Light Pay Coin

The Future is Here with Contactless Payment Technology

By

The Light Pay Coin Team

August 2018

Version 1.1.0

Table of Contents

Abstract

First and foremost, thank you for taking the time to read the documentation on Light Pay Coin (LPC). Our international team has given lots of effort in building this open-source, cryptocurrency project. We are pleased to provide this overview. Because of the ever-changing landscape of the cryptocurrency industry, this paper is a living document that will be updated from time to time as needed. However, in doing so, we will attempt to maintain the original objectives of this project. LPC is a next-generation, hybrid cryptocurrency based on proof-of-stake (POS) mining and masternodes. This project is a fork of the open-source project of PIVX (which is ultimately a fork of the open-source project, Bitcoin) and leverages the innovations of previous generations of cryptocurrencies.

LPC is distributed within a two-tier, hybrid network for securing the blockchain by (a) confirming transactions, (b) ensuring the privacy of transactions, and (c) facilitating instant transactions. As in other masternode networks, owners of LPC are compensated by the network through a dynamic allocation of rewards based upon LPC owner contributions to the network as confirmation nodes and masternodes. This incentive structure encourages LPC owners to utilize the digital currency for securing the LPC payment network; this is conceivably more profitable than selling the cryptocurrency on the open market. In addition to securing the network, the primary mission of the LPC project is to create an easy-to-use contactless payment system for peer-to-peer, retail, and government transactions worldwide. By creating the next generation of user-friendly wallets, point of sale devices, and automatic teller machines (ATMs), the LPC network will facilitate mass adoption of this innovative financial technology. A long-term goal of this project to position the digital currency of LPC as a medium of exchange, store of value, and a unit of account, ultimately satisfying the defining characteristics of money in this digital age. This process is a natural evolution in Internet technology in which cryptocurrencies will disrupt the financial industry (based on paper fiat currency) in a similar way as the digital transformation of the early 1990s Internet disrupted the traditional paper publishing industry.

Usage of Light Pay Coin

By creating Light Pay Coin (LPC), we made a cryptocurrency that would allow for the safe and secure storage of LPC in a cryptographic, digital wallet. Moreover, we have developed a financial model that would generate income for LPC owners while utilizing LPC itself for the security of the LPC blockchain. We have also inherited, through a selected fork of PIVX, the ability to provide for near instant payments through SwiftTX. This allows LPC owners the ability to transfer LPC within seconds across a global network of masternodes. This makes LPC ideal for worldwide cashless payments through contactless, point of sale devices. To address the issue of previous first-generation cryptocurrencies, the network provides the owner the option to ensure fungibility of LPC through the inherited functionality of PIVX's Zerocoin Protocol.

One of our main goals is to design, develop, and supply user-friendly point of sale devices, ATMs that utilize mobile phone near field communication (NFC) technology, and easy to use wallets. We will build the next generations of automatic teller machines (ATMs) for exchanging from one cryptocurrency to any other cryptocurrency and from one cryptocurrency to any government fiat currency. LPC will be the first cryptocurrency in the point of sale and ATM payment network. This will allow for mass adoption of LPC worldwide for both regular consumers and businesses to pay for goods and services. Thus, LPC will make it easier and safer than traditional payment solutions, which are susceptible to billions of dollars in fraud each year.

Blockchain Technology Overview

For those who are new to the cryptocurrency industry, a blockchain is a way of storing data or a digital record of transactions. This record is immutable and cannot be changed. Digital records are combined into blocks and then these blocks are cryptographically and chronologically linked together in a "chain" using complex mathematical algorithms. Each block is linked with the previous block and contains a complete set of all records that came before it. New blocks are always added to the end of the chain. Computers running on the same network perform the encryption process known as hashing. When all computers in the network complete their calculations and receive the same result, a confirmation is made. Then the block is given a unique digital signature. This block is then added to the digital register, which is updated across all computers in the network. Once this is complete, the block cannot be altered, and it is virtually impossible to fake or change once added to the blockchain. Only new entries or data can be added to subsequent blocks. This makes it impossible to hack the network - as each computer in the network would need to be hacked simultaneously.

With traditional relational database systems, data can be Created, Read, Updated, and Deleted (i.e., CRUD). With respect to a blockchain database, data can only be Created, Read, Appended, and Burned (CRAB). This is what distinguishes traditional databases from blockchain-based databases. Moreover, traditional databases are usually centralized. However, blockchain databases are decentralized and can be distributed on a global scale, which ensures that the network is always available. This technology also allows the potential to store personal data securely as the hashing process is irreversible. If a malicious actor attempts to change the registry, it will not match the registries held by other computers. This builds consensus within the network as the longest chain in the network is the one that is used and results in any altered registries or any other shorter chains in the network being disregarded.

Proof-of-Stake

At the heart of the proof-of-stake algorithm is the storage of all the operations in the LPC wallet with the distributed database. Synchronization of the wallet nodes of LPC running on proof-of-stake is carried out through the peer-to-peer network, P2P. Thanks to proof-of-stake, it is possible to implement cryptocurrency with high security conditions to avoid hacker attacks and fraudulent actions. Moreover, it is more efficient and environmentally friendlier than proof-of-work, which utilizes lots of energy with application specific integrated circuit (ASIC) machines. The system using the proof-of-stake method is based on the principles of decentralized management in the absence of a single controlling authority, which does not allow a malicious actor to know exactly which version of the block is valid. In simple terms, the definition of the principle of the proof-of-stake algorithm can be given as follows: The more LPC possessed in a wallet, the more credibility that wallet node will be given in the permission-less network. Thus, the wallet will likely receive a block reward because of the relative weight that wallet contributes to the protection of the network. The amount of time a wallet participates in protecting the network is also a factor. From a security standpoint, proof-of-stake is not only mining, but the wallet also stakes the LPC amount to ensure against the validity of the transactions placed in blocks. By having a wallet with a large amount of LPC and staking that amount, this decreases the probability that the owner of the wallet is acting in a malicious manner to harm the network. Thus, wallets with high LPC amounts are given a greater preference in confirming transactions than wallets with smaller LPC amounts. An LPC wallet node serves in the first layer of the hybrid cryptocurrency network by confirming transactions on the blockchain, selecting a network masternode for instant transactions, and creating the next block for storing future transactions. A discussion of the second layer LPC network is described next.

Masternodes

Masternodes play an important part of the LPC network. A masternode network is the second layer of the LPC network that donates processing power to confirm transactions instantly utilizing the SwiftTx technology inherited from PIVX. A masternode then receives a reward for the work performed – one reward per block every 60 seconds. These rewards are directly paid to an LPC wallet that is linked to the masternode. Using masternodes also ensures the stability and security of the entire network. These nodes serve a special purpose within the network to mix various transaction amounts to increase fungibility and anonymity of transactions. This is done by the process of obfuscation, which is also inherited through the open source PIVX codebase.

Obfuscation

The LPC network has a focus on the anonymity of payments through the implementation of PIVX's Zerocoin Protocol. This provides a level of privacy by mixing various amounts of LPC within the masternode network. This protocol consumes sent funds through a special algorithm and goes through several iterations, thus providing a high level of anonymity. The implementation of the preliminary algorithm makes the transactions completely unknown to everyone except the sender and the receiver of funds. This makes attacks on the network increasingly difficult. Here is a brief description of how the technology works: A user determines through the wallet the depth of anonymization and the amount of funds s/he wishes to send. The wallet then "shreds" the transaction into predetermined smaller amounts. These smaller amounts are then sent across the masternode network and intermixed with other users' coin transactions also being anonymized, using the master registry for coordination. These coins are not processed but will be mixed in again with another round of transactions, depending on how many mixes the LPC user has selected. The maximum amount of mixes the wallet can generate is eight; however, LPC can be mixed again by following the same procedure. These mixed coins will show up on a separate balance sheet for the anonymous payment to be made.

SwiftTX

LPC uses SwiftTX technology, which allows users to conduct a transaction without waiting for traditional confirmations on the blockchain. The technology uses a network of second-level master logs, which detects transactions marked as “SwiftTX”. These master logs then lock the transaction input and sends a confirmed transaction message to the network. As a result, the transaction takes about 2-5 seconds, while ensuring that no double spending can occur. After sending a confirmation message, the transaction is recorded in the network, as usual. This means that LPC can compete with the ease, convenience, and speed of traditional debit or credit card payments today.

Roadmap

The following is the Roadmap for 2018-2019

Stage 1
▪ Project inception and team formation
▪ Recruiting core team members
▪ Initial whitepaper release
▪ Official website launch
▪ LPC network launch

Stage 2
▪ Private presentation to high network individuals
▪ Shipping company presented LPC workflow
▪ Companies confirmed intention to integrate
▪ Platform code optimized

Stage 3
▪ Marketing campaign
▪ Coin sale
▪ Road show
▪ Customer development

Stage 4
▪ Block explorer launch
▪ Wallet release for Windows, Linux, and iOS
▪ Presale
▪ Masternodes.online listing
▪ Bounty launch
▪ CryptoBridge listing
▪ Coinexchange.io listing July 18
▪ Cryptopia Exchange listing August 18

Stage 5
▪ LPC squad reward for Discord members
▪ Shared masternode services partnerships
▪ Local store partnerships
▪ R&D partnership announcements
▪ Rewards program for investors

Stage 6
▪ Masternode services listing partnership.
▪ Extend market campaign
▪ Website improvement
▪ Launch of non-contact payment options (i.e., point of sale devices)
▪ Launch ATMs
▪ Community development

Specification

Coin Name:	Light Pay Coin
Ticker:	LPC
Algorithm (Proof of Work/Proof of Stake):	Quark
Block Reward:	3 – 26 LPC
Masternode Collateral:	1000 LPC
Masternode Reward:	90% - 65%
Staking (Proof of Stake) Reward:	10% – 35%
Block Time:	60 seconds
Total Supply	21,000,000 LPC
Premine:	90,000 (LPC) (~0.43%)

Profit Diagram

Phase	Block Range	Reward Per Block	% Masternode Reward	% Staking Reward	MN Reward (Coins)
1	20001 - 30000	4	70	30	2.8
2	30001 - 40000	6	65	35	3.9
3	40001 - 50000	8	65.5	34.5	5.24
4	50001 - 60000	10	66	34	6.6
5	60001 - 70000	12	66.5	33.5	7.98
6	70001 - 80000	14	67	33	9.38
7	80001 - 90000	16	67.5	32.5	10.8
8	90001 - 100000	18	68	32	12.24
9	100001 - 110000	20	68.5	31.5	13.7
10	110001 - 120000	22	69	31	15.18
11	120001 - 130000	24	69.5	30.5	16.68
12	130001 - 140000	26	70	30	18.2
13	140001 - 150000	25	70.5	29.5	17.625
14	150001 - 160000	24	71	29	17.04
15	160001 - 170000	23	71.5	28.5	16.445
16	170001 - 180000	22	72	28	15.84
17	180001 - 190000	21	72.5	27.5	15.225
18	190001 - 200000	20	73	27	14.6
19	200001 - 210000	19	73.5	26.5	13.965
20	210001 - 220000	18	74	26	13.32
21	220001 - 230000	17	74.5	25.5	12.665
22	230001 - 240000	16	75	25	12
23	240001 - 250000	15	75.5	24.5	11.325
24	250001 - 260000	14	76	24	10.64
25	260001 - 270000	13	76.5	23.5	9.945
26	270001 - 280000	12	77	23	9.24

Continued

Phase	Block Range	Reward Per Block	% Masternode Reward	% Staking Reward	MN Reward (Coins)
27	280001 - 290000	11	77.5	22.5	8.525
28	290001 - 300000	10.8	78	22	8.424
29	300001 - 310000	10.6	78.5	21.5	8.321
30	310001 - 320000	10.4	79	21	8.216
31	320001 - 330000	10.2	79.5	20.5	8.109
32	330001 - 340000	10	80	20	8
33	340001 - 350000	9.8	80.5	19.5	7.889
34	350001 - 360000	9.6	81	19	7.776
35	360001 - 370000	9.4	81.5	18.5	7.661
36	370001 - 380000	9.2	82	18	7.544
37	380001 - 390000	9	82.5	17.5	7.425
38	390001 - 400000	8.8	83	17	7.304
39	400001 - 410000	8.6	83.5	16.5	7.181
40	410001 - 420000	8.4	84	16	7.056
41	420001 - 430000	8.2	84.5	15.5	6.929
42	430001 - 440000	8	85	15	6.8
43	440001 - 450000	7.8	85.5	14.5	6.669
44	450001 - 460000	7.6	86	14	6.536
45	460001 - 470000	7.4	86.5	13.5	6.401
46	470001 - 480000	7.2	87	13	6.264
47	480001 - 490000	7	87.5	12.5	6.125
48	490001 - 500000	6.8	88	12	5.984
49	500001 - 510000	6.6	88.5	11.5	5.841
50	510001 - 520000	6.4	89	11	5.696
51	520001 - 530000	6.2	89.5	10.5	5.549
52	530001 - 2100000	6	90	10	5.4

Conclusion

The LPC Team prepared this document to provide a brief overview about cryptocurrencies in general and LPC in particular. We discussed our primary goal of creating the next generation of user-friendly wallets, point of sale devices, and contactless ATM machines for worldwide use. From a technology perspective, evidence supports the view that proof-of-stake/masternode technology is not only secure, but also environmentally friendly and more efficient that proof-of-work consensus models. LPC is based on next-generation technology such as SwiftTX, Zerocoin Protocol, proof-of-stake and second-layer masternodes inherited from proven, open-source technologies. The contribution of LPC to the cryptocurrency revolution is to usher in user-friendly devices to facilitate mass adoption. We will do this through a combination of first-of-a-kind partnerships and unique business models.

A long-term goal of this project to position the digital currency of LPC as a medium of exchange, store of value, and a unit of account, ultimately satisfying the defining characteristics of money in this digital age. This process is a natural evolution in Internet technology in which cryptocurrencies will disrupt the financial industry (based on paper fiat currency) in a similar way as the digital transformation of the early 1990s Internet disrupted the traditional paper publishing industry.

Appendix: R&D Partnership Overview with the University of Central Florida

Light Pay Coin: Research, Development, & Commercialization Project

Background

Light Pay Coin (LPC) is a next-generation, hybrid cryptocurrency utilizing a two-tier, open network involving proof-of-stake (POS) consensus and masternodes for specialized network functions (instant and/or private transactions). LPC is designed to be a medium of exchange, a store of value, and a unit of account within an emerging digital economy. LPC will use near field communication (NFC) payment technology to transfer funds via mobile devices to point of sale terminals, other phones, and ATMs. LPC's goal is to become one of the fastest and most convenient modes of digital payment in the world, revolutionizing the financial services industry. A person's smartphone can replace one or more bank cards and perform the functions of both a general communication device and payment platform for personal, business, or government use.

LPC in partnership with the University of Central Florida will assist in conducting research and development activities to support the commercialization of the blockchain-based payment platform. This project will include several phases involving Industrial & Organizational Psychology, Human Factors Psychology, Computer Science, and Engineering. Both students and professors will be involved in the development of this next generation platform for digital assets. Digital currency is the first use case, followed by other assets and credentials (e.g., transcripts, micro-credentials, certificates, and degrees).

Goal

The ultimate goal is to build and commercialize user friendly (a) cryptocurrency wallets, (b) point of sale devices, and (c) contactless ATM machines. This will allow for buying and selling LPC and other cryptographically secure digital assets using mobile devices with near field communication (NFC) technology.

General Approach

There are several phases of research, development, and commercialization activities that will be implemented through a series of task orders. Time allocation and human resource needs are determined on a project by project basis, commencing in the Fall of 2018. Separate task orders will be created involving the design, development, and integration of user interfaces (UI). Task orders will be associated with the following:

(a) Software UI design of (1) wallets, (2) point of sale devices, and (3) contactless ATMs

(b) Software UI development of (1) wallets (2) point of sale devices, and (3) contactless ATMs

(c) Acceptance testing of the UI and penetration testing of entire software application.

(d) Hardware UI design of point of sale devices and contactless ATMs

(e) Hardware UI development of point of sale devices and contactless ATM

(f) Hardware and software integration and prototyping

(g) Acceptance testing of prototype

(h) Pilot testing on Florida Lambda Rail network

(i) Pilot test (beta) with customers for personal, business, and government use