control of the validation process. If votes must be paid for with work, then it is hoped that it should be unprofitable to mount such an attack.

7 However, Eyal and Sirer (2014) describe a type of coordinated attack by miners holding only 25% of Bitcoin’s hashing power that can compromise the blockchain implying that Bitcoin is only 25% BFT.

In practice, many Bitcoin and Ethereum nodes are owned by the same real-world agent or are part of mining pools in which hardware may be owned by different agents, but which coordinate their efforts and share rewards. Some Bitcoin pools have chosen to self-identify which makes them vulnerable to pressure from state-actors or others. Mining pools are so concentrated at this point that if no more than three were to collude, they could mount a successful 51% attack. In effect, Bitcoin is not validated by thousands of independent nodes but depends instead on the honesty of three or fewer agents. Put another way, if Bitcoin has 10,000 nodes, an attack by only three agents would be successful. In a real sense, this means that the BFT of Bitcoin is only 3/10,000 or .03%.

One must wonder why these pools do not, in fact, merge. In any industry, mergers create market power. For example, if there are four firms selling cellphone service each making $\$X$ per year in profits, the monopoly created by merging all four firms would make more than $\$4X$ in profits. At worst, the merged firm could simply proceed as if it was still four separate firms and make exactly $\$4X$. Taking advantage of monopoly pricing or economies of scale, however, would certainly bring profits above $\$4X$. Merging is in the interest of the shareholders of all four firms. In the same way, if three mining pools are each making $\$X$ in net profits from mining rewards and transactions fees, the merged pool could make at least $\$3X$ by continuing to act as they did before. On the other hand, the merged pool would be able to mount a successful 51% attack and take over the Bitcoin blockchain, gaining whatever additional profits this might entail. The fact that they do not choose to do so must mean that something besides the PoW protocol is keeping them honest. The most likely candidate is the fear that stealing bitcoins would result in a hard fork[8] that would prevent the merged pool from profiting from its theft. In other words, to the extent that PoW blockchains are trustworthy, it is only because of the belief that "code is law" is a lie. It is in fact the threat to break protocol, not the protocol itself, that keeps Bitcoin and Ethereum safe.

Proof of Stake (PoS) is the other main approach to verification. Several banks, for example, might set up a private blockchain in which the members vote on whether a new block is correct and should be added to the chain. The banks put their reputations at stake in this case.[9] Stake can also be established by posting a bond (money or tokens), investing in the performance of useful services on a platform, providing resources such as storage or bandwidth, participating in platform activities, etc. Voting power is then distributed in proportion to the stake. In many cases, stakeholders choose

8 In this case, the "hard fork" would involve breaking protocol and ignoring the "validated" blocks containing transactions that were judged as stealing coins. New blocks would be added starting from the last "honest" block. More generally, a hard fork takes place when part of a group decides to take a project in a new direction starting from the existing code base, dataset, or other IP. This is usually because the group has a different vision for the best path forward. Hard forks are especially problematic in context of blockchain because it breaks the rule that "code is law" by creating a fork with new laws and protocols. Even if the motivations are pure, if you can break the law for good, you can break the law for bad. Hard forks are very corrosive to the trustless, anonymous, distributed nature of blockchain.

9 Note that since all the participating banks are in the same sector, their economic fortunes are highly correlated. In a recession or financial crisis, all banks are likely to be under financial pressure, the threat of bankruptcy, and the possibility of being taken over by the Federal Reserve. It would not be at all surprising if a financial crisis, such as the one that began in 2007, were to result in five out of eight banks in a PoS blockchain being placed under federal supervision or forced to merge. Bank officers might be willing to take desperate measures to survive. The threat of a lost reputation is not much of a deterrent to a bank or any firm facing extinction. In addition, the identity of the validators is known and so they can be pressured by state-actors to break validation protocol in support of legal judgments or state policy.

a smaller set of delegates to be their proxy and represent their interests.[10] Depending on the implementation, PoS approaches are both cheaper and more scalable than PoW. On the other hand, they generally offer a BFT of 33% or less, so these advantages come at the cost of some security. Of even more concern is that PoS protocols depend on the honesty of the stake-weighted super-majority of agents who have decided that it is worthwhile to acquire stake, and on the nonmanipulability of the voting or delegation system. Since the number of voting stakeholders or delegates (tens or hundreds) is typically much smaller than the number of validating nodes used by PoW blockchains (thousands or tens of thousands), collusion by validators is much more likely. It is not clear how much confidence a claim of 33% BFT should give us even if we believe it to be true.[11]

It is worth noting that even if stake-holders are numerous and anonymous, we run into the same concentration problem that we see in PoW protocols. If the profit a validator gets from posting a bond is worth it, why not post the same stake under many identities? At worst, each identity makes enough profit to pay for the opportunity cost of posting the bond. Creating enough identities to gain the majority of the total voting stake makes it possible for a single real-world agent to take over the blockchain. Again, it is only the threat of out-of-protocol actions that creates disincentives to make such an attempt.

## 2.2 Cost

Visa and Mastercard charge merchants a fee of about 25¢ plus 2.5% of the value of the transaction to use their networks. These transactions costs are very high, certainly too high to make it practical for a customer to make a micropayment of a few cents to a merchant or content provider. One of the great promises of blockchain-based cryptocurrencies is that they will make financial transactions more efficient. If Bitcoin, Ethereum, or any of the other alt-coins now in existence found a way to allow people to make transactions quickly, cheaply, and securely, it would revolutionize the financial industry.

The Ethereum and Bitcoin platforms have transactions costs that range from tens of cents to tens of dollars. Blockchains that depend on PoW protocols must have very large networks of validating nodes. Users ultimately bear the costs of having thousands of nodes using electricity and wasting CPU cycles to solve the cryptographic puzzles required to win block rewards and validate transactions.[12] In other words, high transactions costs are baked into PoW based cryptocurrencies.

10 There are also many hybrid approaches that use variations and combinations of PoW and PoS, include complicated governance procedures, or are based on Directed Acyclic Graphs (DAGs). We discuss some of these below.

11 If a fixed set of stakeholders validate a blockchain, then honest behavior depends on the incentive structure faced by these specific agents. For example, one might be confident that the reputational damage of dishonest behavior would be enough to make Bank of America or Deutsche Bank behave correctly. When voting stakeholders can choose actions that affect their voting power, however, dishonest agents, who have the most to gain from subverting the blockchain, have the greatest incentive to expend the effort required. Thus, protocols that use escrowed tokens or Proof of Effort of some kind may end up systematically choosing dishonest validators. BFT loses its meaning as a measure of security in such cases.

12 The bitcoin protocol creates a cryptographic puzzle for miners to solve at the beginning of each block. This puzzle can only solved by brute force trial and error. Miners run computers (or more often, large clusters of purpose built computers) to find the solution. Solving the puzzle produces what is called a "nonce". Once the nonce is found, it can be used by anyone to quickly verify that the puzzle has been correctly solved. It is estimated each block requires $10^{25}$ "hashing operations" (guesses) to find the nonce, requiring a total of 35 TWh (terawatt hours) of electricity per year.

Solutions based on PoS blockchains such as Hyperledger fabric have a different set of problems. It is true that using a relatively small number of stake-holders decreases the computational (and other) costs of validating transactions. If only ten or twenty stake-holders are to be trusted with the job of validating millions or billions of dollars in transactions, however, they must be carefully screened. As a result, their identities are often known and users must ultimately trust that the screening process is effective and will remain so. This runs completely contrary to the underlying idea of blockchain as a trustless, decentralized, and distributed ledger technology.

Some approaches to PoS involve larger numbers of stakeholders, but require that they choose to give their share of the voting power to a smaller number of delegates. This speeds transaction confirmation since a relatively small number of nodes/stakeholders are actually doing the work of verification. Such systems are only secure, however, to the extent that the bonds posted by the stakeholders are large in comparison to what they could gain by acting dishonestly. Since posting bonds is costly, these PoS approaches also bake in an inescapable level of transactions costs (similar to those discussed for PoW protocols).

In short, there is no such thing as a free lunch. Either transactions costs are high to cover the expense of staking or computational work requirements, or validation is in the hands of a small number of possibly nonanonymous agents. Unless a solution can be found, cryptocurrencies will never be secure enough to offer a serious challenge to the conventional banking system.

## 2.3 Scalability

Both the Ethereum and Bitcoin blockchains are operating near maximum capacity. The Ethereum blockchain writes blocks about every 10 seconds and currently processes between 4 and 7 transactions per second (with an estimated maximum rate of 15 per second). Bitcoin writes blocks every 10 minutes and processes 2 to 4 transactions per second (with an estimated maximum rate of 7 per second). Neither protocol would be able to scale up to the 2000 transactions per second handled by the Visa network which has an estimated maximum rate of 56,000 per second.

Bitcoin's proposed solution to this problem is called the Lightning network and is similar to Ethereum's Raiden network. Essentially, users are required to lockup tokens on the main Bitcoin or Ethereum blockchains to serve as security for transactions that agents agree to off the main-chain. These off-chain transactions are not validated or committed by the mining pool, but there is a degree of security provided by a system of smart contracts. This allows both parties to cancel or alter transactions until they mutually agree that a transaction is final. There are a great many problems with this approach, but we will not go into detail here.13 However, it is worth pointing out that users must pay normal transactions fees to move coins onto smart contracts and lock them into escrow in order to make them available for use on the Raiden/Lightning networks. Fees also must be paid to bring the results of activities on these side networks back to the main-chains. In a sense, these networks allow users to place value on debit cards that they can use to execute transactions quickly and cheaply without involving the "bank" (the main-chains in this case). However, this

At $0.10 per kWh, this means it cost approximately $3.5B to validate the bitcoin blockchain in 2017. Although wholesale electricity costs are be considerably lower in certain regions, the environmental implications of this waste are the same regardless of the cost of electricity.

requires that the "bank" both issue the cards and redeem them in order to return whatever value they contain back onto the users' main-chain account.

Iota's tangle protocol uses a different approach to increasing transaction capacity. Iota and other Distributed Acyclic Graph (DAG) approaches are not actually based on blockchain, but instead rely on repeated validation, hashing, and transmission of transactions by individual nodes. Eventually, users are supposed to gain confidence that a transaction is valid and finalized based on an evaluation of the number of independent confirmations and the reputation of the nodes involved. The BFT of tangle is not clear. In addition, the number of validators used is relatively small, validator anonymity is difficult to guarantee, and the protocol appears to be open to strategic manipulation on a number of fronts.[13]

As discussed in the previous section, PoS based solutions either use a small number of validators or run into the same scaling issues as PoW approaches.

# 3. GeeqChain Architecture

The GeeqChain ecosystem (the Geeqosystem) is built on a foundation of federated and interoperable instances, each supported by a hub and spoke network of anonymous and decentralized nodes. Each instance has separate application and validation layers with their own blockchains and ledger states. The Geeq application layer is customizable and can contain native tokens and specialized data objects to suit any use case. The validation layer is kept simple, robust, and bullet-proof and contains only GeeqCoin accounts for users and nodes. Basic protocols and the custom business logic of GeeqChain applications is encoded in a series of Governing Smart Contracts (GSCs), which provide the components of the user and node clients1 (the software used to run and interact with GeeqChains). These GSCs are included in genesis blocks that are the foundation of each instance.

## 3.1 Federated Chains

Bitcoin, Ethereum, and most other blockchains trade only in their own tokens. It is simply not possible to move a bitcoin to the Ethereum blockchain or inversely. There is only a single master chain for each of these tokens where transactions can be made and token holdings recorded. Other native tokens may exist in smart contracts, but this is quite different from a system of decentralized federated chains.

GeeqChain, in contrast, is designed to support multiple instances of federated chains that form a Geeqosystem in which users can choose where their tokens are parked. Each individual instance can handle 40 transactions per second (more than either Bitcoin or Ethereum can handle). If this is not enough, new federated instances of GeeqChain can be created by dividing the set of nodes and accounts on the original chain in two. These instances share the job of validating transactions, and

13 For example, see Christine Masters' discussion of Iota at: https://cryptovest.com/education/not-a-iota-the-trouble-with-iota-and-how-to-fix-it/, and Lansana's discussion of HashGraph's centralization and governance problems at: https://medium.com/@Lansana/i-was-wrong-hashgraph-is-actually-very-bad-bf7d9b2e8d99.

.

tokens are able to move freely between them. Since any number of instances can be created, GeeqChain can be scaled up to handle arbitrarily large transactions loads.

Moving tokens from one chain to another requires that they be destroyed on the sending chain before they are created on the receiving chain. A good way to think about this is that tokens are "teleported" from chain to chain. The token disappears on one chain and reappears on another. Protocols are designed to prevent "teleportation accidents" where the token is duplicated elsewhere while not being destroyed on the originating chain, is sent to more than one receiving chain, or is somehow held in a pattern buffer and then recreated later on the originating chain. Of course, it is also desirable to prevent accidents in which tokens fail to materialize on the destination chain, but the consequences of this are far less damaging than unintended duplication.[14] On the other hand, non-token data items such as medical records could be "replicated" locally on several different chains without harm. The owners or creators of these replicated items might be paid fees for allowing this.

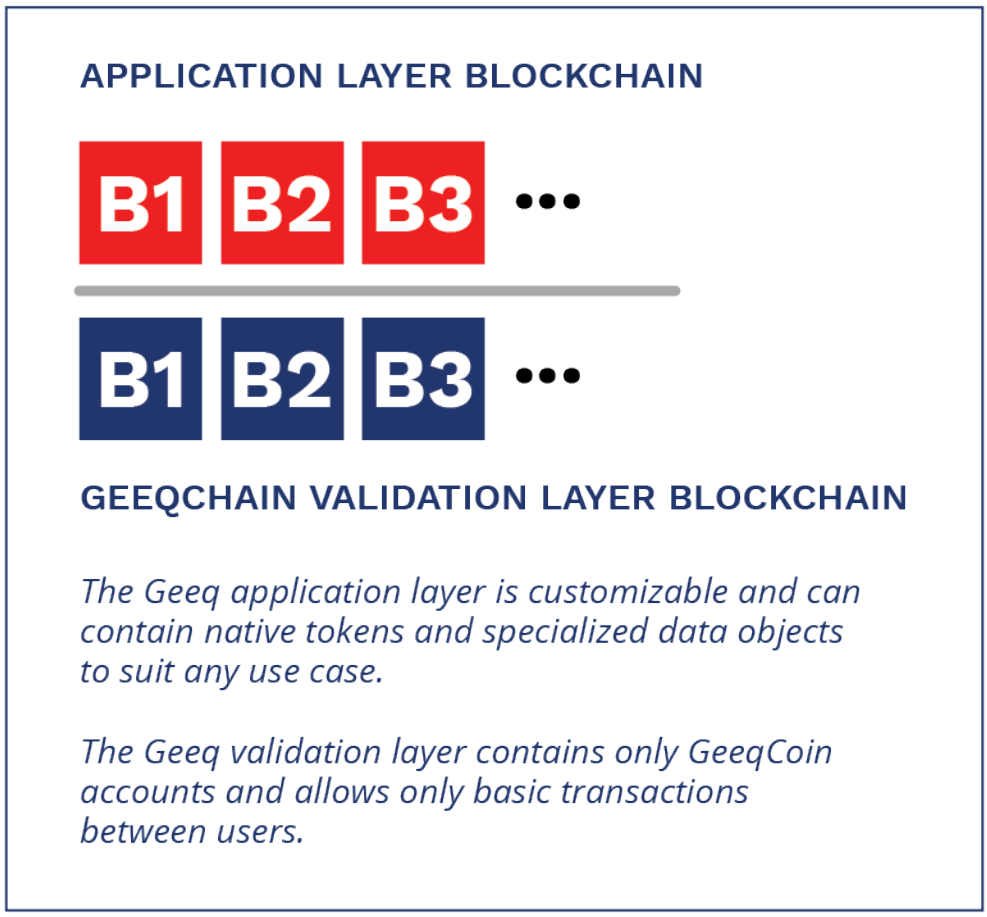
## 3.2 Application and Validation Layers

GeeqChain architecture includes two separate blockchain layers.

The Geeq application layer is designed to allow maximum flexibility. Developers are able to write applications in a variety of programming languages that are then fixed by including them in the application's genesis block. This allows users to know exactly what an application does and to independently verify that the rules are being honestly executed by the network of validators. Applications might include native tokens that are divisible and used for transactions, that tokenize property titles and so are not divisible, that represent ownership of automobiles and so can be created or destroyed by a DMV or other authority, and so on. Data objects of any type could be hashed and kept on the application layer ledger, could be kept off-chain in the IPFS or other data storage solution, could be used as triggering events for smart contracts, etc. Applications could call on outside data-sources, have permissioning or encryption structures, or call on other applications though APIs.

Building in all of these possibilities would create a great deal of complexity and overhead that most developers would never need. Even if GeeqChain did so, it is unlikely we would be able to anticipate what features might be needed in the future. Thus, instead of attempting to build a Swiss army knife that tries to be all things to all users, GeeqChain creates a flexible application layer that is independent of the underlying validation protocol. Developers can create exactly what they need without carrying elements for which they have no use.

14 Recall the consequences of having two Will Rikers in *Star Trek: The Next Generation*, season 6, episode 24 (Second Chances). Unauthorized replication of tokens would completely undermine both the token economics and user confidence in the underlying blockchain. The loss of a star fleet officer or token, on the other hand, is undesirable, but the risk is more at the level of an individual misfortune than an existential threat to the system.




The validation layer is kept simple, robust, and bullet-proof. Users pay transactions fees to validating nodes to move GeeqCoins between accounts, for processing native token transactions, and for running smart contracts that live on the application layer.

The result is that the network of validators functions as a trustless virtual machine to run code written by application developers. Since applications live on their own instance (or instances) of GeeqChain, they do not compete for these services with other applications and so are protected from negative externalities if other applications happen to demand large amounts of computational effort from their own networks. Developers do not need to include code elements or functions that they do not use and this both streamlines applications and reduces potential attack surfaces. Finally, the underlying validation layer is protected from contamination by dangerous smart contract code or having slanderous, racist, or copyrighted material written immutably into the ledger.

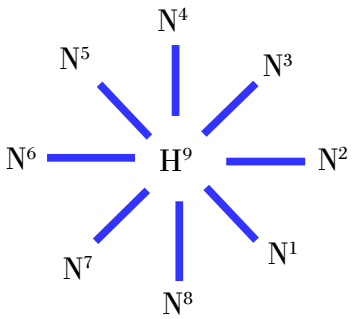
## 3.3 Network and Communications

Nodes are validators of transactions submitted by users for inclusion in new blocks of a GeeqChain. Real world agents (that is, people) download and install a copy of the GeeqChain node client on a computer which can be reached at some IP address. Each active node builds, keeps, and makes available to users, its own copy of the GeeqChain instance it validates.

Bitcoin, Ethereum, and most other blockchains, use peer-to-peer gossip networks to communicate user transactions, distribute newly mined blocks, and transmit other message traffic between nodes. In the case of Bitcoin, for example, users find the IP address of a node and send it a transaction request. This request is then broadcast to a group of peer nodes known to the receiving node, and from there, it spreads out to the rest of the nodes on the network. This is called a "gossip network" since communications are passed from node to node until they are known by the whole of the network. As a result, messages may be repeatedly sent to peers who have already received them from other peers. The time it takes a message to find a path to all members of the network is random and may be non-trivial. Delays in the reception of newly mined blocks, for example, is one of the reasons that Bitcoin experiences forks.

In contrast, GeeqChain uses a random hub and spoke peer-to-peer network. This is more efficient than a gossip network since it transmits the minimal set of messages possible and allows them to reach the entire network more quickly.

The simplest network topology is for a single hub to coordinate the building of each block. For example, a nine node network with node number eight serving as the hub would look like the following:




After any given block B is built and committed, a new hub is chosen randomly to coordinate the building of block B+1. More complicated structures with multiple layers of hubs and random participation rules are possible and may be desirable, depending on the needs of the chain being validated.

The main attraction of gossip networks is that nodes can join and leave anonymously and that no central list or server that might be blocked or manipulated exists. Nodes can come and go as they please. In the Bitcoin protocol, nodes simply broadcast their existence on the gossip network and begin mining blocks. Leaving the network is accomplished by no longer sending or receiving messages on the gossip network.

A hub and spoke network requires a bit more structure. Our approach is to keep a roster of all nodes that are currently part of the network in an Active Node List (ANL) which is maintained as an element of every block that is added to a given instance of a GeeqChain. Membership to the validation network is open, and agents can get themselves added to the ANL by submitting the proper join request transaction to an existing node. Joining as a validating node also requires the posting of a Good Behavior Bond (GBB), explained later. Thus, a join request transaction includes a public key, an IP address, and permission to transfer enough tokens from the public key address to a sys-

tem account to cover the GBB. Agents currently in the ANL can also submit resign requests, in which case the GBB is transferred back to the node's public key account and the node is removed from the ANL.

Note that this ANL approach allows nodes to maintain their anonymity. As in the Bitcoin and Ethereum networks, nothing besides a node's IP address and token account are known. The ANL is also distributed in the sense that it appears identically in the blockchains maintained separately by each of the nodes in the network. There is no central server or single authoritative list that might be blocked or censored.

## 3.4 Genesis Blocks

All instances of GeeqChain begin with a genesis block (block number 0). Blocks of validated transactions are created by nodes in the network and appended sequentially. Genesis blocks are created by GeeqCorp at the request of developers who wish to build applications. This tight control has several motivations.

- It prevents duplication of chain, token, and controlling authority (if any) names.

- It ensures that the chain adheres to the GeeqChain protocols for transaction verification. The 100% BFT that results makes it possible for federated GeeqChains to trust in the integrity of other ledgers and to accept tokens from other GeeqChains.

- It fixes the rules under which the chain will operate. This is done at both the application and validation levels by including copies of the GSCs in the genesis block. GeeqChains can be adapted to many purposes, using different sorts of business logic for native tokens. While the rules for what make a valid GeeqCoin transaction are universal to all federated chains, native tokens might be used to distribute votes, governing power, or profits as rewards for users (as distinct from validating nodes), to tokenize real assets such as stocks, bonds and land titles, and so on. Users can verify that the rules are being followed by doing their own audits and verifications with the help of the GSCs written into the genesis block. Note that the business logic these GSCs contain may also rely on data records written by users into the chain in addition to token transactions.

- The genesis blocks can also include an initial ledger state with initial allocations of native tokens to accounts. The GSCs for applications set out the rules under which these native tokens can be created, destroyed, moved, divided, and so on. This allows users to know going in exactly how the token economics for any given application created on GeeqChain will operate.[15]

This might seem to give GeeqCorp a great deal of power that could lead to potential abuses. However, once a genesis block is created, neither GeeqCorp nor anyone else can alter it or the

15 The token economics, monetary policy, and initial ledger state of GeeqCoins are similarly included in the GSCs of the first instance of GeeqChain created when the mainnet is launched.

operation of the chain that uses it as a foundation. There is simply no mechanism to allow such manipulations to happen. Once launched, each GeeqChain has a life of its own.

# 4. GeeqChain Consensus Protocol

GeeqChain's consensus mechanism is based on two elements. The first is a proprietary protocol for validating blockchain transactions called Proof of Honesty (PoH) which allows GeeqChain to provide users 99% BFT. The second is a system of audits called the Catastrophic Dissent Mechanism (CDM)[16] which brings the security guarantee of GeeqChain to 100% BFT as well as implementing truthful transaction validation in coalition-proof equilibrium.

One of the main attractions of blockchain is the auditability of the records of transactions that allows the accuracy of the ledger state to be independently verified. The problem is that under existing protocols, there is nothing that users can do if they find dishonest behavior. Transactions are sent through a gossip network and so can be seen and processed by all nodes on the network, honest or not. There is simply no way for a user to exclude any nodes he can prove are behaving dishonestly. Even if he could, the protocols define which of the forks that might exist is authoritative. Users have no independent say.

In contrast, PoH takes a new "user-centric" approach to blockchain validation. PoH gives users the authority to determine whether a node, fork, or chain is honest, and to choose to transact only with honest nodes. In other words, users are the arbiters of truth under PoH. Since users hold tokens on the chain which are at risk of being stolen by dishonest nodes, this is inherently incentive compatible. On the other hand, PoW, PoS, Direct Acyclic Graph (DAG), and all other consensus protocols of which we are aware are "node-centric" in the sense that nodes, through some mechanism, are the ultimate arbiters of truth and authority. Since nodes are the agents who might benefit from falsely writing transactions that steal tokens, this creates an inherent conflict of interest.

PoH is extremely simple, but requires three things. First, that users have access to the code and protocols that honest nodes are supposed to run to validate any given blockchain. Second, that the code be deterministic in the sense that a given set of inputs (transactions, blocks, the existing state of the ledger, etc.) produces one and only one output. Finally, that if any node fails to follow the protocol contained in the code, the deviation can be detected and proven by all users.

Of course, it would be unreasonable to think that ordinary users are sophisticated enough to understand a protocol and be able to check a blockchain thoroughly for dishonesty. In practice, checking the honesty of a fork can be done automatically by the client software that users employ to interact with the blockchain (see footnote 15). Due diligence regarding the honesty of forks is therefore effortless and invisible from the user's perspective. The client software can be set to any level of paranoia the user wishes. If a user is about to accept a larger number of tokens, he might have his client inspect the chain and any forks in great detail and insist that the transfer take place

16 See Appendix 1 for a high-level description of the CDM. Readers interested in learning more details about how PoH and CDM work are invited to look at a companion technical paper called "Proof of Honesty: Coalition-Proof Blockchain Validation without Proof of Work or Stake" which also contains proofs of the claims made in this section.

on the fork he considers to be authoritative. On the other hand, if the GeeqChain instance is used for making micropayments between connected devices (IoT or the Internet of Things), then the user may choose to forego due diligence entirely. From a mechanistic standpoint, Proof of Honesty works as follows:

**Proof of Honesty**

1. Chain Discovery: Users discover a given GeeqChain as well as any forks that might exist. In practice, users might be directed to a node that validates an application that a user wishes to use or find a node through a web search or by consulting a forum. Once he discovers any node, however, he can read the ANL and thereby find the IP address of all other nodes that are validating and keeping copies of the GeeqChain.

2. Honesty Checking: Users employ their client software to inspect the chain and its forks, if any, to whatever degree that they wish in order to determine the honesty of the nodes and the validity of the chain or forks.

3. Transaction Creation: Users choose a node and send it a transaction.

To get a sense of how this protocol protects users, suppose that several forks of a given GeeqChain existed. GeeqChain protocol requires that blocks and ledgers contain enough data for users to independently verify that a fork is "honest" in the sense that it contains only valid transactions and that the chain as a whole follows protocol. The absence of the needed data in a fork is in itself proof of dishonesty.

Suppose also that at least one honest node existed who was therefore writing an honest fork. All users can identify both the honest and dishonest forks. Given this, why would any rational user ever accept tokens on a dishonest fork? Such tokens are likely to have been stolen, and are likely to be stolen from any user who accepts them. It would therefore be difficult to convince other users who can also prove that the fork is dishonest to accept stolen tokens at face value in the future. Rational agents will therefore prefer tokens on honest forks to dishonest forks since they are worth more.

Fortunately, if an honest fork exists, PoH allows users to send their transaction to the honest node or nodes that maintain it. All other honest and rational users will do the same. In particular, no rational, honest user would ever send or accept tokens on any of the dishonest forks. As a result, the dishonest nodes would end up writing a fictional ledger that would be completely ignored by self-interested users. The dishonest fork would therefore end up being orphaned. At best, the dishonest fork would include only dishonest agents stealing tokens from one another that no one else would be willing to accept. Given this, the best response of any self-interested node is to behave honestly as well. In short, the existence of a single honest node is enough to compel all the other nodes to follow suit.

To sum up, we have reduced the problem of secure blockchain validation to making sure there exists at least one honest node in the network. It would not matter if there were a hundred or a thousand dishonest nodes in the ANL. If fact, it would not matter if the NSA, Russia, and China

combined their computational resources and flooded the validation network with dishonest nodes. Unlike existing protocols, PoH does not depend on the consensus view of dishonest nodes. Instead, PoH allows users to identify dishonesty and ignore it. Without further elaboration, this simple idea gives the GeeqChain a BFT of 99%.[17]

# 5. GeeqChain as a Solution

GeeqChain has the benefit of learning from Ethereum, which in turn, had the benefit of learning from Bitcoin. Just as Ethereum solved many of the limitations embedded in the Bitcoin protocol, GeeqChain solves most of the problems remaining in Ethereum. In particular, GeeqChain is secure, cheap, fast, and scalable. It can be implemented with fully anonymous verifying nodes, no centralized points of trust or failure, and any level of encryption and privacy protection desired.

## 5.1 Security

We described above how Proof of Honest combined with the Catastrophic Dissent Mechanism give GeeqChains Strategically Provable Security and and 100% BFT. Two additional points are worth discussing here.

First, the CDM are really designed to take care of edge cases that would completely destroy the integrity of blockchains validated by any other protocol in existence. No existing protocol would survive a network which is more than 50% dishonest, while the CDM allows survival even when 100% of the network is dishonest.

Second, PoH by itself provides validation with 99% BFT. An easy way to guarantee that an honest node will always exist is to make sure that there is one trustworthy agent in each validation network. Doing so would ensure that the edge-case that the CDM is meant to deal with never occurs. This could be accomplished by having one or several known and trustworthy agents (banks, accounting or law firms, for example) publicly join the validation network. Such nodes would not be privileged and would have no special power compared to other nodes. However, it is extremely unlikely that such nodes would join in any conspiracy to compromise the blockchain. The fact that they are not anonymous and might therefore be subject to pressure from state actors is not of great concern. Even if these trustworthy nodes were forced to behave dishonestly or violate protocol by court order, they would simply be audited out of the validation network and no harm would be done to the blockchain. Thus, in a practical sense, for a blockchain with a few trustworthy nodes to fail, all of the trustworthy nodes would have to compromised by state actors at the same time that all the rest of the nodes decided to come together as a dishonest coalition of the whole. Even then, we still would have the CDM to rescue the blockchain.

17 Although we call this 99% BFT, it is really $(N-1)/N$ BFT where $N$ is the number of nodes in the validating network. Note that if there is a single honest node, there also exists an honest fork in which all the protocols and logic of the blockchain (business logic, smart contract execution, and so on) are followed and where an honest ledger state may be found.

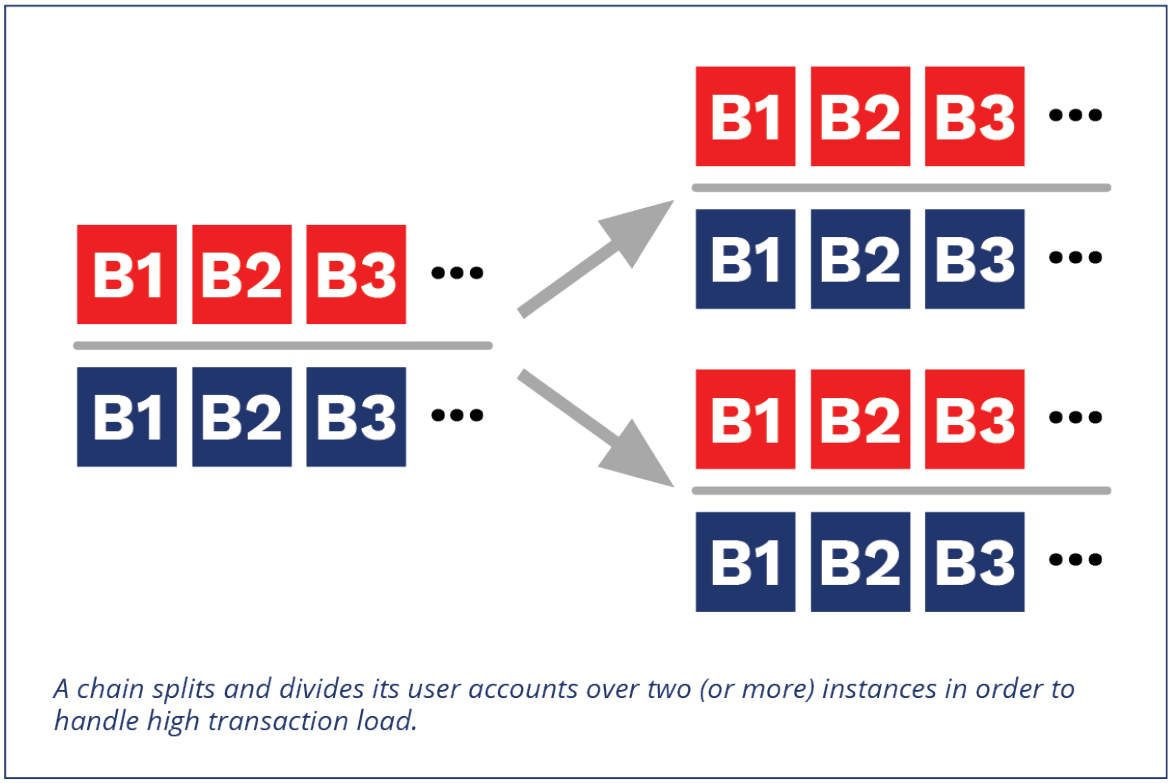
## 5.2 Cost

Using high-side estimates of the amount of bandwidth, compute cycles, storage, and of the costs of these resources, we find that the total cost validation on the 100 node network to be less than $\$.0006$ per transaction. As an example, a transaction of $1¢$ could be validated, committed, and stored on for less than $.06¢$. In contrast, Ethereum transactions cost on the scale of $15¢$ or more and Bitcoin transactions fees can run to several dollars. The cost per transaction scales linearly in the number of nodes. As a result, a GeeqChain that uses N nodes in its validation network, can process a transaction for less than

$$\$6N\times10^{-6}.$$

## 5.3 Scalability

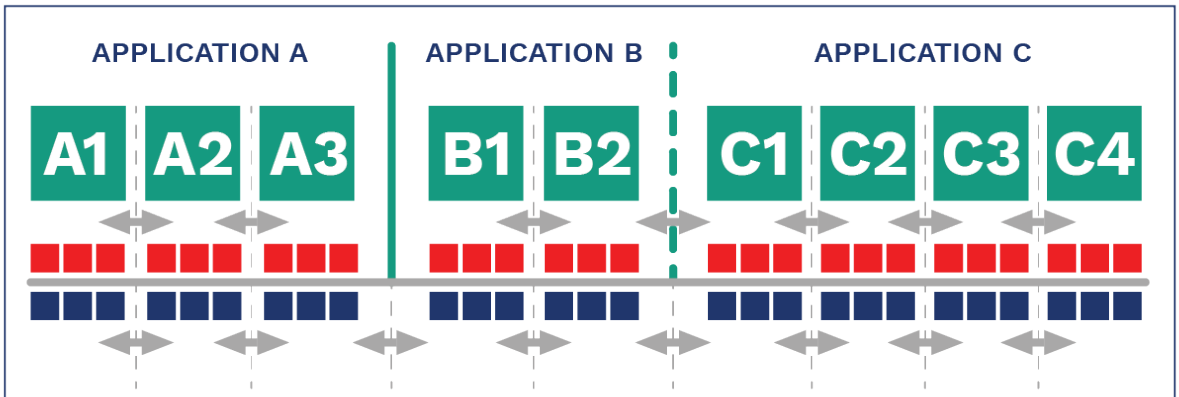
The computational load of running a GeeqChain node (or hub) is relatively small. Home computers should easily be able to handle networks of arbitrarily large size running at 40 or more transactions per second. Ultimately, the number of transactions per second is only limited by the upload bandwidth available to nodes. If a greater transaction volume is required, then a chain is automatically split into as many instances as required to handle the transactions load.




*A chain splits and divides its user accounts over two (or more) instances in order to handle high transaction load.*

## 5.4 Flexibility

Federated chains can be structured to interoperate in a variety of ways. Different applications may choose to exchange applications layer tokens and data objects on any basis they wish. Applications may also choose not to interact with any others. GeeqCoins are always able to move across all instances of all applications within the validation layer. Applications each live on their own instances and have their own set of validators. They are not affected by actions, overhead, or demands of applications in the rest of the Geeqosystem. GeeqChain applications don't step on each others' toes




*Different applications may choose to exchange applications layer tokens and data objects on any basis they wish (Applications B and C). Applications may also choose not to interact with any others (Application A). GeeqCoins are always free to move across all instances of all applications within the validation layer.*

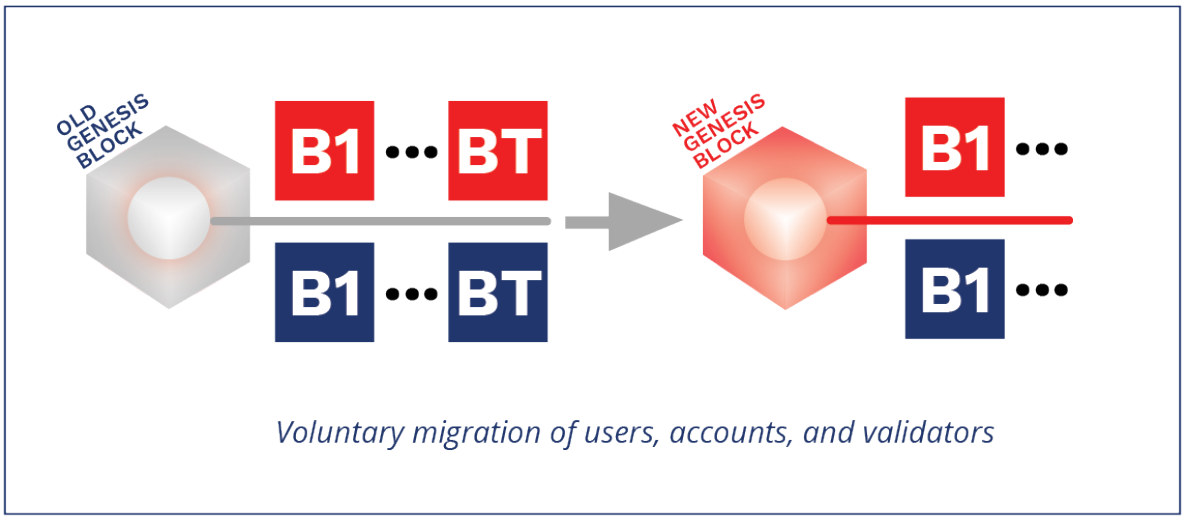
## 5.5 Future-Proofness

Bugs, hacks, upgrades, new functionalities, quantum computing, etc. all make it desirable to be able to let applications evolve and change over time. When hard forks are imposed on unwilling or unwitting users by foundations, developers, or even through complicated governance systems, faith is broken with users and confidence in the platform is undermined.

The system of federated chains that the GeeqChain protocol permits provide an elegant solution to this problem. If an instance of a GeeqChain is found to have bugs, has become obsolete, is not taking advantage of new technologies or meeting current user demands, a new instance could be created with the intention that it replace the existing instance. The new chain would have a genesis block with a new set of validators and GSCs, but no tokens. Users and validators on the old chain could choose to move to the new chain where the rules are different or they could stay where they are. If they choose to move their tokens, their actions are voluntary and within protocol. If they choose to stay, they can continue to live under the old rules. If enough users and nodes support the

continued existence of the original chain, they can trade tokens under the original rules indefinitely.[18]

It will not be too long before 256 bit (or greater) encryption can be broken by quantum computers. This will undermine the security models of all existing blockchains and almost everything else in the cloud. Fortunately, with quantum computational approaches to breaking encryption will come new quantum-proof approaches to encrypting data. GeeqChain's federated architecture allows the creation of new quantum-ready instances of existing chains and applications for users to migrate to as quantum technology matures. This makes GeeqChain more future-proof than any existing blockchain platform.




## 5.6 Monetary Stability

If it were possible to create a "stable-coin" that had a fixed value with respect to fiat currencies, it would relieve a great deal of the public's concern and anxiety about using cryptocurrencies. More generally, the idea of maintaining fixed exchange rates between currencies has a long, but not very happy, history in economics and policy. Central banks over time have often attempted to peg the value of their own currencies to another, to a basket of other currencies, or to a commodity such as silver or gold. Banks support these pegs by standing ready to buy back any domestic currency offered at the promised exchange rate. Unfortunately, such policies have always ended in failure.

18 Hard forks are usually imposed by nodes who collectively decide to alter basic protocol elements or roll back the ledger to invalidate transactions that they consider to be illegitimate. Often this is coordinated by foundations or leaders associated with a given blockchain project. In other cases, the network splits with some nodes choosing one ledger state and/or protocol and the rest choosing another. This can be confusing to users who may have accounts on both forks or who may be asked to choose which fork should hold their accounts. Many new projects include governance systems which make it even easier to change protocols and invalidate "finalized" transactions through voting, staking, or other mechanisms. Users at large do not have any control over what form a blockchain with governance might take in the future. In contrast, GeeqChain empowers each and every individual user to either accept or reject any proposed change to protocols or transactions. Even if all the current nodes and/or a majority of users decide to move to a new instance based on a new genesis block, any users who wish to stay with the original protocols and ledger state may do so. New nodes will appear and offer their validation services to those who stay since they are compensated at the same rate as nodes on the new instance.

GeeqChain proposes to dispense with the idea of a stable-coin and instead develops a new model for a stabilized-coin. At the highest level, this involves keeping a fraction of the fiat currency made from token sales in escrow to be used to smooth out exchange rate volatility and maintain user confidence in the GeeqChain platform. GeeqCorp will sell tokens as the GeeqCoin fiat price on exchanges goes up to fund and replenish a Fiat Stabilization Reserve (FSR) account. In turn, the FSR will be used to buy back and remove GeeqCoins from circulation (putting them in a Token Stabilization Reserve (TSR) account on the chain) if the GeeqCoin fiat price moves down. In effect, GeeqCorp creates additional demand in down-cycles, and additional supply in up-cycles.

Note that this follows, but improves upon, the well-established approaches that nation-states employ to stabilize their own exchange rates. Central banks use their foreign exchange reserves to intervene in currency markets to protect (and in some cases, decrease) the relative value of their own national currencies. Defending a fixed-peg is understood to be an unwise, and ultimately impossible, policy. On the other hand, standing ready to buy or sell significant assets in the event of fluctuations reduces their magnitude and raises investor confidence in the currency (even heading off many speculative fluctuations before they begin).

GeeqCoin's approach offers two major improvements. First, GeeqChain's monetary policy is verifiably feasible, transparent, and fixed. Nation-states, on the other hand, often make promises that they cannot fulfill financially or politically, have opaque and unpublished monetary policies, and are unable to commit to policies as political and macroeconomic priorities change. Second, running down foreign exchange reserves, raising interest rates, printing money and causing inflation, using tax money to support a currency, and deploying similar fiscal instruments, have real and non-trivial costs to a nation and its citizens. In contrast, implementing GeeqChain's monetary policy does not have a direct impact on anyone. The policy is fully pre-funded by design and produces the public good of stabilized token value for the benefit of all members of the Geeqosystem.

A total of 50 million GeeqCoins will be premined with a nominal issue price of $1. These will be be sold in public and private sales or distributed to founders, advisors, and contributors. No additional GeeqCoins will be issued unless and until the market price of GeeqCoin rises to $3. If the price stays below the $3 level, 50 million GeeqCoins are all that will ever exist.

If GeeqCoin prices triple relative to their nominal issuance value of $1, it can only be because the use and transactions volume of the platform have grown as well. Generating additional liquidity is in the interests of the Geeqosystem and will facilitate growth, development, and stability. New GeeqCoins will therefore be produced under an algorithmic monetary policy designed to stabilize GeeqCoin's value. See "The Geeq Project Roadmap and Tokenomics" for complete details.

# 6. Token Use and Business Plan

Ultimately, blockchains can only control things that exist on the blockchain. For example, no blockchain can transfer dollars from one bank account to another. Only real world banks can do this. No blockchain can give you ownership of a house or impose a legal penalty on an agent who violates a contract. Only real world governments and courts can do this.

The reason that cryptotokens exist is that they can be controlled in an immutable and trustless way on blockchains. Tokens can be transferred from account to account, can represent claims, legal obligations, or ownership of assets, and can be held in escrow and used to penalize misbehaving agents. This matters only to the extent that tokens are valued by agents in the sense they that are willing to exchange them for dollars, commodities, work and other things that are useful in the real world, or that courts are willing to enforce claims based on tokens or data in the blockchain.

Given this, a question any blockchain project should address squarely whether it really needs to issue a native token at all. If so, the next question is how many tokens are really required.

GeeqCoin's main function is to pay nodes for their validation and virtual machine services. Each time a user makes a transaction request, nodes also create a transaction fee payment that transfers funds to each node's account. The resource costs to nodes of processing transactions is relatively small, however, attracting nodes, incentivizing them to remain live on the network, and making it costly for nodes to spam or grief the network requires that they be compensated at reasonable levels. (This is why armored car guards are better paid than security guards working in a mall.) Thus, GeeqCoin is needed since the only way to pay nodes is with an on-chain native token. The more applications that are built on GeeqChain and greater the overall transaction volume, the larger the number of GeeqCoins needed to keep the system running.

In addition, given its low transactions costs and rapid transaction finality, GeeqCoins are well suited for micropayments and, in fact, for payments or exchanges of value any size or kind. The monetary policy that serves to stabilize GeeqCoin's value also makes it useful as an escrow instrument and as a way to penalize agents who do not fulfill obligations encoded in smart contracts. Below, we outline several use cases, and show how this integrates into an overall business plan that works in the interest of all agents in the Geeqosystem.

## 6.1 Micropayment Platform

To fix ideas, consider the following example of a GeeqChain based micropayment application. This might be implemented as part of a smart city system to allow citizens to pay for parking, bridge tolls, subway fares, items in vending machines, or minor city services, a platform where consumers buy entertainment, gaming, and other content on the Internet from various providers, or where IoT devices make micropayments via GeeqChain to buy and sell services (CPU cycles, sharded storage, or electricity produced by solar panels, for example).

Transaction Fee Structure

| | |
|---|---|
| Fixed fee to the node receiving the transaction: | .1¢ |
| Percentage fee paid and divided over nodes: | .25% |
| Percentage fee paid to GeeqCorp: | .25% |
| Maximum fee for any transaction: | 10.1¢ |

Transactions Demand

| | |
|---|---|
| Transactions per second: | 10 |
| Average transaction amount: | 25¢ |
| No transactions over $20 | |

If there are 10 transactions per second, there would be a total of approximately 300M per year with a total value of about $80M. If there were 100 validating nodes, each node would receive about 3M transactions per year and be paid $3k in fixed fees. The nodes collectively, and GeeqCorp individually, each get a fee of .25% of the total transactions value, or $200k. This gives each node a revenue of $5k and a net profit of $3.2k. GeeqCorp gets a pure profit of $200k. (We explain below the reason for GeeqCorp's share.)6.2 General Payment Platform

Suppose instead that an instance of GeeqChain was deployed as a general payment platform such as PayPal or Visa/MC. Using the same very low fee structure outlined above, suppose there were 100 validating nodes, 10 transactions per second, but all transactions were over $20. This would imply an annual transaction volume of over $60B. Given that Bitcoin transaction volume in 2017 was about $500B, this is not an unreasonably high estimate. In this example, nodes get a revenue of $150k per year while GeeqCorp gets a net profit of $15M.[19]

## 6.3 More General Use Cases

The two-layered, federated architecture of GeeqChain make it uniquely adaptable to almost any use case. For example:

- Tokenized trading of stocks, bonds, and other assets
- Internal payment networks such as those used on college campuses
- Tokenized transfers of land and automobile titles
- Logistics chains and provenance verification
- Interbank settlements
- Distributed business processes such as real estate transactions, payments of medical and other insurance claims, and coordination of independent contractors and gig economy workers
- Auctions and other two-sided markets (think Craig's List and Ebay)

19 It is worth pointing out that the magnitude of potential profit is much larger than the $25.5M that the project plans to raise in private and public token sales, especially as the Geeqosystem grows and includes many applications, large and small. See "The Geeq Project Roadmap and Tokenomics" for more details.

- Identity and credential verification
- Storing and sharing medical and educational records in privacy compliant ways
- Storing and making available verifiable and immutable public records to improve transparency and responsiveness of government bodies and agencies at all levels.

In some of these examples, GeeqCoin would be needed to complete a secure but trustless transaction. For example, GeeqCoin might be held in escrow and transferred under smart contracts for interbank settlements, real estate transactions, or two-sided markets. In other cases, GeeqCoins would be needed to pay more substantial virtual machine fees to nodes for applications with complicated smart contracts. For example, smart contracts might automate business processes or coordinate permissioning to allow authorized agents to see private financial or medical records stored on external storage services such as IPFS. In all cases, nodes are required to post Good Behavior Bonds in GeeqCoins to become validators. The amount of this stake is proportional to the value of the transactions, data, native tokens, or of what is represented by the native tokens on any given instance of GeeqChain.[20]

## 6.4 Business Plan

GeeqChain is fundamentally about aligning incentives so that agents can interact and work together without needing to trust one another. GeeqCorp's business model follows the same pattern. Transactions fees are shared between validating nodes and GeeqCorp. This implies that the more instances of GeeqChains that exist, the more developers who build applications on the platform, and the greater the transactions volume overall, the more GeeqCorp profits. Clearly, building the Geeqosystem benefits developers, token holders, users. Unlike many projects in which founders benefit mainly or exclusively from money raised through token sales, Geeq's team profits mainly if it continues to build, expand, and improve the platform. We don't ask users to trust us to look after their interests, this is blockchain, after all. Instead we ask users to verify that if we do what is best for us, we do what is best for them as well.

To further these ends, we have set aside 10% of new token revenue specifically to support and develop the Geeq Community. We plan to fund hackathons, provide grants for creating code libraries that can be used by application developers, sponsor events and learning opportunities for coders and others interested in GeeqChain, and do other forms of community outreach. GeeqChain is a more flexible and secure platform than any currently available. The larger the community building applications and experimenting with the technology, the more quickly its benefits will become apparent. We certainly do not have a monopoly on creativity or insight into the best way to solve problems. GeeqCorp is therefore committed to fostering and supporting the blockchain developer community.

GeeqCorp will also jump-start this process by writing its own applications that can be customized for use by enterprises, businesses, and other organizations. As an example, universities often have internal payment networks that allow students to buy books, meals, and other things using their ID

20 See the companion technical paper for details.

cards. This can easily be done on GeeqChain's application layer by creating a branded accounting token that has a fixed value which is backed by the sponsoring organization. This simple template can then be customized and has the potential to be reused thousands of times by different enterprises.[21] Not only does this provide a less expensive and more secure solution than is currently available, but it creates transaction demand for GeeqCoin and grows the Geeqosystem. Developers, users, token holders, and GeeqCorp all benefit as a result.[22]

# 7. Conclusion

GeeqChain is a scalable, inexpensive, and computationally light approach to validating blockchains using a new protocol called Proof of Honesty. The PoH uses anonymous actors as validators who are free to join and leave the system as they please. The mechanism gives all actors strong incentives to behave honestly, both as individuals, and as members of coalitions who might otherwise benefit from compromising the integrity of the blockchain. If there is at least one honest node, it will write an honest block to a valid chain. Users are able to discover honest chains and will always choose it for their transactions. Dishonest chains become orphaned. In other words, if even one node is honest, no tokens can be stolen from rational users. As a result, GeeqChain is 99% Byzantine Fault Tolerant (BFT).

We further develop a system of self-enforcing audits called the Catastrophic Dissent Mechanism that imply that honest behavior on the part of all nodes is the only coalition-proof equilibrium of the validation mechanism. That is, even if nodes are free to communicate, collude, and conspire to act in unison, any self-interested coalition will find that honest behavior gives its members the highest possible payoff. As a result, PoH with CDM creates a blockchain with Strategically Provable Security.

The GeeqChain protocol allows the creation of a Geeqosystem of federated chains. This brings three key advantages. First, it is possible to split a GeeqChain into two or more federated instances and partition the user accounts among them. As a result, GeeqChain is infinitely scalable. If the transactions load becomes too large for one chain to handle, new federated instances can be created until each handles an efficient number of transactions per second. Federated instances can also be merged if transactions volume drops off. Second, new genesis blocks can be created with new features and functionalities. Users and validators can be offered an opportunity to migrate to the new instances bringing their tokens and data with them. This means that improvements, alterations, and bug fixes can be implemented without breaking protocol, creating hard forks, or

21 Thousands of universities, hospitals, and corporations with large campuses use third parties to enable cashless payment systems using ID cards. These cards may be restricted to meal plans and internal fees, extend to dollar transactions at bookstores and local businesses, and may even incorporate credit and debit card functions. CBORD is one of the major providers of such services and charges fees to participating merchants of up to 6%. Additional fees are charged for ATM use, debit card transactions, and even for recharging prepaid versions of such cards. Hong Kong has long used the "Octopus Card" for bus and subway fares and now has an extensive network of merchants who accept this prepaid card for various goods and services. Other cards of this type are linked directly to the VISA or MC payment networks and have standard credit card fees.

22 GeeqCorp's parent, Terepac Corporation, has long experience in the IoT sector. Another early application Geeq-Corp plans to produce will integrate Terapac's "One Machine" hardware and software stack with GeeqChain.

depending on complicated and manipulable governance structures. Users and validators can vote with their feet and can choose to move to the new instance of the application or stay with the old one if they prefer. Third, all GeeqChain instances have separate validation and application layers. This means that applications can be created on their own instance of GeeqChain with their own network of validating nodes and be customized to include any work-flow, business logic, token economics, data-objects, and smart contracting code a use case requires. Applications on different instances can be configured to share tokens or data with one another or may choose to be completely separate. As a result, GeeqChain offers a flexible alternative to Ethereum's ERC20 standard on which to build new blockchain platforms.

Perhaps the most important aspect of GeeqChain is that it offers this level of security and flexibility at extremely low cost. It is not burdened by large networks doing proof of work or stakeholders that need to be compensated for posting large bonds. Validating networks of any size can be used in which each node can still be run on a standard home computer using existing broadband connections. The cost of validating transactions on a 100 node network is less than .06¢ and scales up linearly with the number of nodes.

Finally, the token that powers the validation layer of the Geeqosystem uses an algorithmic monetary policy to stabilize its value. This is intended to increase user confidence in the platform and make GeeqCoin a safer and more attractive medium of exchange for microtransactions and even for larger exchanges of value.

In conclusion, the GeeqChain platform using PoH solves the most significant outstanding problems facing blockchain today. GeeqChain can scale to handle arbitrarily large numbers of transactions per second. GeeqChain can be deployed as a system of federated chains that share a common token or which interact with heterogeneous tokens using different business logic. GeeqChains can be upgraded or altered without the use of hard forks or breaking the rule that code is law. GeeqChain can be implemented with enough anonymity and decentralization to protect user privacy and satisfy most cryptoanarchists, or to comply with KYC, AML and other regulatory requirements. Finally, GeeqChain offers an unprecedented level of transaction verification security at a lower cost than any existing platform.

# Appendix 1. Strategically Provable Security

Needless to say, 99% BFT is an enormous improvement over existing consensus protocols that offer 50% BFT at best. But what if there are no honest nodes? Even though users can see this, PoH depends on the existence of an honest fork, so it would seem that users are out of luck in such a case. The Catastrophic Dissent Mechanism is designed to deal with the possibility that 100% of the nodes are dishonest and able to coordinate their actions to steal tokens or otherwise compromise the integrity of the blockchain.

## Appendix 1.1 An Example of a Unanimity Consensus Game

Let us begin with a motivating example that provides some basic intuition for how the CDM works. Consider the following:

Agents are offered a chance to play a game in exchange for a one dollar admission fee. Each player who pays the fee is sent to a room where a name is written on the wall. Players are asked to write this name on a piece of paper. The papers are then gathered and compared. If they all have the same name, then each player is paid two dollars. If there is any disagreement about the name, all players get zero (which gives each a net payoff of negative one dollar).

It is easy to see that truth-telling is a Nash equilibrium. Suppose that one agent sees that all other players have reported the truth. Clearly, his best response is to tell the truth as well. Reporting the correct name gives the agent a net payoff of $\$1$ while any other report gives him a payoff of $-\$1$.

Unfortunately, this game has many other Nash equilibria as well. For example, suppose at least three players make different reports. All players would get a payoff of $-\$1$ in this case. Since no single player could change his report and generate unanimity, all of the player's strategy choices result in a payoff of $-\$1$. In other words, all reports are (equally bad) best responses for any individual agent.

Alternatively, all the players might get together before the game is played and agree to coordinate on one specific untrue report. In that case, each player would get a payoff of $\$1$ and no single player would benefit from unilaterally changing his report and telling the truth. Of course, coordinating on a false report does not yield a larger payoff than coordinating on the truth, nevertheless, both are Nash equilibria.

In the context of blockchain, it might be the case that players could profit substantially if they coordinated their efforts. Suppose we modified the game so that if all players write down the same name, then the named agent gets $\$1000$. Truth-telling and discoordinated reports would still be Nash equilibria, however, players would profit more if they coordinated correctly. For example, they could agree to write down one of their own names and then split the $\$1000$ received. In so doing, players would still get the $\$1$ payoff for their unanimous reports and would get an equal share of $\$1000$ in addition. Agents, therefore, have a positive incentive to collude, unlike the simple game first described.

To fix this, we could alter the game again to allow a small amount of auditing. Suppose we required all agents to sign their reports. If the reports are unanimous, then agents get a payoff of $\$1$ and $\$1000$ goes to the agent they name. However, if the reports are not unanimous, then the door to the room is opened, and the name on the wall is read. Any player who wrote down the correct name would get a payoff of $\$1$ plus an equal share of a $\$1000$ bonus. Players who lie would receive nothing and be banned from ever playing the game again.

With this addition, truth-telling becomes a dominant strategy. That is, regardless of what other players report, it is a best response for each individual to report the truth. Better still, truth-telling is a coalition-proof equilibrium. That is, no group or coalition of agents, including the coalition containing all the agents, could profit from lying. Even if all agents were able to agree on a false report, any single agent who reneged on the agreement and told the truth instead would get a payoff of $\$1001$. If several agents reneged, they would get to share the bonus divided among the set of defectors (which would be more than the $\$1000$ shared over all players that a coordinated false report gives). Thus, truth-telling is always a better strategy than lying or trying to collude. In other words, truth-telling is the *only* coalition-proof equilibrium. As a result, there would never actually be a need to do an audit and pay the bonus.

## Appendix 1.2 The Catastrophic Dissent Mechanism

We build on the intuition of the unanimity game above to provide a validation protocol that is 100% BFT. More specifically, we develop the Catastrophic Dissent Mechanism (CDM) and show that when combined with PoH, the result is a blockchain with Strategically Provable Security (SPS).

Byzantine Fault Tolerance is the standard metric of blockchain security. We showed above how PoH could achieve 99% BFT. Nevertheless, BFT is ultimately not a good way of thinking about how nodes behave. Nodes on a validation network are not automata that innately work correctly or incorrectly, honestly or dishonestly. Nodes are the agents of the human beings who program and run them. Thus, any meaningful security measure must encompass the motivations and optimal responses of these humans given whatever they might believe about the behavior of other users and validators on the system. In other words, to be meaningful, a security measure should have a game theoretic foundation. With this in mind, we offer the following:

**Strategically Provable Security (SPS)**: A blockchain has Strategically Provable Security if truth-telling and faithful execution of the protocol by all the validating nodes is the only coalition-proof equilibrium for any reasonable belief structure.[23]

We achieve SPS using the CDM which works as follows:

**Catastrophic Dissent Mechanism**

1. Verifying Current Ledger State (CLS) agreement: Before sending a transaction to the hub that is randomly selected to coordinate the building of a block, each node checks the CLS of all the

23 An equilibrium is coalition-proof if there does not exist an alternative joint strategy profile for the coalition of the whole, any subcoalition, or a single agent that yields a higher payoff to all members of the coalition. Also note that if a protocol satisfies SPS, it is also 100% BFT.

other nodes in the validation network. If they are identical to its own, then all nodes are behaving honestly (or at least identically). If any CLS is different, or if the node detects any other dishonest behavior, then the node can initiate an audit.

2. Auditing dishonest nodes: Initiating an audit requires that the node create a special audit transaction and send it to the current hub. The transaction includes a formatted description of the claimed dishonest behavior and supporting evidence from the block or CLS kept by the dishonest nodes. Note that all honest nodes will detect the same dishonest behavior and will create identical audit transactions.

3. Checking audit claims and punishing dishonest nodes: These audit transactions are included in the set of transactions sent back to the nodes by the hub for validation and inclusion in the next block. Nodes verify the audit claims, and if they are true, write a punishment transaction that confiscates the GBBs of the nodes found to be dishonest and shares them equally over nodes who sent in the audit transactions that exposed the dishonest behavior. In addition to confiscating the GBB, honest nodes also write a special ANL transaction ejecting the dishonest nodes.

Now consider what it would take to hold a coalition of all the nodes together in unanimous conspiracy of dishonest behavior. How much could such a conspiracy steal and distribute to its members? This depends on how users would react to blockchain validated by 100% dishonest nodes. Would users simply walk away from their accounts, or would the tokens have some residual value? The smaller the residual value, the less benefit there is from forming such a conspiracy.

The CDM includes a Catastrophic Recovery Procedure (CRP)[24] that allows users to reconstruct the chain starting from the last honest block if they can prove that all nodes are behaving dishonestly. This is a messy and undesirable procedure, but it implies that eventually, a new honest fork will come into existence. As a result, the accounts on the dishonest chain maintained by the 100% dishonest network of validators will ultimately be orphaned. This seems to imply that the only way to profit from dishonest coordination is to somehow move the stolen tokens off the chain before this happens. Of course, this is literally impossible. Tokens can only exist on the chain. Thus, dishonest nodes would need to find a way to *move the value* of the stolen tokens off-chain if they hope to profit.

Moving value off-chain would require that some gullible agent or agents agree to give up something in the real world (or on a different blockchain) to the dishonest nodes in exchange for stolen tokens. For example, a gullible agent might agree to "buy" stolen tokens and transfer dollars to the bank accounts of dishonest agents, or transfer the title of a car to dishonest agents in exchange for tokens written to the gullible agent's account on the dishonest fork. To make this scam work, the conspiracy would need to find gullible agents who are willing to give up significant value despite the fact they could easily prove that the tokens are stolen and will have no value when the CRP is complete. How much might be stealable is unclear, but the CRP will limit this severely.

24 Readers may also wonder what happens if the current hub is dishonest. Why would a dishonest hub send an audit transaction to nodes to verify when this would result in its ejection from the network? See the companion technical paper for details and also for a description of the CRP.

Given this, the CDM works much like the consensus game outlined in the previous section. Suppose that 100% dishonesty allowed the nodes to steal and move off-chain a certain amount of value. Then if the Good Behavior Bonds (GBBs) are sufficient to make launching an audit on dishonest nodes more profitable than joining the conspiracy and sharing the value that can be stolen, then no such conspiracy is sustainable. The companion technical paper calculates the size of the GBB needed and proves that the CDM implements truth-telling in coalition-proof equilibrium.

# Appendix 3. The Roadmap

# Appendix 4. Our Team

# The Geeq Team

## Ric Asselstine

### Chief Executive Officer and Founder

For Ric Asselstine, building out GeeqChain and its flexible platform will be viewed from the future as an inevitable, timely step in Ric's life-spanning habit of bringing disruptive innovations to market.

Up close and in his own time, Ric is a true visionary who has been attuned to the potentials of technology since his first start up in internet search software in 1995. Ric went on to cofound Terepac Corporation, a company originally positioned to develop advanced electronics miniaturization techniques for elegant, inexpensive instruments, which naturally evolved to be (and continues as) an early and successful entrant in the Internet of Things space.

It was about the time Ric fit all the pieces of IoT together, that he saw blockchain coming down the road. As an enterprise solutions guy, Ric realized existing blockchain methods were neither secure nor affordable enough to do what they should. Unwilling to settle for blockchain with holes, he reached out to John to invent the missing pieces, and GeeqChain was born.

Geeq is beyond fortunate to have such a seasoned executive as Ric. Ric has the talent for pulling together the right people, and the patience and know-how to navigate all the legal, financial, regulatory, and jurisdictional hurdles required to bring GeeqChain from inception to world-wide adoption. There is no "can't" in Ric's vocabulary. It's all about "what we can and will do, but let's be smart about it and change the world".

Ric is a graduate of Wilfrid Laurier University (BBA), University of Windsor (MBA) and is the CEO of Geeq Corporation and its parent company, Terepac Corporation.

## Dr. John P. Conley

### Chief Economist and Founder

John P. Conley is an expert in game theory, mechanism design, mathematical economics, and public economic theory. He began his career in the Economics Department at the University of Illinois, where he was promoted to full professor, and eventually moved to Vanderbilt University. John has been a visiting professor at Harvard University, Boston University, Université Paris 1, and Academia Sinica, Taipei. He

founded and continues to edit two academic journals and has long been active in the open access research community.

For the last ten years, John has focused his research on the economics of information and communications technology. Understanding the economics of the Internet, cloud computing, open and closed source software, Software as a Service, connected devices, etc. required him to develop a strong expertise in computer science, network and communications protocols, cryptography, and information theory.

John spent the 2016-2017 academic year as a Visiting Researcher at Microsoft Research in Redmond. He began working on projects involving biometrics, privacy, and the game theoretic aspects of WiFi, PCS, and other radio protocols. In late 2016, he started to explore blockchain as a possible tool to help with these projects. He quickly came to realize how vulnerable existing blockchain consensus protocols based in algorithmic game theory were to attack and manipulation. This led him to explore how economic mechanisms could be combined with elements of information theory and network protocols to produce distributed ledgers with a security guarantee that was really trustworthy. The result was a new consensus protocol called Proof of Honesty ™ which became the foundation of GeeqChain. John also developed the Geeq Project's innovative algorithmic monetary policy which makes GeeqCoin the first smart contract stabilized token.

John is a graduate of the University of Chicago (B.A.) and the University of Rochester (Ph.D.). He enjoys cooking, woodworking, classic cars, and long walks on the beach.

## Darryl Patterson

### Chief Technical Officer and Founder

Darryl has been coding professionally since 1993 (and as an amateur since he was 12). As the CTO of Terepac Corporation, he has been developing IoT solutions long before IoT was even a term. Darryl has learned how to take a research project and turn it into a successful commercial product. He led the engineering team at Terepac, overseeing the scale-up to mass production, the development of the hardened firmware, and the architecture and development of a full-stack IoT solution and software platform.

Darryl is experienced in hiring and managing teams to solve technological problems and has worked on projects for many companies over the years including Dell, Xerox, Intel, GM, Bell Mobility, AmEx, and the Bank of Montreal. He is skilled in a variety of languages and environments such as PHP, NodeJS, Golang, Solidity, IoT MQTT, MongoDB, and RESTful API. Darryl understands the value of structuring projects as logical subsystems and keeping teams on track and coordinated. He also sees the foundational importance of testing and quality assurance and, in particular, making sure that software, hardware, and network elements work together as a robust system in addition to functioning correctly as separate elements. Darryl's exploration of blockchain

began in 2016. He believes that highly scalable and fast blockchain applications will enable a whole new generation of IoT solutions and will help them to go mainstream quickly.

While management and leadership are necessary for any project to succeed, Darryl believes that community is also essential. He is active on GitHub, has taught programing and developed certificate programs at a local college, headed a PHP user group in Toronto, and participates in many other outreach and educational activities. In the case of GeeqChain, Darryl will oversee the development of common code libraries, make sure that the architecture and other aspects of the project are well-documented, and work to make connections between the Geeq Team and the broader community of developers and enthusiasts. Blockchain is a tool that can empower, protect, and create new possibilities in a variety of ways. Helping developers produce creative and innovative applications and making the potential and power of blockchain clear to users is part of the core mission of the Geeq Project. Darryl also likes boating.

## Dr. Stephanie A. So

### Chief Development Officer and Founder

A co-creator of the Geeq validation protocol, Proof of Honesty, Stephanie So is an economist and policy analyst by training. She has always worked to integrate her domain expertise with advances in the technology sector. In 2001, Stephanie was the first to use data mining and machine learning on social science data at the National Center for Supercomputing Applications. In 2003, she was the first economist certified to use the national Pediatric Health Information Systems database. Stephanie started modeling distributed networked processes in health care and patient safety in 2004, and she developed a home visit scheduling and notes management system in 2013. She has most recently turned her focus to blockchain.

The common thread throughout Stephanie's career is her interest in the challenges of people struggling to solve joint optimization problems in the face of physical and/or mental adversity—and how those people might be aided by access to technology. She holds strong convictions that GeeqChain can be used to align incentives for people and organizations of all types, to improve health, well-being and efficiency. This is why she is working tirelessly to ensure GeeqChain will work securely for everyone, under any circumstances.

Stephanie is a graduate of Princeton University (A.B.) and the University of Rochester (M.A., M.S., Ph.D).

Pet peeves: Changes to the original food pyramid
Wishes she had: Rhythm

## Lun-Shin Yuen

### Chief Architect

Lun is a Silicon Valley technologist and entrepreneur who began his career as the third engineer at Intuit. Between 1988-2017, Lun's job positions were described variously as "Head of Engineering", "CTO", and "Principal Software Engineer". He was instrumental in leading development during the high growth early stages of Career Central, Paycycle and Intuit/Quicken.

Lun enjoys the excitement of working through the development process and the thrill of the rapid scale up in companies' life cycles. At Intuit, he found it profoundly rewarding to deliver a financial software program built for ordinary individuals that was then adopted by tens of millions of people.

Lun oversaw the expansion of Quickbooks into their international versions and keeps the needs of both end users and businesses in mind as he works to provide complete solutions in the technology space.

Lun brings rich and deep technical expertise in areas that range from cloud infrastructure to mobile platforms in the fintech space. His proven experience in providing innovative, user friendly services in secure computing environments makes him a key asset as Geeq's Lead Architect.

Lun attended the University of California at Berkeley (B.S. in Electrical Engineering and Computer Science) and Stanford University (M.S. in Computer Science), which evidently gave him a lifelong love for ultimate Frisbee.

## Dr. Eric Ball

### Advisor

Eric has spent most of his career in finance roles at large corporations. His longest tenure was as Senior Vice-President and Treasurer at Oracle Corporation, from 2005-2015. In that role, he raised $52 billion in debt financing to fund 105 acquisitions made by Oracle.

In 2017, Eric co-founded Impact Venture Capital, an early-stage technology venture firm, with Dixon Doll and Jack Crawford. Impact VC focuses on technologies that cut across multiple customer verticals and has invested in companies in artificial intelligence, autonomous vehicles, internet of things, software, and fintech. Eric enjoys the variety of working with different business models, identifying new investment opportunities, and meeting with potential investors for this venture fund.

Eric believes GeeqChain offers an alternative architecture for blockchain that scales better than any other, and has the potential to disrupt the foundational use of blockchain technology. He reminds us that offering a superior technology is a necessary, but not sufficient, condition for success and that Geeq's success will be measured by gaining adoption in a crowded market. As Geeq works toward that success, however, Eric's valuable guidance in the complicated worlds of traditional finance, fintech, and crypto-finance will be a tremendous advantage for Geeq to emerge and flourish in the international marketplace.

Eric is a graduate of the University of Michigan (A.B.), University of Rochester (M.A. and MBA), and the Peter Drucker School at Claremont Graduate University (Ph.D.)

Least-documented analyst day: Was attended by Kim Kardashian, who gave the financial review to the Wall Street analysts (but also strictly forbade anyone but her photographer take any photos).

Eric has survived: A charging elephant, a zebra stampede, Grade-5 rapids, and coaching little league baseball.

## Jay Coshan

### Advisor

From a young age, Jay has realized venture through his passion for psychology and analytical thinking. Successful by the age of 18, Jay began building a property portfolio, enabled by a career in professional online high stakes poker which he continued over the next 8 years.

After 8 years of accumulating and renting properties, Jay transferred his personal experience and understanding of risk management to the world of property development. Here he particularly enjoyed the intricate subjective nature of planning and the evaluation of each site's unique development potential; selling multiple sites for over one million British pounds.

Jay was humbled to be introduced to emerging blockchains and believing in the potential made the decision to shift focus entirely and immersed himself fully. Excited and determined to aid the industry reach to the masses, Jay began enthusiastically growing his network, backing and working alongside teams and individuals to further blockchain implementation.

Jay is delighted to be backing and lending his experience to GeeqChain, which he describes as one of the rare and beautiful projects where someone is building a real and truly disruptive technology that will further the foundation for blockchain adoption.

Jay was the youngest player in England to hold a golf course record at the age of 14, but fortunately for the rest of us, decided to play poker seriously instead.

Although on the face of it Jay looks like the ultimate workaholic, he has always followed his passions and doesn't view a single day as so.

## Dr. Gene Deszca

### Advisor

A consultant and advisor in organizational change, Gene helps businesses and individuals effectively adapt to their evolving realities, enact strategies and change leadership. He has delivered developmental initiatives for middle and senior level managers in public and private sector organizations and mediated educational labor disputes. Gene's interest in entrepreneurship has led to his involvement with a number of early stage firms. He has served on private sector advisory boards and was a member of a publicly traded board (Turbosonic) for 4 years, prior to its acquisition in 2013. He also served six years on the Board of Directors of the Society of Management Accountants of Canada, from 2005 - 2011.

Gene has published and/or presented more than 100 papers, cases, monographs and technical papers, as well as five books. In July 2017, he retired from his position as a Professor and the Associate MBA Director at Wilfrid Laurier University. Gene's current research interests are focused on the evolution of organizations under the stress of market and technical disruption, organizational change and transformation, and the effects of such factors on the people who work there. In addition, Gene has known Ric for over 20 years. This is what makes Gene the perfect addition to Geeq Corporation—he knows how to guide this particular organization and its leadership toward maximum positive disruption of the blockchain industry.

## Blaire Gateman

### Advisor

After graduating from the University of Guelph with a literal passion for building, Blaire started his own construction company. An expert in scale ups and organic growth, he built his business to more than 500 employees over the span of 34 years and counting. His company completed projects across Canada, including the construction of some of Canada's most prestigious golf courses.

An expert in contract negotiation and in nurturing long term working relationships with disparate businesses, Blaire's long history of large and prestigious projects, resulting in satisfied customers and employees. will lend the precise advice Geeq Corporation needs to onboard Geeqs of all kinds: businesses, developers, and users, as they discover the potential of interacting with Geeq's flexible platform.

Hobbies: Blaire is a non-stop builder who varies the scale for fun. He has never stopped building homes and, when he can be found in his own home, he enjoys building fine furniture. If anyone doubts blockchain will ever be put into practice, please note the Geeq team is full of people who won't be satisfied until they see positive, tangible changes made real in the external world.

## Kurt Hoppe

### Advisor

Kurt Hoppe is the Global Head of Innovation at General Motors and is willing to share the secrets of his tremendous track record as an Advisor to Geeq. Kurt has driven the development and launches of award-winning, value-added services, focused at the intersection of Connected Consumer IoT devices, digital services, and Tier-1 service providers. At GM, Kurt's team is at the forefront of rapid prototyping and in-market testing of Connected Car services. Prior to GM, Kurt's career-long portfolio of accomplishments includes leadership roles in international IoT platform and services applications in: multi-screen media and entertainment, home automation, eHealth, and eGovernment services for global service providers and their subscribers.

Not surprisingly, Kurt graduated at the top of his Computer Science class at the Royal Military College of Canada and studied Human Computer Interaction and AI at the University of British Columbia. Kurt's success in the widespread adoption of IoT strategies and B2B solutions have earned him the trust of global enterprises, such as AT&T, Time Warner Cable, Best Buy, Chrysler and GM. Geeq will call on Kurt frequently to ensure Geeq's platform and products are developed with ready input from enterprises and consumers about what they want and need.

## Murray Gamble

### Advisor

Murray Gamble is President of The C3 Group of Companies, a multi-disciplinary engineering, contracting and applied technology organization headquartered in the Waterloo Region. Murray is an active entrepreneur who has established a number of companies with his partner, Cameron Wood. Murray is a mentor to several start-up technology companies, and sits on the boards of directors of corporations, industry associations, academic institutions, and not for profit organizations, including the Golden Triangle Angel Investors Network and the Board of Governors at the University of Waterloo.

Murray is well-known for his dedication to collaborative community building and has become increasingly involved in all aspects that drive the area's vibrant economic development and growth.

A graduate in civil engineering from the University of Waterloo, Murray is one of Geeq's many links to the developer talent pools, research institutions, and thriving businesses that have coalesced in Waterloo.

## Tom Hunter

### Advisor

As our legal and compliance expert, Tom ensures Geeq Corporation's foundation is safer and better thought out than the great majority of our competitors. He is a partner at the international law firm Gowling WLG in the Waterloo region office, which has been focused on technology and startups for many years. Tom specializes in assisting entrepreneurs with startup and growth-oriented companies, M&A, and all aspects of equity and debt financing. He also serves as an office leader member of the firm's Technology Industry Group. Tom has served as lead counsel for more than $1.5 billion of profitable exits for high-tech and traditional economy clients, and he currently serves on eight private technology company boards based in the Waterloo region technology cluster.

A strong community supporter, Tom is currently the Co-Chair of the Resurrection Secondary School Council, past Chairman of the Board of Governors of St. Mary's General Hospital, and the past Chair of the Waterloo Region Catholic Schools Foundation. He is actively involved with the Schlegel Centre for Entrepreneurship at Wilfrid Laurier University and is a member of the Advisory Council for the Centre for Business, Entrepreneurship & Technology at the University of Waterloo. Tom is a frequent guest lecturer on matters relating to M&A, financings, corporate governance, entrepreneurship and privately-owned enterprises. He was a contributing author to the recently published book, *The Entrepreneurial Effect: Waterloo*.

In spite of and in concert with Tom's extremely busy schedule, Tom has positioned the Geeq Corporation to enter the world's markets with all engines set to go.

## Dr. Simon Wilkie

### Advisor

Simon is a polymath who has the uncanny ability to identify, understand, and integrate every aspect of any technical problem he studies. To wit: Simon is a theoretical economist who has used his core training in game theory and market design to become an expert in all matters related to the telecommunication industry: the technologies used, how they coordinate or interfere with each other, and the economic, legal, industry, and consumer

trade-offs that must be considered when entering new markets or making regulatory and policy decisions about existing markets.

Simon started out as a Post-Doctoral Fellow and became a Member of Technical Staff at Bellcore, the major research and development arm for the seven regional telephone companies formed after the breakup of AT&T. Simon's basic research in cooperative and non-cooperative game theory, as well as characterizations of bargaining solutions, led him next to the California Institute of Technology. In residence at CalTech for a total of ten years, Simon spent a year in Washington, D.C. when he was appointed Chief Economist of the Federal Communications Commission. Simon is now a pre-eminent authority on spectrum auctions and telecommunications policy and regulation, with a detailed knowledge of the telecommunications protocols, bandwidth, and network configurations that will be required for the Internet of Things.

Simon also has served as the Chair of the Department of Economics at the University of Southern California, with co-appointments in the USC Law School and USC's Annenberg School for Communication and Journalism, and soon will become the Dean of the Monash Business School in Melbourne, Australia. Friends for years, Simon and John most recently overlapped at Microsoft Research, where Simon focused mechanism and market design and the monetization of data from IoT telemetry for enterprise customers, while John worked on the blockchain architecture that would enable such efforts.

Best summary of Simon's personality: He's Australian.

# References


Aiken, S. (2018) "Lightning Network: 27 concerns about UX and centralization" https://medium.-com/crypto-punks/lightning-network-ux-centralization-b517037b92ec.

Cachin, C. and M. Vukolic (2017) "Blockchain Consensus Protocols in the Wild" ArXiv e-prints, http://adsabs.harvard.edu/abs/2017arXiv170701873C.

CNBC (2018) $1.1 billion in cryptocurrency has been stolen this year, and it was apparently easy to do" https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html.

Conley, J. (2018) "Proof of Honesty: Coalition-Proof Blockchain Validation without Proof of Work or Stake" Manuscript. https://www.geeq.io/wp-content/uploads/2018/08/technical-paper.pdf

Conley, J. (2018) "The Geeq Project Roadmap and Tokenomics" Manuscript. https://www.geeq.io/wp-content/uploads/2018/08/tokenomics.pdf

Diar.co (2018) "Lightning Strikes, But Select Hubs Dominate Network Funds" https://diar.co/volume-2-issue-25/.

Eyal, I and E. G. Sirer (2014) "Majority is not enough: Bitcoin mining is vulnerable" In Financial Cryptography and Data Security 18th International Conference, FC 2014, pages 436–454.

Gou, S, (2017) "Cypherium: A Scalable and Permissionless Smart Contract Platform", Draft v1.0. www.cypherium.io/wp-content/uploads/2017/03/cypherium_whitepaper.pdf

Lansana (2018) "Why Hashgraph will never replace Blockchain" https://medium.com/@Lansana/i-was-wrong-hashgraph-is-actually-very-bad-bf7d9b2e8d99.

Zheng, Z., S. Xie, H.-N. Dai, and H. Wang (2017). "Blockchain Challenges and Opportunities: A Survey" International Journal of Electric and Hybrid Vehicles, pp. 1–23.

# Disclaimer

This document does not constitute a solicitation or offer to buy or sell any security or any token in Geeq Corporation and cannot be relied upon for making an investment decision. This document has been prepared and circulated for informational purposes only and is not intended to provide investment, legal, accounting or tax advice or recommendations to any recipient and should not be considered a recommendation to purchase or sell any particular security or token. You should consult your tax or legal advisor about the information contained in this document. This document does not constitute an offering memorandum of Geeq Corporation under applicable Canadian securities laws and does not attempt to describe all material facts or material information regarding Geeq Corporation, its business and operations or its tokens. Any private offering of tokens will only be made to qualified accredited investor. Geeq Corporation has not filed a prospectus or offering memorandum with any securities commission or similar authority in Canada or elsewhere in respect of the tokens and, accordingly, the tokens will not be qualified for sale in Canada or elsewhere and may not be offered or sold directly or indirectly in Canada or elsewhere, except pursuant to an exemption from the prospectus and registration requirements of applicable securities laws. No securities commission or similar authority in Canada or elsewhere has reviewed or in any way passed upon the merits of an investment in Geeq Corporation or its tokens, and any representation to the contrary is an offense. All of the information contained in this document is for preliminary discussion purposes only. Final terms and conditions may change without notice and are subject to further discussion and negotiation.