Motivus: Transactional Artificial Intelligence

www.motivus.ai

O. August 13, 2017 R. Jan 6, 2017.

Abstract.

Motivus is a secure blockchain platform providing a marketplace for machines, people and applications to transact micro services and utilities specific to artificial intelligence. Motivus provides an easy to use interface and access to a full featured ecosystem. Through Motivus developers can build, publish, distribute data and applications with a token powered network that supports smart contracts, interoperability, storage and distributed computing infrastructure.

Introduction

Designed for the speed, security, data ownership, scale and throughput required for artificial intelligence, Motivus brings these capabilities into the hands of developers, data scientists, and researchers. Machine processes and utilities are distributed as utilities across the network each with specific capabilities. Some utilities are fully autonomous such as GPU processing hardware, algorithms, and AI modeled predictions while others are HITL (human in the loop) services like scientists and human data annotators. An application on Motivus can connect utilities together by passing the output of one utility to the input of another creating processing pipelines or railways. For example a computer vision process may first need to detect the text in an image, followed by a second process detecting the faces of people in that image. Lastly, a process for determining the emotions of those people of the faces detected all to produce a final analysis of the objects in the image.

Utilities on the network which provide these algorithms, data sources, annotations or hardware receive tokens by those people, processes or machines which utilize these utilities. The native token that powers this economy is called a MOT which stands for machine of things. MOTs are exchangeable with the other utility tokens on the network to reduce holding requirements and failures caused by fragmentation. This interoperability across tokens on the network is important to ensure the utility value over the monetary value of the tokens. Elected delegates with the greatest stakes are rewarded for witnessing these transactions across the network.

We believe transactional artificial intelligence creates a value-based ecosystem on the blockchain introducing a marketplace for all possibilities in artificial intelligence. Such an open system liberates the raw material of artificial intelligence — “data”, from single corporation control giving it both permanence and community governance. Further the decentralization of algorithms, datasets, processes and compute power rids of bias which enables risk and decisioning discrimination making artificial intelligence less a threat than a centralized institution.

MOT Tokens

Blockchains/cryptocurrencies utilize tokens to create a secure system of utilization. As a result, Motivus issues a cryptocurrency token called MOT. MOT (machine of things) is used to pay fees in order to generate transactions and use the platform. MOT tokens can be acquired through various means, such as purchasing them from an exchange, earning them as a utility provider or directly from another individual.

Network

The focus of Motivus is on scale, speed, access and security. The node.js powered platform makes it easy to rapidly deploy new nodes. The network is capable of processing thousands of transactions per second to support applications that utilize artificial intelligence.

The components necessary to create this network are:

- Utilities

- Proof of performance
- Oracles
- Manifests
- Railways
- Storage

Blockchain applications as Utilities.

Each utility and service is exposed on the network as a node. Utilities are powered by tradable digital tokens that can be used as currency, access control or a representation of any asset value. These tokens use standard API's making them compatible with any wallet or exchange. The utility tokens can execute a programmed ruleset automatically. Each utility token is wrapped in a standardized API making it easier to connect, coordinate and ultimately transact across the network. The protocol for each of these tokens supports on-chain and off-chain services allowing developers to be creative when designing new use cases centered in artificial intelligence. By default Motivus has a utility for voting which can be extended. Utilities can be used for a myriad of services. Utilities can process predications, provide hardware infrastructure, manipulate data and even provide a dataset (trained as a model or raw) as output.

New utilities require approval to be added to the network. This is to prevent pollution of non-relevant utilities and to reduce the footprint of running a full un-tapered node. The approval process to add new utilities is managed via an election process which a group designated

on the network participate in. The people who make up this group are called Oracles. They are qualified by an on-network process.

Proof-of-Performance

The voting utility, Proof-of-performance; is an autonomous, 2D neural network network which can make predictions based on unsupervised datasets namely votes. This voting system is used to calculate weights of network participants in order to elect delegates, quantify oracles — among other things.

Parameters used in proof-of-performance:

(A) Speed - the elapsed time between votes. The discriminated cases for speed are based on an unnatural pace of answers/votes being submitted. The net calculation of speed is based on machine calculations against moving averages. (B) Accuracy - based on the frequency of providing results shared with the consensus. This calculation is based on elections that improve usable confidence scores in model predictions (C) Redundancy - frequency in reacted answer. Calculated by the volume of weighted correct contributions weighted over time.

When key network contributions are identified, new elections are spawned where these contributors can become oracles, where their votes can have greater impact to the network.

Oracles.

Oracles are critical to the integrity of the network. Oracles are HITL (human in the loop) participants elected across the network who have been qualified to participate in validating the conditions of key aspects of the network. Initially the Oracles are hand picked to participate in the network to strategically seed the networks capabilities, drive utilization and hone in on key areas of focus (artificial intelligence).

In order to keep the value in the utilization of the network strong, only select utilities can be added. Adding new utilities to the network require Oracles to approval the addition. This approval is made through an election process. Oracles must continue to participate in the network to maintain their status as Oracles.

The criteria for qualifying as an Oracle are based on:

(a) Recency - calculated based on the oracles most recent activity contributing to the network. (b) Frequency - based on the volume of contributions to the network. (c) Quality - the impact of activity made by the Oracles. (d) Accuracy - the historical success of voting for the winning candidate in the election process.

Manifests.

Utilities on the network can be linked together to produce high value processing pipelines which we call Railways. These pipelines can mix data sets, storage, calculations, voting and computing amongst other

things made available on the network. In order to execute each pipeline, a transaction must be created which includes a manifest. A manifest is a set of instructions which indicate the input data, utilities to interface and output destination. These instructions are required to be sent with each on network transaction. The manifest includes the address of the origin source application making the request including address, data, railway route (utility nodes). An example manifest:

```
{
	address: dfj2039rsodvnsvnvmsd02e9jfsdn2f90efd,
	data: {
		format_encoding: base64,
		data:
iVBORw0KGgoAAAANSUhEUgAAAAEAAAABCAYAAAAfFcSJAAAADUlEQVR42mP8z8BQDwAEhQGAhKmMIQAAAABJRU5ErkJgg
g==,
		ref_id: 120391
	}
	railway: [
		{
			address: 203023ej23kenksfnseoinf293f0nsdlfn,
			amount: 0.00020001,
			amount_type: mot,
			input_data:  120391,
			output_data: 203023ej23kenksfnseoinf293f0nsdlfnx120391 //hex mash of  address and
output ref id
		},
		{
			address: eofjfkdlfof8ffj5474jfj2930fkd893o4jfjdo4,
			amount: 0.0000001,
			amount_type: mot,
			input_data: 203023ej23kenksfnseoinf293f0nsdlfnx120391 //hex mash of  address and
output ref id,
			output_data eofjfkdlfof8ffj5474jfj2930fkd893o4jfjdo4x
203023ej23kenksfnseoinf293f0nsdlfnx120391 //extended data chain
		}
	]

}
```

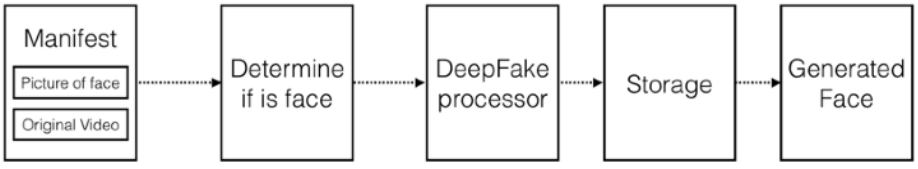
The mapping reference of Utilities in a manifest contain the following:

Address	The address node of the resource (utility, etc)
Amount_Type	The type of token to transact (default MOT)
Amount	The amount of tokens you want to exchange in the transaction. (The exchange rate is automatically calculated)
Input_Data	The input data to be transacted. By default a base64 encoded string. This string can be an address, image, etc. This is set by the header of the encoding. The address can be linked to an existing node on the network. Use a hex encoding to link the utilities.
Output_Data	The output data as a referenced node on the network. Use to link utilities across the network.

Railways.

Railways are defined as a specific set of utilities networked to execute a case. The premise of the network is artificial intelligence, resulting in many of the railways being used repeatedly and often at high volumes. This ensemble of processes is set by the requirements in the request's manifest. The decentralization of these railways allows reduction on production overhead for developers.

In the example below we illustrate a railway that is used for generating deepfakes. Deepfakes use existing video footage and a machine learning algorithm. This algorithm is able to take the face of a person and seamlessly overlay it onto the body of another inside a video clip. Often the resulting video is indecipherable from the original.



The railway used to mount this process on Motivus and expose for use in a an application are as follows:

DeepFake Railway - generate video using deepfake from existing video footage. The manifest requirements:

a. Input face of a person
b. Input of an original video clip
c. The first utility in the railway takes the image and detects face.
    a. If there is not a face, return a blank response to terminate the process and prevent unnecessary activity on the network
    b. If there is a face, return the cropped data of the face
d. In the second utility, the detected face from the first nodes output is used to mash up the face of the original video clip. The output is sent to the final utility.
e. The final utility takes the newly generated media and saves it to a storage block accessible via the address set in the output node. At any point people can access the output address and view the resource.

Transactions.

Each operation on the network requires a signed transaction request including the manifest. The transactions are recorded through delegated proof of stake. Delegated Proof of Stake (DPOS) is a fast, efficient, decentralized, and flexible consensus model which helps achieve a key requirement of speed. DPOS leverages the power of stakeholder approval voting to resolve consensus issues in a fair and

democratic way. All network parameters, from fee schedules to block intervals and transaction sizes, can be tuned via elected delegates. Deterministic selection of block producers allows transactions to be confirmed in an average of just 1 second. Perhaps most importantly, the consensus protocol is designed to protect all participants against unwanted regulatory interference. Transactions may occur between external applications making requests, utilities in the network and other machines.

Security

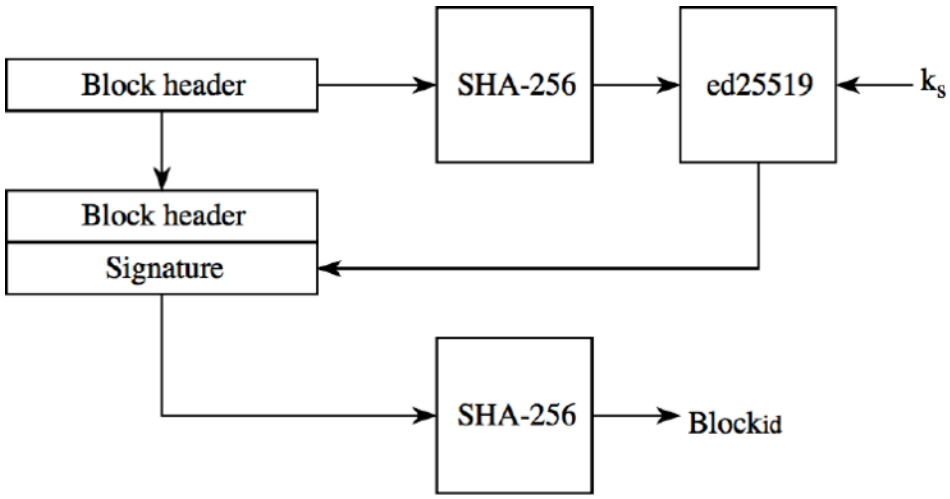
Motivus uses cryptographic hashing in order to secure all aspects of the system. The system uses EdDSA as it provides a much faster mechanism for hashing and providing security rather than ECDSA which is found in many other cryptocurrencies, such as Bitcoin.

A keypair is consists of a private key and a public key. A private key is a piece of information known only to the owner of the key. The public key is derived from the private key and can be used to validate that the private key belongs to the owner, but not provide access to the owners private key. Elliptic curve cryptography is used to generate cryptographically secure key pairs. The process used to generate the key pair operates under the following assumptions: When a user creates an account, a BIP39 mnemonics (the passphrase) is generated for the user. This passphrase is hashed using the SHA-256 hash function into a 256 bits string. This hash is subsequently used as a seed in ed25519 to generate the private key key store and derives its public key kp.

An address or the wallet ID is derived from the public key. The public key is hashed using SHA-256 then the first 8 bytes of the hash are reversed. The account ID is the numerical representation of those 8 bytes, with the 'L' character appended at the end. The following figure is the representation of an address and its associated account details.

Blocks

A blockchain is composed of blocks, and a block is composed of a header and a list of confirmed transactions. When a delegate is assigned a slot and has a node running, that delegate generates the next block and confirms up to 25 transactions from the transaction pool. These confirmed transactions are added to the payload of the block and subsequently signed into that block.



The block header contains all the information about the block. The following fields compose the block header:

- A 32 bit integer identifying the version of the block

- A 32 bit epoch timestamp of when the block was created
- The 64 bit Id of the previous block
- A 32 bit integer corresponding to the number of transactions processed in the block
- A 64 bit integer corresponding to the total amount of MOT transferred
- A 64 bit integer corresponding to the total amount of fees associated with the block
- A 64 bit integer corresponding to the MOT reward for the delegate
- A 32 bit integer corresponding to the length the payload
- The 256 bit hash of the payload
- The 256 bit public key of the delegate who generated the block

Storage

The network has a distributed storage system in order to reduce bottlenecks caused by high frequent transmission of large payloads. Datasets that are re-used shouldn't be transmitted in a manifest, instead the datasets should be recorded in storage and remotely accessed using a reference

Incentives and Network Rewards.

On Motivus, there are various incentives provided to make running a node appealing. The first of these is the block generation reward and the other reward is the accrual of fees for securing the network as an active delegate for the round in which that delegate participates.

As with bitcoin and nearly all other blockchain systems, Motivus rewards the block generator a fixed amount of tokens per block successfully generated and accepted by the system. In Motivus's system, all active delegates that successfully participate are rewarded for securing the network.

The block reward linearly decreases over the lifetime of the network, providing significant incentive to actively participate as an active delegate. The reward will decrease every 3.000.000 blocks from the initial reward block.

Conclusion.

We have proposed a system for transactional artificial intelligence. We started with a series of Ethereum powered smart contracts however found challenges in getting the speed necessary due to unpredictable network congestion. Additionally exposing distributed hardware pools for GPU's became a challenge. To solve this we used a lighter weight blockchain and delegated proof of stake to overcome speed, scale and distribution bottlenecks. Further by adding Oracles network pollution is almost eliminated optimizing resource utilization.

References.

[1] “Trane/TPAI,” http://www.trane.ai/whitepaper, Aug 2017.

[2] http://cr.yp.to/highspeed/coolnacl-20120725.pdf

[3] “Ark”, https://ark.io/Whitepaper.pdf