

World Eco Money

Eco-friendly, Layer 1 Blockchain

WEM Blockchain

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

NOV 2023, Rev. 2.5

Abstract.

Common Issues:

Unfortunately, the vast majority of blockchains 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's take a look at some most profound issues:

1. Unpredictable(i) and rather substantial(ii) **fees** that creep up quickly due to factors mostly beyond the user's control.
2. As the number of transactions increases, so does the time(i) it takes to confirm a block.

Although some 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 in milliseconds, 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.

3. **Volatility** of native coins(i): Because most blockchains only support a single(ii) native coin on the first layer that has no fixed value and isn't linked to any tangible asset, its value is determined by the volatile cryptocurrency market.

4. Second Layer

The majority of StableCoins on the market today are tokens rather than actual coins. Because they were built on top of another blockchain, adding another layer to that one.

Tokens have been developed primarily for traders who need to fix their profits.

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" so this is another central authority and trusted party.

A SmartContract is, by definition, a piece of code that must be audited before it can be even trusted. Owner of the SmartContract may or may not have access to functionalities like pausing, stopping, blacklisting and/or other "features" of a similar nature.

To put it simply, a token is a SmartContract that represents another trusted party and is not a cryptocurrency.

4. 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.

Proposed Solution:

We want blockchain and its native cryptocurrency to be:

1. Fast, (almost) instantly conducted transactions.
2. Stable, pegged to a physical asset or currency, such as real world hard currency.
3. Cheap to use, low, fixed, predictable commissions.
4. Layer 1, on its own blockchain.
5. Decentralized, allowing anyone to participate
6. Interchangeable, bridged to other networks

To implement a fast cryptocurrency, we must build a brand new blockchain with near-instant transaction capabilities, as well as redesign how blocks are generated and indexed (see the WEMNIT protocol).

To ensure a stable value for the native StableCoin (WEM coin), we will design the blockchain as follows:

We create bridges to all major blockchains starting with Ethereum and Bitcoin.

Once a supported cryptocurrency has reached the bridged wallet and confirmed, there are 2 (or more)[4] ways we can address it:

Phase A: It will be converted into a StableCoin and/or token of our choice that will be used as collateral.

Phase B) The liquidity providers will be responsible for allocating appropriate crypto collateral (single or portfolio), but conversion must occur at the current USD rate.

After that, exactly the same stable number of WEM coins will be minted and credited.

If WEM Coin must be converted back into one of the supported cryptocurrencies, it will be burned (transferred to a zero address without a private key).

WEM blockchain is designed to use low and fixed fees in the following ways:

- * 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.

The Core Principles:

We believe in being fast enough, not necessarily the fastest. We strive to be affordable to the majority, not just the cheapest. And we prioritize providing a trust-less system that is open to anyone, rather than aiming to be the most trusted. Join us on this unique journey as we redefine success based on these three core principles.

Those essential tradeoffs will be acceptable in most applications anyway, allowing us to focus on what matters most: resolving the blockchain trilemma of decentralization, scalability, and security.

1. Introduction

To achieve our objectives, we have agreed to the following "limitations":

. Transaction completion time: 1 to 5 seconds max! depending on transaction value in simple 3 tiers. WEMNIT protocol processes transactions according on their value, with only three speed tiers: **transactions up to \$10,000 USD are limited to one second completion**, whereas transactions of \$1,000,000 or more may take a little longer because more validation cycles must be conducted.

. Transaction fees: 0.01 cent to 0.99 cents max! depending on transaction value in simple 3 tiers. With just three tiers - 0.01 cent, 0.50 cents, and 0.99 cents - based on the transaction amount, we ensure that every transaction remains affordable without compromising on the quality of service.

. Node availability: 10 to UNLIMITED shards and nodes depending on transaction volume.

COINS:

* WEM Coin

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

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

WEM Coin has been created to challenge other StableCoins[5] that exist today mostly on top of Ethereum or other WEB3 blockchains as Layer 2 smart-contract centralized tokens.

* EMA Coin

Every EMA coin holder has a stake in the WEM blockchain, which can be delegated to a stake pool to collect rewards. EMA will eventually be usable for a wide range of WEM blockchain apps and services.

* There's more native Layer 1 coins can (and will be) created.

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 WEM 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, WEM Coin relies on a decentralized blockchain (WEMblockchain) that runs the WEMNIT protocol, which is an extended version of the D-PoS[3] protocol.

RESUME:

WorldEcoMoney is a proof-of-stake blockchain platform which enables anyone to build any kind of applications within its ecosystem.

Although we provide on-chain SmartContract auditors, we strongly encourage people to use our Layer 1 coin builder to create custom coins and use Smart Contracts for more complex applications such as exchanges and escrow portals.

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": "12Xna7YZwQDsHo7gzDdhviKhcgDZDNFuaaNwy3drDnigve1URFb
ZNicFkawDyvNxUZgNoFykwfbCpEPWyeYeUbWxT49f9",
  "from": "WEM12Xna7YZwQDsHo7gzDdhviKhcgDZDNFuaaNwy3drDnigve1URF
bZNicFkawDyvNxUZgNoFykwfbCpEPWyeYeUbWxT49f9",
  "to": "WEM1X3KEbESdznBtm2eeBtVQmxgDXcE8Hq6yu5zEkD9AouySSYjuiBXJ
x7AxLqBZnZe6gp51s1yEvXKRLD16bsrnxE",
  "value": "10",
  "rem": "",
  "timeclient": "1640084459",
  "merkt": "",
  "hash": "60a22f7520f329c263faaf6b74b675eeddbbf954a023461674d8e8b086c
d75f",
  "sign": "11208ee3231979874e7272e452fcbc432892f13232bf768851916141f8db
3d1ad9db77b9c2051864402f64050d90e3bec2c9c9d249f21529a58c21b7cdc8c
a7e",
  "node": "WEM12Xna7YZwQDsHo7gzDdhviKhcgDZDNFuaaNwy3drDnigve1URF
bZNicFkawDyvNxUZgNoFykwfbCpEPWyeYeUbWxT49f9",
  "trxid": "090250c90237190bc891f14bca68ed408974c2b9edd567342477cf547dc
9fb1b00542f9356e823059edd2600c5aa9175c6f5cd955c74b81af2f822bb49bba
3a7"
}
```

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

WEM blockchain 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

WEM blockchain is a community-driven, decentralized, blockchain.

Instrument 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 and stable as possible. Transparency of the system is a main priority.

Anyone can run a WEMNIT node in order to participate in the WEM 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 WEM 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 real 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 WEM blockchain.

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. WEM blockchain 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. WEM blockchain accomplishes this by limiting the number of transactions per wallet in a short and fixed period of time that currently equals 1 second exactly. 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 the End User:

- * Pay instantly for the goods anywhere around the globe with a single, stable currency by just using a mobile phone.
- * Keep your money safe.

For Merchants:

- * Increase sales by accepting an additional payment method.

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:

- * Profits can be fixed in a StableCoin on Layer 1 decentralized network.

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

8. Privacy

WEM blockchain 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 WEM 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 blockchains and coins such as BTC, ETH, and various other cryptocurrencies, allowing WEM blockchain and its native instrument WEM Coin to be used as it was intended, as real peer-to-peer money.

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

1. Transaction speed has been significantly increased to roughly one second.
2. WEM Coin's volatility has been mitigated by linking it to real-world currency (USD) through the usage of other cryptocurrencies as collateral.
3. Transaction fees are predictable and kept to a minimum.
4. Layer 1 decentralized infrastructure doesn't call for any trusted third parties.
5. WEM blockchain bridges 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/>
- [5] <https://en.wikipedia.org/wiki/StableCoin>
- [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