BlackHat Coin

community-driven self-funded decentralized
blockchain focused on privacy

White Paper

v. 0.9.2

Contents

TABLE OF CONTENTS

INTRODUCTION ____ **3**

DESCRIPTION OF BLACKHAT COIN PROJECT ____ **4**
- Main aims
- Brief of advantages
- Coin information
- Project socials

FEATURES AND BENEFITS ____ **7**
- Secure anonymous payments
- Proof of Stake (POS), Staking.
- Cold Staking
- Masternodes
- Decentralized Governance
- BlackHat Community Treasury

ECONOMIC MODEL ____ **11**
- Block rewards
- Bounty bonus program

ROADMAP ____ **16**

INFERENCE ____ **17**

INTRODUCTION

Privacy is necessary for ensuring freedom on the internet. When your transactions are being watched — or when your transaction history is available to be known — a person isn't free to make their own decisions. With other digital currencies, bad actors are able to match people to their balances and details about parties involved, amounts and trends.
Zcash Team

Today we often come across the thought leaders' statements that a concept of privacy in a contemporary world needs a revamp. Some of them refer to the change in the socio-communicative patterns of the communities (availability of information on various social media); some draw attention to the uselessness of efforts aimed at protecting data due to the vulnerabilities of information systems and possible leaks; others advocate the creation, due to the abundance of open data, of added value for business (the basic principles of contemporary advertising) or the opportunity to contribute to discoveries being important for the entire mankind (e.g. a Google project related to an attempt of early detection of epidemics based on user requests).

And while in terms of granting access to our personal data to any applications or provision of actual information about ourselves on social media, it is up to us to make decisions, every time making a reasoned choice and understanding the consequences, in the field of financial transactions such freedom of choice has been constantly and increasingly limited. It is the issue of privacy of peoples' finances that has given rise to the creation of a number of cryptocurrency projects focused on the increased confidentiality of user transactions (Monero, Zcash, Dash, SmartCash, ZeroVert, and many others) only during the last 5-10 years.

The solution to maintaining confidentiality under the existing conditions is surely the development and use of as many privacy-related projects as possible. The risk of compromising one's own privacy is possible and necessary to diversify using various systems. The BlackHatCoin team proposes to solve this issue, in addition to other means, by means of our project, which has incorporated the best industry-specific trends.

DESCRIPTION

BlackHat Coin Project, launched April, 2021, is a community-driven self-funded decentralized blockchain focused on privacy which is implemented on zk-SNARK Sapling protocol by Electric Coin Company.
The monetary policy of BlackHat Coin is designed to enable a sustainable infrastructure service capable of supporting scalable, decentralized, and resilient node infrastructure, allowing for instant, private transactions globally.

MAIN AIMS

- to make crypto easy for anyone. You don't have to have any mining equipment, just your computer, laptop or even Raspberry Pi;
- to build strong decentralized self-governed community;
- mass adoption: we will do our best not to be just a trading asset, but also a payment method in any store willing accept payments in secure way;
- to provide instant and secure transactions all over the world.

MAIN ADVANTAGES IN BRIEF:

- Energy saving mining (POS);
- High privacy level (zk-SNARK);
- Low fees;
- Governance / DAO;
- Community driven.

PROJECT SOCIALS:

Website:
https://blackhatco.in

Telegram:
https://t.me/BlackHatCoin

Discord:
https://blackhatco.in/discord

Twitter:
https://twitter.com/blkcoin

Weibo:
https://weibo.com/u/7624298845

COIN INFORMATION

Symbol	BLKC
Maximum sypple	21 m (premine 1 m)
Consensus	PoS (Hot & Cold PoS)
Block Time	~1 minute
Block Size	Max 2 Mb
Transactions per second	173 TPS (theoretical maximum)
Blockchain	BlackHat
Pre-sale price	0.7 $
Masternode Collateral	5 000 BLKC

FEATURES AND BENEFITS

Secure anonymous payments.

- The privacy layer of BlackHat Coin implemented on zk-SNARK technology (from ZCash) which provides fast and anonymous untraceable payments.
- Interchangeability There is no difference between coins, no matter how they were obtained.
- Compromising is impossible. The history of the coin origin cannot be traced.
- Guaranteed anonymity: only the sender and the recipient can know about the transaction when making transactions using a zero-knowledge proof protocol.
- Untraceable transactions. The zk-SNARK protocol hides any external data other than the time mark.

Proof of Stake (POS), Staking

- Keeping your wallet switched on and holding coins in it you not just receive rewards but also strengthen the network.
- With Proof of Stake (POS), cryptocurrency miners can mine or validate block transactions based on the amount of coins a miner holds.
- POS was created as an alternative to Proof of Work (POW), which is the original consensus algorithm in Blockchain technology, used to confirm transactions and add new blocks to the chain.
- POW requires huge amounts of energy, with miners needing to sell their coins to ultimately foot the bill; Proof of Stake (PoS) gives mining power based on the percentage of coins held by a miner.
- POS is seen as less risky in terms of the potential for miners to attack the network, as it structures compensation in a way that makes an attack less advantageous for the miner.

Cold Staking

- You can delegate your coins for staking to another wallet which is switched on 24/7 (hot wallet). Hot wallet stakes delegated coins on your behalf but have no access to them. The rewards go directly to your wallet. All coins remain under your full control in your wallet. Your wallet could be switched off keeping your private keys and coins safe while hot wallet stakes coins for you.
- It's possible to delegate coins from different multiple wallets to one hot wallet for cold staking.

Masternodes

- Masternodes is the second layer of network security which provides additional blocks and transaction validations.
- Starting your own Masternode you're also strengthening the network and receiving rewards.
- Anyone who started Masternode can participate in Decentralized Governance voting for the proposals to determine if the proposal should be funded. This voting is decentralized and anonymous, since the owners and their Masternodes are located in different parts of the world.

Decentralized Governance

- Decentralized Governance is the system of proposals which is submitted to the blockchain network to be voted by Masternodes, to determine if the proposal should be funded.
- Each started Masternode has a capability to vote for each proposal (a vote per Masternode for each active proposal) thereby setting the vector of network development. Therefore, only community-validated initiatives will be funded.

BlackHat Community Treasury

- % of block value will be potentially allocated for the Community Treasury to fund an implementation of proposals that received sufficient % of Yes votes. This funds will be generated at each superblock (approx. each month).
- The budget will not be allocated each month in full. Only valid proposals will be funded and only a required amount of coins will be generated.

BLACKHAT COIN ECONOMIC MODEL

BlackHat blockchain creates a new block every 60 seconds. Each of these blocks create “X” new BLKC, and (may be) created “Y” new BLKC for the Community Treasury. X and Y will be decreased every 3 months (see the math below).

- BlackHat Coin has a variable percentage of the reward per block.

Block reward will be decreased every 3 months by 20% (about ~50% yearly). Minimal block reward (2 BLKC) will be reached approximately in 3 years.

reward reduction schedule		
Approx. timeline	**Block Height**	**Reward for 1 block (X)**
Premine	1	1 m BLKC
Premine for bounty program	2 - 100	the exact amount will be determined at the end of the Bounty program
Fair start	101 - 2000	0.1 BLKC
First 3 months	2001 - 129 600	20 BLKC
4-6 months	129 601 – 259 200	16 BLKC
7-9 months	259 201 – 388 800	12.8 BLKC
10-12 months	388 801 – 518 400	10.24 BLKC
…		
more than 3 years	>1 425 600	2 BLKC

- % of BLKC allocated to the Community Treasury and (may be) created with the Super Block and paid to a funded proposal. Treasury reward also will be decreased every 3 months.

To understand the math of the Community Treasury of the BlackHat economic model you need to know that: its a system that allows for funding to be generated for community proposals. Proposals are submitted to the system by the community, and they are voted on once a month. Those proposals that pass are issued the funds they have requested. This fund issuance occurs in a "Super Block", which occurs every 30 days. The available funds for each Super Block equals the number of blocks since the last Super Block, times the number of BlackHat allocated for the Super Block from each block.

The math here is fairly simple (for example for first 3 months, when Y=1): 1 BLKC per block, and one block every minute, for 24 hours for 30 days works out to be 30 days x 24 hours a day x 60 minutes per hour x 1 BLKC per block.

30 x 24 x 60 x 1 = 43 200 BLKC allocated to the Treasury per Super Block. This forms the Treasury Community budget available for the proposals.

Treasury reward math		
Approx. timeline	**Reward for 1 block (Y)**	**Super block reward**
First 3 months	1 BLKC	43 200
4-6 months	0.95 BLKC	41 040
7-9 months	0.9 BLKC	38 880
10-12 months	0.85 BLKC	36 720
…		
3 years and more	0.45 BLKC	19 440

When the Super Block is created each month, the Masternodes reach a consensus on the proposals that have met the required number of Yes votes. To be considered for funding, the difference between the Yes votes and No votes must be greater than 10% of the number of Masternodes on the network.

For example, if there are 200 Masternodes, a proposal must have 20 (10% of 200) more Yes votes than No votes. The proposals are sorted by their “net Yes” votes (Yes votes minus No votes) and they are then paid in order from highest “net Yes” to lowest.

The total BlackHat required to fund all the passing proposals is rarely identical to the budget (43 200 BLKC with Y=1). If the total funds needed for all passing proposals is “under budget”, not all 43 200 are created. For example, if all passing proposals total 40 000 BLKC, then only 40 000 BLKC are created and paid to those proposals. This does not mean that the full budget of 43 200 BLKC was created. This Coin Emission is what is meant by ‘allocated’;

Y BLKC is allocated from each of the 43 200 blocks between Super Blocks to form the budget, but only enough to fund the proposals is actually created when the Super Block is created. In the example scenario, the extra 3,200 BLKC are not created in the first place. Only the 40 000 BLKC needed are created.

Conversely, if the passing proposals exceed the 43 200 BLKC budget, proposals are paid out in order until there is not enough room in the budget to pay any of the further proposals.

It is possible that exactly 43 200 BLKC can fund passing proposals, with nothing remaining. But, this is rare. However, it is important to realize this is not exact. It is also important to realize that the BLKC for Community Treasury is created at the Super Block, whereas the other X BLKC (as block reward) is created with each standard block.

- BlackHat Coin relies on both stakers and Masternodes to possess its native token, BLKC, to help decentralize, govern, and secure the network.
- Both Masternodes and Stakers earn rewards. Block reward is divided between Stakers and Masternodes as follows: 40% PoS and 60% Masternodes.
- Users of BlackHat pay a small transaction fee per transaction.
- All transaction fees are burned, removing coins from the total supply.

BOUNTY BONUS PROGRAM

As a reward for joining the BlackHat Coin community in Telegram and Discord, you will receive 0.5 BLKC to your account in the Referral program.

For the registration of each Invited Participant who entered the Referral Program by your registration link (first level referral participant), confirmed by the BlackHat Coin in accordance with these Terms and Conditions, bonus coins in the amount of 0.25 BLKC will be accrued to your account in the Referral Program.

For the registration of each Invited Participant who entered the Referral Program by registration link of your first level referral participant (second level referral participant), you will also be accrued with Bonus Coins in the amount of 0.15 BLKC.

For registering as an Invited Participant in the Referral Program using someone else's referral link, the user, in addition to 0.5 BLKC for the registration receives a reward in the amount of 0.1 BLKC.

The limitation of the accrual of remuneration for an invitation to the Referral Program is set on the second level referral participant, that is, for registering a referral participant of the third level and higher (fourth, fifth, etc.) you do not receive remuneration.

More details at https://fair.blackhatco.in/

PRODUCT DEVELOPMENT ROADMAP

April, 2021

"Coin Fair" and "Bounty bonus program"

May, 2021

End of Pre-sale and Bounty bonus program.

Wallet release (Windows, Linux, Mac) and start of the BlackHat Coin blockchain.

Q2, 2021

Finalize our website https://blackhatco.in

Q2, 2021

Vindax.com
Crex24.com
Dex-trade.com
listings

Q2, 2021

Web wallet release

Q3, 2021

Cold staking release

Q3, 2021

Decentralized Governance for MN owners

Q3, 2021

Restructuring of the BlackHat Project website

Q3, 2021

Mobile wallet

Q3, 2021

Staking support for Web Wallet (shared staking pool implementation)

Q3, 2021

New exchange listing

Q4, 2021

BlackHat Merchant Payment Processing System

Q4, 2021

Faucet development and release (free BLKC for everyone)

Q4, 2021

Official automatic OTC

Q4, 2021

New exchange listing

Q1, 2022

BlackHat Coin ecosystem expansion

To be continued

INFERENCE

The major problem with central banks or corporate currencies is the concentration of power and data. That is, you become dependent on centralized structures that can exercise very precise control over those involved.
V.D. Buterin

Privacy technologies are to further evolve. Maintaining full-scale transparency will not make the cryptocurrency field perfect, but we should enable high-level government agencies and regulators to control the turnover of transactions to track those wishing to use the anonymous system pursuing criminal purposes.
Jonathan Levine, Chainanalysis

In recent years, the number of projects in the field of the cryptocurrency economy has grown several hundred times. Various leaders of the crypto industry (Vitalik Buterin, Brian Armstrong, etc.) have repeatedly spoken about the major problems related to a significant increase in the number of users of the crypto community and the desire of governments and states to control this market segment. According to the BlackHat Coin Project Team one of the main problems nowadays is the issue of user transaction privacy.

Today it is not a secret to anyone that artificial intelligence-based systems for analyzing cryptocurrency transactions have been developed, terms of tokens use have been tightened, the interests of various centralized projects have been lobbied in every possible way. The regulating authorities of different countries approach the issue of deanonymization in different ways, though the essence remains the same: full-fledged total control.

Under the guise of the idea of combating criminal activity, creating a sort of a balance of privacy and control over illegal activities, as well as lobbying business interests, government bodies and large commercial companies try to develop conditions infringing the right to personal secrets of a person. Protecting our rights, we have to wear black hats, ladies and gentlemen! The era of privacy has began. No one shall be subjected to arbitrary interference with his privacy (https://blackhatco.in).