MOTION

Moving Ideas Forward

Abstract. Motion (MTN) aims to provide investors and corporations the means to transfer assets including money, property, and shares from one holder to another. This can all be accomplished in a transparent, conflict-free way, all the while avoiding the service fees associated with traditional methods of asset transfer using an intermediary.

1. Introduction

The introduction of Bitcoin in 2009 brought a plethora of innovative possibilities for blockchain technology. Hundreds of new cryptocurrencies have since been produced, each bringing new ideas, and new possibilities. However, with the huge expansion in blockchain technology came new challenges and vulnerabilities. Motion's development team aims to fill the gap in the funding industry by creating a blockchain that ensures the safe and secure transaction of assets between two users, while maintaining anonymity. Motion is a decentralized blockchain platform optimized to support smart contracts with the foresight of helping the transfer of assets via the blockchain. The Motion project applies a combination of the protocol of Bitcoin and that of Dash to create a blockchain specifically aimed at smart contracts. This is done through the use of both Proof of Work (PoW) and Proof of Stake (PoS) technologies. While Bitcoin and Dash have revolutionized the financial industry, they have lost their integrity as a decentralized cryptocurrency due to the creation of Application-Specific Integrated Circuit (ASIC) mining equipment. These machines allow a few people to control the majority of the network, defying the original goal of decentralization. Motion aims to solve this problem by using an ASIC resistant algorithm to give the general public equal footing and stop any person or entity from performing a 51% attack.

2. Smart Contracts

Motion smart contracts are a secure computer based protocol that assists with verifying and enforcing a contract that has been negotiated between two entities. Smart contracts cannot be altered without the approval of both parties, and are confirmed with every block on the blockchain, reinforcing the negotiated contract. Traditionally, using this technique, the transaction would take hours or days to complete, and would cost a significant amount of money. Through the Motion platform, smart contracts between investor and creator will be tracked on the blockchain without a middleman to profit from the exchange. Our goal is to also bridge the gap between creators and the global community. Using smart contracts, creators can build and market their ideas within the Motion platform.

2.1 Real World Application

Smart contracts define the rules and penalties around an agreement similar to traditional contracts, but they also enforce those obligations automatically. Smart contracts are made up of three key features:

- A contract is written between two entities. This contract is then added to the blockchain as code. The individuals involved are anonymous, but the contract is public.
- An event, like an expiration date, is hit and the contract executes itself according to the coded terms.
- Regulators can use the blockchain to understand the activity in the market while maintaining the privacy of individual actors' positions.

To better understand this, suppose person **A** wants to buy a house from person **B**. This can be done using the Motion blockchain. **A** sends the agreed price to the smart contract. **B** sends the digital entry key and all required ownership paperwork to the smart contract. Once both parties have met the terms of the contract, the assets will be automatically distributed as agreed upon. If the terms were not met by the specified date, both **A** and **B** get their assets back and the contract is terminated. In the same way, smart contracts can be used for a large variety of situations ranging from financial derivatives to insurance premiums, breach contracts, property law, credit enforcement, financial services, legal processes and crowdfunding agreements[1].

2.2 Smart Contracts' Characteristics

Smart contracts provide the following essential characteristics:

- Autonomy: the two parties involved create the agreement and define the terms without the need for a broker or a lawyer.
- Trust: the content of the contract and all of its related material are encrypted on a shared ledger.
- Backup: there is no chance of losing any important material as all documents are duplicated many times over on the blockchain.
- Safety: your documents are safe on the blockchain thanks to advanced cryptography.
- Speed: the code executes automatically, which can significantly facilitate business processes.
- Accuracy: smart contracts avoid the errors that come from manually filling out forms.

2.3 The Future of Smart Contracts

While smart contracts are an incredibly innovative idea, it is nowhere near perfect. Using the previous example, what happens if person **B** sends the wrong entry key? What happens if the house being sold is condemned before the sell date? With a traditional contract, a simple court session can rescind the terms of the contract. In the blockchain, the contract performs no matter what. This is why the Motion team believes that there is still a lot of work to be done to solve these problems. The future of Motion lies in untangling these issues.

3. ASIC Resistant PoW

When Bitcoin was created, it set out to solve the centralization problem that banks and other financial institutions introduce. These entities have total control of all assets that the general public trusts them with, and they can, as has already been shown around the world, prohibit people from accessing their own money. Big financial institutions can also manipulate the market value of a currency. The creator of Bitcoin Satoshi Nakamoto once said "One CPU, One Vote"[2], referring to the decentralized PoW aspect of Bitcoin. With the birth of Application-Specific Integrated Circuit (ASIC), the original decentralization goal of Bitcoin was jeopardized, as these machines can mine Bitcoin and Dash thousands of times more efficiently than any desktop computer. This created a monopoly, where a few people with the capital to purchase and maintain these ASICs now had control over the network, and are able to manipulate prices for their own benefit.

The Motion team fully understands the danger of these ASIC machines. Motion's PoW hashing algorithm is X16R, which intends to solve this problem by constantly disrupting the ordering of the hashing algorithms. The X16R hashing algorithm is made up of 16 hashing algorithms that operate in a chain fashion. The ordering depends on the last 8 bytes of the hash of the previous block[3].

The 16 hashing algorithms are as follows:

0 → blake	**8** → shavite
1 → bmw	**9** → simd
2 → groestl	**A** → echo
3 → jh	**B** → hamsi
4 → keccak	**C** → fugue
5 → skein	**D** → shabal
6 → luffa	**E** → whirlpool
7 → cubehash	**F** → sha512

This reordering does not make it impossible to build an ASIC, but makes it more difficult and expensive. The Motion team is committed to keeping Motion ASIC resistant, and will make any necessary changes in the future to ensure it remains that way.

4. LWMA Difficulty Algorithm

The Linearly Weighted Moving Average (LWMA) difficulty algorithm is currently one of the best algorithms. This is because it has the lowest standard deviation during constant hash rate, allowing it to be very stable all the while maintaining the fastest response to hashrate changes[4].

The LWMA algorithm estimates the current hashrate in order to set the difficulty. The block time is maintained by dividing the harmonic mean of the difficulty by the linearly weighted moving average of the block times as shown below:

$$d = harmonicMean(D) \times t/movingAvg(T)$$

The variables in the equation are defined below:

d	Next difficulty
D	Past difficulties
t	Target block time
T	Past block times

5. Motion Network

The Motion network, like many other blockchain networks, is a peer-to-peer (P2P) network in which full nodes, partial nodes and miners work together to ensure the security and stability of the block chain.

Full nodes store the complete blockchain ledger locally, which could become very resource intensive, since full nodes have to store all the transactions that ever happened.

Partial nodes don’t store the complete ledger, they use a simplified payment verification (SPV) mode which only requires them to maintain a part of the blockchain. Partial nodes connect to full node clients and use bloom filters to ensure that they only download transactions which are necessary for their operation[5].

5.1 Masternode Network

The masternode network is a network of full nodes. These nodes maintain a copy of the entire blockchain and all past transactions. These nodes allow peers on the network to receive updates. Masternodes provide a level of service to the network that is essential.

To operate a Motion masternode, an amount of 1,000 MTN is required. This amount is never forfeit. Instead, it can be seen as a bond to prevent a Sybil attack[6], and masternode operators earn interest for providing this service. To ensure a stable network, masternodes must not go offline for more than one hour. If the masternode goes offline for more than one hour, the masternode will lose its current place in the block reward queue, and the operator must broadcast a new signed start message.

5.2 Mining Network

Miners have the option to download the entire chain of transactions locally and behave as a full node, or download a part of the blockchain to become a partial node.

The Motion team understands the importance of having a diverse network of miners, and as such, will strive to accommodate their needs and make Motion a profitable and convenient option.

As such, the Motion developers have developed a one-click miner for mining MTN. This software will make mining MTN more agile and straight forward. Motion also has an official mining pool located below:

https://mine.motionproject.org/

Miners are encouraged to use both the official MTN one-click miner and mining pool. The Motion team will aim to quickly address any feedback, and will be constantly updating the mining software with new features.

5.3 Block Rewards

A total of 1,051,200 MTN, approximately 4.8% of total supply, was pre-mined by the developers of Motion. This amount will be used for several purposes, including listing on exchanges, listing on mining pools, paying for marketing campaigns and establishing a healthy number of initial masternodes to help secure the network.

The block time of the Motion network is set to approximately two minutes. The blockchain has been set to issue 1 MTN block reward up to block 500. This is done to prevent the first miners and masternode operators from accumulating an unequitable amount of MTN, defeating the purpose of decentralization. With a two minute block time, this insta-mine protection will last approximately 17 hours after the genesis block.

After block 500, Motion block reward will be set at 20 MTN, and will decrease by 50% every 2 years to combat inflation. Once the block reward reaches 1.25 MTN, no more halving will take place, and the reward will not change until the maximum supply of 22,075,700 MTN (including the pre-mine) is reached. The block rewards and supply are as follows:

Reward	Block Height	Circulating Supply	Duration
1	0	500	17 hours
20	500	10,512,500	2 years
10	526,100	15,768,500	2 years
5	1,051,700	18,396,500	2 years
2.5	1,577,300	19,710,500	2 years
1.25	2,102,900	21,024,500	4 years
0	3,154,100	21,024,500	∞

A pre-mine of 1,051,200 MTN is not included in the above table.

The block rewards will be distributed between masternodes and miners at a 60/40 ratio. This means that masternodes will receive 60% of the block reward as compared to miners, who will earn 40%. Masternodes are paid in a round-robin fashion. The hash of each proof-of-work block is used to create the pseudorandom list of masternodes in the order in which they will get paid. This is to avoid any possibility of manipulation. Only one masternode is paid per block creation. The masternode reward is limited by the number of active masternodes at the time the list is generated. Calculating the daily income of an operator with n masternodes can be done as shown below:

$$S = \frac{n}{t} \times r \times b \times p$$

The variables in the equation are defined below:

S	Total daily income of operator
n	Number of masternodes owned
t	Total number of active masternodes
r	Current block reward
b	Daily average blocks created
p	Percent of masternode payment

For example:

You are a user and an investor in Motion and you got 2,000 MTN. If you locked the coins, you owned 2 full masternodes. If this takes place by block 1,000 with 100 active masternodes, S can now be calculated using theses variables.

n	2
t	100
r	20
b	720
p	60%

And this operator's daily income would be:

$$S = \frac{2}{100} \times 20 \times 720 \times 60\% \\ = 172.8\,MTN/day$$

The developers plan to create a one-click masternode setup tool to make the setup easier and more straight forward.

6. Advanced Motion Transactions

In order to build a blockchain that can be adopted by the public, two main features are essential; transaction speed and privacy. Bitcoin's slow block time can lead to extremely long transaction times. Additionally, Bitcoin's only method of transaction privacy is based on obscurity. In other words, once multiple wallets' users have been identified, any transaction between the users are no longer private. Motion implements two features to ensure instant transactions and privacy.

6.1 InstantSend Feature

In order for Motion to be widely used, transactions need to be as fast as swiping a credit card. Motion uses a method called InstantSend. Every time a miner finds a block, the miner will get assigned a "winning" hash. This hash will then be used to select 10 pseudorandom masternodes, and delegate them to be the InstantSend Authority. These masternodes will then monitor the network for InstantSend transactions, and upon finding any, they will lock them up in the network as pending transactions. The InstantSend Authority masternodes will then broadcast this message to the other masternodes in the network. Any additional transactions broadcasted that use the same inputs but attempt to send to a different address are rejected, preventing double spending. Within one second after the transaction has been made, both the sender and receiver will observe the transaction with five confirmations.

6.2 PrivateSend Feature

One of the most essential aspects of cryptocurrency is privacy. A user or entity should be able to make transactions and be sure that they are untraceable and private. To ensure privacy, Motion will adopt a feature called PrivateSend. PrivateSend is a novel, decentralized coin-mixing service that creates an on-demand system of removing the history from coins on the network. When multiple parties submit their MTN for PrivateSend, they will be queued by the masternode network. Once three users are in the queue, the process begins. PrivateSend begins by breaking your transaction inputs down into standard denominations (0.01 MTN, 0.1 MTN, 1 MTN, and 10 MTN). Your wallet will send a request to a masternode, which will then mix up your inputs with the two other users, and instruct all three wallets to pay the now-transformed input back to themselves. The process is repeated a number of times with each denomination. Each time this process is repeated, it's called a round, and the funds become exponentially harder to trace.

The probability of a single transaction being traceable after PrivateSend has been applied is highly unlikely, and can be calculated as shown below:

$$100\left(\frac{a}{m}\right)^{r}$$

The variables in the equation are defined below:

a	Number of attacker masternodes
m	Total number of active masternodes
r	Number of rounds

7. Motion Wallet Platforms

A key component in creating an innovative blockchain is the Motion wallet. Building on existing wallet designs, the Motion wallet streamlines the user experience further by providing a user friendly interface that implements the complex features of Motion, all the while maintaining accessibility and adaptability.

A desktop wallet has been developed for Windows, macOS, and Linux/Unix environments.

To make Motion more applicable in the real world and facilitate integration, Motion is working on developing wallets for all the major mobile platforms. This will make MTN much more accessible to the daily consumer, allowing functionalities like InstantSend to occur by simply scanning a QR code.

8. Conclusion

Motion's blockchain aims to revolutionize the business world by integrating and improving the technology behind smart contracts. This will enable companies to create ecosystems that not only support their business processes, but help them become more efficient and secure. The Motion blockchain introduces transparency and immutability to businesses and their customers. This encourages accountability among parties. However, as with any major technology adoption, the Motion blockchain and smart contracts still require a lot of work to reach its' full potential, and the Motion team is focused on tackling all the obstacles that will be faced along the way. Motion's goals can be summarized with three words; Moving Ideas Forward.

References

[1] Rosic, Ameer. "Smart Contracts: The Blockchain Technology That Will Replace Lawyers." *Blockgeeks*, blockgeeks.com/

[2] Satoshi Nakamoto, Bitcoin: A Peer-toPeer Electronic Cash System, 2008

[3] Black, Tron, and Joel Weight. "X16R: ASIC Resistant by Design." 2018, www.ravencoin.org/wp-content/uploads/2018/01/X16R-Whitepaper-3.pdf.

[4] Zawy12. "LWMA Difficulty Algorithm." *Github*, github.com/zawy12/difficulty-algorithms/issues/3.

[5] "What Are the Types of Nodes or Peers in a Blockchain." *BlockchainSemantics*, www.blockchainsemantics.com/blog/nodes-bitcoin-blockchain/.

[6] John (JD) Douceur, The Sybil Attack, 2002