The PlanetPay project

DAO platform to pay the planet's people for meaningful work

Technical White Paper July 2018

Contents

1: Introduction

The PlanetPay project requires the use of a truly decentralized DAO (Distributed Autonomous Organization), the PLP DAO combined with an advanced cryptocurrency (PLP).

The PLP DAO

A DAO is an autonomous service machine implemented in software in which people can participate and be economically active.

DAOs are network centric systems of organizations that operate through rules encoded as computer programs called smart contracts which exist on a distributed public blockchain.

They rely on the ability of blockchain technology to provide a secure digital ledger that tracks financial interactions across the internet, hardened against forgery by trusted time-stamping.

This approach eliminates the need to involve a bilaterally accepted trusted third party in a financial transaction, thus simplifying the operation of the DAO.

As a self-learning machine the DAO will optimize the transactions across the network.

The extraordinary thing about DAOs is that no single entity owns them and that they have no conventional management structure or board of directors.

Whereas there are a number of ICO initiatives attempting to create DAOs of one type or another, what is unique about the PLP DAO is that it is a development of a number of existing real world systems but tailored to operate autonomously.

Virtually all current DAO initiatives are skeuomorphic, meaning that they attempt to automate tasks and functions which are part of existing organizations. The PLP DAO develops and implements original, empirical research so that only essential tasks and functions are included, and new, original functions are created.

It is clear to us that an enterprise which operates through a DAO cannot merely automate existing procedures used to administer companies, but needs its own rules and way of operating.

Arguably, there are no pure real world DAOs active in the world today apart from the "Bitcoin System" (Bitcoin and many of its derivatives) – that system is a genuine DAO because no one individual can control it and no individual needs to get involved in voting or deciding which decisions to make – people such as the miners get involved or drop out voluntarily and the DAO, the System, couldn't care less who they are or whether they participate or not – it is oblivious to them.

In the same way, the PLP DAO is being designed to carry out its functions and controlled by incentives to create a win-win scenario for all of the stakeholders involved in the PLP DAO System.

Conceptually a DAO must operate autonomously, meaning that it makes decisions based upon data which must be continually revised in order to reflect the reality of the DAO's environment

The PLP DAO is a private system which depends upon mainly private data – customer state (invoiced, unpaid, paid) – service provider state (service completed, pending, not started) -

escrow account balances.

External data is delivered directly to the network via the on-chain oracles.

The PLP DAO Structure

Conceptually the system looks similar to online work exchanges such as Upwork or Freelancer. These are websites which allow people seeking work to apply for tasks to be done, allow those offering work to do so and act as a middleman between the two.

In the DAO the middleman is eliminated.

In addition to the work exchange, the site includes the functions of a bank which enables balances earned to be retained in the system and withdrawn as PLP tokens or other cryptocurrencies at will.

Other banking functions include lending exclusively to entities who have built up reputations with the system over time and eventually dealing in real estate and project financing.

A messaging system is a required part of the network.

Technically DAOs are essentially a bundle of self executing smart contracts, including hashed time-locked contracts, which operate across a system such as the EVM (Ethereum Virtual Machine).

Because all of the functions that the system is required to perform need to be executed across a distributed network, that network needs to be optimized to overcome the slow operating times currently experienced with such systems.

Building the PLP DAO

Our plan is initially to control the system centrally until it is able to operate by itself, as it is better to have a working system which is distributed but not autonomous than the other way around.

All along our development client safety and security is of prime importance, and the final part of the jigsaw will be the autonomous part.

The PLP Cryptocurrency

The PLP cryptocurrency is a very fast and (almost) free transactional currency designed to be used in the PlanetPay platform for work / mutual assistance administration via the PLP DAO.

PLP is based on a DAG (Directed Acyclic Graph), and in effect is a port of the Byteball cryptocurrency which was released in December 2016.

The Byteball cryptocurrency has a number of advanced features such as secure smart contracts, payments via email, conditional payments and on-chain oracles. Despite these advanced features, it is let down by being highly centralized without a (in our opinion) credible strategy for future decentralization and therefore of little interest to the wider cryptocurrency community.

A DAG needs to be able to identify its main chain, which is like a cord running in one direction around which all of the other transactions migrate. In Byteball the main chain is defined by one or more “witnesses” who need to send transactions to the network at regular intervals and whose transactions define the main chain. These witnesses must be trustworthy to only post on that chain, hence they effectively centralize the system.

An additional consensus mechanism therefore needs to be added to the DAG.

The PLP system is therefore being designed to become truly decentralized by combining the current Byteball technology with the PARSEC consensus mechanism which has been developed and released by the developers of the SAFE network.

PARSEC claims to be the world's first completely decentralized, open source, highly asynchronous, Byzantine Fault Tolerant consensus mechanism.

PARSEC solves a well-known problem in decentralized, distributed computer networks: how can individual computers (nodes) in a system reliably communicate events that have taken place on the network to each other where a proportion of the nodes are malicious (Byzantine) and looking to disrupt the system. Or to put it another way: how can a group of computers agree on which transactions have correctly taken place and in which order?

The PlanetPay team, under their Project Manager, Howerd Oakford who is a very experienced FORTH developer, is porting these two technologies into FORTH in order to ensure a very robust, very fast, secure and truly decentralized system.

There is no mining required in the PLP system so it is truly environmentally friendly.

References

1. Anton Churyumov, Byteball
   https://byteball.org/Byteball.pdf

2. Parsec Consensus Mechanism
   https://docs.maidsafe.net/Whitepapers/pdf/PARSEC.pdf