ZIMBOCASH

Blueprint for a Decentralised Currency in Zimbabwe

www.zimbo.cash

Contents:

WHAT IS ZIMBOCASH?

ZIMBOCASH is a decentralised currency for Zimbabwe. Our broader goal is simple – we want to establish a decentralised currency that is fixed in supply but available to all Zimbabweans. We want to see the economy of Zimbabwe transformed with sound money.

The goal is for trust to be restored in the money and banking system. ZIMBOCASH is based on a decentralised blockchain – a revolutionary technology that enables a fixed supply of money and a reliable payments system.

Only Zimbabweans may join. Each person who registers will get an allocation of ZIMBOCASH. From October 2019 the allocation will be 12 500 but this amount available will halve each 3 months. If members introduce others, they can earn more.

We will launch an initial token based on a decentralised platform. The registration database will be converted into ZIMBOCASH coins transferable with an online wallet. The system will facilitate fast and secure transactions in a decentralised payments system.

In addition to facilitating transfers between account holders, ZIMBOCASH will be **listed on a cryptocurrency exchange**. Each person will only be able to sell ZIMBOCASH on the exchange when they have made six transfers to others. **While we want people to be able to cash-out, our goal is to establish a transactional currency on the ground in Zimbabwe using the latest price as a reference.**

Currencies are established using the *Network Effect*. Each person who joins, adds value to all in the community. Zimbabwe has been crippled by faulty money and the banking system – ZIMBOCASH has the potential to solve these financial issues by fixing the supply of money.

www.zimbo.cash

VISION

Our goal is to use blockchain technology to establish a decentralised currency that is fixed in supply and available to all Zimbabweans. We desire to provide a fast, secure and simple payments platform, listed on reputable exchanges and available for ordinary people to use in day-to-day trade. We want to see the economy of Zimbabwe transformed with sound money.

MISSION

1. To develop a network of Zimbabweans who own and trade ZIMBOCASH in day-to-day transactions.

2. To establish a decentralised currency token and wallet system using the latest and best cryptocurrency technology available.

3. To obtain a free-floating and liquid market value for ZIMBOCASH on reputable exchanges with substantial buyers and sellers.

4. To create global demand and interest for the first on-the-ground cryptocurrency system.

CORE VALUES

Sound Money

We believe in sound money – that money should be limited in supply. We believe that people should be able to trust the money and the financial institutions that they use. We believe that people should be able to securely store their money in various wallet applications without fear of expropriation or theft. We believe that money printing is extremely destructive and destroys the fabric of a nation. We believe that Sound Money

is a foundation for developing an economy and that only in this way will there be sustainable savings, trade and wealth creation on a national scale.

Relationships

We believe that our services can only be provided through local and international partnerships which are necessary for gaining access to resources, services, and communities outside our reach. We believe in partnering with stakeholders including local authorities and networks to achieve the longer term goal. We believe in consensus-based decision making but also in appropriate delegation of authority with clear decision-making limits and responsibilities, to senior and line management.

Long Term Thinking

We believe in planning for the long term. We would rather see long term value creation based on the development of a sustainable services, rather than short term benefits.

Decentralisation

We believe in empowering individuals to own and control their ZIMBOCASH. As a movement ZIMBOCASH respects regulators and competitors. However, we value individuals and communities and want to see ZIMBOCASH impact Zimbabwean individuals living on the ground in Zimbabwe and around the world.

Service and Social Responsibility

We believe that the foundation of our business is serving others by identifying and meeting needs, solving problems, service-leadership and value-oriented approach to our business.

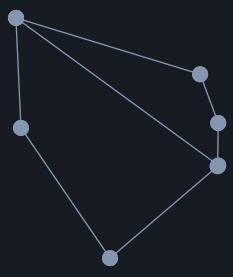
A ZIMBOCASH MOVEMENT

Money printing is the cause of fuel shortages and empty stores in Zimbabwe. When money is created on a grand scale by central banks, it robs ordinary people of value and ultimately undermines the productive capacity of a nation.

With the current landscape, Zimbabweans cannot practically remit funds out of the country. However, with ZIMBOCASH listed on an international cryptocurrency exchange, you will be able to make payments to anyone globally and easily be able to convert it into well-known cryptocurrencies.

The best part of ZIMBOCASH is that once the blockchain has been launched, there can be no more money created – in other words, the supply of ZIMBOCASH will be fixed from this date onwards.

With the severe problems in the money and banking system, Zimbabwe is one of the few countries in the world where you will be able to implement an on-the-ground cryptocurrency – ZIMBOCASH has the ability to fulfil the dream of peer-to-peer payments on a mass-scale.



EXISTING CHALLENGES

ZIMBABWE'S CHALLENGES

Zimbabwe has not been able to maintain a stable fiat currency for over two decades. As of 2019 – ten years after the country's first hyperinflation – the country has been experiencing a second great inflation period with Zimbabwe dollars. Stores are emptying and fuel supply has been intermittent. There is diminishing trust in the current monetary environment. With the currency problems, the banking system is effectively insolvent. People and businesses face extreme difficulties in making international payments. There is capital flight resulting in a money printing spiral. Ordinary people on the ground have very little money.

Since the last hyperinflation, the population has traded with US dollars, British Pounds, South African Rands and other currencies on the street and lately, the country uses Zimbabwe Dollars. With the multicurrency regime being scrapped, foreign currency is in short supply. There are queues at the fuel stations and shortages in the stores. Prices are rising on a daily basis. Money printing is leaving its devastating mark on the country.

CRYPTOCURRENCY'S CHALLENGES

The established cryptocurrencies such as Bitcoin, Ethereum and Monero are already playing a very small role in Zimbabwe but have several weaknesses. They will not be traded on the street as the primary medium of exchange any time soon. Bitcoin introduced revolutionary ideas around a decentralised currency and banking system – it has several strengths but simultaneously several weaknesses that we can learn from.

Major Strengths of bitcoin:

1. Fixed money supply – There is a maximum total supply of 21 million bitcoins. No more bitcoins can be created above this threshold. The public has a guarantee that the money supply is, in fact, limited. This provides a good platform for bitcoin as a currency.

2. Fast – Transaction speeds have been, until recently, relatively fast. This has enabled bitcoin to act as a competitor to the transactional banking system.

3. Decentralised and Open – Anyone can transact in bitcoin without fear of censorship or coercion. There is no centralised party who controls the system. It is a fully open banking system available to all people.

4. Borderless – Bitcoin can be transferred to anyone around the world with no restrictions, exchange control or additional fees.

5. Censorship resistant – the proof of work algorithm makes it extremely difficult for the blockchain to ever be changed. Combined with decentralisation, bitcoin as a banking system is very difficult for governments to control or restrict.

However, it has weaknesses which make it inadequate as a transactional currency for people living on the ground in a country. These include:

Major Weaknesses to learn from:

1. Scalability – Bitcoin can only handle a few transactions each second – far below what would be required on a global or even local scale. In December 2017, the system reached its transacting limit and over 220 000 transactions backlogged in the queue. Miners started to charge high transactions fees for people to jump the queue. This scalability problem has not been solved to any major degree and still is a major weakness on bitcoin as a banking system.

2. Substantial size of database – the bitcoin database can only increase in size and after 10 years is over 210 gigabytes. The cost of carrying this large database by the thousands of miners translates into increased transaction costs and in reduced decentralisation.

3. Very costly to run – Proof of Work has been exceptionally powerful in establishing an immutable ledger. However, the processing power required is prohibitive and translates into transaction costs.

4. Limited security– the bitcoin database keeps a record of all payments in and through all accounts. If anyone were to find out what account numbers you used, they would have a complete record of all your transactions and balances.

5. Long private keys – whenever you receive bitcoins, you get a new private key which is long and complex. This makes it cumbersome to receive and record and ultimately reduces the quality of bitcoin as a banking solution.

6. Centralised holdings – According to BitInfoCharts, 87% of all mined bitcoin is held by just 0.5% of the wallets. This means that the price of bitcoin is very exposed to a few individuals/exchanges.

Without addressing these weaknesses bitcoin will struggle to become a major on-the-ground transactional currency. However, bitcoin has pioneered the technological breakthroughs with decentralised currency and banking. ZIMBOCASH aims to keep the benefits of the bitcoin system and amend the protocol such that the weaknesses are diminished/ eliminated. The final goal is to develop a decentralised currency system.

WHAT IS DIFFERENT ABOUT ZIMBOCASH?

- **ONLY ZIMBABWEANS**
  Zimbabweans both local and international can join. Everyone who registers will be given 12 500 ZIMBOCASH with a further 1 250 ZIMBOCASH for referrals and 12 ZIMBOCASH for each unique click you receive on your personal ZIMBOCASH link.

- **NO MORE MONEY PRINTING**
  Once the blockchain has been launched, there will be no more ZIMBOCASH created. The total money supply will be fixed.

- **SCALABLE**
  The ZIMBOCASH blockchain is flexible and extremely scalable.

- **WALLET PLATFORM**
  ZIMBOCASH provides the latest in financial technology with mobile wallet functionality.

- **INTERNATIONAL TRANSFERS**
  ZIMBOCASH is borderless with a decentralised node-base facilitating transfers to anyone with no red-tape or exchange control.

- **INTERNATIONAL EXCHANGES**
  Once the ZIMBOCASH currency has been established, we aim to list it on a cryptocurrency exchange for interoperability with the other global cryptocurrencies.

ZIMBOCASH
Uniquely Zimbabwean, Globally Recognised

PHASE 1: ZIMBOCASH REGISTRATION PROCESS

The ZIMBOCASH blockchain will be launched in four phases. The first phase is a registration phase – which itself will have eight stages with the number of ZIMBOCASH coins allocated halving with each stage. The goal is to get it into the hands of as many people as possible to create a trading network.

1. All Zimbabweans – both locally and abroad – can join the community and register for their ZIMBOCASH at *https://zimbo.cash*.

2. Basic detail will be required in the registration form including:
    a. Email address
    b. Either a Zimbabwean cell phone number or a Zimbabwean ID number
    c. Password (to access your ZIMBOCASH when these are issued)
    d. Email address of the person referring you (so we can give them additional ZIMBOCASH)

3. Allocation of ZIMBOCASH:
    a. Each ZIMBOCASH community member will be issued ZIMBOCASH when they join – the amount is 12 500 ZIMBOCASH in the first stage but will reduce with each stage.
    b. In addition, each community member will receive a further 1250 ZIMBOCASH for every person who registers using their email address as a reference.
    c. On registration, each person will also receive a unique ZIMBOCASH link to share via WhatsApp, email or social media, and will receive 12 ZIMBOCASH for each unique person who clicks on that link.

PHASE 2: ZIMBOCASH LAUNCH

The total number of ZIMBOCASH to be allocated will be based on the total number of registrations. Once the total number of registrations has been established, the total number of ZIMBOCASH will be finalised, taking into account a further 15% allocation each to funders and founders.

On allocation, we'll establish a testnet system with the goal of facilitating trade in ZIMBOCASH with simplicity of use and secure functionality. This will be based on an appropriately secure decentralised platform using the latest in cryptographic delegated proof of stake technology.

PHASE 3: ZIMBOCASH EXCHANGE

Once the initial beta system has been launched, ZIMBOCASH will be listed on a cryptocurrency exchange and the initial trading established. A float will be established and international buyers will then be able to purchase ZIMBOCASH at a price established by supply and demand.

ZIMBOCASH account holders may only sell their ZIMBOCASH on the exchange once they have made transfers to others – each person must make six transactions per batch. Account holders will be allowed to sell 10% of their ZIMBOCASH per batch on the exchange. This only applies to the ZIMBOCASH that has been allocated when people sign-up. People who purchase ZIMBOCASH will be able to sell their ZIMBOCASH with no restrictions.

The purpose of ZIMBOCASH is to become a tradeable currency. While it is important to give people the opportunity to cash out, there should be a reward for those who are actively transacting.

PHASE 4: ZIMBOCASH BLOCKCHAIN INFRASTRUCTURE

The ZIMBOCASH blockchain will be based on the latest cryptographically secure technology at the time of launch. Our goal is to provide a cryptographically secure, decentralised and scalable token system. Our thinking at this stage is to adopt a fork of a mimble-wimble architecture, which provides for a snapshot of the balances on each wallet address at a point in time rather than a list of aggregate transactions. This approach provides a fast, scalable and low-cost transaction system, with appropriate security, decentralisation and fixed-currency base.

Rather than adopt an inflation model to pay for block processing fees, the total number of ZIMBOCASH coins will be fixed. The system provides for a nominal transaction fee on all transfers paid out by the receiver subject to a nominal limit.

ZIMBOCASH PARTNERSHIP WITH ZIMBOPAY

The ZIMBOCASH project is based on a partnership between the ZIMBOCASH founders and ZIMBOPAY.

ZIMBOPAY is a separate company established with the goal to provide the full wallet and payment functionality required for ZIMBOCASH.

Founders and funders will participate in the blockchain by acquiring 15% each in the coins issued and in participating in a portion of the transaction fees. The incentive is to first establish a service in Zimbabwe that transforms the economy. Then it is to be profitable in the long run. The goal is to develop an ecosystem that all parties can participate in.

TECHNICAL DETAILS

ZIMBOCASH's goal is to be a decentralised currency and payments platform. Mimble Wimble technology provides the technical solution to these needs.

Mimble Wimble is flexible enough is to establish a blockchain that will scale effectively and be able to facilitate a high volume of small, day-to-day payments – i.e. to reflect what a decentralised payments system would look like in a blockchain.

In short, the blockchain needs to be able to handle the volume and scale of micro-payments as required on a large scale, while simultaneously providing all the security and decentralisation that are available with existing cryptocurrencies.

HOW DOES MIMBLE WIMBLE WORK?

Mimble Wimble technology is an approach to blockchain technology that keeps only the latest balances for each account – i.e. a snapshot in time – on decentralised nodes. These balances are updated as transactions are made in a similar sense to how a distributed server synchronises with other computers. This approach contrasts with the bitcoin blockchain which keeps a full record of all historic transactions from its inception to the present.

The Mimble Wimble concept provides a much lower data load and is vastly cheaper, faster and simple to update – enabling even small computers access to the system. The consensus protocol will further use three criteria for nodes to be selected for transactions:

- synchronisation speed– only nodes that can synchronise quickly, while maintaining a balance of ZIMBOCASH can operate the server.

- length of time as a node – nodes that have been facilitating transactions for longer will be allocated more transactions.

- minimum balance – each stake needs to maintain a minimum balance of ZIMBOCASH to facilitate transactions.

In the explanation below, we have tried to avoid cryptocurrency terms which are often complex and misunderstood and have rather used terminology that is in use with current computer networks. A blockchain is a database that is held on many computers at the same time and is updated in a batch process on a regular basis. The revolutionary idea of a blockchain is that you can update these computers without a central server.

The minimum data that is required for a currency server would be the latest balances of each account on the database. Mimble Wimble technology keeps these records on the distributed computers only.

WHY MIMBLE WIMBLE?

The initial promise of bitcoin as a currency and payments platform has not been fully realised – while bitcoin is a "reserve currency" of sorts, it has substantial weaknesses as a transactional currency.

None of the follow-up currencies have fully addressed the needs of an on-the-ground money and there has been insufficient development of

decentralised banking and currency alternatives. Interest has, by and large, moved on to other blockchain applications.

Bitcoin has several strengths but simultaneously several weaknesses. These are discussed in detail on page 7 above. Because of these weaknesses, it is unlikely that bitcoin will be used as a transactional currency any time soon.

Any cryptocurrency that aims to provide a fixed-based currency and a decentralised payments system will need to solve these problems.

Strengths of bitcoin

1. Fixed money supply
2. Fast historic transaction speeds
3. Decentralised
4. Open
5. Borderless
6. Censorship resistant
7. Widely accepted

Weaknesses of bitcoin

1. Not Scalable
2. Burgeoning size of total database
3. Very costly algorithm
4. Limited security of data
5. Multiple long private keys
6. Very centralised holdings
7. User-unfriendly wallets

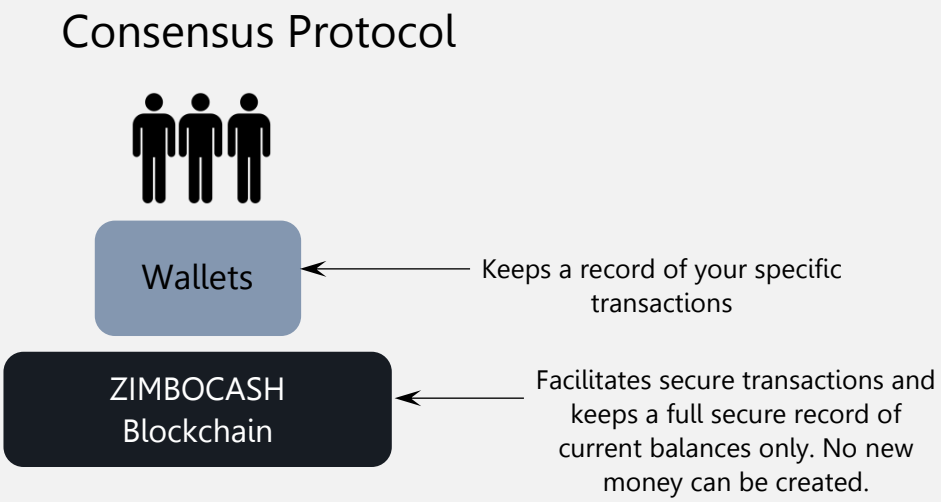
Mimble Wimble is a technology that addresses these weaknesses while maintaining the strengths pioneered by bitcoin.

HOW DOES MIMBLE WIMBLE WORK?

Most blockchains keep a record of all transactions since inception. While this information can be useful, it has a cost since every computer on the network must keep a full synchronised copy of the database. In bitcoin's case, this blockchain is cumbersome and is over 210 gigabytes in size.

However, maintaining a full copy of transaction history on every node isn't how a centralised payments system typically works. In the example of a national payments system, there are usually multiple levels – it starts with a reserve bank which keeps a record of the base money supply. People who make payments, however, can only deal with retail banks via their various wallets and bank account interfaces (for example mobile money, an online banking profile or debit card payments network). It is the wallet providers and retail banks that will keep a record of the transaction history.

Mimble Wimble uses a similar approach however it does so without the need for retail banks or the reserve bank. The ZIMBOCASH blockchain establishes the total supply of ZIMBOCASH – no more ZIMBOCASH can be created over time. The blockchain will keep a list of balances for each account and ensure that the total supply of ZIMBOCASH cannot be changed.



This makes the database much easier for people to hold and allows for a much wider distribution of decentralised nodes.

If someone wants to access their ZIMBOCASH balances and make transactions, they can do so by using a wallet that connects to the ZIMBOCASH blockchain.

These wallets will be able to retain a transaction history of each of your transactions. Special transaction history nodes will keep a full copy of the transaction history of the blockchain and will be able to charge a fee to those needing transaction records for a broader spectrum of transactions.

However, the base requirement of decentralised nodes on the blockchain will be to maintain a simple general ledger balance of the blockchain while validating transactions against those balances.

THE SNAPSHOT LEDGER

The snapshot ledger will include the following fields at a minimum (additional information will relating to any nodes will be kept by the relevant nodes).

Account Number	Balance	Current month & year	Public Key	Transaction Level

1. **Account Number**

   The account number is a unique identifier for the individuals who own the account.

2. **Balance**

   The balance indicates the latest account balance. It is a snapshot at a point in time.

3. **Current month and year**

   This is used as the SALT for the hashing of the account number.

4. **Public Key**

   Each account holder is issued with a public-private key set. This field captures the public key.

5. **Transaction Level**

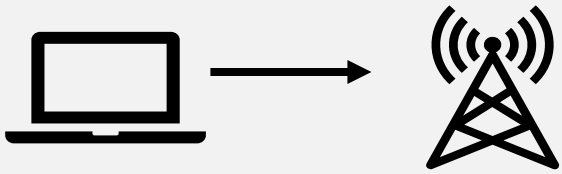
   This relates to the number of transactions that are performed.

NODE PROCESSING

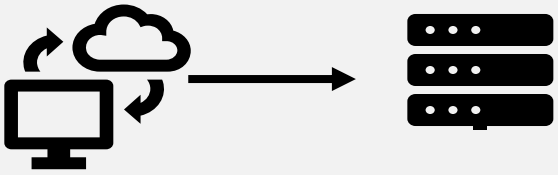
In a decentralised blockchain, nodes operate on a combined basis as a server. With a server, there is a RAM-function (i.e. short-term memory for transactions waiting to be processed), a cpu-function (i.e. processing), and a hard-drive-function (i.e. storage of the database).

The decentralised nodes therefore need to operate each of these processes, however, because each node is decentralised, there is an additional function required – which is a routing-function. In other words, the nodes need to facilitate communication between each other such that the packets of data

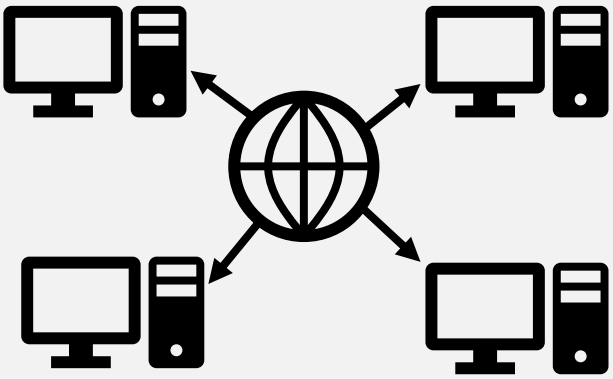
are sent and received by all the nodes and the final database is synchronised between the nodes appropriately.



Transaction broadcast to the network



Transaction received by nodes and queued for processing in a MemPool



Transactions batch processed on the SnapShot database.

Nodes prepare a hash of the file and send both a clean and signed (encrypted) version. Consensus is achieved following 51% node agreement as evidenced by encrypted signatures

ROUTING AND DECENTRALISED CONSENSUS

The system works easily when there are a few nodes synchronising. However, as more nodes get added to the system, the synchronisation becomes increasingly difficult to facilitate and requires more and more time in-between each batch update.

This is similar to the idea of a crowd of people. If there are many people in the crowd, then relaying a message to all unique participants in the crowd (especially when there are many others talking in the crowd) becomes harder to synchronise and manage.

This is why the SnapShot database is a preferable database option – it is simple to confirm, light in data load and easy to synchronise between nodes. However, it is inevitable that when the number of nodes synchronising increases to a certain level, it will slow down synchronisation speeds.

SCALABILITY – SPLITTING THE BLOCKCHAIN

As synchronisation speeds decline, the system is faced with a challenge – either it can continue to accept new nodes on the network and require the additional processing power to synchronise the SnapShot database with the additional nodes – or it can split the database processing requirements between the nodes. This can only be performed because a record of balances is being kept – half of the balances are moved to one database and the other half to the other database. This is known as Sharding.

When the speed of synchronisation slows beyond 30 seconds, the database will be split into two blockchain databases, divided between available Database Nodes. Because the database is primarily a record of final balances, it is easy to split equally in two. This is not the case with traditional blockchains which require that the full transaction record be kept by all parties.

In other words, when the processing demands of the ZIMBOCASH transactions get too large for one single decentralised database, the blockchain is split with transactions on the system "clearing" between different ZIMBOCASH blockchains. This allows for scalability and speed while retaining the key aspect of decentralisation.

A person who transfers ZIMBOCASH to another person on the same database will use the existing blockchain. However, if a person wishes to transfer money to someone who has an account on another side chain, the two database systems will need to "clear" between each other. The final net total number of ZIMBOCASH remains fixed in supply.

LIMITED SUPPLY: FEE ALLOCATION BASED ON TRANSACTIONS

In a typical blockchain model, tokens are created on an on-going basis to pay for the node processing power. However, with the ZIMBOCASH system, the number of ZIMBOCASH coins are fixed in supply, on launch of the blockchain. There are no new ZIMBOCASH created going forward from this date.

The node fees are funded by a small transaction charge paid for by the person who receives ZIMBOCASH in any transaction. This is a fixed percentage of the transaction of 0.5%. This approach provides for a direct correlation between transaction activity and node reward.

Separation of Processing Services Required

With a direct transaction fee, the specific services required for fast decentralised node activity can be separated and allocated based on this fee. This includes a separation of three specific services: Broadcasting the transaction, Processing the Transaction, Validating the Transaction and Storing the Database. The following services would be required:

1. Validate the hash of the previous database for each of the nodes that signed off the balance
2. Receipt of a transaction request signed with a private key and broadcasting to other nodes for processing
3. Validation of transaction authenticity against the public key of that account number and transaction record by other nodes
4. Update of batch information to the decentralised database/ synchronisation.
5. Storing the latest database by Database Nodes
6. Hashing the latest database and signing it with a unique private key
7. Clearing between database nodes that have separated into a side-chain (for split databases)

Reduced Maintenance of Database Information

The hashed result of the database is then compared with each node – each node confirms their final hash and signs the hash with their private key. in the network. Consensus is achieved when 51% of the nodes in the network agree with the result.

PAYMENT CONFIRMATIONS – FULL TRANSACTION NODES

What the snapshot database does not provide, is a record of historic transactions. This becomes problematic because one of the important functions of a banking system (and therefore a cryptocurrency system that provides banking services) is that it can provide a record of who transferred to whom.

This is solved by enabling Transaction Nodes who retain a combined database of all transactions on the ZIMBOCASH system – i.e. a record of the snapshot databases at each point in time, together with the tree of the

hashes (so that it can be proved cryptographically that the historic transactions took place).

These Transaction Nodes will require much more data storage capacity – and have much more reliable and fast network connections. They will be compensated for this role and function because they will be able to charge an additional fee for people who are looking for a proof of payment.

This approach provides a unique double benefit – it allows the minimum required data possible to ensure that the blockchain is as decentralised and censorship resistance as possible, while simultaneously providing a transaction record that can be cryptographically traced to the latest blockchain (through the use of a Merkle Tree). It also ensures that the full cost of retaining the full transaction record is applied only to those who will pay for it.

In other words, the full transaction record does not need to sit on all the nodes of the blockchain – but only on select Transaction Nodes who can then prove cryptographically that the transactions are valid.

SECURITY

The fact that most nodes will retain only a SnapShot Database allows additional security to be added to the system –

1. Encrypted Public Key Infrastructure: In contrast to Bitcoin's transaction record – which requires a private-public key pair to be generated for every historic transaction, ZIMBOCASH requires only one private-public key pair, to access the account and to validate transaction requests on the account.

A transaction request must be signed by a private key for each account. Each account can make multiple payments using the same public-private key pair.

The default setting for this would be for the public-private key pair to be reissued every two months, however, the account holder would be able to change the key pair as and when s/he needs to, or delay the change for as long as s/he needs to.

To change the public-private key, a new key pair is generated and encrypted with the old public key. The account holder accepts this new key pair by using the old private key to unencrypt the old key pair and sends the public key back to the account as proof of signature.

2. Each account number changes regularly. The account numbers are a hash that changes but has fixed inputs. It is a concatenation of the email address, the password and the month and year of the last transaction (which field will be included in the database for ease of reference). This allows the account holder to easily access their account with information that they retain, however outsiders can't trace the changing account number without access to the underlying detail.

   The date of the last transaction is retained on the public database as a "salt" field, which makes the hash of the result more difficult to crack.

   This is contrasted with bitcoin – if you need someone to pay you in bitcoin, you need to share a bitcoin account number with them. This number has a publicly available record of all historic transactions against that account which is available for anyone to inspect – characteristics which would not be suitable for an on-the-ground payment system.

With a changing account number, it becomes difficult for the general public to keep a track of general balances and provides a level of privacy. In addition, historic transactions become difficult to trace.

3. The historic balance of ZIMBOCASH under each account is encrypted using the public key of each transaction.

   The private key is used to decrypt the balance of the account, if the account holder wishes to send an amount.

   If the account *receives* any ZIMBOCASH, the system will encrypt that amount, together with the account number of the person making payment – which will combined be encrypted with account holders' public key. Each payment receipt is kept as a separate record for the longer of one month and the time it takes for the account holder to log into his/her account again. This provides a verifiable transaction record for a period of one month on the snapshot database.

   When an account holder logs onto his account, he can accept the combined balance, which is confirmed by the private key.

   This process ensures that no-one can see what balances are held under any account – both the amount of ZIMBOCASH in the account and the amount of the transaction are encrypted.

4. The system provides for the ability to have multiple-signature accounts – for instance in the scenario where a company needs to have appropriate controls over its assets, the specific account number could have multiple account passwords and private keys to ensure that no single person has full access to the ZIMBOCASH coins.

5. Time-Release: Because payments on the database are binding once they have been made, it is beneficial to some parties to have a time-release function. Payments would require sign-off twice – both at the beginning of a period and at the end of a set period. For example, if an account holder wanted a one-week restriction on that account, it could specify that the ZIMBOCASH associated with that account could only be released with a person who has the private key, at the beginning of the week and at the end of the week. This provides some protection against opportunists wishing to steal the ZIMBOCASH.

   For further security, the Time Release function could provide for a multiple signature process – one party signs at the beginning of the Time Release, and another party signs at the end of the Time Release.

ZIMBOCASH PROJECT PLAN

Phase	Milestone
Phase 1	Sign-up Process
Phase 2	Initial Testnet System
Phase 3	Launch on exchange
Phase 4	Launch blockchain

FINAL WORD

ZIMBOCASH has the power to be the solution to Zimbabwe's money problems and to be a force of real wealth creation for an entire nation. We are excited to be creating the future and, in the process, to restore to Zimbabweans what has been lost over the last twenty years.

RESTORING WEALTH

Any Zimbabwean can register. An allocation of ZIMBOCASH is given to each person who register. Once a market price is established for ZIMBOCASH, you will be able to buy and sell goods and services with a reference to the market price.

RESTORING TRUST

ZIMBOCASH is a trusted decentralised fixed-base currency and banking system. It is based on the best practice, next generation, cryptocurrency technology. No longer is the Zimbabwe money subject to devaluation because of money printing. Zimbabweans have freedom to transfer ZIMBOCASH to others locally and internationally.

RESTORING INTERNATIONAL PAYMENTS

With the international exchange, ZIMBOCASH becomes a means for making international payments – with conversion into well-known cryptocurrencies. No exchange control applies to ZIMBOCASH holders. However, ZIMBOCASH holders will need to first make the requisite transfers to others on the system to enable their ZIMBOCASH to be released for sale on the exchange.

RESTORING ZIMBABWEAN PRIDE

ZIMBOCASH is a uniquely Zimbabwean brand. ZIMBOCASH is only available to Zimbabweans. We believe ZIMBOCASH has the ability to lead a reformation in the country that we love. ZIMBOCASH restores the Zimbabwean sense of pride.

RESTORING ZIMBABWE IN GLOBAL LEADERSHIP

No other country in the world can successfully implement a localised cryptocurrency. The ZIMBOCASH cryptocurrency is about to catapult Zimbabwe to a global leader in cryptocurrency banking and finance.

Be a part of the movement.

ZIMBOCASH

www.zimbo.cash

DISCLAIMER

This *Blueprint for a Decentralised Currency in Zimbabwe* has been prepared for information purposes only. If you wish to register for ZIMBOCASH, you will be required to agree to the Terms and Conditions and Privacy Policy, which will regulate the relationship between you and ZIMBOCASH. This document is not part of those terms.

This presentation may contain information proprietary to ZIMBOCASH and accordingly may not be reproduced, or disseminated in whole or in part without the ZIMBOCASH team's consent. This presentation may contain information which has not been independently verified by ZIMBOCASH.

Neither the ZIMBOPAY nor the ZIMBOCASH teams provide any guarantee to the accuracy of or the conclusions reached. ZIMBOPAY and ZIMBOCASH do not make and expressly disclaim all representations and warranties, express, implied, statutory or otherwise, whatsoever, including, but not limited to: warranties of fitness for a particular purpose, suitability, usage, title or noninfringement; that the contents are free from error; and that such contents will not infringe third-party rights. Any liability of whatsoever nature and howsoever arising on the part of ZIMBOCASH or ZIMBOPAY, their directors, officers, employees and agents relating to the contents is hereby expressly disclaimed. This presentation is intended for information purposes only and does not represent a commitment, proposal, recommendation, offer open for acceptance or agreement to enter into a transaction. This document is subject to copyright.

2/10/2019