



BB BITBLOCKS

WHITEPAPER

TABLE OF CONTENTS



- 1.ABSTRACT
- 2.INTRODUCTION
- 3.SPECIALIZED OVERVIEW
- 4.LIMIT LEVEL
- 5.UNIT VALUATION
 - 5.1 SPECIFICATION
- 6.EXCHANGING
- 7.PROGRESSIVE MODEL
- 8.RISK FACTORS
- 9.DISCONNECTED MINING
- 10.OBJECTIVE
- 11.REFERENCES



1.ABSTRACT

The ascent of the cryptocurrencies in the past couple of years has prompted expanded flexibility, better approaches to exchange, create and hold value, and to raise stores for business. The last one in its ICO shape is rapidly turning into a prominent decision for seed gathering pledges in new tech businesses. Cryptocurrencies however broadly experience the ill effects of a few wasteful aspects with regards to raising funds for organizations whose items have a more physical nature, for example, apply autonomy or different kinds of assembling. To exacerbate it, propelling an ICO battle has just turned into an exceptionally costly process for most beginning organizations. The issues originate from the way that cryptocurrencies (for the most part) depend on 'evidence of-work', while for a beginning organization 'confirmation of-proprietorship' would be a considerably more reasonable decision since the idea of the offering is solely in share value. Subsequently, just a couple of non-IT/non-Fintech organizations have figured out how to adjust the cryptographic money model and transform it into a fruitful ICO, while the customary Angel/VC course is still more common for such organizations. What's more, different issues (principally originating from the many-sided quality of how present day cryptocurrencies function) constrain numerous organizations from currently utilizing them for raising money.

This white paper diagrams a basic new model, which does not depend on customary blockchain standards, while still holding the advantages of cryptocurrencies. The model additionally shows highlights of customary cash, and fusing new special advantages. The proposal demonstrates is for a straightforward, worldwide, decentralized, self-controlling framework for budgetary exchanges.

2.INTRODUCTION

The center component in the new model is called BitBlocks. BitBlocks is a grouping of 1024 bits which adjust to a specific arrangement of tenets.

Legitimate BitBlocks units can be put away and later traded for physical merchandise, administrations, or computerized content in a procedure called Trading.

The way toward making new BitBlocks units is called Mining, in which processing power is utilized to produce a piece of 1024 bits which can be considered as a substantial BitBlock.

The BitBlocks economy does not depend on a blockchain. Rather, it is comprised of little groupings of Miners accumulated around substances called Operators - IT center points whose design is to perform approval of DICE units, and to keep up a database of DICE units related with that specific administrator. Any kind of element can be an administrator in the worldwide DICE economy.

Cases may incorporate all business or non-business associations, a family or even a solitary person.

Administrators are considered as restricted and put stock in parties (just inside the extent of DICE related with the administrator), and every other client are considered as dishonest gatherings.

Each BitBlocks unit is related with just a single administrator for whose sake it has been mined. The unit itself, notwithstanding, is legitimate in the worldwide economy paying little mind to which administrator it is related with. Recently mined BitBlocks are at first possessed by the "digger" who has mined them, and their esteem is added to the capitalization of the administrator for whose benefit they have been mined. Thusly, it is in an administrator's own interest to promote having whatever number of Bitblocks as could be expected under the circumstances mined and circulating in the economy and related with them as the administrator.

Each individual can act as their own "digger", and/or can "dig" for another administrator for excess.

Administrators are totally free from each other, however BitBlocks units are worldwide.

3.SPECIALIZED OVERVIEW

Advanced Address

An advanced mark is a grouping of bits, used to recognize whether somebody is who they claim to be. BitBlocks validation is taken care of by awry encryption (1) of all messages amongst clients and administrators.

Each mineworker or administrator has their own match of keys - an open key and a private key. The user's open key is the thing that the whole system knows (i.e. it's freely accessible), and the private key is the thing that only the mineworker/administrator know (i.e. it's totally private). Amid introductory enlistment of the key combine, the client picks a secret key which is private. That private secret key is then used to produce a 160-piece open key, which fills in as their street number and personality in the BitBlocks economy. Information encoded with the client's open key must be unscrambled with a similar client's private key, which only they will know.

Along these lines a system peer who starts correspondence with another associate dependably encodes active messages utilizing the beneficiary's open key (i.e. postage information) and will get every approaching message scrambled utilizing their own open key.





BITBLOCKS

Extremely fast. Zero transaction fees.

Send, receive and confirm payments within seconds.

Staking - Forget power-hungry mining rigs-stake and earn interest.

Community Driven - Become part of a powerful support network of like-minded users.



4. LIMIT LEVEL

All together for an administrator to acknowledge another BitBlocks unit, the primary condition is that the hash of the BitBlocks unit needs a specific least number of its slightest critical bits all set to zero.

This esteem, together with the BitBlocks timestamp, decide the estimation of a Bitunit.

As of this present record's date, the default limit level is **$N = 40$**

BitBlocks convention implies that a unit can be esteemed just inside the ($N - 10 \dots N + 10$) territory.

In this way, for $N = 40$, unquestionably the least adequate edge would be $N_{min} = 30$, and without a doubt the most extreme would be $N_{max} = 50$.

However, there is no characterized "most extreme", since the limit level is put away in 8-bit space, the hypothetical greatest edge would be 256 (put away as esteem 0 in the field).

Administrators set the individual limit level as per the stage they are in, and to the mining specialty they are focusing on. Setting the edge too low would bring about the mining of a vast amount of low-esteem BitBlocks units. Setting the limit too high would bring about troublesome and powerconcentrated mining thus creating just a little amount of high esteem BitBlocks units.



5.UNIT VALUATION

The estimation of a BitBlock unit is ascertained as: $v = (k * 2(b-z) * 2(z-N)) \oplus 2(Nmax)$

Where v is the estimation of the unit, b is the quantity of trailing zero bits in the hash, and z is the limit level for all time set in the DICE unit.

N is the default edge, $Nmin$ and $Nmax$ are individually the $N-10$ and $N+10$ restricting qualities.

The parameter k is a revision factor separately set by the administrator for units with particular timestamps. The default an incentive for k in all non-elite cases is 1. All together for a DICE unit to be viewed as substantial, it needs to fulfill the condition $b \geq z \geq Nmin$. In the event that a substantial unit is delivered however $b > Nmax$ - the unit is as yet legitimate, yet its esteem is topped at $(Nmax)$. Hence a unit produced at the default limit level N , and having precisely N trailing zero bits, will have the estimation of one DICE.

... Since units are produced binarily, the valuation recipe dependably creates an outcome which is a number in forces of 2, for units with esteem 1 or more noteworthy.

A similar equation can likewise be communicated in an alternate frame to improve the computation of units with values under 1 (i.e. edge level $z < N$):

$$v = (k * 2(b-z) 2(N-z)) \oplus 2(Nmax)$$

By applying without a doubt the base worthy limit esteems $Nmin$ and $Nmax$, the recipe demonstrates that the smallest conceivable division of a DICE unit **1 1024** and the most noteworthy single DICE esteem is 1024. Since divisions are double, not decimal, a proposed augmentation to the IEC prefixes [6] for a **1 1024** part is "mibi", thusly 1 DICE = 1024 mibiDICE, and 1 kibiDICE = 1024 DICE.

Specifications



Algo: Script
Type: POW + POS
Address letter: B
RPC port: 21327
premine: 3%
Max supply: 500m
Block time: 15s



POS REWARD: POS start after block 20k

Block 20k-100k	500%
Block 100k-200k	250%
Block 200k-300k	125%
Block 300k-400k	60%
Block 400k-500k	30%
Block 500k-1mil	10%
Block 1mil+	1%

POW REWARD

POW start after block 3.2k

Block 3.2k-100k	= 50BBK
Block 100k-200k	= 40BBK
Block 200k-300k	= 30BBK
Block 300k-400k	= 25BBK
Block 400k-500k	= 20BBK
Block 500k-600k	= 15BBK
Block 600k-700k	= 10BBK
Block 700k-800k	= 9BBK
Block 800k-900k	= 8BBK
Block 900k-1000k	= 7BBK
Block 1000k-1500k	= 6BBK
Block 1500k-2000k	= 5BBK
Block 2000k-3000k	= 3BBK
Block 3000k-4000k	= 1BBK
Block 4000k-5000k	= 0.5BBK
Block 5000k+	= 0.1BBK



6.EXCHANGING

Exchanging the BitBlocks economy depends on possession asserts as opposed to dynamic exchanges. No record of exchanges exists anywhere in the system. The procedure can be depicted in a couple of summed up steps: 1. Current proprietor gives BitBlocks units to the new proprietor. This could be as computerized content (twofold record, email), or physical frame (paper note, document stockpiling gadget). Units are encoded with the new proprietor's open key. 2. Current proprietor puts a claim for new possession to the administrator who handles the specific BitBlocks unit utilized as a part of the exchange, giving the hash of the unit. 3. New proprietor checks the BitBlock, and furthermore puts a claim for new possession to the administrator of the BitBlocks, giving the hash of the provided unit. 4. Administrator confirms the legitimacy of the unit, and the two claims, and stores it in its private database with the address of the new proprietor as the enrolled proprietor of the DICE which gave the hash. 5. Administrator sends a reaction message to the two gatherings educating them about the difference in responsibility for unit.

This is rehashed for each BitBlocks unit engaged with the exchange.

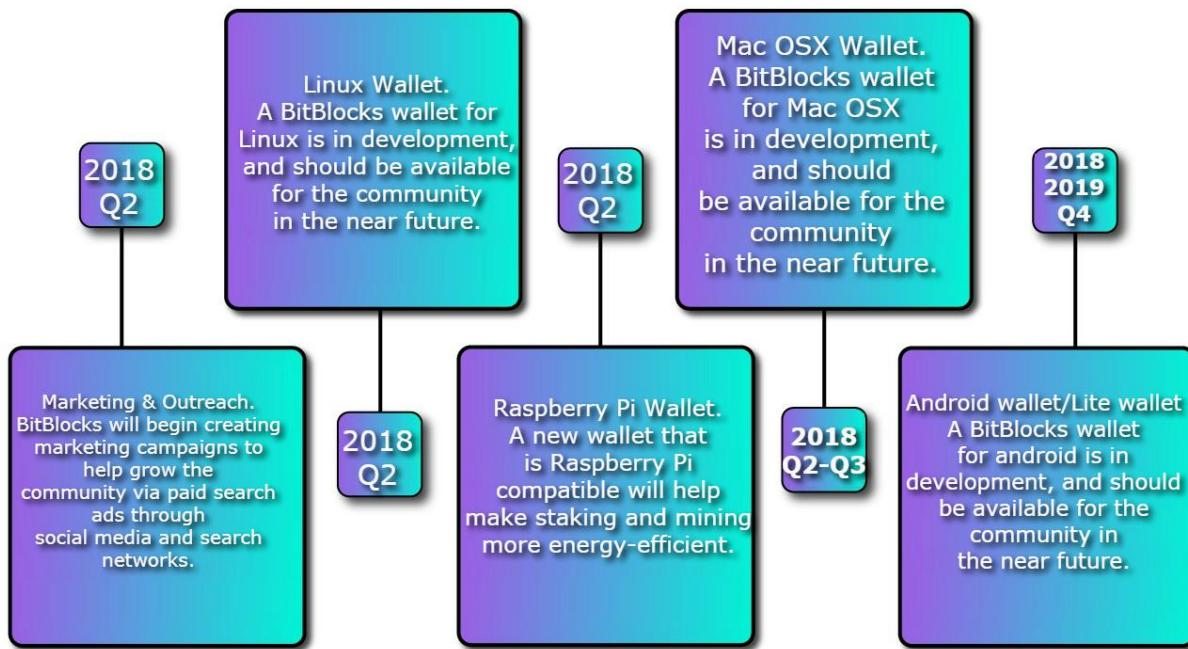
The procedure for one unit can be envisioned in the accompanying graph:

It can be seen that an effective exchange of possession can just happen when the accompanying conditions are met:

1. The current and the new proprietor both have the real BitBlocks unit in its crude frame.
2. The unit is a substantial BitBlocks unit.
3. The unit is known to the administrator.
4. The administrator perceives the present proprietor as the lawful proprietor of the unit.
5. The current and the new proprietor have both educated the administrator about the up and coming difference in responsibility for BitBlock unit giving and coordinating hash created from the BitBlocks.

It is imperative to take note of that between exchanging parties BitBlock units are traded in their crude frame, while claims put to the administrator are just made utilizing the hash of those units.

Roadmap



7. PROGRESSIVE MODEL

Genuine Decentralization

BitBlocks does not have a solitary record like what was introduced with the run of the mill blockchains. Rather, there are the same number of records as there are administrators in the worldwide biological community - some of them open, others private.

Strengthened Security

Another correspondence convention which makes it for all intents and purposes difficult to hack and take BitBlocks. Notwithstanding that the physical idea of Bitblocks requires having a duplicate of the real information structure.

8. RISK FACTORS

IMPORTANT NOTICE: PROSPECTIVE SUBSCRIBERS SHOULD CAREFULLY READ THE WHOLE OF THIS OVERVIEW DOCUMENT. TOGETHER WITH THE "LEGAL CONSIDERATIONS, RISKS AND DISCLAIMERS" AVAILABLE ON BITBLOCKS WE RECOMMEND THAT YOU CONSULT WITH A LEGAL, FINANCIAL AND TAX PROFESSIONAL OR OTHER ADVISOR FOR FURTHER GUIDANCE PRIOR TO PARTICIPATING IN THE BITBLOCKS LIMITED SALE. YOU ARE STRONGLY ADVISED TO TAKE INDEPENDENT LEGAL ADVICE WITH RESPECT TO THE LEGALITY OF THE BITBLOCKS SALE IN YOUR JURISDICTION. YOU SHOULD NOTE THAT YOUR ACKNOWLEDGMENT AND ACCEPTANCE OF THE BITBLOCKS SALE'S TERMS AND CONDITIONS REPRESENTS THAT YOU HAVE SOUGHT PRIOR INDEPENDENT LEGAL ADVICE.

9. Disconnected Mining

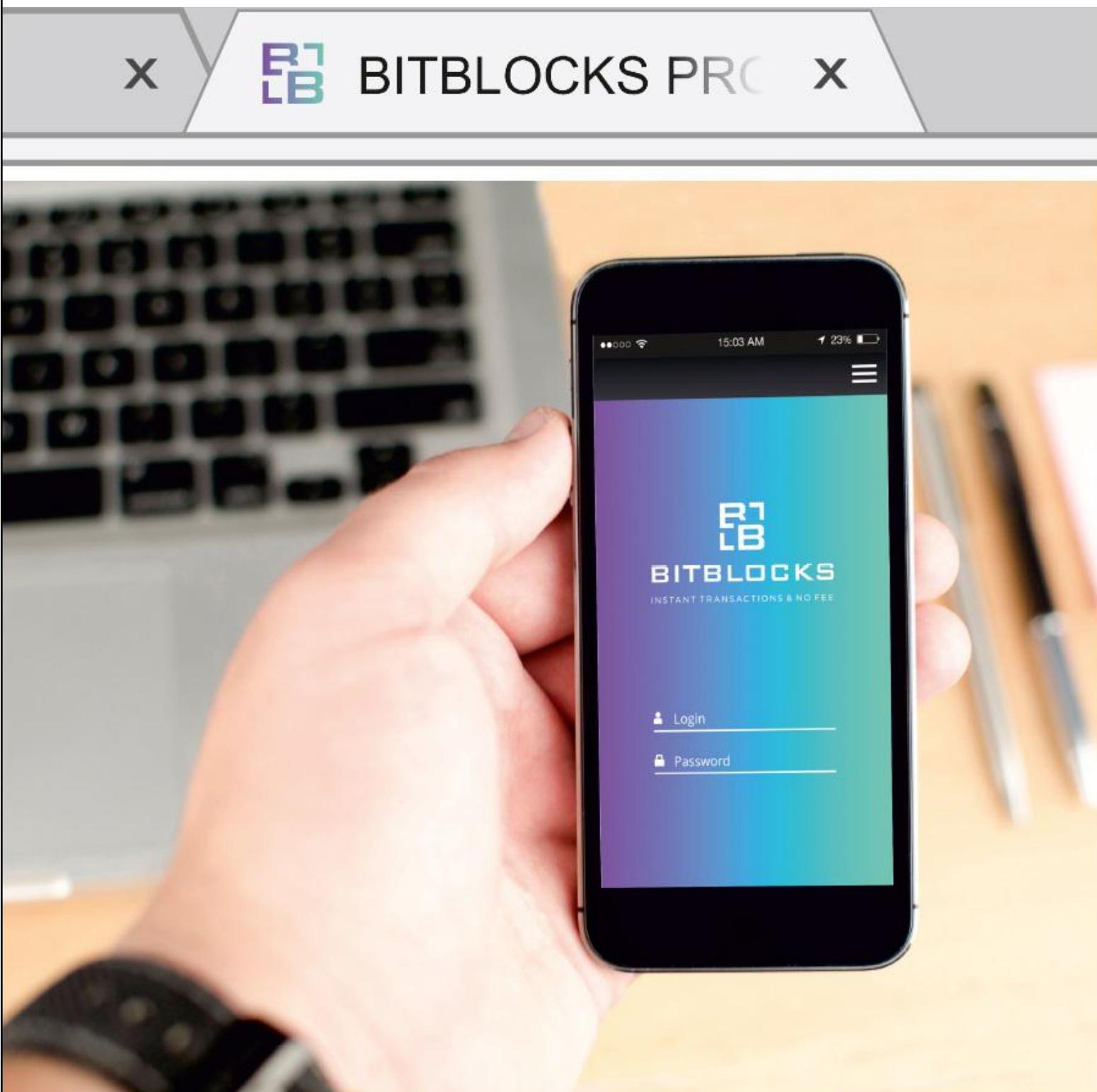
BitBlocks can be mined securely without the dread that another person is.

10.OBJECTIVE

The BITBLOCKS network was designed with the goal of developing a next-generation payments network that could gain widespread adoption by consumers.

To develop a distributed ledger-based payment system that provides a streamlined user experience, while harnessing the power of advanced financial tools, and removing the need for financial intermediaries. We have set out to achieve the following objectives:

Objective 1: Reliability → OBJECTIVE 2: Zero fees → Objective 3: Ease-of-use



11. REFERENCES

www.bitblocksproject.com

<http://github.com/BitBlocksProject/BitBlocks>

<https://bbk.overemo.com/>

<http://explorer.bitblocksproject.com/>

SOCIAL MEDIA:



https://twitter.com/BitBlocks_



<https://www.facebook.com/BitBlocks>



<https://bit.ly/2GadG4D>