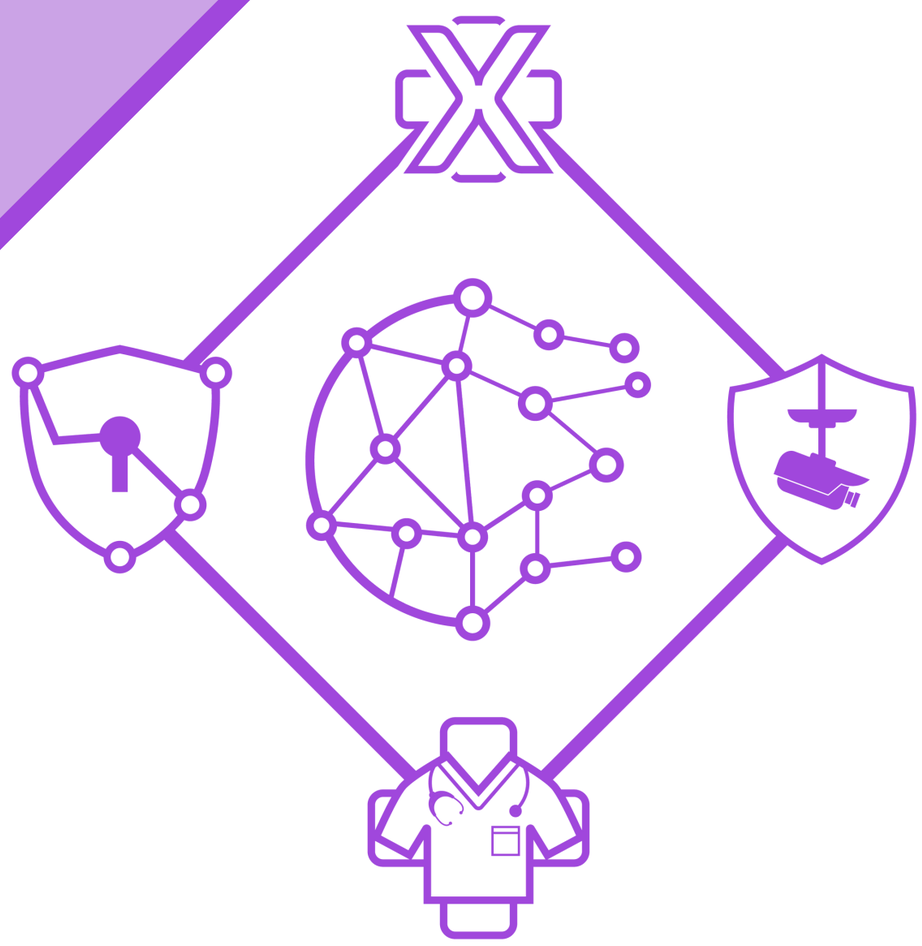


X-ID GLOBAL LLC

Giving you control of your data

X-ID GLOBAL LLC

WHITE PAPER

Table of Contents

Legal Disclaimer

It is requested to read this legal disclaimer section with full attention. This white paper does not bind any individual to enter into any contract or enter into any binding legal commitment to the contribution. This white paper also does not constitute any form or any part of any opinion which can be considered advice, or which can sell, or which can solicit any offer by Trillions to purchase our token nor shall it be considered a part of any effect which can be used for the formation of contract or investment decision.

This white paper also does not have any capacity to bind any person to enter into any contract or consider it a binding legal commitment to the contribution of the whitepaper. Even no sales and even no cryptocurrency or any other form of payment can never be accepted based on this white paper. But be sure that any advancement or any date or any new information about this token will be made available for the private and public contributors.

It is also announced that the white paper has not been examined by any regulatory authority and it has not been approved by any legal firm so the information given in this white paper cannot be taken under the laws or any regulatory authority or under any rules of any jurisdiction. It is hereby announced that its publication, its distribution, its dissemination do not imply the applicable laws, the regulatory requirements, and the available rules.

NO REPRESENTATION & WARRANTIES

The Tokens and the Available Information (including the Website and the White Paper) are supplied "as is" and without any explicit or implied claims or guarantees of any kind. You accept all responsibility and risk for your use of the Available Information and the purchase and usage of any quantity of Tokens. If applicable legislation prevents all or part of the foregoing limitation of responsibility from applying to you, the limits will only apply to you to the level permitted by law. X-ID makes no assurances or promises about the outcomes that may be attained by utilizing this white paper. No one should make an investment choice without first contacting a financial professional and completing their due diligence and research.

No Advice:

Nobody is obligated to sign a contract or make a legally binding promise to donate as a result of reading this white paper. This white paper also does not constitute any form or part of any opinion that could be construed as advice, or that could be used to sell or solicit any offer by our token, nor should it be construed as a part of any effect that could be used in the formation of a contract or an investment decision.

Limitation of liability:

X-ID takes no responsibility for any loss or injury coming from the use of this website's content, including written content, links to third-party websites, data, quotes, charts, and buy/sell signals.

Investment risks:

Cryptocurrency trading has a high level of risk and is not appropriate for all investors. Before trading cryptocurrencies, tokens, or any other digital asset, you should carefully consider your investment goals, degree of experience, and risk appetite.

Introduction

The continual changes in the digital revolution make it increasingly important every day to stay on top of the new requirements that we must meet in a world dominated by innovation and scientific progress. These changes and advancements make it imperative to take the next step in order to capitalize on the opportunities that each new innovation, discovery, or progress in any field of knowledge brings.

X-ID is a novel decentralized platform integrated with existing applications to store and transfer the personal data of users securely and effectually. The necessity for a more secure manner of storing and transferring people's personal data while offering the user complete access and control led to the creation of X-ID. Personal data storage is riddled with privacy and security concerns. Even the most well-known internet services have been victims of data theft and security breaches. When trust is placed in a centralized service provider for all data storage, it may be harmed by centralization concerns such as deleting user data on purpose or failing to send user data due to a technical failure.

The significant shift to remote employment during the pandemic presented a big new target for cybercriminals. Many employees working from home were utilizing unprotected personal smartphones and laptops during a pandemic. Financial services, health care, government, and retail employees have shown to be particularly appealing to fraudsters. During the COVID-19 outbreak, cybercriminals used tried-and-true strategies including phishing, social engineering, and other hacker tools to extort millions of dollars from organizations. X-ID tackles security issues of a user against hacking and data breaches by making sure to store their data in the decentralized system.

X-ID is an emerging platform that will be built on blockchain and has features of transparency and security, which we believe is crucial for long-term feasibility and decentralization. X-ID is a community-oriented platform that provides blockchain integration to people where they can save their data.

X-ID is creating an advanced and highly secured infrastructure to become an unstoppable decentralized data storage foundation for the world. The use of technology will facilitate and turn cyber networks more reliable and secure which will lead to a strong financially connected, empowered, and enabled society.

X-ID has Following Key Features:

Vision

X-ID aims to build a platform utilizing blockchain technology in conjunction with existing applications to build an effective infrastructure to maintain and deliver on-demand personal data giving them full control over their life. X-ID network constitutes an innovative ecosystem to attract more people to digital assets while maintaining their privacy, security, authority, and autonomy. Our objective is to increase secure global economic freedom. We envision a world where people can get a fast, sound, and authentic ecosystem through which users of X-ID can provide and store data to cyber networks undauntedly for their business.

X-ID Vision is Encapsulated With Three Main Components;

VISION STATEMENT

Community-Focused

More focused on supporting and caring for community

Innovation

To be the world's most crypto-centric platform

Wealth-Building

Embarking new wealth raising strategies worldwide

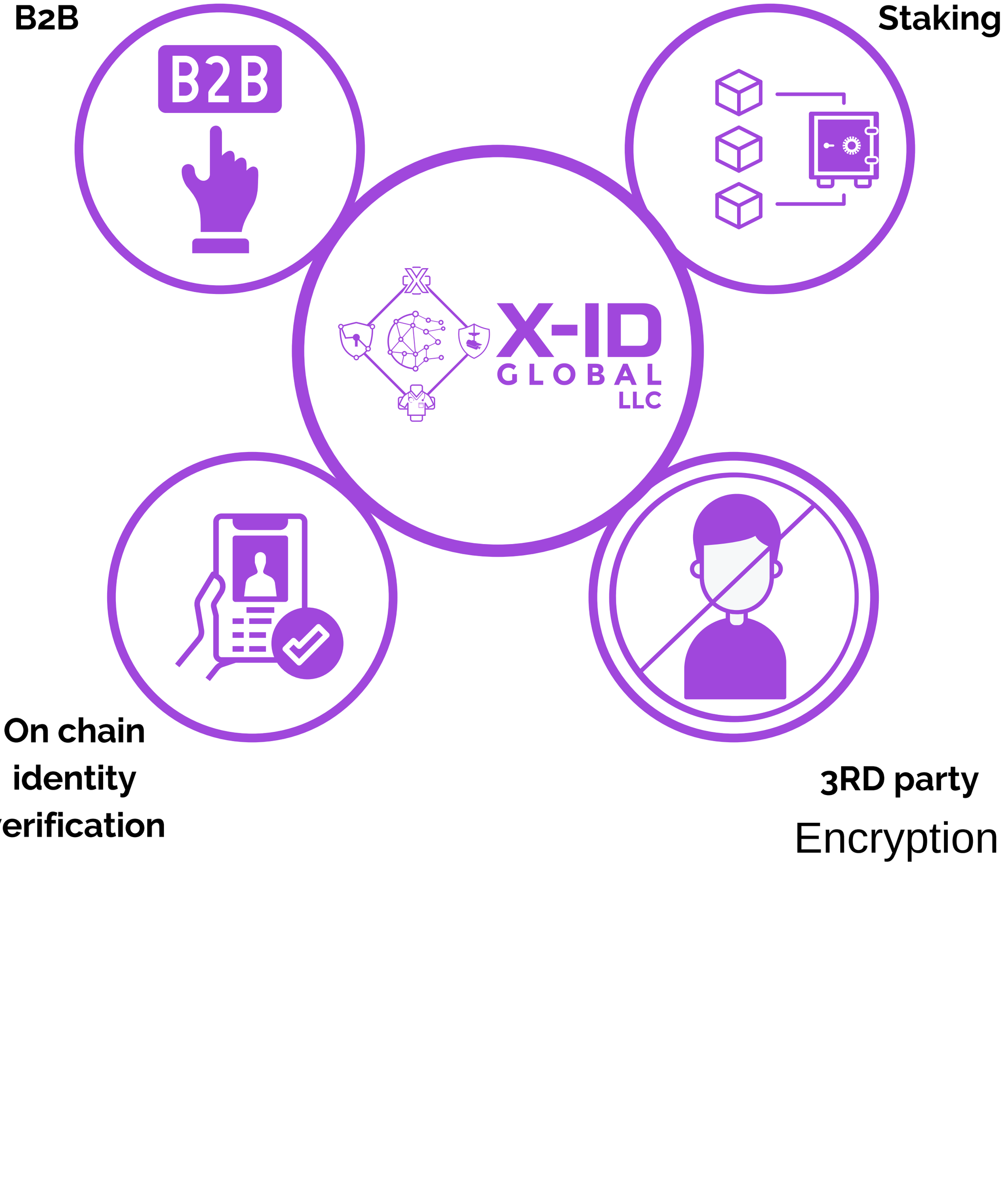
Mission

Our mission is to take "X-ID" to new heights by providing customers with a secure, innovative, user-friendly, one-stop-shop platform to give everyone in the world an equal chance to manage and improve their financial security. X-ID's future and mission are to integrate digital applications and other cyber networks with the X-ID platform which is an unlimited resource of high-end, exclusive, futuristic, sophisticated space to live and secure data to avoid cyber breaches and violations. We will focus to keep our users on board as long as possible by offering exclusive options. Our focus is to;

- Create a reliable, useful, and secure decentralized platform
- Make the cyber world a better place by providing secure and independent platforms to people.
- Our mission includes the creation of a next-generation complete all-in-one platform and giving every person in the world an equal chance to manage and improve their financial and Data security by using X-ID.
- Implementing innovative projects.
- Operate as a community-focused and community-driven digital asset, fully decentralized in every sense of the word.

MISSION

Ecosystem


B2B
Staking
X-ID
GLOBAL
LLC
On chain identity verification
3RD party
Encryption

Staking

X-ID works on the secure Blockchain, which is working on a proof of certification. It offers exemplary staking services. By utilizing comprehensive security methods and offering a Secure Asset Fund for users, X-ID assures that users' money is protected (SAFU). At the time of writing, our staking technique is undoubtedly one of the safest and most environmentally friendly ways to make passive income. The platform uses a secure wallet and a double-checking method to hold all staked tokens.

The staking contract is written in a way that prevents inflation. When more and more people will stake X-ID, the contract will automatically reduce the coins it gives. As more people, especially institutional investors, recognize the crypto market's profitability and efficiency, staking is gradually becoming a method of obtaining passive income by simply staking or locking funds in a wallet. Companies that stake tokens to gain API user access and information will have a 25% rate that can be adjusted by end-user votes. The tokens that are generated at a 25% rate will be used to pay end users for access to the data. If a company folds or no longer wants access to end-user data, the tokens they do have left will be returned back to X-ID Global to use as they see fit.

Since holding cryptocurrencies necessitates certain technological crypto know-how and compliance criteria, X-ID staking platforms are useful for allowing investors, including those lacking technical knowledge of cryptocurrencies, to hold proof of stake (PoS) tokens and receive rewards. In response to the tremendous increase in crypto staking, staking platforms that allow investors to receive staking incentives have sprouted up. If you're interested in earning a passive income by staking, this is the place to be.

Benefits of Staking

NO HARDWARE IS REQUIRED

Unlike proof of work, there is no need for specific equipment or hardware for crypto holding. Proof that staking works without the need for any special equipment. The only requirement is to Stake the TOKENS for an interval of time by the holders on any exchange or dapp.

PASSIVE INCOME

Stakeholders earn incentives by Staking and controlling their digital wealth. The incentive for keeping is passive income for the recipient.

SCALABILITY

Scalability is a term that is frequently used in the Blockchain ecosystem. It refers to a computational process's potential to be use do generate in a variability of ways. Proof of stake protocols, as shown by X-ID in higher transaction outputs and lower fees, make for greater scalability.

ECO-FRIENDLIER

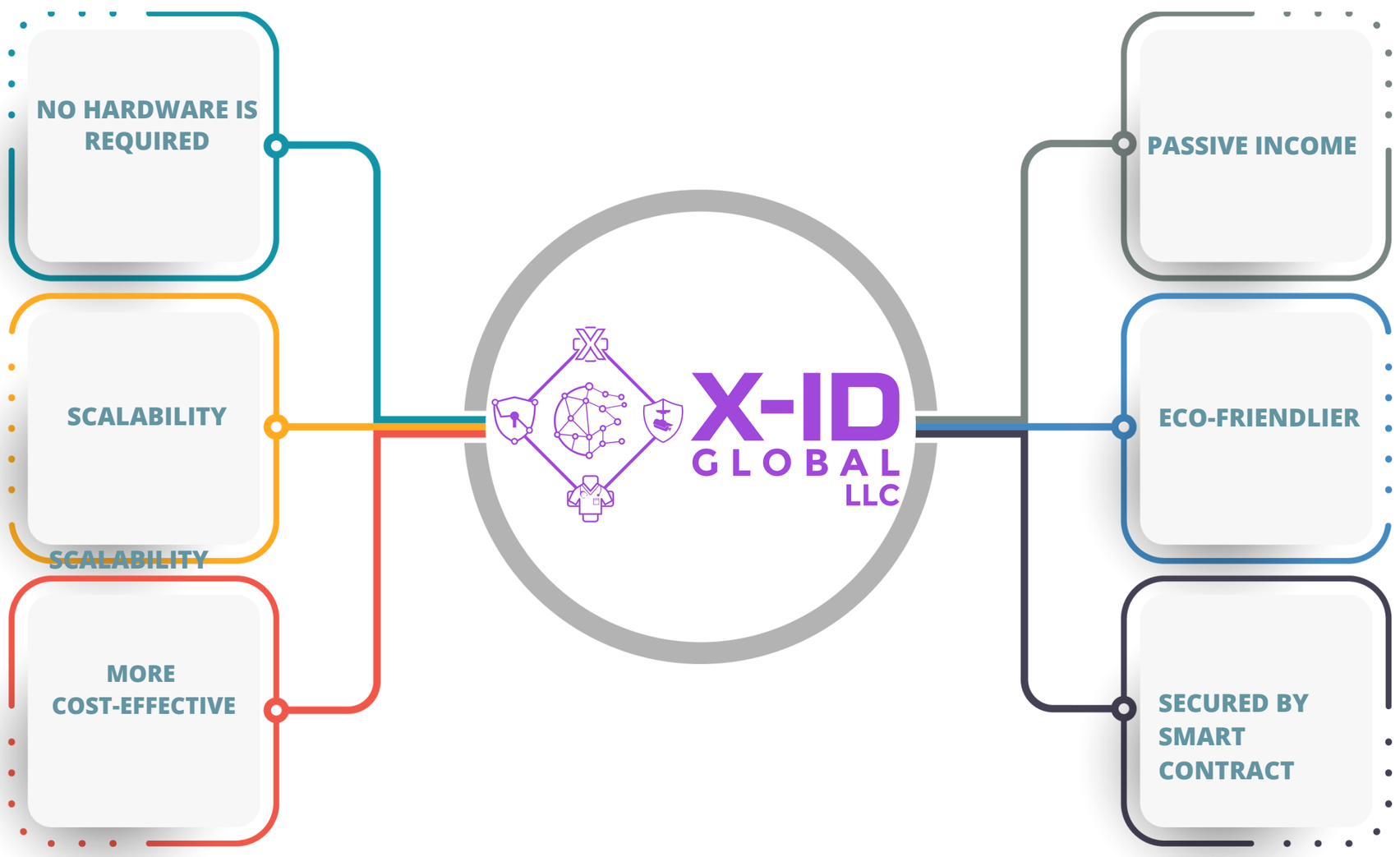
One of the major benefits for Staking Token is that it dont needs continuous supply of energy to validate the Transaction. As a result, it is environmentally friendly.

MORE COST-EFFECTIVE

Proof of stake blockchains are usually low-cost and low-energy systems that don't require any special or expensive hardware. PoS is less expensive and less harmful to the environment than proof-of-work chains.. So, the stackers can earn more passive income by using the X-ID platform.

SECURED BY SMART CONTRACT

The biggest issue in the modern world is security and privacy, and X-ID provides a swift and stable portal that is backed by the X-ID ecosystem making him superior to others. X-ID is offering a highly secure and fast platform to the users for holding crypto.

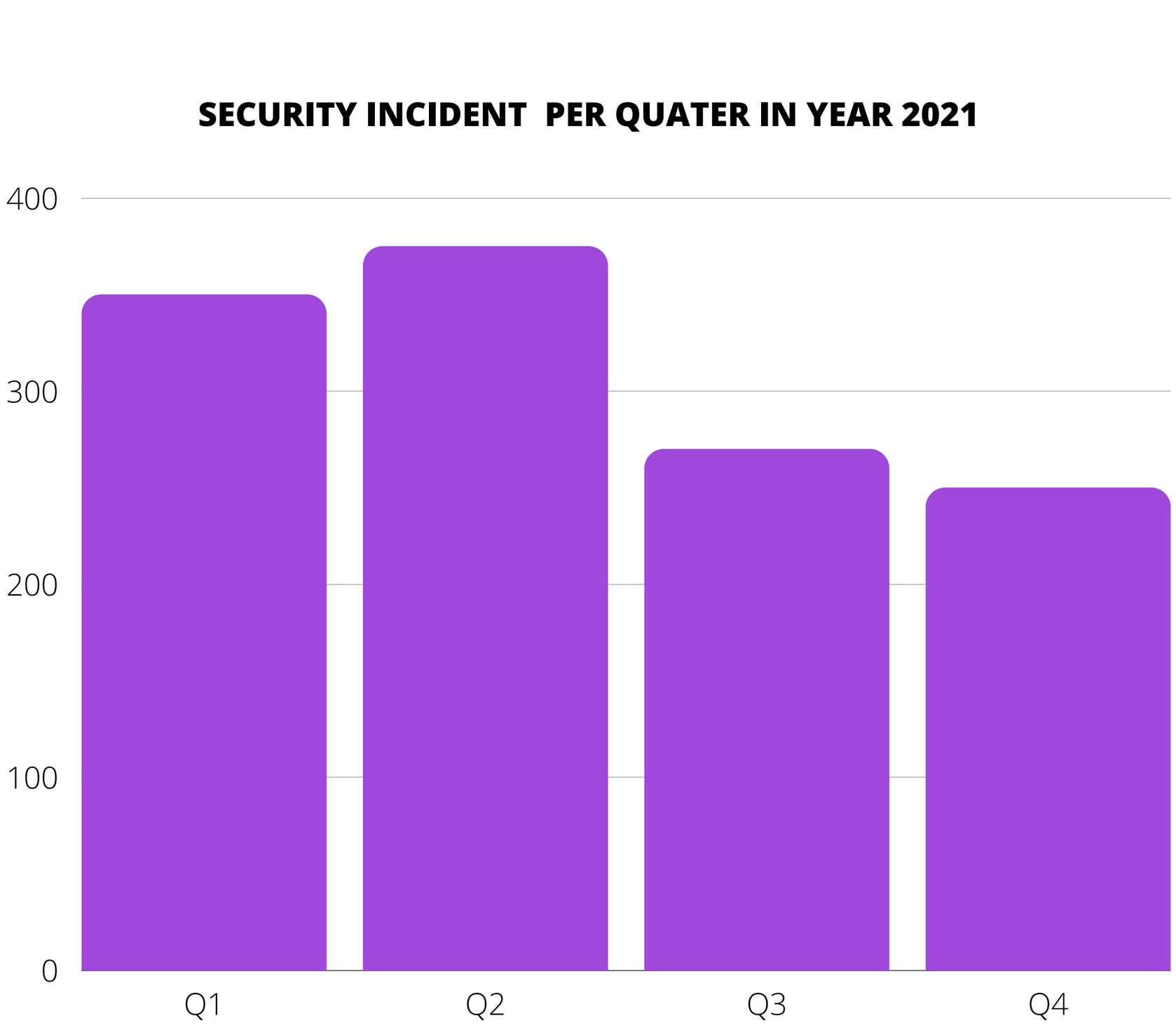


Data breaches in 2021

In 2021, IT Governance found 1,243 security incidents, aggregating 5,126,930,507 records breached. In comparison to 2020, this leads to an increase of 11% in security incidents (1,120). Over the same period, however, the number of records breached declined substantially (20.1 billion).
However, it's worth emphasizing that, in the vast majority of situations, the organization does not publish the number of records affected, either because it doesn't know or because it isn't obligated to do so. As a result, the true number of records breached will be far larger.

Meanwhile, it has long been believed that the pandemic will have a severe impact on businesses' cyber security procedures, with some referring to the data protection hazards associated with remote working as evidence.

We discovered 727 publicly known security events in the first six months of the year. Around this time, countries all around Europe began to loosen their restraints. On July 19, the United Kingdom celebrated 'Freedom Day,' with the repeal of social separation and mask laws, while similar decisions were made at the state level in the United States.
These decisions coincided with a drop in the number of data breaches in the second half of the year, with only 515 publicly known cases detected.



Challenges of Database validation

An accurate and compliant database helps avoid pitfalls, personalize customer journeys, and streamline sales and marketing campaigns. However, maintaining database integrity for the sales and marketing team can be challenging for multiple reasons. Delving deep into the challenges of data validation and quantifying its impacts can help organizations improve their bottom line. Let's look at some of the recurring challenges that B2B enterprises face with their data validation processes:

Lack of data standardization and duplication:

One of the key issues with B2B organizations is that they lack data standardization, validation of documents, and uniform data storage guidelines. Data comes from a variety of sources and gets integrated into the CRM. This is further exacerbated since data lives in silos. Often enough, the companies don't have a robust deduplication engine, leading to duplicate data being stored in the system.

Absence of automated tools:

Another critical challenge with data validation is the non-implementation of AI-based data validation engines. the database requires automated tools to validate the database with Natural Language Processing capabilities to keep the data refreshed and relevant. Manual validation of data leads to errors and repetitions within the database.

Lack of expertise in database management systems:

One of the fundamental challenges of database validation is that companies don't have expertise in data maintenance and management processes. They leave their marketing and sales team to shoulder the responsibility of data validation manually. This leads to the storage of irrelevant and stale in the system. Often, teams within the organization don't understand the business use case of data validation and struggle to associate a business cost with their data quality programs. It becomes difficult to prove a return on investment to business leaders.

Solutions of database validation

We propose a new blockchain-based platform for user modeling that allows users to share data while maintaining control and ownership. Our new platform addresses three major issues: ensuring user privacy and control, as well as providing sharing incentives. It keeps track of who shared what, when, with whom, how, and why. To ensure that all participants act honestly, the smart contract imposes double deposit collateral. In all of our cases, the node responded quickly and at a reasonable transaction cost.

When managing your network, developing an app, or even organizing paper files, sound security is no accident. Companies that consider security from the start assess their options and make reasonable choices based on the nature of their business and the sensitivity of the information involved. Threats to data may transform over time, but the fundamentals of sound security remain constant. As the Federal Trade Commission outlines in Protecting Personal Information: A Guide for Business, you should know what personal information you have in your files and on your computers, and keep only what you need for your business. You should protect the information that you keep, and properly dispose of what you no longer need. And, of course, you should create a plan to respond to security incidents.

There's another great source of information from the FTC about keeping sensitive data secure: the lessons learned from the more than 50 law enforcement actions the FTC has announced so far. These are settlements—no findings have been made by a court—and the specifics of the orders apply just to those companies, of course. But learning about alleged lapses that led to law enforcement can help your company improve its practices. And most of these alleged practices involve basic, fundamental security missteps. Distilling the facts of those cases down to their essence, staff from the FTC's East Central Region present in this article five lessons that touch on vulnerabilities that could affect your company, along with practical guidance on how to reduce the risks they pose.

1: Start with security

From personal data on employment applications to network files with customers' credit card numbers, sensitive information pervades many companies. Experts agree that the first step in managing confidential information is to start with security. Factor it into the decision-making in every department of your business—personnel, sales, accounting, information technology, etc. Collecting and maintaining information "just because" is no longer a sound business strategy. By making conscious choices about the kind of information you collect, how long you keep it, and who can access it, you can reduce the risk of a data compromise down the road. Of course, all of those decisions will depend on the nature of your business.

2: Control access to data sensibly

Once you've decided you have a legitimate business need to hold on to sensitive data, take reasonable steps to keep it secure. Not everyone on your staff needs unrestricted access to your network and the information stored on it. For your network, consider steps such as separate user accounts to limit access to the places where personal data is stored or to control who can use particular databases. For paper files, external drives, disks, etc., an access control could be as simple as a locked file cabinet. Administrative access, which allows a user to make system-wide changes to your system, should be limited to the employees tasked to do that job.

Solutions of database validation

3: Require secure passwords and authentication

If you have personal information stored on your network, strong authentication procedures— including sensible password “hygiene”—can help ensure that only authorized individuals can access the data.

Insist on complex and unique passwords

“Passwords” like 121212 or qwerty aren’t much better than no passwords at all. That’s why it’s wise to give some thought to the password standards you implement. For example, you can require employees to choose complex passwords and train them not to use the same or similar passwords for both business and personal accounts.

Store passwords securely

Don’t make it easy for interlopers to access passwords. Three of the FTC’s settlements in this area have alleged that:

- The company stored network user credentials in the clear, readable text that helped a hacker access customer credit card information on the network;
- The business allowed customers to store user credentials in a vulnerable format in cookies on their computers; and
- A company failed to establish policies that prohibited employees from storing administrative passwords in plain text in personal email accounts.

In each of those cases, the risks could have been reduced if the companies had policies and procedures in place to store credentials securely. Businesses also may want to consider other protections—two-factor authentication, for example—that can help protect against password compromises.

Guard against brute force attacks:

Remember that adage about an infinite number of monkeys at an infinite number of typewriters? Hackers use automated programs that perform a similar function. These brute force attacks work by typing endless combinations of characters until hackers lock into someone’s password. Implementing a policy to suspend or disable accounts after repeated login attempts may help to eliminate the risk of brute force attacks.

Protect against authentication bypass:

Locking the front door doesn’t offer much protection if the back door is left open. In one settlement, the FTC charged that a company failed to adequately test its web application for widely-known security flaws, including one called “predictable resource location.” As a result, a hacker could easily predict patterns and manipulate URLs to bypass the web app’s authentication screen and gain unauthorized access to the company’s databases. The company could have improved the security of its authentication mechanism by testing for common vulnerabilities.

Solutions of database validation

4: Store sensitive personal information securely and protect it during transmission

Use strong cryptography to secure confidential material during storage and through all phases of transmission. The method will depend on the types of information your business collects, how you collect it and how you process it. Given the nature of your business, some possibilities may include Transport Layer Security/Secure Sockets Layer (TLS/SSL) encryption, data-at-rest encryption, or an iterative cryptographic hash. Make sure the people you designate to do that job understand how your company uses sensitive data and have the know-how to determine what's appropriate for each situation. Several companies have unnecessarily risked attacks that could have been prevented if the companies' implementations of SSL had been properly configured.

When considering what technical standards to follow, keep in mind that experts may have already developed effective standards that can apply to your business, including widely-accepted encryption algorithms. Savvy companies don't start from scratch when it isn't necessary and could subject data to significant vulnerabilities if deviating from tried-and-true industry-tested and accepted methods for securing data.

5: Segment your network and monitor who's trying to get in and out

When designing your network, consider using tools like firewalls to segment your network, thereby limiting access between computers on your network and between your computers and the internet. Another useful safeguard: is an intrusion detection and prevention tool to monitor your network for malicious activity.

6: Offers Encryption and Validation

X-ID is proficient enough to manage everything so that data has not been altered in any way. X-ID is encrypted by nature which makes it possible to provide proper validation. Smart contracts can be used with X-ID to ensure that certain validation happens when certain conditions are met every time. If in any case, someone does change a data, all the ledgers on all the nodes in the network verify that change is done.

7: Offer Secure Data Storage

X-ID is the best way to secure the data of the shared community. Utilizing the capabilities of the X-ID nobody can read or interfere with any sensitive stored data. It is helpful to handle the data that is distributed across a network of people. Moreover, the technology could also be useful in public services to keep public records decentralized and safe. Apart from that business model can save a cryptographic signature of a data or huge form of data on an X-ID. This would allow users to remain to ensure that the data is safe. X-ID is used in distributed storage software where huge data are broken down into chunks. This is available in encrypted data across a network in a way that means all data is secure.

8:Unfeasible to Attack

Talking about X-ID it is unfeasibly hard to hack or attack. X-ID is decentralized, encrypted, and cross-checked which allows the data to remain strongly backed. As X-ID is fully loaded with nodes to hack most of the nodes concurrently is impossible. Being one of distributed ledger technology its most fundamental attributes are data immutable. It offers a whole new level of succeeding security where any action or transaction cannot be altered or counterfeit. This technology valid every transaction to get confirmation from multiple nodes on the network.

Security Protocols

There are three types of identification that are used in security protocols for authentication purposes. It is either something the user knows or has in their physical possession. One or combination can be used in conjunction with each other to accomplish authenticating.

Core Principals:

Something that you know:

These include things like usernames, passwords. PIN, and answering security questions.

Something that you have:

These are the physical items that you have in your possession such as yubikeys, badges with RFID chips, smart cards, and smartphones.

Something that you are:

This covers biometric data, like fingerprints, voice, and facial recognition.

Layers of Authentication

a.Normal authentication – requires only one means of authentication such as using a PIN to unlock your smartphone.
b.Two-Factor – require the use of two or more means of authenticating such as using a password in conjunction with a yubikey. Even the use of your bank card with a PIN and chip.
c.Multi-Factor – This uses multiple means of authenticating such as username, password, and facial recognition to gain access to a system.

What sets X-ID apart from everyone else

We use a combination of all these methods and more to accomplish the most secure platform for keeping user data integrity. Using blockchain as the platform to accomplish this is the most effective and secure means to protect the end user's data.

Process of Authentication

Once each level of user information is validated using secure/trusted third-party software, the information is automatically stored on its respective token using a uniquely generated ID at the time of inception. This information is not publicly available or available on any public system after the check had been confirmed. Any request for users' information must be validated and approved by the user before any information is released. The user is notified by email or phone app and must be approved.

Once the approval by the end-user is given, a fourth token is used to validate data integrity to ensure that no unauthorized changes have been made. The token would also be utilized to validate the requesting company to ensure valid requests. Take note that once permission is given to an entity by the user, verification does not have to be given again. Also, the user will have the ability to revoke access and a notification will be sent to the respective company. Companies would have to sign up under an enterprise account to participate in the program and have access to user data. The company would have to be thoroughly verified to participate and must adhere to strict standards to ensure that security is held as the top priority. They would need use to use tokens to pay for the transactions. Companies will have to purchase API (Application Programming Interface).

The tokens are required for staking purposes and are needed to earn gas which is used to request access to user information as well as for invoking smart contracts that are in place. A small fee will be paid to the company. The rewards will be based every week.

Why choose X-ID?

Transparency & Immutability

With X-ID, each time exchange of coin is recorded on the blockchain, an audit trail is present to trace where the coin came from. This can not only help improve security and prevent fraud in exchange-related businesses, but it can also help verify the authenticity of the traded assets.

Lower Fees and Security

The fees associated with X-ID transactions are far less than those associated with debit, credit cards as well as wire transfers, and BACS payment.

Transaction Traceability

X-ID is far more secure than other record-keeping systems because each new transaction is encrypted and linked to the previous transaction. X-ID is formed by a complicated string of mathematical numbers and is impossible to be altered.

Ease to use

Ease of use is the reason why X-ID has value. All you need is a smart device, an internet connection and instantly you become your own payments and money transfers.

Safe & Secure

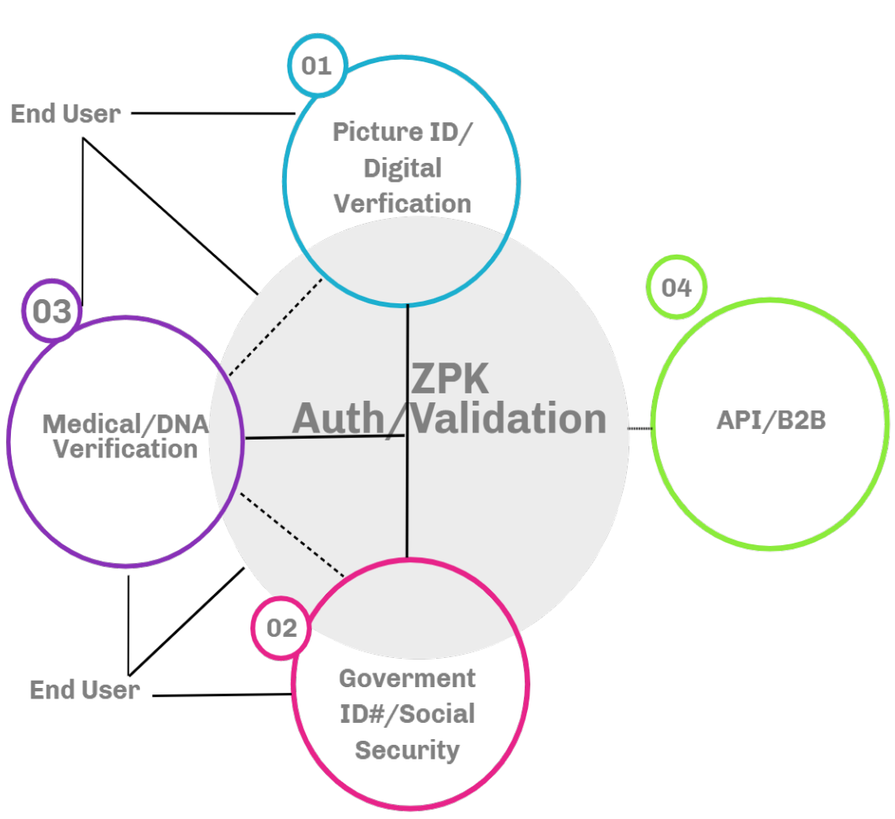
X-ID is a safe and secure platform which is audited and our technical team is continuously improving the security of the system to ensure the safety of platform.

Open for global participants

X-ID facilitates the transaction and brings them closer to a wider audience. An added benefit of X-ID use is that it's completely decentralized, so trading can be done freely across borders. The use of technology will facilitate a financial revolution that will leave everyone more financially connected, empowered, and enabled. X-ID has no border so these can be used no matter where you are located globally. This also has a huge effect on international payment fees. Traditionally international transfers have much higher fees than domestic transfers and payments. International payments and transfers with crypto are the same as domestic.

Tokenomics

TOKEN DETAIL



NAME

X-ID

SYMBOL

X-ID

Blockchain

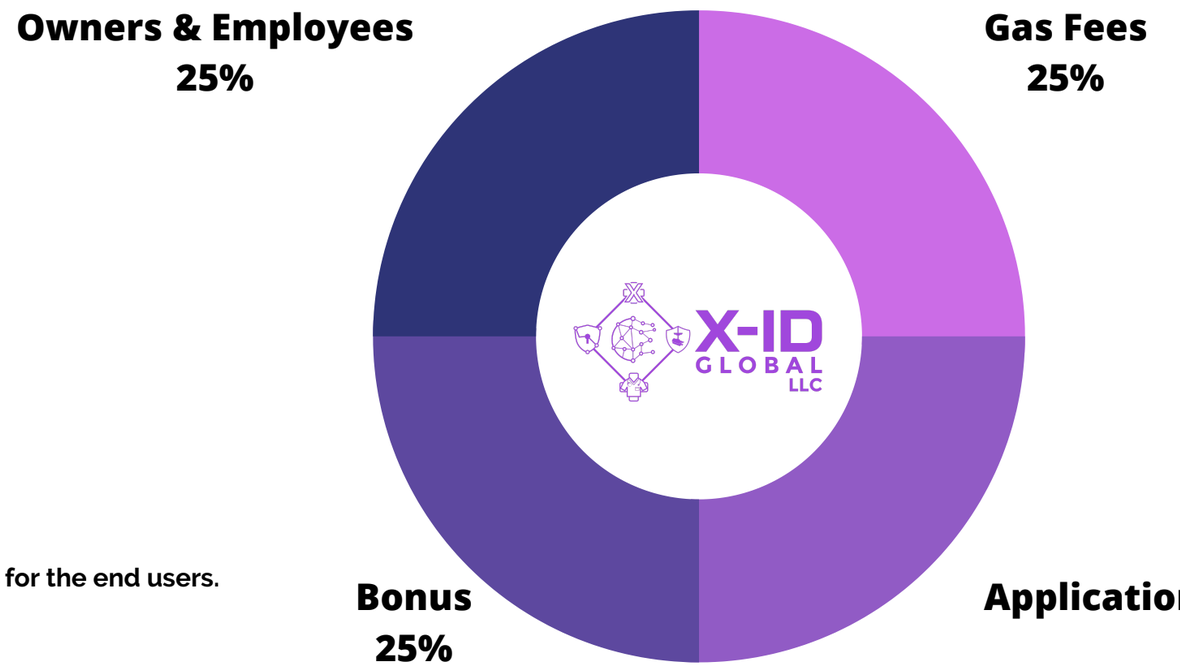
X-ID Blockchain

Total Supply

31,709,116,868,000 Token Launched at launch

TOKEN DISTRIBUTION

Users who do not validate their information in the system after a 5-year period from the start date of the launch will not gain the benefits of the 4000 tokens incentive. Those tokens will be given back to the system pool so it can be used in the following ways.



Gas Fees

25% of the tokens will be used for all gas fees

Application Development

25% will be used by the company to further develop applications for the end users.

Bonus

25% will be given as a bonus to all end users who validated their information before the 5-year period.

Owners & Employees

25% will be given back to the company owners and employees.

RoadMap

2023

Q2

- Open Source X-ID.com Launched
- X-ID.com open to all participants
- Identity Validator Toolkit built

Q3

- Validator Functionality Expansion
- First X-ID.com IDV Toolkit operational with government ID document, email and phone validation
- Validators can set fiat prices that are automatically converted to xid in their identity.com processes
- Identity Validators can offer their validation services directly to Requesters in a B2B solution
- MVP SDK available for select Identity Validators & Identity Requestors on X-ID.com

Q4

- X-ID.com Growth and 3rd Party Validator Integration

2024

Q1

- Expansion of Decentralized Identifiers (DIDs)
- Establish the SOLID DID method on Harmony and ZPK
- Use Harmony and ZPK as a low-cost, Layer-1 storage solution for DID documents
- Explore multi-device identity profiles and secure account recovery
- End-to-end encrypted credential sharing using DIDs

Q2

- Marketplace v2 on Harmony
- Enable low-fee micropayments for compensating credential issuers with xid
- Enable passive payment of xid for Validators

Q3

- On-chain Identity Verification
- Enable identity checks with on-chain smart contracts while maintaining user privacy with ZPK