EMA Coin

Eco-friendly, Layer 1 Coin

on

WEM Blockchain

Mark Karodine
Alex Kooistra
wemblockchain@proton.me
www.worldecomoney.com

February 2023, Rev. 1.1

Abstract.

The PROBLEM:

Unfortunately, the vast majority of cryptocurrencies known today have several major design flaws that render them unsuitable for their primary purpose: to ease peer-to-peer payments and eliminate the need for trusted parties.

Let us look at some profound issues:

1. Expensive and unpredictable fees can add up quickly based on factors largely beyond the user's control.

2. As the number of transactions increases, so does the time it takes to confirm a transaction.

Although some large Layer 1 PoS networks may generate blocks every 20-30 seconds, it is still too sluggish for many applications, making it unsuitable as a payment method.

Other large networks claim to be able to process millions of transactions per second, but this comes at the expense of scalability and increased demand for node

hardware and connectivity, all of which make decentralization more difficult and costly.

In some PoS protocol implementations, a higher "bidder" can gain 51% network control, posing a severe security risk to the integrity of the entire blockchain.

There are other issues as well, but even the ones stated earlier make peer-to-peer payments challenging enough.

3. Second Layer.

While transactions can be processed much faster at the token level, most of them have one major drawback:
By their nature, tokens are SmartContracts that have an "owner" who can "modify" them, so this is another central authority and trusted party.

Even if modification is disabled, the owner of the private key for the SmartContract may or may not have access to other functionalities like pausing, stopping, or other "features" of a similar nature.

A smart contract is, by definition, a piece of code that must be audited before it can be trusted.

To put it simply, a token is a smart contract that represents another trusted party on which to rely and is not a cryptocurrency.

The SOLUTION:

We want cryptocurrency to be:

1. Fast, instantly conducted transactions.
2. Cheap to use, low, fixed, predictable commissions.
3. Layer 1, on its own blockchain.
4. Decentralized, allowing anyone to participate
5. Interchangeable, bridged to other networks
6. Volatile, but backed by collateral.

*. To implement a fast blockchain with near-instant transactions, we'll redesign the way blocks are created and indexed (see the WEMNIT protocol).

* We designed our blockchain in the following way to implement low and fixed commissions:

* The list of costs cannot be changed faster than X days (currently set to 90 days).

* The smallest commission should be one cent.

* The maximum commission may not exceed X% (currently set to 0.01%) of the transaction amount.

1. Introduction

EMA Coin allows any two willing parties to transact directly with each other without the need for a centralized, trusted third party.

EMA Coin is intended to be a simple, fast, decentralized, cheap, scalable, and environmentally friendly Layer 1 cryptocurrency that can be used for peer-to-peer payments.

WALLETS:

Digital signatures provide cryptographic proof of wallet ownership.
Hierarchical Deterministic (HD) wallets derive their keys from a 12-word passphrase
as described in BIP-39, which has been proven to be the best practice.
WEM infrastructure will leverage that with minor adjustments[1].

The next step is to bind wallet IDs to the user's phone number.

To make transactions easier, funds can be transferred simply between phone numbers.

A wallet ID can be linked to a user's phone number.

After registering a phone number with the blockchain, any node would be able to resolve it to a EMA Coin wallet ID.

NETWORKS:

Blockchain and protocols have to be written from scratch to achieve our goals. Cloning or modifying any existing blockchain software and/or protocols is not an option, as all the issues of those projects will be cloned as well.

The WEM Near Instant Transaction (WEMNIT) protocol accomplishes this much faster; the WEM blockchain becomes more scalable than PoW, for example, and much more environmentally friendly.

The network itself requires minimal structure. Messages are broadcast every time transactions occur and once another block is formed.

If the network becomes overloaded, WEMNIT enabled Community Nodes are added in random order from TestNet to MainNet.

Priority is given to the oldest nodes.

To check wallet balances and prevent double-spending, EMA Coin relies on a decentralized blockchain (WEMblockchain) that runs the WEMNIT protocol, which is an extended version of the D-PoS[3] protocol.

2. Transactions

The transaction works as follows:

* The wallet connects to one of the WEM top-level domains hard-coded into the node core and receives an updated list of nodes.

* The wallet can reconnect to the nearest node if necessary. At this point, wallets are able to receive transactions from the network.

* The wallet generates a unique pair of keys as well as the receiving address[1] Once a valid transfer address and sufficient amount to transfer are provided and confirmed using the correct user password, the wallet will generate a raw transaction and sign it with the wallet private key before sending it to the connected node.

* The node will broadcast the received transaction, validate it, and send it to all Delegated Nodes

The transaction will be received and validated by the node using the wallet's public key (derived from the sender address).

If everything is true, node will sign this transaction, and as a result, an ID will be added to the transaction and sent back to the wallet.

Node will broadcast this transaction to other Delegated Nodes that have been chosen for creating and signing the block for confirmation and inclusion in the block.

Each delegated node will generate an independent block of valid transactions that must correspond to other delegated nodes.

If at least 70% of Delegated Nodes have identical blocks, it's deemed valid and added permanently to the blockchain.

All of this information is sufficient to run a fully functional distributed ledger.

Example of transaction data:

[{
"timenode":"1640084459",
"block":"",
"vernode":"101",
"verclient":"101",
"keyopen":"12Xna7YZwQDsHo7gzDdhviKhcgDZDNFuaaNwy3drDnigve1URFbZNicFkawDyvNxUZgNoFykwfbCpEPWyeYeUbWxT49f9",
"from":"WEM12Xna7YZwQDsHo7gzDdhviKhcgDZDNFuaaNwy3drDnigve1URFbZNicFkawDyvNxUZgNoFykwfbCpEPWyeYeUbWxT49f9",
"to":"WEM1X3KEbESdznBtm2eeBtVQmxgDXcE8Hq6yu5zEkD9AouySSYjuiBXJx7AxLqBZnZe6gp51s1yEvXKRLD16bsrnxE",
"value":"10",
"rem":"",
"timeclient":"1640084459",
"merkt":"",
"hash":"60a22f7520f329c263faaf6b74b675eeeddbbf954a023461674d8e8b086cd75f",
"sign":"11208ee3231979874e7272e452fcbc432892f13232bf768851916141f8db3d1ad9db77b9c2051864402f64050d90e3bec2c9c9d249f21529a58c21b7cdc8ca7e",
"node":"WEM12Xna7YZwQDsHo7gzDdhviKhcgDZDNFuaaNwy3drDnigve1URFbZNicFkawDyvNxUZgNoFykwfbCpEPWyeYeUbWxT49f9",
"trxid":"090250c90237190bc891f14bca68ed408974c2b9edd567342477cf547dc9fb1b00542f9356e823059edd2600c5aa9175c6f5cd955c74b81af2f822bb49bba3a7"
}]

All this data is sufficient to maintain a fully functional distributed ledger.

3. Blockchain

WEM Blockchain is a distributed ledger, a smart, decentralized database shard made up of community nodes that run the WEMNIT protocol.

A block consists of the previous valid block ID, the current block ID, a list of all transactions that occur during that period, and a list of Validators' (Delegated Nodes) that make that block valid (or invalid).

* Although the blockchain data will remain largely unchanged during implementation, the structure of the WEMNIT protocol may change:

An Example of a Block:


```
  "{{BLOCK ID}}": {
    "time": "1640081830",
"preid":"e852ab5c2526e38eae8975707d992401d5e329824fcdefcf1aac93cfa3c364568","id":
"3dcbbf241f4c6f4c47d6e5707d992401d5e329824fcdef233de499d6335f4213",
    "trnids": [
 "10587b070e96ecfed9c8a694deb4bc32c0b88649d6e7f022e7634bf2ca1dc8df",
"5218adba0a250cec8a9b2fae852ab5c2526e38eae897b20970609d04371aa435","91e72270bc5a3e3f4948c77b056181cf1aac93cfa3c363cbc5930b241965ee5b" ],
"validnode": [
      {
        "address": "...",
        "sign": "..."
      },
      {
        "address": "...",
        "sign": "..."
      }
    ],
 "invalidnode": null
  }
```

4. WEMNIT Protocol

EMA Coin works on the WEMNIT protocol, which is a delegated proof-of-stake protocol consensus mechanism based on fast, dynamic Practical Byzantine Fault Tolerance[6] and proactive recovery.

All participating nodes have to stake in order to be chosen as block Validators'. The WEMNIT protocol has been written from scratch and optimized for speed and scalability.

Byzantine Fault Tolerance can be achieved if the correctly working nodes in the network reach agreement on their values. There can be a default vote value given to missing messages, i.e., we can assume that the message from a particular node is "faulty" if the message is not received within a certain time limit. Furthermore, we can also assign a default response if the majority of nodes respond with the correct value.

Leslie Lamport proved that if we have 3m + 1 correctly working processors, a consensus (an agreement on the same state) can be reached if at least m processors are faulty, which means that strictly more than two-thirds of the total number of processors should be honest.

Types of Byzantine Failures
There are two categories of failure that are considered. One is fail-stop (in which the node fails and stops operating) and the other is arbitrary-node failure. Some of the arbitrary node failures are given below:

* The inability to return a result
* Respond with an incorrect result.
* Respond with a deliberately misleading result.
* Respond to different parts of the system with different results.
As the number of nodes increases, the system becomes more secure.

5. Nodes, Stakers, Rewards

EMA Coin is a community-driven, decentralized, cryptocurrency.

EMA Coin transactions incur a small fee. This small fee ensures the following:
1. No spam transactions can enter the network.
2. Participants can get paid for running their nodes.

Although all transactions are subject to a small fee, the WEM community's main goal is to keep those fees as small as possible. Transparency of the system is a main priority.

Anyone can run a WEMNIT node in order to participate in the EMA Coin network. Anyone can become a Validator and receive a portion of the reward from each validated block.

In order to become a Validator, a node must do two things:
1) Join TestNet and become fully operational there.
2) Deposit collateral.
3) Sign MainNet Node Agreement.

To become a Validator node, a certain amount of collateral specified in the MainNet Node Agreement must be deposited in a major cryptocurrency such as Bitcoin, Ethereum, or EMA Coin.

Following that, the node is added to a test network and awaits selection. Nodes are selected randomly when the number of transactions increases.

The WEMNIT protocol does not favor those who deposit the most;

To ensure decentralization, all Validators' must deposit the same amount and will be chosen pseudo-randomly to validate each block.

Validators' nodes will be chosen randomly to join the MainNet from the TestNet when the transaction volume increases.

Unless a node violates the MainNet Agreement, selected nodes will never leave the MainNet; even if volume drops, once selected nodes will remain in the MainNet indefinitely.

6. Payment Verification

Every time funds change hands remotely, there are 3 things that must be confirmed:

1. Release of funds authorized by the legal account or wallet owner. Currently, in financial institutions, it’s done by checking the person's physical ID or PIN code. None of these methods is as secure as digital signatures, which are used by the vast majority of cryptocurrencies, including EMA Coin.

After verifying the wallet owner's signature, a node that receives transactions from a wallet generates a Transaction ID and broadcasts it to Validating Nodes.

2. The proposed transaction amount is equal to or less than the account or wallet balance. Currently, financial institutions have to check account balances (databases) against the proposed amount. EMA Coin verifies wallet balances by querying an open (decentralized) ledger.

Every Validating Node double-checks ownership of the wallet as well as fund sufficiency before a transaction can be added to the block.

3. The funds that stack in the loop between transactions cannot be double spent. EMA Coin accomplishes this by limiting the number of transactions per wallet in a short period of time. After that time, we can confidently assume that the transaction is complete.

Every Validating Node checks Mempool, and if a wallet has already placed a transaction, further wallet activity will be denied until the current transaction is complete.

Use of the Merkle tree[7] simplifies transaction verification.

7. Applications

For Developers:
* Create your own Layer I coin with the desired properties.
* Participate in maintaining the WEM core software.

For Investors:
* Participate in exciting sustainable projects while earning dividends on your investments.

For Traders:
* Trade Layer 1 decentralized network.

Because all tokens are smart contracts, they have a single authority that controls the smart contract private keys. That is, smart contracts are technically owned. That means SmartContract is just another trusted party.

Those mentioned above are just a few examples of why EMA Coin was created in the first place. EMA Coin can and most likely will be used in other applications in the future.

8. Privacy

EMA Coin blocks data stored in a public ledger. All blockchain transactions can be viewed theoretically by anyone with a wallet ID.

HD (Hierarchical Deterministic) Wallets[7] used by EMA Coin add a second layer of privacy by allowing funds to be (re)distributed among multiple differently looking wallet IDs associated with a single master account.

Another approach under consideration for the future is the Floating Genesis Block. Technically, this strategy would erase the entire blockchain history and establish a new genesis block with current to-event ledger data.

9. Conclusion

The payment system we've presented addresses a slew of issues with most major coins such as BTC, ETH, and various other cryptocurrencies, allowing EMA Coin to be used as it was intended, as real peer-to-peer money.

Due to some outstanding concerns, EMA Coin developed in a somewhat different way than WEB 3:

1. Transaction speed has been significantly increased to roughly one second.

2. Transaction fees are predictable and kept to a minimum.

3. Layer 1 decentralized infrastructure eliminates the need to rely on any trusted third party.

4. WEM Blockchain interconnection allows users to access other blockchains and decentralized exchanges and trade cryptocurrencies between them.

WEMNIT D-PoS protocol ensures that things are green, fast, and scalable.

Although the WEMNIT protocol has matured tremendously, it is still in its infancy and under heavy development. There's more to it!

10. References

[1] https://en.wikipedia.org/wiki/Cryptocurrency_wallet
[2] https://en.wikipedia.org/wiki/Byzantine_fault
[3] https://en.wikipedia.org/wiki/Proof_of_stake#Delegated_proof_of_stake_%28DPoS%29
[4[https://www.investopedia.com/tech/goldpegged-vs-usdpegged-cryptocurrencies/
[6] https://www.microsoft.com/en-us/research/wp-content/uploads/2016/12/The-Byzantine-Generals-Problem.pdf
[7] https://www.investopedia.com/terms/h/hd-wallet-hierarchical-deterministic-wallet.asp
[8] https://en.wikipedia.org/wiki/Merkle_tree