WhitePaper

- Coin Name - SRKCoin
- Type – Virtual Currency
- Promoter – SRK Corporation
- Ticker - SRK

ICO At a Glance

Total Coin Supply	ICO Launch Date
45 Million Coins	26th Jan 2018
Initial Coin Supply	Coin Launch Price
4 Million Coins	27 USD / Coin

TimeLine

Concept Design →	April 2017
Team Development →	June 2017
Legal Structure →	July 2017
Software Development →	August 2017
Website Development →	October 2017
Pre-launch Preparation →	December 2017
ICO Launch →	January 2018

Abstract

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an on-going chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and re-join the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Overview - I

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be vary of their customers, hassling them for more information than they would otherwise need.

Overview – II

A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party. What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

Transactions - I

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership. The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent.

Transactions - II

The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank. We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced, and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be time stamped and widely publishing the hash, such as in a newspaper or Usenet post. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

Proof of Work - I

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof- of-work system similar to Adam Back's Hashcash, rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash. For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it. The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote.

Proof of Work - II

The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added. To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

Network - I

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Network - II

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one. New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

Incentive - I

By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended. resources to add gold to circulation. In our case, it is CPU time and electricity that is expended. The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction.

Incentive - II

Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free. The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree, with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored. A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

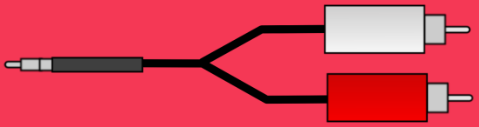
Simplified Payment Verification - I

It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it. As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker.

Simplified Payment Verification - II

While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

Combining and Splitting Value



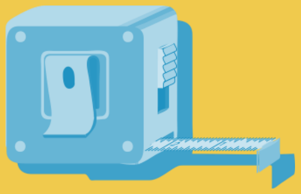
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender. It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were. As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

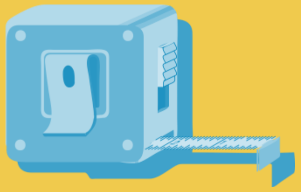
Calculations - I

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were. As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.



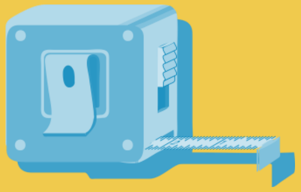
Calculations - II

We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows: Given our assumption that p > q, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind. We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late. The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment.



Calculations - III

Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction. The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value: To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point: Rearranging to avoid summing the infinite tail of the distribution... Converting to C code... Running some results, we can see the probability drop off exponentially with z. Solving for P less than 0.1%...



Derivations

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and re-join the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

Why Invest in SRKCoin - I

After the launch of first successful Cryptocurrency in the form of Bitcoin in the year 2009, the digital currency and its alternatives have caught on big time in place of traditional currency. SRKCoin is one of these alt coins that makes use of Blockchain and peer to peer technology.

The question now arises is why should one use SRKCoin instead of traditional money. Well SRKCoin being a cryptocurrency, it offers amazing and awesome benefits that are not available when you use regular currency like (INR, USD or GBP).

Since it is a decentralized system there are no Govt. and banking systems included in the complete transfer of money, that enables quick and safe transfer of money.

Why Invest in SRKCoin - II

When you send money via the traditional banking system they take a significant amount as commission or charges, whereas we you go for SRKCoin the charges are significantly low. It must be noted that you can send smaller amounts using the SRKCoin with ease, when using the prevalent cash and banking system when sending smaller amounts the banks or payment gateway systems used to cut so much amount as fees that it was as good as sending nothing, but this can be eliminated using SRK coins. Now you can easily transfer even smaller amounts with marginal charges. Forget the autocratic behaviour of banks and money transfer funds and experience money transfer the new and convenient way or should we say SRK-coin way.

Features - I

Transfer securely
As SRKCoin works on peer to peer technology using the most secure block chain algorithm you can safely transfer your money. SRKCoin is Safe & Secure.

Works everywhere
One of the biggest plus points of SRKCoin is that works from anywhere. Users can send and receive payments from any point of the globe to other point of the globe using internet as a medium.

Privacy protection
SRKCoin ecosystem is built for privacy right from the bootstrap. So no need to worry regarding your data and information. It's completely safe and encrypted.

Features - II

Fast payment

Gone are the days when you had to send or receive money and wait for it to arrive or reach at the destination. Here comes SRK coins that helps in transfer of funds almost instantly in matter of minutes.

De-centralized

SRKCoin is a completely decentralized system, meaning no government or banking institutions are involved in the transaction.

Multiply Your Money

Don’t just add to your wealth, multiply it. SRKCoin has the potential to increase in a super-fast manner in turn enabling you to multiply your wealth.

Security

SHA-256 encryption
SRKCoin uses the Much Trusted **SHA-256 encryption** for both its Proof-of-Work (PoW) system and transaction verification. The security of the SRKCoin protocol lies in one of its fundamental characteristics, the transaction blockchain.

As SRKCoin works on peer to peer technology using the most secure block chain algorithm you can safely transfer your money. SRKCoin is Safe & Secure.

Disclaimer - I

1. Prospective ICO Participants should inform themselves as to the legal requirements and tax consequences within the countries of their citizenship, residence, domicile, and place of business with respect to the acquisition, holding or disposal of the Tokens, and any foreign exchange restrictions that may be relevant thereto. The distribution of this White Paper and the offer and sale of the Tokens in certain jurisdictions may be restricted by law. This White Paper does not constitute an offer to sell or the solicitation of an offer to buy to any person for whom it is unlawful to make such offer or solicitation.
2. SRKCoin is not providing you legal, business, financial or tax advice about any matter. You may not legally be able to participate in this private unregistered offering. You should consult with your own attorney, accountant and other advisors about these matters (including determining whether you may legally participate in this ICO). You should contact us with any questions about this ICO or the Tokens.

Disclaimer - II

3. It is the responsibility of any persons wishing to acquire the Tokens to inform themselves of and to observe all applicable laws and regulations of some relevant jurisdictions. Prospective ICO Participants should inform themselves as to the legal requirements and tax consequences within the countries of their citizenship, residence, domicile, and place of business with respect to the acquisition, holding or disposal of the Tokens, and any restrictions that may be relevant thereto.
4. This White Paper constitutes an offer of Tokens only in those jurisdictions and to those persons where and to whom they lawfully may be offered for sale. This White Paper does not constitute an offer to subscribe for securities except to the extent permitted by the laws of each applicable jurisdiction.
5. Nothing in this White Paper is intended to create a contract for investment into SRKCoin, and each potential ICO Participant acknowledges that SRKCoin will rely on this assertion of an ICO Participants statement with respect to compliance with the laws of the jurisdiction in which the ICO Participant is legally domiciled.

Find Us

https://www.facebook.com/SRK-Coin_-142617156407373

https://twitter.com/srk_coin

https://www.linkedin.com/in/srk-coin-023966157/

srkcorpint@gmail.com

https://www.srkcoin.com/

http://newico.srkcoin.com/

Resources - I

W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust

requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.

S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

Resources - II

A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy,

IEEE Computer Society, pages 122-133, April 1980.

W. Feller, "An introduction to probability theory and its applications," 1957.

Koinster, "White Paper Generator," http://whitepaper.koinster.com, 2017.

S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.