Bywise: The next generation of cryptocurrencies as a payment method

Felipe Martins[1] and Vitor Sulzbach[1]
[1] *Devel Blockchain*

I. INTRODUCTION

On October 31, 2008 the Bitcoin white paper[12] was published. Until that time, there was no secure cryptocurrency without using a central institution. this barrier made impossible to use any digital currency on high scale as a fiat asset. Some proposals were made, but none implemented security and decentralization simultaneously.

Bitcoin created an auditable system, without a central institution and through proof of work (POW) made it more profitable for a malicious node to work on favor of the network than against it. Despite having some defects such as the lack of privacy, it was the first cryptocurrency to bring security and decentralization, allowing the great growth in value and volume of transactions that it obtained in the last decade.

This scenario can be seen as the global race for the first cryptocurrency that managed to simulate the scarcity of an asset like gold in a scalable and reliable way, a revolution that allowed the existence of a new market environment [14].

Since 2009 several *cryptocurrencies* have been specializing in niches. Ethereum created an extremely flexible platform in blockchain capable of processing smart contracts, generating tokens, among other features[2]. Monero has generated a network that makes anonymous transactions[17]. Stablecoins like Tether and DAI are able to set the crypto price based on a real asset such as dollar or gold. These are some of the specializations and abstractions of the initial idea of Satoshi Nakamoto, which try to solve problems slightly different from the initial one.

Despite efforts, there is no cryptocurrency present in the daily transactions of the population. Some projects were conceived, such as DASH, Zcash, Monero, Litecoin, BitcoinCash, BitcoinSV, but they did not achieve a result that compares with a fiat asset.

According to Mohania and Singh[11] there are some partial or complete differences between fiat currencies and cryptocurrencies, one of them being the volatility of the asset. Since crypts are not tied to a central institution or to an existing resource such as gold or silver. Consequently, it is a big risk to store assets on the blockchain.

Unfortunately, this characteristic is intrinsic to the nature of a decentralized currency and although it drives away industries and brokers that do not want risk, it also brings benefits such as transparency in the expansion of the volume of assets and other aspects of governance.

Another difference is the precariousness of current crypts as a payment system compered to physical money and its digital presence, creating a barrier that limits the use of crypts in retail. Are they:

- Currency volatility adds risk to asset usage.
- High transfer rate between wallets makes its use less attractive.
- There is no guarantee of payment in the case of instant sales.
- High resistance from merchants and consumers, it is necessary that the crypto be beneficial for both.
- Accessibility of the merchant and consumer in the use of the asset.
- Low scalability due to the delay for approval of the transaction by the blockchain and few transactions per second.
- Hacking risk and cybersecurity knowledge needed for users.

Just like 12 years ago, there is a race for the first cryptocurrency to enter the daily lives of the population. Like Bitcoin's history, this path is gradual and possibly slow, but it can be achieved as long as these barriers are broken in a single solution.

As previously mentioned, other projects obtained significant results, but very far from a fiat assets. As with pre-Bitcoin cryptos, none simultaneously solved these problems.

A. Historic

DASH: The *Digital Cash*(DASH) intends to be used as a means of payment in everyday transactions[5]. this cryptocurrency has positive usability points, such as instant transactions, however it is based on the bitcoin architecture, which is not scalable and cannot be easily loaded onto a website without third party services[9].

Monero: Monero is a cryptocurrency specializing in anonymity. Through a shuffling algorithm, transactions respect the principles of non-traceability and disconnectability proposed by T. Okamoto and K. Ohta[13]. Part of its algorithm is based on bitcoin, so it presents scalability problems, despite having variable parameters such as block size[10].

Zcash: Zcash is a cryptocurrency focused on optionally visible transactions. It is a good alternative for tax auditing and legal procedures, as it allows you to generate a key that only read transactions[3]. Unfortunately,

there are several scalability problems as it is a fork of Bitcoin and the contingency plans fail in terms of financing the development.

Others Altcoins: Several altcoins, forks from the bitcoin repository, have been developed in order to allow a greater volume of transactions. Bitcoin Cash is a direct fork of the Bitcoin repository and aims to increase the size of the block, which proportionally increases the amount of transactions per second. BitcoinSV is a fork of Bitcoin Cash that seeks to be more faithful to the project idealized by Satochi Nakamoto. Litecoin uses the Bitcoin structure but is optimized for a high number of transactions per second. All of these have, in a greater or lesser extent, the limitations that the Bitcoin architecture brings, such as non-scalability, slow transactions and problems with congestion and tax volatility.

B. Governance

In August 2017 there was one of the worst events in the history of bitcoin, the hard fork that originated BitCoin Cash[19]. The coin was split into two chains and no one was sure which currency would be considered the official Bitcoin. This scenario generated chaos among the stakeholders who did not know how to proceed, the price of BTC fell a lot in the first days and then gave rise to the historic Bull Run. The price and transactions volume of the currency was so absurd that the fees passed 50 dollars per transaction, causing many people to lose interest in the currency due to its volatility and high rates.

This event had its origin in ideological differences between Bitcoin developers. Some of them believed that the high rates could be reduced by increasing the block size from 1MB to 8MB. This difference was resolved in a very immature manner, causing problems for the entire network.

If a governance system had been established from the beginning, the decision could have been democratic, the network would have voted for the option it considers most comfortable, in an organized manner, without harming the cryptocurrency.

This is just an iconic example of how a hard fork damages a crypto, other cases have also occurred, but they are not the only problems of lack of governance. A coin is usually launched with only the basic principles of its design, with time and investments it is developed, going beyond the initial idea. Several stakeholders are involved in this process, such as miners, exchanges, daytraders, among others, and it is recurrent that one of them ends up taking control of the project, directing the currency to their interests.

If a group has the majority of the decision-making power, it may suffer from unhealthy decisions in the long run, after all every groups are essential for the currency's livelihood and need to be considered for its durability.

An example of good management is Tezos, which has a modular architecture[8]. Its proposal is the easy exchange of blockchain architecture, just remove the desired module and replace it with a new one. This modular project associated with voting system within the network allows the currency direction to be democratically decided. When a technical or ideological divergence arises, the network will not split into a hard fork, only with votes will the friction be resolved.

C. A Bywise

Bywise intends to enable the use of cryptocurrencies in everyday transactions. It is part of the third generation of crypts and is not a fork of an existing project. It is built from scratch based on seven pillars:

Pilar 1 *Scalability*

Pilar 2 *Safety*

Pilar 3 *Usability*

Pilar 4 *Governance*

Pilar 5 *Privacy*

Pilar 6 *Real-world applications*

Pilar 7 *Stability*

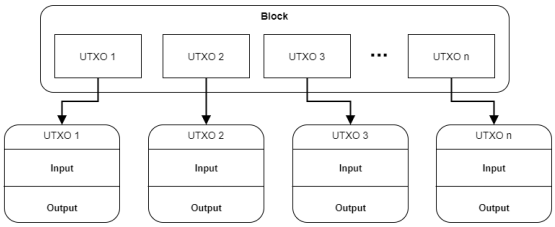
These pillars are guides for the development of the cryptocurrency, which despite not being finalized, has already validated by simulation various innovations and concepts.

These innovations include the maximum rate of 100 million transactions per second without breaking the network into sidechains, they also include a new secure instant transaction system, a new block system, defi conversion to satellite stablecoins, multi-step security, more accessibility to systems , shopkeepers and users. These are some of the main innovations designed that will be further explored in the following chapters.

II. THE BLOCK

Cryptocurrency blocks are packages filled with transactions. These transactions have inputs and outputs where the amount of input currency must be equal to the output, except when it is foreseen the creation of currencies for investors, developers and/or miners. This structure forms a ledger that shows the transaction history since the beginning of the network.

FIG. 1. Standard block



A node that wants to mine a block must assemble it through a shared transaction storage called memPool, usually choosing the transactions that pay the best rates. The block with an increment is used to assemble a number using a method called hash function.

Finally, the nodes compete to be the first to find a hash smaller than a specific target. The winner spreads his valid block across the network and takes the gains from mining. As soon as a contest ends, the new block enters the blockchain and another contest starts, forming a cycle.

A. The Limitations

The Bitcoin Network has known limits. A block takes an average of 10 minutes to enter the blockchain, reaching 4000 transactions, which leads to a maximum value of approximately 6.67 transactions per second[16].

$$\frac{maxTransactions}{blockTime} = \frac{4000}{10 * 60} = 6.67 \qquad (2.1)$$

Bitcoin-based forks and networks bring changes such as block size and block processing time to maximize scalability. As an example we have Bitcoin Cash which has a block size of 8 MB and an average transaction size of 480 bytes, which reveals an approximate maximum rate of 56 transactions per second.

$$\frac{maxTransactions}{blockTime} = \frac{\frac{8*(1024*1024)}{250}}{10 * 60} = 55.92 \qquad (2.2)$$

Other variations try similar strategies, but do not come close to the 65,000 transactions per second of the payments giant VISA[18]. Today cryptos that reach very high rates use other forms of consensus, such as the Proof of Stake, which is gaining a lot of popularity with the EOS cryptocurrency, however there are many doubts when it comes to security, also they do not have the massive experimental validation that bitcoin gave to the Proof of Work.

Coins that use proof of work do not increase their block size far beyond 8 MB and do not greatly reduce the average entry time of blocks as forks may occur on the blockchain.

The forks happen when two nodes generate a valid block in the contest almost simultaneously, the two transmit to neighboring nodes and the network is divided based on which block the nodes receive first. These phenomenon happen with a certain frequency but luckily there are algorithms to decide which ledger will be continued, without the need for intervention.

Christian Decker and Roger Wattenhofer modeled the likelihood of forks happening on bitcoin's blockchain[4]. This probability is directly related to the size of the block and the average time to close a tender.

If a blockchain has very large blocks and a very low average tender time, the network generates forks faster than regenerates them, being divided constantly into several sidechains with their own ledger.

It is also not ideal that the rate of appearance of forks is close to that of treatment. Small forks can be almost harmless but the problem becomes relevant when the network is separated into large forks and the blockchain can end up growing separately[7].

The only solution is intervention, where only one ledger will be selected, the parallel ledgers and their transactions will disappear as if they had never occurred. The losses are colossal because a lot of money ends up being circulated in parallel and the transactions are suddenly reversed. Obviously all the physical money spent on these transactions is not reversed with the blockchain and much of it will not be recovered.

Another concern regarding the division of the network are 51 % attacks. When the network divides, the computing power also divides, if a group has more than 50 % of the fork's computational power, it is possible to make double expenses, something that has already been done even in the bitcoin blockchain when there was a major division in sidechains. due to version update issues[7].

Therefore, stability and security problems make it impracticable to change a lot the block time or its size. The network would not come close to carrying out VISA's 65,000 transactions per second without breaking, and even if it were enough to increase the speed of the blockchain by two or three times, the propagation of blocks on the network will be proportionally worse, being only an exchange between speed and security.

To increase scalability to very high values, it is necessary to do more than balance variables. It is necessary to review all the processes on the network to find wasted computing power and reassess the need of some steps.

III. BLOCK STRUCTURE AND PROPAGATION

One of the processes reviewed at Bywise is the complete validation of the block before transmission to other nodes. This measure is extremely necessary because an attacker can perform an spam attack, generating a huge amount of invalid blocks to congest the network.

During validation each node ends up holding the information for a while, generating a delay. This delay

increases the propagation time of the block, allowing another valid block to appear and generate a fork in the network, even if temporary.

This phenomenon is called block collision and to minimize it, the network must propagate a block very quickly. The smaller the time window available for collision, the less likely it is to happen.

To avoid spam the block needs to be validated before being transmitted, but optimizations can be made. Bywise's strategy is to use the network's mempool to preprocess transactions.

Due to the use of mempool any cryptocurrency already knows the transactions long before they officially enter the blockchain. You can then validate all mempool transactions even before a block is ready. The block hash serves as an identifier and, if necessary, can also check for changes.

By storing only the transaction hashes in the blocks and using sha-256, the block will be made up of 32-byte hashes. If each block has 10 MBs then we have a rate of 546.1 transactions per second.

$$\frac{maxTransactions}{blockTime} = \frac{\frac{8*(1024*1024)}{32}}{10*60} = 546.1 \qquad (3.1)$$

When a block is propagated, a node will verify that the transaction hashes are in the mempool and marked as valid, reducing almost all the delay in the propagation of the block due to validation.

This addition is extremely efficient, with a speed gain of almost 10 times compared to bitcoin Cash, however it still is very little close to the number of transactions per second of the major credit card companies.

Bywise uses its own block architecture, called **Uniform Data Distribution, UDD**(Uniform Data Distribution), formed by transactions and slices as shown in the figure 2. This architecture creates a "superblock" made up of smaller block hashes instead of transactions. These smaller blocks are called slices and carry transaction hashes.

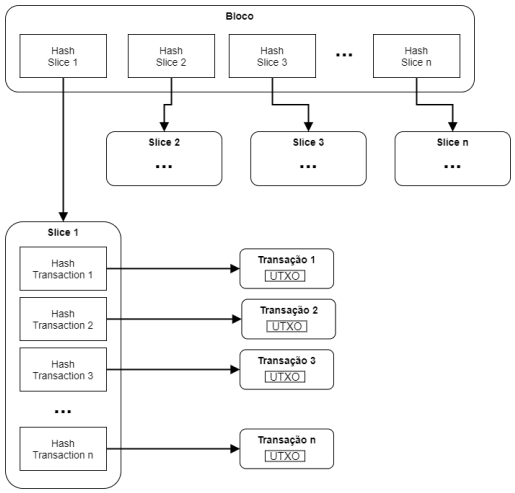
A new mempool is added to the blockchain to contain the slices, which are also pre-validated. Likewise in the propagation of a block, the step of validating the slices becomes unnecessary.

This structure is multiplicative, allowing a much larger number of transactions per block. If Bywise has 1 MB slices and a block with a maximum of 10 MB, the maximum number of transactions per second is quadratic and returns an absurdly high value of almost 17 million transactions per second.

$$\frac{maxTrans}{blockTime} = \frac{10*((\frac{1024^2}{32})^2)}{10*60} \approx 1.79*10^7 \qquad (3.2)$$

What allows such high values of transactions per second is the quadratic nature of the block stratification associated with pre-validation of slices and transactions, if these elements were revalidated before the transmission of the block, the propagation would be absurdly slow, generating forks in the network.

FIG. 2. Blocks, Slices and Transactions



Another change made is the limitations of blocks and slices being made in number of transactions and not size in MBs, since hashes of fixed size and not whole transactions/slices are stored.

It is also expected that with slices of 32,768 transactions (1 MB), one or two slices per block would occur at the beginning of the network. This phenomenon can open breaches for attacks or dishonest practices.

In order to avoid a few slices in a block, the blocks were divided into regions, each region has a maximum of transactions per slice, something similar to the epics of a cryptocurrency roadmap, but with the IDs of the slices instead of the IDs of the blocks in the ledger.

Region	Start	End	Transactions for each Slice
1	0	100	10
2	100	1.000	100
3	1.000	10.000	1.000
4	10.000	100.000	10.000
5	100.000	600.000	100.000

TABLE I. Bywise block regions

To use slices that contain many transactions, it is necessary to first fill in the smaller slices, hardly a block will have less than 1,000 transactions, which is enough to fill

the first 100 slices. The number of transactions per block in this model exceeds 60 billion total and more than 100 million per second.

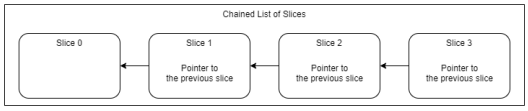
IV. CONSENSUS

As Bywise stratifies the Block in Slices and transactions, it is necessary to create a new consensus algorithm. A variation of bitcoin's proof of work is used, where block mining is similar. The contests are generated continuously by the network and the first to generate a valid block wins the mining fees. The POW consensus gives the security validated by bitcoin over the years.

The transactions also don't change their validation mode, the difference in this case is that the validation occurs before the transaction enters the mempool, and it is not necessary to revalidate it in the transmission of the block.

The slices are entirely new entities. Since the high transaction rates is one of the pillars of the currency, it would not make sense to use any POW algorithm in the layers below the block due to the chances of collision and resource consumption.

FIG. 3. Chained List of Slices



Slices are released into the network freely by nodes that have at least a defined amount of coins, and make up a linked list where each position points to the previous one. A launched slice must mark its position in the list, and can only occupy that space. Considering the candidates for each position, priority will be given by the rules:

Rule 1 *The first slice of the list will be the one that has the smallest difference between your hash and the hash of the previous block.*

Rule 2 *Positions after the first will be defined by the smallest difference between your hash and the hash of the previous slice.*

It is natural that new slices and lists appear while a block is made or propagated, so it is not necessary to use the most updated chain according to these rules. This measure is taken to avoid constant collisions between emitted blocks and new slices lists. Even if a miner can ignore the biggest chain, new ones cannot be forged because each slice points to the previous one, making it economically unfeasible to produce blocks against the main list.

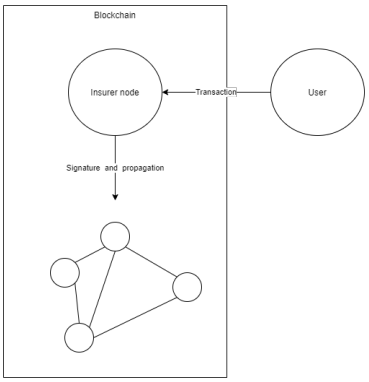
As this system is stratified, each part may undergo changes, such as migration from POS to POW and vice versa, all based on the governance systems established in this document.

V. INSTANT PAYMENTS

Instant payments are already a reality in the world of cryptos, some currencies have this function but with some problems related to security of purchase.

Bywise is able to make instant payments using insurance nodes, which are responsible for insuring the purchase if it does not enter the blockchain. If the wallet has no balance and the insurance node makes the mistake of signing the purchase, the amount will be deducted from their funds.

FIG. 4. Instant transaction posting



A wallet must define its insurance node if it wants to carry out instant transactions. These transactions are valid as soon as the node signs them, a very fast process as it does not depend on blocks or any other structure.

For an insurance node to launch a transaction, only one rule must be respected:

Rule 1 *The sum of transactions launched by an insurance node cannot exceed the balance of his wallet.*

Thus, the security of the network is guaranteed, and it is not possible to raise the insurance node to approve a bad transactions.

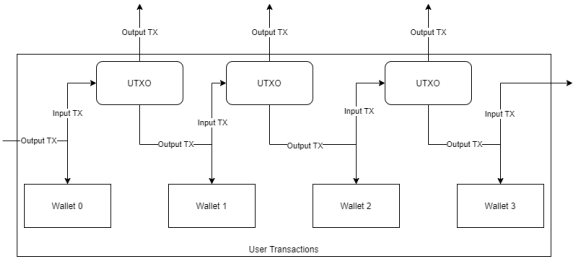
VI. PRIVACY

In bitcoin any node on the network can see all the transactions already carried out. This feature gives the possibility of auditing, allowing anyone to validate the entire transaction history of the network. As a result, security is increased but all user privacy is lost. If a wallet is linked to a real identity, such as an institution or person, its balance and transactions will no longer be private.

Other cryptocurrencies allow complete anonymity, but without audit permission, creating a scenario where fraud on the network cannot be detected. Legal problems can also arise because monetary systems without auditing are not tangible by law, which are ideal for schemes of corruption, trafficking, money laundering, among other illegal activities.

Trying to reconcile auditing and privacy, Bywise uses each wallet only once, so the user balance being the sum of the balances of the wallets in use.

FIG. 5. Bywise User Wallets



With this measure, the network grows in a chaotic way, even if an identity is linked to a wallet, it is unlikely to trace the identity through the network in the long term, however the system is still auditable and any fraud in the network can be detected.

VII. USABILITY

Many cryptocurrencies fail in their goals due to lack of usability. Whatever is the final objective, it is extremely necessary that stakeholders are able to use the product.

Today most web sites use large providers and simplified graphics systems in their design. Old languages are still very present in the modern web, one example is PHP. According to W3 Techs PHP is still used in 78.9% of sites at least on the server, approximately 4 out of 5 websites[15].

This means that four fifths of the internet has inherent limitations of the PHP language. Several limitations are also found on websites made in large hosting companies, which generally transforms the complexity of setting up a blog or store in a few visual steps or a simple deploy of html / css / js files. A major player in the website market is Wordpress, W3 Techs estimates that at least 38.8% of the entire web uses wordpress, several limitations also apply.

Among the problems of this scenario is the use of low level sockets, the same ones that are used in practically all blockchains. For a store to implement direct communication with the blockchain it is necessary to use VPNs or more dynamic and expensive technologies, and even if integration is possible it is still necessary to have a team of technicians, programmers or a great know-how of the technologies used.

If it is necessary to implement a physical point of sale, there are also associated problems. Low-level sockets have some advantages, but not all components of embedded systems provide good support for such technology. The quality of mobile networks is a challenge for the transmission of information. The price per unit of an electronics is greatly affected by each additional software requirement, such as the need for more memory, storage or operations per second. Several limitations exist in the design of an electronic product and you cannot outsource such limitations expecting to be compensated in hardware.

For greater usability, Bywise uses HTTP requests and websockets in most of its communications. This allows the creation of plugins on all types of hosting and technology sites, in addition to simplified use in embedded systems.

Dependence on third parties in the use of a plugin is also an issue. To process payments on a website, companies like Picpay or Paypal can be used, but all charge fees as a business model. The use of HTTP requests and websockets allows Bywise developers to compose plugins and components for any platform without the aid of third parties, which eliminates the recurring service fees.

VIII. GOVERNANCE

Lack of governance is a serious problem in the cryptocurrency market. Even the most consolidated like Bitcoin have already suffered from a lack of governance, with the most iconic example being the hard fork Bitcoin Cash, which separated the bitcoin network in two, severely damaging the price of the currency.

In addition to hard forks, small targeting decisions are important. Tezos is an example where governance is a differential, its modular architecture allows the exchange of its protocols and architectures in a simple way, these exchanges are guided by a voting system within the blockchain[8]. Even if it is not instantly noticeable, small decisions greatly influence a cryptocurrency over time.

There are several groups in a currency environment, miners, investors, dayTraders, exchanges, among others. To prevent a specific group from dominating currency decisions, Bywise has a voting system within the blockchain where the weight of the vote is based on the amount of Bywises a wallet has.

IX. STABILITY

Every economy in the world needs a minimally stable currency, if not obtained, it has many consequences, the population is never sure of the values of products in the markets, a bank needs to charge high fees on any loan, a trader who sells his stock for an amount may have way less in the next day, among others.

Looking at the importance of stability in commercial environments, Bywise sees as a necessity the implementation of a DeFi system within its blockchain for currency conversion, having as basis the collateralized debt positions(CDPs) and the oracle nodes.

If a user wants stability within the blockchain, simply save resources in the form of satellite tokens with prices based on fiat currencies.

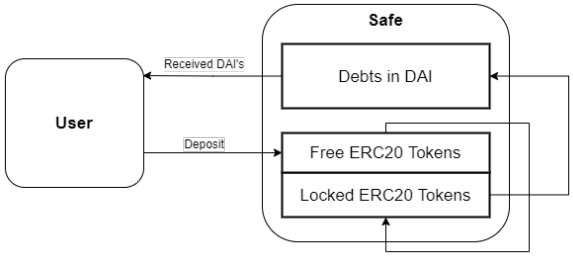
A. Collateralized Debt Positions(CDPs)

Collateralized Debt Positions(CDPs) were introduced by the cryptocurrency DAI a few years ago and form the basis of a decentralized stablecoin within the ethereum blockchain[6]. With a broker-like service, the MAKER platform is able to issue smart contracts that exchange a wide variety of ERC20 tokens with DAI's at a stable value of 1 DAI to one dollar.

The CDPs function as a safe where an ERC20 ethereum token is stored in exchange for DAI's. As the funds used do not leave the platform, the system is auditable and brings a lot of reliability.

The creator of the safe get a debt in exchange for the DAI's, which locks all or part of the assets. Multiple debts can be created as long as there are unblocked tokens. As each safe contains only one type of ERC20 token, a user can create several safes.

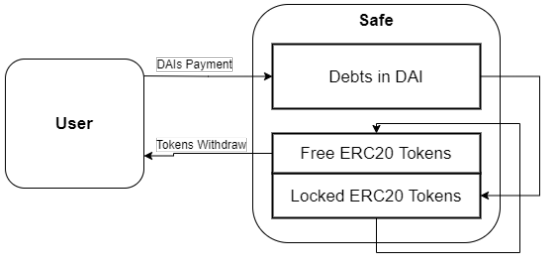
FIG. 6. Purchase of DAIs



The user can withdraw assets that are not locked and a debit can be extinguished upon payment. The payment is increased by a fund withdrawal fee that controls the flow of DAI's.

This fee is called the stability fee, which interferes with supply and demand and consequently its price. Thus, the DAI stabilizes its value when it moves away from the target (1 USD).

FIG. 7. Withdrawal of locked assets



B. Oracles

The market price of each token is defined in real time through nodes called oracles. This are democratically voted by the community to define the conversion value of each ERC20 token into dollars.

There is also an extra layer in the blockchain responsible for the security of the oracles, being one of its measures delaying the targets by 1 hour so that it is possible to stop an attacker who takes control of the oracles.

C. Bywise

CDPs and oracles are able to regulate the price of a token based on a fiat currency or asset like gold/silver. Using this widely validated system Bywise can stabilize tokens on its blockchain. For each fiat currency in the world, you can have a corresponding token of the same price.

In this scenario, a trader/broker who wants to use Bywise in his activities can trade and store stable tokens while the user can use Bywise or any other satellite token.

X. ENERGY EFFICIENCY

Blockchains that use POW need a lot of computing power. The transactions require validation and the block needs to be mined through tenders, which requires enormous energy expenditure.

Asics are the equipment with the best speed and energy efficiency when calculating hashes, reaching absurdly high values of hashes per second. As an example we have the Antminer S19 Pro, which reaches 110 TH/s and has 4400 Watts of power, which is equivalent to 25 GH/W.

Even if this equipment improves the energy efficiency of the algorithm, miners are always competing with each other and the difficulty of the contest tends to increase to fix the block time at 10 minutes[1]. Networks with work-proof algorithms are regulated, keeping energy expenditure almost constant as a result.

As chapter III shows, Bywise is able to process many more transactions per block, in addition to using algorithms optimized for speed in the selection of slices. If in the same 10-minute contest the blockchain processes a much higher volume of transactions, the computational cost per transaction will be much lower, which increases energy efficiency.

[1] Bitcoin.org. Bitcoin - block chain. https://developer.bitcoin.org/devguide/block_chain.html. Acessado em outubro de 2020.

[2] Vitalik Buterin. Ethereum white paper: A next generation smart contract and decentralized application platform, 2013.

[3] Electric Coin Co. Zcash basics. https://zcash.readthedocs.io/en/latest/rtd_pages/basics.html. Acessado em outubro de 2020.

[4] Christian Decker and Roger Wattenhofer. Information propagation in the bitcoin network. *IEEE P2P 2013 Proceedings*, 2013.

[5] Evan Duffield and Daniel Diaz. Dash whitepaper. https://github.com/dashpay/docs/raw/master/binary/Dash%20Whitepaper%20-%20V2.pdf, 2014.

[6] Maker Foundation. The maker protocol: Makerdao's multi-collateral dai (mcd) system. https://makerdao.com/pt-BR/whitepaper/. Acessado em fevereiro de 2021.

[7] Bitcoin Github. March 2013 chain fork post-mortem. https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki. Acessado em outubro de 2020.

[8] L.M Goodman. Tezos — a self-amending crypto-ledger white paper. https://tezos.com/static/white_paper-2dc8c02267a8fb86bd67a108199441bf.pdf. Acessado em outubro de 2020.

[9] Dash Core Group. Getting started - merchants. https://docs.dash.org/en/stable/merchants/getting-started.html. Acessado em outubro de 2020.

[10] Monero Research Lab. Monero scalability. https://www.getmonero.org/resources/moneropedia/scalability.html. Acessado em outubro de 2020.

[11] Dr. Sarvesh Mohania and Dr. Shriti Singh. An analysis of cryptocurrency and its challenges. *EPRA International Journal of Multidisciplinary Research*, pages 104–107, 4 2020.

[12] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[13] Tatsuaki Okamoto and Kazuo Ohta. Universal electronic cash. page 324–337, 1991.

[14] N. Popper. *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*. Harper Paperbacks, 2016.

[15] W3 Techs. Usage statistics of php for websites. https://w3techs.com/technologies/details/pl-php. Acessado em outubro de 2020.

[16] Erlend Solberg Thorsrud. Long-term bitcoin scalability. https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2562793/19811_FULLTEXT.pdf, 2018. Acessado em outubro de 2020.

[17] Nicolas van Saberhagen. Cryptonote v 2.0. https://cryptonote.org/whitepaper.pdf, 2013.

[18] VISA. Visanet: o poder de conectar o mundo. https://www.visa.com.br/sobre-a-visa/noticias-visa/nova-sala-de-imprensa/visanet-o-poder-de-conectar-o-mundo.html. Acessado em outubro de 2020.

[19] Nick Webb. A fork in the blockchain: Income tax and the bitcoin/bitcoin cash hard fork. https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1361&context=ncjolt, 2018. Acessado em outubro de 2020.