WHITE PAPER™

ziftrCOIN :
A Cryptocurrency to Enable Commerce

WHITE PAPER Released October 9, 2014, updated December 6, 2014

Follow us on Twitter for the latest on @ziftrCOIN

Abstract

In this paper we introduce the technical specification for a new cryptocurrency aimed at simplifying the process for everyday people to acquire and use digital currency. While several digital currencies have demonstrated that serious implementations, such as Bitcoin and Peercoin, really can be useful tools with intrinsic value, there remain practical problems that need to be addressed in order to support widespread commercial use of digital currencies. We propose a new digital currency that builds on the best features of the digital currencies that have come before, increases security, enables the network to come to a consensus more quickly, and strengthens decentralization via a protocol we call Sign to Mine™. To support our digital currency, we will develop helpful online shopping tools and APIs in order to address problems affecting both individuals and organizations seeking to use digital currency.

TABLE OF CONTENTS

1.0 What is Digital Currency?

Paper money and coins are abstract representations of value in the form of paper or metal that are managed by a government authority. Because they are managed by a government, they are also known as fiat currency. Checks, credit cards, and electronic transfers extend the abstraction of value to the digital realm, but require the support of trusted authorities in the form of banks and credit agencies. Digital currencies (cryptocurrencies) are a further abstraction of value quite similar to credit cards and electronic transfers, but different from fiat currency by not being intrinsically tied to a government issued currency and not requiring the support of a central financial agency such as a government, bank, or credit card agency.

Banks allow the safe storage of money when it is either impractical or undesirable to carry all your money with you. Banks and credit card companies work together to support credit cards, which allow consumers both to carry much less (if any) physical cash and to transact with a vendor without actually being physically present at the vendor's location. Digital currencies address the same set of needs without involving any centralized and trusted authority in the transactions by using a specific algorithm for achieving consensus that a transaction can be trusted. The lack of dependence on a central financial authority makes it an attractive financial tool for those wishing to avoid financial risks due to unscrupulous bankers or governments, vendors and individuals who must pay high fees to financial institutions for their service, and individuals who do not have bank accounts.

2.0 On Network Consensus

2.1 THE BYZANTINE GENERALS' PROBLEM

Operating without the use of a centralized entity, however, has its disadvantages. In particular, it is hard to come to distributed consensus about the true state of the system. Bitcoin was the first financial program to solve the distributed consensus problem, known more generally as the Byzantine Generals' Problem.

In this problem, a group of generals surrounds a city and wishes to attack the city but needs a majority of the generals to commit to attacking at the same time in order to launch a successful attack. To communicate, the generals send messengers to one another, which in turn creates a delay between when messages are sent and when they are received. In addition, some generals actually seek to thwart the attack and thus will not relay messages or will possibly even relay fabricated messages. The Byzantine Generals' problem is to find a decision making algorithm for deciding when to attack the city such that, even with a few bad actors in their midst and high latency in their communication, a majority of generals can still come to a consensus about the correct time to attack.

The parallel problem in the digital realm involves a group of hackers ready to devote their computing power to cracking a password by brute force. In order to be successful, the hackers need to apply a majority of their computing power at the same time to ensure they will crack the password, as they will have a small interval of time after they start to make attempts before they are noticed and locked out. Like the generals, their communication is done through a network which has non-negligible latency and there are a few hackers in their midst who wish to thwart their attack.

The Bitcoin protocol provides a solution to this problem, allowing a distributed group of mostly honest individuals with latency in their communication to come to a consensus. Bitcoin does this by using "Proof of Work" (PoW) puzzles to prove that nodes have access to computing power and to show others in the network what the owner of that computing power believes is the current state of the system (their proposed consensus). If nodes agree with a proposed consensus created by another node, they can solve another PoW puzzle built upon that proposed consensus to show their computing power is dedicated to the same proposal. In addition, if a proposal is altered by a dishonest node while relaying a message, then the PoW puzzles will no longer be valid and the node receiving the message will know that the message was relayed incorrectly. When enough nodes have solved linked PoW puzzles, each node can individually see what the consensus of the network is by looking for the proposal with the longest chain of solved PoW puzzles.

2.2 TRANSACTION MATURITY AND BLOCK GENERATION RATE

While solving the Byzantine Generals' Problem is a remarkable theoretical advancement in itself, the Bitcoin protocol can also be used to come to a consensus on any number of things, including a consensus on ownership of currency. One of the greatest problems with the current protocol, however, is that making a transaction and then waiting for the network to obtain a consensus on the new ownership of currency takes longer than it does in standard transactions using fiat currency. We propose a novel way to allow the network to come to a consensus at a much faster rate.

After a transaction is announced to the Bitcoin network, the sender must wait 5 minutes (on average) for their transaction to be verified by miners through inclusion in a block. Once a transaction has been included in a block, it is said to have 1 confirmation, and is considered by most to be mature (irreversible). Although different entities have different block depth requirements before considering a transaction safe to not be reversed, at least one block is always needed to be considered secure.

Blocks are generated at different frequencies in various cryptocurrencies. Selecting a target block generation time involves a tradeoff between quickly confirming transactions and the ability of the network to come to a consensus. If the target block generation time is too long, then blocks are generated infrequently and it takes an inconvenient length of time before transactions are considered mature. Conversely, if the target block generation time is too short, then it is more likely that blocks will be solved nearly simultaneously. This causes the network to split its time mining on both chains, on which more simultaneous blocks may be solved, and the effect can sometimes be a tree of blocks rather than the desired linear chain of blocks. See figure 1 for a diagram showing the branching effect in the block chain.

A tree of blocks is undesirable because nodes can be working on different branches which contain different transaction sets, and thus a consensus is not achieved. Furthermore, nodes will not accept transactions that reference Unspent Transaction Outputs (UTXOs) which exist on other branches, causing the system to be incompatible between some parties. When this happens, the system is essentially rendered useless as no consensus is ever achieved.

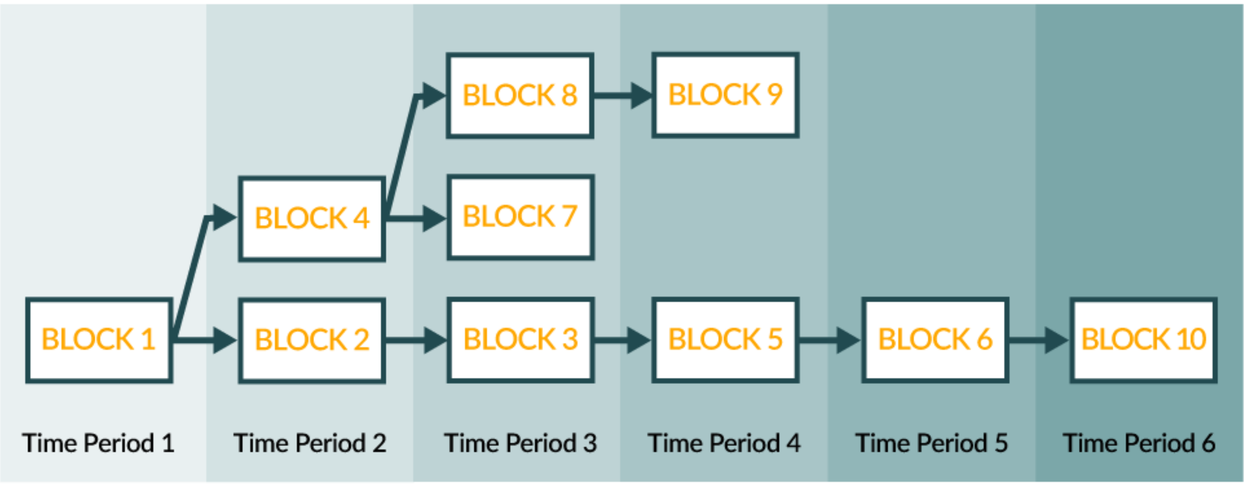


FIGURE 1: A block chain can become a 'blocktree' due to a branching effect if blocks are generated too quickly. Image source: [1]

The Bitcoin developer(s) chose a 10-minute target block generation rate likely because obtaining a consensus was valued over convenience. This has made the system very robust and transactions can almost surely be trusted not to be reversed after 1-2 confirmations (inclusions within a block). However, for many places where currency is used, it is infeasible to wait 10+ minutes before accepting a transaction. We propose a system that will allow transactions to become confirmed more quickly and stymie the creation of many branches through the use of a tiebreaking procedure that compares the amount of coin age destroyed.

2.3 COIN AGE DESTROYED

Coin age is simply the product of the amount and the age of a UTXO, typically measured in coin-days. Standard Proof of Stake (PoS) uses coin age destroyed as a substitute for hashing power because, similar to hashing power, it is hard to obtain, can only be used once before it is destroyed, and those with a greater amount are likely to be trustworthy as they have significant stake in the success of the system. That is, they have a considerable amount to lose if the system fails, so it can be expected that they would not take any actions that would make the system more likely to fail.

When UTXOs are used in a new transaction, any coin age that had accumulated is destroyed. We propose using this destroyed coin age as a tiebreaker in our PoW coin to encourage the network to come to a consensus quickly in the event of a tie.

2.4 COIN AGE DESTROYED AS A TIEBREAKER

We will use coin age destroyed as a tie breaker in the event that two blocks are solved at roughly the same time. Under our system, the node with the most stake in the system is the one that wins in the event of a tie. When nodes hear of a new solved block, they essentially start a 13-second timer. If before the timer ends they hear about a new block and the new block contains more destroyed coin age than the previous block contained, then the node will choose it as the new correct chain. The goal is that when honest nodes hear about two (or more) new blocks within a short time period, they will all pick the same new block and broadcast it to their peers. This allows the network to quickly decide which is the correct block in the event of a tie and come to a consensus more quickly.

It is possible that some nodes will hear about blocks within their 13-second limit and others will not. In this case, some nodes will be mining on chains that are unlikely to ever be accepted by the network. In the case of Bitcoin, however, some nodes mine on stale blocks nearly every time there is a tie. Under our system, it should theoretically happen much less frequently.

It may be the case that multiple new solved blocks have the same amount of destroyed coin age and, thus, nodes have no way of breaking the tie between the two solved blocks. If this were to happen, then nodes would choose the block they received first as their correct block. However, this will not be very likely to happen because miners can destroy coin age in their coinbase transaction as well (which is different from miner to miner). It is advantageous for a miner to do this, as it increases the chances that their block will be accepted in the case of a tie. Now miners must compete to accumulate both hashing power and coin age, where hashing power allows them to solve blocks and coin age lets them win in the case of a tie. Since we will use a quite low target block generation frequency (on the order of one new block per minute), ties will actually be far more frequent than they are in Bitcoin. Thus, miners will compete for coin age regularly as their block reward will depend on it.

2.5 INCENTIVIZING MINERS TO INCLUDE TRANSACTIONS

In Bitcoin, there is currently no real incentive for miners to include transactions other than benevolent intent to increase confidence in Bitcoin. The fees that are provided in Bitcoin provide little incentive themselves, as fees typically total roughly 0.1 BTC, just 0.4% of the approximately 25.1 BTC rewarded for solving a block. In fact, miners are typically disincentivized from including transactions because doing so creates larger blocks to distribute to one's peers, and therefore a greater propagation time. This is a problem for Bitcoin miners because a larger propagation time causes a greater chance for blocks to be rejected in the event of a tie.

This is not an abstract theoretical threat to the network. This threat is real enough that within the Bitcoin network, there are frequently miners which don't include any transactions other than their own coinbase transaction (with the 25 BTC reward) so as to have the lowest propagation time possible. At the time of writing, the block chain is 315,126 blocks long and we need only go back to block 315,076 [2] to find a block that contains no other transactions other than its coinbase transaction. If all miners were this selfish, the Bitcoin system would fail to verify transactions and the entire system would fail to be useful.

Our system will reverse this incentive scheme, creating an incentive for miners to verify transactions for the network. Using coin age destroyed as a tiebreaker incentivizes miners to include transactions that add destroyed coin age to their block because if they do, their blocks will actually be more likely to be chosen in the event of a tie.

2.6 LIMITING EXCESSIVE FEES

An interesting benefit of using destroyed coin age as a tiebreaking measure is that we are now in a position to partially eliminate fees for users of our coin. It is no secret that users of any system hate fees, though they are a necessary component to almost any service. In cryptocurrency, however, fees are mostly a spam-prevention measure rather than a way for miners to gain significant profit. As mentioned above, fees typically account for roughly 0.4% of a miner's reward in Bitcoin.

Rather than using loss of currency as a way to prevent spam, however, we can now use destroyed coin age. Miners will include transactions in their block if they have a fee OR if they contribute to the destroyed coin age for their block. Both provide the miner some benefit, the fee being a monetary gain and the destroyed coin age causing the miner's block to be chosen in the event of a tie. Since there is only a finite amount of coin age in a cryptocurrency at any one time and it becomes used up once it is utilized in a transaction, this can stand as a viable replacement for fees. If a user does not have any coin age accumulated in their wallet, then they will likely have to provide the standard transaction fee to the miners in order to have a miner include their transaction in a block in a timely fashion.

3.0 A Return to Decentralization

In June of 2014, GHash.io, one of the largest Bitcoin mining pools, had more than 50% of the mining power for a sustained period of time [3]. GHash.io also has a history of double spend attacks [4], making its dominance even more threatening. Whenever a single entity has control over the majority of the mining power, it threatens the very thing that makes cryptocurrencies so indestructible and useful: decentralization. Without decentralization, we may as well designate a trusted authority, start using a massive database, and save all the energy that is currently being expended upon mining.

When large pools like GHash.io obtain 50% or more of the network's hashing power, it opens the system up to many attacks ranging from 51% attacks to Double Spends. Although most pools are not likely to commit such an attack, other more subtle attacks may be conducted without notice. For example, pools can falsely report shares of non-existent miners to claim more than the designated pool operation fee. Pool participants trust the pool operator not to do this, but it would be very hard to detect if it were actually done.

There are many proposals to limit the size of pools. One proposal from Ittay Eyal and Emin Gün Sirer, of Cornell University, is known as Two Phase Proof of Work (2P-PoW) [5]. The first part of these two phases is to maintain backwards compatibility with the current Bitcoin PoW protocol. In our coin, however, we will have no need for such backwards compatibility, so we will use an algorithm similar to the second phase of Eyal and Sirer's proposal, an algorithm which we have named Sign to Mine™.

3.1 SIGN TO MINE™

Sign to Mine™ (S2M) is a mining algorithm that requires the miner who solves a block to be able also to spend the reward for that block. Under this system, a pool with many anonymous miners would not be feasible because all miners in the pool would be able to accept rewards according to their shares when others solve a block, but then abscond with the whole block reward when they are the one to solve a block. Thus, a certain level of trust should be established before allowing a miner into one's pool. Instead of miners in a pool only trusting the pool operator, as is the case for current pools, with S2M all members of a pool must trust all other members of the pool.

S2M works by adding a `headerSig` field to the block header. The miner produces a signature for the contents of the block header (everything except the signature field) and the signature is verified when the miner attempts to spend the block reward. In addition, the coinbase (block reward) transaction must be sent to only one Pay-to-Pubkey-Hash address. When validating transactions that spend a coinbase reward, honest nodes verify that the public key given in the `scriptSig` script can both be used to verify the signature of the solved block and corresponds to the address the coins were sent to in the coinbase transaction. In addition, nodes should also verify that all spending of coinbase rewards happen at least 1,000 blocks after the block was solved.

For the reader who is familiar with cryptocurrency, it may not come as a surprise that the header does not also contain the public key which may verify the signature and the receiving address in the coinbase transaction. Just as most standard Bitcoin transactions do not reveal the public key until an address is spent from, we also choose not to reveal the public key in S2M until absolutely necessary. The benefits of this are twofold. First, not including the public key requires less storage space for block headers. Second, the security of the system is also increased by not revealing the public key until necessary. Even if `Secp256k1`, the Elliptic Curve that most cryptocurrencies use, were ever compromised, attackers would still have a very small time period to derive the private key from the public key before the money could be transferred.

One benefit of this addition to the block header is that PoW blocks no longer require a nonce field because the Elliptic Curve Digital Signature Algorithm (ECDSA) is non-deterministic. Rather, one can simply repeatedly sign the same block header and double hash the result until the resulting hash is below a certain threshold. The range of possible signatures is much greater than the range of possible 32 bit nonces, so there won't be any need for the extraNonce in coinbase transactions.

3.2 THE NEED FOR POOLS

Pools are not entirely bad. They provide a genuinely useful service in that they limit the variance of rewards for miners. That is, rather than receiving large rewards at infrequent intervals, miners can instead receive smaller rewards at more frequent intervals. We seek to establish a way to minimize the variance of rewards for miners even though we place serious limitations on the size of pools through S2M.

One way that our coin will minimize the variance of rewards is simply by distributing rewards more frequently. Our coin will have a block generation rate of 1 block per minute, which means that rewards will be distributed approximately 10 times more frequently than they currently are in Bitcoin. However, this still may not reward miners at sufficiently frequent intervals. To fill this void, we have devised a way to allow decentralized pools. As alluded to above, members using this pooling software should ensure that they trust those with whom they mine. We will facilitate this exchange of trust through a social mining platform website that will help to gauge the trustworthiness of its users.

3.3 SOCIAL POOLS

Pools can still be created even with the Sign to Mine™ algorithm. Rather than the few large pools that currently exist in Bitcoin, however, there will be many more dynamic small pools. To facilitate this, we have a devoted server whose job it is to create private/public key pairs for each member of a pool and distribute them. The server keeps track of work done by each miner and distributes the reward when nodes actually solve blocks. It is able to do this because it has access to the private keys that were originally distributed to each of the miners. See figure 2 on page 13 for a visualization of key distribution.

If a user does misbehave and try to spend the coins before the server can distribute the reward, then the server will be able to see which key was used to spend the coins and alert the other pool members to which member has stolen the coins from the pool.

3.4 SELFISH MINING

One possible flaw in our system is that nodes may profit disproportionately from their hashing power by engaging in what has become known as Selfish

Mining. Introduced by Ittay Eyal and Emin Gün Sirer [6], Selfish Mining involves solving blocks and then waiting to make them public until the last possible second that the block could still be accepted, causing others to waste their hashing power mining blocks that will eventually be orphaned. This attack could be exacerbated in our system because selfishly waiting to release blocks until others are released and true block discovery ties are indistinguishable.

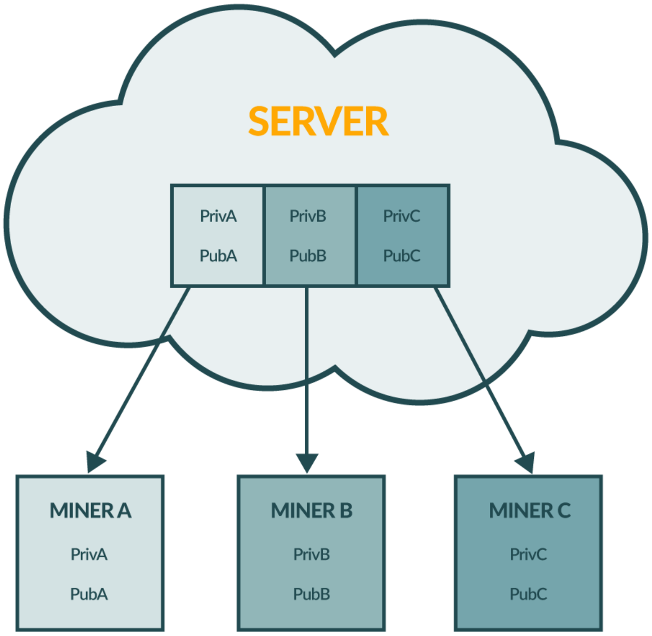


FIGURE 2: Pool server distributes private keys that are used to mine.

However, although this type of attack has been made slightly easier in one way, we also increase the difficulty of this attack in another way. Under our system, attackers now need large amounts of hashing power and coin age to destroy. To successfully take advantage of Selfish Mining, the malicious miner must save up more coin age than is typically destroyed in a block and be fortunate enough to produce blocks faster than the rest of the network. Both of these are serious limitations that, together, make this attack unlikely to be a serious issue. In addition, it is important to note that this attack does not disturb the security of the system. Although it could theoretically give pools a slightly higher than expected revenue, it causes no real issues for users of our coin.

4.0 Scalability

Arguably, the scalability of the Bitcoin protocol is seen as one of the largest inhibitors to Bitcoin adoption. The three problems in particular that plague the Bitcoin community are the ever increasing block chain size, the 10 transactions/second limit, and the inability for new nodes to participate without first processing the block chain for weeks on end. The first problem we accept as an essential part of cryptocurrency. For the latter two, however, we propose new and innovative solutions.

4.1 A GROWTH-DEPENDENT BLOCK SIZE LIMIT

The Bitcoin protocol currently places an arbitrary block size limit of 1MB to prevent DOS attacks caused by malicious miners distributing extremely large blocks. This is a short-sighted limit, not allowing for wide acceptance of the currency. For instance, the Bitcoin network could not process 10,000 transactions/second, as Visa is designed to handle [7]. In fact, the 1MB limit imposes roughly a 10 transactions/second limit on the system [8], effectively limiting the growth of Bitcoin.

We will remove this hard limit in favor of a growth-dependent maximum block size. There must be a limit to prevent attackers from artificially bloating the block chain, but this limit should change with time as the coin becomes more widely accepted. We will allow blocks that are up to 200% of the median of the last 100 blocks. This both allows for a steady growth rate of the network and prevents excessively large blocks.

4.2 FULL NODE BLOCK CHAIN PROCESSING

The block chain is currently about 25GB and is growing at about 1.1GB per month [9]. In most desktop wallet clients, the entire block chain must be parsed before the node can actively participate in transactions on the network. This can be a time consuming process for most standard computers, taking a week or more. While we do not have a solution to the growing size of the block chain, we do propose a solution which will allow full nodes to participate and make transactions soon after downloading the desktop client.

To do this, nodes will first download all block headers and verify the basic validity of those headers. This will give them enough information to participate in the network as a lightweight node while a background thread runs, downloading block contents and then verifying them starting at the genesis block. Certain features that rely on having the full block chain will have to be disabled temporarily while this process is running. During this initialization period, the validity of transactions is established through other nodes' referral of transactions and the depth of the transaction within the block chain. This feature will make cryptocurrency much easier to use for everyday people, eliminating the need to wait several weeks before being able to participate.

5.0 Further Technical Specifications

QUICK COIN STATS

VOLUME

10 billion ziftrCOINs over 10 years

DISTRIBUTION

Block reward is constant for 2.5 years, then linearly down to minimum block reward

PRE-MINE

4.5% of ziftrCOINs

PROOF

Proof of Work

MINING ALGORITHM

Keccak with Sign to Mine™

BLOCK GENERATION

1 block per minute

DIFFICULTY RETARGETING

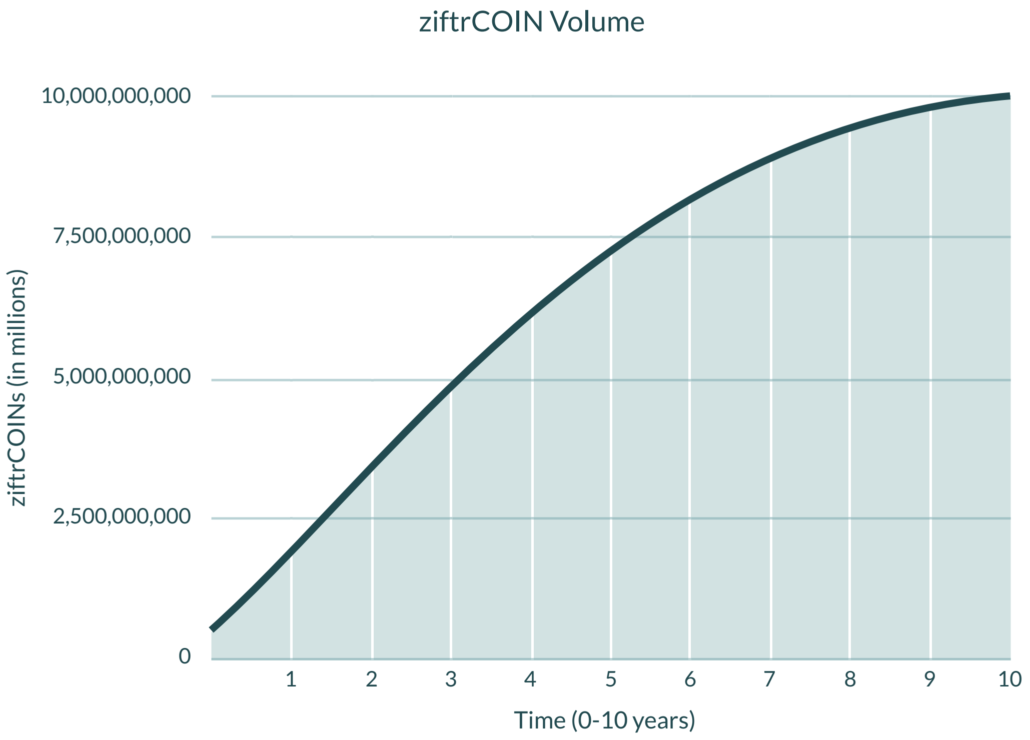
Digishield

TIEBREAKER

Coin age destroyed

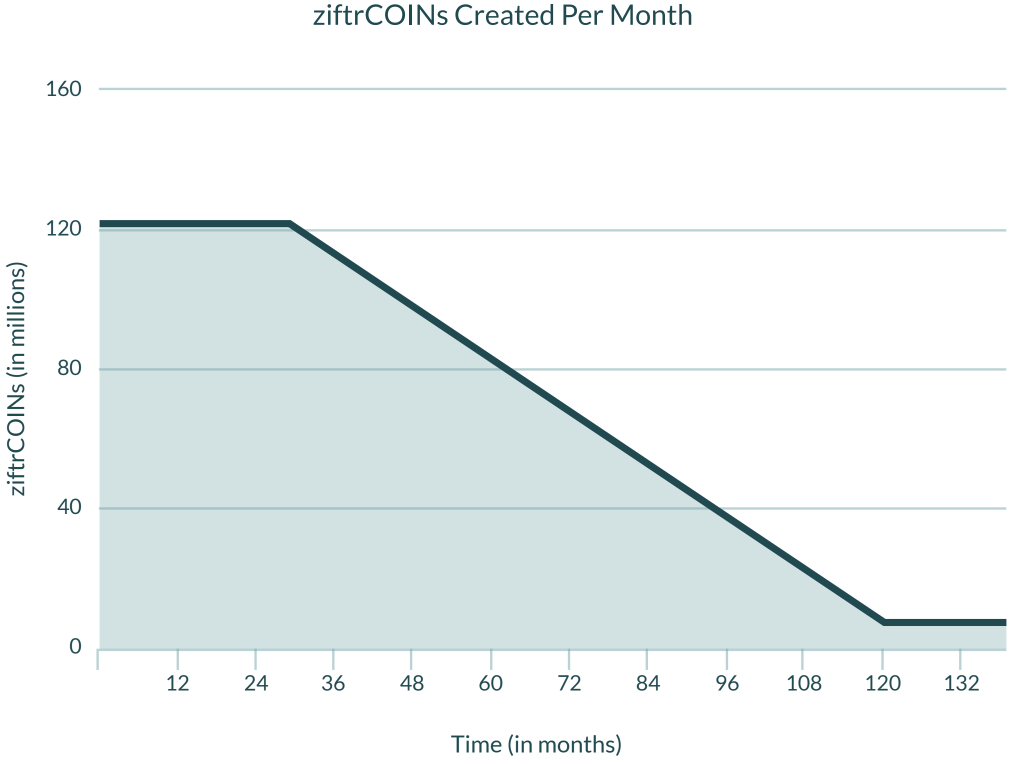
5.1 VOLUME

10 billion ziftrCOINs will be mined over a period of 10 years.



5.2 DISTRIBUTION

Coins will be distributed at a constant rate of approximately 2,793 coins per block for 2.5 years. After that there is a linear decline in the block reward until we hit the minimum block reward of roughly 190 ziftrCOINs per block. This minimum reward serves to both offset the loss of coins by users and reduce the burden of users who must pay fees to incentivize miners.



5.3 PRE-MINE

We are pre-mining 4.5% of the total ziftrCOINs, 66.7% of which we will give away to consumers. In doing this, we hope that more consumers start to become familiar with cryptocurrency. To further achieve this goal, we are developing a mobile wallet that will hold all major types of cryptocurrency, including Bitcoin, Litecoin and ziftrCOIN.

In addition to helping us seed the marketplace with consumers who have coins to spend, our ziftrCOIN pre-mine will give us the opportunity to raise some capital to curate the currency and will provide us with the necessary funding to create tools that are equipped to support a new coin. In order to maintain complete transparency with the community, we have created a reference on the ziftrCOIN pre-mine, as well as the purpose of all pre-mined coins, in the table below.

Amount (ziftrCOINs)	Purpose	Availability	% Total coins / % coins available after 1yr
300 Million	To be given away to users via promotions. • 100 coins to first 1 million users • 50 coins to next 2 million users • 20 coins to last 5 million users	At coin launch.	3% / 15.3%
50 Million	To be sold in our Presale	At coin launch.	0.5% / 2.5%
25 Million	Saved for employees and advisors	1 year from coin launch.	0.25% / 1.3%
25 Million	Saved for employees and advisors	2 years from coin launch.	0.25% / 0%
25 Million	Saved for employees and advisors	3 years from coin launch.	0.25% / 0%
25 Million	Saved for employees and advisors	4 years from coin launch.	0.25% / 0%

Coins reserved for employees and advisors will be used as incentives to promote the use of ziftrCOIN, ziftrPAY, ziftrSHOP and ziftrWALLET over the course of the next four years.

When consumers conduct transactions within Ziftr's retailer network, we will redeem each ziftrCOIN for at least $1/coin, for up to 5% of the purchase. If ziftrCOINs are currently trading on the open market for more than $1/coin, then we will use the market price and the 5% limit is removed. We can afford to do this because, when users spend ziftrCOINs using the Ziftr® shopping cart, retailers pay us a small percentage of the transaction as a reward for bringing them new customers.

We're spreading out the distribution of our employees' and advisors' coins over a period of 1-4 years to incentivize the growth of ziftrCOIN and the tools that support it. To demonstrate our commitment to what we're doing, we're locking these coins in the blockchain, where the first 25% won't be available to use until one year has passed and the remaining 75% will be distributed evenly over the course of the three years that follow. This also serves to show that we intend to be here four years from now, and not to mine and sell our coins quickly in a "pump and dump" scheme, as has become all too common in the cryptocurrency world.

5.4 PROOF

The ziftrCOIN network will be secured using Proof of Work.

5.5 MINING ALGORITHM

We will use the NIST chosen Keccak, a memory-hard 512-bit hashing algorithm, along with our Sign to Mine™ protocol, to mine ziftrCOINs. Essentially, the header must contain a signature of the header's contents, which must be verified with the script spending the coinbase transaction. This ensures that the one who solves the block also has the capability to spend the block, which limits large pools. With Sign to Mine, miners should make sure they trust those with whom they are mining, as anyone in the pool has the ability to spend the reward for the blocks they solve.

5.6 BLOCK GENERATION

Blocks will be generated, on average, at a rate of 1 block per minute.

5.7 DIFFICULTY RETARGETING

Difficulty retargeting in ziftrCOIN will be done using Digishield (http://www.digibyte.co/digishield), a highly tested and lauded difficulty retargeting algorithm.

5.8 TIEBREAKER

Coin age is simply the product of the amount and the age of an Unspent Transaction Output (UTXO), typically measured in coin-days. When UTXOs are used in a new transaction, any coin age that had accumulated is destroyed. We propose using this destroyed coin age as a tiebreaker in our PoW coin to encourage the network to come to a consensus quickly in the event of two miners solving a block at nearly the same time (within 13 seconds). To accrue coin age, ziftrCOINs must have a minimum 1-day age and are limited to a maximum 100 days of age.

6.0 ziftrCOIN's $1 Minimum Redemption Value

As we mentioned in section 5.3, we're giving away 300 million ziftrCOINs to the first 8 million people who sign up and selling 50 million ziftrCOINs through a presale. We're guaranteeing a minimum redemption value of $1 per coin for up to 5% of each transaction conducted within Ziftr's retailer network when ziftrCOIN is valued at less than $1 on the open market. Please see below to learn how these coins will be distributed.

First 1 million users	100 free ziftrCOINs
Next 2 million users	50 free ziftrCOINs
Next 5 million users	20 free ziftrCOINs
ziftrCOIN Presale	50 million ziftrCOINs

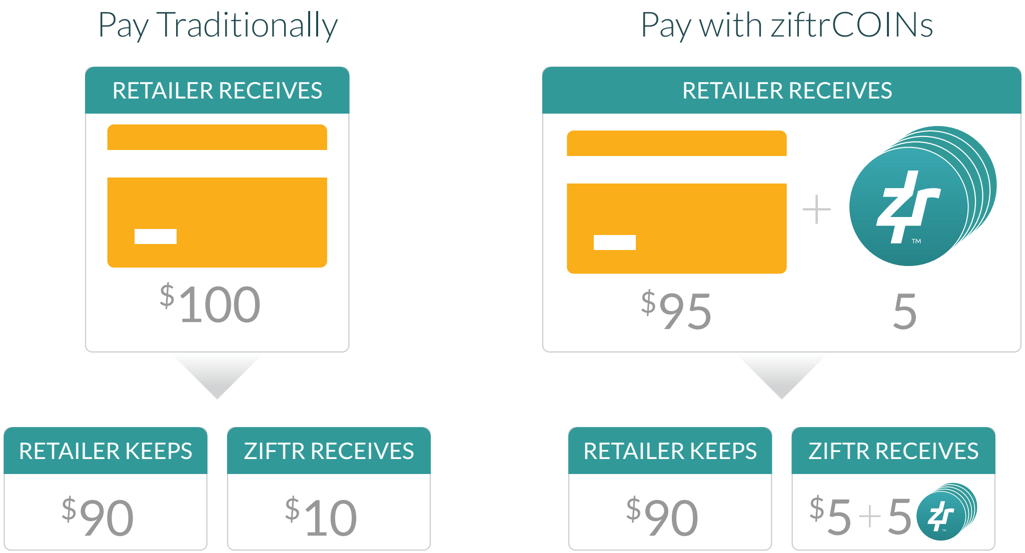
At this point, you must be asking yourself, "what's the catch?" A $1 minimum redemption value sounds too good to be true, but it isn't. Let us explain.

6.1 HOW WE CAN REDEEM EACH ZIFTRCOIN FOR A MINIMUM VALUE OF $1

Each time a user conducts a transaction on Ziftr's website or within Ziftr's retailer network, a portion of the total amount goes to us for lead generation and advertising. In other words, our retailers give us a percentage of the transaction value as a reward for bringing them customers. However, when users conduct transactions with ziftrCOIN, we'll take less than the standard amount for ourselves so that we can give part of it to the user in return for their ziftrCOINs. The $1 minimum redemption value is guaranteed because we'll use part of our own compensation to ensure that the value is never less than $1 on our website or within our retailer network.

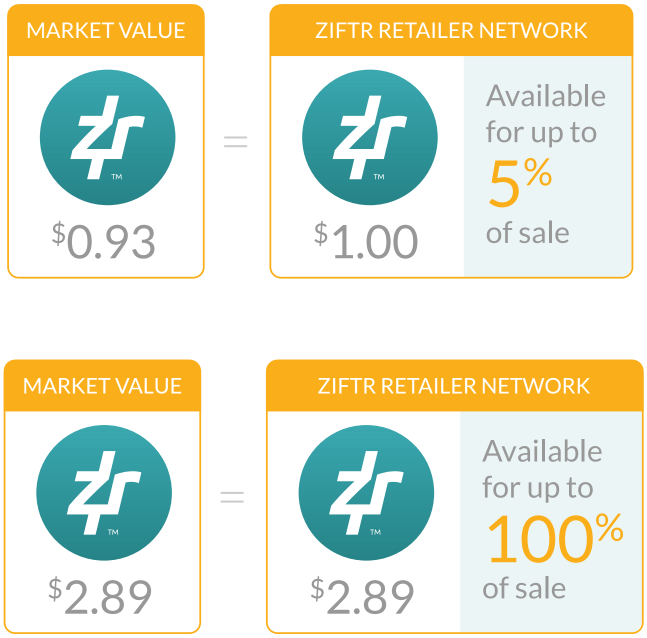
Currently, we have a large retailer network that continues to grow every day - with more and more big brands beginning to accept ziftrCOIN, Bitcoin, Litecoin and other cryptocurrencies via adoption of our Ziftr API.

The diagram below shows how the process works traditionally and how it will work when customers use ziftrCOINs. In this example, a user is purchasing an item worth $100.



6.2 HOW CAN YOU BENEFIT FROM ZIFTRCOIN'S $1 MINIMUM REDEMPTION VALUE?

When ziftrCOIN is valued below $1 on the open market, we will redeem each ziftrCOIN for $1 when used within our retailer network. When ziftrCOIN is valued at more than $1 on the open market, users will be able to spend as many ziftrCOINs as they wish for each purchase. The diagram below explains how this process will work at checkout. As you can see, it works just like a coupon.



MARKET VALUE

$0.93

=

ZIFTR RETAILER NETWORK

$1.00

Available for up to 5% of sale

MARKET VALUE

$2.89

=

ZIFTR RETAILER NETWORK

$2.89

Available for up to 100% of sale

Of course, each ziftrCOIN can also be sold or traded on a cryptocurrency exchange at any time.

7.0 Conclusion

In this paper, we have analyzed some of the strengths and weaknesses of digital currency, and put forth solutions to many of the current issues discussed. We will soon finish implementing these solutions in order to create a coin which will address what we believe are the most important hurdles to widespread adoption. These hurdles include both technical limitations and a greater need to support users in spending digital currency.

In creating our coin, we have considered and addressed many concerns of consumers, retailers, economists, and miners. We have also designed our coin to strengthen the digital currency network by both enabling the system to come to a consensus more quickly and inhibiting centralization through our Sign to Mine™ protocol. In addition, we have provided a method for increasing the transaction rate to a level that is useful for commerce. These improvements will truly enable commerce in the digital age.

Equally important as solving current technical problems in digital currency, however, is providing strong support for users who wish to start using digital currency. We will make acquiring digital currency easier for users by offering a temporary "faucet" for distributing ziftrCOINs to the open market. That is, the first 8 million users of our ziftrCOIN cloud wallet will receive free ziftrCOINs. Furthermore, we will use our deep experience in professional application and e-commerce software to create a suite of applications that will make working with the digital currency extremely painless.

We are confident that creating a digital currency that is aimed at the needs of consumers and vendors, and is supported with tools for ease of use will help attract more people to start using cryptocurrency.

References

[1] Philip Koshy. “what is bitcoin?”, July 2012. URL http://www.bitcoinsecurity.org/ 2012/07/22/what-is-bitcoin/.

[2] Block height 315076, August 2014. URL https://blockchain.info/block-height/315076.

[3] Steve Shanafelt. Mining pool giant ghash.io reaches 50% of bitcoin hashing power, June 2014. URL http://www.bitcoinx.com/ mining-pool-giant-ghash-io-reaches-50-of-bitcoin-hashing-power/.

[4] mmitech. Ghash.io and double-spending against betcoin dice, November 2013. URL https://bitcointalk.org/index.php?topic=327767.0.

[5] Ittay Eyal and Emin Gün Sirer. How to disincentivize large bitcoin mining pools, June 2014. URL http://hackingdistributed.com/2014/06/18/ how-to-disincentivize-large-bitcoin-mining-pools/.

[6] Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable, November 2013. URL http://arxiv.org/pdf/1311.0243.pdf.

[7] Timothy Lee. Bitcoin needs to scale by a factor of 1,000 to compete with visa. here’s how to do it., November 2013. URL http://www.washingtonpost.com/ blogs/the-switch/wp/2013/11/12/bitcoin-needs-to-scale-by-a-factor-of-\ 1000-to-compete-with-visa-heres-how-to-do-it/.

[8] Maximum transaction rate, January 2014. URL https://en.bitcoin.it/wiki/ Maximum_transaction_rate.

[9] Blockchain size, August 2014. URL https://blockchain.info/charts/blocks-size? timespan=30days&showDataPoints=false&daysAverageString=1&show_header= true&scale=0&address=.

About ziftrCOIN

ziftrCOIN, the first digital currency developed for online shoppers, aims to revolutionize shopping by putting cryptocurrency into the hands of consumers and enabling them to conduct simple, secure transactions at their favorite online retailers.

For the latest updates, sign up on our website and/or follow us on Twitter.