

# BitXoe

## Whitepaper

VERSION 1.4 - 2021

# BITXOE - BITCOIN ESCROW PLATFORM

Bitxoe is the most private, secure, peer-to-peer custody-less encrypted platform for buying and selling products and services as well as swap XOE token with others cryptocurrencies.

## CONCEPT OF BITXOE

People exchange cryptocurrencies without counter-party risk by using a trust-less escrow concept. The peer-to-peer platform allows the crypto community to skip the middle-man and trade on their own terms, whether it's bitcoin, ethereum, xoe or any other mutual agreement between two people.

The trades executed using the Bitxoe platform are confidential via end-to-end encryption, and, unlike traditional over-the-counter platforms, the escrow mechanism is decentralised. The only time the escrow arbiter can step in and transfer cryptocurrency is if it receives explicit digital permission to resolve a dispute — but even then the contract code only allows the arbiter to transfer escrowed ether to one of the parties.

## INTRODUCTION

While cryptocurrency has succeeded in enabling people to conduct peer-to-peer transactions in a trust-less way, there has been no such solution for entering or exiting the crypto-economy. Because of the inherently insecure properties of centralised exchanges, billions of dollars have been stolen, lost, and destroyed in the hands of even the most popular services.

Although the number of cryptocurrency exchanges has grown, there has been little progress in eliminating trust from cryptocurrency on-boarding. Instead, blockchain financial innovators are replicating the vulnerable systems of Wall Street stock exchanges and banks — the same systems that provoked the global financial crisis, and the same systems that motivated the genesis of Bitcoin.

## CONCEPT OF BITXOE

The prime advantage of a cryptocurrency over fiat is the elimination of the need for an intermediary. Instead of relying on an institution to keep a record of your balance (i.e. a bank), blockchains use a distributed ledger of transactions verified by a large network of computers. The result is that it's impossible for anybody to access your digital wallet without possession of your secret key, regardless of other circumstances.

As long as your wallet's private key is kept secret, your cryptocurrency is secure — the idea is similar to keeping an ounce of gold in a home safe. Instead of trusting somebody to hold your cryptocurrency for you, you only need to have trust in the laws of mathematics and the thousands of computers auditing the ledger around the clock.

But when you deposit or buy cryptocurrency on a centralised exchange, you don't hold the private key to it. Instead, you need to trust the exchange, in the same way, that you trust a bank, to hold on to your money and keep an accurate record of your balance.

Bitxoe is a non-custodial platform, meaning it never asks for your private key(s). We don't ask you to trust us to hold on to your balance, because we know central reserves have a bad track record, plus the burden of safeguarding a large store of ether poses many other hurdles better avoided. Your Bitxoe wallet is kept encrypted in your web browser.

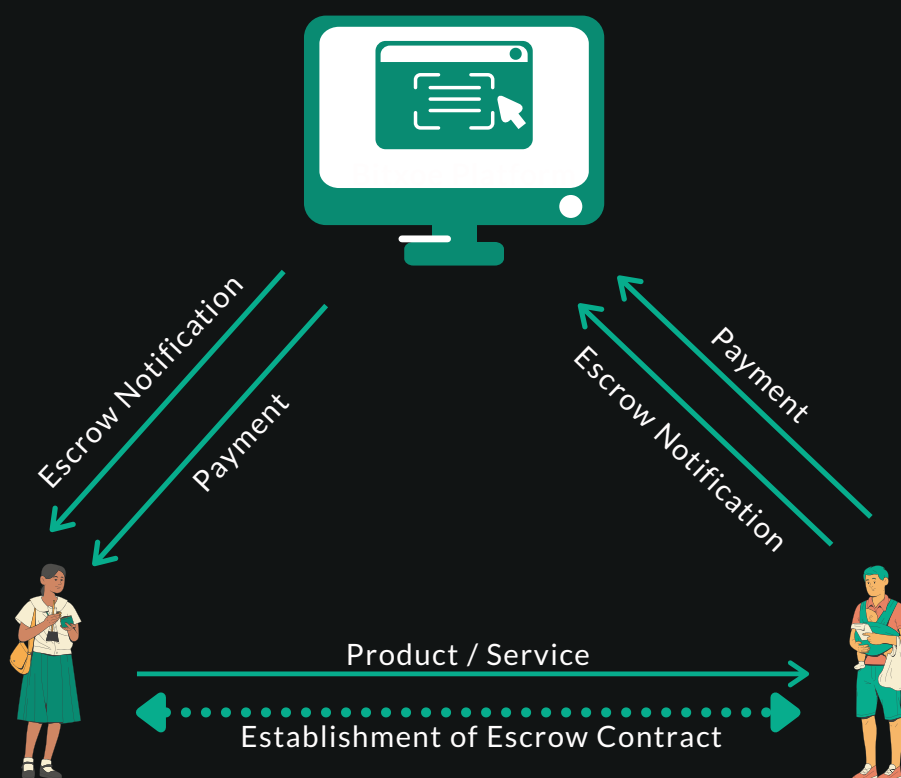
## Over-the-counter crypto

Since the invention of cryptocurrency, early adopters have been seeking alternatives to on-exchange trading. Having a central authority like an exchange keep record of customer balances and identities in a database, and facilitate transfers of local currency to cryptocurrency and vice versa, has always been viewed as counter-intuitive to the peer-to-peer nature of Bitcoin.

Over the counter trading, which is where two parties exchange with one another directly without the supervision of an exchange, has been popular in cryptocurrency since Bitcoin's beginnings. OTC trading grants flexibility, as there are no restrictions on what you can swap for cryptocurrency, and person-to-person transactions don't involve a financial intermediary. However, exchanging cryptocurrency with strangers online and in-person carries a major risk: how do we ensure that both parties are going to hold up their end of the bargain, and not vanish as soon as money or cryptocurrency hits their account? This exposure is known as counter-party risk.

## ESCROW WORKING MODEL

The experience of buying or selling on the Bitxoe platform differs from an exchange or an ordinary escrow service provider. Unlike an exchange, Bitxoe doesn't accept deposits or process withdrawals and there is no automatic matching algorithm. Unlike a normal escrow arrangement, Bitxoe doesn't hold any cryptocurrency or fiat in trust; the crypto portion of the trade is put in trust through a decentralised escrow mechanism.



Using Bitxoe.com, an ordinary trade works like this:

**STEP 1.** Alex posts a public offer to buy or sell a product or service. Offers can be posted publicly for anyone else to find. An offer is an advertisement stating a user's intentions for a cryptocurrency (for example, "I am willing to sell this product for 100 XOE").

**STEP 2:** Camila responds to the offer for 100 XOE. When a user responds to an offer, a trade is opened between the two parties, between Alex and Camila. The person responding to the offer enters the exact amount of XOE they want to buy or sell, and the rate is locked into the trade. Now, Alex and Camila can communicate with each other via an encrypted conversation.

**STEP 3:** Alex and Camila confirm and agree on the escrow terms of the transaction. The two parties introduce each other and chat about the exchange. The seller will let the buyer know if they have any non-standard terms (for example, a maximum limit on the buyer's first trade or a request to verify their identity), and both parties will come to a mutual agreement on how the escrow transaction is going to take place.

**STEP 4:** The buyer places the funds in the escrow transaction. This takes place with a transaction to a Binance Smart chain (with one click). The escrow transaction provides proof-of-funds to the buyer and allows for a much safer trade.

As soon as the XOE token is escrowed, a payment window countdown begins. The buyer is expected to initiate payment within this window, or else the seller will have the ability to cancel the escrow. This prevents the seller's funds from being locked due to an unresponsive buyer.

**STEP 5:** Knowing that the XOE tokens are in escrow, the buyer can allow the download of the product — if the seller doesn't get the discussed product offered, a dispute resolution process can assist them. Without the protection of escrow, the seller could simply vanish after the buyer sends money.

Once the buyer has received the product, they can terminate the payment window by clicking "Mark as Received". The seller no longer has an opportunity to cancel the escrow.

**STEP 6:**

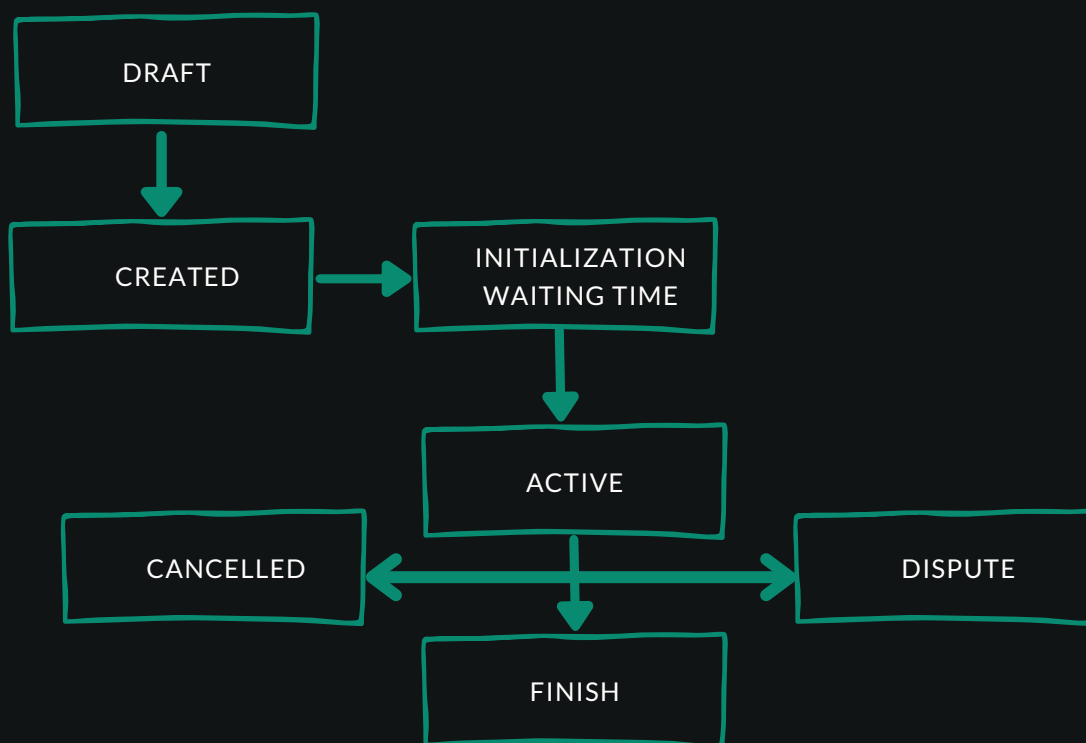
Scenario A: The seller successfully confirms the payment and releases the escrow. Trade complete! The XOE tokens are released from the escrow to the buyer and both parties are happy. Now each party can give each other feedback to contribute to a web of trust, which makes the platform safer.

Scenario B" Somebody raises a dispute. Either party can raise a dispute to call in a third-party arbitrator (currently Bitxoe staff) to make a resolution. The arbitrator is given two keys: one to decrypt the messages, and another to resolve the escrow.

The arbitrator may ask for evidence, such as proof of payment from the buyer, to help determine which party is the rightful owner of the XOE tokens. It might take minutes, hours, days or even weeks for them to reach a decision depending on the complexity of the dispute.

Once the arbitrator is satisfied one way or another, they can direct the ether in escrow to be released to one of the parties. The contract code doesn't allow them to send the ether anywhere else.

## ESCROW LIFECYCLE



The escrow transaction has the following states:

- **Draft:** An escrow transaction is in the process of being created; escrow in this state is not saved in the database.
- **Created:** the user has filled in all the necessary parameters. In this state, the escrow is first stored in the Database.
- **Initialization Waiting Time:** The escrow transaction is pending payment or initialization.
- **Active:** The escrow is activated and ready to be executed. Available features deposit and refund, and cancel the escrow by the creator.
- **Cancelled:** The escrow is cancelled by the creator of the transaction. The only function available is a refund.
- **Done:** The escrow was successful, funds are sent to the escrow creator.
- **Dispute** The terms of the escrow were not fulfilled by the buyer, the only function available is a dispute.

## PLATFORM ADVANTAGES

**EASY TO USE:** The platform is easy for anybody to use, no matter their background. The platform is built to work on all web browsers without any extra software, and it's not necessary to read this document to understand how to use the platform.

**RISK-FREE ENVIRONMENT:** While billions of dollars have been lost through unorganised buying selling systems. Users are in safe hands on Bitxoe as the platform never holds any XOE or direct involvement in the escrow transactions.

**FASTEST ESCROW PLATFORM:** The bitxoe enabling person-to-person payment methods allows super-fast buying-selling settlements – often less than five minutes.

**END TO END ENCRYPTION:** The platform leverages an end-to-end encryption scheme to protect messages in transit from eavesdropping by hackers and oppressive regimes.

**SETTING OWN TERMS:** The users can define their own terms and conditions of buying-selling their product and services and anyone will be interfering in this.

**OPPORTUNITIES:** Bitxoe allows you to start your own market and shop. The users will earn a daily income while selling the products and services through the bitxoe platform.

**IMMEDIATE SETUP:** Users can start an escrow transaction immediately after signing up to the platform. Since bitxoe is not a cryptocurrency exchange and we have no legal obligation to collect the identities of users.

**WIDE Reach:** Since the platform was launched in beta in the third quarter of 2020, it's already seen people in more than 45 countries. Soon there will be no other peer-to-peer escrow platform for cryptocurrencies with more users than bitxoe.

Bitxoe to accelerate worldwide adoption of cryptocurrency, for the aforementioned reasons.

## DESIGN SPECIFICATIONS

Before stepping into the specification, we should understand why some decisions were made over others. As will be better explained later, Bitxoe isn't completely decentralised, however, this fact doesn't mean the platform isn't safe from hacking, surveillance, and censorship.

Long before the development of Bitxoe began, its creators laid out a set of rules that the platform must follow. These are the principles we decided must be characteristics of the finished product to ensure a frictionless experience. Each design requirement below has been met:

**Extreme Portability:** Bitxoe must work in all modern web browsers without extra software. Needing to install a browser extension is a big hurdle for users who aren't tech-savvy, or who don't trust third-party software on their device.

Also, relying on external software creates device-compatibility issues and could pose security threats outside of Bitxoe's control.

**Multi-device synchronicity:** Bitxoe should work seamlessly across many devices. People trade on the go, especially when dealing with different products and services. The platform needs to work on desktops, laptops, tablets, and phones at the same time.

**Asynchronous:** Users must not need to be online to accept a new trade or receive an encrypted message. This means that secure information must be able to be exchanged entirely asynchronously. To accomplish this, it's necessary to have somewhere to reliably store encrypted data and allow users to retrieve it later.

**Expectancy of crypto-bankruptcy:** Users must not need any ether in their wallet to use any part of Bitxoe. This requires some trickery because every interaction with the blockchain costs ether as payment for computational work.

The Bitxoe platform will be many people's first interaction with cryptocurrency, so we expect many buyers to lack any ether at all, which means they won't be able to interact with smart contracts at their own expense. Because of this, Bitxoe has a system allowing users to interact with the blockchain at no up-front cost via a proxy mechanism.

**Self-explanatory UX:** Users shouldn't need to read the technical documents to understand how to use Bitxoe. While every decentralised service has a duty to educate users on the basics of distributed ledger technology, we recognise that the majority of the general public is probably not going to understand every detail, and that shouldn't matter. Lots of effort is going towards making sure the user interface is friendly for all users, no matter their background.



## HYBRID DE[CENTRALIZATION]

Bitxoe is not a completely decentralised system. Instead, it's a blend of centralised and decentralised components to construct a cocktail of security and usability. Bitxoe is centralised in the same way that end-to-end encrypted instant messaging apps Signal, Telegram, Wickr, Viber and WhatsApp each rely on centralised servers.

The decision to avoid a full decentralised system is to be able to meet all of the important design constraints described above. Many of these constraints will become less of an issue in the future as the world transitions to decentralisation; the long-term goal is to decentralise more components over time as the Binance Smart Chain ecosystem matures.

For the purposes of explaining the whole project, our design is split into three components. You'll notice that this document has been divided by each system fits into these categories:

- The Centralised layer, which includes web 2.0 – they don't involve cryptography or distributed technology. The Centralised layer is mainly used to store and transport encrypted payloads and metadata. The centralised layer is made up of our API, servers and databases. It's important to note that Bitxoe is carefully designed so that no sensitive information is disclosed to the centralised layer.
  - The Bitxoe system keeps in mind that centralised systems can be compromised or replaced. For example, the front-end won't display any messages unless the sender signature is valid, and no funds can be stolen in the event of a hack.
  - What to expect:
    - E-mails & SMS notifications
    - Offers
    - Bans & anti-spam
    - Storage and transport of encrypted blobs
- The Cryptography layer, which includes secure things protected by cryptographic algorithms such as end-to-end encryption. The Cryptography layer is used to secure and verify all kinds of sensitive information.
  - This includes, for example, signing and encrypting messages between users, creating digital signatures for various purposes, unlocking encrypted wallets and signing transactions. These computations happen off-chain in the web browser using the Web Crypto API.

## HYBRID DE[CENTRALIZATION]

- What to expect:
  - Diffie-Hellman key exchanges
  - Encrypted messages
  - In-browser ether wallet
- The Blockchain layer, which includes immutable things on the Binance Smart Chain such as the escrow contract. The Blockchain layer involves anything to do with the blockchain. This includes any interaction with our smart contract(s). In the first version, LocalEthereum only uses the public Ethereum blockchain.
  - What to expect:
    - Escrows via a smart contract

## AN IMPORTANT QUESTION

Q: Why don't we use the blockchain for the entire system?

A: The Bitxoe platform currently only uses blockchain technology where its application is helpful and the pros outweigh the cons.

The term "blockchain" has become a mostly meaningless buzzword. To answer this question, it's worth recounting what blockchain solves and where it might be inappropriate. A blockchain is an immutable public ledger. Blockchains let us agree on the order of a set of records without trusting a central authority. The introduction of blockchain technology solved the double-spending problem of digital cash and paved the way for the cryptocurrency boom we know today.

Blockchain technology has proven to be a tremendous invention, but it was never meant to be the be-all-end-all to security. The underlying mechanisms that Ethereum and Bitcoin use to verify and secure information (known as Elliptic-curve cryptography) were invented decades earlier.

When there is an advantage to having a public immutable record of something, blockchain is the answer. When there no benefit, it doesn't make much sense to use a blockchain. When this is the case, stand-alone cryptography is the solution to your problem. In fact, adding blockchain into the mix only creates new problems:

- Erosion of privacy (everything on the blockchain is public)
- Cost (every change to the ledger involves a transaction fee)
- Untimeliness (transactions can take minutes or longer to propagate)

## VALUE CREATION

Bitxoe token creates value through its escrow marketplace and captures some of the value generated on the platform by entitling token holders to use the XOE token during each and every escrow transaction, assuming these entities contribute to the network and stake XOE.

This model provides clear incentives to hold XOE tokens over the long term, significantly reduces velocity and adds genuine utility. In time, the transaction volume should increase, helping to create a thriving ecosystem in which the goals of investors, asset providers, consumers and the bitxoe team and advisors are aligned. The XOE token will also increase user retention and lower user acquisition costs. In addition, it will incentivise users to generate more revenue for the platform by buying and providing more computing power and by recruiting other users.

## TOKEN DISTRIBUTION

Bitxoe is partnering with accredited companies to implement best practices for all security and regulatory processes. A leading smart contract auditor has been appointed to ensure the code governing the XOE token is free of bugs and works as intended.

Treasury and future allocated tokens will be stored with a trusted and insured third party. This will provide oversight for token distribution, and ensure secure storage for all tokens and capital.

## TOKEN SECURITY

Bitxoe is partnering with accredited companies to implement best practices for all security and regulatory processes. A leading smart contract auditor has been appointed to ensure the code governing the XOE token is free of bugs and works as intended.

Treasury and future allocated tokens will be stored with a trusted and insured third party. This will provide oversight for token distribution, and ensure secure storage for all tokens and capital.

## FUTURE DEVELOPMENT

This whitepaper is the first draft and will be updated in the future. While maintaining the current version, the Bitxoe team is continuously working on the platform development. Especially as the ecosystem surrounding Binance smart chain improves, components of Bitxoe where there still remains some elements of trust will be replaced in the near future.

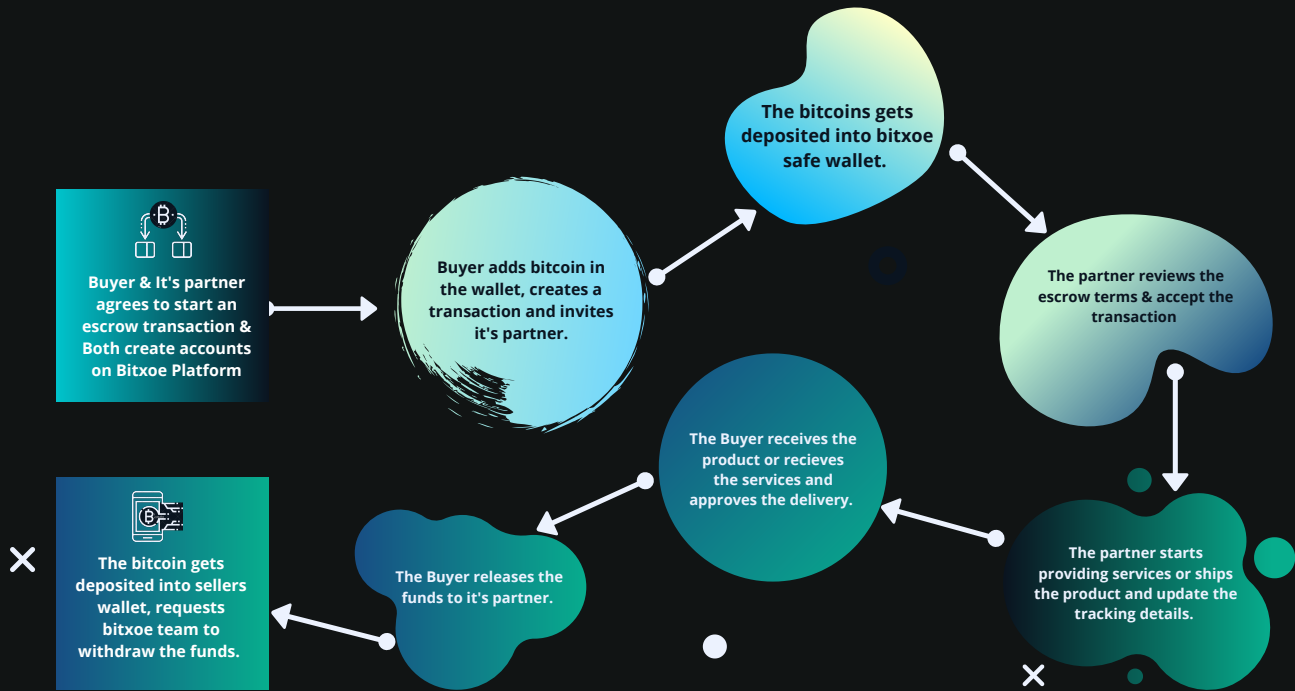
Some of the features we're currently investigating include:

- Integration of third-party wallets (e.g. MetaMask, Binance Chain, Mist, wallets).
- Decentralised escrow arbitration.
- Native mobile applications

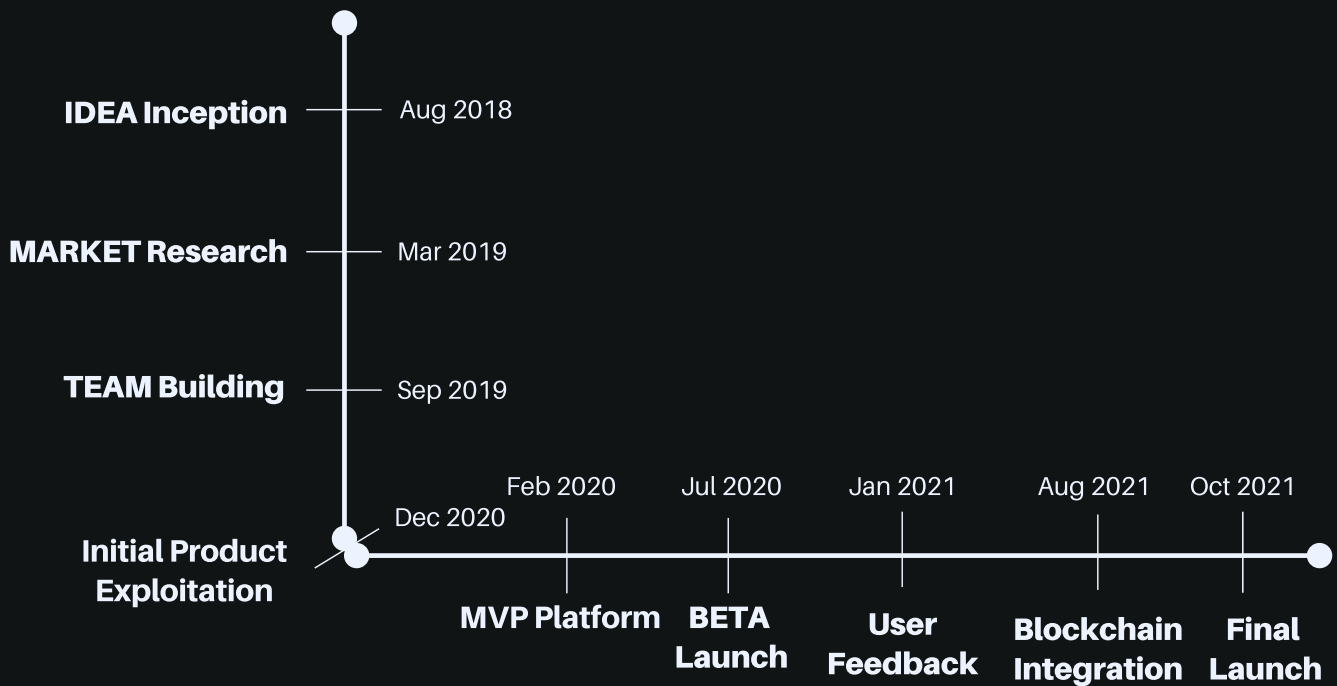
Lastly, thank you for reading the whitepaper.

Published on April, 2021.

## BITXOE ECOSYSTEM



## ROADMAP



## THE CORE TEAM



### **Devashish Biswas**

Founder / CEO, - Marketing / PR / Product Development

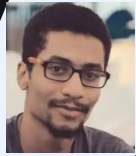
Experienced professional with years of experience in software development, digital marketing & public Relation. Sound knowledge of Blockchain technology and leader in sales & partnership, has a good network in crypto community.



### **RANJIT SINGH**

CTO / Product Development

13 year of experience in software development, database management along with information system security. He has been excellent technical consultant with extensive experience as Robotic Process Automation (RPA) Developer. BluePrism Accredited Developer



### **Arsalan Ahmed**

Software Developer

4+ Year o experience in software Development, Deep knowledge, problem solver, energetic



### **Ramika Batra**

Marketing & Partnership Manager

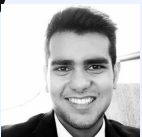
6+ Years of experience in , partnership and expert in client retainion



### **Ritvik Sen**

Sales & Business Development

5+ Years of experience in the areas of business development, finance, marketing.



### **Ashish Sharma**

Legal & Trademark

Experienced Paralegal with a demonstrated history of working in the legal services industry. Skilled in Intellectual Property.

## LIABILITY DISCLAIMER

To fund the development of the bitxoe ecosystem, 1000,000,000 BEPS20 tokens [onward called XOE Tokens or Bitxoe Token) will be created on the Binance Smart Chain and get sold to the public. XOE token will allow the user to access and use the escrow transaction on the Bitxoe platform.

The information set forth herein may not be exhaustive and does not imply any elements of a contractual relationship. Its sole purpose is to provide relevant and reasonable information to potential XOE TOKEN Holders so they may determine whether to undertake a thorough analysis of the company with the intent of purchasing XOE Tokens.

Nothing in this White Paper shall be deemed to constitute a prospectus of any sort or a solicitation for investment, nor does it in any way pertain to an offering or a solicitation of an offer to buy any securities in any jurisdiction.

This document is not composed in accordance with and is not subject to laws or regulations of any jurisdiction, which are designed to protect investors. Bitxoe is not intended for sale or use in any jurisdiction where the sale or use of digital tokens may be prohibited. XOE Token confers no other rights in any form, including but not limited to any ownership, distribution (including but not limited to profit), redemption, liquidation, proprietary (including all forms of intellectual property), or other financial or legal rights, other than those specifically described in the White Paper.

Certain statements, estimates, and financial information contained in this White Paper constitute forward-looking statements or information. Such forward-looking statements or information involve known and unknown risks and uncertainties, which may cause actual events or results to differ materially from the estimates or the results implied or expressed in such forward-looking statements. This White Paper may be modified to provide more detailed information.

All Rights Reserved: No part of this document may be copied or reproduced without the express written permission of © Bitxoe.com