



AUTHORS: RANDY DU, NICOLAOS MELLIOS

UPDATED JUNE 1, 2021, VERSION 1.50*

Important Note:

The information in this white paper has changed since last published. There is no obligation or undertaking to update or revise, or to publicly announce any update or revision to, any of the information contained herein. This information should not be relied upon for any purpose. This white paper contains forward-looking statements that are not guarantees of future performance. Actual results and activities since the date of the white paper have differed materially in certain cases. Where actual results or activities have been consistent, they are not intended to, and may not, be predictive of results, activities, or developments following the date of viewing. This white paper is not an offer to sell, and is not soliciting an offer to buy, the Blocpal Tokens referenced herein. Nothing in this white paper shall be deemed to constitute a prospectus of any sort or a solicitation for investment. The information in this white paper does not constitute a recommendation by any person to purchase Blocpal Tokens or any other cryptographic token or currency.

*Contributing editor: Neil Kothari



Table of Contents

Abstract	3
Introduction	4
BlocPal Blockchain.....	7
Key Features of the BlocPal Token	10
Appendix A – Technical Specifications.....	13
Specifications	13
Proof-of-Work / Proof-of-Stake Hybrid Consensus Algorithm.....	13
The “Payload”	14
Know-Your-Customer (KYC).....	15
Dynamic Maximum Block Size	16
Blockchain API	16
Source Code Release	19
Blockchain Pool Mining	19



Abstract¹

BlocPal International Inc. (“**BlocPal**” or the “**Company**”) has implemented a permissioned blockchain which is a derivative of PeerCoin 0.8.6 (2018-03-10) open-source code with significant enhancements (the “**BlocPal Blockchain**”). The BlocPal Blockchain facilitates the creation of transactions using distributed ledger technology (“**DLT**”). PeerCoin itself is based on the source code which powers Satoshi Nakamoto’s Bitcoin blockchain. In addition to features customarily found in the Bitcoin blockchain, the BlocPal Blockchain is intended to provide:

1. proof-of-work and proof-of-stake hybrid consensus algorithms which facilitate the recording of transactions;
2. a data member (or “payload”) which has been added to each block to offer the ability to tokenize assets with unique hash-keys that are tracked through every transaction on the BlocPal Blockchain;
3. know-your-customer (KYC) parameters managing trade permissions of blockchain addresses, necessary for compliance with regulatory requirements and which is enabled through the use of application program interface keys (“API Keys”) held by BlocPal and which can be shared with other parties as the BlocPal Blockchain becomes fully distributed; and
4. a dynamic block size setting which allows for the growth of a block size based on transaction volume and enables faster processing times.

BlocPal tokens (“**BlocPal Tokens**”) can be thought of as ledger entries on the BlocPal Blockchain which grant certain rights to holders of these BlocPal Tokens. These ledger entries exist in duplicative form across every copy of the BlocPal Blockchain held on local computers (each a “node”) which interact with BlocPal Blockchain software code through the Internet. Transactions occur on the BlocPal Blockchain in generally the same manner as Bitcoin transactions to enable the transfer of information. BlocPal’s proprietary merchant interface and wallets (“**BlocPal Applications**”) are designed to maximize the usefulness of information communicated and stored on the BlocPal Blockchain, including by reading, from public addresses, the number of BlocPal Tokens and other information held in these addresses. Holders of the BlocPal Token have the right to participate in the positive cash-flows of BlocPal (as determined in accordance with a token rights agreement). BlocPal Tokens are required to communicate transaction information on the BlocPal Blockchain, since transaction data (or payloads) *are included* in the same transaction script which moves BlocPal Tokens from one location (or public address) to another. In addition, BlocPal Tokens are “consumed” each time a transaction occurs in accordance with the software protocol and BlocPal Tokens must be provided to reward BlocPal’s service providers who create (or “mine”) blocks of transaction data to form an immutable book of record on the BlocPal Blockchain.

BlocPal is building viable use cases for the BlocPal Blockchain through its financial technology (FinTech) applications and establishing, through the security (i.e. financial asset) and

¹ This White-Paper is intended to provide an overview of the key features of the BlocPal Blockchain and some technical specifications (located in Appendix A of this White-Paper) for review by the “mining community”. BlocPal assumes that the reader has some knowledge of blockchain technology and this whitepaper is not intended to be a comprehensive overview of all of the functionality or risks associated with the BlocPal Blockchain.



utility features of its BlocPal Token, the infrastructure to eventually create a decentralized blockchain. BlocPal's vision is to be at the forefront of integrating and aggregating financial technology, merchant applications and traditional payment processing systems and using the BlocPal Blockchain to manage the vast amount of data and processing required for such purpose. As the popularity and usefulness of the BlocPal Blockchain grows, BlocPal believes that enterprise users will be encouraged to develop their own applications for use with the BlocPal Blockchain, and in turn, create demand for BlocPal's creative input and the BlocPal Tokens which underpin the BlocPal Blockchain.

Current holders of BlocPal Tokens must qualify under the accredited investor exemption or otherwise be eligible to hold BlocPal Tokens under applicable securities laws. Until a prospectus or registration statement is filed and approved in connection with BlocPal Tokens, trading of BlocPal Tokens is not permitted. Such filings are key for decentralization of the BlocPal Blockchain.

Introduction

The invention and ongoing progression of blockchain based solutions creates opportunities to provide innovative financial services. Emerging blockchain solutions offer an array of opportunities to enhance the way not only traditional fiat currencies are used, but the way global commerce and end-user technology functions. From transparency to privacy, from inclusion to security, from control to convenience, blockchain technologies are disrupting the world we know today. BlocPal Applications are intended to leverage the significant opportunity created by blockchain technology and to work effectively with the BlocPal Blockchain to offer an enhanced user experience and transactional functionality to bridge the "last-mile" of e-commerce and merchant solutions with the complex backbone of payment infrastructures and encrypted asset repositories (or crypto assets).

In particular, while digital currencies like Bitcoin and Ethereum have evolved offering new alternatives to traditional currencies, the 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 more effectively spend digital currencies to acquire goods and services. There is an ever-growing need for a solution that enables users to "spend" and not just "invest" with cryptocurrencies.

As the number of smartphone users has grown to around 3.3 billion users in 2021 (Source: Statista 2021), our target market of enterprise customers are increasingly embracing this evolution in technology to provide an enhanced user experience and to offer services which more fully integrate with payment systems. Similarly, digitization and blockchain present new opportunities to further enhance FinTech solutions, to provide faster, more convenient services to users and change the way people expect to receive financial services. BlocPal Applications, working together with the BlocPal Blockchain, are in a position to leverage the unification of evolving financial services platforms and enterprise strategy.

BlocPal's vision is to permit enterprises to have new opportunities to build stronger "digital relationships" with their customers via their smartphone. Many companies have built mobile apps to act as a digital storefront for their business with the goal of increasing profit. These mobile app storefronts provide many advantages over traditional websites, including:

- o improved customer loyalty and retention
- o easy digital payments, ordering and convenience for customers



- o reduced transaction fees
- o more payment options for customers
- o new revenue streams via financial services offered to customers
- o delivering relevant FinTech services to underserved or target markets

BlocPal Applications use standard programming language to interact with the BlocPal Blockchain and information which is stored within each transaction on the chain. Payload data recorded in transactions may also be stored off of the BlocPal Blockchain in permissioned databases – and referenced in each transaction using “receipts” represented by encrypted hash keys. This permits the BlocPal Blockchain to manage significantly greater data than without this attribute and is a critical feature of the BlocPal Blockchain which improves the usefulness of BlocPal Applications. In addition, the BlocPal Blockchain is intended to provide an innovative backbone to the payment processing and other activities of BlocPal. Utilizing blockchain technology and incentivizing the use of BlocPal Tokens by paying holders of BlocPal Tokens a percentage of the Company’s cash flows is intended to create the potential for “network effects” and encourage the creation of an infrastructure for global payment processing utilizing the BlocPal Blockchain.

BlocPal Applications are generally comprised of BlocPal’s own wallet (the “**BlocPal Wallet**”) and a merchant terminal application which integrates with the BlocPal Blockchain. BlocPal Applications are also integrated with global payment networks as necessary to enable the functionality of these applications. BlocPal is continuing to review the regulatory parameters and requirements to provide the intended functionality to transact in crypto currencies and contracts over the BlocPal Wallet. For example, further registrations with securities regulatory authorities and integration with a qualified custodian that holds the private keys for cryptocurrencies may be required to provide the intended functionality for BlocPal Applications and the BlocPal Blockchain.

Tokenization

BlocPal Applications use the information stored in each transaction / public address on the BlocPal BlockChain to record the entitlement of each holder to an underlying tokenized asset (including the BlocPal Token itself). This entitlement is represented by information held in each transaction payload which embeds significant information relating to:

- o The amount of the underlying tokenized asset owned by the holder of the asset;
- o The nature of the tokenized asset and its properties;

In order for a party to transact and modify information stored in a payload, a transaction would need to occur on the BlocPal Blockchain, which communicates information from one public address to another. The user who initiates a transaction (which could be an enterprise user or its customer) would require a “private key” to the address which stores the underlying information. The public address which comprises the destination of the transaction would also be associated with a private key. At the moment, BlocPal uses the BlocPal Blockchain to both send and retrieve transaction information and holds relevant private keys, including API Keys for this purpose. It is anticipated that BlocPal’s enterprise customers and merchants will eventually be able to create their own applications for use on the BlocPal BlockChain. In order to do so, they will need to acquire BlocPal Tokens, which are necessary to fund the creation of blocks and to confirm transactions on the BlocPal Blockchain. BlocPal believes that permitting other merchants to use the platform and develop their own wallet interfaces will create “network effects”. At the moment, BlocPal provides this fully integrated service, including the development of wallets and related customer facing applications. In



addition, BlocPal funds transactions by remitting BlocPal Tokens to the “miners” who help confirm transactions. A complete discussion of the number and rights associated with each BlocPal Token is provided later in this White-Paper.

Transaction Processing

The BlocPal Blockchain allows for dynamic maximum block sizes to help with accommodating larger volume of transactions. Dynamic block-sizing is generally determined based on the average number of transactions that have occurred over the BlocPal Blockchain over a preceding time-period as specified in the software code. The use of dynamic block-sizing can also speed up transaction processing as well as maintain low transaction fees which are key features of the BlocPal Blockchain relative to the Bitcoin blockchain. Payload sizes are typically required to be optimized for best performance. Importantly, large files can be transferred to third-party data storage systems and the receipt or file location stored in the payload for retrieval. However, a special enterprise application (including a BlocPal Application) is required to integrate and access this information.

Private Keys

Only the owner of a “private key” can amend information on the BlocPal Blockchain or any information which is stored and referenced in a transaction payload “off-chain”. Information derived from private keys must correspond with public keys (which in each case are represented by a unique “hash”). Miners have access to algorithms which are used to check to ensure that the information produced by a private key (or signatures) and the public key on record match. Importantly, signatures cannot be reverse engineered to create the private key given the nature of the algorithms being used. Ultimately, these features are critical to generating and authenticating transactions on the BlocPal Blockchain. Recipients must possess the correct private key to transfer a BlocPal Token and any related payload script which corresponds to a public address. When BlocPal Tokens are sent to a public address which has no corresponding private key, they are lost (or burned). Since BlocPal runs a “permissioned” blockchain, it presently has the ability, through API Keys, to grant permissions to public addresses to transact on the BlocPal Blockchain by associating them with special codes as discussed in the technical specifications section of this White-Paper. Eventually, these API Keys can be shared with enterprise customers who wish to build their own applications for use on the BlocPal Blockchain and in order for it to become fully distributed.

BlocPal does not integrate the BlocPal Blockchain with all of its BlocPal Applications. The reason is that certain enterprise relationships require significant transaction processing speed and data management. At the moment, the average amount of time to confirm a block on the BlocPal blockchain is about 2.5 to 5 minutes. This contrasts with the time required on the Bitcoin Blockchain (which is 10 minutes). Such processing speeds are expected to improve as the Company introduces “proof-of-stake” mining, as discussed below. In addition, the BlocPal Blockchain is not used in circumstances where “tokenization” of blockchain assets (including cryptocurrency) is not required to provide the full suite of BlocPal’s services. However, the BlocPal Token remains eligible to receive distributions from cash flows generated by the Company through its wider enterprise solutions. In that sense, a single BlocPal Token has potentially wide sources of economic value derived from cash flows as well as the utility of the BlocPal Token to fund the mining of blocks and confirmation of transactions. BlocPal may, in the future, separate the rights associated with its BlocPal Tokens into one or more tokens, particularly if that facilitates regulatory compliance. Any such separation would not be intended to constitute a formal “fork” of the BlocPal Blockchain, but



simply the representation of rights in a different token “envelope” to facilitate the potential utility and to manage the security features of the BlocPal Token as presently constituted.

BlocPal Blockchain

The BlocPal Blockchain is intended to enhance the functionality and security of BlocPal Applications, and in the future, enterprise applications that are designed to optimize the use of the BlocPal Blockchain. Users who have downloaded a BlocPal Wallet may digitally sign any assets, or “tokenize” them on the BlocPal Blockchain, subject to the permissions granted to their public address through API Keys held by BlocPal. BlocPal is developing several use cases for BlocPal Applications and is continuing to explore opportunities to utilize the BlocPal Blockchain, including as it evolves its regulatory and compliance framework to permit asset tokenization and transfer of crypto assets using the BlocPal Blockchain. In addition, the BlocPal Blockchain will eventually provide the ability for developers to build digital applications utilizing the following core features to perform secure and compliant financial transactions:

1. Digitally sign any assets (“tokenize”) and securely trade assets on the blockchain using the “payload” features of the BlocPal 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. Implement solutions which comply with the regulatory requirements for transactions requiring know your client (“KYC”) and anti-money laundering (“AML”) protection by leveraging the use of API Keys which grant relevant permissions to public addresses;
3. Transparency and security of transactions through the use of a blockchain infrastructure;
4. Scalability and low cost transactions which utilize enhanced features of the BlocPal Blockchain, including dynamic block-sizing and eventually proof-of-stake mining (which does not require miners to “race” to find a solution to add a new block, and grants a miner that right based on the number of coins the miner owns and the length of ownership);
5. Faster authorization of transactions as “proof of stake” mining is introduced and the features of dynamic block-sizing are utilized.

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 confident with how it performs.
- Balance of security vs. features: Increased functionality provided by new blockchains also comes at the price of introducing risk in security. BlocPal carefully selected only the key features required to upgrade on top of the Bitcoin blockchain in order to mitigate the risk of introducing new vulnerabilities.

Dynamic block sizing and proof-of-stake mining is expected to reduce the time required to confirm transactions as the use of the BlocPal Blockchain grows and BlocPal moves to a more decentralized blockchain environment. In addition, with the creation of a reliable BlocPal Blockchain, it is expected that enterprise customers may develop their own applications for integration with the BlocPal Blockchain which would increase the “network effects” of the BlocPal Blockchain. However, with BlocPal’s current blockchain, BlocPal Tokens are still necessary to fuel transactions over the BlocPal Blockchain (just as bitcoins are required to transact over the Bitcoin blockchain) increasing the demand for these BlocPal Tokens.

Transactions and The BlocPal Wallet

Transactional data is recorded on the BlocPal Blockchain and is immutable using encryption technology. The contents of each transaction are represented by a specific hash key which is based on the relevant algorithm incorporated into the BlocPal Blockchain. The encryption methodology requires the hash key to be combined with other hash keys to create a new hash. The process of combining hash keys among several transactions occurs through a “merkle tree”. The creation of blocks of transactions, each represented by a unique hash key, occurs through a “proof-of-work” consensus method. Under the “proof-of-work” consensus method, transactions are recorded on a new block in the BlocPal Blockchain by “miners” who generate encrypted hash-keys (using an ASIC-resistant X16r algorithm) by adding their own random data string to the transaction. This data string must result in a hash-key which has a certain number of leading zeros (similar to the process used for the Bitcoin blockchain). ASIC-resistant implies that specialized computing resources built to facilitate the mining of Bitcoin transactions are not required to mine BlocPal Blockchain transactions given the nature of the X16r algorithm.

Since miners are required to use their own computing resources to derive this data string, they are compensated for each transaction. At the moment, the only miner that is permitted to produce an addition to the BlocPal Blockchain is BlocPal International Inc. All other miners contribute to the mining process through a process of “pooled mining” and are ultimately rewarded based on the amount of “hash-power” they contribute to the mining of each block. The system is referred to as a blockchain since each hash which is created to represent a “block” of transactions is dependent on the prior block. In order to change a transaction on the blockchain, every block after such change would be impacted. The blockchain is considered “immutable” since the amount of processing power and computing energy (hash-power) required to change these blocks would likely exceed the benefit, which will occur when the BlocPal Blockchain becomes fully decentralized. At the moment, BlocPal is the only miner and owns sufficient computing resources to amend the blockchain. In this sense, BlocPal operates a *centralized and permissioned* blockchain. This will change over time as new



miners join the BlocPal BlockChain, and a framework is established in compliance with regulatory requirements to distribute BlocPal Tokens to miners.

The first miner to produce the hash-key (which at the moment can only be BlocPal) earns a minimum of 256 BlocPal Tokens. These “tokens” represent a numeric total that is attributable to a public address. BlocPal divides the BlocPal Tokens among the various miners who contribute to the mining process. Their contribution is recorded based on the amount of “hash-power” they contribute to mining the block. BlocPal delivers the relevant number of tokens to each miner’s public address. In order to qualify as a miner on the BlocPal Blockchain, each miner must enter into a consulting agreement with the Company and is subject to a basic KYC process. Each miner is also a “node” that is required to download a full copy of the BlocPal BlockChain and “listens” for new blocks as they are created. When a new block is created, miners will also confirm the addition of each block by “testing” and reaching consensus that the hash-key is correct. The number of confirmations are reported on BlocPal’s website and reflect the certainty of the block creation process. Once a sufficient number of confirmations are established, miners will have confidence that the transaction has been properly hashed.

Since the number of BlocPal Tokens are capped, in the future they will need to be acquired from other holders of BlocPal Tokens or from BlocPal’s own store of BlocPal Tokens directly, to fund transactions. As and when enterprise customers develop their own applications for use on the BlocPal Blockchain, they will need to acquire BlocPal Tokens to fund transaction costs.

Presently, a BlocPal Wallet is required to enable a holder of BlocPal Tokens to access and transact with transaction information held in public addresses and stored on the BlocPal Blockchain. Similar to using an email address, when someone wants to transfer a BlocPal Token to another person, they can send it to that person’s public wallet address on the BlocPal Blockchain using a transaction, which includes within it the relevant scripting language and hash keys (including specific keys that facilitate the “tokenization” of assets as discussed above). Once this transaction is validated through the “mining process” on the BlocPal Blockchain, the token is then recorded on the BlocPal Blockchain as belonging to the user at the public address. Users can see transactions as they are formed over BlocPal’s own explorer (see <https://explorer.blocpal.com/>). At the moment, BlocPal does not grant holders of BlocPal Tokens the ability to transact with other holders since the holders of these tokens are entitled to a profit distribution which deems the token a security. The only transactions which occur on the BlocPal Blockchain involve the transfer of payload information (which consumes as little as .00000001 of one BlocPal Token) from one public address to another public address (which are typically associated with users of the BlocPal Wallet) and the conveyance of certain tokenized non-crypto assets, in the same manner that a money services business operating a platform would record the conveyance of funds held in book-entry form from one account to another (BlocPal is registered as a Money Services Business in Canada). As these assets are “tokenized” on the BlocPal Blockchain, these transactions, and the creation of blocks still require confirmation by miners. Upon confirmation of a block, new “tokens” are created from the BlocPal Blockchain’s “coinbase address”, issued to BlocPal and then distributed to miners pursuant to their consulting agreement with BlocPal. Eventually, the total number of BlocPal Tokens will approach the maximum permitted by the software code, as discussed in the next section.



Key Features of the BlocPal Token

Issuances to Date:

The following section summarizes the key features of the BlocPal Token including relevant security features and the process by which BlocPal enables individuals to hold and transact in BlocPal Tokens:

- Over one billion BlocPal Tokens (or 1,111,111,111 BlocPal Tokens, to be precise) with the profit distribution and utility features described in this White-Paper may be generated on the BlocPal Blockchain, which limitation is embedded in the BlocPal Blockchain software code.
- A total of 599,142,361 BlocPal Tokens were issued to BlocPal in the genesis block. The remaining BlocPal Tokens will be generated and issued to miners over time.
- BlocPal has “transferred” BlocPal Tokens from itself to third-parties who executed subscription or similar agreements to purchase BlocPal Tokens. Each BlocPal Token (whether held by these third-parties or miners who provide services to BlocPal) is entitled to a pro-rata portion of BlocPal’s cash flows as described below (which is intended to represent the “security” feature of a BlocPal Token).
- BlocPal Tokens are also required to “reward” miners to help generate blocks on the BlocPal Blockchain and to facilitate the creation of transactions as contemplated by the software code (which is intended to represent the “utility feature” of a BlocPal Token).
- Although the total number of BlocPal Tokens are capped, a significantly greater number of transactions (including for the purposes of creating a tokenized asset) can occur on the BlocPal Blockchain since each BlocPal Token is divisible into one / one hundredth millionth of one BlocPal Token (or .00000001 BlocPal Tokens).
- The BlocPal Blockchain cannot be used to create new BlocPal Tokens which are not native to the blockchain (similar to Bitcoin), however for practical purposes given the divisibility of a BlocPal Token (similar to the manner in which Bitcoin is divisible into “Satoshis”), it is expected that the BlocPal Tokens available for conducting transactions (including the tokenization of assets) on the BlocPal Blockchain will never be exhausted.
- The complete technical features of the BlocPal Blockchain are included in Appendix A to this White-Paper.

Trading of BlocPal Tokens on the BlocPal Blockchain:

- The Company performs full “KYC” on each holder of BlocPal Tokens and has marked public addresses that have met relevant requirements through API Keys held by BlocPal.
- Each holder of a BlocPal Token requires a BlocPal Wallet to have access to and read the number of tokens owned by such holder on the BlocPal Blockchain.
- At the moment, only BlocPal, investors, employees, consultants and miners who are eligible have acquired BlocPal Tokens.
- BlocPal can prevent transfers of the BlocPal Token. Trading of tokens is not currently permitted on the BlocPal Blockchain as it is deemed to be a security for security law purposes.



However, the BlocPal Blockchain is used to enable the recording and transfer of information attributable to individuals that have passed BlocPal's KYC process. Only BlocPal can initiate transfers of any portion of a BlocPal Token to facilitate a Transaction (and also funds these transactions from its own repository of BlocPal Tokens) and in that sense, the BlocPal Blockchain is currently used a means to store relevant information for its users who transact in traditional currencies, and not as a means to transact or exchange BlocPal Tokens.

- In the future, when enterprise customers create their own applications, they may need to acquire BlocPal Tokens which may be used to pay miners (i.e., fund transaction costs) and to incentivize mining which is when BlocPal expects the BlocPal Token to gain further utility.

Issuance to Miners:

- The BlocPal Blockchain presently uses a proof-of-work hybrid consensus algorithm, and will eventually utilize "proof-of-stake".
- Mining is not permitted outside of BlocPal's mining pool and will not be opened up until permitted under securities regulations.
- As discussed above, Miners are granted BlocPal Tokens (i) for validating transactions or (ii) recording transactions on a new block of BlocPal's Blockchain.
- The number of rewards granted to miners is fixed at 256 BlocPal Tokens, and halves every 1,000,000 blocks until year 2089. Unlike the Ethereum BlockChain, the number of tokens granted to Miners does not fluctuate based on the complexity of the payload or scripts.
- BlocPal will also eventually introduce a "proof-of-stake" consensus algorithm which requires Miners to transfer tokens to a wallet address. Depending the number and age of the relevant tokens "staked" such miners (or "minters" in the context of a proof-of stake) will be given the opportunity to validate the transaction. In the event the minter "spoofs" the transaction or behaves fraudulently, it can lose the number of tokens staked which encourages good behaviour and enhances the immutability of the BlocPal Blockchain.

Key Terms and Conditions of BlocPal Tokens:

Distribution Rights:

- Currently, the only right granted to a holder of BlocPal Tokens is the right to receive, commencing in calendar year 2022, a Pro Rata Portion (as defined below) of an aggregate amount which equals 33% of the Company's Cumulative Adjusted Operating Cash Flow, net of cash flows which have already formed a basis for a prior distribution (such amount, the "**Distribution Amount**"). These distribution rights are qualified in their entirety by the token rights agreement to be entered into between a holder of a BlocPal Token and the Company. BlocPal does not require its enterprise customers to fund the mining of transactions.
- "**Cumulative Adjusted Operating Cash Flow**" is intended to be the aggregate Adjusted Operating Cash Flow of the Company since the Company's date of incorporation (being November 8, 2017). "**Adjusted Operating Cash Flow**" shall be calculated as net cash flow from operating activities as reflected in the consolidated statement of cash flow of the Company that is included in the audited financial statements of the Company adjusted to (i)



exclude for such purposes cash flow from BlocPal's affiliates or subsidiaries (as defined in the BlocPal token rights agreement) which are included in Adjusted Operating Cash Flow and (ii) include for such purposes cash dividends received from BlocPal's affiliates or subsidiaries as reported in the consolidated statement of cash flow of the Company, in each case as approved by the Company's board of directors.

- For purposes of the calculation of the Adjusted Operating Cash Flow, cash flow from the sale and purchase of blockchain assets, including cash flow from the sale and purchase by the Company of BlocPal Tokens (excluding cash proceeds from an Initial Sale) and cash flow for interest paid and interest received, will be included in the calculation of Adjusted Operating Cash Flow regardless of their classification in the statement of cash flow of the Company. An "Initial Sale" refers to the first sale and transfer of a BlocPal Token by the Company to an initial purchaser. No distributions shall be made while Cumulative Adjusted Operating Cash Flow is negative.
- "Pro Rata Portion" for any BlocPal Token holder means a fraction, the numerator of which is the number of BlocPal Tokens held by such BlocPal Token holder, and the denominator of which is the number of BlocPal Tokens held by parties including the Company or its subsidiaries provided that any BlocPal Tokens that are converted to another financial instrument of the Company at an exchange ratio to be determined upon the time of such conversion, may continue to be included in this calculation in the Company's sole discretion or as otherwise agreed with a token holder.
- Other than the above, a BlocPal Token does not (a) provide the holder with rights of any form with respect to the Company or its revenues or assets, including, without limitation, any voting, distribution, redemption, liquidation, proprietary (including all forms of intellectual property) or other financial or legal rights; and (b) provides the holder with any ownership, equity, or other interest in the Company.
- The Company retains all right, title and interest in all of the Company's intellectual property contained in the BlocPal Tokens, including, without limitation, inventions, ideas, concepts, code, discoveries, processes, marks, methods, software, compositions, formulae, techniques, information and data, whether or not patentable, copyrightable or protectable in trademark, and any trademarks, copyright or patents based thereon. Holders are not permitted to use, reverse engineer, modify, or alter any of the Company's intellectual property for any reason without the Company's prior written consent.
- Holders of BlocPal's BlocPal Tokens have no right to vote or participate in the Company's shareholder meetings or in the corporate governance of the Company. In addition, holders of BlocPal Tokens shall have no rights to receive any reports, notices and other information of the Company.



Appendix A – Technical Specifications

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 Targets:

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.ⁱ

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. BlocPal 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.ⁱⁱ

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 IPFSⁱⁱⁱ) 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^{iv}

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 published on GitHub. The blockchain has undergone significant testing since being launched in September 2018.

Blockchain Pool Mining

BlocPal's official mining pool is open to everyone, subject to certain restrictions. Please visit <https://pool.blocpal.com/> to learn more about mining the BlocPal blockchain.

ⁱ Proof of Work, Proof of Stake and the Consensus Debate, <https://cointelegraph.com/news/proof-of-work-proof-of-stake-and-the-consensus-debate>

ⁱⁱ 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>

ⁱⁱⁱ InterPlanetary File System, <https://ipfs.io/>

^{iv} BlocPal blockchain API, <http://explorer.blocpal.com/info>