What is Timekoin?

Timekoin is a long tested set of protocol rules and software implementation for an open encrypted electronic currency system on a public network. Timekoin is not a clone of other existing digital currency systems (such as Bitcoin, Litecoin, etc). Timekoin is a very different and unique way to secure transactions and create currency. Timekoin uses custom RSA encryption and SHA hashing to secure transactions. Transactions work like clockwork, being processed every 5 minutes. Transaction processing is not dependent on Currency creation and this makes it unique among other popular digital currencies. This separation of the two systems allows each to function independently of the other. The design of Timekoin allows it to function on computer systems or devices (such as the Raspberry Pi) with minimal effort needed to maintaining security and speed.

How Does the Economy Function?

The Timekoin economy runs on very simple rules. These rules are enforced by all peers participating in the network.

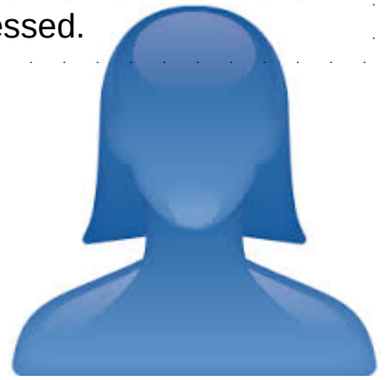
- No hard limit on currency creation. There is no cap of the maximum amount of currency that will ever be created.
- All Timekoins are whole numbers. No Decimal point currency is used to avoid rounding and accuracy errors.
- Transactions cost nothing except the CPU time it took your computer to encrypt the transaction.
- No Double-Spending a balance for obvious reasons.
- No Spending to yourself. Transactions such as this are ignored.
- 100 Transaction queue limit. Each public key may only queue 100 transactions to be processed by the network for each 5 minute transaction cycle. This insures the network is not flooded with bogus transactions.
- Currency Generation is restricted to a single IP address per public key basis to combat fake servers. Currency Generation is also capped at 100,000 generation transactions per public key. No server is immortal in Timekoin.
- Any peer can generate currency, but must be elected by the network peers first. There is a network fee to request election by the other peers. The fee is the number of generating servers total; paid to each unique public key before being considered for peer election. The election process is random to give each peer an equal chance of winning.
- Elected peers are allowed to create currency so long as they remain online and generate at least 1 unit of currency every 8 hours, otherwise the peer loses the elected status and must be elected again to generate currency.
- Elections are chosen at random times in the future based on the forward movement of time and seeded by the Transaction History of the Timekoin network. Every Transaction in Timekoin changes the future.
- Generating currency (for elected peers) is chosen at random times in the future based on the forward movement of time and seeded by the Transaction History of the Timekoin network. This organic randomness makes it nearly impossible to predict far into the future for any type of possible exploitation.

How are transactions processed in Timekoin?

Bob wants to send Timekoins to Jane.

Step 1: Bob creates an encrypted transaction with his Private Key. In the transaction, is his Public Key to decrypt the data. The decrypted data contains the Public Key of Jane and how much to send her. The transaction also contains a SHA256 hash of the intended recipient (Jane Public Key). Finally, Bob creates another SHA256 hash of the entire Transaction Data to help verify that the transaction has not been damaged or tampered with while in transit.

Step 2: Bob takes this transaction data and broadcast it into the Timekoin network. Every 5 minutes, all Timekoin servers are creating a temporary Queue of transactions to be processed. Bob's transaction is included in this queue, waiting to be processed.



Step 3: Once the 5 minute wait is finished, all the Timekoin servers (simultaneously) begin processing the list of transactions in the Queue. The transaction is verified against tampering. If the SHA256 hash does not match the transaction data, it is discarded. Next, the data is decrypted. From this, the servers know that Bob (public key) wants to transfer Timekoins to Alice (public key). The servers check if the SHA256 inside the encrypted data matches the public key of Alice. If this check fails, the transaction is discarded. The servers check the history of all of Bob's transactions. They tally up how many Timekoins have been sent to him and how many he has sent to others. If his remaining balance is equal to or greater than the amount he is sending to Alice then the transaction is verified as acceptable. The transaction is then moved into the Timekoin transaction history with any other transactions that pass verification as well. Now that the new transaction is in the history, any future transactions can reference it for balance checking in the future.

Step 4: After all transactions are processed, all the Timekoin servers create a SHA256 hash of all the transaction data that was just processed and saved into the transaction history for that 5 minute block of time. This SHA256 hash becomes the new lock on the data that can be tested again in the future to make sure no damage or tampering has taken place.
This is what Bitcoin does to lock transactions and create currency at the same time. Bitcoin makes it's network peers compete against each other. Timekoin does not do this. It doesn't matter which peer found it first, thus network peers work together; not against each other.

How is currency created in Timekoin?

A: The Timekoin protocol allows a list of servers to create currency in small, gradual amounts for the time they participate in the network processing transactions. Before any server can do this, it must be elected by all the network peers. The election process is just servers that wish to join the list, sorted by public key and IP address. The process for selection is Random in the Timekoin network, so any server seeking this role has as good of a chance as any other server to be chosen by the Timekoin network. The more servers that are competing to join the list, the more peer elections that will take place. Timekoin elections are gradual and often only take place only a handful of times per day. That is by design for Timekoin to prevent a large entity from entering into Timekoin to produce large amounts of currency and then leaving with it just as quickly as it came in.

What is the security record of Timekoin?

A: The Timekoin protocol was first conceived of in February of 2010. Afterwards it had some development and finally a website by 2011. Some beta software releases were put out for testing and by 2012, Timekoin had hit version 1.0 stable release. Ever since then, the Timekoin network has been live and running 24/7 for years without a single exploit or hack. The Timekoin team even put up a bug bounty for security exploits that no one has been able to collect yet.

What happens if someone owns the majority of the existing server nodes? Can he (A) re-write history and/or (B) double-spend?

A1: Bob owns a server farm and has access to the largest share of Timekoin server nodes. Bob decides that since he has the majority, he should be able to create a transaction that rewards him millions of Timekoins for free. He starts by modifying Timekoin to disable safeguards for any Transactions he creates. He then sends his crafted Transaction into the Timekoin network for processing. What happens in Timekoin during this attack?

A2: When the Timekoin servers begin to process his transaction, the first issue they will encounter is that no one at the phantom public key address has 1 million Timekoins to transfer to Bob. So Naturally, the transaction would be discarded and never added to the transaction history.
But... Bob's server farm has ignored this check and added to the history anyway. So now a large majority of the Timekoin servers have this bogus transaction in the history and the other minority does not.

A3: After this process, all the honest Timekoin servers are communicating with Bob's server farm. The first issue that arises is that the last batch of Transactions don't match the SHA256 hash that Bob's servers are presenting. This triggers an audit where the honest Timekoin servers begin to start polling Bob's server farm to request data to prove that the transaction in question is valid. Because Bob created a false transaction from a Public Key that does not exist, there is no way for Bob's server farm to provide any proof of the origin of the transaction. This triggers more and more audits of the honest servers against Bob's server farm. Because it takes 100% of all network peers to change the transaction history, the honest Timekoin servers begin to purge Bob's server farm from the network. Eventually leading to a complete shut out for Bob.

B1: Using the same process above, Bob instead decides that he will instead try to double-spend his balance. He will create (2) transactions that breaks the rules against double-spending and makes sure that his server farm will allow it. Unfortunately for Bob, the same process that prevented him from tampering with the transaction history previously also applies to double-spending as it would count as a tampering of the transaction history, needing 100% peer agreement to be changed.

If someone runs a lot of nodes, how will the average Joe be able to get elected if the election queue will comprise of a large number of nodes under this someone's control vs. 1 of the average Joe's home server?

A: The Timekoin protocol allows a list of servers to create currency in small, gradual amounts for the time they participate in the network processing transactions. Before any server can do this, it must be elected by all the network peers. The election process is just servers that wish to join the list, sorted by public key and IP address. The process for selection is Random, so any server seeking this role has as good of a chance as any other server to be chosen by the Timekoin network. The more servers that are competing to join the list, the more peer elections that will take place. Eventually Joe's server will be elected, but he will have the odds stacked against him when someone else is also trying to get a large batch of controlled peers elected. Timekoin elections are gradual and often only take place only a handful of times per day. Joe's competition will need a lot of patience and time to get all of the controlling servers elected. It will cost money to patiently wait for this process. That is by design for Timekoin to prevent a large entity from entering into Timekoin to produce large amounts of currency and then leaving with it just as quickly as it came in.

If there are 100 nodes, and 99 nodes are trying for a hostile takeover, with 1 remaining node having the "true" transaction history, can that node propagate the "true" transaction history to correct the other 99 nodes and to make these 99 nodes change their transaction history?

A: The Timekoin protocol would not protect the 1 Lone server because as far as that 1 Lone server is concerned, 100% of the network is telling it something is wrong with the transaction history. The only saving grace would be that the hostile peers would not be able to feed invalid transaction data to the Lone server because it would still refuse to save it. But the combined effect would be that from whatever point in time this Lone server encountered a network full of hostile peers, only valid transactions could be processed and the hostile peers might simply refuse to send anything to the 1 Lone server. Thus leaving it basically isolated from the entire network. It would be the flip side of a bunch of honest peers removing a hostile peer from the network.

Can Timekoin address / cope with a sybil attack?

A: Timekoin has no reputation system. The closest thing to it is a peer failure score. When peers report data that is invalid or contrary to what the server knows to be true with transaction data or foundation hashes for example, this increases the peer failure score until it reaches the threshold set by the server administrator. Once this level is reached, the peer is kicked from the server connection list. The only thing that builds reputation in Timekoin is having a transaction history that can be verified mathematically by SHA256 data calculations from its own database. There is no added benefit for another hostile server to keep the lowest score, except to avoid being kicked from that other servers connection list which any honest server would not have issues with.

How is Timekoin affected by the coming Quantum computer age?

A: No encryption scheme is invulnerable. All encryption can be defeated with enough processing power and time. What sets Timekoin apart is that the users can upgrade encryption difficulty on the fly. This means it will always be a step ahead of Quantum computers and thus makes it future proof against such attacks. Quantum computers have to be built with more and more Qubits to quickly defeat strong levels of encryption. Timekoin can simply increase encryption and always remain one step ahead of such computers. There is no theoretical limit to what Timekoin can use and process but there is a finite limit to what size of Quantum computers can be physically built. The math available to Timekoin is infinite.

Example: It would take a “perfect” 3,072 Qubit Quantum Computer to crack the default 1,536 bit encryption of Timekoin. Right now as of this writing, there is no perfect quantum computer that big. Imperfect quantum computers are easier to make but it could take over +15 million qubits to work. It might happen next year or 20 years from now. Large “perfect” qubit quantum computers would take even longer. Timekoin users won’t sweat it because they can transfer their balance to a bigger encryption key in only 5 minutes. That means quantum computers will always be chasing Timekoin encryption used by its users and never catch it.