BlocPal International Inc.

BLOCKCHAIN WHITEPAPER

AUTHORS: RANDY DU, NICOLAOS MELLIOS

MAY 1, 2019, VERSION 1.0.2

Table of Contents

Abstract 2

Introduction 2

Global Factors 2

Opportunity for Blockchain 3

BlocPal Blockchain 4

Specifications 5

Proof-of-Work / Proof-of-Stake Hybrid Consensus Algorithm 5

The “Payload” 6

Know-Your-Customer (KYC) 8

Dynamic Maximum Block Size 9

Blockchain API 9

Source Code Release 11

Blockchain Pool Mining 11

BlocPal Wallet and API 12

Security Token and Path to Full Decentralization 13

Future Enhancements 14

Abstract

A peer-to-peer blockchain design extending the vision of Satoshi Nakamoto's Bitcoin[i] blockchain with the following key enhancements:

1. Proof-of-stake / proof-of-work hybrid consensus algorithm (utilizing Peer Coin's design)

2. X16R proof-of-work mining algorithm

3. A new data member has been added to the block, the "payload," which offers the ability to digitally sign any asset ("tokenize') and trade this asset on the blockchain

4. Know-your-customer (KYC) parameters managing trade permissions of blockchain addresses, necessary for compliance with regulating authorities

5. Dynamic maximum block size setting allowing for growth of block size based on transaction volume

Source Code:

BlocPal's source code is a derivative of PeerCoin[ii] 0.8.6 (2018-03-10) with implementation of the significant enhancements outlined above.

Introduction

Global Factors

- Advances in technology are dramatically changing consumer behaviour and expectations within the financial world.

- Customer satisfaction is measured in a matter of seconds. There is an increasing demand for instant results, security and uber convenience which is evolving how people expect to interact within the global financial ecosystem.

- Customers have much more choice now available to them. Customers are no longer limited to shopping at stores within their neighborhood. Merchants must now work harder to keep their customers, consequently making loyalty and retention programs even more important today.

- The processing power of a 1980's supercomputer is now available to anyone in the world via any smartphone.[iii]

- The number of smartphone users is forecast to grow from 2.1 billion in 2016 to around 2.5 billion in 2019 (Source: Statista 2019).[iv]

- The demand for instant gratification has made businesses rethink the way they offer their services. For example, mobile phone apps have changed the way a taxi may connect with its customer or how a restaurant may book a reservation or how a movie studio can reach its audience. Similarly, digitalization presents new opportunities for FinTech, providing faster, more convenient services to users and changing the way people expect to receive financial services.

- Millennial consumers avoid face-to-face interactions at their local bank and prefer the speed and convenience of digital services.

- Biased news and misleading information that is difficult to filter is made widely available to us today via the internet and media creating general distrust in what we read and hear from centralized sources.

- Trust in government is generally declining according to an OECD report published on March 27, 2017, with reference to key factors including competence, values, corruption, fairness, fiscal policy and openness.[v]

Opportunity for Blockchain

- The invention and ongoing progression of blockchain based solutions creates opportunities to provide innovative financial services that institutions today are unable to offer. Emerging blockchain solutions offer an array of opportunities to enhance the way not only traditional fiat currencies are used and looked at, but the way global commerce, technology and the world at large function. From transparency to privacy, from inclusion to security, from control to convenience, blockchain technologies are beginning to disrupt the world we know today.

- The peer-to-peer, transparent and secure nature of digital currencies and blockchain technologies offer us an opportunity to create balance with today's centralized financial systems.

- Digital currencies like Bitcoin and Ethereum have evolved offering new alternatives to traditional currencies. However, transaction costs and required confirmation times for these digital currencies have risen making micro-payments between consumers and merchants impractical.

- With the increasing interest and demand for the convenience of cryptocurrency, there is a rapidly developing market beginning to seek out ways to spend digital currencies. There is an ever-growing need for a solution that enables users to "spend" and not just "invest" with cryptocurrencies.

- Regulation of blockchain solutions and digital currencies is required for global acceptance and widespread adoption.

- Smaller more nimble companies with experience in advanced web and app development are now able to compete with larger financial institutions, leveraging innovations in technology to offer better, faster and more convenient digital services to consumers. As a result, advanced financial services can be more readily available to everyone, including people with limited access to banking services.

- Enterprise companies have new opportunities to implement custom financial solutions for their businesses in order to increase profits. This can be achieved by improving customer loyalty programs, saving on transaction fees, keeping more transaction revenue within the enterprise network and further monetizing their customer/user base.

BlocPal Blockchain

The BlocPal blockchain provides the ability for anyone to build applications on top of it utilizing any of the blockchain's following core features:

1. Ability to digitally sign any asset ("tokenize') and trade this asset on the blockchain, including but not limited to real world assets, currencies, securities, commodities, title ownership, physical goods, supply chain materials, virtual goods, loans, credits and loyalty rewards.

2. Full compliance with regulating authorities for any transaction

3. Transparency and security of transactions

4. Scalability and low cost of transactions

5. Instant authorization of transactions based on the application's design

The BlocPal blockchain was built on top of Satoshi Nakamoto's Bitcoin blockchain for the following reasons:

- Bitcoin has been operating since 2009, making it the most tested blockchain around, as well as the most stable, most used and most reliable.

- Bitcoin has a strong following. Along with the supporters Bitcoin has gathered over the years, the platform also has large miner support and is currently one of the most favored blockchains to mine.

- Bitcoin is one of the simplest blockchains to understand and most developers are familiar and comfortable with it.

- Balance of security vs. features. Increased functionality provided by new blockchains also comes at the cost of introducing more risk in security. BlocPal carefully selected only the key features required to upgrade on top of Bitcoin mitigating risk of introducing new vulnerabilities.

Specifications

- Max Supply of Coins: 1,111,111,111 BPX
- Estimated Blocks Per Year: 200,000
- Block Rewards: 256 BPX, halves every 1,000,000 blocks until year 2089
- Target Block Time: 150 seconds (2.5 minutes)
- Maximum Block Size: unlimited, adjusted dynamically according to blockchain workload
- Consensus: POW/POS Hybrid:

Blocks	POW	POS
1~400,000	80%	20%
400,000~600,000	70%	30%
600,000~800,000	60%	40%
800,000~1,000,000	50%	50%
1,000,000 and later	40%	60%

Proof-of-Work / Proof-of-Stake Hybrid Consensus Algorithm

Requirements:

Provide mining options with reduced energy consumption while maintaining decentralization and equal opportunity for any potential contributors to the mining pool. Further reduce and protect from vulnerability of 51% attack.[vi]

Implementation:

Proof-of-work (POW)):

The mining algorithm is based on X16R. X16R was implemented in order to reduce the risk of domination by existing large mining pools and ASIC mining hardware.

Mining reward can be spent after 24 confirmations (~ 1 hour)

Proof-of-stake (POS)):

Minimum stake age (minimum coin age) is 10 days;

Maximum stake age (stake age of full weight) is 100 days;

The POS reward is the same as POW, and not proportional to coin age. The value of coin age decides the possibility of minting a new POS block, but has nothing to do with the block reward.

The “Payload”

Requirements:

Enable applications using the blockchain to digitally sign (“tokenize”) any currency or asset for trade.

Tokens may represent currencies or any real-world assets (physical or digital) that can have value including but not limited to securities, commodities, title ownership, physical goods, supply chain materials, virtual goods, loans and credits.

Transactions with these tokens (excluding the BlocPal BPX security token) should maintain a layer of privacy and confidentiality for users to help shield them from potential hackers.[vii]

Implementation:

The BlocPal blockchain is optimized for distributed information storage. A new data member (the ***“payload”***) is added to a transaction to persist generic information from any type of application.

The BlocPal blockchain is public and supports multiple applications running on it. The payloads from different applications can co-exist peacefully. For example, app-A cannot create a fake payload for app-B.

Payload Hint:

The hint is an app-specific magic value. All applications running on the BlocPal blockchain are assigned a unique integer value so that the app can skip parsing a payload of another app.

Payload Creator:

This definition is for whoever creates the payload. A creator is also known as the payload *provider*. Usually it is the application running on the BlocPal blockchain that creates the payload.

Payload Owner:

This definition is for the BlocPal accounts that can provide the private key to access the payload data. The payload owner is also known as the payload *consumer* who is the target audience for the payload information.

> For *public* payload, there is no payload owner, everyone can access a public payload on blockchain. For *private* payload, only the payload owner can decode the payload data with the corresponding private keys.

The basic payload data members are:

1. Hint: Unique integer id for payload creator
   It is the system designated app-id. For example, BlocPal-Wallet App has a hint of "1".
2. Sub-Hint: hint of payload content
   It is an app-specific value to tag what kinds of information stored in the payload.
3. Creator Public Key [Optional]
   The public key of payload creator. If it is not specified, then the creator is assumed to be the hosting transaction's output receiver's public key (must be p2pk address).
4. Creator Signature
   The creator's digital signature, signing the hash of payload raw-data and the transaction's time stamp. It ensures the integrity of the payload and prohibit the payload from being cloned to other blocks by attackers.
5. Raw-Data
   The stored information of payload. It can be encrypted bytes of private payload which can only be decrypted by payload owner.

Payload Size:

The payload is stored in a transaction mined in a blockchain, so it must fit in one block. The BlocPal has a dynamic maximum block size to help with accommodating big payloads, however, it is recommended for the app (payload creator) to optimize the payload size for best performance. For example, the app can split big data chunks into small pieces or upload huge files to third party data storage system (such as IPFS[viii]) and save the receipt as payload.

Know-Your-Customer (KYC)

Requirements:

The blockchain must be able to support trade in full compliance with regulating authorities worldwide. Know-your-customer (KYC) identification and verification processes are critical for adhering to Security, Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) regulations. Addresses on the blockchain can be restricted or limited in trade based on user verification and compliance requirements.

Implementation:

Each BlocPal address is associated with a specified KYC level, which defines the transaction allowed.

LEVEL_UNKNOWN (0): /// send to CERTIFIED & BLACKHOLE, the ***default*** one

LEVEL_KNOWN (1): /// send to KNOWN, CERTIFIED & BLACKHOLE

LEVEL_CERTIFIED (2): /// send / receive fund to / from anyone.

LEVEL_BLACKHOLE (3): /// receive fund from anyone, cannot send fund to anyone (safe for solo-mining)

	From Unknown	From Known	From Certified	From Black-hole
To Unknown	N	N	Y	N
To Known	N	Y	Y	N
To Certified	Y	Y	Y	N
To Black-hole	Y	Y	Y	N

The Black-hole level is useful for long term balance holding, it can accept incoming funds but cannot send funds out to any other accounts. Even if the account's private key is hacked, the hacker cannot steal its balance because the account is locked.

Dynamic Maximum Block Size

Requirements:

As transactions on the blockchain grow, so must the size of blocks in order to maintain a fast and healthy blockchain. Block size should grow based on recent transaction volume in order to maintain speeds for transactions and low transaction costs.

Implementation:

The dynamic maximum block size is designed to make sure the BlocPal blockchain can react quickly with the current transaction volumes and scale with growth. The BlocPal blockchain checks the block average usage of the last 580 blocks (~ 1 day) and doubles the new maximum block size if the block usage is more than 61.8% or reduces the block size by half if the block usage is below 5%.

The initial maximum block size is 1M byte.

Note: This feature is critical for enabling applications to eventually scale to handling 1000s of transactions per second.

Blockchain API

An extensive application programming interface (API) has been developed to support the development of applications accessing the features of the BlocPal blockchain. The following list of methods have been made public with more API methods to be made publicly available in the future.

API Documentation[ix]

The block explorer provides an API allowing users and/or applications to retrieve information from the network without the need for a local wallet.

API Calls

Return data from coind

- **getdifficulty**
  Returns the current difficulty.
  explorer.blocpal.com:8080/api/getdifficulty

- getconnectioncount
  Returns the number of connections the block explorer has to other nodes.
  explorer.blocpal.com:8080/api/getconnectioncount

- getblockcount
  Returns the current block index.
  explorer.blocpal.com:8080/api/getblockcount

- getblockhash [index]
  Returns the hash of the block at ; index 0 is the genesis block.
  explorer.blocpal.com:8080/api/getblockhash?index=16918

- getblock [hash]
  Returns information about the block with the given hash.
  explorer.blocpal.com:8080/api/getblock?hash=13138742cfc8fe715a33bf5337ffb0a494a04dd8fb44d617717621c349cb721c

- getrawtransaction [txid] [decrypt]
  Returns raw transaction representation for given transaction id. decrypt can be set to 0(false) or 1(true).
  explorer.blocpal.com:8080/api/getrawtransaction?txid=98d99264e2ed316e960b1c8baf3f79c8adda5888cda92c3db868aaa687ed4b57&decrypt=0
  explorer.blocpal.com:8080/api/getrawtransaction?txid=98d99264e2ed316e960b1c8baf3f79c8adda5888cda92c3db868aaa687ed4b57&decrypt=1

- getnetworkhashps
  Returns the current network hashrate. (hash/s)
  explorer.blocpal.com:8080/api/getnetworkhashps

Extended API

Return data from local indexes

- getmoneysupply
  Returns current money supply
  explorer.blocpal.com:8080/ext/getmoneysupply

- getdistribution
  Returns wealth distribution stats
  explorer.blocpal.com:8080/ext/getdistribution

- getaddress (/ext/getaddress/hash)
  Returns information for given address
  explorer.blocpal.com:8080/ext/getaddress/BBejVGuNvKcZjwFPRji6gn1yu15e68hKZy
- getbalance (/ext/getbalance/hash)
  Returns current balance of given address
  explorer.blocpal.com:8080/ext/getbalance/BBejVGuNvKcZjwFPRji6gn1yu15e68hKZy
- getlasttxs (/ext/getlasttxs/count/min)
  Returns last [count] transactions greater than [min]
  Note: returned values are in satoshis
  explorer.blocpal.com:8080/ext/getlasttxs/10/100

Linking (GET)

Linking to the block explorer

- transaction (/tx/txid)
  explorer.blocpal.com:8080/tx/98d99264e2ed316e960b1c8baf3f79c8adda5888cda92c3db868aaa687ed4b57
- block (/block/hash)
  explorer.blocpal.com:8080/block/13138742cfc8fe715a33bf5337ffb0a494a04dd8fb44d617717621c349cb721c
- address (/address/hash)
  explorer.blocpal.com:8080/address/BBejVGuNvKcZjwFPRji6gn1yu15e68hKZy
- qrcode (/qr/hash)
  explorer.blocpal.com:8080/qr/BBejVGuNvKcZjwFPRji6gn1yu15e68hKZy

Source Code Release

The first release of the open source code for the BlocPal blockchain is scheduled to be published on GitHub in Q2 2019. The blockchain has undergone significant testing since being launched in September 2018.

Blockchain Pool Mining

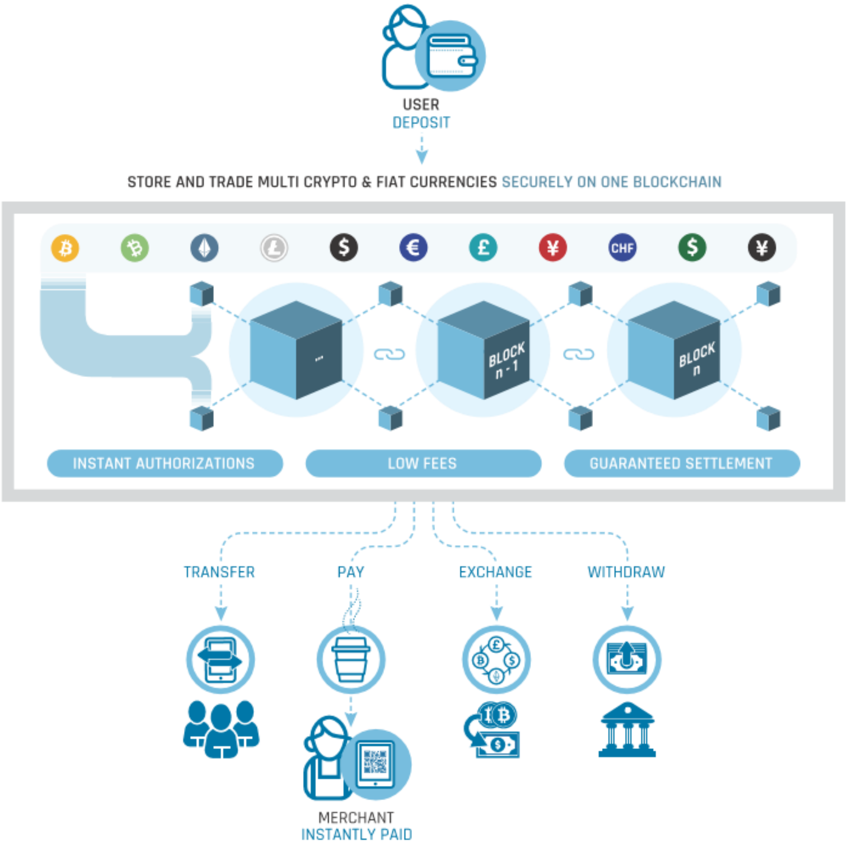
BlocPal's official mining pool is open to everyone. Please visit https://pool.blocpal.com/ to learn more about mining the BlocPal blockchain. When the Security Token Offering (STO) Prospectus for the BPX token is completed, mining will also be open outside of the pool. To learn more about the plans for the Security Token, please go to the section below titled "Security Token and Path to Full Decentralization."

BlocPal Wallet and API

BlocPal International Inc. has developed wallet and merchant terminal applications on top of the BlocPal blockchain to enable instant authorization and guaranteed settlement of transactions for multiple currencies (fiat and crypto) at a low cost and no risk. The BlocPal wallet currently supports USD, CAD, EUR, BTC, ETH, LTC, BCH and BSV with more currencies and other digital tokens representing assets and loyalty rewards to be released. The application has been integrated with global payment networks, exchanges and traditional financial systems (like ACH, EFT and SEPA) and complies with security and money service business regulations.

Published API methods for the BlocPal wallet and terminal application can be found here - https://services.blocpal.com/apidocs/#/merchantapimethods/intro.

Diagram: The BlocPal Wallet - an application using the BlocPal blockchain to digitally sign currencies (fiat and crypto) and other assets enabled for trade with instant authorization and guaranteed settlement.



Security Token and Path to Full Decentralization

The BlocPal Token (BPX) has been designed to be a security token and is subject to security regulations. According to the Swiss regulatory body FINMA, tokens can have three functions: Payment Tokens, Utility Tokens, or Asset Tokens (also referred to as "Security Tokens"). As per FINMA's definition, asset tokens represent assets such as participations in real physical underlyings, companies, or earnings streams, or an entitlement to dividends or interest payments. In terms of their economic function, the tokens are analogous to equities, bonds or derivatives.[x]

In addition to the benefits of the tokens appreciating in value based on increased usage and trade on the blockchain, BPX Token holders are entitled to receive royalty payments of 33% net profit generated from the business activities of BlocPal International Inc. (the "Company"). The remaining 67% is to be retained by the Company to be directed for use by the Company. BPX Token holders have the right to stake the tokens for proof-of-stake mining but do not have the right to vote or control the business of the Company.

As BlocPal International Inc. works to complete a Security Token Offering (STO) Prospectus, current holders of the BPX Token must qualify under accredited investor exemption. Until the STO Prospectus is complete and the BPX token is trading on one or more regulated security token exchanges, the BPX token can only be traded under accredited investor exemption. The STO Prospectus allowing for trading of the token by non-accredited investors is critical for decentralization of the blockchain.

The Company will also use the BPX Tokens as payment currency for blockchain miners, certain advisors and consultants, including engineers, advisory board members and such other service providers as the Company may consider appropriate and compliant.

The Company has been advised that both the Canadian Securities Exchange (CSE) and TSX Venture Exchange (TSXV) are seeking approval of a regulated exchange and/or transfer agency for security tokens. There are many exchanges in Canada, USA, Europe, Korea and Singapore that have expressed intention of becoming a regulated security token exchange and it is likely that there will be at least one or two regulated security token exchanges operational in 2019. Once such an exchange has been approved and operational, the Company intends to apply for the listing of its BPX Tokens. Listing will be subject to the Company fulfilling all the listing requirements of the exchange.

In addition to working closely with regulated security token exchanges to empower trading of the BPX tokens, the Company will begin to work with 3rd party firms who provide KYC compliance services, like iComply (https://icomplyico.com/) and Token IQ (https://tokeniq.io/). These types of independent compliance firms will be designated to provide additional paths for users of the BlocPal blockchain to obtain the required KYC compliance status in order to trade on the blockchain. Independent designated compliance firms providing KYC services is also an important step towards achieving full decentralization.

Future Enhancements

BlocPal International Inc. will continue to add new features to the blockchain based on user demands while prioritizing security of the blockchain. The Payload function already provides much flexibility and creates many opportunities for the blockchain to be used by all kinds of applications. The Company is in discussions with potential partners to enable the BlocPal blockchain to support applications for many verticals, including but not limited to the following.

- Digital rights management
- Asset ownership verification, tracking, attributes
- Commodities trading, secondary markets
- Supply chain management
- Loyalty rewards / token programs

This BlocPal blockchain whitepaper version 1.0.1 is a living document which will evolve through successive updates from time to time. Please always refer to the latest version found at www.blocpal.com/investor/.

[i] Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto, www.Bitcoin.org

[ii] PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, Sunny King, Scott Nadal, www.peerocin.net

[iii] Experts-Exchange, https://pages.experts-exchange.com/processing-power-compared

[iv] Statista 2019, www.statista.com

[v] Trust and Public Policy, How Better Governance Can Help Rebuild Public Trust, Published on March 27, 2017, http://www.oecd.org/gov/trust-and-public-policy-9789264268920-en.htm

[vi] Proof of Work, Proof of Stake and the Consensus Debate, https://cointelegraph.com/news/proof-of-work-proof-of-stake-and-the-consensus-debate

[vii] Six Tools Used by Hackers to Steal Cryptocurrency: How to Protect Wallets, https://cointelegraph.com/news/six-tools-used-by-hackers-to-steal-cryptocurrency-how-to-protect-wallets

[viii] InterPlanetary File System, https://ipfs.io/

[ix] BlocPal blockchain API, http://explorer.blocpal.com/info

[x] FINMA publishes ICO guidelines, February 16, 2018, https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/