G10 COIN

Blockchain 2.0

WHITE PAPER

info@G10Coin.com
www.G10Coin.com

ABSTRACT

Welcome to G10 Coin, the self-amending cryptocurrency with embedded AI. G10 Coin is supported by its own blockchain architecture.

The proof-of-stake system on which the G10 seed protocol is based supports Turing smart contracts processing functionality. The operations of existing blockchains are simply functional modules extracted into a network operation shell. As such by implementing the correct interface to the network shell layer, all existing cryptocurrencies e.g. Bitcoin, Ethereum etc. can exist within G10 Coin ecosystem.

For the rest of this white paper an understanding of the Bitcoin protocol and basic cryptography principles is assumed.

G10 Coin's governance principles will enable greater stakeholder involvement in the evolution of the cryptocurrency. Moreover, the collaboration between stakeholders, regulators and central banks within the G10 Foundation will ensure expedited market exclusivity and market penetration.

G10 is the global standard for Blockchain 2.0.

CONTENTS

1. INTRODUCTION

Since 2008, with the introduction of Bitcoin, a number of blockchain platforms have emerged but have struggled to support functional decentralized applications and complex smart contracts. Transactions performance, latency, fees and user experience does not yet improve upon those mirror the equivalent currently provided by existing centralized services.

The existing blockchain infrastructure is a patchwork of disjointed, intensive processes. These are costly, inefficient and hard to maintain. Moreover the adoption of these platforms is hampered by the opaque ownership/control structures, lack of governance and limited scope to evolve within rapidly changing global environments.

G10's Blockchain 2.0, is creating a completely secure, decentralized, self-governing, collaborative ecosystem, underpinned by an evolving protocol. The G10 software is intended to create a new blockchain architecture designed to enable scaling of all decentralised applications.

Distributed ledger technologies and smart contracts make it possible to bring far greater automation and efficiency to the market, reducing resource burdens. Effective automation can only be built on standardization – a central definition of basic lifecycle events to eliminate inconsistencies between different approaches and the need for constant reconciliation

Without standardization of the underpinning principles of crypto-economics, the application of new technology will recreate the unsustainable and non-scalable infrastructure that exists today.

2. DEVELOPMENT

G10 was formed to address a number of concerns identified by international working groups on blockchain technology. Notably G10 Founder, Sakai Tokugawa's principal involvement in the research project between the Bank of Japan and the European Central Bank, to better understand the possible use of DLT for market infrastructure, highlighted the limitations of global adoption of this technology. The G10 team has sought to address these concerns, and in doing so has formed the next generation of blockchain technology.

During the years of development of G10, challenges were identified around the governance and maintenance that often lead to stagnation, shortages, and political deadlock of blockchain technology.

The G10 team sought to address these limitations through decentralized innovation in protocol design combined with a cohesive, structured ecosystem to encourage collaborative evolution.

A protocol was designed to facilitate the change required. The G10 Foundation will ensure the G10 ecosystem evolves in the manner it has been designed.

3. PRINCIPLES OF G10 BLOCKCHAIN

3.1 SYSTEM OF GOVERNANCE

Governance is the process by which people reach consensus on subjective matters that cannot be captured entirely by software algorithms.

G10 has created unique system of governance that structures governance by both a protocol-based approach and a foundation-based approach.

First generation blockchains, such as Bitcoin and Ethereum, have become subject to a form of centralisation, by concentrating power in the hands of development teams and miners. This creates its own problems, such as the forking that is becoming increasingly prevalent. In addition, a fundamental limitation is that blockchain technology exists in silos, without any market consensus, especially at a national level.

3.1 THE G10 COIN PROTOCOL-BASED APPROACH

The G10 Coin protocol-based approach enables stakeholders to propose protocol upgrades, to vote on proposals and approve of protocol upgrades within the protocol. Approved upgrades are then automatically deployed on the network. Stakeholders will be incentivised to actively participate.

In the absence of a defined governance process, prior blockchains relied on ad hoc, informal, and often controversial governance processes that result in unpredictable outcomes. The G10 system of on ledger voting will enable the blockchain to evolve with significantly reduced examples of forking. More detail to follow below.

3.3 THE G10 FOUNDATION-BASED APPROACH

Societies and Corporate entities of all kinds are governed by rules that detail rights and permitted conduct. These rules may be embedded in constitutions or exist in private contracts imposed by law. Societies and corporations have only been able to evolve and prosper when they have been been able to evolve and prosper when they have been enabled to collaborate and guided by the governing principles. People do not always follow the rules and moreover do not always agree on how the rules should develop. These issues have been exacerbated by the proliferation of cryptocurrencies and decentralised blockchain technology.

There is global consensus that blockchain technology is revolutionary, but the current iterations are disjointed with many shortcomings, such as lack of governance and not secure to transact. For these reasons this technology cannot and will not be widely adopted on any meaningful scale to actually penetrate markets on a global scale.

The G10 Foundation will comprise of representatives that will include a cross section of stakeholders and national endorsers (regulators, central banks and other apolitical organisations). Initially Sakai Tokugawa will also form part of the G10 Foundation.

To retain the jurisdictional impartialness, national endorsers will not be entitled to participate in the ICO or any subsequent funding rounds. For participation in the G10 Foundation, the national endorser shall unequivocally accept G10 Coin as the sole cryptocurrency for its jurisdiction and encourage the further adoption of the G10 Ecosystem.

Representatives forming part of the G10 Foundation, will be entitled to vote on technical enhancements, such as protocol upgrades, but more revolutionary is the ability to shape the way that G10 develops on a global scale. In addition to providing a forum for discussion for members, it is envisaged that members will collaborate to form policies and regulation that will be implemented globally.

This system of governance will continue to be refined through collaboration between all stakeholders.

4. ENHANCED SECURITY & FUTURE-PROOFING

4.1 SECURITY

Global adoption has been hampered by security concerns. The collapse of Mt Gox highlighted the vulnerability of access points for first generation blockchains. Whilst distributed ledger technology ensures that transaction details cannot be corrupted, the net result of several high profile hacking cases has shown how vulnerable existing techniques are. G10 intends on guaranteeing the security of the G10 blockchain and enhancing the encryption of the G10 wallets to minimise the risks of hacking, theft and/or fraud.

Wallet encryption will be reinforced with identity verification. G10 will be layering the G10 wallets with further DLT structures, aimed at creating an identity profile. It is envisaged that public, private and crucially identity keys will be required to access wallets. Anonymity may be retained, as all identity information will remain encrypted and not visible to the public. G10 anticipates the identity profiles created will go on to play a greater role in the G10 ecosystem.

4.2 SYSTEM OF GOVERNANCE

Global adoption has been hampered by security concerns. The collapse of Mt Gox highlighted the vulnerability of access points for first generation blockchains. Whilst distributed ledger technology ensures that transaction details cannot be corrupted, the net result of several high profile hacking cases has shown how vulnerable existing techniques are. G10 intends on guaranteeing the security of the G10 blockchain and enhancing the encryption of the G10 wallets to minimise the risks of hacking, theft and/or fraud.

Wallet encryption will be reinforced with identity verification. G10 will be layering the G10 wallets with further DLT structures, aimed at creating an identity profile. It is envisaged that public, private and crucially identity keys will be required to access wallets. Anonymity may be retained, as all identity information will remain encrypted and not visible to the public. G10 anticipates the identity profiles created will go on to play a greater role in the G10 ecosystem.

First some background. Blockchains record a list of transactions in a way that prevents dishonest use, such as tampering or spending. They allow any computer to keep track of this list by compiling them into a block, which is then encrypted to form a number called a hash.

The encryption process is important. It is an algorithm that is easy to calculate but hard to do in reverse (like factorization). The hash value it produces is a unique property of the block, and any tampering with the records would be immediately obvious because this would change the hash.

New transactions are then gathered together into a new block and added to the existing hash value. This is then encrypted to create a new hash for the new block. This is added to the next list of transactions when they are encrypted, and so on. The result is a chain of blocks that each contain the hash values of all preceding blocks—hence the term blockchain.

All the computers that store these blocks regularly compare their hash values to ensure that they are all in agreement. Any computer that does not agree, discards the records that are causing the problem.

Theoretically a dishonest user could change the list of transactions in their favour, but in a way that leaves the hash unchanged. This can be done by brute force, in other words by changing a record, encrypting the result, and seeing whether the hash value is the same. And if not, trying again and again and again until it finds a hash that matches.

The security of blockchains is based on the belief that ordinary computers can only perform this kind of brute force attack over time scales that are entirely impractical, such as the age of the universe. By contrast, quantum computers are much faster and consequently pose a much greater threat.

The G10 Blockchain will facilitate a transaction between two individuals that contains the information about the sender, the receiver, the time of creation, the amount to be transferred, and a list of reference transactions that justifies that the sender has enough funds for the operation.

This is where quantum mechanics comes in. Parties can verify each other's identities using a technique called quantum key distribution. This sends information using quantum particles such as photons, which cannot be copied by an eavesdropper without destroying them. In this way, the identities of each parties can be assured. The G10 quantum identification system will verify the identity of any other in a way that is guaranteed by the laws of physics. This quantum signature is attached to every transactions making it impossible to tamper with. The G10 blockchain protocol with information-theoretically secure authentication based on a network in which each pair of nodes is connected by a quantum key distribution link.

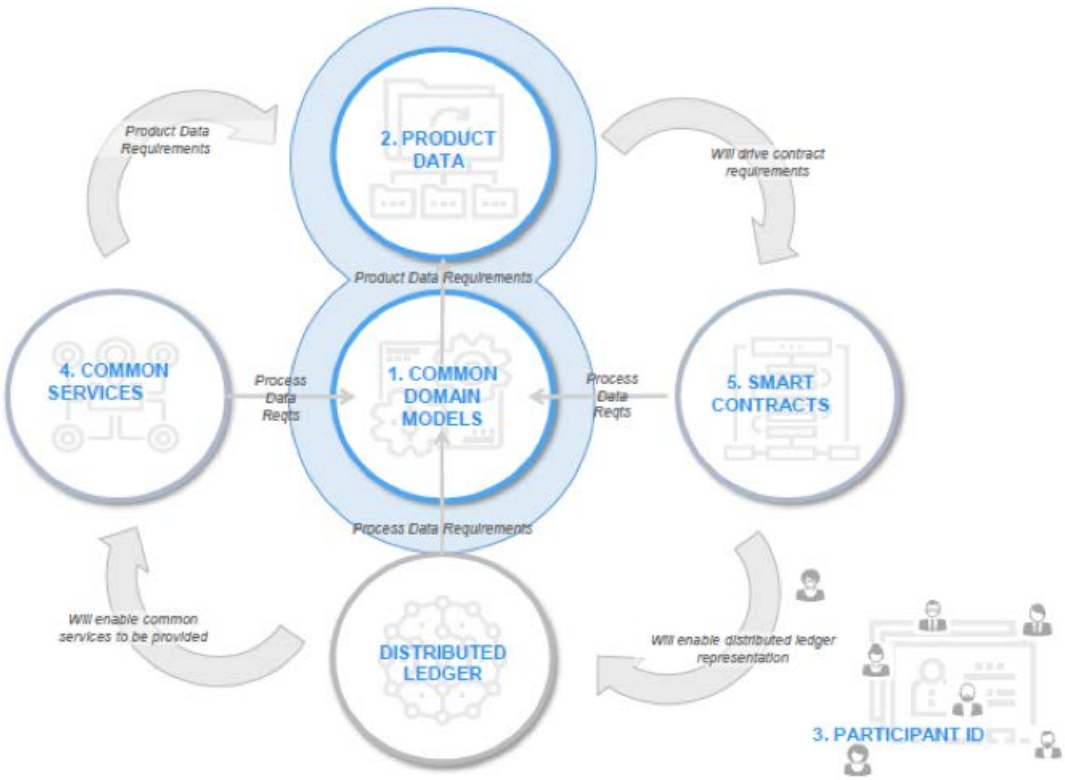
The threat for blockchain technology from quantum computers is a reality for the not too distant future. Any information that is currently stored using conventional cryptography will become unsecure as soon as the first powerful-enough quantum computer is switched on. By addressing this possibility and securing the encryption for the future, G10 Coin will be the most secure cryptocurrency available, with its longevity assured.

5. SMART CONTRACTS

Like many concepts in the current blockchain industry, 'smart contract' are widely misunderstood and shrouded in confusion. The term 'smart contract' confuses the core interaction described. While a standard legal contract outlines the terms of a relationship (enforceable by law) a smart contract enforces a relationship with cryptographic code. Smart contracts in of themselves cannot support complex legal concepts, which will limit the scalability of its function.

G10 proposes the Common Domain Model (CDM). This concept to create a standard blueprint of data and events for all DAPPs built on the G10 network. This will be the genesis for the development of Smart Legal Contracts on the G10 blockchain.

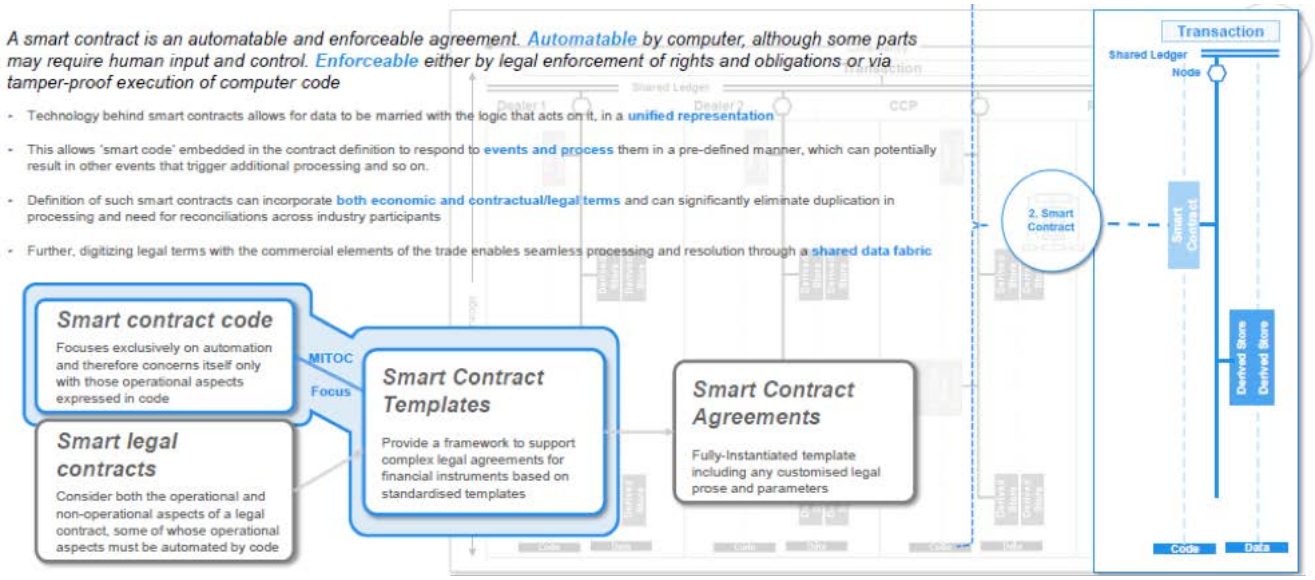
CDM is intended to be more than a data or product standard, but rather it aims to represent the very fabric of how smart contracts are formed, exchanged and managed during their lifecycles. The CDM will act as a unifying standard to facilitate the development of new technologies, including distributed ledgers and smart contracts. Regulatory updates can be made with reference to the standard blueprint, reducing time and effort to interpret and meet regulatory requirements such as reporting, and ensuring accuracy and consistency.



5.1 SMART CONTRACT VALIDATION

5.1.1 LEGAL CORRECTNESS

Formal Representation for a purist might be computer code in a high-level programming language. Such a representation would need to follow the strict syntax of that programming language. As programming languages differ, the same piece of conditional logic would result in different code for different languages. The multiplicity of programming languages used in practice may make it unpalatable to pick any one language. As a result legal drafting across programming languages would be extremely difficult. To address this G10 has designed a new programming language (based on extensions to current language) that is designed to more intuitively follow the flow and terms of legal drafting. There are current examples of languages that have been devised to facilitate smart contract code (such as Ethereum's Solidity), but these are not the most intuitive and are not scalable to more complex legal structures. However, it must be recognised that most live instances of smart contracts (or at least, smart contract code) use these specific languages, and these have a certain amount of traction. G10 software will facilitate smart legal contracts in a manner that meets the needs of the global community.



5.1.2 MATHEMATICAL CORRECTNESS

The correctness of smart contracts running on the G10 blockchain is almost as important as that of the core protocol itself. Smart contract bugs can taint the reputation of the platform they operate, so to mitigate that risk, the G10 development team designed a smart contract language, Donaldson, with correctness and formal verification in mind. Donaldson is statically typed and purely functional. This design largely eliminates large classes of bugs such as the Solidity ABI vulnerability discovered by the Golem project. The language itself looks like a mix between Forth and Lisp. The G10 development team has already successfully proven the correctness of Donaldson contracts, including the multisig contract.

6. PERMISSION MANAGEMENT

There have been a number of recent initiatives to create permissioned blockchains away from the public ledgers. An example of this is the Utility Settlement Coin created by several global investment banks to facilitate financial transactions. Instances such as these are driven by the need for privacy and certainty, but will ultimately continue to segregate the use of blockchain, which will prevent scalability. The G10 inclusive approach, seeks to address differing privacy requirements on the single blockchain, and will render these solitary, segregated approaches obsolete with the expected central bank endorsements.

Permission management involves determining whether or not a message is properly authorized. The simplest form of permission management is checking that a transaction has the required signatures, but this implies that required signatures are already known. Generally authority is bound to individuals or groups of individuals and is often compartmentalized. The G10 blockchain provides a declarative permission management system that gives accounts fine grained and high level control over who can do what and when.

It is critical that authentication and permission management be standardized and separate from the business logic of the application. This enables tools to be developed to manage permissions in a general purpose manner and also provide significant opportunities for performance optimization.

Every account may be controlled by any weighted combination of other accounts and private keys. This creates a hierarchical authority structure that reflects how permissions are organized in reality, and makes multi-user control easier. Multi-user control is the single biggest contributor to security, and when used properly, it can greatly reduce the risk of theft due to hacking.

G10 blockchain allows accounts to define what combination of keys and/or accounts can send a particular message type to another account. For example, it is possible to have one key for a user's social media account and another for access to an exchange. It is even possible to give other accounts permission to act on behalf of a user's account without assigning them keys.

6.1 NAMED PERMSSION LEVELS

G10 software, will enable you to define named permission levels each of which can be derived from higher level named permissions. Each named permission level defines an authority; an authority is a threshold multi-signature check consisting of keys and/or named permission levels of other accounts. For example, an account's "Friend" permission level can be set for the account to be controlled equally by any of the account's friends.

Another example is the Steem blockchain which has three hard-coded named permission levels: owner, active, and posting. The posting permission can only perform social actions such as voting and posting, while the active permission can do everything except change the owner. The G10 software generalizes this concept by allowing each account holder to define their own hierarchy as well as the grouping of actions.

7. G10 PROTOCOL

Much like blockchains start from a genesis hash, G10 starts with a seed protocol. This protocol can be interfaced to reflect virtually any blockchain based algorithm.

At a basic level, a blockchain protocol is comprised of three distinct types:

1. **Network Protocol** – block discovery and transaction broadcasts.
2. **Transaction Protocol** –transaction validation.
3. **Consensus Protocol** - forms consensus around a unique chain.

G10 implements a generic network shell. This shell is agnostic to the transaction and consensus protocol (together the "blockchain protocol").

A blockchain protocol is fundamentally a monadic implementation of concurrent mutations of a global state. This is achieved by defining "blocks" as operators acting on this global state. The free monoid of blocks acting on the genesis state forms a tree structure. A global, canonical, state is defined as the minimal leaf for a specified ordering.

This suggests the following abstract representation:
• Let $(S, \leq)$ be a totally ordered, countable, set of possible states.
• Let $\varnothing \notin S$ represent a special, invalid, state.
• Let $B \subset S^S \cup \{\varnothing\}$ be the set of blocks. The set of valid blocks is $B \cap S^S$.

The total order on S is extended so that $\forall s \in S, \varnothing \leq s$. This order determines which leaf in the block tree is considered to be the canonical one. Blocks in B are seen as operators acting on the state.

All blockchain protocols (be it Bitcoin, Ethereum, etc) can be fully determined by the following:

$$\left(S, \leq, \varnothing, B \subset S^{S \cup \{\varnothing\}}\right)$$

The networking protocol is fundamentally identical for these blockchains. "Mining" algorithms are but an emergent property of the network, given the incentives for block creation.

G10's approach is to make a blockchain protocol introspective by letting blocks act on the protocol itself. We can then express the set of protocols recursively as $P = \{(S, \leq, \varnothing, B \subset S(S \times P) \cup \{\varnothing\})\}$

7.2 PROTOCOL AMENDMENTS

One of the most powerful features of the G10 blockchain is the ability to implement protocol capable of self-amendment. This is achieved by introducing two procedures functions to the protocol:

• set_test_protocol which replaces the protocol used in the test_net with a new protocol (typically one that has been adopted through a stakeholder voter).
• propose_test_protocol which replaces the current protocol with the protocol currently being tested

These functions transform a Context by changing the associated protocol. The new protocol takes effect when the block is applied to the chain. These files are sandboxed and may not make any system amendment.

Many conditions can trigger a change of protocol. At a basic level a stakeholder vote triggers a change of protocol. More complicated rules can be progressively voted in or introduced by the G10 Foundation or AI algorithms. For instance, if the stakeholder desire they may pass an amendment that will require further amendments to provide a computer checkable proof that the new amendment respects certain properties. This is effectively an algorithmic check of “constitutionality”.

Adoption requires a certain quorum to be met. This quorum starts at 80% but dynamically adapts to reflect the average participation. The G10 foundation will have a veto power.

7.3 ARTIFICIAL INTELLIGENCE ALGORITHM

The G10 proprietary AI algorithm will be embedded into the seed protocol to over time enhance the efficiency of the network. The expectation being that as the G10 ecosystem evolves and develops, this algo will continue to learn and suggest improvements. All material suggestions will be subject to the G10 system of governance.

The efficiencies created by our AI algo have been successful in testing and is expected on full deployment to reduce latency, increase block size and arrange transactions more efficiently.

7.4 G-COINS

The initial extent of the token supply will be the number of tokens issued during the crowdsale. We suggest that a single coin be referred to as a “g-coin” and that the smallest unit simply as a “g-unit”. Therefore 1 g-unit = 1/100 of a g-coin.

7.5 SIGNING & MINING

The security of any decentralised currency requires the participants to be incentivised with a pecuniary reward (we are in the process of finalizing a rewards schedule). As explained in the position paper, relying on transaction costs alone suffers from a tragedy of the commons. At G10 we rely on the combination of a security deposits and a reward.

Miners and endorsers will be required to deposit a fix security deposit, in exchange for which they will be rewarded. The purpose of the security deposit is to encourage the continued participation and enhancement of the G10 network. In the seed protocol, mining a block offers a reward and requires a bond. Signing a block offers a reward. The projections were based on a supply of 1 billion tokens and will be revised accordingly. We may increase the number of signatures per block as well as we've found in simulations it can strongly increase the difficulty of forks.

The forecasted reward will be a 39% return on the security deposit, to be reviewed annually (we're currently revising these parameters but will soon finalize a method that makes sense for all parties). G10 understands and accepts the need for returns to be higher in the initial stages to encourage signers and miners.

8. THE G10 NETWORK

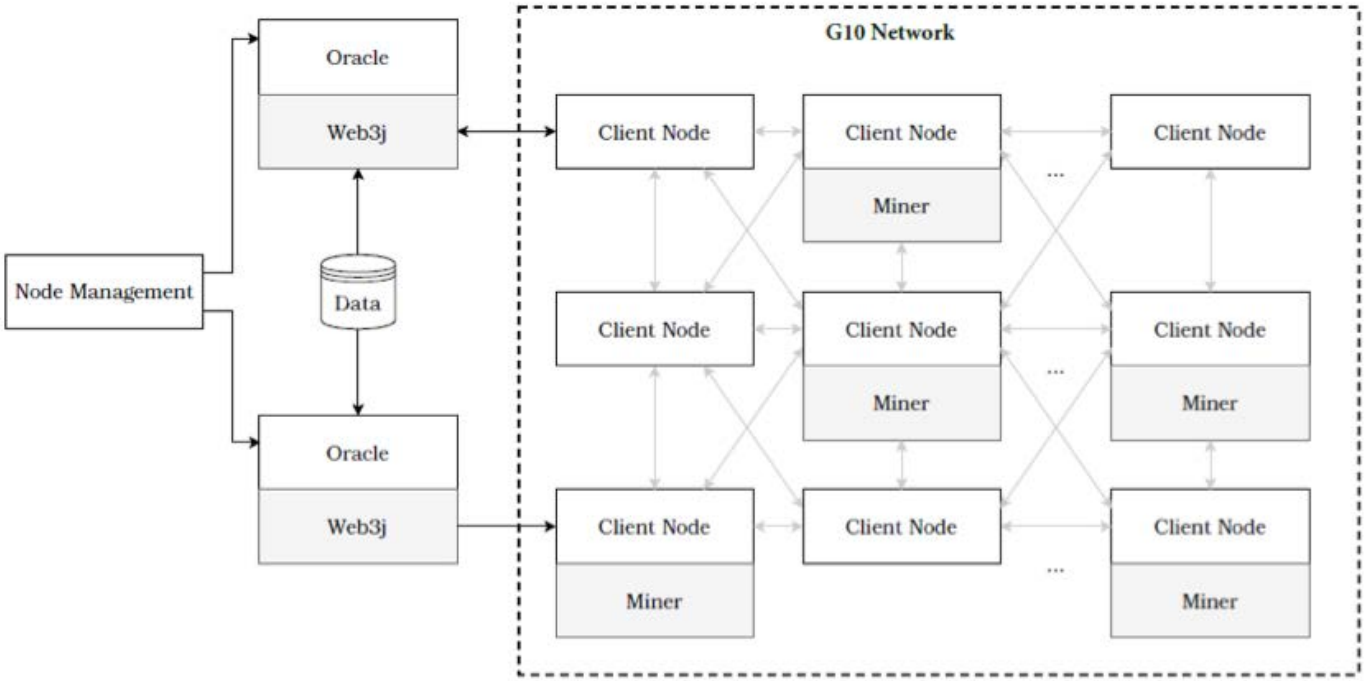
8. The G10 network

Microservice architecture is a network of module services that can be deployed independently from one another. Microservice architecture is an approach to structuring applications whereby they are broken down into smaller independent internal components. The advantages of this is to enable autonomous ownership for different microservices within an application; enhance agility, application micro-components can be developed and tested in autonomous decentralized teams much faster; improved scalability (scaling independent of other components, on-demand scaling); continuous delivery and deployment of micro-components.

A monolithic architecture is much easier in implementation, control and deployment, while microservices require careful management, as they are deployed on different servers and use API.

Such architecture allows technically complicated applications to constantly evolve without the need to wait for the release of a new version of the product to make changes. There is no need to release an updated version of the product, if the changes apply only to a small part of the product. That's why it's possible to customize for various business tasks of every enterprise, department or person.

The G10 software is designed from experience with proven concepts and best practices, and represents fundamental advancements in blockchain technology. The software is part of a holistic blueprint for a globally scalable blockchain society in which decentralised applications can be easily deployed and governed.



G10 Blockchain Architecture

The G10 network shell will interface between a network and the protocol by maintaining the best known chain.

The network shell acknowledges transactions and blocks (which are only propagated through the network if deemed valid) and protocols (modules used to amend the protocol). The most arduous part of the network shell is to protect nodes against denial-of-service attacks.

Every block carries a timestamp visible to the network shell. The protocol design must tolerate reasonable clock drifts in the clients and must assume that timestamps can be falsified.

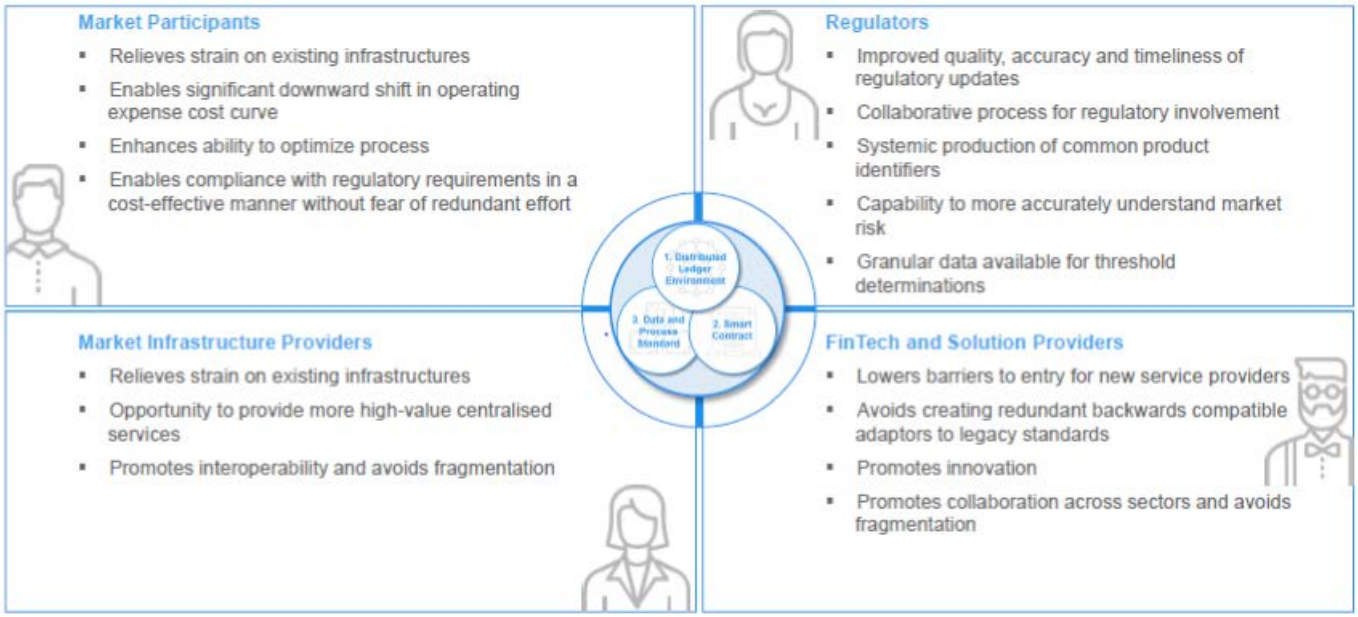
The shell maintains a single chain rather than a full tree of blocks. This chain is only overwritten if the client becomes aware of a chain having processed a large number of blocks. A protocol can identify chains with a low rate of block creation and consider it to be a “weak” fork before disregarding.

9. G10 FOUNDATION

The G10 Foundation will manage the contributions according to its purpose. Initially, the Foundation will budget for 5 years, depending on the amount raised, after which we expect the Foundation to be self sustaining.

The Foundation will have the discretion to pay for services it believes will benefit the protection promotion of the G10.

The primary focus of the G10 Foundation is to ensure the functionality and continued improvement of the G10 eco-system. They will be empowered direct the development of the G10 ecosystem.



9.1 ENGINEERING

The Foundation will seek to retain the original development team and build the team. The G10 projections have been succinctly outlined in the table below.

9.2 RESEARCH

The G10 protocol currently benefits from research in the formal verification and programming language communities at no cost. The initial development team of G10 is committed to formal verification and a keen interest in researching new consensus algorithms for blockchains. The Foundation will look to fund research in this area with its endowment from the fundraiser.

9.3 BUSINESS DEVELOPMENT

The Foundation will spearhead efforts to broaden endorsements, partnerships, marketing, financial transactions, and structure business operations.

It is expected that business development will need to be upscaled to meet our global goals.

10. FUTURE GOALS

The G10 system of governance, will prescribe the Foundation powers to act. All decisions will be collaborative with all stakeholders . The expectation for the Foundation, is to be tasked to build a robust, scalable, and secure ecosystem.

10.1 COMMUNITY

The G10 protocol self amendment mechanism, will evolve and incorporate new innovations over time. The Foundation and stakeholders can make and enforce decisions about changes to the network using the network itself.

All protocol changes should go through the G10 governance mechanism. If a person or party introduces a change via a hard fork, but that change could easily have been instigated inside of G10, the network will reject that change and treat it as illegitimate.

However, some decisions will inevitably arise at a level that cannot be fully addressed within the network. The G10 Foundation will be enabled to act in such scenarios.

G10 network will reward effective proposals by issuing them upon acceptance, creating a robust pecuniary incentive.

10.2 SECURITY

The G10 ambition is to be first to market with a fully functional blockchain encrypted with quantum physics.

10.3 PROJECTIONS

Note: all amounts in USD millions	CURRENT	$10m+	$20m+	GLOBAL AMBITION
ENGINEERING	Development of our current team.	Hire additional talent to maintain and refine code.	Hire talented teams of engineers and designers to develop our proprietary quantum encryption.	Grow the team with other experienced, academically oriented engineers.
HEADCOUNT	4	8	14	24
ESTIMATED COST	0.8	1.5	3.0	
RESEARCH	Continue our use of Phd candidates	Strategically engage the AI community.	Strategic partnerships with AI and encryption firms.	Develop the G10 academy endowed with grants to nurture our own graduates and enhance protocol development and coding.
ESTIMATED COST	0	0.2	0.5	
MARKETING	Assessing PR/ marketing firms.	Continue working with our chosen consultancy.	Host an annual developer conferences globally and run ad campaigns.	Acquire mainstream print outlets to promote the use of DLT technology and further the endorsement of G10 Coin.
ESTIMATED COST	0.1	0.15	4.4	
LEGAL SERVICES	After the fundraiser, the Foundation will instruct a magic circle law firm.	Retain counsel and refine all terms, policies and the constitution for the Foundation.	Retain counsel and refine all terms, policies and the constitution for the Foundation.	Partner regulatory bodies to digitize and map transaction logic from traditional legal prose to a G10 smart contract code.
ESTIMATED COST	0.1	0.25	0.3	
BUSINESS DEVELOPMENT	James Roberts will spearhead business development initially	Develop in-house business development team to further increase official recognition from central banks and regulators.	Establish offices globally for the to further engage end users, governments, central banks and regulators in G10 countries.	G10 Coin will be officially recognised as the global digital currency underpinning all financial and cross border transactions.
YEARLY RATE	0	0.3	0.8	
ANNUAL COST	1.0	2.4	9.0	20+

11. CONCLUSION

We feel we have built a revolutionary seed protocol, enabling stakeholders to have a determinative input to the evolution of the protocol.

G10's true potential, however lies in the G10 ecosystem, the system of governance and the G10 Foundation which provides a forum for central banks, regulators and stakeholders to engage.