Waukeen Whitepaper

A Trade&Wealth-Focused Cryptocurrency

WAUKEEN

Abstract: WAUKEEN is a world-oriented cryptocurrency released on the 10th anniversary of the Bitcoin network. It is a complete bitcoin system based on Bitcoin developed by Nakamoto. It has improved and added a Waukeen timeline algorithm controller (WauTAC). And a two-tier reward network—an Cryptocurrency that is also known as a masternode network and many other new features. It also includes asymmetric hybrid billing technology (Wausend) for improved privacy protection and interchangeability, and instant payment functionality (InstantX) for real-time transaction confirmation without relying on central authority.

H*istorical: Waukeen represents trade and wealth. She is a young and diligent goddess, full of vitality and vitality.Her love for wealth is not only the value of loving itself, but the purpose of loving it.She loves the hustle and bustle of the market and loves bargaining.She is in charge of all transactions on the counter or under the counter – including legitimate transactions and black market transactions.Apparently she is interested in reforms.*

D*ogma: Mercantile trade is the best road to enrichment. Increasing the general prosperity buys ever greater civilization and happiness for intelligent folk worldwide, bringing people closer to the golden age that lies ahead. Destroy no trade goods, raise no restrictions to trade, and propagate no malicious rumors that could harm someone's commerce. Challenge and refute unproven rumors that could negatively impact trade when heard. Give money freely to beggars and businesses, for the more coin everyone has, the greater the urge to spend and trade rather than hoard. To worship Waukeen is to know wealth. To guard your funds is to venerate her, and to share them well seeds your future success. Call on her in trade, and she will guide you in wise commerce.*

B*elief: "The bold find wealth, the careful keep it, and the timid yield it up."*

1. Introduction

In 2009, Nakamoto public Bitcoin The concept, since then, Bitcoin has quickly spread in mainstream applications and commercial use, becoming the first Attract a large number of users The digital currency is a milestone in the history of digital currency.However, from the perspective of completing the transaction, we can find an important issue, that is, the Bitcoin block confirms the transaction for too long, and the traditional payment company has found that the buyer and the seller realize zero confirmation of the bitcoin transaction. Solution, but this solution usually involves completing a transaction with a trusted third party outside of the agreement.

Bitcoin provides a pseudonym transaction that enables a one-to-one transaction between the sender and the recipient, and can always record transactions that have occurred across the network.Bitcoin only provides low-level privacy protection, which is well known in the academic world. Despite this deficiency, many people still believe in the transfer history of blockchain records.

Based on Nakamoto's results, WAUKEEN is the first Cryptocurrency to use the Waukeen Timeline Algorithmic Controller (WauTAC). We have made a series of improvements based on the concept of Bitcoin, which has resulted in a decentralized, privacy-protected, effective anti-ASIC and highly circulated Cryptocurrency that supports tamper-proof real-time transactions. It realizes the original intention of the Bitcoin decentralization reward mechanism, and has a point-to-point secondary network that can provide a service reward mechanism for the WAUKEEN network.

2. Masternode network

The full node is the server running on the p2p network, allowing the small nodes to use them to accept dynamic changes from the entire network.These full nodes require significant traffic and other resources that consume a lot of cost, and thus it will be observed for some time that the number of these nodes on the Bitcoin network is steadily declining. trend To make block broadcast time extra 40 seconds increase. In order to solve this problem, many proposals have been made, such as the introduction of Microsoft research. New rewards program And Bitnodes Incentive plan.

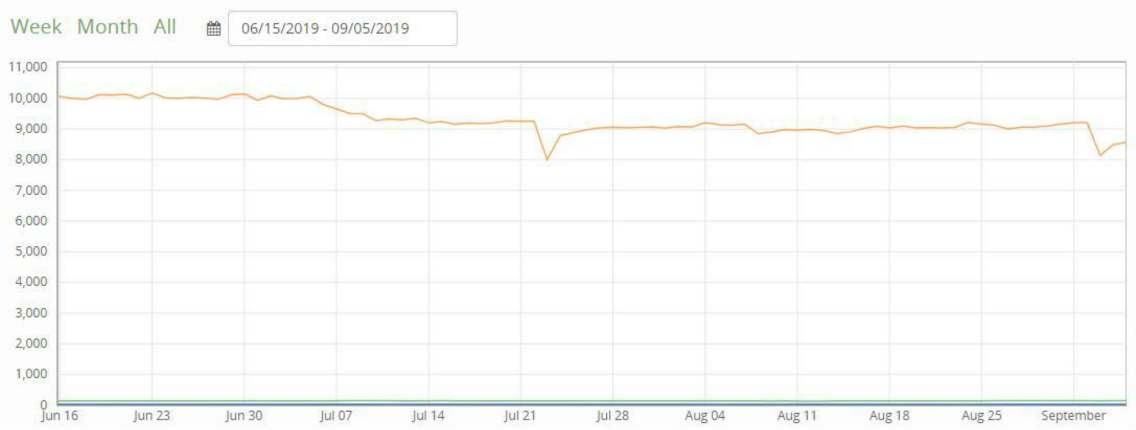


Figure 1: Bitcoin Full nodes in September 2019

These nodes are important to the health of the network, allowing clients to synchronize and quickly broadcast information across the network.We propose to add a secondary network called the waukeen masternode network.These nodes will be highly available and will receive a masternode service reward after providing the network with a service that meets certain requirements.

2.1. Master Reward Program - Costs and Payments

The main reason for the sharp decline in the entire node of the Bitcoin network is the lack of rewards for running nodes.Over time, the number of users accessing the entire network will be more, the demand for bandwidth will be higher, and the capital requirements for the node operators will be more, resulting in an increase in the cost of running the entire node.Considering the rising cost, node operators must reduce their running costs or run a light client, but this is completely detrimental to network health.

Just like the Bitcoin network, the masternode is a full node, but the difference is that the masternode must provide certain services to the entire network and require a certain amount of deposit to join.The deposit will not be lost and is safe when the masternode is running.This allows investors to provide a certain amount of investment income while reducing the volatility of prices while providing services to the entire network.

Running a masternode requires storing 100,000 waukeen, which is equivalent to a block reward in the initial phase.When the masternode is in effect, it can serve clients on the entire network and receive rewards in the form of interest.This allows users to invest in this service, but at the same time get a certain return.The revenue earned by the masternode is from the same mine pool, and about 40% of the block rewards are included in the plan.

Considering that the reward rate of the masternode reward program is a fixed percentage, and the fact that the masternode network node is fluctuating, it is expected that the masternode reward will change according to the total number of masternodes currently in effect.The following calculation formula can be used to calculate the profit of running the main node for a whole day:

(n/t) * r * b * a

n: number of masternodes controlled by the operator

t: total number of masternodes

r: current block reward (current average reward is 10,000 WAUKEEN)

b: the average number of blocks per day. The current WAUKEEN network is usually 1440 blocks per day.

a: average reward for the masternode (average 40% of each block reward)

The profit formula for running the masternode: ((n/t) * r * b * a * 365) / 1000000 (the variables in the equation are the same as above)

Running the masternode requires cost, which creates hard and soft limits on the network for the active node.The soft limit is caused by the cost of configuring the node and the retention of the platform, because waukeen is a currency that focuses on trade and wealth, not just for investment.

2.2. Determine order

A pseudo-random ordering of the masternode is created using a specific determination algorithm.Using a hash algorithm for the workload proof mechanism designed for each block, the mining network can provide security that supports this ordering.

Pseudocode, for selecting a masternode:

```
For(mastenode in masternodes){
    current_score = masternode.CalculateScore();
    if(current_score > best_score){
         best_score = current_score;
         winning_node = masternode;
    }
}
CMasterNode::CalculateScore(){
   pow_hash = GetProofOfWorkHash(nBlockHeight); // get the hash of this block
   pow_hash_hash = Hash(pow_hash); //hash the POW hash to increase the entropy
   difference = abs(pow_hash_hash - masternode_vin);
   return difference;
}
```

The sample code can be further extended to be the masternode, and the calculations for the "second", "third", and "fourth" masternodes are analogous.

2.3. Untrusted Quorum

The current waukeen network has approximately 2,400 activemasternode, and need 1000,000 waukeen guarantee to become a masternode.We created a system in which no one can control the entire masternode network.For example, if someone wants to control 50% of the masternode network, they will have to buy 2.4 billion waukeen from the open market.This will greatly increase the price of the currency, so it is impossible to get so many waukeen.

Under the premise of having a masternode network and guarantee conditions, we use the secondary network in a non-trusted manner for highly sensitive tasks, and no one can control the evolution of the network.Select n pseudo-random masternodes from the pool to perform the same tasks, these nodes can act as referees, and the process does not require the participation of the entire network.

For example, a non-trusted Quorum discovery InstantX, InstantX willuse

Quorum Confirm transaction and lock input.

Another example is that the untrusted Quorum can leverage the masternode network as a decentralized predictor of the financial market, which makes it possible to implement decentralized contracts.For example, if Apple's share price exceeds US$300 on December 31, 2019, it will be submitted to Convention A, otherwise it will be submitted to Convention B.

2.4. Role and service volume certification mechanism

The masternode can provide any additional services to the network.As pointed out in the concept, our first successful applications are Wausend (Asymmetric Hybrid Encryption) and InstantX (Instant Payment).Using what we call a "proof of service" mechanism, these nodes can be required to be online, even if they are at the correct block height.

A malicious person can also run the masternode, but will not provide any substantial service to the network.In order to reduce the probability that these people use the system to make things good for their own nodes, the remaining networks must be pinged to ensure they remain active.This work is done by selecting 2 Quorums in each block through the masternode network.Quorum A checks the services of each block of Quorum B.Quorum A is the closest node to the current block hash, and Quorum B is the node farthest from the hash of the block.

masternode a (1) checks the masternode b (2300)

masternode a (2) checks the masternode b (2299)

Masternode a (3) checks the masternode b (2298)

Checking the network is to verify that the node is in effect, which is done by the masternode itself.1% of the entire network block will be checked.This allows the entire network to be inspected approximately six times a day.In order to keep this system untrusted, we use the Quorum system to randomly select nodes, but we also need at least six checks to troubleshoot a malicious node.

In order to achieve the purpose of deceiving the system, the attacker needs to be selected six times in one round.Otherwise, the purpose of deception is discovered by the system, so that it will not succeed, and so is the other nodes.

Attacker Controlled Masternodes / Total Masternodes	Required Picked Times In A Row	Probability of success $(n/t)^r$	WAUKEEN Required (Symbol: WKN)
1/2300	6	0.0006755%	100,000 WKN
10/2300	6	0.006755%	1,000,000 WKN
100/2300	6	0.06755%	10,000,000 WKN
500/2300	6	0.01055%	50,000,000 WKN
1000/2300	6	0.6755%	100,000,000 WKN

Table 1. The probability of tricking the system representing one individual masternode as failing proof-of-service

Where:
n is the total number of nodes controlled by the attacker
t is the total number of masternodes in the network
r is the depth of the chain

The selection of masternodes is pseudo random based on the Quorum system

2.5. masternode protocol

The masternode broadcasts on the entire network using a series of extended protocols, including the masternode announcement mechanism and the masternode message ping mechanism.These two types of mechanisms are used to confirm that the entire network nodes are in effect. In addition to them, there are also Wausend and InstantX that perform the service volume certification mechanism.

Send 100,000 waukeen to a specific address in the wallet, the activation code naturally generates the masternode that can broadcast on the whole network, and then the secondary private key is generated, which is used to sign all other information, and when running stand-alone mode It can also be used to completely lock the wallet.

Using a secondary private key on two separate machines makes cold mode possible.The primary "hot" client signs the input of 100,000 waukeen, which

involves signing the information using the secondary private key.After that, the "cold" client can discover the information containing the secondary private key and stimulate the masternode.
live.This invalidates the "hot" client (the client is shut down) so that the attacker's access to the active masternode is also unlikely to steal 100,000 waukeen.

When the masternode starts running, it sends the "masternode broadcast" information to the entire network, including:

Information: (100,000 waukeen input, accessible ip address, signature, signature time, contains 100,000 waukeen's public key, secondary public key, public key for donation, percentage of donation)

After every 15 minutes, a ping message will be sent out to prove that the node is in effect.Information:

(100,000 WAUKEEN input, signed with secondary private key, signature time)

Over time, the network removes the failed node, leaving the node no longer being used by the client or reused for payment.Nodes can also ping the network constantly, but if their ports are not open, they will eventually be marked as invalid and will no longer be used for payment.

2.6. Broadcast of the masternode list

New clients entering the waukeen network must discover the active masternodes of the entire network so that their services can be used.Once they join the mesh network, their nodes receive an instruction to request a list of masternodes.The purpose of setting up the cache is to let the client record the masternode and its current state, so when the client restarts, they simply load the file without re-requesting the full list of the masternode.

2.7. Use mining to make payments and mandatory

In order to ensure that each masternode gets the block rewards it deserves, the network must force each block to pay a reward to the correct masternode.If the miners are not willing, their block must be rejected by the network, otherwise cheating will occur.

We propose a strategy in which a masternode represents a Quorum, selects the winning masternodes and broadcasts their information.After the information is broadcast N times, the same target recipient is selected, so that the selected block after the consensus is reached must pay the reward to the masternode.

When mining on the net, the mine pool (the role of the pool is to integrate individual miners) uses the RPC API interface to obtain information about the generated blocks.In order to pay the reward to the masternode, a secondary recipient must be added to the GetBlockTemplate to extend the interface.After the mine pool, broadcast its successfully exploited blocks to keep themselves in sync with the masternode.

3. Asymmetric hybrid encryption payment

We believe that in order to improve the privacy of users on the client side, it is important to implement a standard non-trust system.Clients such as Electrum, Android and iPhone will also embed the same asymmetric hybrid encryption layer directly and make good use of protocol extensibility.This gives users the same experience when sending money using a solid, robust system with asymmetric hybrid encryption.

Wausend is an improved and expanded version of CoinJoin, a software that provides asymmetric hybrid encryption.In addition to the core concept of CoinJoin, we have also implemented a series of improvements, such as decentralization, privacy protection using strong link encryption, the same denomination and passive advanced asymmetric billing technology.

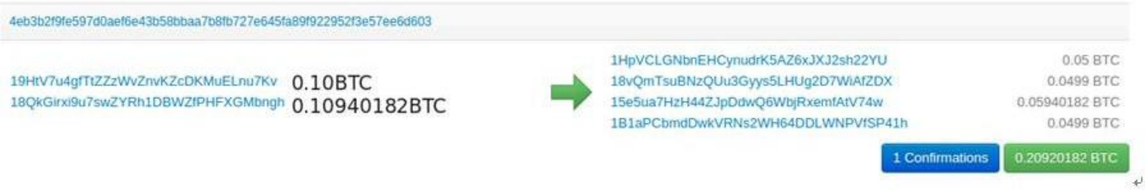
The biggest challenge in improving the interchangeability of privacy and Cryptocurrency is the inability to encrypt the entire blockchain.In a bitcoin-based Cryptocurrency system, you can see which outputs are not sent and which are sent, usually called utxo, and the full name is unused transaction output.This allows each user to act as an honest trade guarantor in the public ledger.Bitcoin's agreement is designed without relying on the participation of third parties. It is crucial to read the user information at any time through the public blockchain without the participation of third parties.Our goal is to improve confidentiality and interchangeability without losing these elements, and we firmly believe that this is the key to creating a successful digital currency.

Using a decentralized asymmetric hybrid billing service within the digital currency range, we can make the currency itself fully interchangeable.Interchangeability is the property of money, and the units that determine the currency must be equal.When you receive funds in the form of currency, the funds should not retain the previous user's usage records, or the user can easily clear the previous usage history, so that all currencies are equal.At the same time, any user guarantees that every transaction in the public ledger is honest without affecting the privacy of others.
In order to improve interchangeability and maintain the integrity of the public blockchain, we propose to use an advanced non-trust system to centralize the

hybrid billing technology. In order to maintain the interchangeability of the currency, the service is directly integrated into the monetary system. It is easy and safe to use for every user.

3.1. Coinjoin tracks the flow of funds through accounts

A simple strategy is to integrate Coinjoin on top of existing Bitcoin, which is simply to merge transactions together.The user's identity is exposed by tracking the flow of user funds in the joint transaction.



4eb3b2f9fe597d0aef6e43b58bbaa7b8fb727e645fa89f922952f3e57ee6d603

19HtV7u4gfTtZZzWvZnvKZcDKMuELnu7Kv 0.10BTC
18QkGirxi9u7swZYRh1DBWZfPHFXGMbngh 0.10940182BTC

1HpVCLGNbnEHCynudrK5AZ6xJXJ2sh22YU 0.05 BTC
18vQmTsuBNzQUu3Gyys5LHUg2D7WiAfZDX 0.0499 BTC
15e5ua7HzH44ZJpDdwQ6WbjRxemfAtV74w 0.05940182 BTC
1B1aPCbmdDwkVRNs2WH64DDLWNPVfSP41h 0.0499 BTC

Figure 2: For example, integrating 2 user transactions into Coinjoin transactions

In this transaction, 0.05 bitcoin is sent using the hybrid technology. In order to track the source of the funds, it is only necessary to add the amount on the right side to match the amount on the left.

Regrouping transactions

0.05+0.0499+0.0001(fee) = 0.10BTC.

0.0499+0.05940182+0.0001(fee) = 0.10940182BTC.

As more users join the process of mixing coins, the difficulty of obtaining results will increase exponentially.However, at some point in the future, the results can still be traced and privacy leaks.

3.2. Direct link and relay link

In other implementations of Coinjoin, it is possible for the user to anonymize the funds and finally send the transaction to a platform or individual that knows the identity of the sender.But this breaks the anonymity and allows others to track user transactions forward. We call this type of attack a "relay link."

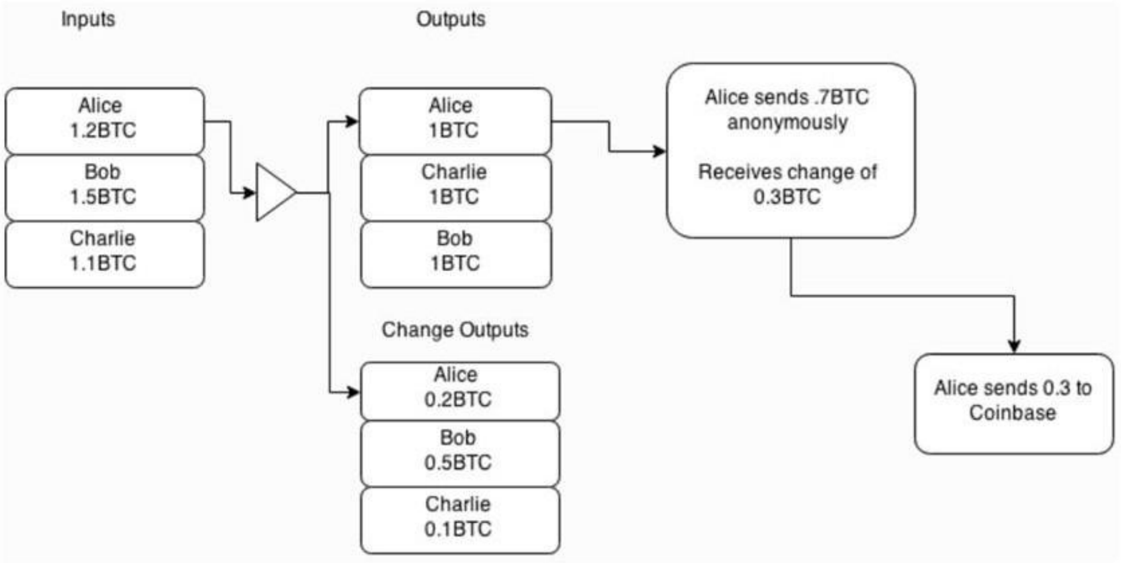


Figure 3: Relay Conversion Link

In this example, Alice sends 1.2BTC anonymously, which outputs 1BTC and 0.2BTC respectively, and then outputs 0.7BTC from the output of 1BTC, leaving 0.3BTC. This 0.3BTC output is sent to the identifiable object, but essentially Alice has sent the 0.7BTC successfully anonymously.

In order to determine the identity of the sender of an anonymous transaction, start with the "exchange transaction" link and trace back through the blockchain until you find "Alice sends 0.7 BTC anonymously".Once you find it, you will find that your user has recently purchased something anonymously to see through this anonymous transaction.We call this type of attack an "intermediary conversion link."

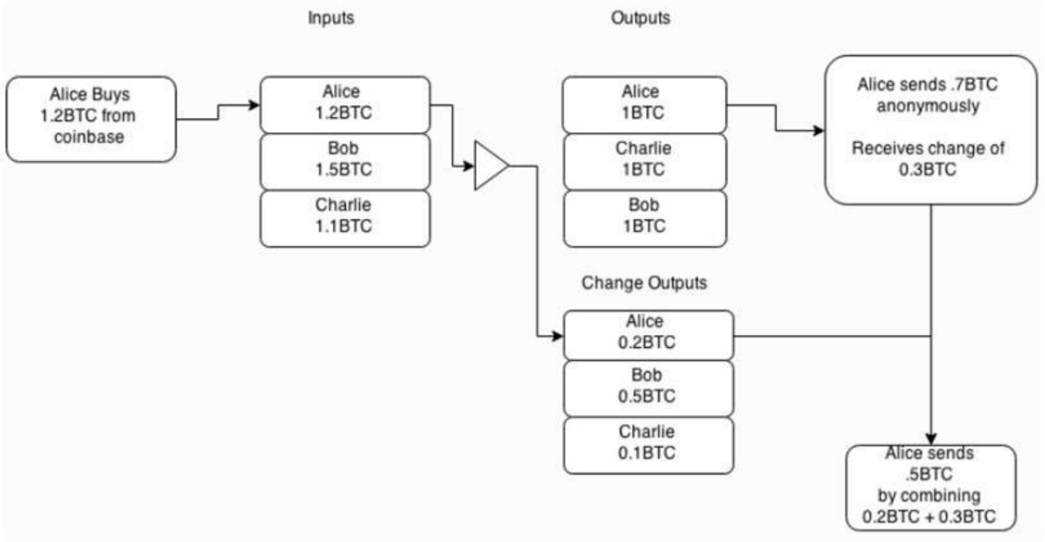

Inputs
Outputs
Alice Buys 1.2BTC from coinbase
Alice 1.2BTC
Bob 1.5BTC
Charlie 1.1BTC
Alice 1BTC
Charlie 1BTC
Bob 1BTC
Alice sends .7BTC anonymously
Receives change of 0.3BTC
Change Outputs
Alice 0.2BTC
Bob 0.5BTC
Charlie 0.1BTC
Alice sends .5BTC by combining 0.2BTC + 0.3BTC

Figure 4: Mediation conversion link

In the second example, Alice spent 1.2 BTC at the coinbase, then anonymized the amount and output it at 1BTC.Then, she spends 1 BTC again, and the remaining 0.3 BTC is combined with the previous 0.2 BTC, which is composed of 0.5 BTC for external output.

Combine anonymous transactions with CoinJoin transactions to organize the entire transaction history before and after, so that you can see through this anonymous feature.

3.3. Enhanced privacy and dos protection

Multi-party transactions can be combined into one transaction, and Wausend makes good use of this. It combines multiple funds and sends them together so that once they are integrated, they cannot be split again.Considering that the Wausend transaction is specifically set for the user to pay, the system is highly secure and the user's currency is very secure.Currently, the asymmetric hybrid billing technology using Wausend requires at least 3 parties to participate.

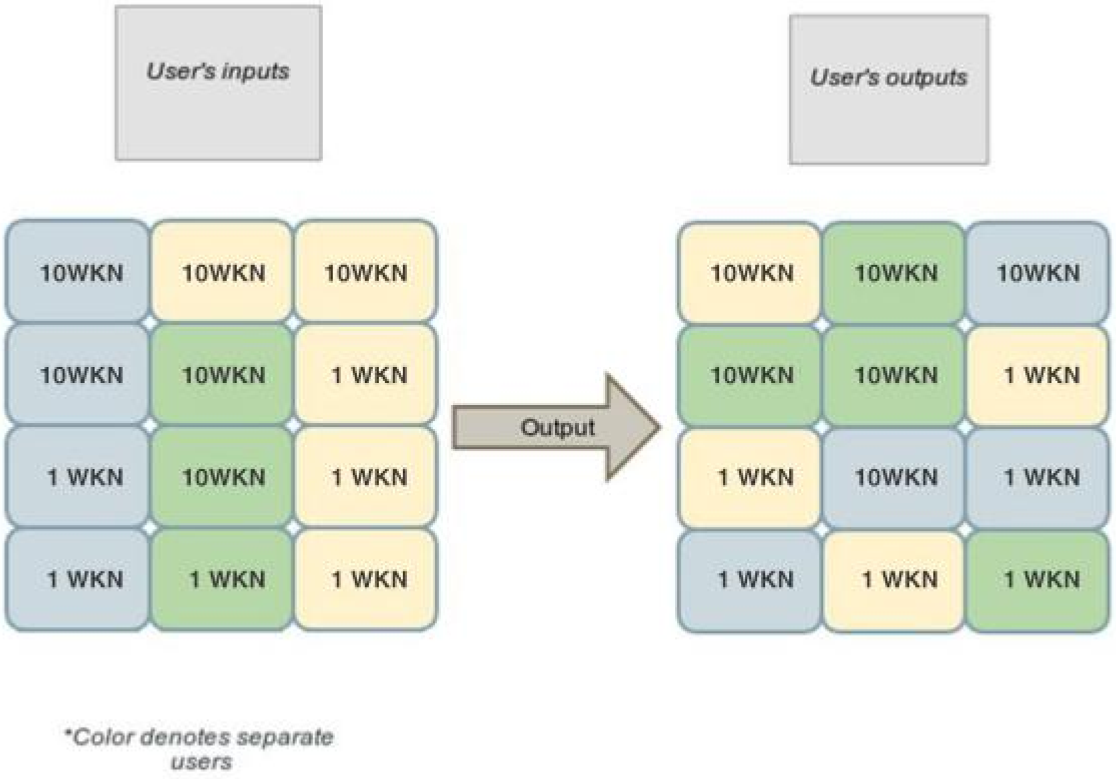


Figure 5: The three users' funds are combined into one common transaction, and the user will export the funds in a new, disrupted form.

In order to enhance the privacy of the system as a whole, we use the same denominations of 1wkn, 1000wkn, 100,000wkn and 10,000,000wkn.In each round of the coin process, all users should enter and export funds in the same face value.In addition to using the same denomination, transaction fees are removed and all transactions are broken down into discrete, independent, unrelated small transactions.

The next step is to deal with possible dos attacks. We propose that all users submit the transaction to the mine in the form of a deposit when they join. The transaction is finally output to the user, and at the same time, the miner can pay a high salary.That is to say, when the user raises the request to the mixing pool, the deposit is provided at the beginning of the transaction.If the user does not cooperate at some point, such as refusing to sign, the deposit transaction will automatically be broadcast on the entire network. The cost of continuing attacks on the mixed billing network is extremely high.

3.4. Passive funds and blockchain privacy protection

Wausend's billing mix per round is limited to 100,000 WAUKEEN, and multiple rounds of mixed billing can complete a mix of a significant amount of encrypted funds.To make user experience easy and attack difficult, Wausend runs in a passive mode.At the same time, the time interval is set, and the user's client needs to connect to other clients through the masternode.Once in the masternode, the user requests that the amount of face value that requires privacy protection will be queued for broadcast throughout the network, but no information will expose the user's identity.

Each round of Wausend process can be seen as an independent event that enhances the privacy of user funds. However, only 3 participants are restricted per round, so viewers have one-third chance to track transactions. In order to improve the quality of privacy protection, links will be used. In the method, funds are sequentially sent through multiple masternodes.

Block chain depth	Possible number of users $(n)^r$
2	9
4	81
8	6561

Table 2. Number of users that may be involved in an n round of mixed bills

3.5. Safety considerations

Since the transactions are merged together, the masternode is likely to "snoop" when the user funds flow.Since each masternode is required to hold 100,000 waukeen and the user chooses a random masternode to deploy their funds, the impact of "snooping" is small.The probability of tracking a transaction through a blockchain is calculated as shown below.

Attacker Controlled Masternodes / Total Masternodes	Block chain depth	Probability of success (n/t)r	WAUKEEN Required (Symbol: WKN)
10/1010	2	0.955%	1,000,000 WKN
10/1010	4	0.0941%	1,000,000 WKN
10/1010	8	0.0093%	1,000,000 WKN
100/1100	2	8.15%	10,000,000 WKN
100/1100	4	0.651%	10,000,000 WKN
100/1100	8	0.044%	10,000,000 WKN
1000/2000	2	25%	100,000,000 WKN
1000/2000	4	6.25%	100,000,000 WKN
1000/2000	8	0.39%	100,000,000 WKN
2000/3000	2	44.4%	200,000,000 WKN
2000/3000	4	19.75%	200,000,000 WKN
2000/3000	8	3.90%	200,000,000 WKN

Table 3. Probability of tracking Wausend transactions across the network when attackers control N nodes

n: The attacker controls the total number of nodes

t: Total number of masternodes in the entire network

r: block chain depth

The choice of the masternode is random

Given the limited supply of waukeen and the low liquidity in the market, it is impossible to control so many masternodes in an attack.

Extending the system by masking transactions that occur on the masternode also greatly increases the security of the system.

3.6. Masking the masternode with a relay system

In Section 3.4, we describe the probability of tracking a single transaction using Wausend's multi-round hybrid billing technology.This can be further enhanced by masking the masternode so that they cannot see the user input/output directions.To do this, we propose a simple relay system that allows users to protect their identity.

Instead of letting users submit input and output transactions directly to the pool, they are allowed to randomly select the masternode from the entire network and then request that its input/output/signature relay be transmitted to the target masternode.This means that the masternode will receive n input/output and n group signatures.Each round of the coin only serves one of the users, but the masternode cannot know which user it is.

4. Instant trading with InstantX

Using the masternode's Quorum, users are able to send and receive instant irreversible transactions.Once Quorum is formed, the transaction's input is locked to the corresponding specific transaction, and the current network-wide transaction lockout time is approximately 4 seconds.If a consensus is reached on the masternode network, all conflicting transactions and blocks will be rejected forever unless they match the transaction-matched ID that was locked at the time.

This will allow merchants to replace traditional pos machines with mobile devices in real-world commerce, allowing users to quickly conduct face-to-face non-commercial transactions as they would with traditional banknotes.This process was completed without the intervention of a central authority.A comprehensive review of this feature can be found at InstantX white paper Found in.

5. Algorithm and mining

5.1.WAUKEEN Timeline Algorithm Controller

The WAUKEEN Timeline Algorithm Controller (WauTAC), unlike any previous cryptocurrency, no longer uses a specific algorithm. The WauTAC controller will schedule the algorithm based on the block time as shown below.

Timeline	Scheduling Algorithm
00:00-07:59	Sha256+X11
08:00-15:59	Scrypt+Lyra2reV2
16:00-23:59	X13+X17

Table 4. Starting from 00:00 daily, the WauTAC algorithm is scheduled in three stages. The first scheduling algorithm is implemented by the bitcoin sha256 algorithm and the Dash X11 algorithm hybrid algorithm.

Using the WauTAC controller scheduling algorithm, it is possible to effectively eliminate the emergence of ASICs specifically designed for digital currency mining, because it is more expensive than CPU and GPU to design ASIC chips for WauTAC.

In the life cycle of Bitcoin, its fans used cpu at the beginning of mining, and soon after using gpu software, gpu quickly replaced cpu.A few years later, the cycle of gpu ended, asic was developed by ASIC, which quickly replaced gpu.

Considering the manufacturing costs and machine manufacturing difficulties of ASIC miners designed specifically for WauTAC, we anticipate that the era of mining monopoly by ASIC will become a history, which gives fans a fair chance of mining.We are convinced that this plays an extremely important role in the distribution of the balance and the growth of the digital currency.

Another benefit of the waukeen timeline algorithm controller is that the high-end cpu has an average return that is close to that of the peer gpu.The power consumed by the gpu has dropped by 50-80%, which is much less than the power of a fixed algorithm for most encrypted digital currencies.

5.2. Mining supply

Waukeen uses another method that reduces inflation caused by mining, which is a 10% reduction in annual supply, which is different from the halving of other digital currencies.In addition, the supply of each block is directly related to the number of miners across the network, and the participation of more miners means less mining incentives.Waukeen's plan for the acquisition will continue in this century, slowly until the end of the century, and finally Mining will stop in around 2100.

6. Conclusion

This white paper describes various concepts designed to improve the Bitcoin protocol, which means better privacy, interchangeability, more master network, better ASIC resistance, and full for the average user. Faster information broadcast on the web.It's all done by using a two-tier stimulus model instead of borrowing other digital currencies like Bitcoin's existing single-tier model.Using this alternative network design makes it possible to add more types of services, such as decentralized hybrid billing techniques, instant transactions, and decentralized predictions using the masternode quorum.