
gemscoin

Abstract. 1

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 ongoing 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 rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction 2

1. Introduction 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, hassling 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. 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.

2. Transactions 3

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 [1], 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.

4.EVOLUTION FROM WEB 1, WEB2, WEB3 TO THE METAVERSE 4

While there is no clear consent about the definitions of Web3 and the difference of the Metaverse, there is a lot of discussion. A lot of crypto enthusiasts like to believe that crypto is the next stage of the internet, while others argue that after the social interaction based Web2 we will see the jump into the immersive Internet called “Metaverse”. Till now it’s not clear where to set the cut and where to differentiate, but the discussion will continue if Web3 is crypto and blockchain or immersive internet with virtual worlds. www.metawebcoin.host 7 METAVERSE EXAMPLES There is no example of a big metaverse at the moment. Different companies, especially game studios, are claiming that they created a metaverse.

- **Meta Horizon Worlds** - Facebook launched a virtual meeting room environment which can be accessed via the company owned Oculus VR headsets and the Horizon Worlds. It allows interacting with peers in virtual meeting rooms with your own avatar but in future it should be also the basis for more offerings coming from Oculus and Meta.

- **Microsoft Mesh Platform** - Microsoft is also pushing into the mixed and extended reality space (XR). Therefore, they are trying to launch mixed-reality elements into Teams in 2022. This should allow avatars and holograms to be at events, meetings and even use it in future for retail experiences and gaming.

- **Roblox** - Roblox started as a gaming world where you can create your own games as a user and give others access to them. After the IPO, they are more pushing towards creating their own metaverse. Teaming up with brands like Vans and Gucci, they offer now also exclusive assents to buy for your virtual self.

- **Minecraft** - Over 140 million users are regularly playing the Lego like game world Minecraft. The company was bought from Microsoft where players create their character, a creation of unlimited virtual worlds on their own incl. digital assets and more.

- **Second Life** - Already founded in 2003 it was one of the first virtual realities where the player could

create an own identity in a virtual world. After many years of development, Second Life is also now expanding with own marketplaces, digital assets and more.

Before we go deeper into the technological details, let’s examine what kind of different elements and foundations need to be in place to enable a metaverse. Creating a virtual world where you can control every aspect and also feel like you are directly in this world has many challenges.

HARDWARE & INFRASTRUCTURE

Due to the massive amounts of data, 3D processing and also live interaction, there is a huge need for the right IT infrastructure. This includes network technologies from 5G and future 6G networks, cloud computing and super specialized virtualization hardware with GPU, TPU and CPU development for the server-side hardware requirements. The second part is the consumer side, where special hardware is needed for the immersive experience. Virtual and augmented reality smart glasses, haptic feedback devices (gloves, suites, etc.) and even mobile phones with better processing powers are needed.

TOOLS & STANDARDS

To make the metaverse really interactive, there need to be common standards and tool sets in place. This includes computer languages, easy to use design tools, commonly used 3D engines, VR/AR/XR standards, asset marketplace standards, transfer protocols, security standards but also more technological standards like geospatial mapping.

PAYMENT & TRANSACTIONS

An important aspect of every metaverse is a functioning ecosystem. In order to make this work, a universal mode of transaction and payment need to be found. This has challenges on several levels as every ecosystem might have their own modes of payment, transaction and makes it then difficult to connect different worlds together.

REGULATORY FRAMEWORKS AND RULES

Like in real world, we require regulatory frameworks and social rules in place. Managing and enforcing these rules in a virtual world could be one of the biggest challenges to solve. In order to make users

feel safe, we need to think about global rules and even laws that govern the virtual world.

IDENTITY MANAGEMENT & AVATARS

A virtual world with a virtual identity might sound good, but to make sure that it’s also safe and not a “outlaw” world, also the verification of the real identity is a must. For this to happen in many worlds, there would need to be a common protocol and something like a meta-identity that can be linked to the own avatars and therefore be able to use avatars and

6. Network **7**

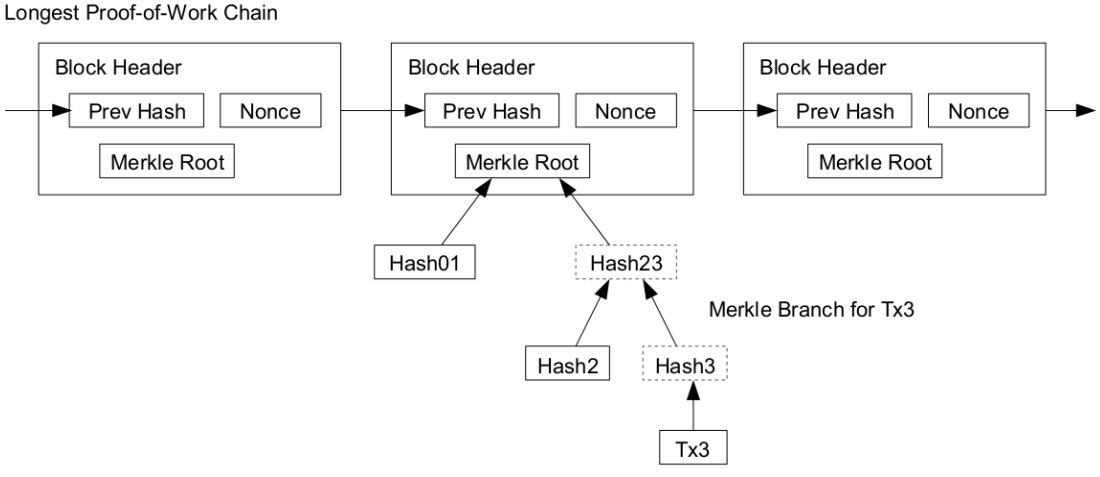
The steps to run the network are as follows: 1) New transactions are broadcast to all nodes. 2) Each node collects new transactions into a block. 3) Each node works on finding a difficult proof-of-work for its block. 4) When a node finds a proof-of-work, it broadcasts the block to all nodes. 5) Nodes 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 proofof-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one. 3 Block Prev Hash Nonce Tx Tx ... Block Prev Hash Nonce Tx Tx ... 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

7. 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, 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.

8. 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 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. 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.

9. TOKENIZATION

GEMS Coin is the utility token for the entire GEMS Finance ecosystem, traded and farmed on decentralized - Centralized exchanges across the Binance Smart Chain, Polygon, Solana &Ethereum*. GEMS is decentralized and owned by its own dynamic community. We welcome and embrace diverse perspectives to build GEMS into the best crypto community. To achieve this goal for every transaction in GEMS network, a 3% fee is distributed to existing holders. That means one can earn more GEMS Coin just by holding it in its wallet.

In each trade, the transaction is charged a fee, which is split in 2 ways:

2% Buy fee = redistributed to all existing holders

2.5% Sell Fee of the GEMS tokens are paired automatically with BNB and added as a liquidity pair on Pancake Swap. Metaweb Token is fully upgradable ERC-20 Token. In future we can add more functions and more product in our portfolio with just a smart contract update.

Tokenomics

Name: GEMS Coin

Contract Address: 0x676055B69a8167ff5e9d84640ED1ab6B4cA43e7C Network: BEP20 Symbol: GEMS Decimals: 18 Total Supply: 1,000,000,000,000 GEMS

Legal Notices

This whitepaper is made available to provide business information and it does not constitute a contract or an offer of sale between the reader and GEMS. The information found in this document is subject to change. This means key aspects of the project may change or be abandoned at any time. This includes, for example, token economics and dates for any planned security coin offering. The information contained in this whitepaper is not written or intended as financial, tax or legal advice. You are encouraged to seek financial, tax and legal advice from your professional advisors. GEMS provides no guarantee as to the completeness, reliability, relevance, or accuracy of information found in this whitepaper. GEMS makes no representations or warranties of any kind, express or implied, and is not responsible for and disclaims all liability for any loss, liability, damage (whether direct, indirect or consequential), personal injury or expense of any nature whatsoever which may be suffered by you or any third party, as a result of or which may be attributable, directly or indirectly, to your access and use of any information contained in this whitepaper. Any plans, forecasts or projections mentioned in this whitepaper may not be accomplished in whole or part due to multiple and compounding factors, including but not limited to defects or limitations in technology, legal or regulatory exposure, sector volatility, corporate actions, and/or market inconstancy.All information contained in this document is intended to be indicative only and is not a statement of GEMS intentions. GEMS reserves the right to revise this whitepaper at any time and for any reason.