ViptoCoin
Securing the Future

Introduction

Are our private lives really “private” anymore? With our personal Identification, the most sensitive information about ourselves, being readily accessed by multiple corporations and online entities, often without our knowledge, it is truly difficult to perceive as such. Your identification is largely entwined with your privacy and should not be disclosed unless it is absolutely necessary. Cryptocurrency eliminates the need for identification from both parties, ensuring true security.

Since the official revelation of blockchain technology: a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system, which took place in 2008, cryptocurrency has become a household name across the world, decorating multiple forums and media.

Although, it has been challenged with minor setbacks in public actualization, such as the December 2017 fever pitch, cryptocurrencies have continued to attract the public and investors alike. Today, some cryptocurrencies have grown by more than 200 percent in value, with some set to exceed the 1000th percentiles.

According to recent studies done by Statista, 35 million parties participated in the cryptocurrency market in 2018 and this number has increased to a staggering 101 million in 2020. This represents a growth of 188 percent. While the global use of cryptocurrency has yet to achieve mainstream acceptance, financial projections indicate that over a 100 thousand merchants currently accept and trade virtual currencies as a formal mode of payment.

An Overview of ViptoCoin

Blockchain technology fulfills multiple purposes such as data storage, payments and operations, with widespread creative utility. We believe that developments in blockchain technology will play an important role as a determinant of the future, as the features of transparency and traceability that blockchain technology is derived from are highly sought after and anticipated to build trust.

ViptoCoin is a fully open-source, community-based cryptocurrency project that was derived from a blockchain built entirely on the NIST5 algorithm, from the ground-up. ViptoCoin is therefore geared to ensure swift and secure transactions at nearly zero-transaction cost.

The blockchain on which ViptoCoin was developed and initialized on, is not only bountiful with features but also stable and reliable - making it an ideal platform for developers to innovate and redefine as

ViptoCoin adopts more mainstream usage.

There are currently 186 million premined ViptoCoins in existence: this is mined purely from the genesis block and the first 2 blocks, which seek to confirm the genuineness of the genesis block.

As of now, ViptoCoin is deemed a fully-operational public cryptocurrency. However, it is an ongoing development project and is subject to further review, innovation, and improvements in every aspect.

➢ **Mission**

To provide communities with an eco-friendly way of carrying out fast and secure online transactions at a low cost by leveraging blockchain technology.

➢ **Attributes**

- Fast and Secure Transactions.
- Eco-friendliness.
- Efficient Frameworks.
- Decentralized and distributed.

➢ **Investor Benefits**

An investment in ViptoCoin, is an investment in an eco-friendly, economically decentralized future. Should you invest in ViptoCoin, you automatically become an owner of the cryptocurrency, ViptoCoin and the entire infrastructure that exists behind its development project.

Methodology and Approach

ViptoCoin is a community-centric cryptocurrency project that aims to create a future-proof environment powered by transparency, autonomy and empowerment. ViptoCoin, as a cryptocurrency project, is backed by an entire community of like-minded and dedicated individuals, whose shared goals include the eventual realization of the aforementioned vision.

Technology Behind the Project

The Algorithm

Security is the primary cornerstone of ViptoCoin. It was built from scratch on the NIST5 algorithm, which has a proven track-record on security implementations. The NIST5 algorithm was developed by pairing the best traits of the five finalist algorithms of SHA-3. These features were acclaimed by the National Institute of Standards and Technology of America. In terms of functionality, the NIST5 algorithm, as applied in ViptoCoin, perpetually chooses the most beneficial characteristics of each component algorithm in order to deliver maximum output, in performance, security and efficiency.

These five component algorithms of NIST5 include:

1. BLAKE
2. Grøstl
3. JH
4. Keccak
5. Skein

Algorithm	Domain Extender	Underlying Primitive	Primitive Size	Hash Size	Security			
					Coll	Pre	2nd Pre	Indiff
BLAKE	HAIFA	Block Cipher	k=512 b=512	224 256	112 128	224 256	224 256	128 128
			k=1024 b=1024	384 512	192 256	384 512	384 512	256 256
Grøstl	Grøstl	A pair of permutations	512 512	224 256	112 128	224 256	$256 - \log^2 L$	128 128
			1024 1024	384 512	192 256	384 512	$512 - \log^2 L$	256 256
JH	JH	Permutations	1024	224 256 384 512	112 128 192 256	224 256 256 256	224 256 256 256	256 256 256 256
Keccak	Sponge	Permutations	1600	224 256 384 512	112 128 192 256	224 256 384 512	224 256 384 512	224 256 384 512
Skein	UBI	Tweakable Block Cipher	k=512 b=512 t=128	224 256 384 512	112 128 192 256	224 256 384 512	224 256 384 512	256 256 256 256
SHA-2[6]	MD	Block Cipher	k=512 b=256	224 256	112 128	224 256	$256 - \log^2 L$	1
			k=1024 b=512	384 512	192 256	384 512	$512 - \log^2 L$	1

Algorithm	Best Attack	Security Margin	Work	Depth of Analysis
BLAKE	Semi-free-start near collision	70%	Practical	High
Grøstl	Semi-free-start collision	40%	Impractical	Very High[8]
JH	Semi-free-start near collision	38%	Impractical	Low
Keccak	Near collision	79%	Practical	Medium
Skein	Semi-free-start near collision	56%	Impractical	High[8]
SHA-2[6]	Collission	62%	Practical	Medium

** NIST Competition Summary http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7896.pdf
** Handbook of Digital Currency Bitcoin Innovation, Financial Instruments and Big Data.pdf

Properties of the Blockchain

The NIST5 is a hash algorithm with a heavy core that can be mined using consumer-grade hardware such as entry-level CPUs and GPUs. The blockchain of ViptoCoin uses a customized version of the NIST5 algorithm, and its properties are as follows:

Maximum Supply	786,000,000
Pre-mined	186,000,000 (Aprox. 23.66%)
Block Size	10 MB
Block Time	60 Seconds
Retarget	Every Block
Consensus	Proof-of-work (PoW)
Transactions per Second	~ 800
Fee	0.00001 VCC

- ***Pre-mined VCC***

  A total of 186 million, which accumulates to approximately 23.66% of ViptoCoin, were pre-mined using Proof-of-Work (POW) mining.

  The distribution and usage of this subset of funds will be allocated to a number of purposes, including but not limited to:

  - Funding further development projects (as specified on our roadmap).
  - Maintenance of platform security.
  - Improvement of the platform's usability.
  - Application to new exchanges.

- ***Fast Payments***

  ViptoCoin (VCC) transactions occur speedily fast - making near-instantaneous transactions. Once the transaction is confirmed in the blockchain, the received amount becomes available for use. This confirmation process takes no longer than a few minutes.

- ***Environment Conscious: Conserving without Compromise***

  The NIST5 algorithm relies on significantly less energy to operate when compared to its counterparts. The conservative aspects of NIST5 have earned the algorithm a solid reputation as a sustainable option for the deployment of systems that are based on blockchains, for it conserves resources without compromising the security of members on the network.

Product Catalogue

The current catalogue of ViptoCoin products include the following applications:

1. Desktop Wallets (Mac OS, Windows, Linux)
2. Mobile Wallets (Android & iOS)
3. Web Wallet
4. Merchant Applications
5. Plugins for eCommerce Applications
6. Centralized Online Payment Gateway
7. Merchant Desktop Software
8. Merchant Mobile Applications

Each product from the ViptoCoin lineup is carefully crafted to enhance the experience of potential users.

The future development of wallets, applications and software are driven by the evolving needs of the community, as well as the availability of utilities to address them. Each product comes with an integrated framework for user support. This framework is comprised of user guides and live support from the ViptoCoin community.

Available Services on ViptoCoin Products and Platforms

The following services will be available on all products and platforms offered by ViptoCoin:

1. Master Nodes
2. Web Wallet
3. Integrated Merchant & User Support
4. PayVipto
5. Atomic Swaps

➢ ***Master Node: Development and Implementation***

The development and implementation of the Master Node is a pivotal element of the development cycle of ViptoCoin, and it provides an array of benefits, including but not limited to the following:

1. Faster Transactions on the ViptoCoin Network.
2. Improved privacy of transactions.
3. Enhanced overall health and stability of the ViptoCoin network.
4. Seamless upgrades to the Decentralization of the ViptoCoin Ecosystem.

The members of the ViptoCoin community can simply initiate and run a Master Node by contacting the core development team, and getting the required Node specifications.

Note: The Development of Master Nodes is currently in progress on the ViptoCoin network. The most recent version of our roadmap provides an insight on target release dates.

➢ ***Web Wallet***

ViptoCoin's Web Wallet offers all the functions of the desktop or mobile version, without the need to install it anywhere. The ViptoCoin Web Wallet is a complete online suite that provides users with a fully functional cryptocurrency wallet, on their preferred web browser.

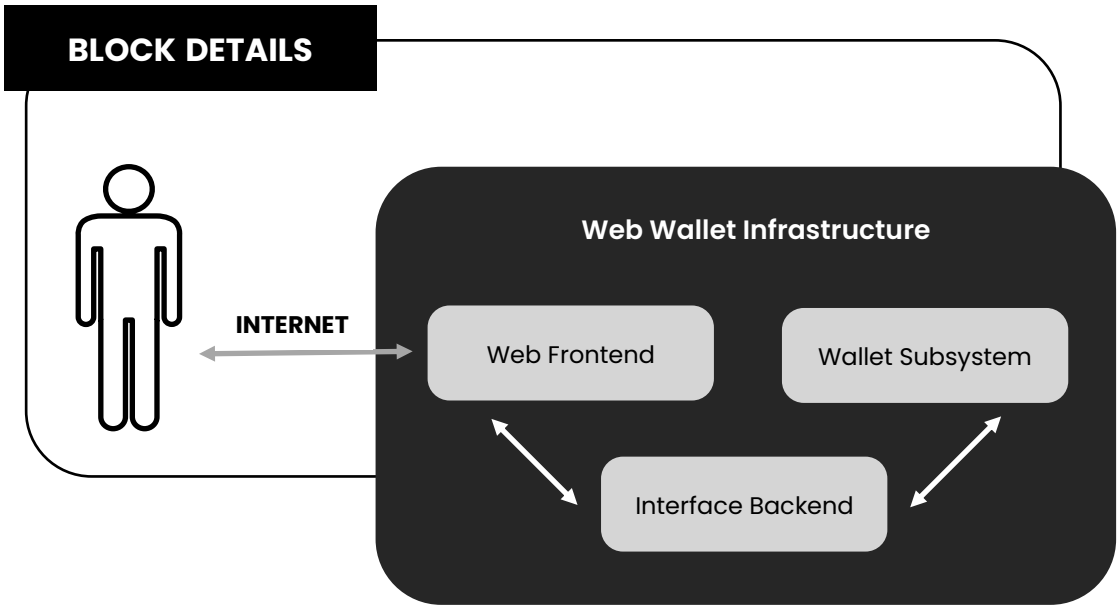
The building blocks of the Web Wallet are as follows:

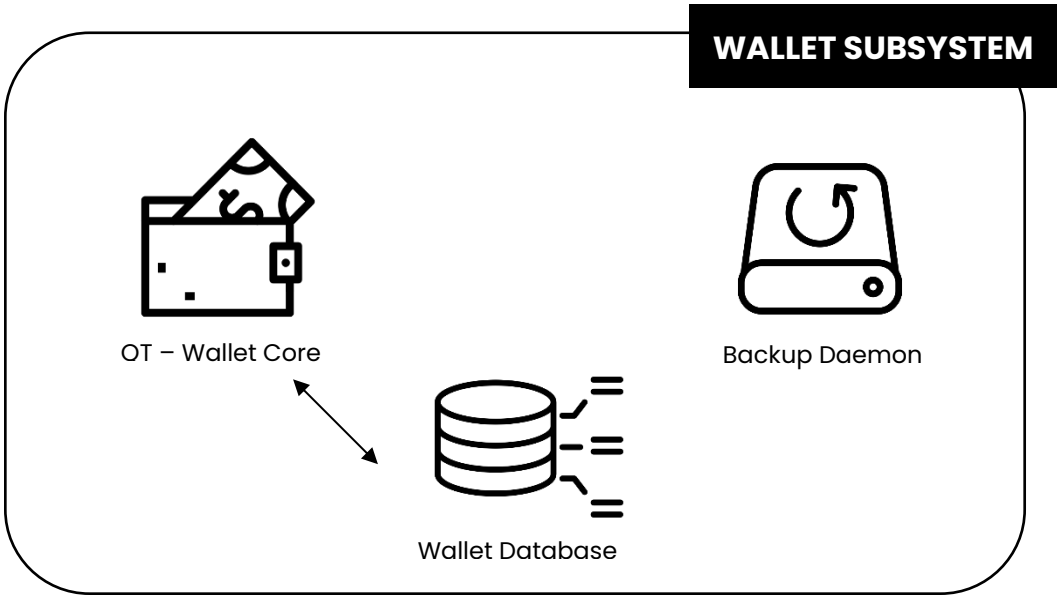
1. Wallet Subsystem
2. ViptoCoin Core
3. Front-end of the Web
4. Optional Mobile Extension Interface

Through the Mobile Extension Interface (MEI), end-users will be able to access their web wallet directly from their personal devices. Not only will it incentivize users to use ViptoCoin, but also pave the way towards new avenues that will rely on the use of ViptoCoin.

The Mobile Extension Interface (MEI), allows integration with third-party applications, precisely social messaging apps such as Whatsapp and Telegram. Through this integration, users will be able to pay for services, including sending and receiving ViptoCoin via social messaging apps - making it an even more convenient process.

The following figures describe the Web Wallet System in further detail:





➢ ***Wallet Subsystem***

The subsystem in the wallet of ViptoCoin is equipped to deliver all the standard features of a wallet, and more.

- The Wallet Core - Send, Receive and Stake ViptoCoin (VCC).
- Wallet Database - Backup Daemon, Full or Incremental backups, User Defined Backup Policies, Disaster Recovery Process, etc.

➢ ***Integrated Merchant & User Support***

The ViptoCoin family of products also includes a support service that provides users and merchants with assistance related to ViptoCoin products and services. We encourage all enquiries from software bugs, to user inquiries.

➢ ***PayVipto***

➔ ***Cross-platform Connectivity***

PayVipto is a community driven payment solution for merchants devised to make transactions seamless and efficient for both the merchant and customer. The codebase that powers PayVipto enables a centralized payment facility that are connected to plugins that share cross-platform connectivity with leading e-commerce platforms such as Shopify, Magento, and WooCommerce to name a few.

➔ ***Buy and Sell with PayVipto***

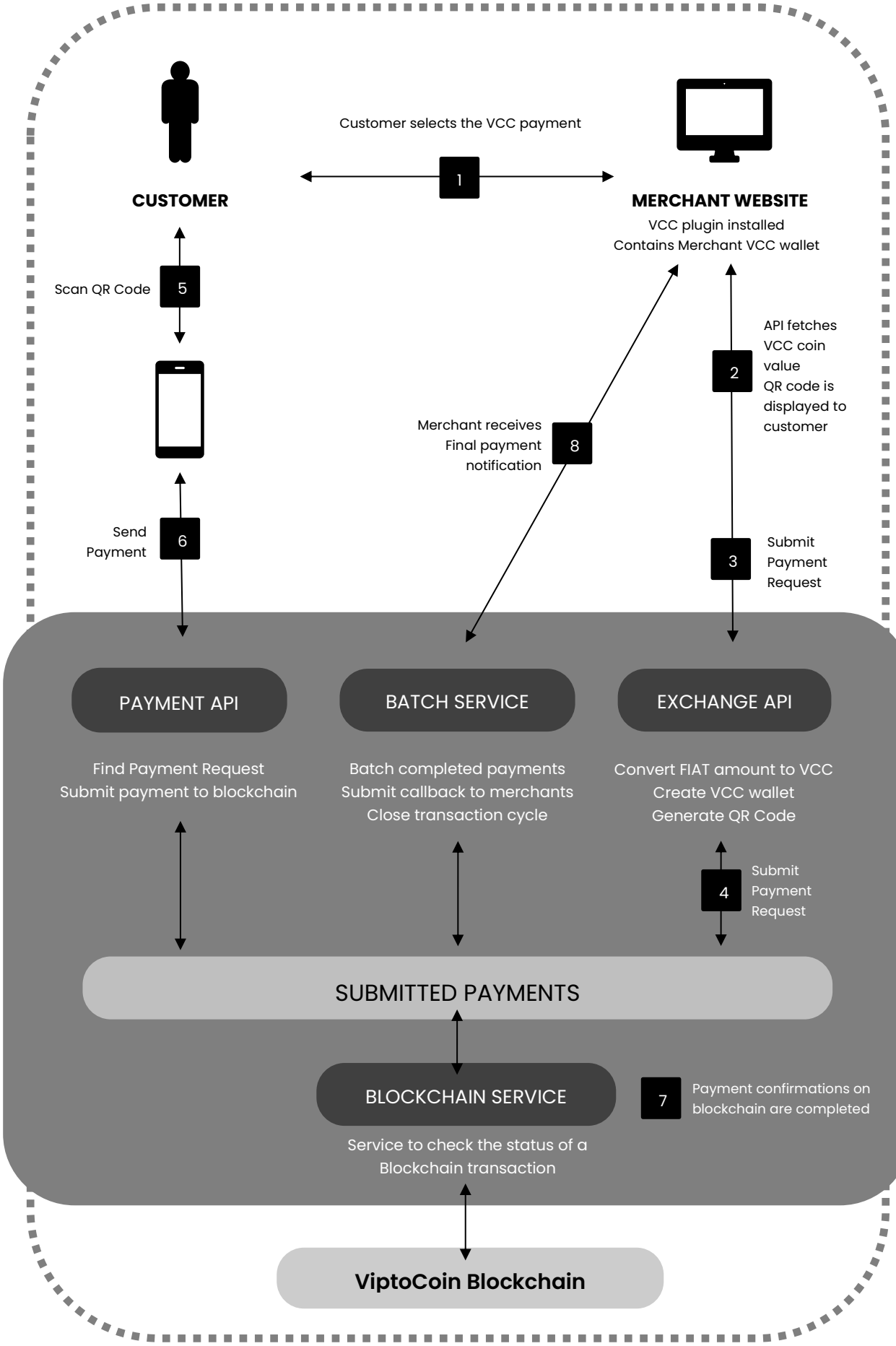
The PayVipto system therefore, allows merchants to receive payments, in the form of VCC in exchange for their goods and services, by simply installing the PayVipto plugin onto their preferred e-Commerce platform. Once the customer chooses VCC as their payment method, the plugin will then convert the relevant fiat value of the selected good or service into ViptoCoin. It is tabulated by referencing the latest official ViptoCoin price data. The customer will then be presented with a payment address along with a QR code.

Once the PayVipto system detects the payment initiation, it will send a validation call to the merchant's website and route the relevant ViptoCoin value through the PayVipto system to obscure the final payment address. Thus, ensuring confidentiality and security, which provides additional easement to merchants who plan on shifting to the PayVipto system.

➔ ***Simple and Easy to Use***

The plugin is not only simple and easy to use, as it also provides merchants with meticulous customizability, allowing them to customize the plugin to fit their own needs. This includes the option of including their own code, via the PayVipto API that is integrated onto the merchant's individual payment page.

The following page shows a chart that illustrates various building blocks of the PayVipto system.


CUSTOMER
Customer selects the VCC payment
1
MERCHANT WEBSITE
VCC plugin installed
Contains Merchant VCC wallet
Scan QR Code
5
API fetches
VCC coin
value
QR code is
displayed to
customer
2
Merchant receives
Final payment
notification
8
Send
Payment
6
Submit
Payment
Request
3
PAYMENT API
BATCH SERVICE
EXCHANGE API
Find Payment Request
Submit payment to blockchain
Batch completed payments
Submit callback to merchants
Close transaction cycle
Convert FIAT amount to VCC
Create VCC wallet
Generate QR Code
Submit
Payment
Request
4
SUBMITTED PAYMENTS
BLOCKCHAIN SERVICE
7
Payment confirmations on
blockchain are completed
Service to check the status of a
Blockchain transaction
ViptoCoin Blockchain

➢ *Atomic Swaps*

Atomic swaps, alternatively known as atomic cross-chain trading, allows two parties to trade tokens from two different blockchains. They are automatic exchange contracts that eliminate the need for centralized third-party entities when executing trades.

➔ *Why use Atomic Swaps?*

The current cryptocurrency market is congested, with more cryptocurrencies being developed every day. The sheer number of cryptocurrencies make the task of exchanging currencies more complicated for those who are thorough with cryptocurrency.

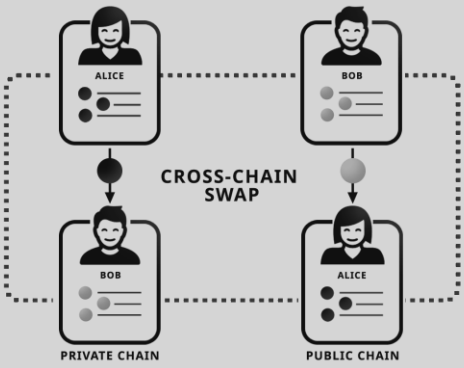
In addition, there is also the looming concern of the absence of an option to reverse a slip up, should a miscalculation occur during a transaction. The potential result? A major loss. This calls for a trusted third-party service to ensure that both sides of a transaction receive a proper resolution, within the trading protocols of crypto exchange.

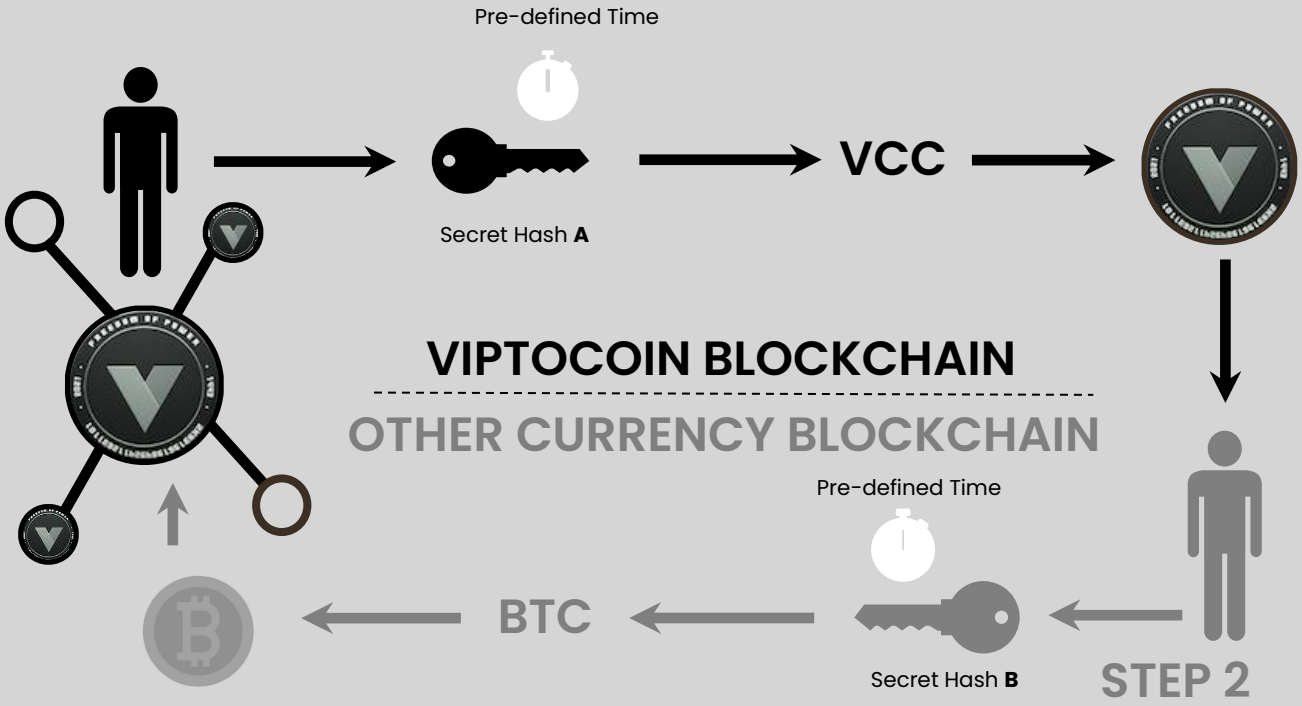
"Atomic Swaps is our solution to this problem."

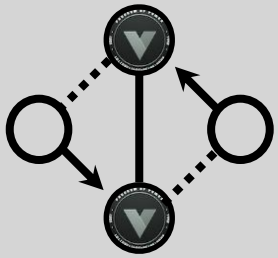
ViptoCoin generates a hash-time-locked contract - a payment wherein the receiver is required to acknowledge the receipt of the payment before a preset time or deadline. This is done by using automatic swap architecture. This contract pairs multi-signature addresses and time-locks to secure the transaction at a mutually agreed price point.

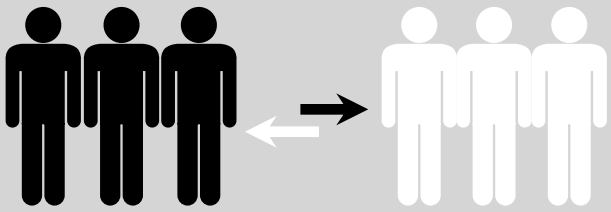
A two-party cryptocurrency that uses atomic swap can simultaneously occur on different blockchains. A shared private code reinforces the security of the atomic swap. The transaction will only be realized with the usage of a shared private code by both parties. Only a private code that is shared by both parties can realize the transaction. The transaction will fail if either of the parties enter an incorrect code - resulting in the return of funds to the original sender. The shared private code therefore, removes the need for third-party intervention.

HOW ATOMIC SWAPS WITH VIPTOCOIN WORK









ATOMIC SWAPS, OR **ATOMIC CROSS-CHAIN TRADING,** IS THE EXCHANGE OF ONE CRYPTOCURRENCY TO ANOTHER CRYPTOCURRENCY **WITHOUT** THE NEED TO TRUST **A THIRD PARTY**

➔ ***Without Atomic Swaps***

Imagine ordering an ice-cream at a diner that only accepts bitcoin as the mode of payment. Now, let's picture the complex series of operations that must occur for the transaction to take place.

1. Access an exchange platform
2. Send the agreed VCC amount to be exchanged
3. Sell VCC for Bitcoin
4. Open a Bitcoin wallet application
5. Transfer Bitcoin to wallet from the exchange
6. Wait for the Bitcoin transaction to confirm
7. 'Promptly' pay for your (melted) ice cream

Now, imagine how inefficient our day-to-day lives can get, if the time it takes to pay for your ice-cream, takes away the reason you wanted it in the first place. Which clearly, is far from satisfactory.

➔ ***With Atomic Swaps***

Now, let's rewind the same scenario back to the beginning, only this time, we will enable atomic swaps.

1. Open the ViptoCoin application
2. Scan the QR code of Bitcoin
3. Confirm the payment within the application
4. Enjoy your (frosty cold) ice cream

Not only does atomic swaps save you valuable time but it also simplifies the transaction drastically. Thus, eliminating the need to check what cryptocurrency is accepted by the shop.

Both, the VCC-blockchain and the non-VCC blockchain would need to confirm the transaction.
If not, the VCC will return to the original wallet.

➢ ViptoCoin Core

ViptoCoin Core is the back-end engine of ViptoCoin and it consists of the following modules:

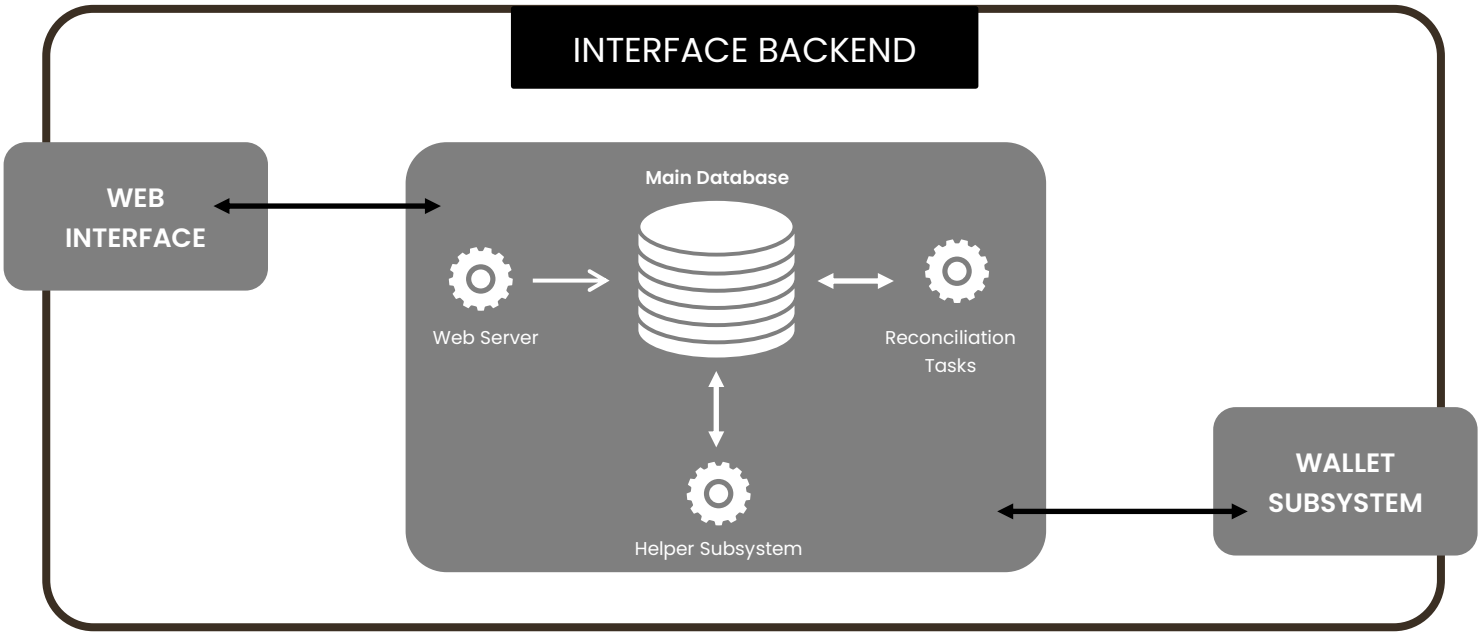
1. Web Server
2. Reconciliation tasks
    a. Reduces the risk of error
    b. Guarantees consistent results, regardless of the volume
    c. Synchronization between the wallet subsystem and the database

3. Helper Subsystem
    a. Carries out the functions of maintaining system health

b. Performs administrative tasks such as backing up data

4. Database
    a. Contains user information
    b. Contains user contacts
    c. Dashboard settings
    d. Configuration settings
    e. Security settings
    f. Profile settings
    g. Contains Wallet information including balances and staking

➢ **The Web Interface**



➢ The web interface is made of three modules: ***Client GUI Server Interface; Server Interface and Requests Serialization; Security and Authentication***. The web interface is the front-end interface that lies between the user and the ViptoCoin Core.

➔ **Client GUI Server Interface**
- Compatibility with the given baseline of browsers/versions
- Ability to run on mobile and PDA devices

➔ **Server Interface and requests serialization**

- Uses secure web sockets to open up communication between the ViptoCoin Core and the front-end system

- The server interface implements a transactional subsystem
- The transactional subsystem implements the serialization of concurrent users requests and vice versa
- Transactions can be synchronous or asynchronous

➔ **Security & Authentication**

❖ **Enforces standard login policies**
- Login form
- Two-factor Authentication

❖ **Web protection features**
- Recaptcha (from Google)
- DDoS (Distributed Denial of Service)

❖ **Private API**
- Implementation of the wallet API by the mobile wallet application (aka - Mobile Extension Interface)

Roadmap

ViptoCoin was founded on a vision. It was brought to life, for the people, to fulfill their day-to-day needs as easily as possible. The ViptoCommunity will continue to redesign and innovate; to work to actively enhance the ViptoCoin infrastructure.

To stay on track with the most recent revisions and updates, please visit: https://viptocoin.com/road-map

Milestones Achieved

2021

Third Quarter

- Completion of block explorer – https://viptotracker.com
- Development of the pool (Proof-of-Work)

Fourth Quarter

- Support for early miners enabled
- Windows wallet released
- Linux wallet released
- Mac OS wallet released
- ViptoCoin's main website launched – https://viptocoin.com
- ViptoCoin's Web Wallet launched – https://viptowallet.com
- Development of online communities and social media pages

Planned Objectives

2022: Fourth Quarter

- Increase the number of nodes on the main network
- Prepare educational material on ViptoCoin
- Begin the development of PayVipto
- Commence a full-fledged marketing campaign to raise public awareness on ViptoCoin
- Begin the development of atomic swaps
- Partner with new merchants to increase the usage of ViptoCoin in day-to-day transactions.
- Release Mobile Wallets: Proprietary iOS and Android Wallet development
- Integration of Payment Gateway

- Begin development of the merchant payment API/Gateway
- TOR Integrated Wallets: Use TOR/I2P networks to boost privacy features (optional)
- Release Atomic Swap
- Listings on more exchanges
- Further additions to merchant base

ViptoCoin Team and Community

➢ The Team

Behind the Cryptocurrency Blockchain and the ViptoCoin (VCC) coin, are a passionate, growing community of coders, developers, business professionals and enthusiastic contributors who believe in the power of cryptocurrency in ensuring a sustainable future.

The ViptoCoin Management & Development Team consists of core developers, project managers, community managers, UI/UX designers, web designers and marketing experts.

Management and Development Team

- ➔ Arttey [@Arttey]
- ➔ Zia [Ziaharif]
- ➔ Ari [arifali1142]
- ➔ Rifga [@fathimathrifga]
- ➔ Zul [@thotho.arif]
- ➔ Izzy [@izzyinu]
- ➔ Alfred [@alifredismail]

➢ The Community

Since its inception, the ViptoCoin Community has been expanding fast and adapting new ways. All the active members of the Management and Development Team, and their expertise will be added to the official project website of the ViptoCoin project. The team is subject to change based on the requirements of the community.

https://viptocoin.com/our-team

All the decisions concerning the team members are made and regulated by Vexeda Co. Private Limited. Anyone can get in touch with our community of developers, contributors, moderators and fellow Viptonians and community members via the Discord server: https://discord.gg/FR88MYReag

Updates & Upgrades to the White Paper

The development of this white paper is yet to conclude and is set to expand with further developments. The White Paper of ViptoCoin is merely the beginning of a much more comprehensive shared document known as an “Open Paper”. The Open Paper will inherently be the ultimate referential technical document of the ViptoCoin Project. Additionally, it will be open to contributors to further ensure uninterrupted development, and upgrades.

The Open Paper is currently available on the official Github page of the ViptoCoin Project for those interested in contributing to the growth of this project.
https://github.com/vexeda/ViptoCoin/blob/main/TheOpenPaper

The ViptoCoin Community, in collaboration with ViptoCoin’s Core Team, is committed to reviewing and updating the Open Paper, whenever and wherever necessary, while implementing additional proposals and projects on a monthly basis.

We welcome the feedback and contribution of every user, for it may bring newer perspectives to the project. Should you wish to share any remarks or suggestions, please feel free to express your constructive opinion.