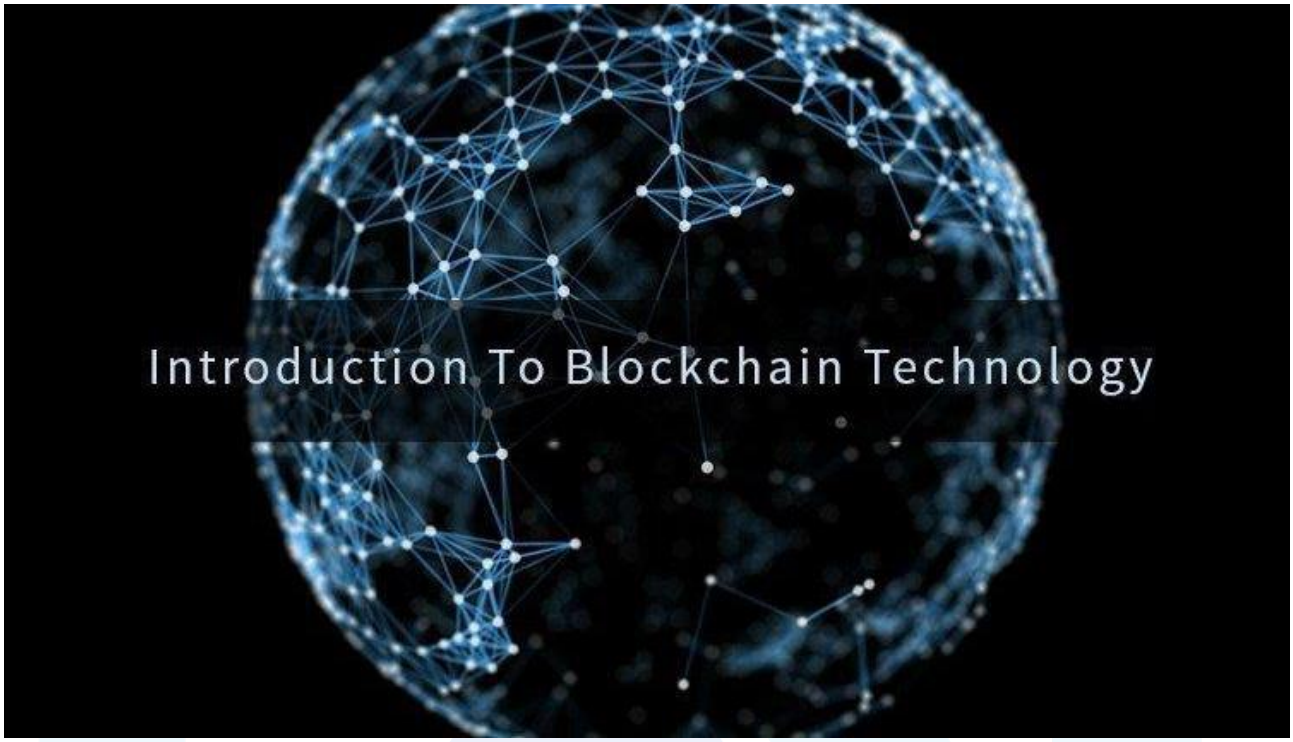
BAW

WHITEPAPER

TABLE OF CONTENT

INTRODUCTION



The world of cryptocurrencies made a landfall on earth in 2007 with Satoshi Nakamoto's treatise on Bitcoin. After an intriguing early-run by Bitcoin, other cryptocurrencies joined the party in no time. However, a greater majority of the ensuing altcoins followed suit with the POW algorithm, which had a train-load of inefficiencies and challenges.

With the immense headways made in digital technology, it was only a matter of time before classical and quantum computing provided some food of thought. Quantum computing has become a direct threat to blockchain as its immense capacity can be used to exploit loopholes in existing blockchains.

One of the recognized efficiency points for cryptos is to avoid dependence on centralized exchanges. Since cryptocurrencies now serve as transaction enablers globally, more safeguards have to be in place. This opening gives a leeway to innovate dependable cryptocurrencies that can serve as medium of exchange without loopholes.

THE BAW SOLUTION

The introduction of cryptocurrencies to humanity began with Bitcoin, and at the time, it was a novel idea. After more than a decade of use and interaction, it is now clear that the single algorithm block mining that defines Bitcoin and most altcoins are susceptible to manipulation by superior technology.

The innovation of Application Specific Integrated Circuits (ASICs), which is a specialized hardware that easily craft the mining hash on single algorithm blockchains have altered the operational landscape. GPU mining and CPU systems are now years behind in terms of efficiency.

In essence, as quantum computing grows, several blockchains will be at risk of hacking by high-efficiency computers. While the emergence of quantum computing has several positives to it, its threat to single algorithm blockchains cannot be overlooked.

The use of artificial intelligence has given social media drivers like Facebook a huge advantage in harvesting user-data. Quantum computing will make the blockchain accessible to big data corporations for clandestine takeovers and hacks. In real terms, the privacy of most blockchains as we know it will cease to exist. Governmental and pseudo-governmental agencies can hijack blockchains with similar algorithms.

It is also noteworthy that at present, scalability is still a problem with many blockchains. The subsisting problem of low TPS that beguiles existing platforms still makes it impossible for a widespread commercial adoption of the blockchain. If VISA has a TPS rate that tops the 24,000 mark, blockchains need to be more efficient to attract such corporations.

On the Bitcoin Blockchain, the biggest limitation is block size limit which means a block gets created in ten minutes. This is a disadvantage that makes the Bitcoin platform churn out a paltry 3 transactions in each second.

A look at what BAW can do and how it surpasses the expectations of stakeholders' in the crypto scene forms the fulcrum of this whitepaper. In terms of progress made since Bitcoin, you can only look in the direction of Ethereum, which gave rise to smart contracts, and a fairly better TPS rate.

For every blockchain, the capacity to process transactions efficiently cannot be overemphasized. To understand why this is the case, you need to appreciate that we have arrived in an era where machine-to-machine communication is at the forefront of modern interactive systems.

In a world where the Internet of Things and machine learning is becoming the pathway, high frequency will be required from all linked systems. An efficient blockchain will enable data exchange that spills into billions of transactions daily. To make this frontier a seamless experience requires that sufficient capacity be developed to drive the scale of transactions expected.

As governments the world over begin to recognize the utility of the blockchain, it becomes trite to opine that a greater efficiency is required from platforms that will drive the issuance of cryptocurrencies.

The possibility of governments issuing national cryptocurrencies is delved into in a later part of this WP.

How BAW can make the dream of national, or sub-national cryptocurrencies possible is also explained further in the other sections
What is important to understood at present is that the growth systems that are Blockchain and cryptocurrency-reliant calls for access to the blockchain in a convenient decentralized manner.
In looking at existing systems, it becomes clear that the routine that requires a holder of cryptocurrencies to go to an exchange before getting value for tokens is unsustainable.
The process as it currently obtains requires that a holder of Bitcoin needs to exchange same for Ether before accessing the Ethereum Blockchain. The same applies for a reverse transaction.

Since the algorithm for operations that drives many cryptocurrencies relies on the POW protocol, waste is unavoidable. Time, resources (energy and money), and environmental degradation are the offshoots of the POW protocol.

It is clear to all and sundry that the POW or the POS Casper model is far from sustainability. Better outcomes can be guaranteed with less resources and environmental protection.

The BAW driven ecosystem is a world of difference from what currently obtains in the blockchain universe.

BAW PLATFORM

Cryptocurrencies and Blockchain have come to stay. Since the current ones are fraught with problems, we designed an improved and innovative solution that leverages existing frameworks.

We are introducing the revolutionary framework that we have tagged as Blockchain 5.0- BAW. With BAW, we are providing a blockchain that is

suitable to drive a variety of applications using a decentralized operational methodology.

Transactions on the BAW Blockchain will be processed at a rate of millions of transactions per second. BAW's innovative features and technologies that solve all the issues are discussed below:

BAW is so innovative with a high throughput while offering smart contract technology. A developer can easily build dApps on the BAW platform. BAW intends to be very flexible, scalable, and with a proven usability in the real world.
BAW will be a universal operating system in the blockchain with vaunted operating system functionality.

BAW Solves Scalability Limitations

We introduce BAW as the dynamically Sharded Multigraph Blockchain that scales transactions to a height 100 TPS to 100 Million TPS from 100 TPS. In a comparison of BAW with existing blockchains, steps are taken to ensure that the obvious difference is seen.

PayPal is one of the most efficient payment systems and it processes 193 transactions per second. On VISA's platform, the upper limit is 24,000 TPS, and this is miles apart from the Bitcoin upper limit of 3TPS. Improvements made on Ethereum Blockchain so far only nets an upper limit of 30 TPS.

For a transaction to be concluded fast on a blockchain, all connected nodes must conclude and reach a consensus. BAW has noted this qualifying requirement for speed by adopting the decentralized Proof of Stake algorithm for transaction validation. This is the fastest route to the million TPS mark.

BAW is optimized to support decentralized apps by allowing such to be developed on its backbone with efficiency. The underlying database and accounts can then be shared across clusters of CPUs by BAW. This is how millions of TPS occurs as dApps are deployed.

On verification of transactions, the DPOS algorithm makes the job faster and efficient. This happens with elected witnesses instead of 51% of blocks as obtains with POW algorithms. In the process, fewer nodes are required to consent to consensus thereby leading to faster transaction times.

BAW efficiency will be optimized by using horizontal and vertical methods to arrive at scalability. Vertical is done by adding more resources like CPUs or memory to the system node. These linchpins increase the resources shared by apps and operating system. The horizontal scalability is done by hosting numerous chains that are parallel and running on the same app. This allows for scalability by ensuring that transaction processing and smart contracts can occur at the same time.

Apart from its off-chain scaling solution that BAW will use, a major way BAW will solve scalability limitation is Sharding.
Sharding involves the sharing of a node to a variety of groups, ensuring that the nodes do not get involved in validating the entire Blockchain's records before a new transaction is done.

Sharding uses the Economics model of division of labor, which shares out responsibilities so that multiple nodes can work on a variety of tarn actions instead of focusing on one at a time.

BAW's Quantum Resistance Encryption BAW makes use of a protocol that is quantum-computing proof. This allows for quantum-resistant transactions, meaning that even with the rise of a lot of quantum computers, our revised blockchain is safe.

Many of these cryptocurrencies that will be wrecked by quantum computing are built on ECDS, which can easily be attacked by the quantum Shor's Algorithm.
In order to protect our blockchain, we intend to use cryptographies of primitive nature, which cannot be hacked by both classical and quantum computers. We will make use of hashes, Lamport signatures, and other such cryptographies.

The Lamport signatures work in a seamless loop with hash functions. Hash functions are not susceptible to quantum algorithms like Shor's Algorithm. Many of these cryptocurrencies using ECDS have the susceptibility to quantum computing takeover.
Whenever a transaction is done in such a blockchain, the address then is susceptible to hacking because ECDS exposes its signature.

Once the signature gets hacked into, that is the end of the funds in that address. The funds are then easily pilfered.

Since our hashes cannot be compromised by Shor's Algorithm or any quantum computing algorithms, our Blockchain 5.0 and the addresses in it are safe from security threats.

BAW's Seamless Global Currencies

The outset of cryptocurrencies was attended by disdain and lack of attention. In the two years to 2018, the rise of Bitcoin became an eye-opener to the world. From an initial war of attrition to drown the use of cryptos, many countries are now considering how to get in on the wave.

In many countries, cashless transactions had gathered momentum with mobile and web-based payments in the ascendancy. The rise of cryptocurrencies has added momentum to the dream of cashless society in several climes. Blockchain offers a desirable platform to drive paperless transactions in a secure manner.

BAW as a platform is designed to host cryptocurrencies of any kind. The import of this is that corporations and governments can leverage this to launch distinct cryptocurrencies.

The Ukrainian government is in the process of creating the e-hryvnia- its own cryptocurrency. This will allow for faster transactions as well as a safe and very reliable payment system. Ukraine is not the only country involved in the blockchain. Its neighbors, Russia is in the process of creating its cryptocurrency- the CryptoRuble. It will be its national cryptocurrency. Belarus is currently allowing its economy to use cryptocurrency investments. Belarus gives Blockchain businesses lower taxes when compared to other firms, to ensure they blossom.

The African scene is not left by the Blockchain trend. Senegal is making plans to become the second African country, after Tunisia, to have its national cryptocurrency, eCFA. It runs on blockchain.
South Africa, through its Reserve Bank- SARB- has created its own, which it christened, the Khokha Project. The project is designed to create a payment system that uses proof of concept. The cryptocurrency will be a tokenized version of the South African Rand.

Governments are not the only ones creating Cryptocurrencies, companies are now involved. Kodak and even Telegram have their tokens.

BAW is designed to host cryptocurrencies of platforms created by governments and corporations. Unlike Ethereum, but we are offering advantages that will make the Ethereum Blockchain seem like child's play.

We have mastered the scalability problem that is affecting a lot of Blockchains, including Bitcoin and Ethereum. Hosting on BAW allows cross-chain exchanges seamlessly.

Above all, we cannot be attacked by Quantum computing, unlike the existing blockchains. Any country or firm that is keen to issue a cryptocurrency is rest assured that their tokens and Blockchains are safe

ARCHITECTURE AND TECHNOLOGY

BAW is made of Various Layers

Network Layer

BAW uses an algorithm that scales the platform to adjust to the rates to transactions. This is made possible by sharding, which is created to scale transaction rates. We intend to use sharding, which breaks the network into tiny shards that can be used to process transactions. All of these wil occur using a parallel processing method so that efficiency is guaranteed.

We will now look at transactions and network sharing.

Network Sharding

Here, we mean sharing the entire mining network into tiny shards in a process that involves two steps. The first has the electing of a loyal set of nodes- the directory service committee, DS committee. This committee is involved in sharding the network and sharing the nodes to their shard. It involves the following:

The Directory Service Committee: this ensures the sharding of the network is done by first electing a set of nodes, christened, the directory service nodes or DS nodes. These nodes are the ones that make up the DS committee. The DS nodes election done depend on the PoW puzzle.

This PoW puzzle can also be called PoWI, and its algorithm is Algo I Every node that was involved in successfully producing a nonce termed as valid for the PoW1 then comes up with the DS block header.

The DS block is usually made up of signature part and header. Immediately a node is involved in doing a PoWI, it generates solely the header of the DS block. The header generated gets to the DS committee in a multicast. The DS committee comes to a consensus on the header of the DS BLOCK before crafting their own signature part.

Immediately the bootstrapping phase is done, the DS nodes' composition is then shown by an already agreed on window size, n0. The new n0 nodes then form the DS committee. The period between the mining of two DS blocks following the other is DS-epoch. The time between both block, DS epoch is done in such a way as to prevent the two blocks from competing. In the DS epoch beginning, a brand new DS node is added to the DS committee, while the oldest one is removed.

This ensures that the number in the committee remains constant. The new entrant into the committee is made the leader of the consensus protocol for that period. If the committee is large like over 800, about 13 should be byzantine with high probability.

Resolution of Conflicts: With BAW consensus protocol, forks are not permitted in the DS blockchain. Forks occur when various nodes resolve a puzzle at approximately the same period. To resolve the conflict, every node in the committee removes the nonce field from its headers. Then sorts in an increasing order.

The new node, which is the leader of the DS committee, then gives his header, which must correspond to the largest nonce noticed. Then he ensures a consensus protocol is run on the DS block header to agree. Immediately they all agree on the header, the remaining part, the signature part, is built. The winner agreed upon becomes the new leader.

Generating Shards:

Immediately after the DS committee gets elected, the main sharding begins in the network. To participate, a node should have performed PoWII. The process of sharding is done again at the beginning of any DS-epoch. The algorithm that covers PoWII is in Algo II. The mixhash and the nonce for PoWII are then sent to the DS committee.

The nodes then accept the exact amount of PoW solutions needed to be sharded. Immediately the exact amount of PoW2 solutions needed get to the DS committee's leader, a consensus protocol is initiated to assent on which set of valid PoW2 solutions is needed. Immediately the consensus protocol ends, the committee's leader churns out the EC-Schnorr multi signature that the DS nodes signed. Over two-thirds of the nodes in the

DS committee must have assented on the acceptable set of PoW2 solutions.

Our network sharding involves using PoW puzzle to elect the DS committee in a very Democratic and decentralized manner. The DS committee then goes about the process of sharding, and the blocks' verification. Then they also verify if a large quorum had shown their interests within the shard.

BAW differs from other Blockchains that use PoW for consensus. BAW only uses PoW to safeguard our platform from Sybil attacks and get involved in sharding.

This means that PoW can easily get replaced by PoS, Ankther Sybil resistant mechanism. We are using both PoW- at a large scale- and PoS at a minor scale because PoW has some security guarantees and PoS is still at its infant stage.

BAW's Consensus Algorithm

Our consensus algorithm can be judged as efficient and totally secure. The DS committee and shards are run via an efficient and totally secured consensus protocol. The protocol allows every shard to come to an agreement on which blocks get proposed.
BAW's consensus protocol depends on the BFT idea- byzantine fault tolerance- while using a high level of optimizations. BFT was used in our consensus protocol design to make sure that there are definite resultant blocks, which removes long confirmation times seen in most Blockchains.

The prior BFT protocols in existence cannot scale over large nodes well because of its long communication bandwidth needed, and the longtime used to converge. We are using an innovative Cosi, a scalable signature scheme. Cosi can ensure BFT protocols become very scalable. Cosi might be seen to not work well in hostile environments like a public blockchain, but we have modified it to function well in our blockchain.

We have added more message rounds and steps to our enhanced Cosi protocol on both the signer and leader's sides to curtail any form of unscrupulous signer or leader. With our added checks, unscrupulous characters are found easily. Our enhanced Cosi can make our BFT protocol very scalable.

Transaction Sharding

BAW uses an account-based design that ensures transactions meant for sharding are sharded based on the sending accounts.

This makes sure that any attack that is similar to replay or double spending is circumvented by those exact nodes' shards. BAW ensures scalability via two choices in its transaction sharding protocol.

BAW ensures that atomic transaction commits are done while not involving the cross-shard communication, which is very complex and expensive.

In BAW, the consensus processes ensure that transactions are processed asynchronously with them. BAW uses a system, called, reject-and-retry to process transactions asynchronously as and immediately the nodes' majority are updated.

BAW's Sharding Friendly Smart Contract Language and Computational Sharding:

OUR smart contracts allow various kinds of apps to be crafted on our blockchain's distributed ledger. Existing Blockchains are fraught with problems that do not allow them to run intensive computational tasks because the computational task will always have to be repetitively validated by every node.

Though it might seem secure, it is expensive to run computational tasks of large scale on such a blockchain.

BAW proposes to make use of a brand new and innovative smart contract language which makes scaling faster and better for a myriad of apps. Our innovative smart contract language will run very well with the sharding embedded in our blockchain.
Our smart contract will ensure that computational resources' sharding is done on our blockchain network through the consensus process' overlay, known as computational sharding. The Computational sharding process ensures that participants in BAW and our apps inscribe the consensus groups' sizes for every subtask.
Every consensus group will get tasked, and they will compute the exact subtask while churning out results. The participant also inscribes the condition on which results will be accepted.

Our smart contract language, since new and innovative, might have some developers confused. We intend to solve this issue by giving developers a front-end higher level language that has its syntax somewhat similar to Solidity.

BAW will come with compilers that can convert automatically the somewhat Solidity smart contracts to our smart contract language. This will ensure that the cost incurred in transferring those smart contracts already existing to our innovative smart contract language will be will be cheaper and have very high throughput.

BAW's Cross-Chain Asset Transfer.

Since a lot of Blockchains exist, there is a need for a Blockchain that can move across one Blockchain to another. Our cross chain asset transfer involves connecting the prior mainly used cryptocurrencies' platforms like Ethereum and Bitcoin, and offer users the perk of having a complete

asset exchange while not bothering to modify the origin chains' system. This ensures that brand new churned out cryptocurrencies and blockchains get incorporated to BAW at a cheap cost.

Other consortium chains can get integrated with BAW.

This feature ensures that assets can easily get transferred to BAW from their original Blockchains. And movement of the assets from BAW to their original Blockchains while trading a myriad of assets on BAW is assured.

BAW makes sure that the cross-chain's transactions are done and assures that the stability of the cross-chain transaction services is possible.

BAW's Transaction Privacy Protection.

BAW ensures that trading parties can easily opt to carry out transactions in our top privacy protection system. BAW ensures that the exchange and transfer of assets are done safely. BAW ensures that owners of the assets are anonymous.

BAW's Functional Extensibility.

BAW intends to be a platform that distributes and allows for the safe exchange of a myriad of cryptocurrencies and other digital assets. BAW ensures that loan and deposit businesses are done for various cryptocurrencies.

BAW will ensure that users can carry out digital assets' transactions via a digital currency medium. BAW ensures that digital assets can be issued and traded on our platform.

OUR BLOCKCHAIN

Blockchain 5.0, BAW, is created with a multi-party computational system, a one-time account generation feature, a secret-sharing threshold, Lamport signature, and other quantum proof cryptographic technologies. BAW annihilates the concerns and shortcomings associated with smart contract and tokens.

BAW is an innovative and out of its league cryptographic app that resolves the issues that plague Blockchains and shows that blockchain as a technology is improving daily. BAW is created by a team of cryptographers that are using various cryptographic schemes that are immune to attacks from both quantum and classical computers.

BAW is a Blockchain that solves all the issues of existing Blockchains like scalability limitations, the limitations of cross-chain transactions, intra-chain transactions, quantum proof encryptions, and a blockchain with a high scalability of 100TPS to 100 million TPS because of its dynamic sharding configuration.

Our blockchain can support smart contract with our unique and innovative smart contracts language while providing privacy for transactions using smart contracts. Programmers can develop apps using BAW.

BAW uses an infrastructure and technology that allows cross-chain transfers to be done easily and fast. BAW is a blockchain that does the following:

• BAW can make the interconnection among Blockchains possible.
• BAW ensures that the cross chain transactions' records are complete.
• BAW ensures that the details of the cross-chain transaction are maintained.

BAW ensures that cross-chain transactions from one public blockchain to another, from one private blockchain to another, and from a public to a private blockchain are possible.

BAW's Smart Contract Virtual Machine and Distributive Ledger

BAW is a distributed ledger that ensures app can run independently while being accompanied by smart contracts and account models used in the implementation of a myriad of functions.

We optimized this by the addition of transactions that are cross-chain transactions while achieving privacy.

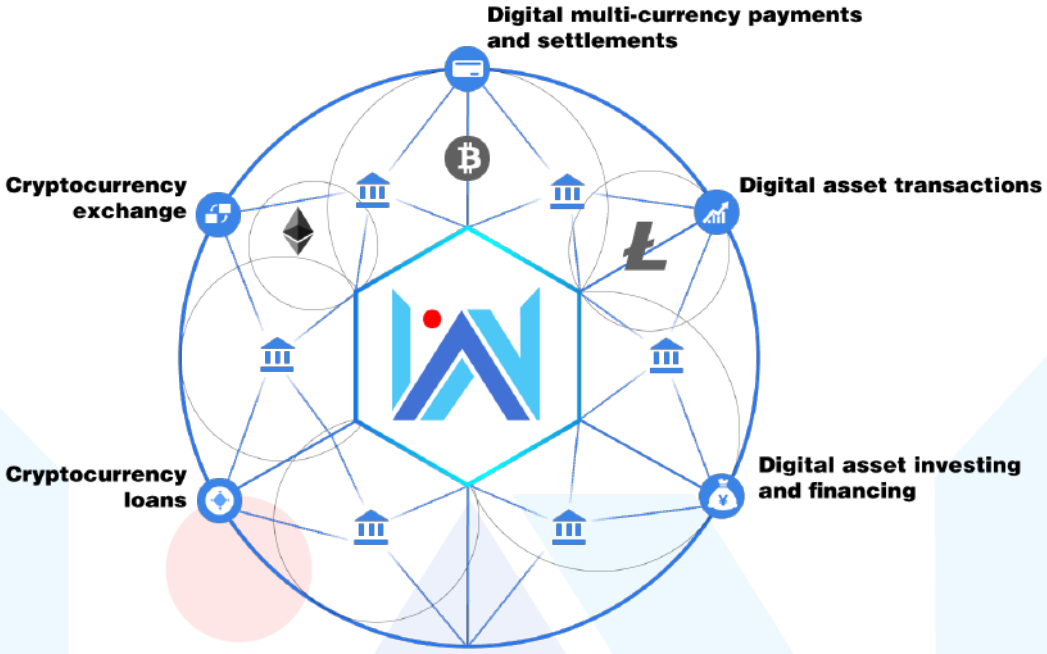
BAW's Native Coin

BAW will have its coin, BAW coin, a native coin and the unit of account of BAW. Our intra-chain and cross-chain transactions use an amount of BAW coin. BAW coin can be used as a security deposit in the nodes that verify cross-chain transactions.

BAW's Consensus Mechanism

While sometimes using PoW to prevent Sybil attack and for the election of DS nodes, BAW also mass use of Proof of Stake (POS) as the consensus mechanism for mere transactions, while also using it to reach consensus.

BAW's Intra-Chain Transaction



The transactions done within our blockchain can be likened to Ethereum but with added privacy system and other innovative systems that are done through the Lamport's signature scheme, working with the ring signature scheme. We are not leaving out the one-time account mechanism.

BAW's Cross-Chain Connection

To allow for easy cross-chain transactions, the Blockchains and assets that will be integrated with BAW will have to firstly be registered to ensure that BAW can easily identify them.

The functions get done through the asset registration and chain protocols. To ensure that cross-chain transactions are possible, BAW makes use of the threshold secret sharing joint anchoring systems and secure multi-party computing schemes to ensure that integration is done at minimal cost.

Integration with our BAW's cross-chain communication protocol, while not altering the implementation of the former chain. BAW is a platform that uses such infrastructure that makes its applications to be seen in

financial apps needed to protect smart contract transactions in both private and public blockchains.

BAW's Cross-Chain Transactions registers a new asset immediately it gets moved from its previous blockchain to BAW. BAW creates a brand new asset while making use of an inbuilt asset template on BAW to move the brand new smart contract using the information of the cross-chain transaction.

In the case of an asset that is registered, it is moved from the prior blockchain to BAW, BAW will give out the tokens equivalent to the existing smart contract to make sure that the previous blockchain assets can be traded on BAW. To show how the transfer from a public chain to BAW, let's use an Ethereum example.

In the Transfer-In Process, Jon wants to transfer 20 ETH to Kate, who is on BAW. Jon initiates a request for a cross-chain transaction while making use of the BAW wallet, then starts the transfer on Ethereum, while Kate's on an Ethereum cross-chain Locked Account.
BAW's verification node gets the request of a cross-chain transaction, does the verification of the said transaction that has already been recorded on Ethereum blockchain, then churns out a brand new smart contract token on BAW, which will correspond with the ETH needed by Kate, who is on BAW.

BAW's Cross-chain Transfer-Back Process: Kate wants to move the 20 ETH she got from Jon to Dave. Kate used his BAW wallet to start a cross-chain transaction with the smart contract's asset given to him.
When the verification node gets the request, it locks the 20 tokens' assets. Once the locking is done, the verification node, while making use of threshold secret-sharing mechanism crafts out an Ethereum transaction. This is done using the transferor's and transferee's account

on Ethereum platform. Once the verification node verifies the transaction on Ethereum platform, the token locked in Kate's account gets cleared. This means that the equivalent asset gets moved back to the previous blockchain, Ethereum.

BAW's Cross Chain Transactions Is Decentralized

On BAW, we are unlike other blockchains that use third parties before cross-chain transactions are possible. The third parties are usually exchanges, mostly the centralized ones that need a third-party custodian account. This means that users have to complete truth the third-party, and that has brought anguish to a lot of users, especially when the exchanges get hacked.

BAW's Unchanged Original Chain and Low Integration Threshold

During our cross-chain transaction solution, the mechanism in charge of account locking is not involved in two-way anchoring. Our solution does not involve that addition of more script extensions to find, then verify the SPV- **Simple Payment Verification.**

Every transaction data gets transferred to the original chain's node after our verification node has reconstructed and integrated them. There is no need to modify the original chain's mechanism to work with BAW. This will reduce the cost of working with BAW.

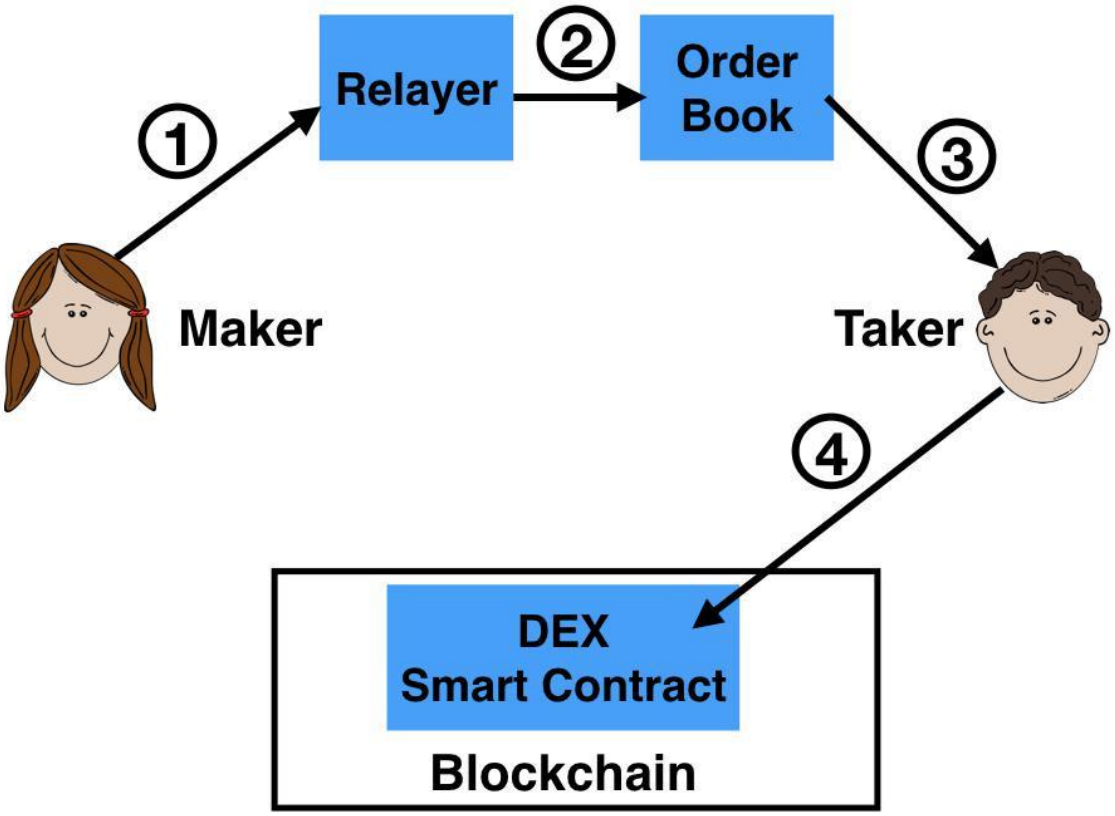
BAW's Cryptography Based Security Guarantee

Many cross-chain exchanges use the algorithm that heaps all the underlying security responsibilities to the users. These exchanges believe that users have to be rational to protect themselves from threat. This is christened, 'Rational Participants Hypothesis'.
While we use elliptic and Lamport's signature schemes, we also make use of:

• Privacy protection system designed for smart contract token transactions built on one-time accounts and ring signatures;
• Threshold secret-sharing infrastructure

Our solution that is built on the platform of multiparty computing, locked account management solution. Every transaction is done via BAW's verification nodes and removes the need for interference by third parties.

BAW's Cross-Chain Transaction Privacy Protection Technology



BAW's cross-chain transaction system allows assets of the previous blockchain exist on BAW in the guise of smart contract tokens when they are transferred to BAW.

On BAW, we provide cover well the smart contract token transactions' initiators with a set of accounts, using our innovative ring signature technology, making it untraceable.

We also allow our smart contracts to have one-time use of accounts to ensure that the relationship between the previous accounts on BAW cannot be found. Using these two methods listed above, BAW attains privacy of the transactions done using smart contract token, while assets'

cross-chain transactions are also achieved under optimal privacy protection, for an improved user-experience.

BAW's verification nodes are grouped into three:
• General verification nodes, also known as validators;
• Cross-chain transaction proof nodes, also known as Vouchers;
• Locked account management nodes, also known as Storemen.

Vouchers are the providers of proof of transactions between the previous and locked accounts.
The voucher pays an amount of security deposit. If the deposit is higher, there is a high chance that the proof provided gets adopted.
If the proof is false, the security deposit gets removed from its holding account. Then the voucher's authorization is revoked.

The Storeman validates the signature in its key's part, then join the parts of the signatures to make a lock account's complete signature.

The storeman is informed by the Validator of its operational actions that are linked to the locked account. The record of operations on BAW is completed at the point when the transaction proof gets to a consensus.

BAW's Security Threshold

BAW's Security falls on the total value. How does this come about?
This depends on BAW's overall value. Immediately the total value of every cross-chain transactions is greater than BAW's total value- the gains from collusion becomes greater than the opportunity cost, which means the possibilities of collusion between validation nodes will improve. We will ensure colluding doesn't occur on our platform.

Creation Of The Private Key on The BAW.

A user can create his or her private key on BAW by making use of our random number generator, and then churn out 256 pairs of random numbers.

Every number will be 256 bits in size. This will lead to a sum of 2×256×256 bits = 16 KiB in total. This makes up the user private key and it can be stored in a private place for usage later.

In creating the public key, he or she will have to hash every of the 512 random numbers in his or her private key. This will lead to 512 hashes that is 256 bits per size. The 512 numbers become his or her public key that can be shared with the world.

Verifying the Signature

When another user, user 2, wants to verify user 1's message signature, user 2 also has to hash the message in order to extract the 256-bit hash sum. User 2 then makes use of the bits in the hash sum to extract the 256 of the hashes in User 1's public key. BAW ensures that user 2 picks the hashes exactly the same way User 1 picked the signature's random numbers. User 2 then hashes every of the 256 random numbers in User 1's signature, giving 256 hashes.

Once the 256 hashes picked by user 2 matches the 256 hashes that was picked from User 1's public key, then the signature is right. If otherwise, the signature is wrong.

Below is a short description of how Lamport signatures work, written in mathematical notation. For a plain English description see the next section. Note that the "message" in this description is a fixed sized block of reasonable size, possibly (but not necessarily) the hash result of an arbitrary long message being signed.

Keys

Let k be a positive integer and let $P = \{0,1\}^k$ be the set of messages. Let $f: Y \to Z$ be a one-way function.

For $1 \leq i \leq k$ and $j \in \{0,1\}$ the signer chooses $y_{i,j}$ randomly and computes $z_{i,j} = f(y_{i,j})$.

The private key K consists of $2k$ values $y_{i,j}$. The public key consists of the $2k$ values $z_{i,j}$

Signing a message

Let $m = m_1 \dots m_k \in \{0,1\}^k$ be a message.

The signature of the message is

$$sig(m_1 \dots m_k) = (y_{1,m_1}, \dots, y_{k,m_k}) = (s_1, \dots, s_k)$$

Verifying a signature

The verifier validates a signature by checking that $f(s_i) = z_{i,m_i}$ for all $1 \leq i \leq k$.

In order to forge a message Eve would have to invert the one-way function *f*. This is assumed to be intractable for suitably sized inputs and outputs.

BAW's Security Parameters

BAW's Lamport signatures depend on one-way hash function's security, its output's length, and input's quality. In the Lamport signatures BAW uses, every public Key's bit and its signature depends on the short messages that require basically s single invocation to a hash function.

Every private key y i,j and its corresponding must have a private key length that is chosen so that when a preimage attack is performed on an input's length, it is not quicker than performing on the output's length, a preimage attack. Our balanced system makes sure that the lengths are equal.

BAW's PoS (WP)

PoW is used by a lot of Blockchains and cryptocurrencies and the mining process in those Blockchains are stressful and not environmentally friendly. With the mining process, such Blockchains can easily be tampered with, with the growth of quantum computing and even ASICs. Since we are creating an innovative blockchain, we opted for PoS. We are not using the normal Casper Scheme for PoS.

Ours is an improved version of PoS Casper. We built on Casper and removed all the flaws of the Scheme.

Our version removes the opportunity of unscrupulous stakers to carry out attacks. It will be impossible for such attacks like 51% attacks to occur because the attacker will need a large percent of the coins in the platform. Even when the attack procures that amount of coins, at a very exorbitant amount, the attacker will lose the coins, his funds, if he attacks.

It will not be profitable to the attacker. Even if the attacker gets more than 51% of coins of the platform- which is impossible- and is ready to lose his funds in the attack, the attack will still not be possible because of risk and stake factors.

Our version annihilates transaction censoring loopholes.

Those miners in PoW can decide not to mine a block with certain addresses, meaning that the addresses get censored from the blockchain. With our PoS version, block creators get chosen at random, it will be hard for the censoring of addresses from the blockchain to happen. If a user tries to force the system into censoring, he or she might lose his stake.

BAW'S APPLICATIONS IN THE REAL WORLD

• BAW can be used in lending and borrowing:
• Once a currency, especially a digital one, is used as a medium of exchange, it can then be used to generate funds for the owners
• Users of digital currencies that are involved in creating value are in need of more of those currencies
• Those who possess the currencies want more value
• Those in possession can easily lend the digital currencies to those in need
• It is like the traditional banking system.

Sources of funds that are not in use are linked to those in need of funds. Let's say, a developer creates a smart contract for a deposit app while setting the interest rate on BAW. Another user then transfers his Ether from the blockchain it is held in- Ethereum- to the BAW smart contract address created via our innovative cross-chain transaction system we have created. The deposit thus made on BAW then gives the corresponding voucher to the user who needs the coins.

During the process, the interest is calculated by the smart contract technology. Immediately the deposit is to be withdrawn, the intermediary address will receive the voucher, and another cross-chain transaction gets done. The ETH then gets unlocked in the original user's account.

BAW can be used for settlements and payments.

In the past, merchants would have frowned at the thought of getting paid with digital assets, but that has changed. A lot of merchants now accept cryptocurrencies. Cryptocurrencies are now seen as a payment method because of the numerous advantages they offer.

Our Blockchain has a distributive multi-currency feature that incorporates a lot of payment solutions, settlements procedures and banking ledgers into an innovative single ledger. Anyone can access this by simply downloading our wallet, and the multi-currency payments and settlements solutions are at the user's fingertips. This removes the need to install various cryptocurrencies' wallets to hold various cryptocurrencies.

BAW introduces A Decentralized Exchange For Transaction and exchange.

Centralized exchanges have ripped off users for a long enough till now. With BAW, the need to use centralized exchanges is obviated. The common problem users' face in centralized exchanges is loss of funds due to hacking. Users will also be spared the exposure of such losses and the rigmarole involved in using many platforms for a single transaction.

On the BAW platform, users can exchange multiple currencies can easily as a result of our multi-currency integration algorithm. Users can conduct peer-to-peer exchange with our smart contact, and delve into trading of multiple currencies.

The issue of privacy is well-catered for within BAW, our privacy enhancement features shields transactions from the glare of the public. We achieve this privacy feat by keeping our fund tracking paths away from the front-end.

Users of BAW are also able to transfer their digital currencies to the platform and execute private transactions securely. Relocating the initiated currencies to their source –platform is also securely supported courtesy of our cross-chain capacity.

Official Website: https://baw.network

Twitter: https://twitter.com/BAWnetwork

Telegram Group: https://t.me/BAWgroup

Telegram Channel: https://t.me/BAWannouncement

Reddit: https://reddit.com/r/BAWnetwork

Medium: https://medium.com/@BAWnetwork

Youtube: https://bit.ly/2K6jgYo