WE HOST THE WORLD

ABSTRACT

Ever since Satoshi Nakamoto released the whitepaper and respective software for Bitcoin, the cryptocurrency ecosystem has continued to grow at a rapid pace. Bitcoin created a platform that anyone could use to transfer funds across the internet without middlemen, banks or counterparty risk. However, once blockchain consensus technology had become deep-rooted and stable, the debate around whether blockchain technology could also be used to enable functions other than the transfer of value.

OVERVIEW

Cryptocurrencies are digital assets equipped to work as a medium of exchange which uses cryptography to secure its transactions and regulate the creation of additional units. It also authenticates these transfers. As opposed to conventional money transfer and banking systems (in which centralized control is owned by single party), cryptocurrency uses a decentralized structure. The control of each cryptocurrency works through a blockchain – a public transaction database. The blockchain functions as distributed ledger, making counterfeit impossible. Cryptocurrencies have emerged as the latest asset class, and trading in these markets are often full exploitation, illiquidity and volatility. The fact that some coins like Bitcoin can rise by 15% in a single day signifies the need for other stablecoins to join the market. The tender age of the cryptocurrency trading world has prevented established trading houses and mainstream investment entities from

involving themselves, but the overall market capitalization for cryptocurrency stands at $200+ billion and still growing. This further signifies the availability of favorable circumstances for young traders to venture in the market and make profit.

RELEVANCE

The blockchain is an undeniably ingenious invention: the brainchild of a person (or group of people known by the pseudonym) Satoshi Nakamoto. Since then, it has evolved into something greater. By allowing digital information to be distributed but not copied, blockchain technology created the backbone of a new type of internet. The creator of Bitcoin solved the 'double spend' problem: the issue that digital information can easily be copied, and therefore a centralized authority was previously required to reflect where funds were located. Originally devised for the digital currency, Bitcoin, the tech community is now finding other potential uses for the platform. Blockchain or Distributed Ledger Technology (DLT) offers a radically different paradigm of storing and managing information online. Decentralized ledgers lack a central point of failure and the associated security issues of traditional databases and top-down protocols, whilst at the same time pose their own unique challenges for effective deployment and maintenance. The advantages in terms of costs, transparency, immutability, security and confidence that are characteristic of blockchain solutions mean that financial businesses, governments and other organizations are exploring applications of all kinds with a view to delivering services more profitably and efficiently.

However, reliable deployment of a new blockchain fit for purpose entails extensive overheads in terms of network infrastructure, development, security and ongoing maintenance. Moreover, use of an existing blockchain (such as Bitcoin) comes with numerous problems for a mainstream business, not least because users have no control over blockchain features or future development. The decentralized structure of the blockchain brings several key features in contrast to traditional centralized approaches:

Transparency it is possible for anyone to track the movement of funds from one account to another.
Immutability once confirmed, a transaction cannot be reversed. No one can interfere with a completed transfer.
Low cost transaction fees are minimal.
Cross-border funds can be sent as easily to someone on the other side of the world as they can to someone in the next room.
Speed due to the flat and transparent nature of the blockchain, transfers show up almost instantly and are typically confirmed in minutes, rather than hours or days.

CONSENSUS ALGORITHM

Consensus is the process by which a community comes to a universally recognized, unambiguous agreement on a piece of information. There are many algorithms society has developed for reaching consensus about who owns what. Every government on earth is a primitive consensus algorithm whereby the population agrees to abide by a certain set of rules enshrined in a constitution. Governments establish courts, judges, and juries to interpret the subjective facts and render a final decision. Most of

the time, people abide by the decision even if they disagree. The algorithms used by cryptocurrencies provide a better way to reach consensus. Cryptographically signed testimony from individuals is recorded in a public ledger that establishes the absolute global order of events. A deterministic computer algorithm can then process this ledger to derive a universally accepted conclusion. So long as the members of a community agree on the processing algorithm, the result of the algorithm is authoritative. The primary consideration is determining what testimony is allowed to enter the public record. Systems should be designed to minimize the potential for censorship. Censorship on the public ledger is similar to preventing someone from voting in an election. In both cases an individual is prevented from impacting the global consensus.

ZEROCOIN PROTOCOL

Zerocoin was designed to achieve anonymity through the use of two operations called “mint” and “spend”. The mint operation produces a zerocoin with a public coin and a secret key. In all of the aforementioned currencies, you can perform a mint transaction that gives up one regular coin of a base currency (e.g., one hexxcoin) to be allowed to mint one zerocoin. So a mint operation basically allows you to exchange one regular coin for one zerocoin. The second operation is called “spend”. If you spend a zerocoin, you provide a proof that you are the owner of a zerocoin (technically, that you know the secret key) and authorize the spending. This is where the anonymity comes into play: The proof that you provide when spending is a zero-knowledge proof and it hides which zerocoin in the blockchain is spent.

Instead of telling the world that a particular zerocoin is spent, the proof reveals only that the person is eligible to spend one zerocoin, but without telling which one it is — it could be any of the minted coins in the blockchain.

PREVENTING DOUBLE-SPENDING

The basic idea raises the impression that double-spending is easily possible. If verifiers do not know which zerocoin is spent, how can they verify that the current zerocoin was not spent before? The solution to this problem is that each zerocoin has a supposedly unique serial number. Only when you spend a zerocoin, the protocol requires you to reveal this serial number and to prove in zero-knowledge that it is the right serial number. Now verifiers can just keep a set of already used serial numbers. If they see a spend transaction with a serial number, which has already been recorded in the set of used serial numbers, they know that this transaction is a double-spend and invalid.

POS & ZPOS ALGORITHM

PProof-of-stake (PoS) is a method designed to solve the biggest drawbacks of proof-of-work (PoW), namely security issues caused by hash monopolization and high cost for the purchase of equipment and their maintenance. For PoS, the higher the stake proportion for the entire coin supply, the higher the acquisition amount for the additional coins issued. In other words, the role of “hash” in the PoW method is equivalent to the role of “stake” in the PoS

method. More simply, it can be conceived as being similar to bank interest. In addition, the PoS method can also achieve strong security just by linking multiple wallets that keep coins inside. In recent years, coins based on the PoS method have been increasing and existing coins are also changing from the POW method to PoS method. Ethereum is a perfect example of this. We use zPoS (zerocoin Proof of Stake), which will be the very few private staking system on the market. In the zerocoin privacy mechanism, you “burn” your coins and get proof of that burn which can later be redeemed for brand new coins. They are called zPoS coins because while they don’t exist on the chain, they are as good as coins when they are redeemed. Your coins are held off the chain and it doesn’t get much more private than that. In normal PoS, you are “mining” with your coins and your staking weight is pegged to your wallet’s balance. In zPoS, you are staking with these off-chain coins. It’s pretty nuts.

MASTERNODE

Masternodes are nodes running the same wallet software on the same blockchain to provide extra services to the network. These services include:

Anonymization increased privacy of transactions
Instant transactions
A decentralised governance
A decentralised budgeting system
Immutable proposal and voting systems

For such services, masternodes are also paid a portion of the reward for each block. This can serve as a passive income to the masternode owners minus their running cost. Investing in Masternode coins gives you the ability of not only being an investor, but part of the decision makers in shaping the coin advancement. Owning one gives a voice to an investor and allows the owner to submit proposals. The foundation of Masternodes is stable and has long-term values at the core of the infrastructure. The founding investors have committed their money for a long term making it stable and increases trust among investors. Investors get capital gains by just running the Masternode services. On top of that, investors are paid in that coin as rewards from each block found. The availability of a stronger community supports the sustainability of a project. This in turn ensures that energy is focused on the project's long-term future instead of pump and dump cycles. Masternodes get constant rewards that are proportionately are allocated among peer reviewed Masternodes. Masternodes continuously check the activity of the peer node, and rewards are only given to high performing nodes having stable high speed internet 5 connections. On top of the block reward, a Masternode gets all public transactions fees done in a block and fees for all private transaction pools started in the block. These inducements encourage uninterrupted connectivity to sustain a high performance network.

WEB HOSTING

Currently, web hosting entails paying a company to store a website's files on a server connected to the internet. Pricing includes the cost of a domain name and a monthly price is

based on the bandwidth and computing resources needed for operation of the site. For small, personal websites, shared hosting (sharing space on a server with other sites) will usually suffice. For businesses and larger enterprises with a complex site and a lot of traffic must use either VPS (Virtual Private Servers) or cloud hosting. VPS hosting involves paying a hosting company for dedicated use of their servers, whereas cloud hosting such as AWS (Amazon Web Services) involves only renting the space you need on a "virtual" server instead of paying to use a physical one. The primary issue with web hosting in its current form is that is incredibly expensive, potentially thousands of dollars per month are spent solely on file hosting. Maintenance and additional security incur further expense. This makes it incredibly difficult for small or medium-sized businesses to have a strong web presence without incurring significant costs. Bithost will be a solution to those high costs and security issues, while still providing the same quality of service. Users will be able to pay with the Bithost asset for hosting service options and switch between these options effortlessly.

BITHOST

BitHost is a fully decentralized cryptocurrency built on the premise of providing anonymity, speed, and reliability through Proof of Stake and Masternodes. By using the Private Send feature, you can transfer assets in a secure and private manner. Bithost also offers InstaSend, enables almost-instant transactions in our network.

BITHOST
A WAY OF HOSTING THE WORLD

BitHost offers IT infrastructure services to businesses via web services — now commonly known as cloud computing. One of the key benefits of cloud computing is that it enables consumers to replace up-front capital infrastructure expenses with low variable costs that scale with business growth. With the cloud, businesses no longer need to plan for and procure servers and other IT infrastructure weeks or months in advance. Instead, they can instantly deploy hundreds or thousands of servers within minutes and deliver results much faster.

Our plan is to build the premier “next generation” hosting and domain service on the blockchain, while also providing normal options like SSL and email. We at BitHost feel that it is time for this technology disrupt the hosting industry as is already underway in the financial and tech service industries. BitHost hosting will have a higher level of security than traditional models and fully intends to compete with the larger hosting and domain service providers in the industry through innovation.

ADVANTAGES

1. More secure SSL.
2. Faster server times.
3. Reinvents the domain.
4. Instant domain transfer to another hosting server
5. Control over your data, i.e., it is not given in the hands of central administrators.

MASTER NODE HOSTING BY SINGLE CLICK

Hosting/shared/parallel masternodes will create a universal platform on which the possibility to customize a masternode is possible in a single click. This platform will include not only easy customization but also a masternode hosting system (that allows maximum protection) and parallel masternodes. Hereafter we are planning to integrate this service with other coins, whose owners will get rewards in BitHost, thereby supporting upward buy pressure.

BITHOSTLIVE.COM

Bithostlive is a platform where people can host masternodes effortlessly and allow you to create and maintain cold wallet masternodes for most coins, without need to deal with servers, terminals, Linux, etc. This reduces the barrier to the masternodes market for both technical and non-technical people.
Setting up a masternode by yourself can be a difficult and time consuming process. Let us save this time, energy and also money by makin sure your masternode is always online, and wallet software is up to date. Never worry about missing income due to downtime or incorrectly configured software. Just earn and enjoy!

SHARED MASTERNODE SERVICE

In the past, investors have found that running a masternode can be quite profitable. Limitations in funding puts a barrier

against those with a larger collateral requirement, however, so a shared masternode arrangement was devised with other community members. Investors experiences have proven overwhelmingly positive in this situation.
If you would like to own a (partial) masternode of a coin (but don't have the necessary funds), the solution is our shared masternode service, which enables you to earn some rewards along with like-minded coin enthusiasts.

DECENTRALIZED AUTOMATED MASTERNODE SERVICE

We are planned to establish decentralized masternode services as well. Once the masternode service is built it can further be decentralized, increasing network security. You can also access your masternodes from anywhere.

ECOMMERCE MARKET PLACE FOR HOSTING SERVICES WITH BITHOST COIN

The Ecommerce marketplace enables the investors to bridge their services from different platforms and is simply accessed from different platforms.

Technical requirements

For each type of masternode we host all require the user to run a wallet. Novice investors mistakenly believe that keeping their coins on an exchange, but such is not the case.

Advantages of remotely hosting a masternode

You don't have to worry about any maintenance or updates or your internet IP address changing. We maintain many redundancies for power failures and internet outage to ensure consistent service cost effectiveness.

Specific technical requirements

Only a working wallet with the required collateral is needed. we can take it from there.

Non-technical service

We have fine-tuned the end user instructions. When setting up a BitHost masternode, we want anyone to be able to set it up with ease.

Trust in online status

Every wallet has a section which will show their masternode status, and some coins even have a website to monitor its nodes.

New masternode types

We are on the lookout for projects with good cost to benefit rations and seek to support the most profitable masternodes. Every masternode shares basic resources such as processors, memory, bandwidth, disk space, and a static IP. We're continually evaluating new opportunities to add to the platform.

MASTERNODE USING POS METHOD

Masternodes are often secured first through mining initially, and later change to a Proof-of-stake method. In mining, block generation time varies according to mining difficulty, and the mining output also changes according to the number of masternodes formed in the blockchain. In general, masternode coins are hybrid in the sense that they consist of both POW and POS methods. They will follow the POW method up to a specific block and subsequently change to the POS method after that.

THE PROBLEM

BitHost is a masternode mediation platform that enables the entire spectrum of users to have easy access to a two-tier incentivized network, also known as the “Masternode Network”. Hosting a masternode is quite out of reach for many individual investors since most masternodes require substantial capital and intricate software engineering to set up. By aiding individuals come together to form a whole masternode, we will be able to encourage more people to participate in masternode investments as well as provide them with a much safer investment channel rather than investing in the exchange market without adequate knowledge.

WHY INVEST IN BITHOST COIN

BitHost coin is a currency that invests in the power of people. It provides a simple wallet setup option for both staking and Masternodes. This coin has over 80% Pure MN block reward phase which is optimal for investment. The masternode network takes advantage of market inefficiency by giving the people the power to shape the coin's future. The concept of giving the coin owners the power to shape the coin's future means that its yield is proportional to the people's effort.

BLOCK REWARD STRUCTURE

Block Start	Block End	Block Reward	MN%	POS%
101	5000	3	80	20
5001	10000	5	80	20
10001	18000	8	80.5	19.5
18001	36000	12	81	19
36001	50000	15	81.5	18.5
50001	64000	18	82	18
64001	80000	21	82.5	17.5
80001	100000	24	83	17
100001	124000	30	83.5	16.5
124001	142000	33	84	16
143001	160000	36	84.5	15.5
160001	184000	39	85	15
184001	200000	42	85.5	14.5
200001	225000	39	86	14
225001	242000	36	86.5	13.5
242001	264000	33	87	13
264001	284000	30	87.5	12.5
284001	300000	27	88	12
300001	500000	24	88.5	11.5
500001	600000	23	89	11
600001	700000	22	89.5	10.5
700001	1000000	21	90	10
1000001	2000000	20	90	10
2000001	2500000	19	90	10
2500001	2600000	18	90	10
2600001	2700000	15	90	10
2700001	2810328	12	90	10
2810328		1	90	10
	Total Coin 60M			
	Block Time 60 Secsonds			