John P. Conley
Stephanie A. So

DARPA ABC Workshop

Geeq

Making Blockchain Secure at the Edge

February 14, 2019

Introduction

This talk will focus on three major points:

- Why are databases and public and private blockchains insecure?
- What do we need?
- How can we get it?

Why Are Databases Insecure?

Databases, distributed and otherwise, have the following problems:

- Firewalls – Subject to hacking, dependent on the competence and vigilance of the network security team, and the care and savviness of the users.
- Centralized – One or a few copies of the data, central control of credentials.
- Access – If users come and go, often from outside the organization, keeping credentials and permissions current is difficult to do securely.

Why are Private Blockchains Insecure?

- Firewalls – As above.
- Centralized – Often one master chain with few copies. Small fixed validator set.
- Access – As above.
- Consensus – Rely on Byzantine Fault Tolerance (BFT) and an honest, unhacked majority.

Why are Public Blockchains Insecure?

- Centralized – Generally one master chain, sometimes less secure side chains or channels.
- Consensus – Both Proof of Work (PoW) and Proof of Stake (PoS), in its many variations, rely on BFT and an honest, unhacked majority.
- Directed Acyclic Graph (DAG) – DAG approaches have an equally bad set of security problems.

What Is Wrong With BFT?

BFT has its roots in algorithmic game theory:

- Agents are often modeled as following *ad hoc* behavior patterns. For example, agents might be assumed to be either honest or malicious-type players since fully rational play may exceed their cognitive limitations.
- Economists don't think that anyone is honest. We assume that agents are self-interested.
- The question to an economist is how to design a game theoretic mechanism that harnesses this self-interest to get the desired outcome.

What Is Wrong With BFT?

Problems with designing a mechanism:

- Multiple equilibria – Proving that there exists a Nash equilibrium in which the validators are honest is meaningless. Games typically have many equilibria, some good, some bad.
- Wrong equilibrium concept – Nash, dominant strategy equilibrium, subgame perfect, sequential ... All are too weak, dependent upon assumptions about information and expectations, and not proof against coordinated actions of coalitions.

What Is Wrong With BFT?

Problems with designing a mechanism:

- Wrong game – A game is a set of players, a strategy space, and payoff functions.
  - Players – Users, ISPs, Sybils, foundations, leaders? Not just nodes.
  - Strategy – Network manipulation, withholding blocks, not following protocols, faking partitions? What actions are available to players?
  - Metagame?
    - Nation states may not care about financial payoffs.
    - The value of the information or assets on a blockchain may exceed the cryptocurrency incentives for validators to be honest.

What Do We Need?

A distributed data technology that:

- Assumes adversaries are already in the system.
- Assumes adversaries are motivated by things besides economic incentives.
- Assumes the adversary can become a large fraction of the nodes/validators.
- Has no central points of failure.
- Is parsimonious and simple.
- **Implements honest behavior on the part of users and validators for the metagame in coalition-proof equilibrium.**

How Can We Get It?

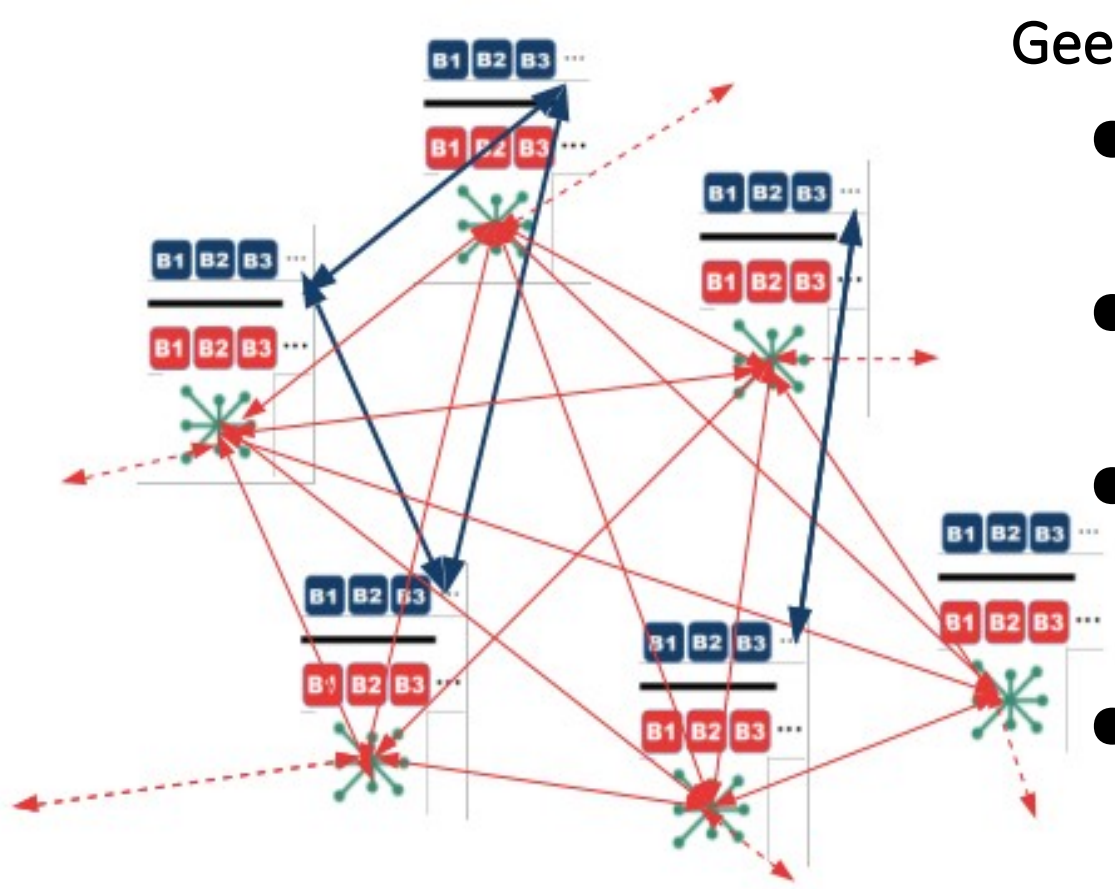
Geeq is a secure ecosystem for independent but interoperable blockchains.

- Proof of Honesty (PoH) – 99% BFT consensus mechanism. PoH works as long as at least one node is honest.
- Catastrophic Dissent Mechanism (CDM) – An audit game/mechanism that implements truth-telling in coalition-proof equilibrium.
- Federated architecture – An ecosystem of blockchains, each with its own independent set of validators and customizable application layer.
- Privacy/Secrecy – Granular permissioning on public blockchains.

Proof of Honesty

- Any attempt by validators to deviate from Geeq's consensus protocol is immediately and automatically detectable to the user through Geeq's user client.
- Users are able to identify and ignore dishonest validators and refuse to accept transaction/messages on provably dishonest ledgers.
- **Security is at the edge rather than depending on the center**
- Users are empowered to protect themselves, which is incentive compatible.
- The BFT requirement that the majority of validating nodes be honest in other protocols builds in an inherent conflict of interest.
- CDM – Ask me later or see our technical paper.

Scalable and Decentralized



Geeq is a network of networks

- Applications can be created on one or several instances of GeeqChain.
- A single GeeqChain instance can execute 40 TPS or more.
- The Geeq ecosystem as a whole can have as many instances as needed to meet any transaction demand required.
- GeeqChain applications don't step on each others' toes and are not affected by actions, overhead, or demands of applications in the rest of the Geeqosystem.

Conclusion

- Existing approaches to distributed data systems have central points of failure, many attack surfaces, and lack flexibility.
- Any security model based on BFT is just not good enough. A majority vote of incompletely incentivized agents with varying agendas is not a dependable way to determine truth, protect value, or secure data.
- PoH allows users to protect themselves from dishonest nodes and makes it unprofitable regardless of their agenda.
- Geeq's architecture allows the creation of ad hoc instances of a blockchain as needed for specific purposes with open participation. This allows coordination of heterogeneous types of agents without endangering other databases or applications and keeping storage and connectivity needs to a minimum.

Thanks for Listening!

For more information:

Geeq.io

White Paper
Technical Paper

Stephanie.So@Geeq.io
John.Conley@Geeq.io

Extra Slides

Geeq

Public Blockchain Infrastructure-as-a-Service

February 7, 2019

What is Geeq?

A secure ecosystem for independent but interoperable blockchains.

- A new protocol that empowers users to protect themselves.
- An architecture with a flexible application layer firewalled from a secure validation layer.
- Unlimited scalability built into the ecosystem by design.
- Unique tokenomics that stabilizes the GeeqCoin and reduces uncertainty.

The Problem

- Security: Proof of Work (PoW) protocols are only 50% Byzantine Fault Tolerance (BFT). Proof of Stake (PoS), and Directed Acyclic Graph (DAG) approaches are only 33% BFT.
- Scalability: Limited TPS and competition for computation, storage, and bandwidth between users.
- Lack of Decentralization: A single mother chain or validator set, governance through a foundation or committee, central points of trust or failure.
- Cost: High transactions fees or large resource costs imposed on users to validate transactions.

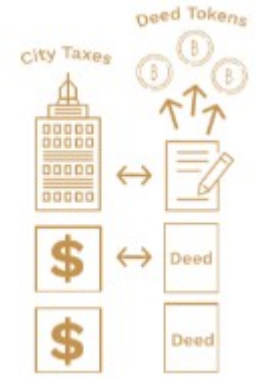
The Geeq Security Solution

- The Geeq Project has developed a new consensus protocol called Proof of Honesty (PoH).
- Unlike PoW. PoS, and DAGs which require that at least 50% of the validation network be honest, PoH works even when almost all of the network is dishonest.
- PoH is not vulnerable to attacks by centralized mining pools, groups of wealthy stakeholders, or even hostile state actors.
- PoH gives 99% BFT and additional audit protocols based on economic mechanism design provide fallbacks ensure that 100% dishonesty is never possible.

How Does PoH Work?

- Any attempt by validators to deviate from Geeq's consensus protocol is immediately and automatically detectable to the user through Geeq's user client.
- Users are able to identify and ignore dishonest validators and refuse to accept payments on provably dishonest ledgers.
- Users are empowered to protect themselves, which is incentive compatible.
- The requirement that the majority of nodes that validate transactions and write the ledger be honest in other protocols builds in an inherent conflict of interest.

Geeq Architecture



Application Layer Blockchain

B1 B2 B3

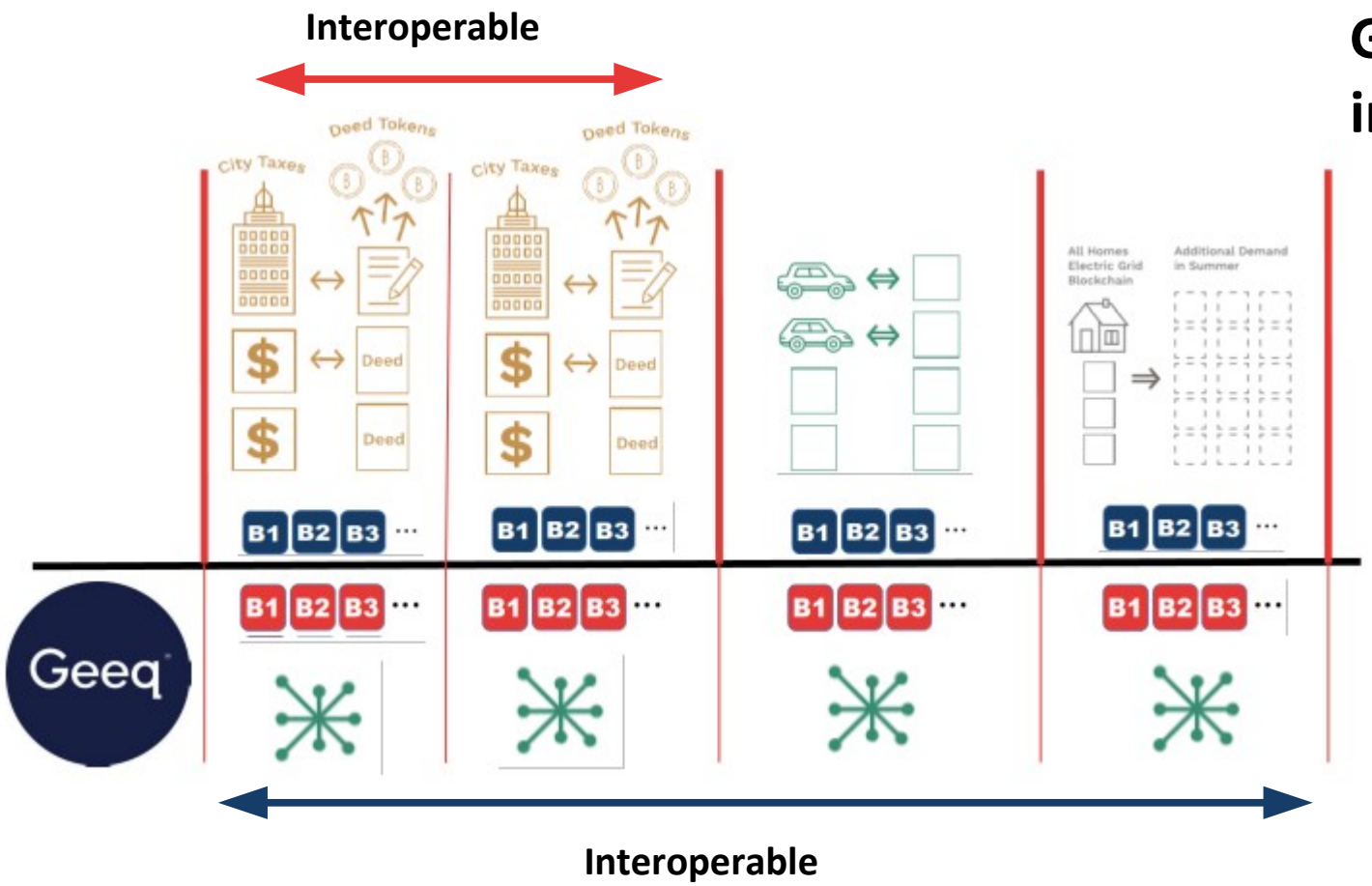
B1 B2 B3

Validation Layer Blockchain

GeeqChain architecture is built on two separate blockchain layers.

- The Geeq application layer is customizable and can contain business logic, smart contracts, native tokens and specialized data items to suit any use case.
- The Geeq validation layer is firewalled and contains only GeeqCoin accounts and allows only basic transactions between users and to pay validators

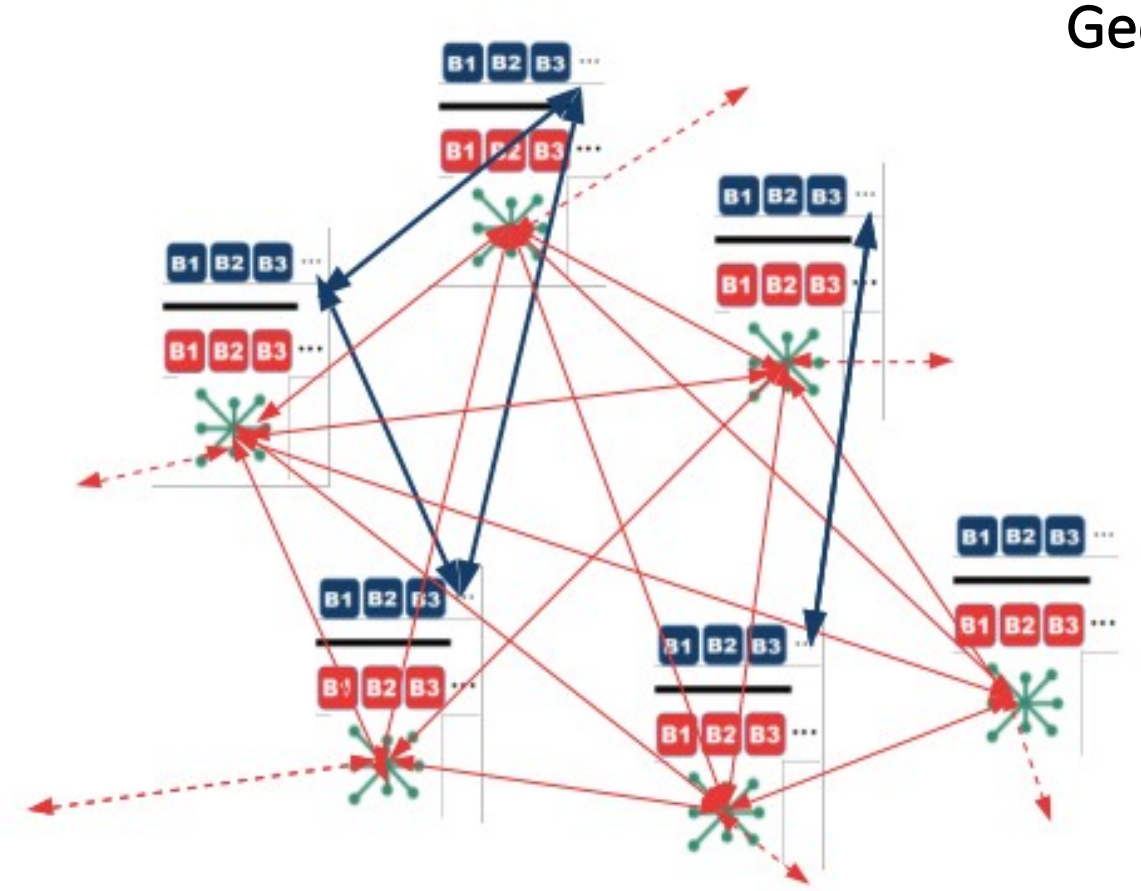
Geeq Interoperability



Geeq's Federated chains can interoperate in a variety of ways.

- Different applications may choose to exchange applications layer tokens and data items on any basis they wish.
- Application may also choose not to interact with any others.
- GeeqCoins are always free to move across all instances of GeeqChain within the validation layer.

Geeq Scalability



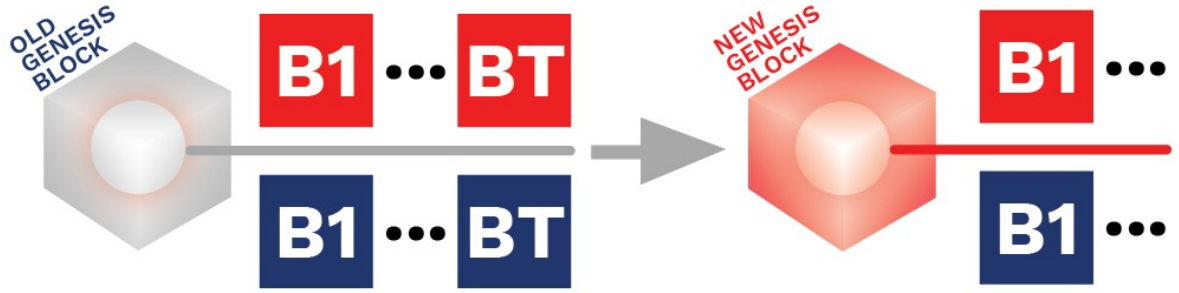
Geeq is a network of networks

- Applications can be created on one or several instances of GeeqChain.
- A single GeeqChain instance can execute 40 TPS or more.
- The Geeq ecosystem as a whole can have as many instances as needed to meet any transaction demand required.
- GeeqChain applications don’t step on each others’ toes and are not affected by actions, overhead, or demands of applications in the rest of the Geeqosystem.

Geeq Decentralization

- No mother chain, side chains, or channels.
- Each GeeqChain is created equal with an independent network of validators.
- Each instance is built from a genesis block that includes a signed copy of both application and validation protocols.
- Code is Law. Hard forks imposed by foundations, developers, governance, or any central authority break faith with users and undermine confidence in the platform.

Future-proof and upgradable



- Bugs, hacks, upgrades, new functionalities, quantum computing, etc. all make it desirable to be able to let applications evolve and change over time.
- Upgrades can be made through the creation of new genesis blocks for applications and then allowing each user and validator to vote with their feet, migrating to the new, or staying with the old, as they choose.
- Code is law and GeeqChain never imposes a new law on unwilling users.

The Best Thing of All

- Geeq is a generalized infrastructure blockchain project.
- GeeqChains can be customized to support standard payment networks, distributed business processes, various kinds of two-sided markets, etc.
- What makes GeeqChain truly unique is that it provides security, flexibility, scalability, and stability at a cost of **less than $.0001** (1/100th of a cent) per transaction.
- This opens up a whole world of new possibilities for applications with high volumes of transactions having low individual value.

IoT on Geeq

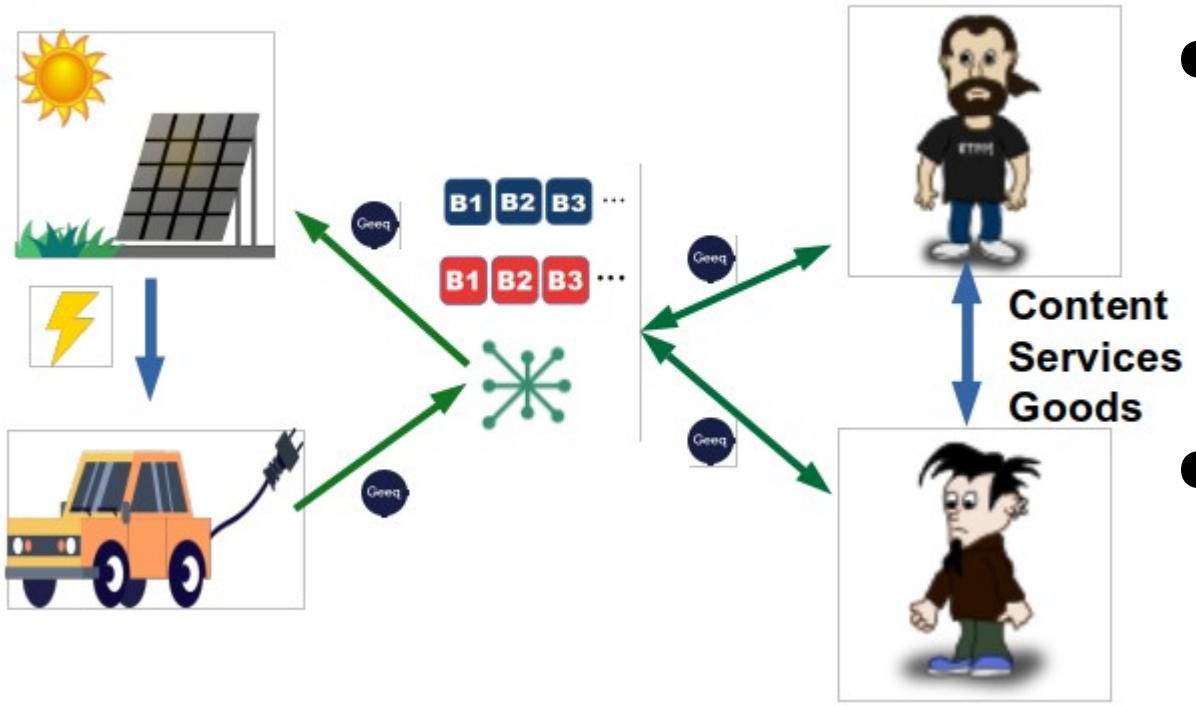
A device can create hourly records on GeeqChain for less than $.90 per year, and minutely records for less than $50 per year.

Recording telemetry from the billions of IoT devices that are increasingly in control of our electronic and physical environments:

- Creates accountability
- Decreases potential liability
- Increases transparency
- Protects privacy

We envision an ecosystem with thousands of GeeqChains.

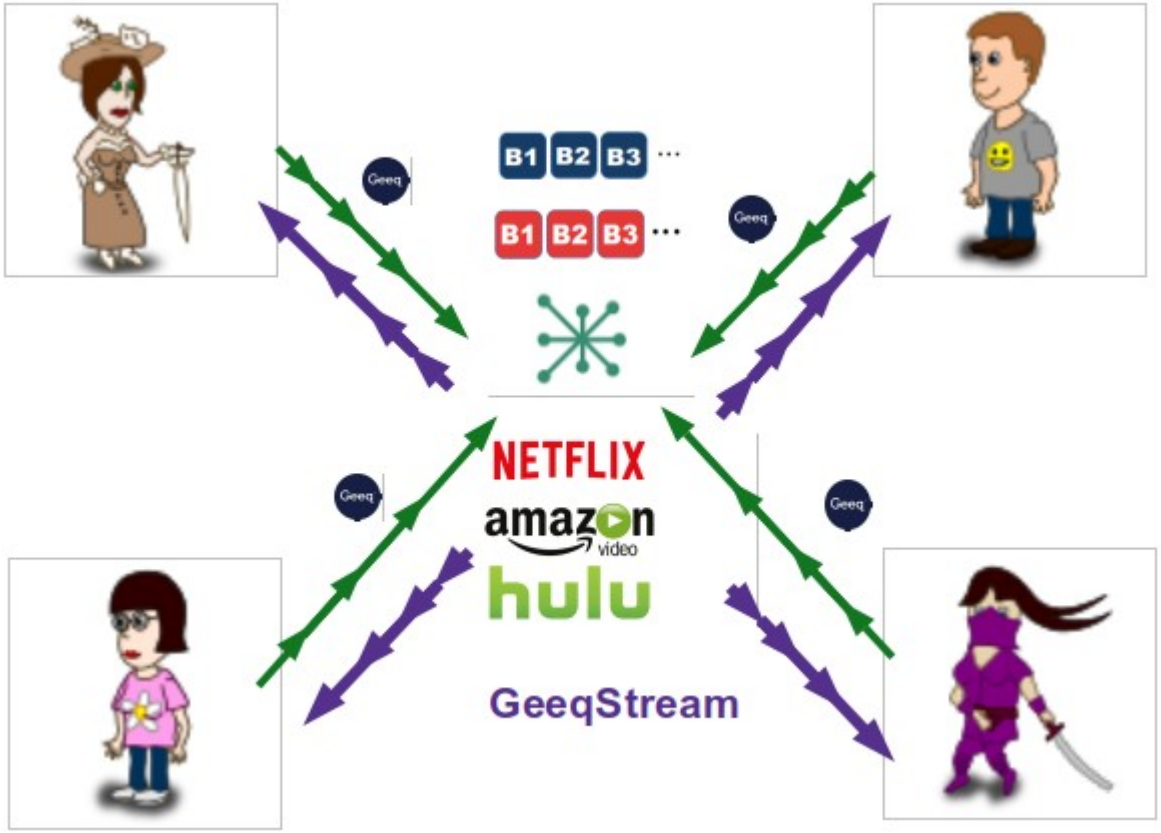
Micropayments on Geeq



Payments of one penny can be made at a transactions cost of 1% or less.

- Person to Person micropayments allow content creators and service providers of all kinds to sell directly to consumers instead of depending on centralized platforms.
- Micropayments also enable Machine to Machine markets and allow devices to act in the interests of their owners instead of their manufacturers.

Streaming Micropayments



- Streaming micropayments allow the debundling of subscriptions so users can pay as they go for games, content, and other services.
- Geeq's proprietary PoH and other technology enables a whole new world of disintermediation and peer to peer economic exchange.

Geeq’s Business Model

Geeq’s basic business model is to charge three times the resource cost for validating transactions.

- 2/3rds is paid to validators
- 1/3rd is paid to Geeq

Validators cover costs and make a profit equal to costs.

Geeq makes the same profit as validators.

Both Geeq and validators are incentivized to participate, build, and improve the Geeqosystem.

Geeq’s Business Plan

- Our parent company, Terepac, produces a full stack IoT software and device sensor platform that is host-object and vertically agnostic (any object, any data). GeeqChain will provide the blockchain layer to this stack.
- Geeq will build out IoT, micropayment, and other basic applications so that GeeqChain will be useful as soon as it is deployed.
- Geeq is partnering with existing IoT, payment, and application developers to build on GeeqChain.
- Geeq has put aside part of our funds to sponsor independent developers to build on GeeqChain.

Problems with Tokenomics

- Volatility of ETH, BTC, and other cryptocurrencies has undermined user confidence in blockchain.
- The large amounts of privately held or non-circulating tokens in Ripple, TRON, Stellar, NEO, and other projects have led to concerns about market manipulation and sustainable value.
- Stablecoins that are not fully asset backed are unworkable.
- Token value is ultimately dependent on token usage and the Quantity Theory of Money. Very few projects do this math when issuing tokens or in defining their monetary policies.

Geeq’s Tokenomics

- The Geeq Validation Layer is entirely powered by GeeqCoin.
- Innovative **Stabilized-Coin** and monetary reserve system dampens unwanted volatility, allows growth, and creates a vehicle for funding new development and community support.
- Monetary policy is committed to an algorithmic smart contract.
- Please see The Geeq Project’s Tokenomics Paper for details.

Compliance

- We always have been and will continue to be compliant with securities and other laws and regulations.
- We have excellent Waterloo based legal support, and compliant financial and crypto services in Gibraltar.
- We are conducting a private token sale to accredited investors which maybe followed by a token distribution event backed by an offering memorandum.

Geeq's Vision

To provide a source of provable and immutable truth that:

- Allows widely distributed agents, including machines, who neither know nor trust each other, to create and share value.
- Provides counter-balance to the growing power of governments, corporations, and other centralized authorities.
- Enables machine to machine markets and records keeping that allows devices to act in the interests of their owners instead of their manufacturers.
- Creates new micropayment based market places that allow people to exchange goods, services, and content without the need for a centralized intermediary.

The Geeq Team

Expertise in: Hardware and Systems Design, IoT Stack Building, Project Development, Game Theory, Economics, Mathematics, Finance, Law, Telecommunications Technology, Medical Informatics

Experience with: Software and Technology Startups and Scaleups, Venture Capital, Oracle, Intuit, Microsoft, Bellcore, General Motors, and research universities including, Vanderbilt, CalTech, UIUC, the University of Waterloo and Wilfrid Laurier.

Focused on: Integrating our expertise to overcome the persistent technological limitations in Distributed Ledger Technology (DLT) and then building a solution that addresses the real problems facing businesses, governments, and consumers.

Ric Asselstine

Chief Executive Officer

John Conley

Chief Economist

Stephanie So

Chief Development Officer

Darryl Patterson

Chief Technology Officer

Lun –Shin Yuen

Chief Architect

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.