Bitweb A new Peer-to-Peer Electronic Cash System .

White Paper

Version 1.2

Website：https://bitwebcore.org

Explorer：https://explorer.bitwebcore.org

Official forum：https://community.bitwebcore.org

GitHub：https://github.com/bitweb-project

Twitter：https://twitter.com/BitwebBTE

Birth background

Bitcoin was released in 2009. With the development of bitcoin, there are many problems.Satoshi want to change the centralized cash system, I have to say that he did, but I believe that the current bitcoin is not what he wants to see.

Problems of bitcoin:

1. Mining needs professional mining machine,As a result, not everyone can participate and use bitcoin.
2. The essence of bitcoin has changed, not as a cash system without a center, but as a tool, more like a game.
3. The transaction speed is slow. The block time of bitcoin is 10 minutes, and 6 blocks are needed to confirm the transaction, resulting in blockchain congestion.

Bitweb wants to solve these problems,so it was born.Bitweb (BTE) is based on the source code of bitcoin. Its code is the latest version. Its code is more complete than LTC and Doge, and some features are ahead of bitcoin.

Bitweb based on bitcoin,It's also a decentralized cash system.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.

Bitweb is an alternative to bitcoin and will stick to its own development path. It is our goal to involve and use more people.

Name: Bitweb
Tinker: BTE
Block Reward:50 BTE
Algo: Yespower
Premine: 2580000
Block time: 60 seconds

Max Supply:84,000,000(84 Million)minable,Absolute86,579,950
Maturity time: 100 Block’s
Proof Type: POW
Diff: LWMA
Address letter prefix: E(33)
Segwit Address prefix: D(30)
Bech32 Address prefix: web
Deffault rpc port: 1604
Deffault p2p port: 1605

Transactions

The block time of bitweb is 60 seconds, which shortens the transaction time by ten times. The blockchain will not be congested.Please read the following for detailed technology.

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.

/src/consensus/consensus.h

```
static const unsigned int MAX_BLOCK_SERIALIZED_SIZE = 4000000000;
static const unsigned int MAX_BLOCK_WEIGHT = 4000000000;
static const int64_t MAX_BLOCK_SIGOPS_COST = 80000000;
```

Proof-of-Work

Bitweb also uses POW,it is a relatively simple and fair consensus mechanism.Bitweb uses yespower of CPU algorithm,Reduce the cost of getting bitweb,Anyone can participate and use it.

View source src/primitives/block.cpp

```
uint256 CBlockHeader::GetHash() const
{
    return SerializeHashYespower(*this);
}
```

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 LWMA.

View source src/pow.cpp

```
unsigned int LwmaCalculateNextWorkRequired(const CBlockIndex*
pindexLast, const Consensus::Params& params)
{
    const int64_t T = params.nPowTargetSpacing;
    // N=45 for T=600.  N=60 for T=150.  N=90 for T=60.
    const int64_t N = params.nZawyLwmaAveragingWindow;
    const int64_t k = N*(N+1)*T/2;
    const int height = pindexLast->nHeight;
    assert(height > N);
    arith_uint256 sum_target;
    int64_t t = 0, j = 0, solvetime;
        for (int i = height - N+1; i <= height; i++) {
        const CBlockIndex* block = pindexLast->GetAncestor(i);
        const CBlockIndex* block_Prev = block->GetAncestor(i - 1);
        solvetime = block->GetBlockTime() - block_Prev->GetBlockTime();
```

```
        solvetime = std::max(-6*T, std::min(solvetime, 6*T));
        j++;
        t += solvetime * j;
        arith_uint256 target;
        target.SetCompact(block->nBits);
        sum_target += target / (k * N);
    }
    if (t < k/10 ) {   t = k/10;  }
    arith_uint256 next_target = t * sum_target;
    const arith_uint256 pow_limit = UintToArith256(params.powLimit);
    if (next_target > pow_limit) {
        next_target = pow_limit;
    }
    return next_target.GetCompact();
}
```

Developer

- Mraksoll
- Jcchain

Development plan

Bitweb released in May 2021.
May to December 2021 use pre mined coins to develop mines and communities. Mines can let more people participate in it, and developing communities can let more people use it.

other

Do you think there is no innovation in this coin? Don't forget that this coin is based on bitcoin,We just want to make some changes and achieve our goals. Bitweb is not a game.Everyone has a different point of view,let our faith come back.

More project features can be viewed in combination with bitcoin white paper.

References

Nakamoto S.(2009):Bitcoin:A peer-to-peer electronic cash system. (http://www.bitcoin.org/bitcoin.pdf)