



Graphene

Litepaper ***November 26th, 2021***

Graphene is a community driven project, and all aspects of can be updated and improved based on community feedback, including the contents of this litepaper.

Graphene website (<https://getgraphene.io>) for the most up-to-date version of this litepaper.

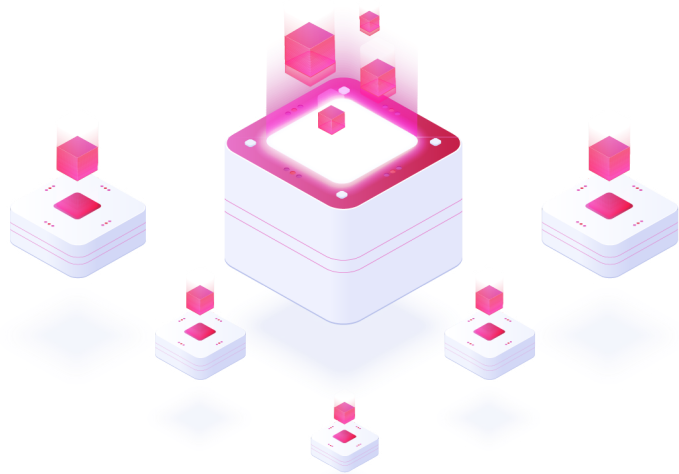
Table of Contents

3	Graphene
5	Graphene's Guiding Principle
6	Graphene's Origin Story
7	The Blockchain Trilemma & Monolithic Blockchains
9	Graphene Platform Highlights
9	Modular Blockchain
10	Gasper Protocol
11	Casper FFG
12	GHOST
13	Sharding
14	Beacon Chain
15	BLS
15	Variable Reward Issuance
18	Graphene DAO
19	Budget Governance
20	Shard Governance

Graphene


Graphene is a next-generation modular cryptocurrency platform designed to be

community driven,
secure, flexible, and
scalable, while
maintaining
maximum
decentralization.



From the beginning, we have wanted to build a highly useful, fully decentralized platform for the community supporting and using Graphene, and this guides everything we do. Graphene is designed to have built-in decentralized autonomous organization (DAO) features. Decentralized budget governance allows anyone in the Graphene community to submit funding proposals and the community has a direct say in allocating that sustainable development funding to help Graphene grow and thrive. Shard governance guides the growth and development of the new types of shard blockchains added to the Graphene platform, and again the community has direct influence over which new shard types are approved and enabled. Incentives are built into the protocol design to reward people for running Graphene validator nodes that perform critical tasks for the network, and to reward developers for deploying decentralized smart contract applications (dApps) that are highly utilized by the community. The Graphene community has sovereignty to make Graphene into exactly the cryptocurrency platform we want it to be.

Robust security is also central to the design of Graphene. The core consensus protocol is designed to have thousands of validator nodes signing or attesting to transactions and blocks as they are proposed and distributed across the network. Validators also look for any violations of the rules and the protocol supports penalties for proven violations and ejection of validators that misbehave. The



protocols also allow for finalization of blocks and transactions once a supermajority consensus is reached, helping to assure users that their transactions are committed, immutable and permanent.

Scalability is a necessary prerequisite for Graphene to act as a global cryptocurrency platform that everyone can use. Many current blockchains have compromised on scalability to the point where any significant usage leads to expensive transaction fees or long waits for transactions to be confirmed. Graphene's sharding architecture allows the network to grow its capacity by 1000x or more as usage increases, so that it can support users everywhere around the world using the platform at the same time while maintaining reasonable fees and fast transaction confirmation times.

Decentralization is the heart of cryptocurrency, and Graphene is designed to maximize decentralization. It's modular design enables different nodes to perform the consensus, execution, and data layer tasks needed to operate the network, and it does so with lightweight nodes to make running Graphene validator nodes accessible to as many people as possible who are willing to stake their Graphene capital to help secure and scale the network. The initial distribution of Graphene is being performed as a fair airdrop of Binance Smart Chain (BSC) tokens to Phore holders on the announced snapshot dates, which will later be converted to Graphene mainnet coins. The Graphene development team is receiving their coins the same way, and we estimate the team holds less than 10% of the total supply, leading to high decentralization of Graphene holders, which is being increased even further as new people join the Graphene community buying GFN tokens on the BSC blockchain.

With this combination of strong community focus, security, scalability and decentralization, we believe Graphene is a revolutionary new cryptocurrency platform that will enable the Graphene community to grow and mature the ecosystem and build useful decentralized applications that provide better solutions than centralized platforms ever could.

Graphene's Guiding Principles

With respect to cryptocurrency platforms, we believe in:



- **Community.** Growing and serving the Graphene community is the primary focus and purpose behind everything we do. We believe the community should have a strong voice and should determine the features and direction of our development efforts.
- **Decentralization.** Decentralization is essential to the concept of cryptocurrencies, and should be maximized.
- **Scalability.** Platforms need to scale to handle the transaction volumes that come with widespread global adoption and regular daily use.
- **Flexibility.** Cryptocurrency platforms should support innovation and new usage models.
- **Functionality.** Cryptocurrencies should provide robust functionality that makes it easier for developers and users to solve real world problems in ways that are difficult or even impossible with traditional, centralized platforms.
- **Sound Money.** Tokenomics should be designed to balance supply and demand, in the long term driving usage to the point where burned transaction fees approach or even exceed issuance.
- **Ease of Use.** Cryptocurrency platforms should continually look to deliver a great user experience, both for developers and end users.
- **Collaboration.** We reject the all too common tribal culture of many cryptocurrency projects. We want to be a bridge rather than an island, and look for opportunities to work together with other cryptocurrency platforms and projects.

- **Respect.** We believe everyone involved with Graphene should be treated with respect—developers, users, investors, and other crypto projects.

If these principles resonate with you, we welcome you to the Graphene community.

Graphene's Origin Story

Graphene was developed by the team behind the Phore cryptocurrency project. The original intent was to add smart contract functionality to Phore by adding a smart contract sidechain. After looking more deeply into the idea, we decided the sidechain concept was not secure enough, or scalable, and it would be much better to build a new blockchain that had all of the properties we wanted for scalability, flexibility, and functionality.

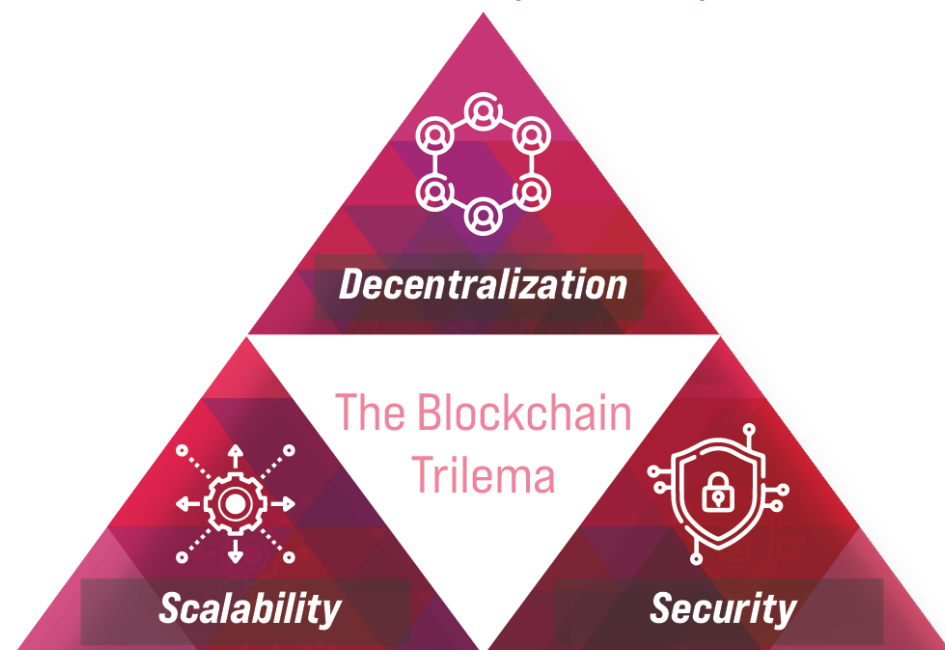
As this new blockchain (originally codenamed Synapse) took form, we realized that what we were building was capable of much more than just adding smart contract functionality. Phore had taken on an identity focused around eCommerce and other decentralized applications, and it became clear that this new blockchain should be launched as its own project, so that it could reach its full potential with its own identity as a revolutionary cryptocurrency platform.

Thus, we decided that Phore would continue building out its vision, and we would launch Graphene as a new project. Because the development of Graphene was partially funded by Phore development funds, Graphene would be airdropped to Phore holders—initially as a token on the Binance Smart Chain, and later converted back into native Graphene coins after the mainnet is launched.

The Blockchain Trilemma & Monolithic Blockchains


Many popular cryptocurrencies are monolithic blockchains – Bitcoin and Ethereum are a couple of well known examples. Monolithic blockchains process every transaction and block one at a time on every full node, limiting their scalability. This is the result of a tradeoff in response to what is commonly referred to as the blockchain trilemma:

Decentralization, Scalability and Security: Pick Two



Monolithic blockchains generally have to optimize for only two of these properties, and make sacrifices on the third. Because decentralization is so essential to cryptocurrencies, and because security is so important, they both chose to sacrifice scalability.

Bitcoin (BTC) limited the operations (OP_CODES) that can be used to define what can be done with a bitcoin. The block size is limited to 1MB (up to 2MB with SegWit



transactions), and a new block is only produced every 10 minutes, leading to scalability of only around 15 transactions per second. There is also a maximum limit on transaction size. Even with these tradeoffs, storing the full bitcoin blockchain requires a lot of space – as of this writing it takes ~374GB of disk space to store the full bitcoin blockchain. As mining hashpower continues to increase, the cost to mine bitcoin increases as well. These work to potentially limit decentralization as the cost to run full nodes and mine bitcoin become too much for many individuals to bear.

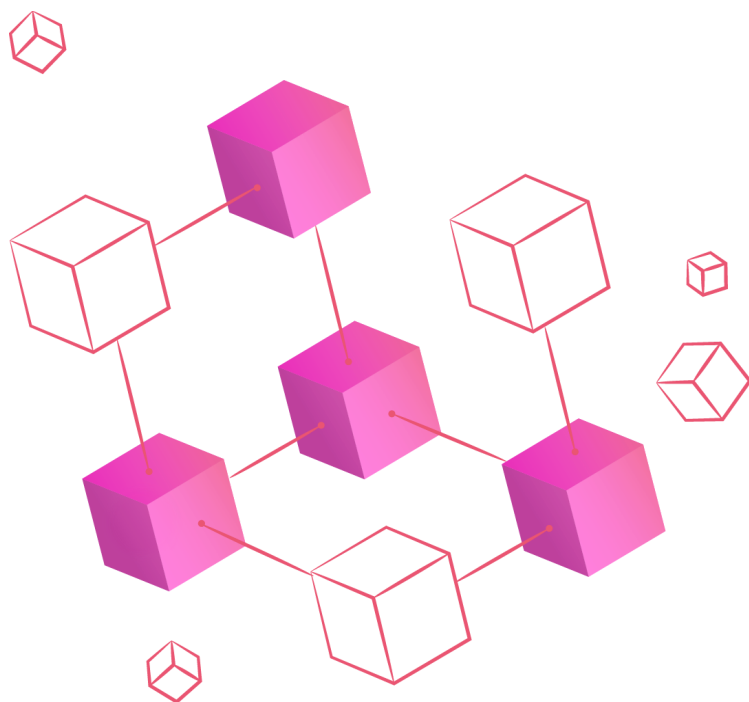
Ethereum (ETH) allows for a much broader range of operations, with an entire Turing complete programming language available to make smart contracts. This increases the ability to execute complex smart contract transactions, but it also means that every Ethereum mining node must process these complex transactions, and every smart contract transaction is competing for block space—smart contracts also have a maximum limit on how much processing can be done (measured as a gas limit). Ethereum's blockchain is also continually growing at an even faster pace than Bitcoin—as of this writing it takes up ~1,061 GB of disk space to store the entire blockchain. Ethereum's maximum transactions per second limit is even lower than Bitcoin, and it could be argued it is less decentralized given the high compute requirements to run a full Ethereum node.

Because of these severe limitations and the high transaction fees that came with them, scalability optimized blockchains with lower transaction costs gained popularity. Binance Smart Chain, Polygon, Solana, and Avalanche are some examples. However, since these are also monolithic blockchains, this focus on execution speed has generally required some sacrifices in decentralization or security. To handle more transactions per second, many of these blockchains limited the number of nodes that can produce blocks and/or raised the hardware requirements nodes. These blockchains are much less decentralized—relatively few nodes have complete control over the block production process. Even with this optimization, the process of block validation and creation is still processing one block at a time with the entire process happening in the same place—at a certain point the hardware for block producing nodes hits a maximum throughput.

Graphene is a new kind of blockchain architecture, and provides a better solution to the Blockchain Trilemma. Graphene is a modular blockchain.

Graphene Platform Highlights

Modular Blockchain



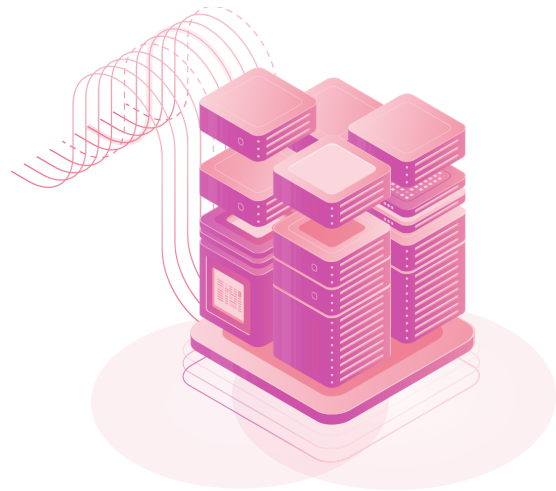
Graphene's modular blockchain compartmentalizes the layers of the blockchain—consensus, data, and execution. Different parts of the network process each layer at the same time, without sacrificing decentralization or security.

This modular architecture unlocks scalability by orders of magnitude, designed to be capable of processing 100,000+ transactions per second, possibly much higher with future development. This high scalability is critical to function as a global cryptocurrency platform, and most current blockchains are not capable of doing this without giving up the very essence of cryptocurrency—decentralization.

Graphene blocks are created by thousands of lightweight validator nodes, on multiple shard blockchains running in parallel. The beacon chain ties all of the shard blockchains together, maintaining a consistent state using rollups and shard attestations. Graphene's proof of stake protocols designed to increase security over most current proof of stake protocols—validators earning proof of stake rewards are also risking their capital on the promise of following the protocol rules, and incur penalties and ejection from the network if they provably violate them, providing a strong incentive to follow the rules and protection for the network when they are not followed.

Gasper Protocol

Graphene will use the Gasper protocol, proposed by Vitalik Buterin and other cryptocurrency researchers as a next-generation consensus protocol that solves several problems with current generation proof of stake protocols.




- **Block Finality.** A common challenge every decentralized blockchain faces is the possibility of nodes having different views of the current state, which can lead to forking—multiple blocks at the same height. Consensus protocols are designed to help resolve this over time, but many cannot guarantee absolute block finality—at any point, the “best” block may change from one fork to another. With Graphene’s protocol, when 2/3 of the validator committee agrees on the best block, it is guaranteed to be final. There are regular checkpoints on the beacon chain that first reach justified status, and then finalized status, and once that is reached, the state of the blockchain up to that checkpoint is final.
- **Nothing at Stake Problem.** Another common challenge with proof of stake protocols is what is commonly called the “nothing at stake” problem—that staking nodes which see multiple forks (blocks at the same height), they are incentivized to add more blocks to every fork they see, because there is no penalty for doing so, and they are rewarded if they add the block that ultimately reaches consensus as the best block. With Graphene, if a staking node votes to approve more than one block at the same height, other nodes can prove this happened and the violating node loses some staked collateral (the node that proved the violation can receive a reward for this) and may be ejected from the network. This will reduce the amount of forking on the network and help the network reach consensus and block finality more quickly.

- **Scalability with High Decentralization.** Graphene validators are randomly assigned to do different tasks for brief periods of time—validating shard transactions and blocks, providing attestation signatures for beacon chain transactions, creating beacon chain blocks, etc. Thousands of validators will be performing these tasks, and the cost of running a validator will be much lower than with most other blockchains, allowing everyone who wishes to stake their capital to participate and receive staking rewards. Since this process is happening on many shards at the same time, high transaction volumes can be processed, and more shards can be added as they are needed to increase scalability and keep transaction costs from skyrocketing as they have on many other blockchains—which in turn enables new use cases like microtransactions which would not be possible with high transaction fees.

Casper FFG

One of the components of the Graphene consensus protocol is Casper FFG (Casper the Friendly Finality Gadget). This is the portion of the protocol that handles justification and finalization of the blockchain state. At a high level, this defines rules such that when 2/3 of the validator committee agrees on the best checkpoint block, it is considered justified. When this 2/3 supermajority is reached for the next checkpoint block to be justified, then the first checkpoint block is finalized.





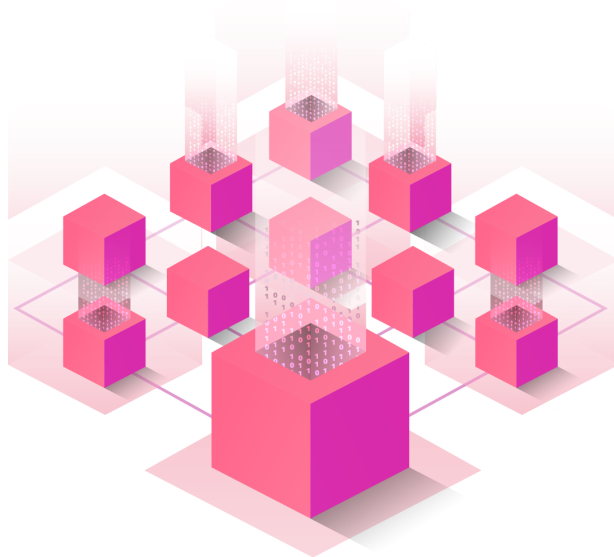
Casper also defines slashing conditions, which are the ways validators can be penalized for breaking the rules. These include voting for two blocks at the same height, or not providing the validator services that it has agreed to provide. For some violations this may begin as a small penalty that increases (e.g., if a short network outage occurs, we would not want to overly penalize the validator), and in other cases it may result in higher penalties and immediate ejection from the validator pool (e.g., provable misbehavior that no honest node would do).

GHOST

Another component of the Graphene consensus protocol is GHOST (Greedyest Heaviest Observed SubTree rule). This is a fork-choice rule that guides nodes as to which block it should add to when there are multiple forks to choose from. Every blockchain needs a rule like this so that a node that may not have a complete view of every message received by every node on the network has some way of deciding which block it should consider the “best” one at any given time. For proof-of-work blockchains like bitcoin, they use whichever block has the most “work”, which is a sum of all the work of all blocks up to that point. Since the work is easy to determine in a proof-of-work blockchain, this is relatively straightforward, but it also implies that a large amount of computation and energy usage is put into creating each new block. Proof-of-stake solves this energy usage problem by using a different protocol for proposing new blocks that does not require this high energy use and computation, but by eliminating this, it needs another way of determining which block is “best” at any given time.

The GHOST rule requires a node to consider whichever block has the most validator attestations as the best one. This includes attestations of any other forks beyond the block being considered—so if one block has two child blocks, and another block at the same height has four child blocks, all of the validator attestations for all of the child blocks are included in each calculation. Block hashes are used as a tiebreaker. These validator attestations thus act in a similar way of measuring the work in proof-of-work blockchains, and helps the network converge on consensus by including all of the attestations for child blocks since even if some validators disagree on the next child block, they all agree on the parent block being the best.

Sharding



The Graphene sharding architecture provides a way for the Graphene platform to securely allow for many shard blockchains to run in parallel.

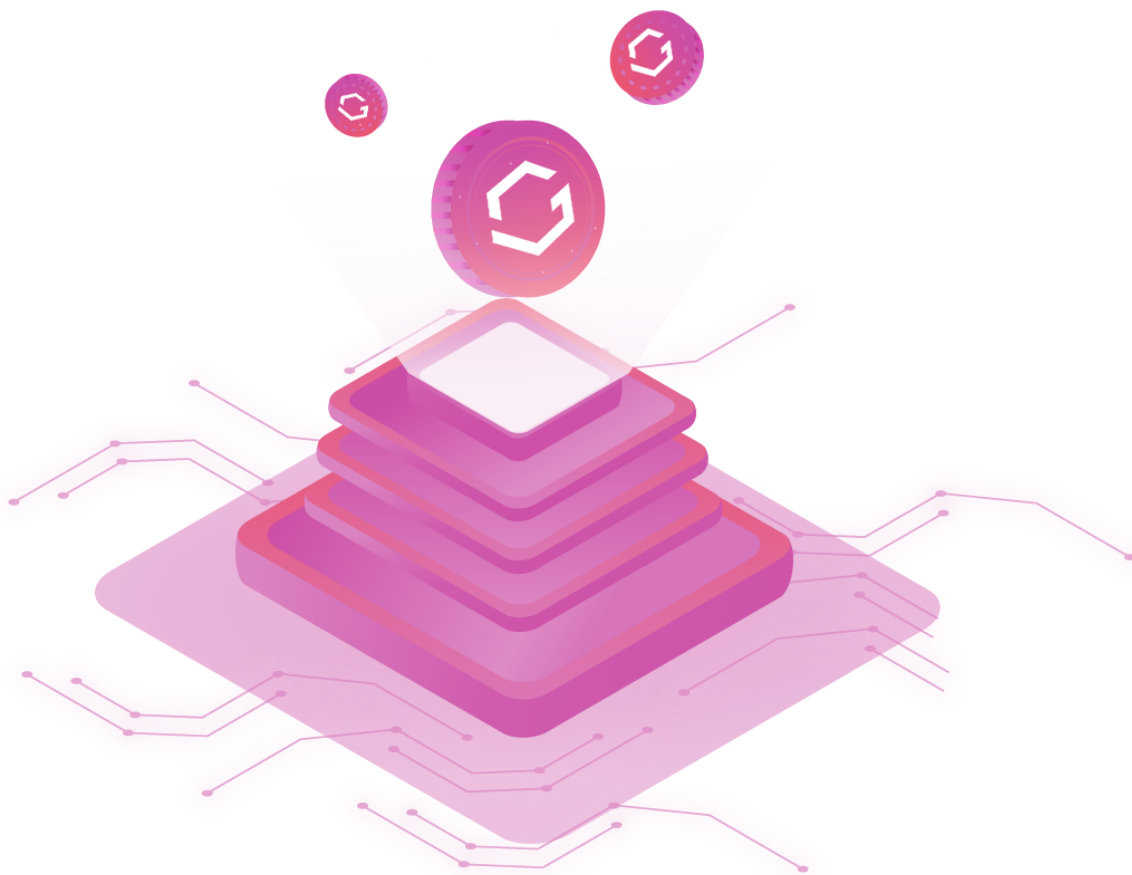
More shard blockchains can be added as they are needed, and they may one day number in the thousands. In addition to having many shard blockchains, there can be different shard types. The initial design for Graphene includes a transfer shard type which will allow for fast, secure transfers, and also a smart contract shard type that will allow for full Turing-complete smart contract and dApp development. This can be extended by the Graphene community in many directions—there could be shards added that include privacy features, identity features, decentralized storage features, etc.—and the shard type can be optimized for whatever features it includes, so that any tradeoffs it is making do not affect any other shard types, and it can be optimized for its own purpose.

The shard module in Graphene provides an API that provides functions for the most common operations that would be the same for just about every type of shard that might be developed. This allows for new shard types to be developed fast, since they don't need to reinvent the wheel to perform basic operations that would likely be exactly the same even if they are designed for a different purpose.

The Graphene community will use the built-in DAO features to determine the future direction of which shard types will be added, which is described further below.

Beacon Chain

The Graphene beacon chain ties together all of the shard blockchains, and contains rollup transactions that summarize and finalize the activity on the Graphene network, and allow Graphene coins to traverse the network across different shard blockchains without the security challenges that often exist with cross-blockchain transactions. It also contains certain other transactions, such as registering new validators as they join the network. The beacon chain along with the sharding architecture work together to allow for high transaction throughput without compromising decentralization or security.



BLS

Graphene has its own native Golang implementation of the Barreto-Lynn-Scott aggregation signatures. This is a key component in the Graphene architecture, as so many of the operations on the network require many validator signatures to be collected and stored to attest to the validity of a transaction or block. The main benefit of the BLS signature aggregation method is scalability—with a limited time to collect, validate and store these signatures, any unnecessary delay would limit the number of validators that could participate. This efficient signature aggregation method allows the architecture to scale to higher numbers of validators participating in signing off on transactions and blocks, increasing both security and decentralization.

Variable Reward Issuance

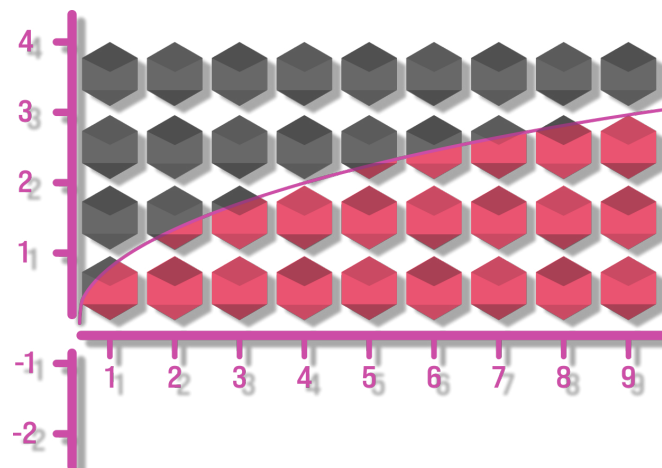


With many existing blockchains, the total token per block is fixed—it may be increased or more often reduced at certain time intervals, but for any given time period it is a set amount per block.

This style of issuance offers a predictable issuance rate, but also creates some imbalances. For example, if we use a hypothetical example of an staking issuance rate of 5% of the total supply per year, and assume half of the token balance was receiving rewards, then the annualized ROI for staking would be 10%. However, at the beginning, there may be only a few nodes staking—if the network began with only 5% of the supply staking, then those nodes would initially be receiving 100% of their staked balance in rewards per year..

Graphene uses a different reward mechanism, tying the overall rewards to network activity. The final tokenomics are still being finalized. The primary issuance mechanism will be that tokens will be issued as validator rewards and a decentralized development budget to fund ongoing development and community projects. The issuance is intended to remain low, either starting or trending towards $< 5\%$ issuance per year, while at the same time providing enough incentive for people to run validators by making it profitable to do so after considering hosting costs.

The validator reward mechanism will When the first validators join the Graphene network, they receive the initially set base reward. For the sake of using round numbers, let's assume hypothetically that this base reward would pay a validator 20,000 GFN per year in rewards. With Phore's reward structure, the second node added to the network would cut this in half, but with Graphene it would have only a slight reduction—maybe each node would receive 19,999 GFN per year. However since there are now two nodes, you might notice this means more overall rewards are being paid—39,998 GFN instead of 20,000. If two more nodes were added, the each node might receive 19,997 GFN, with the total rewards increasing to 79,988. What these examples are illustrating is a square root function, which looks like a curve:



At first, adding more validator nodes only slightly decreases the rewards per node, and increases the overall rewards paid almost linearly. This provides a higher incentive to run validators up to a certain point, with each validator receiving close to the full reward, but when there are enough, the reward pool increases less, and the ROI for running a validator will decrease more until it reaches market equilibrium. The benefit of this reward structure is that issuance of GFN rewards is tied to

network activity—when there is less validator activity, there is less issuance, so there is not much inflation of the supply. When there is more validator activity, there is more issuance—and that also means there is more activity on the network, which means more transaction fees are being burned by the staking protocol to offset supply inflation. It also provides a natural mechanism for reducing inflation during periods of low network activity, thus helping to preserve the value of the GFN coins since less is being issued.



Graphene will also have a reward structure for smart contract developers, which will provide a direct incentive for developers to deploy their dApps on the Graphene platform. This will be in the form of a partial rebate of the transaction fees generated by the smart contract. The specific numbers are still being researched. As a

hypothetical example, if a developer deploys a popular Graphene dApp that generates 100,000 GFN in transaction fees over a period of time, they might receive 10,000 GFN as a reward, which they can use any way they wish—they could use it to fund additional development, share some or all of it with the users of their dApp, provide incentives to new users to drive further growth, etc. Attracting both developers and users to the platform are important to Graphene's long term health, and this direct incentive provides developers with another reason to choose Graphene.

This reward structure balances issuance with network activity, and still provides a strong incentive for GFN participants to run enough validators to keep the network secure. Note that this also means that the exact issuance rate cannot be known in advance—it would depend on how much network activity there is and how many validators are running at any given time.

Graphene DAO

Graphene will have a built in Decentralized Autonomous Organization (DAO) structure using on-chain governance. This is consistent with our community driven philosophy, giving the GFN holders a direct voice in the direction of the project, making it into the platform you want it to be. The two primary DAO structures being built out initially are Budget Governance and Shard Governance.



Budget Governance

The budget governance DAO will allow issuance of up to a specified budgeted amount of Graphene coins at regular time intervals, which are paid to fund development efforts that are first proposed and then voted on and approved by the Graphene community.



This will be done using a completely decentralized protocol—anyone in the Graphene community can pay the proposal fee to submit a development proposal, which will include a description of the work being done and the requested amount of funds. These proposals will then be viewable by the Graphene community, and GFN owners will be able to vote yes or no on each proposal.

The proposals that meet all of the threshold criteria to make the valid proposals and that receive the most community support will be approved and paid in GFN coins at the specified time intervals, up to the maximum budget amount.

This budget governance system provides the Graphene project with a sustainable and resilient source of funds for ongoing development. Because it is fully decentralized, with no one having any privileged access to the funds, it also provides more long term sustainability as it does not depend on any specific individual or organization—if something happened to the current Graphene team, another individual or team could request the same funds and continue developing Graphene.

These funds can also be used to fund conferences, ambassador programs, marketing efforts, or any other purpose that the community feels would benefit Graphene's development.

Shard Governance




Graphene will also have a decentralized system for deciding which new shard types should be added to the Graphene network.

20

One of the great new capabilities of the Graphene platform is that different shard types can coexist and be optimized for different use cases. Initially we have planned to implement the Transfer shard which will be optimized for transfer of value exchange, similar in capabilities to Bitcoin and Phore, and the Smart Contract shard which will be optimized for Turing complete smart contract capabilities similar to Ethereum. Other shard types can be added that would be optimized for any number of specific use cases, providing dedicated block space and flexibility to add consensus rules and change parameters to fit the needs of that use case.

To begin the shard governance process, the shard developer will submit the proposed shard type code along with their description and request for approval for it to be added to the Graphene network. We will then have a code review phase where other skilled developers will review and sign attestations endorsing the shard type code—this will help prevent malicious, trivial, or low quality code from being added to



Graphene, and help inform Graphene community members who don't have the time or skill to meaningfully review the shard code.

Once the shard proposal has enough endorsements, it would proceed to be voted on by the Graphene community. If it receives enough support, it will be added to the Graphene network—and here's something you might not have expected: it will be added automatically, similar to how a smart contract would be uploaded to the blockchain, in most cases not requiring users to upgrade their wallets and validator nodes to be able to use the new shard type.