Cyberscope

Audit Report

HashBit BlockChain

January 2023

Github https://github.com/HashBitorg/hbc20

Commit 069d9937282b98ceadc7c4f53de2d42e99c1d730

Audited by © cyberscope

Table of Contents

Contracts Review

Blockchain Github	https://github.com/HashBitorg/hbc20
Commit	069d9937282b98ceadc7c4f53de2d42e99c1d730
Node Github	https://github.com/HashBitorg/node-info
Commit	933d815a1eb57726dd38a36b0ab7023e01210d8f
Explorer	https://explorer.hashbit.org/
Chain Id	11119
RPC	https://rpc.hashbit.org/

Audit Updates

Initial Audit	2 January 2023

Ethereum

Ethereum is a decentralized, open-source blockchain platform that enables the creation of smart contracts and decentralized applications (DApps).

At its core, Ethereum is a blockchain-based decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud, or third-party interference. These smart contracts are written in a high-level programming language, such as Solidity, and are compiled into bytecode that can be run on the Ethereum Virtual Machine (EVM), a runtime environment that executes the smart contracts.

Ethereum is often referred to as a "world computer" because it allows anyone to run any program, as long as they are willing to pay for the computation. This has led to the development of a wide range of decentralized applications, or DApps, on the Ethereum platform, covering areas such as finance, governance, and social media.

Ethereum is powered by a cryptocurrency called Ether (ETH), which is used to pay for the computation required to run applications on the Ethereum platform. ETH is also used as a store of value and as a medium of exchange, similar to Bitcoin.

Ethereum Virtual Machine

The Ethereum Virtual Machine (EVM) is a runtime environment for executing smart contracts on the Ethereum blockchain. It is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud, or third-party interference.

The EVM is implemented as a part of the Ethereum blockchain, and is responsible for executing the bytecode of smart contracts. This bytecode is produced by compiling high-level programming languages, such as Solidity, into a format that can be run on the EVM. Once a smart contract has been deployed to the Ethereum blockchain, it is stored in the blockchain and can be executed by the EVM when triggered by an external event, such as a user interaction or the arrival of data from an external system.

The EVM is designed to be lightweight and efficient, so that it can be run on a wide range of devices, from high-powered servers to low-powered IoT devices. It is also designed to be secure, with a number of measures in place to prevent fraud and tampering.

Overall, the EVM is an important part of the Ethereum platform, enabling developers to build and deploy decentralized applications that can run on the Ethereum blockchain.

HashBit

HashBit is a rapidly growing open-source blockchain created in may 2021. HashBit has become one of the safest, fastest, longest and most decentralized blockchain in existence.

Blockchain

HashBit is Ethereum Virtual Machine compatible. That means that the blockchain/ virtual machine runs the bytecode that has been compiled for the EVM. This allows smart contracts written for the EVM to be run on HashBit, providing a degree of interoperability between different blockchain environments.

HashBit relies on a system of Proof of Authority consensus that can support short block time and lower fees. The most bonded validator candidates of staking will become validators and produce blocks. The double-sign detection and other slashing logic guarantee security, stability, and chain finality.

HBC20

HBC20 is the extended variation of ERC20 standard in the HashBit ecosystem. ERC20 is a technical standard used for smart contracts on the Ethereum blockchain for implementing tokens. ERC stands for Ethereum Request for Comment, and 20 is the number assigned to this request.

The ERC20 standard defines a set of rules that a token contract must follow, allowing it to be integrated with other contracts and exchangeable on cryptocurrency exchanges. These rules include:

- How the total supply of tokens can be stored and accessed
- How tokens can be transferred from one address to another
- How the balance of a token can be checked for a given address
- What information is available about the token, such as its name, symbol, and decimal precision

The ERC20 standard has become the most widely used standard for creating tokens on the Ethereum blockchain. Overall, the ERC20 standard has helped to bring greater interoperability and standardization to the Ethereum ecosystem, making it easier to develop and exchange tokens on the platform.

Audits Timeline

Ethereum blockchain has been audited several times.

geth

https://github.com/ethereum/go-ethereum/blob/master/docs/audits/2017-04-25_Geth-audit_Truesec.pdf

clef

https://github.com/ethereum/go-ethereum/blob/master/docs/audits/2018-09-14_Clef-audit_NCC.pdf

Discv5

https://github.com/ethereum/go-ethereum/blob/master/docs/audits/2019-10-15_Discv5_audit_LeastAuthority.pdf

Discv5

https://github.com/ethereum/go-ethereum/blob/master/docs/audits/2020-01-24_DiscV5_audit_Cure53.pdf

Audit Approaches

There are several approaches that have been taken from the various Ethereum blockchain audits reports. These approaches involves:

Code review

This involves manually reviewing the code of smart contracts and other applications that are running on the Ethereum blockchain. This can help to identify vulnerabilities, security flaws, and other issues that may impact the security and reliability of the Ethereum blockchain.

Static analysis

This involves using automated tools to analyze the code of smart contracts and other applications without actually executing them. This can help to identify issues such as syntax errors, code smells, and security vulnerabilities.

Dynamic analysis

This involves executing the code of smart contracts and other applications and analyzing the behavior of the Ethereum blockchain during runtime. This can help to identify issues such as performance bottlenecks, security vulnerabilities, and other issues that may impact the reliability and stability of the Ethereum blockchain.

Testing

This involves creating and executing test cases to validate the behavior of smart contracts and other applications running on the Ethereum blockchain. This can help to identify issues such as functional errors, security vulnerabilities, and other issues that may impact the reliability and stability of the Ethereum blockchain.

Performance

Ethereum's performance is determined by a number of factors, including the complexity of the smart contracts being run, the number of transactions being processed, and the current level of network congestion.

One measure of Ethereum's performance is its transaction throughput, which refers to the number of transactions that the network can process in a given time period. As of 2021, Ethereum's average transaction throughput was around 15 transactions per second (TPS), although the network is capable of processing significantly more TPS under optimal conditions. This is significantly lower than some other blockchain platforms, such as Visa, which can process thousands of transactions per second.

Another measure of Ethereum's performance is the time it takes for a transaction to be processed and included in a block (known as the confirmation time). This can vary depending on network conditions, but on average it takes around 15 seconds for a transaction to be confirmed on the Ethereum network.

Vulnerabilities

Smart contract vulnerabilities

Smart contracts, which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code, can contain bugs or vulnerabilities that could be exploited by attackers.

Denial of Service (DoS) attacks

A DoS attack is a type of cyber attack in which the attacker floods a network or system with traffic, disrupting its normal operations. Ethereum has been vulnerable to DoS attacks in the past.

Wallet vulnerabilities

Ethereum wallets, which are used to store and manage Ethereum and other cryptocurrencies, can also be vulnerable to hacking or other types of cyber attacks.

51% attack

A 51% attack is a type of attack that occurs when a single entity or group of entities controls more than half of the computing power on a proof-of-work (PoW) blockchain. This allows them to potentially alter the transaction history and block new transactions from being processed.

51% Attack Vulnerability

The 51% Attack could provide the following abilities to the attacker:

Reverse transactions

An attacker could potentially reverse transactions that have already been completed, allowing them to double spend their own coins.

Block new transactions

An attacker could block new transactions from being added to the blockchain, effectively halting all activity on the network.

Deny service

An attacker could use their control of the network to deny service to other users, preventing them from accessing the network.

Overall, 51% attacks are a potential vulnerability for proof-of-work blockchain networks, and steps should be taken to prevent them from occurring. This includes decentralizing the network and encouraging a diverse group of miners to participate.

HashBit Approach

Proof of Authority (PoA) is a type of consensus mechanism used in blockchain networks. It is similar to the more well-known proof-of-work (PoW) mechanism, but rather than relying on miners to validate transactions and create new blocks, it uses a set of "validators" who are pre-approved by the network to do so.

In a PoA network, the validators are responsible for verifying transactions and adding them to the blockchain. They are chosen based on their reputation and trustworthiness, and are typically selected by the network's creator or a group of trusted individuals.

One of the main benefits of PoA is that it can be more efficient than PoW, as it does not require miners to perform resource-intensive calculations in order to validate transactions. This can make it faster and cheaper to process transactions on the network.

Overall, PoA is an alternative to PoW that can offer some benefits in certain situations, but it also has some potential drawbacks. For example, it relies on the trustworthiness of the validators, and if a validator becomes compromised or malicious, it could potentially lead to problems on the network.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

https://www.cyberscope.io