CrypticCoin

# WHITEPAPER

## NON TECHNICAL OVERVIEW

**Security, Anonymity & Privacy All In One!**

https://crypticcoin.io/

# Forward

All technologies have both advantages and disadvantages. That's why we are combining technologies into the creation of one coin. CrypticCoin gives our users the ability to choose, compare and eventually use the confidentiality mechanism that best suits them. CrypticCoin is a coin designed for the discretion of users by offering them the appropriate tools.

As a basis, we decided to implement a mix of an enriched version of the ZeroCash Protocol (zk-SNARK systems protocol) and a Hybrid version of Verge (Stealth Addressing Technologies). However, we make no claims that CrypticCoin will offer only these two mechanisms, over time, other privacy technologies (e.g., Confidential Transactions) will be implemented in CrypticCoin.  Over time other privacy technologies will be added to CrypticCoin.  CrypticCoin also has proprietary enhanced security measures built in to further enhance the system of security within the CrypticCoin Ecosystem.

It is with such functionality that CrypticCoin will be presented to the community.  We suggest and encourage users have shielded transactions enabled by default.

# Introduction

Most cryptocurrencies are based on blockchains in which payment transactions are stored "as is" in a decentralized ledger. Because the blockchain is public, said details such as a sender’s public address, recipients public address, and payment amount about each transaction as well as the history of all transactions can be viewed by anyone. While public addresses are not explicitly tied to users' real identities, there are ways to learn more about users, their spending habits and relationships with each other using information stored in most blockchains. In most cases, wallets used for making transactions do not support anonymity features while connecting to blockchain nodes. A user's location can be determined by IP address of the used device and privacy of the transaction is eliminated.

**CrypticCoin (CRYP) is a decentralized and open-source cryptocurrency that aims to connect best practices regarding the privacy and anonymity for its users. CrypticCoin allows users to engage in direct transactions rapidly and a high level of privacy.**

# MAX SUPPLY DEFINED

**As of 1-18-2018 there were roughly 7,598,607,351 people exist on Planet Earth, therefore maximum supply of 7,598,607351 coins will be distributed. One for every person on Earth. We all deserve to control and manage our own privacy!**

# Security, Anonymity & Privacy All In One!

WHITEPAPER
NON TECHNICAL OVERVIEW
https://crypticcoin.io/

## Enriched ZeroCash Protocol Integration

CrypticCoin further enhances levels of security and privacy by using the Zerocash protocol to its advantage.  Utilizing the ZeroCash Protocol improves privacy by adding levels of transactions and ensures that payment transactions do not contain any public information about the sender’s address, recipient's address or any transferred amounts. This is achieved by adding a sub-coins level to the existing base-coins. Each user can convert base-coins into sub-coins (1:1) to be able to make more private payment transactions. Users can also convert sub-coins back into base-coins (1:1) at any time when they want.

CrypticCoin further utilizes the enriched Zerocash functionality by implementing two new types of transactions: Fresh Mint transactions and Pour transactions, which are recorded to the public ledger as well.

A fresh mint transaction allows users to convert a specified number of base-coins (debited from any one of the owned base-coins accounts) into the same number of sub-coins (credited to any one of the owned sub-coins accounts).

The fresh mint transaction itself consists of a cryptographic commitment, which specifies the amount of converted sub-coins, owner address and unique serial number. The commitment is based on the SHA-256 hash function, that allows to hide both the converted amount and owner address. However, the commitment is constructed so that anyone can verify that the committed sub-coin has the claimed value.

# Enriched ZeroCash Protocol Integration

A pour transaction allows a user to make a private payment, by consuming some amount of sub-coins owned by the user in order to produce the same amount of sub-coins to the recipient. The correctness of the transaction is validated via the use of zero-knowledge proof (https://en.wikipedia.org/wiki/Zero-knowledge_proof).

A pour transaction, for (up to) two input sub-coins and (up to) two output sub-coins, involves proving, in zero knowledge, that:

- The user owns the two input sub-coins.

- Each one of the input sub-coins appears in some previous mint transaction or as the output sub-coin of some previous pour transaction.

- The total value of the input sub-coins equals the total value of the output sub-coins.

The pour transaction consumes the input sub-coins by revealing their serial numbers, but does not reveal any other information such as the amount of the input or output sub-coins, or the addresses of their owners.

The pour transaction can also output some amount of base-coins. This feature can be used to convert sub-coins back into base-coins or to pay transaction fees.

For a pour transaction, anyone can verify that the zero-knowledge proof contained therein is valid. For efficiency, our integrated use of the Zerocash Protocol uses "Zero-Knowledge Succinct Non-interactive Arguments of Knowledge" (zk-SNARK) systems, which are zero-knowledge proofs that are particularly short and easy to verify.

## Privacy on/off options for transactions

With CrypticCoin users have the ability to choose what type of transaction they want to make - public or private.

A public transaction is recorded to the CrypticCoin public ledger in an unchanged form with the sender's public address, recipient's public CrypticCoin address and payment amount of CRYP transferred.

This type of transaction can be done if it is necessary to prove to a third party that the sender did, in fact, make a particular transaction.

A private CrypticCoin transaction is recorded to the public ledger using a one-time public key which is generated by a special algorithm. When analyzing blockchain, such transactions are not traceable on a public ledger and can not be uniquely mapped to another transaction, so there is no possibility to analyze the activity of any network member using the public ledger, with whom and in what quantity exchanged in the transactions.

Private transactions will be improved by the implementation of the ZeroCash protocol, which completely hides the transferred amount and the transaction metadata. It will increase the privacy of payments by consuming coins transferred by a sender in order to produce the same amount of new coins for a recipient. So, received coins will not have a history. Regardless of a transaction type, the connection between a user's wallet and the blockchain are anonymized by default through hiding the user's real IP address when making transactions.

High levels of privacy and anonymity are achieved by the effective integration of such technologies as: Hybrid Stealth Addressing, ZeroCash protocol and IP Obfuscation.

## Hybrid Stealth Addressing

When users create a CrypticCoin account they will have a private view key, a private spend key, and a public address. The spend key is used to send payments and the view key is used to display incoming transactions destined for users accounts. Users do not need to interact with these keys directly, all accounts (and their corresponding keys) are managed by a user's wallet. Nevertheless, the owner of the wallet can access them if necessary. Both the spend key and view key are used to build your CrypticCoin public address, which users present to a sender for receiving payments. Users can increase their privacy by providing different CrypticCoin public addresses for senders (users create separate accounts for interactions with different senders). But even in this case, all user transactions with a particular sender are linked with each other in public ledger using the same CrypticCoin public address.

**We have enriched the Stealth Addressing technology which allows users to publish one address for everyone (a Hybrid Stealth Address) and at the same time greatly increases the privacy of received payments.**

Hybrid Stealth Addresses allow/require the sender to create random one-time CrypticCoin public addresses for every transaction on behalf of the recipient. So, the recipient will have all of their incoming payments go to unique CrypticCoin public addresses on the blockchain, where they cannot be linked back to either the recipient's published addresses (stealth or public) or any other transactions addresses.

These unique CrypticCoin public addresses can only be recovered and spent by the recipient. By using Hybrid Stealth Addresses, only the sender and receiver can determine where a payment was sent. No one else will have the ability to link the wallet addresses together by investigating transactions on the blockchain.

# Hybrid Stealth Addressing

**Hybrid Stealth Addressing key features:**

- Hybrid Stealth Addresses cannot be linked publicly to either the randomly created one-time CrypticCoin public address or any other one-time CrypticCoin public addresses.

- Hybrid Stealth Addresses can be recovered and spent by the recipient only.

- Only the recipient can link together all the payments made using their Hybrid Stealth Addresses.

Hybrid Stealth Addressing functionality is achieved through the Elliptic Curve Diffie-Hellman (ECDH) cryptography system. CrypticCoin Hybrid Stealth Address is a string that consists of a public view key and the public send key of the recipient. While making a payment, any sender is able to calculate a unique one-time public key for the recipient's new output on basis of this Hybrid Stealth Address. ECDH algorithm ensures that the one-time public key cannot be reverse engineered and that nobody else can duplicate it. This output can be located by the recipient's wallet during scanning the blockchain with wallet's private view key. After the output is detected and retrieved, recipient's wallet can calculate a one-time private key that corresponds with the one-time public key of the output. So, the recipient's wallet always knows about the current available balance. The recipient can spend the relevant output with their wallet's private spend key.

## IP Obfuscation

To improve the privacy of connectivity between a user's wallet and the blockchain, all wallet distros (full and lightweight) will support anonymity features out of the box. This is done via integration of IP obfuscation service into distros.

Tor ("The Onion Router") is used as an IP obfuscation service. It is a decentralized system that enables anonymous communications through a network of relays which serve to obfuscate IP addressing information by bouncing connections from node to node at random, effectively eliminating any information trails.

Tor redirects the users internet traffic through a free worldwide relay network to hide users location and interests from anyone who monitors networks or makes traffic analysis.

Tor uses the onion routing mechanism, which is implemented by nested encryption on the application layer of TCP/IP stack.

Tor encrypts transmitted data, including the next node destination IP, and sends it through a virtual circuit of randomly selected relays.

Each relay in a virtual circuit decrypts only the necessary layers of the data packets to find out which relay the data came from, and to which relay to send it next. The relay then rewraps the package and sends it on.

The last relay decrypts all layers of encryption and sends the original data to the intended destination without knowing the IP address of real origin source.

## IP Obfuscation

Because the routing of all communication is partially hidden at every hop in the virtual circuit, the onion routing mechanism eliminates the possibility that the final communicating peers can be determined by anyone who may apply surveillance to the network.

Tor's use is intended to protect the personal privacy of users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored.

IP obfuscation functionality will be expanded by I2p technology integration within wallets. I2p (invisible internet project) is a highly obfuscated tunneling service using ipv6 that is similar to Tor, but has some other major advantages.

Instead of circuit based routing with Tor, I2P performs packet based routing that is similar to the internet's IP routing. In addition, I2p does not rely on a centralized directory service to get route information as Tor does. It uses distributed hash tables (DHTs) to coordinate the state of the network, so network routes are updated dynamically. Also, I2p establishes two independent simplex tunnels for traffic to and from each host as opposed to Tor's single duplex circuit.

## Wallets

CrypticCoin offers desktop users full QT-based wallets and light-weight Electrum-based wallets for all popular operating systems (Linux, MacOS, Windows).

CrypticCoin will offer mobile users “easy-to-use” lightweight Electrum-based wallets with unique design for popular mobile operating systems (Android, iOS).

All CrypticCoin wallets support anonymity features by default through hiding the user's real IP address when making transactions, i.e. all wallets have Tor integration out of the box. So, the wallets have no built-in ability to connect to or broadcast user data over clear internet.

To increase user security, wallets have multi-signature support, which requires more than one key to authorize a transaction. Also, wallets are able to handle P2P QR-code scan transactions with instant verification. Clients are able to also import QR-codes from paper wallets to pull balances from cold storage if desired. A lightweight Electrum-based wallet does not need to download the whole blockchain, instead it requests the necessary information from secure remote Electrum servers which handle the rest of the CrypticCoin network. Electrum servers do not store user accounts with private keys. Private keys never leave user devices and are not shared with Electrum servers.  Lightweight Electrum-based wallets are fast with low resource usage, have no delays for primary synchronization and are always up-to-date.

## Wallets

A lightweight Electrum-based wallet helps protect users from their own mistakes and allows users to recover their wallet with a secret seed phrase. Additionally, it offers a simple and easy to use cold storage solution. This allows users to store all or part of their coins in an offline manner. While using the lightweight Electrum-based wallet, transactions are completed via Simple Payment Verification (SPV), a technique that allows for the wallet to verify transactions through proof of inclusion; a method for verifying if a particular transaction is included in a block without downloading the entire block. SPV allows for nearly instant payment confirmations because it acts as a thin client that only needs to download the block headers, which are drastically smaller than full blocks.

## FreeCO

CrypticCoin is not launched through an ICO. The founders have paid for the development and launch of the CrypticCoin and its corresponding ecosystem without raising millions of dollars using an ICO. Instead of distributing the initial share of CrypticCoins only between founders, the team and advisors, CrypticCoin will reward the initial community of early adopters as well.

In the beginning, CrypticCoin will launch the Free Coin Offering (FreeCO) and give away free coins to early adopters, who will be participating in the FreeCO. Furthermore, there will be long-term post-FreeCO to incentivize community members, encourage active participants and promote CrypticCoin to make our community grow.

The amount of coins that will be distributed during FreeCO is limited to 5% of the CrypticCoin total supply. The amount of coins that will be distributed during post-FreeCO is limited to 10% of the CrypticCoin total supply.

Here at CrypticCoin it was decided to do things differently and give free coins to the community. Most importantly, we want to encourage the inclusion of newbies to the crypto space to make it more known what the potential of cryptocurrency is. It is the vision of the CrypticCoin team to build and launch something they believe in. CyrpticCoin offers security, anonymity and privacy for every human being.

## FreeCO

Free CrypticCoins will be distributed through a one-time links mechanism during FreeCO and post-FreeCO. The one-time link represents a gift certificate for some amount of free CrypticCoins (designated by a CrypticCoin admin that carries out the will of the founders and advisory team). The community members will receive their free CrypticCoins using these one-time links. All that is needed is to follow the one-time link and present the CrypticCoin address to which the corresponding amount of CrypticCoins will be transferred immediately from the FreeCo or post-FreeCo pool.

## Economics

CrypticCoin launches with a capped supply. Only 7.6 billion (7,598,607,351 to be exact) CrypticCoins will be issued ever. In total CrypticCoin will have 55% pre-mined CrypticCoins and 45% CrypticCoins available for mining for about 6 years. The purposes of 55% pre-mined CrypticCoins are the following:

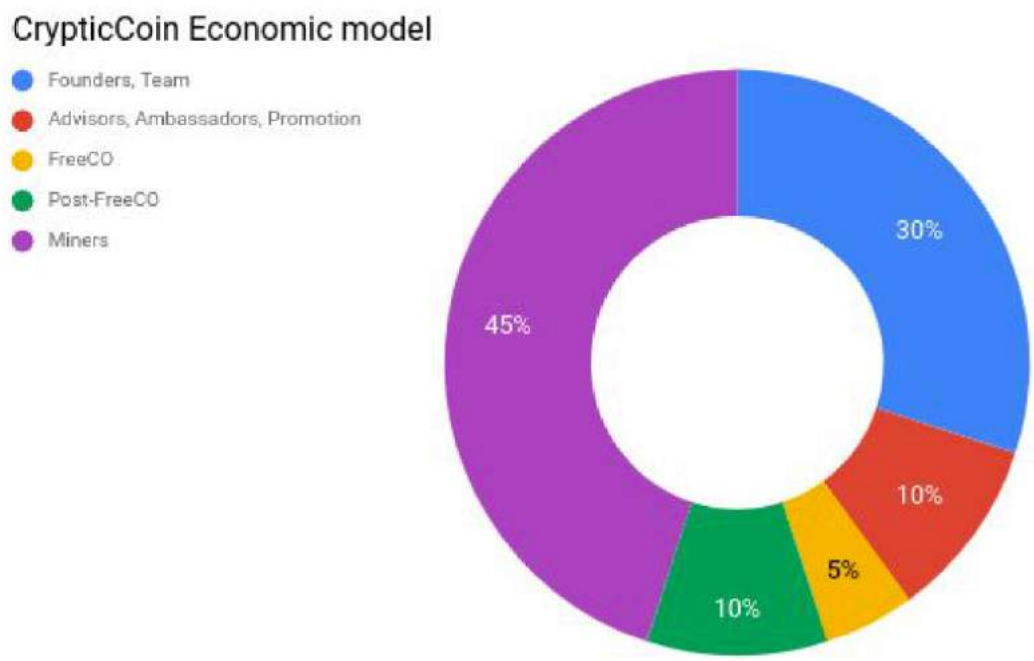
- 30% pre-mined CrypticCoins will be reserved for founders and team.

  This amount will be transferred to 30 wallets (1% to each wallet).

- 10% pre-mined CrypticCoins will be reserved for advisors, ambassadors and expansion and growth purposes. This amount will be transferred to 20 wallets (0.5% to each wallet).

- 5% pre-mined CrypticCoins will be reserved for FreeCO and will be transferred to a dedicated address of the FreeCO pool.

- 10% pre-mined CrypticCoins will be reserved for post-FreeCO and will be transferred to a dedicated address of the post-FreeCO pool.



## Multi-Mining

CrypticCoin supports multi-mining that combines the 5 Proof-of-Work hashing algorithms: Scrypt, Blake2s, X17, Myr-Groestl and Lyra2REv2.  It means that a wide range of people with different types of mining devices have equal opportunities for mining CrypticCoins. In addition, multi-mining allows the CrypticCoin to have higher protections against Sybil Attacks compared to other cryptocurrencies, which support only single PoW hashing algorithm.  All 5 mining algorithms have the same target block time and only their hash rates are impacted due to the target difficulty.

# Roadmap (Future Plans)

CrypticCoin will be constantly improved by implementing new features and expanding its ecosystem. Such continuous development is performed by the core development team that consists of several permanent contributors. The development of the following tasks are scheduled:

- Forum platform that allows users to suggest any ideas that will be useful for the CrypticCoin community. Such ideas will be assessed by the community through a voting mechanism within the CrypticCoin forum. The ideas selected by the voting will be crowdfunded and implemented.

- Official mining pool that will support mining based on any of 5 Proof-of-Work hashing algorithms used in CrypticCoin (Scrypt, Blake2s, X17, Myr-Groestl and Lyra2REv2).

- Unique and easy to use mobile wallets for Android and iOS platforms. For CrypticCoin participants, these wallets will be as user-friendly as possible.

- Wallets with built-in I2p integration. The wallets have improved anonymity features and will be offered to CryptoCoin users for more robust IP obfuscation.

- Encrypted p2p chat between CrypticCoin network members. Instant messaging system that ensures encryption and privacy of P2P (Peer-to-Peer) communications.

- RSK smart contracts integration. RSK (Rootstock) is a two-way pegged sidechain that extends CrypticCoin by adding the smart contracts functionality.

- Launching the company for the debit cards connecting the virtual card and plastic card. Issuing the debit cards, which will support fiat currencies (EUR, USD, etc.), the CrypticCoin, other cryptocurrencies and will have native exchange capability between supported currencies. CrypticCoin development roadmap is presented below.

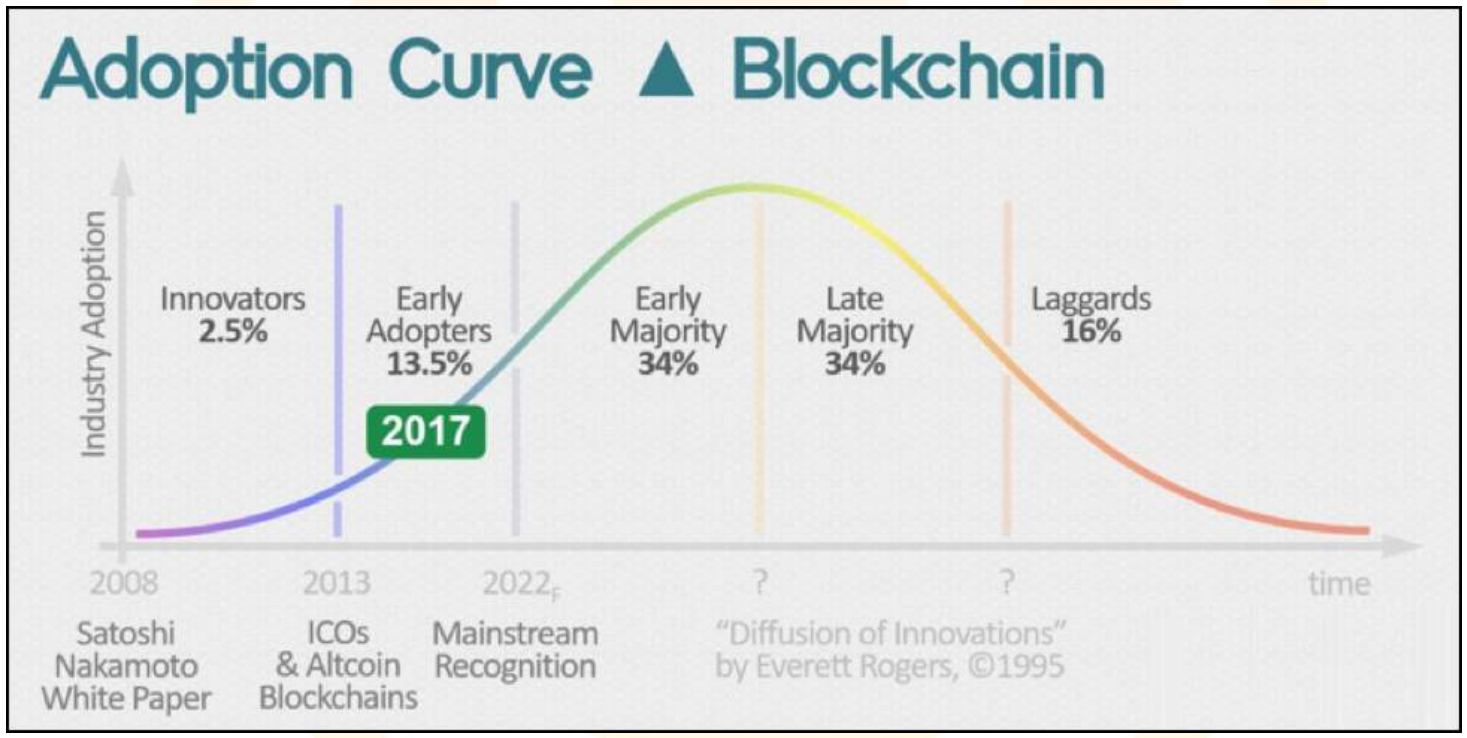
The roadmap can be slightly changed by adding additional tasks and rescheduling current and new tasks.

# Roadmap (Future Plans)

# Roadmap (Future Plans)

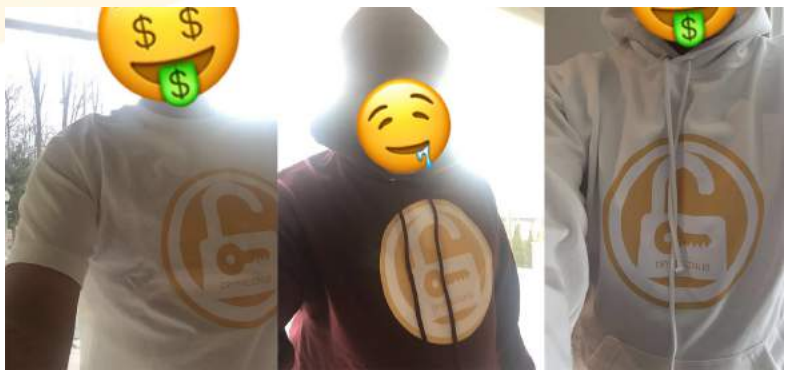
**Website Transaction Inclusion**

Our intention is for early adopters to have increasing options for spending and also expanding the CrypticCoin community.  In the future we would like more websites to accept CRYP as another form of payment. Currently a few sites (Etsy/Overstock) chose to accept only certain cryptocurrencies, but this is also an opportunity for vendors to add a revenue stream.

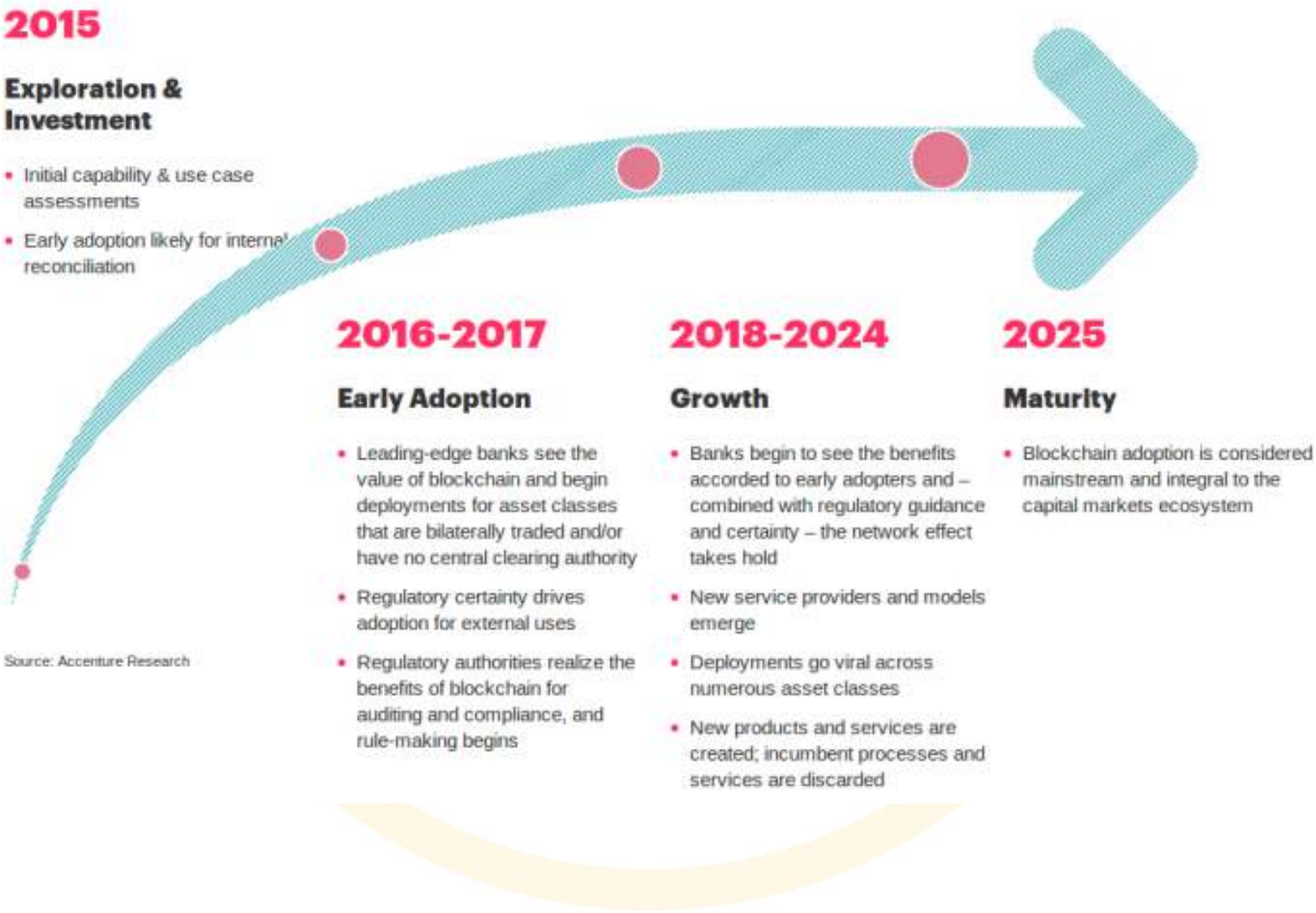



**Marketplace creation:**

Push for acceptance of CRYP online and offline.  CrypticCoin even has plans for merchandise for the fans.



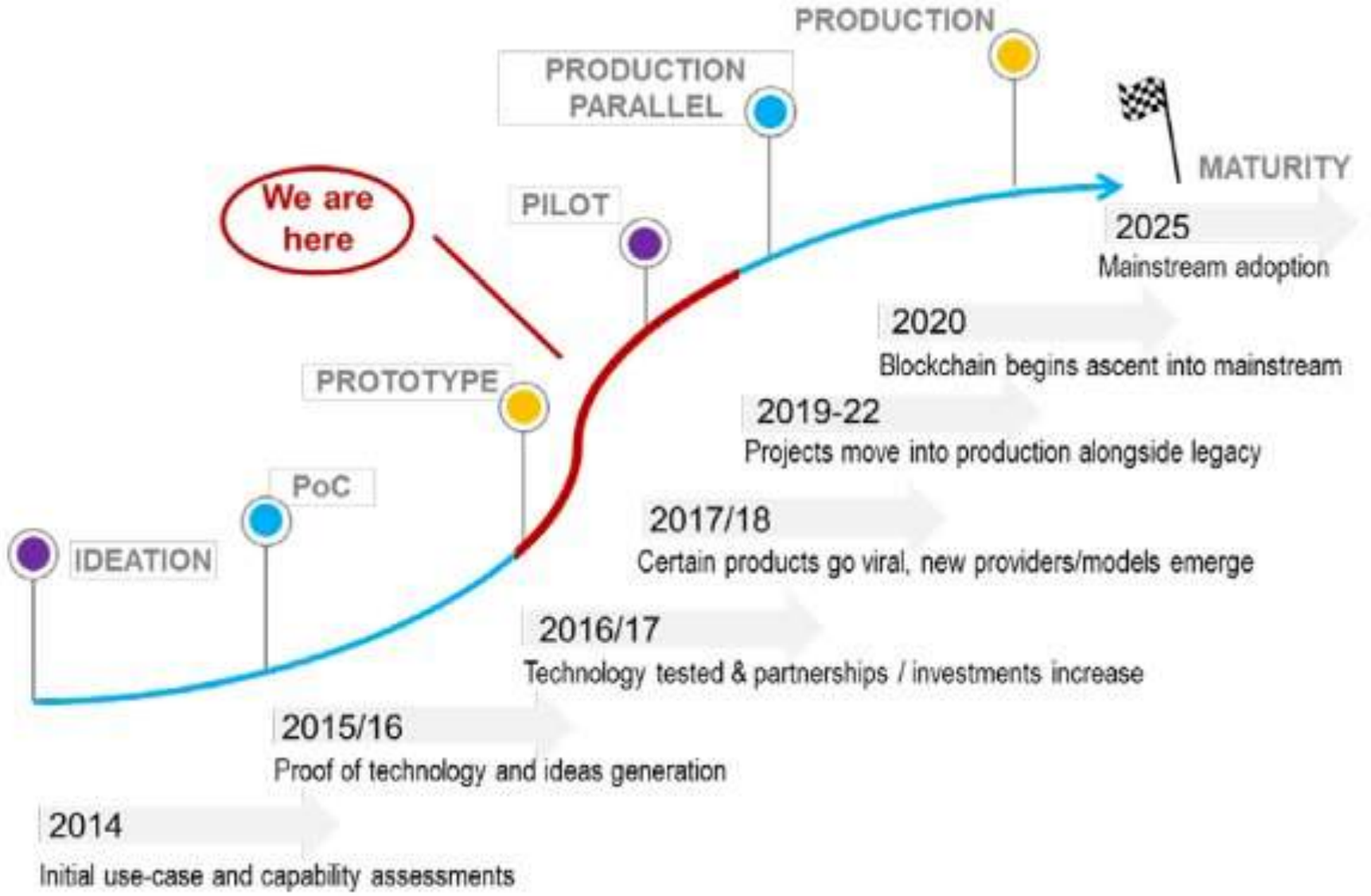
# Roadmap (Future Plans)




This diagram shows the expansion of the market from exploration and investment all the way to maturity.  Most are not aware that we are in an early adoption mode.

# Roadmap (Future Plans)

**Figure 45: Development timeline – where are we now?**




Source: Accenture, Credit Suisse estimates

Featured here is another diagram showing where we are currently in the space. CrypticCoin is in position for the best time for growth and expansion of blockchain technology.

# Privacy Coin Comparison

CrypticCoin

**8 PRIVACY COINS : 2018**

A DETAILED BREAKDOWN OF 7 PRIVACY COINS
COMPARED TO THE CRYPTICCOIN FRAMEWORK

| PRIVACY COIN DETAILS | CrypticCoin | Bitcoin | Monero | ZCash | ZCoin | PIVX | Navcoin | Verge |
|---|---|---|---|---|---|---|---|---|
| Circ. Supply - Millions | 7,600 | 16.8 | 15.8 | 3.5 | 4.3 | 55.7 | 62.5 | 14,700 |
| Total Supply - Millions | 7,600 | 21 | 16 | 3.5 | 4.2 | 55.7 | 62.5 | 14,500 |
| Max Supply - Millions | 7,600 | 21 | ⊗ | 21 | 21 | ⊗ | ⊗ | 16,500 |
| Block Time - Seconds | 30 | 600 | 120 | 150 | 600 | 60 | 30 | 30 |
| PoW Mining | ✓ | ✓ | ✓ | ✓ | ✓ | ⊗ | ⊗ | ✓ |
| PoS Staking | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ✓ | ✓ | ⊗ |
| I2P | ✓ | ⊗ | ⊗ | ⊗ | ⊗ | ✓ | ✓ | ✓ |
| Masternodes | ⊗ | ⊗ | ⊗ | ⊗ | ✓ | ✓ | ⊗ | ⊗ |
| Privacy Tech | Mixing | ⊗ | Ring CT | ZK-Snarks | ZeroCoin | ZeroCoin | Dual Block-TOR | Mixing |
| Native TOR | ✓ | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ✓ |
| OBFS4 | ✓ | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ✓ |
| ZeroCash Protocol | ✓ | ⊗ | ⊗ | ✓ | ⊗ | ⊗ | ⊗ | ⊗ |
| Stealthed IP | ✓ | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ✓ | ✓ |
| Stealth Addresses | ✓ | ⊗ | ✓ | ✓ | ✓ | ✓ | ⊗ | ✓ |
| Stealth Send | ✓ | ⊗ | ✓ | ✓ | ⊗ | ⊗ | ✓ | ✓ |
| Nodes Online / 24 hrs | ? | 12100 | 2,900 | 1,200 | 1,700 | 2,100 | 280 | ? |
| Voting Governance | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ✓ | ✓ | ⊗ |
| Mobile Wallets | Q2 | ✓ | ⊗ | ⊗ | ✓ | ✓ | ✓ | ✓ |
| Light Wallet | ✓ | ✓ | ✓ | ✓ | ⊗ | ✓ | ✓ | ✓ |
| Hardware Wallet | ⊗ | ✓ | ⊗ | ✓ | ⊗ | ⊗ | ✓ | ⊗ |
| Avg Transaction Fee | 0.01 CRYP | 0.0003 BTC | 0.01 XMR | 0.001 ZEC | 0.13 XZC | 0.003 PIVX | 0.0003 NAV | 0.01 XVG |
| Development Fund | ✓ | ✓ | ⊗ | ✓ | ✓ | ✓ | ✓ | ⊗ |
| Smart Contracts | Q4 | RSK beta | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ? |
| CRYPTICCOIN.IO | | | CRYPTICCOIN.IO | | | CRYPTICCOIN.IO | | |
| No ICO | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Market Cap | Unknown | $152,178,780,330 | $3,162,716,223 | $782,014,139 | $151,413,609 | $205,790,470 | $65,261,594 | $430,892,442 |
| Price | Unknown | $8,888 | $199.74 | $223.44 | $34.99 | $3.69 | $1.04 | $0.029271 |
| All Time High | Unknown | $20,000 | $494 | $926 | $153 | $14 | $4.71 | $0.27 |
| Possible x Gain | Unknown | 2.25 | 2.4 | 4.1 | 4.3 | 3.7 | 4.5 | 9.2 |

The privacy coin comparison above articulates a brief comparison between CrypticCoin and many other existing privacy coin options in the market.  It is our belief that CrypticCoin will grow and evolve to stand toe-to-toe and even surpass the coins featured in this list.


# WHITEPAPER

NON TECHNICAL OVERVIEW

https://crypticcoin.io/