ziftrCOIN™

WHITE PAPER • RELEASED OCTOBER 9, 2014, UPDATED JULY 21, 2015

ZIFTRCOIN:

A CRYPTOCURRENCY TO ENABLE COMMERCE

Follow us on Twitter for the latest on @ziftrCOIN

ISBN: 978-1-61323-038-1

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 by incentivizing miners to prove knowledge of the transaction data they 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 messages 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 his or her 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 due to transaction malleability.

Blocks are generated at different frequencies in various cryptocurrencies. Selecting a target block generation time involves a trade-off 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.

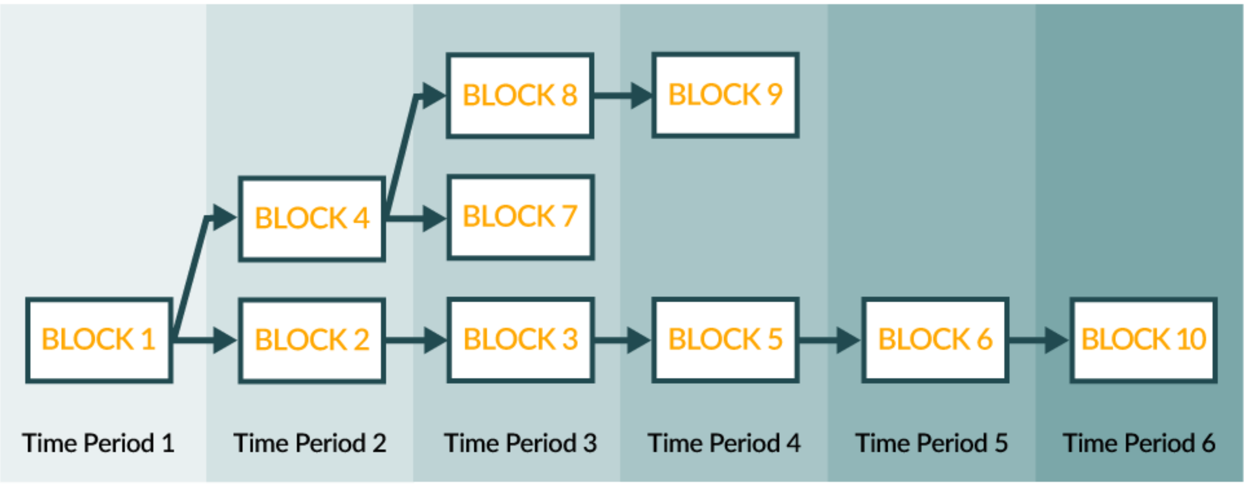


FIGURE 1: A block chain can become a 'block tree' due to a branching effect if blocks are generated too quickly.[1]

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 tie-breaking procedure that compares the amount of sufficiently mature coins spent in each block.

2.3 CHAIN TIE-BREAKING STRATEGIES

When two chains are known to a node, the chain with more work must always be considered the correct chain. However, when two chains with the same amount of work are present, we must have a way to choose the locally correct chain. We will call this strategy the chain tie-breaking strategy. For example, the chain tie-breaking strategy of Bitcoin is to choose whichever block was seen by the node first. In general, this works well as a chain tie-breaking strategy, but it has some flaws.

The main flaw of the chain tie-breaking strategy used in Bitcoin is that it unintentionally disincentivizes miners from including transactions into their blocks. The fees that are provided in transactions 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. 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. When blocks take longer to spread through the network, other miners continue to mine on their best-known block until the newly found block arrives. If during the time when the first block is spreading through the network a different miner solves a block that is much smaller, then that block may be able to propagate through the network faster and become accepted by more miners even though it was not the first block solved.

This is not an abstract theoretical threat to the network. This threat is real enough that within the Bitcoin network, there are frequently miners who 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 network would fail to verify transactions and the entire system would fail to be useful. We propose a more effective chain tie-breaking strategy that actually incentivizes miners to include transactions.

2.4 MATURE COINS SPENT

Ideally, miners who include more real transactions into the blocks that they mine would have an advantage in the chain tie-breaking procedure over selfish miners who try to keep their block size as small as possible. However, transactions can easily be made just for the purpose of increasing a block's transaction count. Thus, we cannot use just the raw number of transactions in a block as a metric in determining the winner of a block race. Instead, we use the number of sufficiently mature coins spent in a block as the default chain tie-breaking procedure. Essentially, blocks with more mature coins spent are chosen in the event of a tie, where only transaction inputs that spend outputs that are at least 60 blocks old (approx. 1 hour) count toward the mature coins of a block.

However, this tie-breaking procedure is intended to be used for cases where there is a legitimate tie – one miner solving a block during the time when another block is propagating through the network. Once honest miners hear about a new block, they will start mining on it rather than continuing to mine on the old block in an attempt to replace it with another block containing more mature coins. Thus, the chain tie-breaking procedure also has to take into account when blocks are received by only using the chain tie-breaking procedure described above within a short interval after receiving a new block. To summarize the chain tie-breaking strategy that ziftrCOIN uses, when nodes hear of a new solved block, they essentially start a 13-second timer. If before the timer ends, the node hears about a new block and the new block spends more mature coins than the previous block did, then the node will choose it as the tip of the new correct chain.

2.5 LIMITING EXCESSIVE FEES

An interesting benefit of using mature coins spent as a chain tie-breaking metric 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 the contribution of mature coins spent to a block. Miners can include transactions in their block if they have a fee OR if they contribute to the mature coins count for their block. Both provide the miner some benefit, the fee being a monetary gain and the mature coins being spent causing the miner’s block to be chosen in the event of a tie. If a user does not have any fully mature coins in his or her wallet, or not enough sufficiently mature coins, then he or she will likely have to provide the standard transaction fee to the miners in order to have a miner include the transaction in a block in a timely fashion.

2.7 A MARKETPLACE FOR SPENDING MATURE COINS

Using mature coins spent as a tie-breaking metric gives miners an incentive to spend mature coins in their block. These mature coins being spent may be partially from the miners’ own supply and partially from normal transactions distributed through the system. Users of the system could theoretically submit private transactions to a miner that send coins to themselves and spend mature coins in the process. The miner, receiving the boost in mature coins spent in his or her block, could reward the submitter with a small profit once the coins have been used to help the miner successfully publish his or her block to the network. Different miners could offer different rates for submitting such private transactions, inducing a marketplace for spending matured coins, and yielding a small profit for users of the coin as a reward for actively taking part in securing the system. This is similar to the annual yield present in Proof of Stake systems.

The obvious problem with this, however, is that there is no way for miners to verify that the private transactions submitted to them were not also given to any other miners. To counter this, miners can factor this into their rates for mature coins, and can ban certain users for spending certain outputs that have been submitted as private transactions.

It is important to note, however, that this is a theoretical marketplace that could coexist with ziftrCOIN. There is no guarantee that any such marketplace will exist; we are just commenting on the fact that the incentives would be lined up for it to exist.

2.8 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 Gun Sirer[5], 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.

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 mature coins to be spent. To successfully take advantage of Selfish Mining, the malicious miner must save up multiple batches of mature coins, each spending more mature coins than is typically spent 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. Selfish mining could, theoretically, give a miner a slightly higher than expected revenue, but it causes no real issue for users of the coin.

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.

One important distinction to make is that concentration of miners into pools only becomes truly centralized when pool operators have control over which transactions are mined and which block is built upon. When pools function solely as a solution to limit the variance of rewards for miners, they pose no threat to the network. We propose a solution where miners can optionally prove knowledge of the transaction data they are mining to earn a larger reward than miners who blindly do work given from a pool.

3.1 PROOF OF KNOWLEDGE

In order to incentivize miners to control the set of transactions they mine, ziftrCOIN makes use of an augmented Proof of Work algorithm that rewards miners for proving knowledge of the transactions in their block. Verifiably proving knowledge of transaction data is an optional part of the mining algorithm, but if completed, it lets the miner claim a 5% higher block reward. Proof of Knowledge was made as an optional part of the algorithm because many miners value the convenience of not needing to run their own full node. In the long term, however, when mining is very competitive and profit margins become very thin, miners will likely need to mine with Proof of Knowledge in order to stay profitable.

One advantage specific to the way ziftrCOIN has implemented Proof of Knowledge is that although the miner is required to know all of the transaction data in the block, verifying the work only requires one extra transaction from the block and a Merkle branch proving its inclusion within the block. This is especially advantageous for SPV nodes, which need to be able to verify block headers without downloading all of the block's data. To achieve this, mining with PoK is done by randomly sampling transaction data. In addition, mining with PoK turned on requires essentially no extra work, as it only requires an extra XOR of that transaction data into an intermediate hashing state.

The most obvious attack on this system is that a pool may be created that uses Proof of Knowledge for the 5% bonus, but does not include any transactions into its blocks to avoid high bandwidth. This is mitigated in two ways. First, the network uses the count of mature coins spent in blocks as a tiebreaker, so such a pool would lose some of its blocks to honest miners who do include transactions which spend mature coins. Second, it is possible to make use of canonical transaction ordering and Invertible Bloom Lookup Tables to efficiently communicate between pool and miner which transactions are being mined. Implementing a pool like this would make pools that mine empty blocks obsolete, as they would yield lower payouts and lose in all chain tiebreakers.

The result of using Proof of Knowledge is that miners are incentivized to build their own blocks rather than use the work given from the pool. Miners can still use pools to limit variance, but by incentivizing miners to know their own transaction data, no single user has control over a large portion of the network's hash power.

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.[6] In fact, the 1MB limit imposes roughly a 10 transactions/second limit on the system,[7] effectively limiting the growth of Bitcoin.

We 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 allow blocks to become marginally larger over time. 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.[8] 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 makes 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 30 years

DISTRIBUTION

Distribution is set to match standard distribution curves for adoption of common technologies

PRE-MINE

4.5% of ziftrCOINs

PROOF

Proof of Work

MINING ALGORITHM

ZR5 with Proof of Knowledge

BLOCK GENERATION

1 block per minute

DIFFICULTY RETARGETING

Every 4 blocks

TIEBREAKER

Mature coins spent

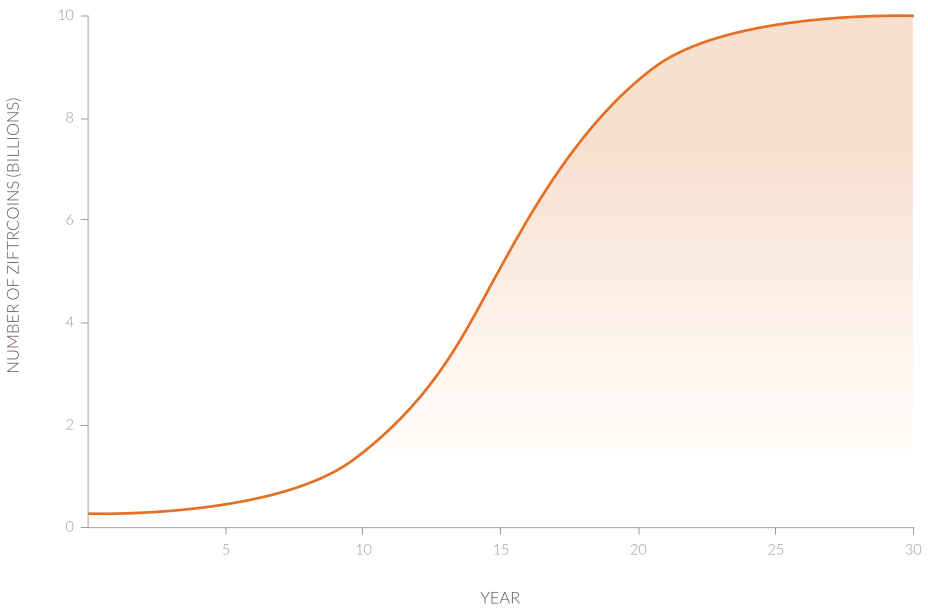
BLOCK SIZE LIMIT

Starts at 1MB and is dynamically allowed to increase a maximum of 10% every 3 months

5.1 VOLUME

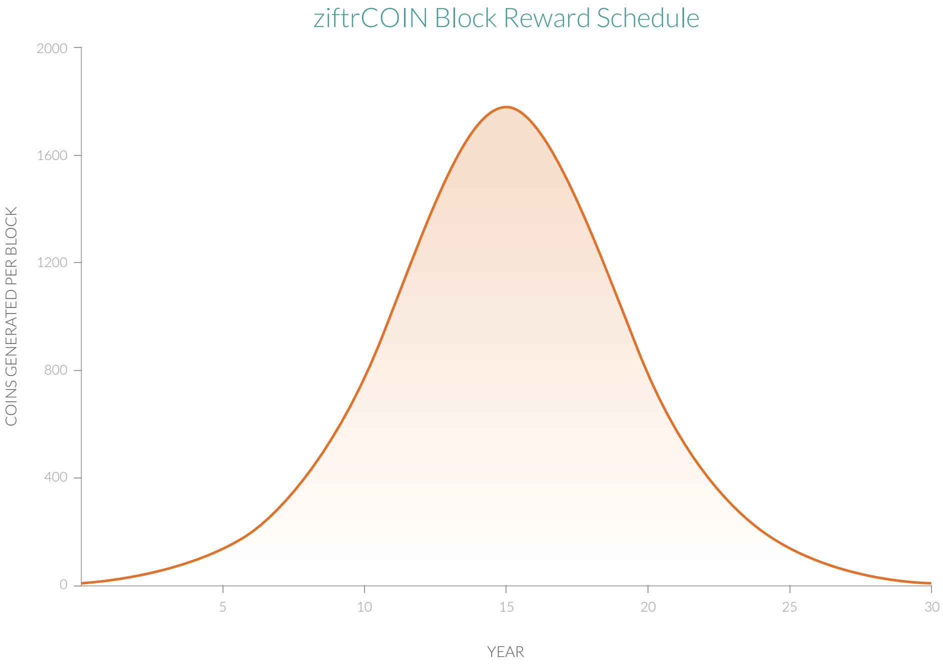
Most coins follow a halving block reward distribution that incentivizes early adopters to participate before the block reward drops. Instead, we decided to try to match the distribution with common adoption curves for new technologies. In total, 10 billion ziftrCOINs will be mined over a period of 30 years. The graph below shows the planned distribution.

ziftrCOIN Distribution Chart



5.2 DISTRIBUTION

The distribution of ziftrCOINs follows a standard bell curve. The block reward is constant throughout the day, changing after a day's worth of block. As detailed in the previous section, this curve was chosen to model the adoption rates of new technologies.



5.3 PRE-MINE

We pre-mined 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 have developed 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 gave us the opportunity to raise some capital to curate the currency and provided 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 merchant 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, merchants 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 block chain, 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 is secured using Proof of Work.

5.5 MINING ALGORITHM

The exact hashing algorithm used is a combination of the 5 finalist algorithms that NIST selected as candidates for SHA3 (BLAKE, Grøstl, JH, Keccak and Skein). The first in the series, Keccak, is executed, and then the order of the next four is determined based on the result. In addition, there is an opt-in process of mining with Proof of Knowledge of transaction data that allows miners to gain a 5% increase in rewards. Read more about this here.

5.6 BLOCK GENERATION

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

5.7 DIFFICULTY RETARGETING

Difficulty retargeting is done every 4 blocks.

5.8 TIEBREAKER

ziftrCOIN uses a custom chain tie-breaking algorithm to choose locally correct chains in the event that a new block is solved while another is propagating. When nodes hear of a new solved block, they essentially start a 13-second timer. If before the timer ends, the node hears about a new block and the new block spends more mature coins than the alternate block did, then the node will choose it as the tip of the new correct chain. This allows the network to quickly come to a consensus as to the correct chain in the event of multiple blocks simultaneously being solved.

5.9 BLOCK SIZE LIMIT

There is not a hard cap on the block size limit in ziftrCOIN. Instead, if both the mean of the last 3 months' worth of blocks is greater than 2/3 of the current block size limit and the median is greater than 1/2 of the current block size limit, then the new block size limit for the next 3 months is increased by 10%. This allows for the network to grow dynamically according to its use, and avoids the need for a hard fork when transaction volume spikes.

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 reserved 50 million ziftrCOINs to sell in a presale. We're guaranteeing a minimum redemption value of $1 per coin for up to 5% of each transaction conducted within Ziftr's merchant 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

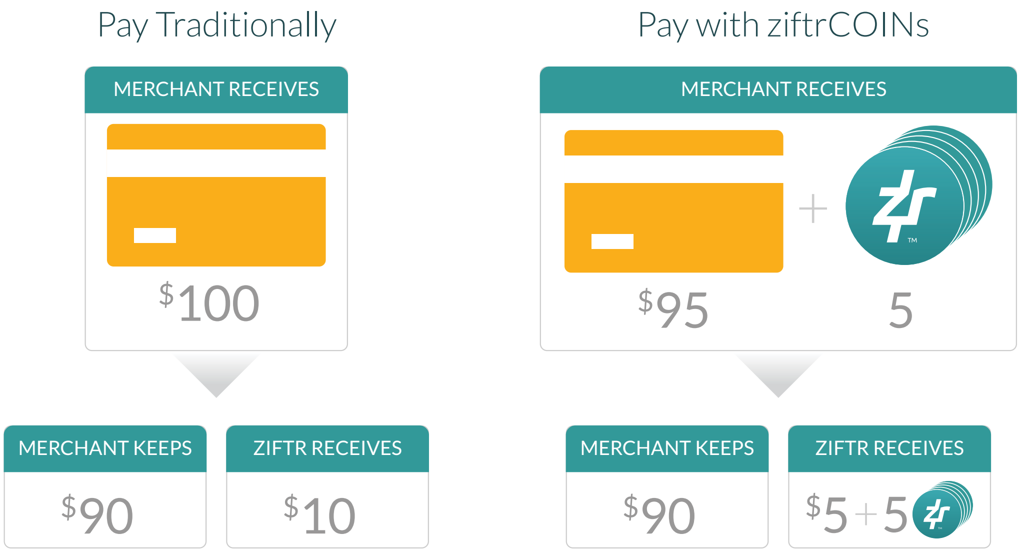
At this point, you must be asking yourself, "what's the catch?" A $1 minimum redemption value sounds too good to be true, but it isn't. Let us explain.

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 merchant network, a portion of the total amount goes to us for lead generation and advertising. In other words, our merchants 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 merchant network.

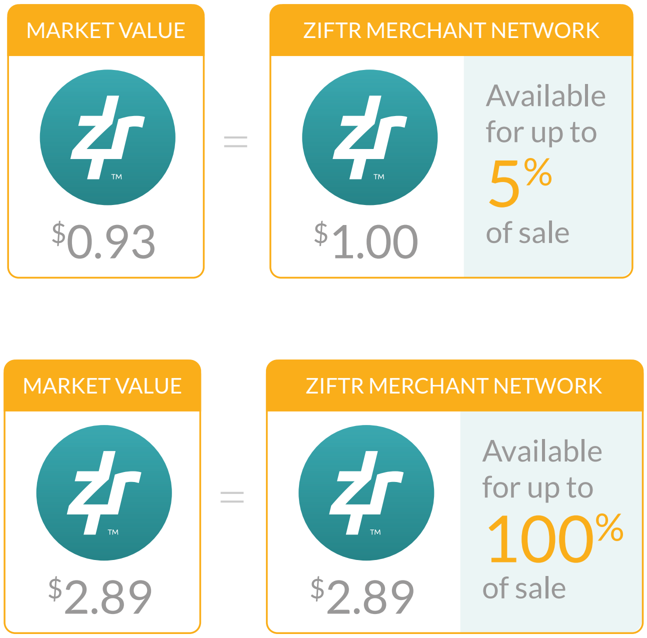
Currently, we have a large merchant network that continues to grow every day - with more and more big brands beginning to accept ziftrCOIN, Bitcoin, Litecoin, and other cryptocurrencies via adoption of our ziftrPAY API.

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 merchant 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.



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 have implemented these solutions in order to create a coin which addresses 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, merchants, 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 augmenting Proof of Work with Proof of Knowledge. 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. Furthermore, we will use our deep experience in professional application and e-commerce software to market a suite of applications we have developed 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 Gun¨ 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] Timothy Lee. Bitcoin neëds 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/.

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

[8] 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 merchants.

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