PEPEGOLD (PEPGD) – Digital cash system for the globetrotters

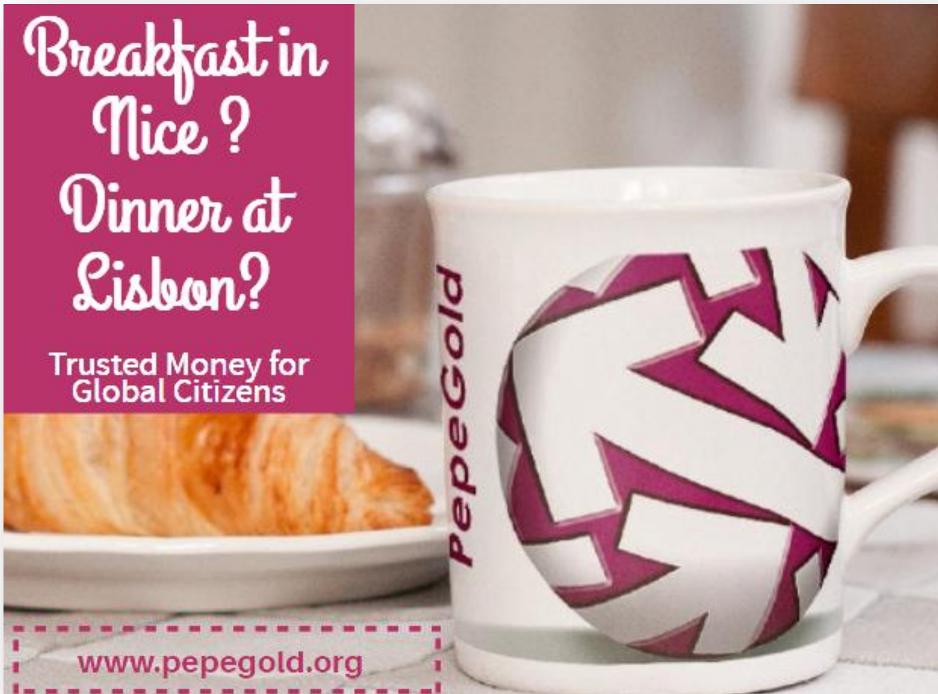
www.pepegold.org

Abstract

Experience the world and all its flavors!

Food loving globetrotters from all around the world find it difficult to keep track and make payments at the local food courts in cinemas, shopping malls, road side joints, cafeterias etc. PepeGold is developed with a vision to make it a globally accepted currency for the food courts and food loving travelers all across the world. PepeGold works towards bridging the international borders of money and language to become a leading replacement of local food vouchers or food cards accepted at food courts and restaurants. Food is the basis for business the activity of any person. Food production and sales are and will be growing as the population grows. Our platform will be put up to provide an equal access to a global market of consumable food items to the consumer food products and foodstuffs together with the modern financial instruments. This will create a vast market of readymade food with fair prices. PepeGold provides benefits to humanity through contributions to free food distribution. It is the only crypto-currency that rewards individuals for Spending on food contributions without the need for a central authority to distribute rewards.

A 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.

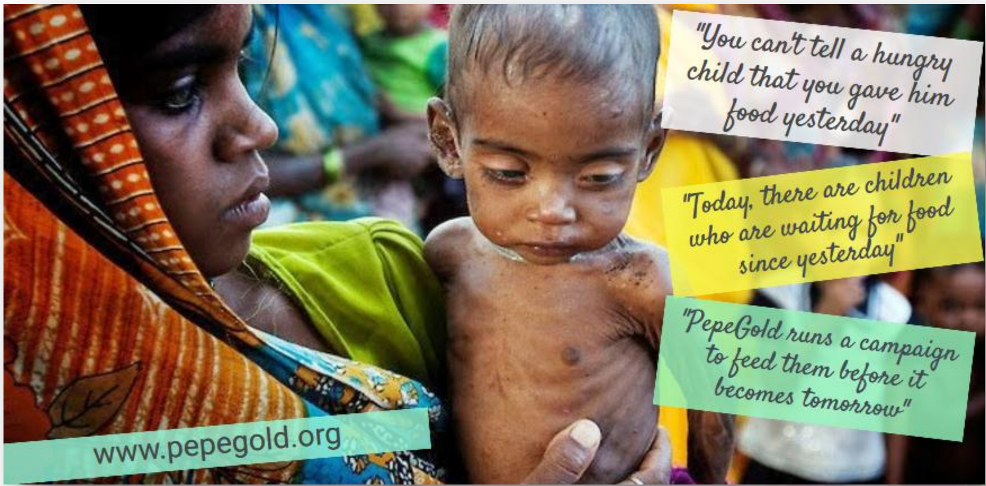


1. Introduction

PEPEGOLD (PEPGD) is a blockchain ecosystem, architecturally designed to create a global marketplace of food courts and readymade food outlets inclusive of cafes, restaurants, shopping malls, theatres etc. with the opportunity to add other platforms. 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 nonreversible services.

With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, asking them for more information than they would otherwise need. 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.

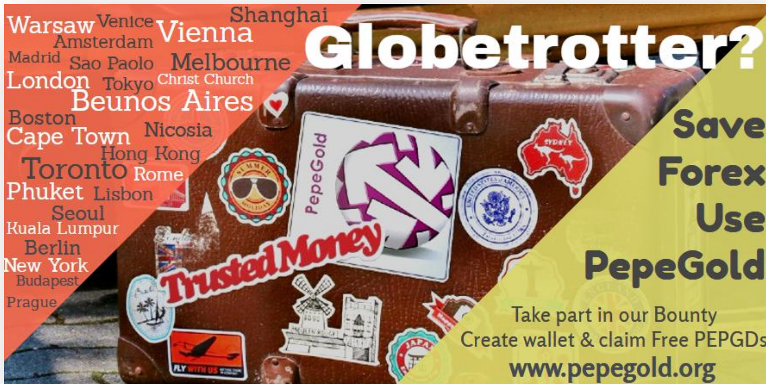
PepeGold is a decentralized, open source math-based digital asset (crypto-currency). It performs transactions peer-to-peer cryptographically without the need for a central issuing authority.



We plan to collaborate with government and non-government organizations in the integration of blockchain technologies to solve actual global problems, such as famine relief, disaster relief, and support of small farmers and uncontrolled global migration of agricultural population.
As a payment instrument, the platform will use its cryptocurrency – PEPEGOLD (PEPGD). All the parties of the transactions can freely exchange PEPGD for goods and services, buy and sell PEPGD on exchange markets.

2. Mission

The Mission of PEPGD as a business platform is to form a fully-featured ecosystem, bringing together all agents (sellers, buyers, money exchangers, banks, etc.) into a single blockchain platform.
Merchants of food products, such as coffee shops, restaurants, grocery stores, gastro-boutiques, will have access to the global market proposals directly from the manufacturers, for example, to the tea from a plantation in Sri Lanka, chocolate from a small manufacturer in Belgium or wine from a small winery in France. Similarly, consumers of food available, such as, tourists, local buyers, business visitors, etc. will have access to local markets without having to worry about the local currency and exchange rates.



Our goal is to provide a platform with simple and clear instruments available for travelling people who are not familiar with the world of blockchain technologies. We understand that apart from the technological limitations of blockchain-platforms, which are going to be solved over time, there are conception limitations of the common users, who are not ready (and don't have to) to key into the technology, and should have a wide and convenient set of instruments to solve their everyday tasks as the consumers. Based on this we are going to build a platform focused on the customer's needs. Consumers as well as the providers and distributors, will get equal access to PEPGD, creating a comprehensive global competition environment for producers of food and agricultural products. With minimum skills, the users will be able to find customers and suppliers, using the interactive map of Food Courts and outlets. The smart cards can be filled without involving foreign exchanges, and there is no need to maintain minimum Forex for daily expenses in a travelling destination. Lots of intermediaries will be excluded from the transactions, and this will provide significant cost savings while travelling. It will allow travelers to be better equipped with daily expenses in a traveling country especially if the exchange of local currency is higher.

3. Transactions

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. 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.

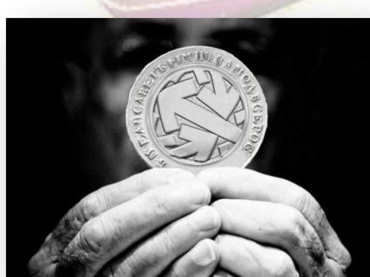
Timestamp Server

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

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system, 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. 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.



4. Network

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. 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.

5. Incentive

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. 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. 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, and using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favor him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

6. Reclaiming

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 8GB of RAM as of 2018, 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.

7. Simplified Payment Verification

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 time-stamped 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.

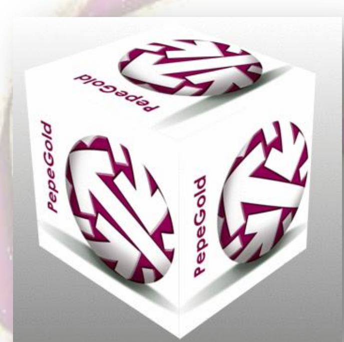
As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long 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.

8. 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.

9. 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.



10. Conclusion

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 rejoin 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.

11. Quick Facts

Algorithm	Scrypt
Type	PoW
Coin name	PepeGold
Coin abbreviation	PEPGD
Address letter	P
RPC port	32940
P2P port	32939
Block reward	50 coins
Block halving	210000 blocks
Coin supply	26250000 coins

12. Contact

EMAIL info@pepegold.org
WEBSITE www.pepegold.org
WALLET https://wallet.pepegold.org/

SOCIAL MEDIA

Slack: http://pepegold.slack.com
Facebook: https://www.facebook.com/pepegoldcoin/
Twitter: @PepeGoldCoin
Telegram: https://t.me/pepegoldcoin
Discord: https://discord.gg/8Upw6EG
Reddit: https://www.reddit.com/user/WeLuvPepeGold/
Bitcointalk: https://bitcointalk.org/index.php?topic=3045622