GAT - Global Asset Token *beta*

Empowering digital finance and the proliferation of economic equality.

Abstract

The global asset token has been created to facilitate a means of exchange between users that provides an irrefutable transaction history, the capture of fiscal income, the creation of credit, and the distribution thereof. The primary motivation of the GAT project is to empower both individuals and institutional bodies to bring about a system of financial accountability that is both simple and effective for users and institutions to harness in the pursuit of a more equitable future.

Introduction

The GAT project has been created with the following set of capabilities.

1. The ability for users to exchange digital currencies.
2. The ability for fiscal income to be captured from transactions.
3. The ability for credit to be created by institutional bodies.
4. For the proceeds of fiscal income to be distributed amongst registered organisations (representing municipal functions).
5. For the means of exchange to be architected in such a fashion as to allow high transaction throughput, analogous to that which can be performed on centralised means of asset exchange (e.g. visa, master card).

Solutions that exist in the digital currency space, address some of the above, however there is yet to be an asset, and means of exchange defined that could adequately be leveraged at both a national and international level as a replacement of the legacy systems upon which we currently rely.

This paper will focus on the technical aspects of implementing the global asset token, rather than the broader socio-economic objectives upon which the project has been initially commissioned. It is also Worth noting that given the beta nature of this project, the implementation defined below is both subject to change, as well as highlights challenges for which solutions are yet to be defined. These challenges are documented in the final section, and form the basis of the ongoing development of the GAT project, as the organisation seeks to define the most optimal means of achieving the objectives set out above.

GAT setup

For a complete and comprehensive guide to establishing the GAT client and transaction nodes, it is encouraged to consult the documentation at http://gatoken.org/docs however, in brief the process of establishing a transaction node requires the download of a verified installation bundle from the GAT website (http://gatoken.org/download) and for the host operating system to have Nodejs pre-installed. Node can be downloaded directly from https://nodejs.org/. Having downloaded both components, and established NodeJS in the environment you wish to run your peer, simply open a Terminal or command prompt and enter.

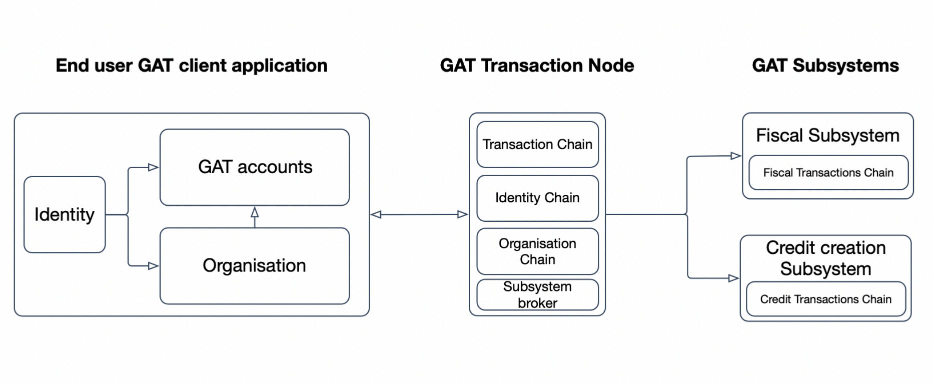
```
node GAT.js
```

This will connect your node with other peers (a collection of verified peers is pre-built into the executable, and this list is added to as other peers are connected to the network), and allow you to process transactions on the behalf of users. In future there will be additional authentication steps required to establish a peer and connect to the GAT network, however for the purposes of demonstration in this beta release, these authentication mechanisms have been omitted.

Architecture

The below diagram represents the overall architecture of the GAT crypto currency. The key points of which are as follows.

1. The GAT iOS application. This serves as a wallet for the storage of GAT, and a means of connecting to the distributed network of nodes that facilitate transactions.
2. The GAT transaction node. This brokers transactions between users, and connects with other transaction nodes to facilitate the shared ledger upon which all transactions are settled.
3. The GAT Fiscal Sub-system. This subsystem is responsible for capturing and distributing fiscal income generated from transactions between users.
4. The GAT Credit creation subsystem. This subsystem is responsible for the creation and distribution of credit (newly minted units of currency)



The above components rely on a collection of data models here expressed in JSON format that can be directly associated with the following subheadings functions. For a complete list of data models and how data models can be combined, please visit the documentation available at http://gatoken.org/docs

The identity object

```
{
        "id":"%GUID%",
        "type":"primary",
        "created":"%DATE_CREATED%",
        "first_name":"%FIRST_NAME%",
        "middle_name":"%MIDDLE_NAME%",
        "last_name":"%LAST_NAME%",
        "dob":"%DOB%",
        "picture":"%PICTURE_BASE64%",
        "protected":{
                "genasis_key":"%GENKEY%",
                "recovery_code":"%REGEN_CODE%",
                "identity_hash":"%IDENTITY_HASH%",
                "biometrics":[],
                "contact":[],
                "assets":[],
                "dividends_transactions":[],
                "pension_transactions":[],
                "locations":[],
                "affilliated_org":[]
        },
        "gat_accounts":[],
        "security_delegates_ids":[],
        "additional_linked_ids":[],
        "authenticated_ locations":[],
        "disgressionary_fiscal_distrebution":[],

}
```

Description:

The identity object hosts information that relates to the individual, many of the fields in the above themselves have supplementary objects (for example there is a model for contact information representation documentation for which can be found in full at the GAT website). At a high level and identity can be associated with one or more GAT accounts, the model for which is defined below, and it is within this account, holdings of GAT or alternative digital currencies (Digital dollars for example) can be held.

The information entered at the time of identity creation is secured with a public private key pair generated on the installation device, this insures the security of the data when it is submitted to the blockchain and will allow only for decryption by the holder of the private key, and authorised organisations who can request decrypted copies of particular fields (these requests are both fielded and executed from within the GAT Mobile wallet and only on authorisation of the identities owner).

The organisational object

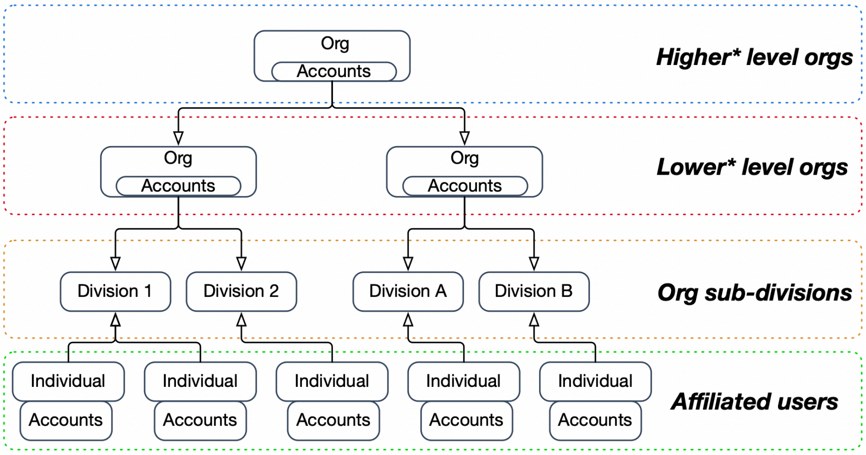
```
{
        "uuid":"%UUID%",
        "type":"%TYPE%",
        "name":"%ORG_NAME%",
        "parent_org_id":"%PARENT_ORG%",
        "function:":"%FUNCTION%",
        "description:":"%DESCRIPTION%",
        "administrators":[],
        "share_templates":[],
        "share_holders":[],
        "affilliate_divisions":[],
        "affilliates":[],
        "division_account_ids":[],
        "fillings":[],
        "created":"%CREATED%",
        "status":"%status%",
        "division_locations":[]
}
```

Description:

An organisational identity can be established from the above format. An organisation can be either public or private. In the event of an organisation being registered as a public body, governance institutions will add the organisations ID to the Registered Municipal Organisations blockchain (a subset of the organisation chain in the above diagram). Organisations have a tiered structure, they can contain divisions, as well as be agglomerated by a higher tier organisation.

Administrators affiliated with “higher” level organisations, carry authority in “lower” organisations. Individuals can be affiliated with both private and public organisations, and in addition organisations can be affiliated with multiple GAT accounts.

The below diagram demonstrates the hierarchy and affiliation between organisations, accounts, and individuals.



The Account Object

```
{

        "uuid":"%UUID%",
        "owers_ids":[],
        "owners_ids_hashes":[],
        "transaction_in":[],
        "transaction_out":[],
        "transaction_hashes":[],
        "chain_hash":"%CHAIN_HASH%",
        "protected":{
                "genasis_key":"%GENKEY%",
                "regen_code":"%REGEN_CODE%"
        },
        "type":"%TYPE%",
        "created":"%CREATED%"

}
```

Description:
The account object contains a collection of keys, historic transactions, and the hash of the current balance of the account. This hash is updated by individuals that transact with a specified account. There is a one-to-one association between an individual and an account, and similarly there is a one-to-one association between an organisation and an account. Though as per the above diagram, configurations can be establish such that account hierarchies permit control of assets in accordance with the hierarchical standing of one organisation relative to one another**.**

The token object

```
{
        "uuid":"%UUID%",
        "from_account_holder_id":"%TO_ACCOUNT_ID%",
        "to_account_holder_id":"%TO_ACCOUNT_ID%",
        "transaction_currency_symbol":"%VALUE%",
        "transaction_currency":"%VALUE%",
        "value":"%VALUE%",
        "created":"%DATE_TIME%",
        “owner_chain”:[],
        “minting_batch_id”:”%MINTING_BTACH_GUID%”

}
```

Description:
The token object represents an individual unit of value, a token by default assumes a currency type of GAT, however dependent on the transaction being created from the credit creation subsystem, coins of different currency types may be minted. We will see more on the minting process in a subsequent section.

The transaction object

```
{
        "uuid":"%UUID%",
        "to_account_id":"%TO_ACCOUNT_ID%",
        "from_account_id":"%FROM_ACCOUNT_ID%",
        "value":"%VALUE%",
        "created":"%DATE_TIME%",
        "authentication_hash":"%AUTH_HASH%",
        "old_balance":"%OLD_BAL%",
        "signed_new_balance":"%NEW_BAL%",
        "location":{
                "lat":"%LAT%",
                "lng":"%LNG%",
                "location_meta_data":"%LOCATION_META_DATA%"
        },
        "TO_fiscal_capture_subsystem_id":"%TO_FISCAL_SUBSYSTEM_ID%",
        "TO_fiscal_contrebution_value":"%TO_CONTRIBUTION_VALUE%",
        "TO_fiscal_contrebution_value_perc":"%TO_CONTRIBUTION_VALUE_PERC%",
        "FROM_fiscal_capture_subsystem_id":"%FROM_FISCAL_SUBSYSTEM_ID%",
        "FROM_fiscal_contrebution_value":"%FROM_CONTRIBUTION_VALUE%",
        "FROM_fiscal_contrebution_value_perc":"%FROM_CONTRIBUTION_VALUE_PERC%",
        "TO_auth_from_hash":"%TO_AUTH_FLOW_HASH",
        "FROM_auth_from_hash":"%FROM_AUTH_FLOW_HASH",
        "TO_auth_flow":[],
        "FROM_auth_flow":[],
        "status":"%STATUS%"
}
```

Description:
The transaction object records a transfer of tokens from one account to another. Many of the fields in the above model are optional, however the mandatory fields that are not automatically generated are to_account_id and from_account_id. Prior to a transaction being permitted, the balance of the senders account is checked by the recipient to ensure sufficient funds in the requested currency exist to fulfil the transaction. Fiscal income is also captured as part of the transaction object (the recipient of income is noted under TO_fiscal_capture_subsystem_id).

Interactions

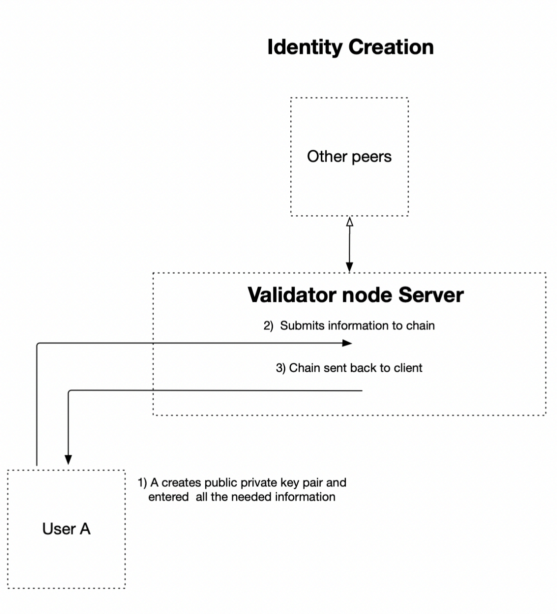
To facilitate the overarching objectives of the project, below documents the interactions between users, organisations, nodes and subsystems.

The interactions set out below are ordered in succession of when assets are created and exchanged. The below also assumes that all components of the system have been set up, and connectivity between peers has been established (as per the set up steps defined above).

The process of minting individual units of currency is covered in a subsequent section, however the below does define the process by which funds are transferred between accounts and between accounts and subsystems.

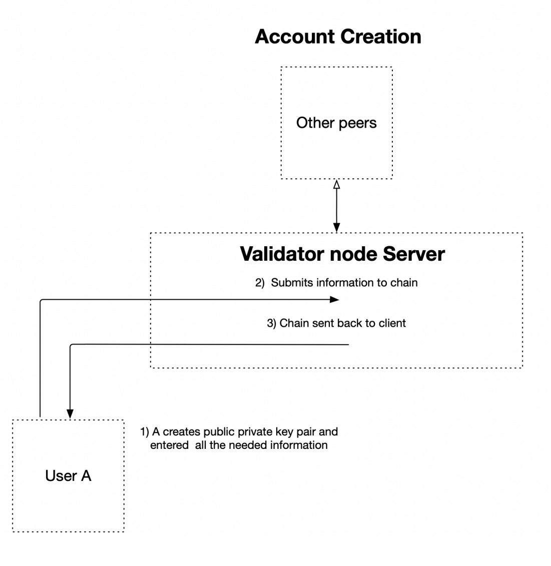
Step 1. Identity Creation

When a user downloads the GAT wallet they will be invited to create an identity, this takes a collection of pieces of information that uniquely identifies the individual (as noted in the identity model above). The information is signed with the public private key pair generated on the device and uploaded to the bound GAT transaction node.


Identity Creation
Other peers
Validator node Server
2) Submits information to chain
3) Chain sent back to client
User A
1) A creates public private key pair and entered all the needed information

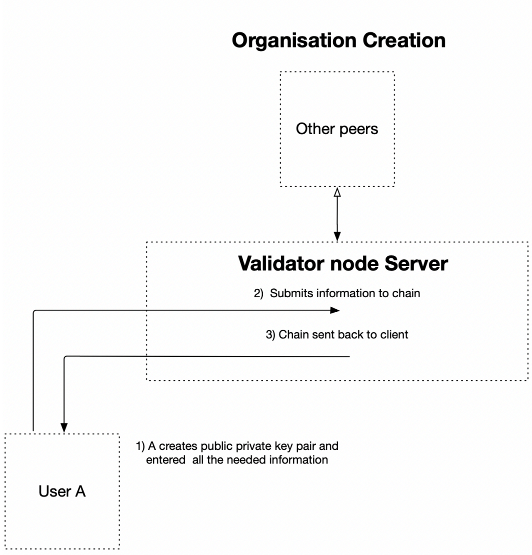
Step 2. Account Creation

A user is then invited to create an account, the wallet will automatically generate a unique identifier for the account however the user can also specify a name for the account such that identification is made easier. Every account has a distinct public private key pair, and it is with this key pair individual units of currency are signed, concerning ownership by the signing account. Every account is created with a password and a recovery key, the recovery key allows for the account to be re-established with a new public private key pair (to cover a case where an individual loses their phone or client device). Once an account has been created it will be uploaded to the bound GAT Transaction node.


Account Creation
Other peers
Validator node Server
2) Submits information to chain
3) Chain sent back to client
User A
1) A creates public private key pair and entered all the needed information

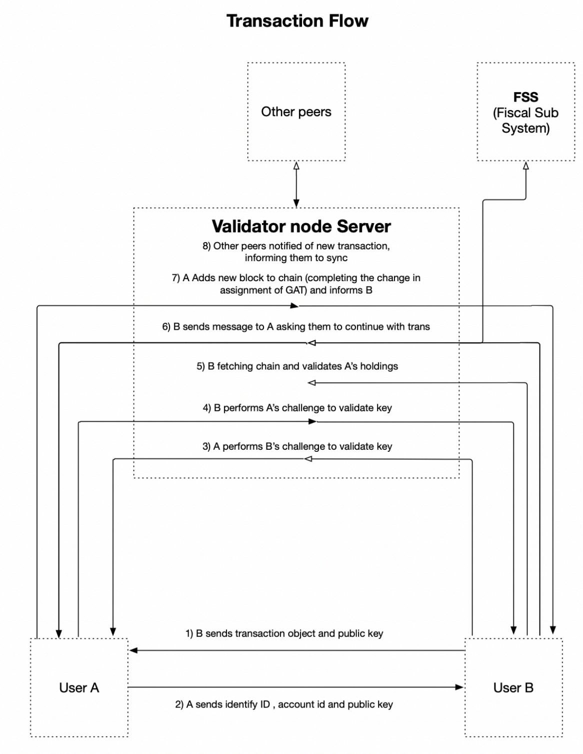
Step 3. Organisation Creation (optional)

A user may optionally wish to create an organisation, this as previously noted can be a public or private body. The creator (and any assigned administrators identities) have executive authority over any named GAT accounts (holding funds) and the appointment of other administrators and creation of divisions. Every organisation has a public private key pair that will used to permit executive actions, which in addition to the above, allow for the change in status or type of an organisation. Having entered the requisite information for the establishment of the organisation, the organisation is uploaded to the bound GAT Transaction node.


Organisation Creation
Other peers
Validator node Server
2) Submits information to chain
3) Chain sent back to client
1) A creates public private key pair and entered all the needed information
User A

Step 4. Transacting

Having established an identity and an account, a user can begin to transact with other users. The process of initiating a transaction begins with the transacting peers exchanging information. The payment request must provide a transaction object with several fields omitted, while the payee must provide their identity (ID) and the account (ID). This initial exchange is performed by the sender and recipient reading QR codes representing this information on each other's devices simultaneously. The client implements a Zk-Snark that challenges the transacting parties to prove their identity by requesting they decrypt a message sent from one party to the other, this is performed in a bidirectional fashion between both transacting parties such that upon completion, both have independently verified the other transacting party has ownership of funds to be transferred. Once the scan is complete, the remaining steps of the transaction are handled by the client and the bound GAT Transaction node. The below diagram sets out the remaining steps.


Transaction Flow
Other peers
FSS
(Fiscal Sub System)
Validator node Server
8) Other peers notified of new transaction, informing them to sync
7) A Adds new block to chain (completing the change in assignment of GAT) and informs B
6) B sends message to A asking them to continue with trans
5) B fetching chain and validates A's holdings
4) B performs A's challenge to validate key
3) A performs B's challenge to validate key
1) B sends transaction object and public key
User A
User B
2) A sends identify ID , account id and public key

Upon the completion of the transaction, both peers can refresh their balances and observe their new holdings. Note also that a configurable proportion of the transaction value is delivered to the fiscal subsystem. From here registered public organisations can be funded from the proceeds of transactions.

Minting

The minting of new units of currency (of any denomination) begins with the Minter acquiring a public private key pair from the GAT organisation. This key pair, is used to sign all units of currency created. All distributed keys are baked into all official clients (the GAT Mobile Wallet for example) such that tokens received (units of currency) can be validated by a user for authenticity. While there are no limits to the amount of credit created as part of any distinct mining process, the GAT Organisation ultimately has the authority to recognise, or otherwise prevent circulation of coins/tokens minted from a particular key pair. All units of currency are imbued with a minting batch ID, dependent on the batch ID, particular units of currency can be created for use only in the facilitation of specific types of transaction. For example a coin/token could be created that would permit its owner to exchange a given value of GAT (or another currency denomination) for only a particular good or service. In context this could be the creation of credit for students to use to support college and university financing.

Fiscal income distribution

Fiscal income is distributed between verified organisations. The verification process of organisations who perform municipal functions is conducted in conjunction with the GAT Organisation, a representative of the organisation will work with local and national governments to ensure the appropriate organisations are represented on the Organisation Chain (hosted by GAT transaction nodes).

Fiscal income can be distributed either by centralised authorities (registered GAT organisations representing government departments) or by users electing specific allocations of fiscal income to causes they specifically would like to fund.

These two distribution mechanisms can be set by geographic boundaries (see documentation for the usage of location specific fiscal distribution) and lays the ground work for a societal evolution towards a direct democracy model.

Security

While many of the aspects of the GAT infrastructure are secured with public private key cryptography, additional measures will be created to further secure individuals identities, and their confidential information. A peer review is required to ensure there are no fundamental areas of weakness in the current implementation, and that all future versions beyond beta, preserve, persist, and enhance security.

Challenges and commentary

There are a broad range of challenges and commentaries associated with the current beta release of GAT and related governance systems. The below list is by no means exhaustive, however identifies the key areas of development that are required and form part of the overarching roadmap for the GAT Organisation.

Wallet

1. The greatest challenge for all client applications is security. The possibility that an individuals funds could be fraudulently misappropriated must at all costs be prevented. This will require an evolution of our authentication mechanisms to ensure that in the realm of a quantum powered future, such mechanisms are adequately architected to defend against any possible attack.

Identity

1. A mechanism needs to be devised to allow partial description of a users identity object, and for the detail exposed to be viewable only for the specified purpose, for a specified time.
2. Individuals require a whistleblower function to alert the GAT Organisation two instances of malpractice and fraud.

Organisational

1. The vetting of organisations to be permitted funding from fiscal revenue needs to be involved. In the outline posed above and as per current implementation, an organisation deemed to be in the public good is one that can be created (and verified) by an organisational body registered with the GAT Organisation. This promotes two challenges. Firstly the sheer number of municipal functions that would require vetting by the GAT Organisation are significant, and in taking such a responsibility the GAT Organisation would perpetually become the arbiter as to whether an organisation effectively provided the municipal functions they were initially charged to dispense. This represents an impossibility for the GAT Organisation to deliver a consistent vetting process globally. Secondly in the event that organisations created for the public good were verified as such by individuals within the jurisdiction of the organisations remit, additional safeguards would have to be afforded to prevent sections of the electorate being pressured into verifying , fraudulently, an organisation that would intern be able to receive fiscal income improperly.

Token

1. A conversion mechanism needs to be defined to allow assets of one denomination to be converted to a new denomination.

Transactions

1. The transactional architecture can evolve in the years ahead such that the majority of mobile bound client applications (wallets) can participate in the GAT network as verifying nodes, (this as opposed to the current model where client applications must connect to a transaction node, which itself is part of a peer-to-peer network of other transaction nodes. For clarity the primary challenge preventing such a network topography relates to cellular signal processing and request routing by carriers. Carriers leverage GNAT to route outbound requests and responses. However prevent mobile clients on carrier networks from serving files (as a GAT transaction node requires) consistently. Some carriers support NAT traversal in a fashion that would permit a mobile device requesting and serving files, but conceivably until such a network architecture is ubiquitous, mobile wallet applications will need to remain connected to a GAT transaction node to facilitate an exchange. With the arrival of SpaceX's Starlink project, in the decades ahead a desirable network topography may be created such that an evolution toward this model could take place.

Fiscal capture and distribution

1. Additional nuances in how fiscal income is captured need to be implemented. This would permit differing levels of "tax" being generated from distinct collections of individuals. Notionally a tax system could be implemented under a fundamentally new paradigm, where, individuals working in sectors whose roles in the global economy are diminishing, as a result of technological innovation, would be both required to pay less, and receive more in the form of a dividend payment direct to the users account, as a form of social security. This could be implemented at a national or international level, and lays the ground work for an international basic income to buy goods and services. This in turn would become prudent and relevant at such a point where mechanisation and technological proliferation reach, to such an extent, where, an individuals value to society is (from a purely economic standpoint) significantly diminished.

Credit creation challenges

1. The means by which credit is created, and to whom specifically such powers are granted poses a unique challenge. Ultimately it may be beneficial for these rights to be granted by democratic consensus and for powers to be rescinded without appeal if a significant portion of the electorate believe such powers are being improperly exercised.

Credit distribution challenges.

1. Preventative measures need to be implemented to prevent denominations of the GAT Token being created that can only be spent by particular individuals.