Black Hole Coin

BLACK HOLE COIN WHITEPAPER

Stable / Safe / Economic / Fast

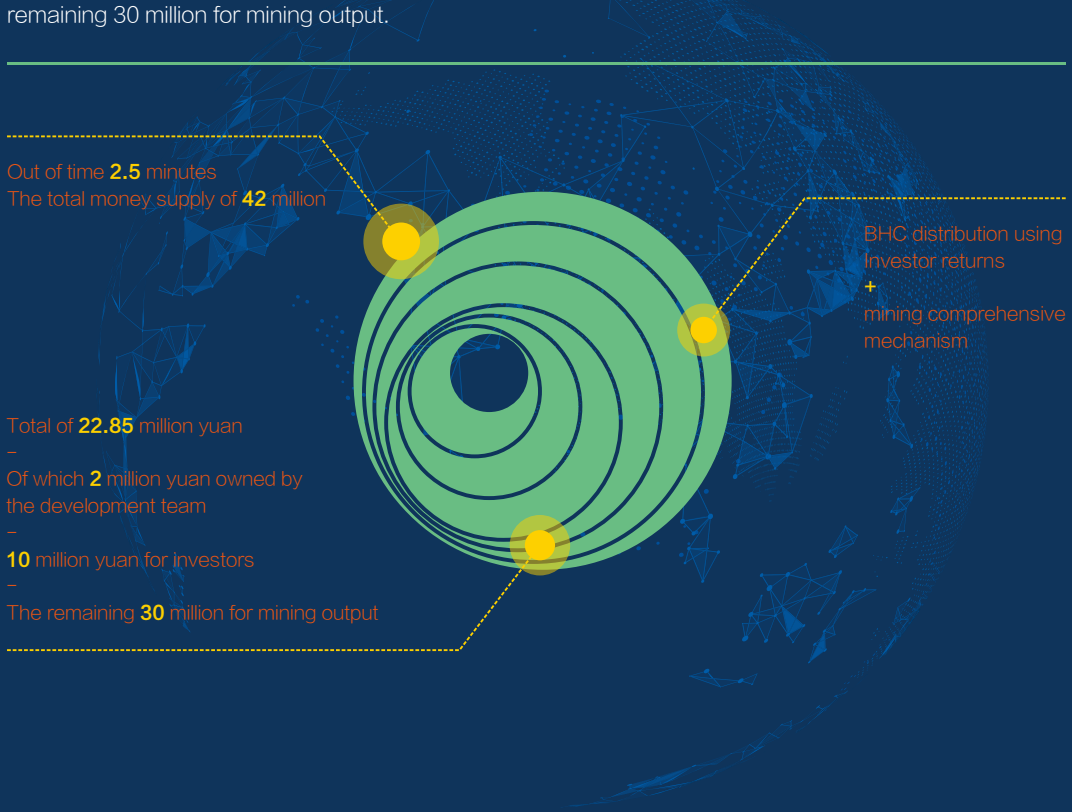
01.

ECoin

Black Hole Coin (BHC) is an encrypted currency that protects privacy by using a zerocoin protocol. It is the first to achieve the coin agreement of the encrypted currency, through the use of zero knowledge to ensure that the relevant information on both sides of the transaction from leakage.

BHC out of time 2.5 minutes, the total money supply of 42 million, the output half of the cycle for 4 years. BHC to remove the founder of the reward, during which 20% of each output is still owned by miners. BHC was developed by the top European virtual coin development team, with most of the members working for Oxford University and Heidelberg University graduate students and two Chinese students. BHC distribution using Investor returns + mining comprehensive mechanism, in ensuring the development team early development costs on the basis of the late protection of miners and investors interests.

BHC total of 22.85 million yuan, of which 2 million yuan owned by the development team. BHC received $ 500,000 in early investment, and 10 million yuan for investors. Income for publicity, landing trading platform to promote the development of BHC fund account and follow-up application development, the remaining 30 million for mining output.



02.

Background

Since the transaction history of Bitcoin is completely open, everyone can query your wallet cash inflows and outflows in the chain chain with your wallet address, and can be traced back to the ultimate origin of these bits, The address sent after the build. This poses a huge threat to personal privacy. Many loyal fans are unable to wait to find a completely avoid the government to monitor the virtual currency. On the basis of this background, anonymous virtual currency Dash (Zisha) Zcash (ZEC) and Zcoin (XZC) and other anonymous coins born, a lot of technical coins are playing anonymous concept, and in the virtual currency investment circle caused a great sensation, to the original Development team and absenteeism, investors bring excess returns.

With the anonymous coins technology in the ascendant, miners and virtual coin enthusiasts are also rushing to this technology, but for many virtual coin investors, the current anonymous coins really safe, according to the development team's team members revealed that some Anonymous coins so far cannot query the block chain, even without an encrypted wallet, individual anonymous coins appear black swan event. BHC team respect and pay tribute to the previous coveted team developers and their predecessors, we in a humble psychological development of anonymous coins, in respect of learning on the basis of more emphasis on improving the mechanism, so that the real concept of anonymous.

03.
Team

John Wilson
Software Engineer & Teaching Assistant

Stanford University
2015.09 - 2017.06 1 year and 10 months
Stanford, CA
- Winter 2015-2016, 2016-2017:
Teaching Assistant for CS142 - Web Applications
- Fall 2015-2016:
Teaching Assistant for CS251- Bitcoin and Crypto Currencies

Cryptography Researcher

Stanford University
2016.01 - 2017.03 1 year and 3 months
- Working on implementing optimized BLS signature library in C++.
- Exploring costs and benefits of using BLS signature aggregation in the Bitcoin protocol
- Explored feasibility of code isolation in Erlang and Elixir.

Software Engineer Internship

Airbnb
2016.06 - 2016.09 4 months
San Francisco Bay Area
- Product Security

Stanford University
2015 - 2017
- Master of Science (MS) Computer Science

04.

Advantage

Bitcoin and subsequent replacement coins try to enhance privacy anonymity through coin and ring signature techniques, but there is still a lack of. First, the coin and the signature node in the malicious or broken members are breaking the anonymous defense line breakthrough. Furthermore, anonymous technical architecture is the key to understanding the degree of privacy of encrypted money. The first two anonymous solutions are limited by the number of coins and the ring signature size. Each coin and ring signatures are limited by the number of transfers, which are then limited by the size of the virtual currency block chain. So the previous attempt can only guarantee the privacy of hundreds of transfer.

With the BHC, the anonymity has been significantly enhanced. Anonymous transfers are no longer limited, and their anonymous architecture has "minted coins" coinage. Anonymous transfer capacity of up to several million, enough to make the existing anonymous technology to become an ancient and backward representative. BHC to solve the problem encountered before the virtual currency. BHC uses the coin agreement, through the zero-knowledge encryption to achieve a complete anonymous. Zero knowledge proves that the goal of owning the BHC without knowing the identity of the owner. BHC through the wallet zerocoin protocol, re-generated BHC and then converted to track the BHC.

05.
Features

Any technology like the BHC may be used for good or bad aspects, but the development team firmly believes that good aspects will be much higher than bad aspects, through history, business freedom has proven to prevent war, promote prosperity, Cultural exchange. The BHC is intended to facilitate the existence of legitimate users who are already aware of the risk of using encrypted currency with a fully transparent public ledger and the risk of disclosing all of its financial details using Bitcoin.

Because there is already a pre-existing mechanism for such activities, the BHC does not affect the status of such activities, and it provides significant benefits for legitimate users.

Even if there is no BHC, there may be illegal transactions through the existing financial system. Bitcoin is also faced with a review of the regulatory authorities involved in money laundering. BHC can help ensure business freedom. People should be able to trade freely as long as it does not violate the well-being of others or personal freedom. We also believe that business freedom also promotes the peace and prosperity of nations and cultures. By ensuring financial privacy, BHC can directly guarantee interchangeability, which is a basic attribute of free business.

06.

Vision and planning

We want to promote a completely anonymous and cannot track the encrypted currency; it is Black Hole Coin - referred to as BHC, Chinese name black hole. It is an encrypted currency that uses zero-pass cryptography to protect transaction privacy.

Project development

May 7, 2017 landing in China, is the domestic promotion stage. Miners began zto enter the mining, May 23 BHC began to start ICO. Since landing in China, in the domestic virtual coins have been a huge response. A just launched the technical coins, just less than half a month, digging arithmetic reached the peak 11G, in the known anonymous currency, no one can so quickly reach such a high power. Which in itself also shows that this technology has been recognized by everyone, the technology has also experienced a lot of technology coins circle of repeated scrutiny. BHC total of 42 million, of which 12 million pre-excavation, mining 21 million, the remaining 9 million reserve ready pos, that is, posing wallet BHC, in order to dig money in the purse, the more money in the purse The increase in age, the more the digging the coins. Pre-dug 12 million BHC, the team has 2 million for the node plan and has been locked. BHC received $ 500,000 in early investment, and 10 million yuan for investors. The proceeds will be used for future BHC public relations, on the platform costs and BHC to change the more advanced algorithm required funds, the team did not take a point.

Planning risk

Encrypted money is an early and high-risk industry, investing and participating, need to be cautious and cautious, be careful and careful! As the nature of the currency book, there may be some attacks, timing attacks, such as force attack. However, these can be prevented and avoided, as long as the "coin coin" and "coin agreement spending" between a little longer, you can prevent timing attacks. And the team after the follow-up workload verification mechanism algorithm to the team in 2013 original GKS algorithm, this algorithm for the asymmetric encryption algorithm (also known as public key encryption algorithm), can resist GPU, FPGA, ASIC mine, to prevent 51% Attack, to ensure that the encrypted digital currency circulation algorithm is more secure. And the wallet increases to the center of the main node masternode reward system, further expand the optimization of anonymous transmission function, improve the real anonymous trading method.

07.

Why need your support

Features: 1, Black Hole Coin (BHC) is through the use of coin agreement (zerocoin protocol) to protect the privacy of an encrypted currency. It is the first to achieve the coin agreement of the encrypted currency, through the use of zero knowledge to ensure that the relevant information on both sides of the transaction from leakage.

Features: 2, with the BHC, the anonymity has been significantly strengthened. Anonymous transfers are no longer limited, and their anonymous architecture has "minted coins" coinage. Anonymous transfer capacity of up to several million, enough to make the existing anonymous technology to become an ancient and backward representatives. BHC to solve the problem encountered before the virtual currency. BHC uses the coin agreement, through the zero-knowledge encryption to achieve a complete anonymous. Zero knowledge proves that the goal of owning the BHC without knowing the identity of the owner. BHC through the wallet zerocoin protocol, the furnace generated BHC

Features: 3, compared to Dash, Monero and Zcash, black hole (BHC) is indeed the preferred solution for current anonymous transactions. We are also deeply aware that the anonymous implementation of black dongles has many advantages over other encrypted currencies, such as expansibility, audibility, anonymous setting and usability.

Features: 4, compared to Zcoin, the Zcoin team and its investors will receive 20% of the proceeds from mining, for a total of 2.1 million, four years before the first half. BHC to remove the founder of the reward, during which 20% of each output is still owned by miners.

Features: 5, BHC wallet has built-in block browser, making it easier to query block information.

Capital use: BHC received $ 500,000 in early investment, and 10 million yuan for investors. The proceeds will be used for future BHC public relations, on the platform costs and BHC to change the more advanced algorithm required funds, the team did not take a point.

The reason for the support: now the entire encrypted money area is really bustling, but only a few of them are substantial innovation, rather than simply cloning other encrypted currencies. We believe that only the original innovation and continuous development of the encrypted currency can survive, with the conservative competition in the influence of currency continued to decline and to support more innovative project development, we have witnessed the occurrence of all this. With the support of everyone, with a substantial innovation in the currency can be better development, encryption money industry can be better to flourish, diversified development, not just a few encrypted currency dominate the majority of the market.

Our commitment and return: The supporter of BHC, is out of the trust of the team, the team successfully completed all the chips, will give a certain reward, specific incentives (development team to write). Suggestions: you can get some of the coins from the coins to get feedback, then encounter problems, participate in the ICO players, the team priority to solve.

08.

Big event

In the past, the anonymous coins created a new era of virtual coins, but what was the original intention of developing anonymous coins, investment? Hype? We are in the virtual currency on the road to meditate on the road, the most fundamental purpose is circulation. An anonymous coin is first of all its technological innovation, and the most important reason is its liquidity. In the early stages of development, our team has individual team members to use its scarcity to speculation, but we finally give up the idea, individual members and investors also withdrew from the team, so that the progress of lagging behind, but we did not forget the beginning, Down. Would rather give up the immediate interests, but also to be perfect. Special thanks to the two Chinese and Australian students during the strong support of funds, because they require confidentiality, do not do a detailed description here.

09.

Other Innovations and Roadmap

Algorithm to ensure security

BHC current workload verification mechanism using the Lehman co-scrypt algorithm, the follow-up workload verification mechanism algorithm to the team in 2013 original GKS algorithm, this algorithm for the asymmetric encryption algorithm (also known as public key encryption algorithm), can resist the GPU, FPGA, ASIC mine, to prevent 51% attack, to ensure that encrypted digital currency circulation algorithm more secure.

Why scrypt algorithm

Zcoin is use lyra2Z algorithm and many other zcoin fork like Kurrent and hexxcoin are use X11 algorithm as proof of work.But another many GPU and ASIC miners want to mine altcoin with scrypt algorithm.Like Litecoin,scrypt is used by many altcoins and proven to be very stable and easy for miner.

Why BHC and not Zerocash

Zcash can hide the transfer amount, but the BHC does not have this feature. So relative to the BHC, Zcash is not vulnerable to timing attacks (side channel attacks), but also Zcash there may be undetectable infinite inflation issue issue. There are two major steps in the coin agreement: the first step: "coin", "Public coin" (open coins, no privacy attributes) into a data structure called the accumulator. The Accumulator Collector answers questions about whether a candidate is a member, without revealing membership. The second part is the "zero currency agreement spending" stage, the user can achieve zero knowledge to prove that someone in the accumulator with the currency without having to tell which currency. With the zero proof of the "coin agreement spending" proof, you can produce a completely no historical transaction record of the new BHC. Because each BHC in the adoption of "zero currency agreement to spend" to achieve anonymous before the need to implement the "coin coin", by analyzing the "coin coin" and "coin agreement spending" between the time to attack. It is possible for the user to carry out the "zero currency agreement" transfer immediately after the "coin coin" transfer, so assuming that there is such a behavior, the probability is assumed to be a "coin coin" with a specific "zero Currency agreement spending "associated. However, as long as the "coin coin" and "coin agreement spending" between a little longer, you can prevent timing attacks.

Why BHC and not Zerocash

Because ZCash hides the number of transfers, it can be more effective against timing attacks than the BHC. But also bring a greater risk:In essence, there is no "scarcity" for Zcash, and few have been able to prove it on the basis of the first principle of mathematics / cryptography. Zk-Snark uses extremely complex cryptography. Only a handful of encryption experts can understand the ZK-Snarks principle. The principle of encryption behind the coin protocol has a long time, and the coin protocol paper is also a frequent visitor of recent years. And most of the encryption academic experts can understand the principle of coin agreement. Zcahs' bug is that someone can print unlimited money, and no one can know. Using this bug, you can infinite money supply and manipulate the market. There are many examples of the collapse caused by changing the money supply. The most typical case is the 2010 value of the value of overflow (value overflow) bug, the bug to make the total amount of Bitcoat 90 billion.

August 15, 2010, Bitcoin 74638 block, a 184,467,440,737.09551616 bit currency transfer design three addresses. 2 addresses received 92.2 billion bits of currency, and find the block of people are more than the previous does not exist 0.01 bit currency. According to technical staff analysis, hackers are through the use of large integer overflow vulnerability, bypassing the system balance check, the successful implementation of the attack "

In Zcash, this bug is quiet and unobtrusive. If Zcash has a similar bug, then in the case of no one knows, a person will be able to have 99.9% of the Zcash market value.

The last example of the encrypted currency bug is The DAO, brutally hackers worth $ 50 million tokens attack.

In the okTurtle blog, Greg Slepak wrote. However, this situation is more serious than the DAO, Zcash code than the DAO complex degree out of several index level, the failure of the index is also a high level of serious. Zcash's current situation is: it is impossible to know whether the attack is successful. Unless the saboteurs themselves warn, we can know that Zcash has been attacked and the boat has gone. The higher the value of Zcash, the higher the risk. There is no retracement at all.

In addition to the original bug, there is another problem. Because ZK-Snarks high-cold technology, Zerocash for the bottom of the basic principles of cryptography few peer review possible. But the BHC did not worry about this. There are few academic experts who understand the theory of Zcash cryptography. If the temptation of millions of dollars, that is, the most noble academic experts may also cross the moral boundaries. In contrast, BHC even if there are bugs, but also in the sun, everyone can know the total did not change.

On the other hand, the BHC mechanism is weakened by the risk factor: everyone can see the supply of BHC. But by contrast, if Zcash is broken, no one can detect the circulation of super inflation.

Zcash relies on the assumption that all encryption algorithm parameter generators are not conspiracy to do evil. As long as there is a fair not evil, then safe and sound. Otherwise they can be any double flower.

10.
Others

Project positioning
New arrogant coins, safe, transparent, fast confirmation, wallet built-in block query, graphics, CPU, mining can be mine, so that everyone can participate. Thus reflecting its core values -universal.

Project progress
May 7, 2017 landing in China, is the domestic promotion stage. Miners began to enter the mining. The current team at home and abroad have a strong reputation of the platform ready to land Owned users / members: Members to reach 1,000 people, are real players fans, coins circle miners flocked, calculate the peak power to 11G, more than a small zero of the arithmetic.

Mobile Wallet

Black Hole Coin

BHC FOUNDATION

www.blackholecoin.io