Graphite White Paper

v1.1; last edit date: 8th of August 2024

Our Vision

Graphite is a finance-oriented blockchain platform focussing on:

- the formalization of crypto interactions based around a KYC scheme;
- low and stable transaction costs;
- efficient block validation via a Proof-of-Authority consensus;
- income for entry-point nodes.

At Graphite, we believe that reputation is the cornerstone of any formal, well-functioning and successful market. We aim to provide this kind of market to our users by implementing:

- A reputation-based system
- An efficient KYC verification ('Know Your Customer') procedure
- A series of transaction filters based on reputation (utilizing KYC, etc.)

Our emphasis on reputation by no means conflicts with our respect for anonymity and privacy. Graphite's goal is not to prohibit the anonymity of users and transactions, but rather to respect privacy whilst creating an ecosystem that encourages reasonable transparency. Our vision is to provide a functioning blockchain platform that encourages users to switch from the 'shady' crypto markets to Graphite's more formalized market.

The Graphite blockchain's second key point is related to how it processes transactions. The standard Proof-of-Work (PoW) blockchain is not only unproductive, but also dangerous in the long-term insofar as it wastes huge amounts of electricity and computational power. For this reason, Graphite utilizes a Proof-of-Authority (PoA) algorithm that offers 1,400 tps worth of network capacity without the need for excessive computational resources.

In addition, Graphite employs a processing engine which implements transparent transactions fees and eliminates Ethereum-like cases of so-called 'gas betting' during block sealing.

Graphite's transaction architecture creates a unique opportunity for both entry-point transport nodes and authorized nodes acting as block sealers to earn income. Most blockchains do not allow this for transport nodes at all.

Within Graphite, it is not only theoretically possible to earn income, but it is realistically possible for almost any market participant: it does not require significant server resources to support an income-generating transport node.

Graphite's ultimate end goal is to build an ecosystem where any user contributing to the workability of the network gets to earn a fair reward.

Graphite
Key Differentiators

- Reputation-based system
- Account activation
- KYC verification procedure
- ZK KYC concept
- KYC transaction filters
- ‘One user, one account’ policy
- Trust score
- Platform-based P2P lending
- PoA consensus mechanism
- Income for transport nodes
- Plain transaction fee
- Legalization and compliance

Reputation-Based System

Graphite's reputation-based system is designed to formalize the crypto market.
The system involves:

- Account activation (i.e. wallet confirmation), whereby a user pays a small fee in order to perform outgoing transactions;
- Effective and secure KYC verification through off-chain interactions;
- Transaction filters for counterparty accounts based on KYC.

The features described above ensure that one user has one account, not multiple.

Graphite's emphasis on reputation does not involve any prohibition of anonymity or privacy violation.

Intro

The practical incorporation of reputation into the blockchain is Graphite's biggest differentiator.

In reality, we all use reputation as a way to distinguish different people and organizations in our day-to-day lives. Another's reputation plays a large role in determining the extent to which we trust them; the saying, «His reputation precedes him» exists for a reason.

Graphite's unique system brings the notion of reputation into the blockchain. In a way, it could be conceptualized as a combination of blockchain mechanics with more traditional transaction systems which aims to take the best of both worlds whilst eliminating the worst. No existing crypto market caters to the needs of the market participants who place a high value on reputation — these are our future users.

To successfully implement our vision, at the MVP stage we rely on the following practical 'reputation-centric' features (with more to come later):

- Account activation (i.e. users activate an account by paying a fee before making transfers);
- A KYC verification system with multiple compliant KYC centers;
- KYC transaction filters (i.e. users select their counterparties based on their KYC tier);
- The Trust Score, which serves as a rough estimation of a user's credit rating.

We believe that these features will serve as the basis for an exchange system offering a digitized, but concrete, reputation metric for each of its members.

An important thing to stress at this point is that by no means do we wish to eliminate the privacy and reasonable anonymity that are greatly valued by most blockchain users.

The private data of Graphite users will always be safe and protected. We expect our data requirement to be less intrusive than that required to get an American Express credit card which later inevitably exposes the user to a flood of sales calls. Also, Graphite users' data (even in an obfuscated form) will never be shared with 3rd parties for monetary purposes.

Account Activation

Graphite users need to activate their wallets in order to get network permission to send outgoing transactions, otherwise they will be rejected by the network. Users need to pay a small fee in order to activate their account.

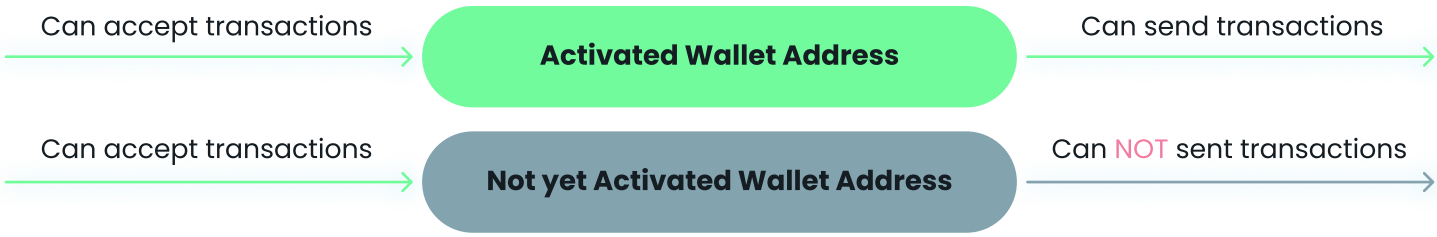
This feature decreases the number of one-off accounts used for fraudulent activities and contributes to the 'One User, One Account' policy.

Graphite users need to activate their accounts with a small fee to be able to start sending outgoing transactions on the network.

The need for account activation is the result of how wallet addresses work on a blockchain. A common problem with a blockchain is that wallet space is often congested with millions of wallets that were used for a small, often illegal, one-off transaction.

To prevent such cluttering from occurring, a user needs to activate their account by paying a small fee to create a blockchain record showing that this specific address is now activated.

Upon activation, an account is granted permission to send transactions to the Graphite blockchain.



Account Activation in Graphite

The payments for account activation will go to the Graphite Foundation and will be used for the further development of the Graphite ecosystem.

Note: Account activation is not the same as a KYC verification; but rather, an account needs to be activated first to then proceed to KYC.

KYC

Graphite has implemented a secure and effective KYC verification procedure.

Compliant KYC centers perform KYC verification using the standard document criteria. For each new verification, a KYC center is randomly chosen and the verification takes place off-chain directly between a user and the respective KYC center.

Upon completing a KYC verification, users can have 1 of 3 KYC tiers:

1. An email address is confirmed;
2. The person's name and physical address are confirmed;
3. The person's identity is confirmed with a video.

The KYC level of each wallet address is publicly stored on the blockchain and is able to be viewed by anyone at any time, but private data such as names, emails, etc., is **never p**ublished on the blockchain and is kept entirely off-chain.

KYC is a cornerstone of our reputation-based system.

KYC verification is needed for general legality and fraud prevention. Any formal financial system is unworkable without some form of KYC. Graphite has implemented a KYC verification mechanism that is both secure and effective.

Obviously, Graphite does not publish users' private data on the blockchain. Only the KYC tier, determined by the KYC verification procedure, is stored there. Graphite users' personal information will never be available on the blockchain.

In the future, Graphite will implement a 'KYC as-a-service' feature that will offer Graphite users an easy way to pass 3rd party KYC procedures. Read more about this in the 'Graphite's Future Plans' section.

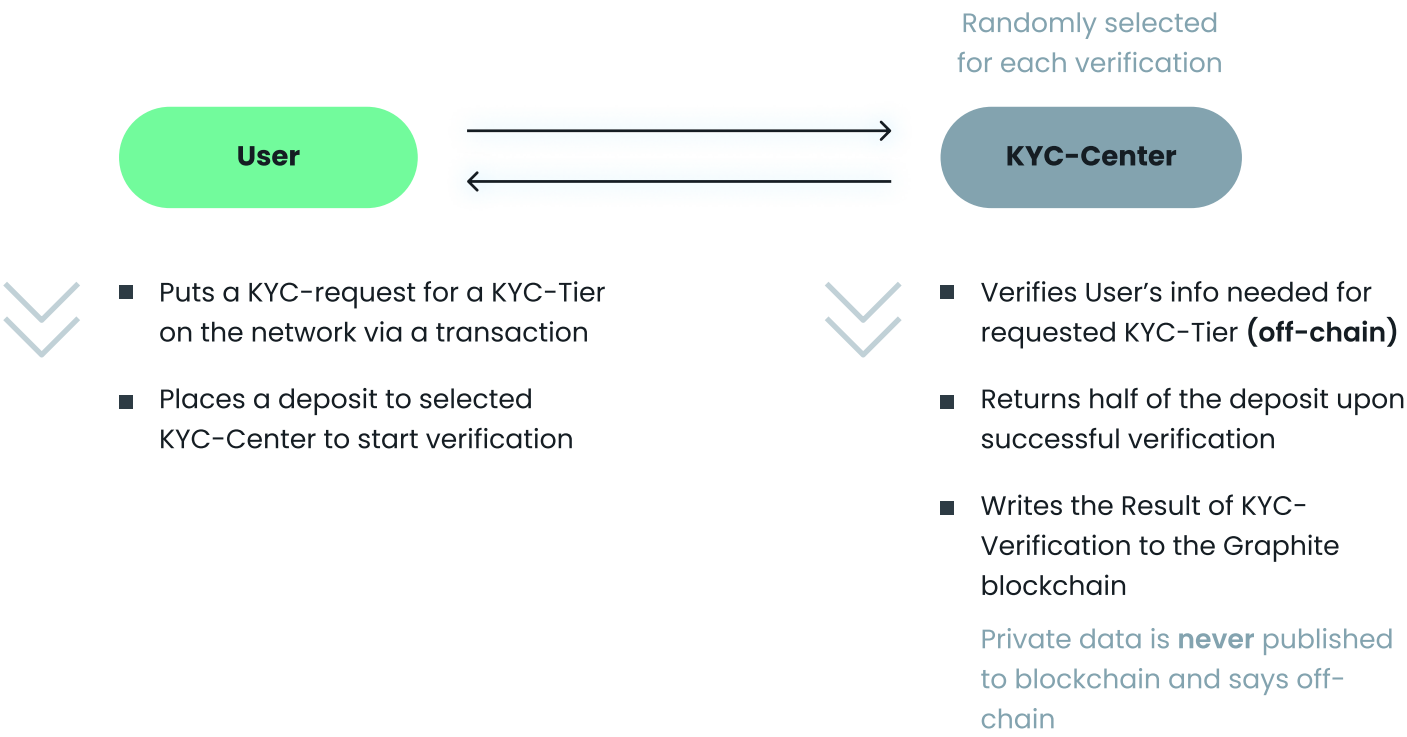
How it works:

There are 3 available tiers (levels) of KYC verification for a user (each level involves having passed all of the previous levels):

- Confirmed authenticity of an email address.
- Confirmed name, surname and physical address.
- Identity confirmed with a video.

Each tier increases the user's individual credibility score. KYC Tier 3 gives a user the maximum credibility score.

KYC Verification Process



The diagram above broadly illustrates the KYC verification process

KYC Verification Flow Step-by-Step Description:

A user requests a KYC verification of a certain tier through a smart contract which is activated by carrying out a particular type of transaction. The user must also place a deposit worth double the fee for the KYC verification in total;

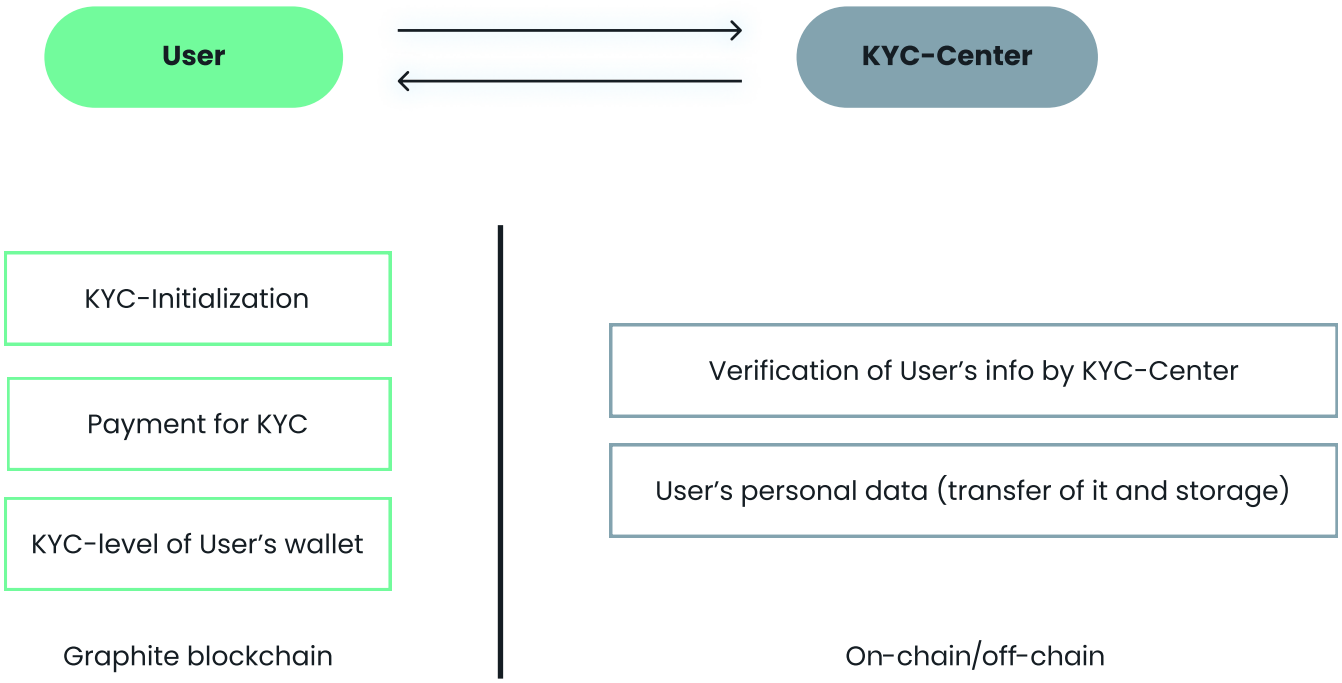
In response to this request, a user receives a randomly generated ID from the KYC center that will be associated with them for the duration of the KYC verification;

The user interacts off-chain and directly with the KYC center to go through the verification process;

In the case of a successful KYC verification, the KYC center will activate a smart contract to record on the blockchain that this user has a certain KYC tier confirmed. Afterwards, half of the user's deposit is returned and the other half is sent to the account of the KYC center;

In the case of an unsuccessful verification attempt, the full deposit will be transferred to the KYC center account and the blockchain will record that the KYC verification for that particular account was unsuccessful.

Blockchain / off-chain interaction in KYC-Verification



The scheme above shows the necessary on-chain and off-chain interactions for KYC

ZK KYC Concept

What is Zero Knowledge Proof

Zero Knowledge Proof (ZKP) is a cryptographic concept that allows data verification without revealing the data itself. The proof occurs by encrypting data to an undecryptable format that only allows confirming the data's actuality through receiving a TRUE or FALSE reply.

ZKP Use Cases

KYC system based on ZKP doesn't reveal users' data but is still can verify its validity for the financial system. ZKP can be implemented in a custom KYC system to make it more reliable and secure for users.

Implementation Concept

This repository contains an automated distributed KYC system using Zero Knowledge Proof (ZKP) with the SNARK algorithm.

The system composes of several independent components:

Core:

- Prover;
- Verifier;
- Verifiable Data Registry (VDR).

Technical:

- Dispatcher;
- Trusted Setup;
- User.

Detailed components description

Prover

It's one of the two main ZKP system components. It composes a mathematical instance known as Proof, which represents initial data in an encrypted form and can't be decrypted directly to access the data behind it. The only way to work with the Proof is to challenge it and verify if the data behind the Proof meets these requirements.
The software part of the Prover is located on VDR (Verifiable Data Registry) to minimize security risks of data transportation between distributed components.

Verifier

The second initial component of the ZKP system. It works with the Proof and checks if the data meets suggested requirements, giving back the result of verification: either "Yes" (True) or "No" (False).
The software part of Verifier is located on the blockchain and is available for any node.

Verifiable Data Registry

VDR is a third-party Data Registry that verifies and contains every user's data. It's essential for KYC procedure as it provides true-by-default data that helps to identify users. The main requirement for the VDR from the ZK KYC system is the ability to extract data from the Registry in a text form, which is the only form suitable for the Prover.

Dispatcher

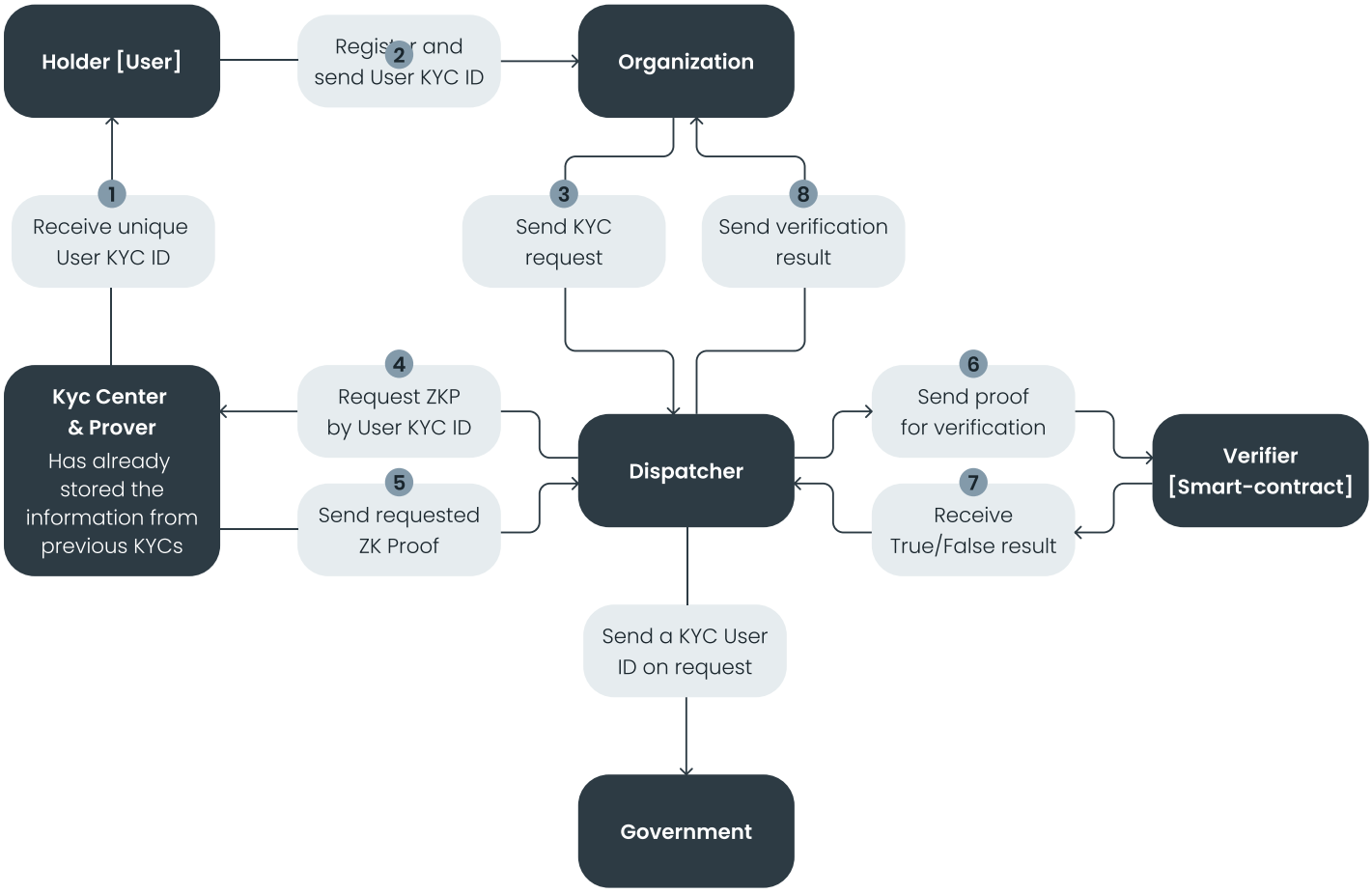
It's a transporting node that establishes communication between the User, Prover, and Verifier. The Dispatcher is delineating the responsibilities of the different components and minimizes harmful behavior possibilities. Each element has limited credentials and can't use excessive knowledge for cheating.

User

It's a client of Dispatcher. The user makes KYC queries, providing personal ID (the valid type for chosen VDR) and VDR ID for KYC verification. The user has no details of the underlying system and only receives an answer from Verifier transported by Dispatcher.

Trusted Setup

It's a component that ensures Prover and Verifier have the same origin and the system functions without third-party intervention. In case when Trusted Setup mismatches between Prover and Verifier, the Verifier will reject the received Proof whether the Proof contains correct data or not.



KYC Transaction Filters

Graphite users can protect their wallets from suspicious incoming transactions by utilizing KYC Transaction Filters.

Users can create rules, or 'filters', which act on the network level and will reject any incoming transactions from accounts with a lower KYC level than that specified by the filter.

Available KYC filters:

- KYC Tier 3 (maximum fraud protection level)
- KYC Tier 2
- KYC Tier 1
- Activated Account

This feature decreases the number of one-off accounts used for fraudulent activities and contributes to the 'One User, One Account' policy.

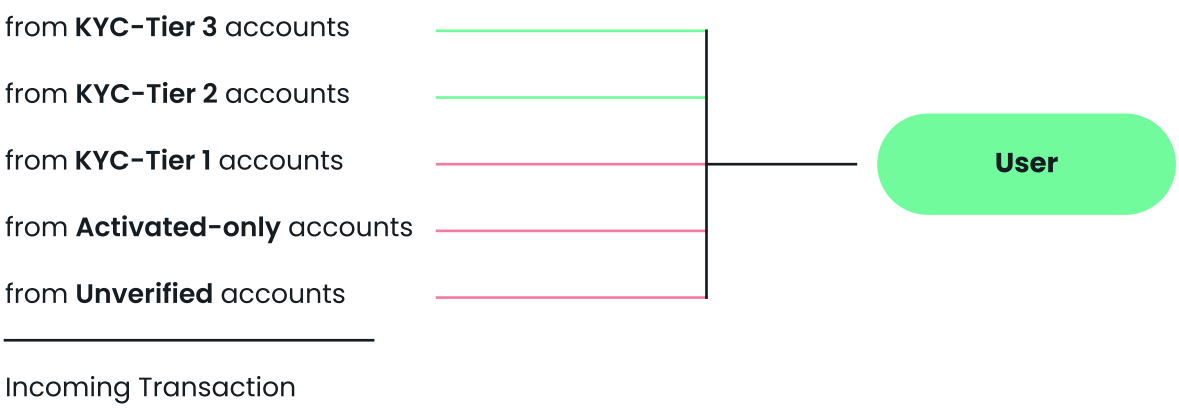
In most circumstances, many of us would prefer to avoid doing any business with questionable parties and Graphite helps its users to do just that. Graphite users can select certain filters to act on their transaction circle (i.e. for incoming transactions). If a counterparty user participating in an incoming transaction doesn't fit the filter, their transactions will be rejected at the network level.

For incoming transactions, a user can create filters to:

- Accept all transactions;
- Only accept transactions from activated accounts;
- Only accept transactions from users with a KYC tier no less than that selected (i.e. Tier 1, 2 or 3).

How KYC Transaction Filters work

- User sets a filter for incoming transactions (it's set as KYC-Tier 2 in the example)
- The network processes incoming transactions based on the active KYC Transaction Filter set by the recipient. If the recipient applies a filter for KYC-Tier 2, only transactions from accounts that meet or exceed this KYC tier will be accepted; rejects the rest.



The scheme above shows the necessary on-chain and off-chain interactions for KYC

‘One User, One Account’ Policy

Graphite’s account activation feature and KYC transaction filters inevitably limit the number of cases when one user has hundreds of wallets. In other words, Graphite establishes a common ‘One User, One Account’ practice.

Such a practice leads to a much healthier market environment that puts Graphite in a category closer to conventional financial systems but without their well-known drawbacks.

Trust Score

Another aspect of the reputation system for Graphite users is the Trust Score. The Trust Score of a user is a numeric value that shows their credibility. A user’s Trust Score is a function of the:

- Time passed since account activation;
- KYC verification level and time since KYC verification;
- Number of accounts that account transacted with;
- Weighted average of the Trust Scores of other address that this account has transacted with;
- Amount of currency residing in the wallet;
- Total amount of currency used in the account’s transactions;
- Number of fraud claims directed to the account.

Currency lenders may use the Graphite Trust Score to estimate a credit rating for a user so as to calculate a risk and interest rate in any specific case. The graphite team looks to the future and regards the scor trust and reputation as a foundation for personal bonds.

Consensus Mechanism: PoA with Polymer 2.0

Graphite is based upon a Proof-of-Authority consensus mechanism which uses a Polymer 2.0 algorithm as its blockchain.

Each epoch, 10 top-tier nodes are selected from amongst the blockchain's authorized nodes. These top-tier authorized nodes have double the chance of becoming a sealer node.

The top-tier authorized nodes are selected on the basis of their performance during the previous epoch. Node performance is defined as the average number of transactions the node has added to the blocks for which it was a sealer.

New authorized nodes are added to the network through a multisig system smart contract.

A fraudulent authorized node can have its status revoked by a vote that has the support of ⅔ of all authorized nodes.

Graphite utilizes a Proof-of-Authority (PoA) consensus mechanism. This mechanism of block validation prevents:

- The excess use of electrical and computational resources;
- So-called 'gas betting' and huge delays between transaction initiation and confirmation in the blockchain;
- Common cryptocurrency fraud.

A PoA algorithm requires a set of authorized nodes for the network to be functional. Authorized nodes are responsible for blockchain validation. For every block, there is an authorized node with a 'sealer' function. When a new block is sealed, this sealer node receives an income from the fee on the new block's transactions (50% of the fee for transactions that have defined entry-point nodes and 100% for the ones that do not).

Authorized nodes are selected on the basis of strict compliance with criteria set by the Graphite Foundation. A multi-signature system smart contract is used to grant the role of an authorized node.

How PoA Works in Graphite:

- An epoch is composed of 2000 blocks with a new block being generated every 3 seconds;
- At the beginning of every epoch, 10 top-tier authorized nodes are chosen on the basis of their performance. Top-tiers have double the chance of becoming a sealer;
- A random value is generated by Oracle. This random value determines the sealer of the block;
- The chosen sealer node generates a new block:
  - Transactions in the memory pool are processed and all invalid transactions are rejected;
  - A complete block made up of only valid transactions is created and signed;
  - This block is sent to other authorized nodes for validation.

- Then, the other authorized nodes perform a block validation:
  - Each authorized node approves or rejects the block on the basis of whether:
    1. The new block is generated by the sealer node of the previous block;
    2. There are no other blocks generated by the same sealer node;
    3. All transactions inside the block are valid.
- Upon reaching a consensus of authorized nodes, the new block is added to the Graphite blockchain and the sealer receives an income from commision fees.
- If a consensus is not reached, then the block is rejected and a slashing mechanism is triggered.

Oracle Random Value Generator

True randomness cannot be achieved within a blockchain and so a separate, external Oracle system is attached to Graphite. The key function of Oracle is to return a random value for each and every unix_timestamp. This value is subsequently used to determine the sealer node for the relevant block.

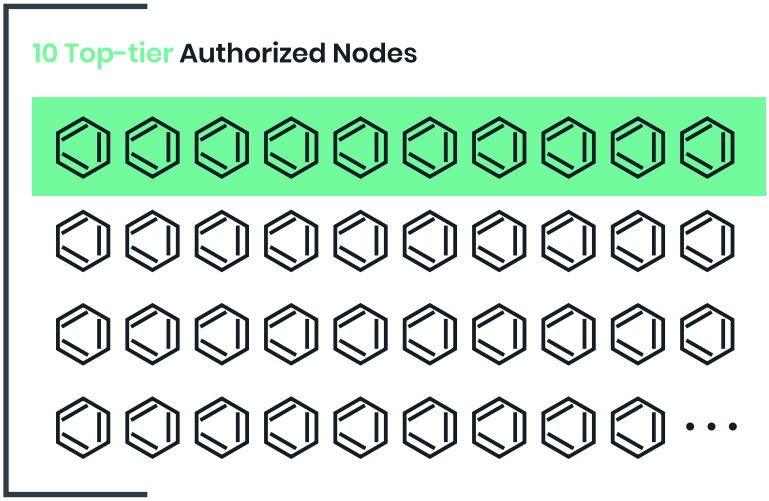
In the interests of fault tolerance, Oracle is composed of five different servers with identical, pseudorandom generators. Each server returns the same random value for each unix_timestamp.

Top-Tier Authorized Nodes

Authorized nodes should be able to sustain a certain uptime & performance. The ability to do so is rewarded by the designation of Top-tier Authorized Node status. Top-tier authorized nodes have double the chance of becoming a sealer node for the block compared to regular authorized nodes and in this way top-tiers are able to earn more.

Top-tier authorized nodes are selected at the start of each epoch. The selection is based on performance during the previous epoch. 10 nodes with the highest performance score become top-tier authorized nodes for the next epoch.

Authorized Nodes pool



Top-tier Authorized Nodes

- 10 Authorized Nodes with best performance are selected as Top-riers
- Top-tiers are chosen for each epoch based on perfomans at the previous epoch
- Rewarded for high performance: 2x chance to seal a block

Performance = avg. number of transaction that Sealer node added to a sealed block

New Authorized Nodes added through multisig system smart-contract.

Revocation by 1/2+1 votes of Authorized Nodes

Node performance is defined as the average number of transactions the node has added to the blocks for which it was a sealer. The performance metric correlates to uptime, CPU power and the network capabilities of a node.

Revocation Mechanism

In order to create an anti-fraud mechanism for authorized nodes, Graphite has implemented a voting mechanism. There is a dedicated field in every block which a sealer can use to add the address of an authorized node that has been expelled for fraudulent activities after a vote has been held. Upon receiving 1/2+1 support amongst all the sealers in the epoch, the system revokes an authorized node's status.

Ethereum-Compatible VMs

Graphite has built an industry-standard Ethereum-compatible VM capable of running Solidity smart contracts.

No additional development resources need to be spent to utilize and execute smart contracts from Ethereum on the Graphite network.

Instead of inventing the wheel, Graphite is implementing virtual machines for nodes that are capable of running Solidity smart contracts.

This means, that Graphite users can utilize already existing Solidity smart contracts (i.e. Ethereum smart contracts). It conveniently works out-of-the-box and requires no additional development resources.

On top of that, since a PoA consensus is governing the Graphite blockchain, Graphite smart contracts will work faster and more efficiently compared to Ethereum smart contracts.

In future releases, Graphite will enhance the usability of its smart contracts by enabling a 'prepaid gas' option for its users.

Graphite Differentiator: Transport Nodes Income

Graphite Nodes

The Graphite Nodes Ecosystem has three key types of nodes on its network:

- Transport and Entry-point Nodes;
- Authorized Nodes;
- Graphite Foundation Nodes.

Each type serves its purpose and ensures high network performance and practical usability.

Usually, standard transport nodes do not earn an income in most of the blockchains currently on the market. So one of the key differentiators of Graphite is that it actually allows its regular entry-point transport nodes to earn an income. To put it simply, it is easy to create a transport node and start making money with it by allowing Graphite users to send transactions to the network from it.

Income for Entry-Point Nodes; How It Works Step-by-Step:

- The transaction sender includes the ‘originating node’ address in the data field of the transaction;
- The transaction is not accepted by the entry-point node if the ‘originating node’ differs from the actual node's address;
- After the block containing the transaction is sealed, the entry-point node is rewarded with 50% of the transaction fee (i.e. the fee); the other 50% goes to the authorized node serving as a block sealer.

Income for Entry-Point Nodes

Entry-point nodes in Graphite are transport nodes that also act as an initial point of transaction entry to the network. Unlike any other blockchain, Graphite allows its entry-point nodes to earn an income from part of the transaction fee.

This feature of the network makes it possible for users to start making an income as an entry-point node without the need for huge server resources.

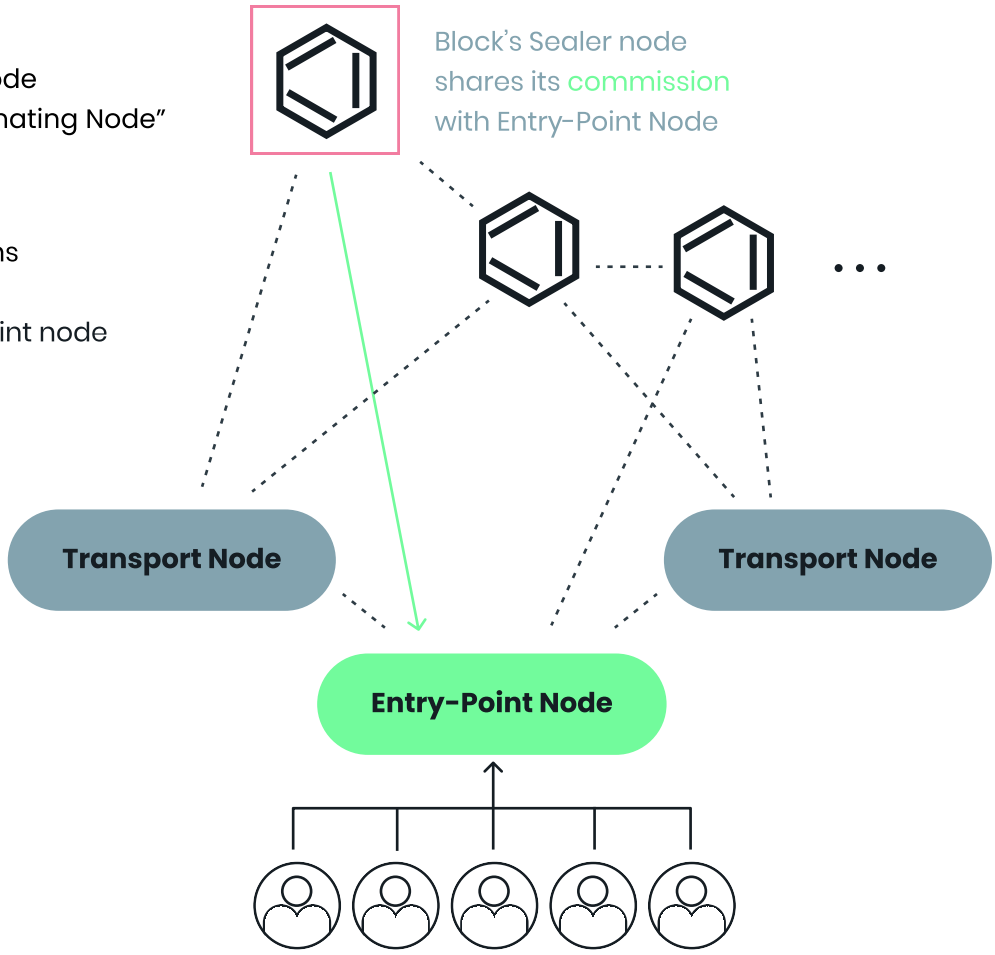
The income for transport nodes in Graphite is technically achieved by adding a field for the incoming node address to a transaction record. When a user fills this field with a valid 'originating node' address, the transaction fee will be the standard rate (i.e. the lowest possible fee).

On the other hand, the fee for anonymous transactions (i.e. without a complete 'originating node' address) will be increased; but, to be clear, we do not in any way prohibit anonymous transactions.

Entry-Point Nodes Income

- Entry-Point Node gets transactions from connected users
- For these transactions, this Node is the one written in the "Originating Node" field of transaction
- Authorized Node that acts as a Sealer for the transactions sheres 50% of a transactions commission with the Entry-Point node

Authorized Nodes pool



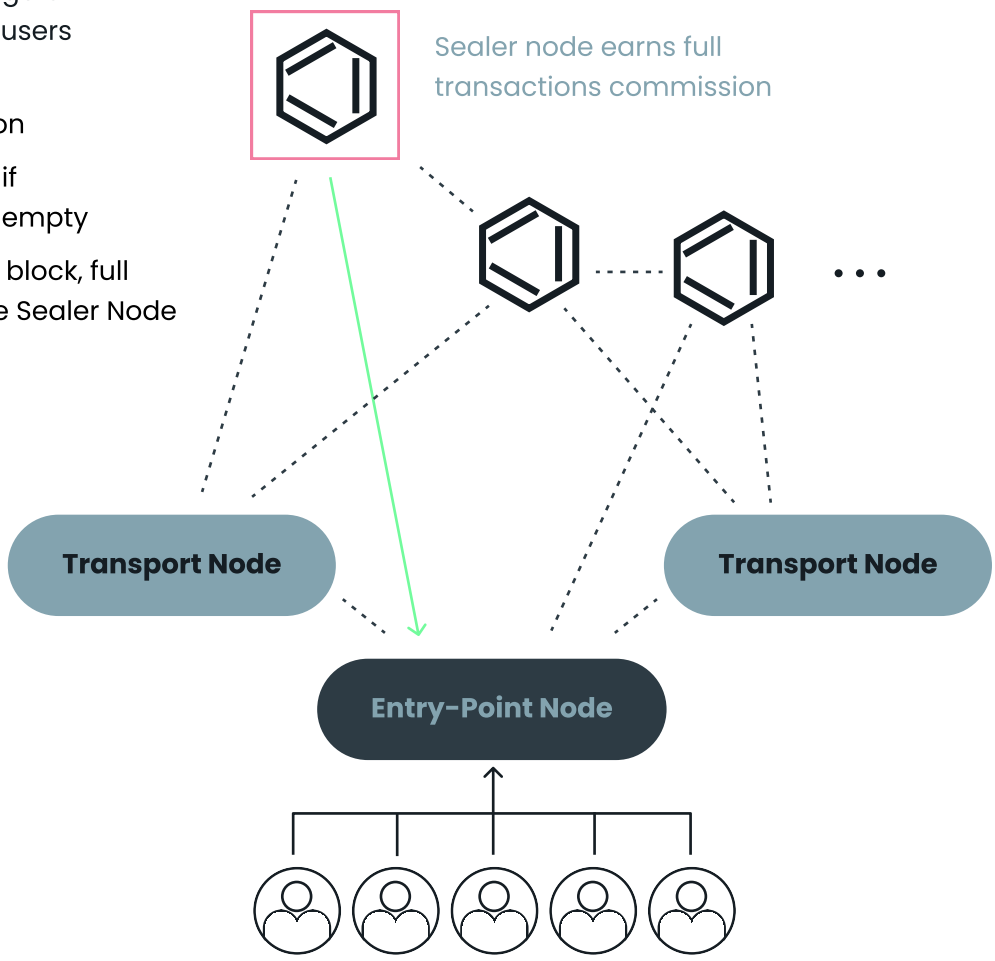
Income for Entry-Point Nodes Scheme

The ‘originating node’ address is necessary for a transport node to receive its reward for the initial admission (i.e. point of entry) of a transaction to the Graphite network. The address of the ‘originating node’ essentially serves as an identifier for the node set to receive the income.

Of course, this system inevitably decreases anonymity since everybody on the network will see a particular node related to a specific transaction. But, realistically, most users would have no interest in these matters and would simply choose the node (i.e. wallet provider) that is the closest and provides the best additional services.

Anonymous Entry-Point Nodes

- Anonymous Entry-Point Node gets transactions from connected users
- “Originating Node” address **is left empty** for the transaction
- Transaction cost is increased if “Originating Node” address is empty
- Transactions get into the new block, full commission is received by the Sealer Node



Anonymous Entry-Point Nodes Scheme

For users who value anonymity and privacy, it will be possible to create a Graphite transport node and use it to send transactions with no ‘originating node’ data; again, Graphite doesn’t make them to reveal which node was used as an entry point for a transaction if the user does not wish to reveal it.

In other words, in order to earn money, Graphite network participants would focus on providing great performance and user experience by acting as an entry-point node for other users’ transactions instead of simply performing pointless and wasteful calculations. We believe this is the best way forward for any blockchain transaction system.

Authorized Nodes

Authorized nodes of the Graphite network are responsible for the validation of new blocks. The pool of authorized nodes consists of compliant authorized nodes and Graphite Foundation nodes which are always available.

Graphite authorized nodes are the primary core of the network, they act as block validators. For a server to become a compliant authorized node of the Graphite network, it must pass a compliance test.

The compliance test for authorized nodes will be described in detail in a dedicated document. For now, we will note that the compliance process involves:

- Passing the highest level KYC verification
- Technical requirements, including:
  - SLA for 99.9% server uptime;
  - A server hosted in a Tier 3 or Tier 4 data center or higher;
  - High server speed and performance;
  - 2TB SDD.

After becoming a legitimate authorized node, the node will be able to validate blocks and earn income.

Graphite will take note of its nodes with the best and worst performance and implement a mechanism to reward authorized nodes for good performance.

Graphite Foundation Nodes

Graphite Foundation nodes are meant to ensure that the Graphite network is live and functioning in any situation (even when all other nodes are down).

16(incl. 7 validators) high-class Graphite Foundation nodes, managed and maintained by the Graphite Foundation, will support the uptime of the Graphite network.

Graphite Transactions

We are designing the Graphite network to be an efficient system for transactions. We aim to solve common and historic issues facing users, for example:

- having to spend up to 25% of the transaction sum in fees in order to add it to the blockchain;
- waiting for minutes to get transaction confirmation.

This is all very inconvenient and unreliable.

The Graphite network transactions are designed to be swift and reliable by ensuring:

- A less than 10 second wait for a transaction to get from the sender to the receiver and be added to the blockchain;
- 1400tps (transactions per second) of network bandwidth.

Our current model of transaction fee gives Graphite users a classic network-load based fee model.

Graphite's Future Plans

We want Graphite to live and grow, therefore we are committed to adding new features to the platform.

These new features will include:

- Differentiation between authorized nodes based on uptime & performance which will affect fee size;
- A dedicated KYC service so that once a Graphite user has completed their KYC, they have automatically completed it for all our partner companies.