authon

Whitepaper

Version: 20230910-10

Table of Contents

Introduction

1.1 Summary

In an ever-evolving digital world, the process of authenticating and standardizing certificates and diplomas remains tedious and complex. As of 2022, Authon emerges as a transformative Web3 decentralized application, designed to streamline and simplify the authentication and validation of a variety of digital assets. Primarily, Authon focuses on identification assets, certificates, diplomas, and even NFTs, establishing a platform where individuals can securely manage and validate these essential digital documents.

The fundamental underpinning of Authon is its unwavering commitment to true decentralization, impartiality, and inclusivity, ensuring accessibility to users, regardless of their blockchain expertise. What sets Authon apart is the robust integration of biometric security, transforming individual biometric data into a unique, encrypted blockchain identity. This unique approach adds an extra layer of security and personal ownership to digital identity management.

Central to the Authon ecosystem is the utility token, $AUTH. This token facilitates the notarization and storage of digital assets on the platform, with fees for these services dynamically calculated in $AUTH. Importantly, the platform ensures the validation of assets remains free for all users, promoting accessibility and widespread adoption. By incorporating dynamic fee calculation, Authon remains affordable and resistant to potential price surges, establishing a tokenomic model that balances the interests of users and institutions alike.

The Authon team is steadfast in its mission to solve not only the issues of today but also the challenges of the future. With Authon, validating the authenticity of a college degree or verifying the authenticity of personhood can be accomplished in seconds through a user-friendly mobile application. Transactions are secure, free, and do not necessitate a separate wallet, redefining the way we manage, authenticate, and validate digital assets in the age of blockchain.

1.2 Purpose

At its core, Authon is committed to securely and redundantly digitizing identities on the blockchain. An individual's identity comprises various elements, starting from birth certificates and national identity registrations and extending to the diplomas and certificates earned over time. Authon understands that as individuals grow, their identities evolve and diversify, necessitating a dynamic and secure digital management system.

Employment history, financial transactions, legal documents, and passports are all essential components of an individual's identity, serving to validate their persona for various requirements. Authon aims to offer a comprehensive platform that strives to securely store and link these documents to a unique, biometrically-secured blockchain identity, and also aims to enable seamless authentication.

In a nutshell, Authon spearheads the digital transformation of an individual's most valuable asset - their identity. It presents a secure and user-friendly solution that respects the diversity and complexity of individual identities, heralding a new era in digital identity management.

1.3 Avalanche

Avalanche is the open-source blockchain platform that Authon runs on. It allows launching decentralized applications and enterprise blockchain deployments in one interoperable, highly scalable ecosystem. Avalanche is among the notable decentralized smart contracts platforms built with the goal of accommodating the scale of global finance, and it offers near-instant transaction finality.

Avalanche consensus combines the benefits of Nakamoto consensus (robustness, scale, decentralization) and all the benefits of Classical consensus (speed, quick finality, and energy efficiency) without the disadvantages. Over time, people have come to a false understanding that blockchains have to be slow and not scalable. The Avalanche protocol employs a novel approach to consensus to achieve its strong safety guarantees, quick finality, and high-throughput.

1.4 The Problem

1.4.1 HR Document Validation

Recruitment process in many industries is rife with forgeries, ranging from counterfeit diplomas issued by non-existent educational institutions to altered documents from reputable universities. The issue of counterfeit credentials, potentially exacerbated by centralization and digitization, poses a notable challenge for universities, employers, and recruiters. According to Employee Benefit News (EBN), employers face a cost of 33% of an employee's annual salary when hiring replacements, with potential losses mounting up to $15,000 for a wrong hire. The implications extend beyond financial loss, posing serious legal and reputational risks and potentially endangering lives, such as in cases where fraudulent credentials result in unqualified individuals undertaking sensitive tasks like construction design or medical treatments.

1.4.2 Medical History

Patient data and medical history are vital to healthcare delivery, yet the current systems for maintaining and accessing this information can be insecure and inefficient. With data dispersed across various healthcare providers and institutions, ensuring the authenticity and accuracy of these records becomes increasingly challenging. Inaccuracies or omissions in a patient's medical history can result in severe consequences, including misdiagnosis, inappropriate treatments, and delays in care.

1.4.3 Event Ticket Validation

Ticket fraud is a significant issue in the entertainment industry, with counterfeit tickets leading to financial losses for consumers and damage to the reputation of event organizers. Despite numerous attempts to tackle this issue, counterfeiters continue to exploit the vulnerabilities in the current centralized ticketing systems.

1.4.4 KYC/AML

In the current financial system, Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations require customers to submit personal information for verification, a process prone to delays and errors. Moreover, these requirements can expose sensitive customer data to potential security breaches, identity theft, and fraud.

1.4.5 Traveler Authentication

For travelers, the process of validating visas, hotel reservations, and other travel documents can be tedious and time-consuming. Moreover, these documents are often susceptible to fraud and forgery, causing substantial inconveniences and potential risks for travelers and authorities alike.

1.5 The Solution

As we delve deeper into the digital era, the importance of secure and verifiable credentials becomes paramount. Authon aims to respond to this increasing need with a proposed solution that is innovative, designed to be tamper-proof, swift, and user-friendly..

1.5.1 Biometrically Secured Identity

Authon introduces an avant-garde approach to digital identity management, marrying biometric technology with blockchain encryption. The platform seeds private keys from biometric inputs, ensuring that an individual's unique physical traits safeguard their digital identity. This process eradicates the need for remembering complicated passwords, significantly reducing the risk of unauthorized access or impersonation.

1.5.2 Decentralized and Immutable Validation

Authon leverages the Avalanche blockchain for storing cryptographic hashes of various digital assets, ranging from educational certificates to other types of identification. These assets are stored on the InterPlanetary File System (IPFS), capitalizing on its peer-to-peer decentralized network. The combination of these two technologies ensures the immutability, redundancy, and robustness of stored data, making fraudulent alteration or loss of data practically impossible.

1.5.3 Secure and Controlled Sharing

Every piece of data encrypted and stored on the Authon platform can be securely shared by the wallet identity owner with any party of their choosing. The encryption method is robust, ensuring that only the intended recipient with the correct decryption key can access the shared data. This way, sensitive personal information remains under the complete control of the owner at all times.

1.5.4 Universal and Seamless Validation

Authon provides end-users with an intuitive Web3 application and mobile app that allow them to validate the authenticity of these assets seamlessly. The universal access to this data, granted through the platform's smart contracts, enables anyone to build their own validator. This feature creates a vast potential for the ecosystem's expansion, cementing trust and reliability in digital assets and credentials across various use cases.

In sum, Authon is poised to redefine the landscape of digital asset verification, adding a new layer of security and control in a user-friendly manner. The platform's unique approach to combining biometric technology, blockchain encryption, and decentralized storage offers a comprehensive solution to the challenges of the digital era, thus contributing to the evolution of financial markets.

1.6 Risk Management

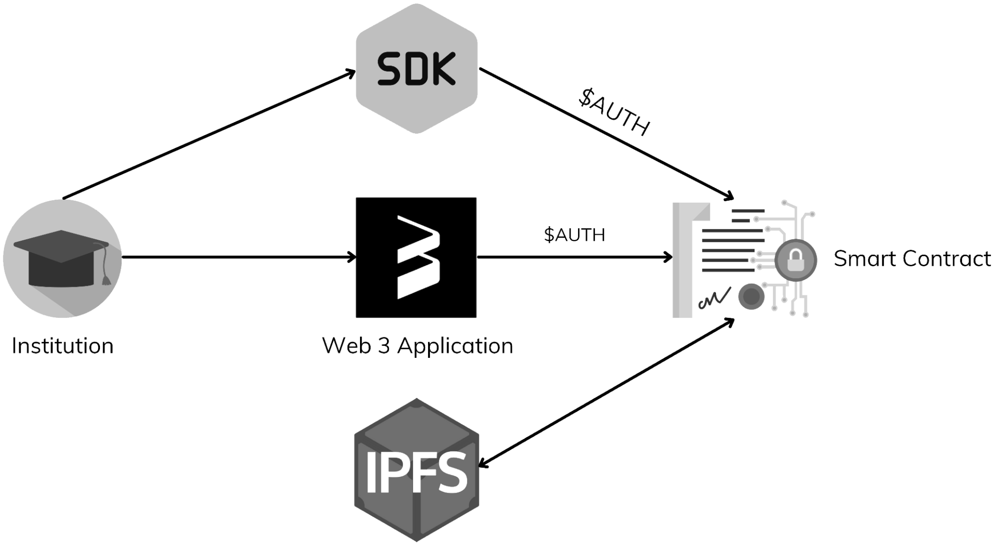
Like all blockchain-based platforms, Authon relies on miners or validators to authorize transactions, which can range from basic token transfers to executing EVM smart contracts. The primary incentive for these validators is the "rewards" given in the native currency of the blockchain upon the successful completion of each transaction. If token valuation becomes less rewarding for the validators, there could potentially be challenges for the blockchain, such as the availability of sufficient computing power to validate transactions.

However, Authon's design incorporates extensive risk mitigation strategies to address these challenges. The failure of the blockchain doesn't spell an end for Authon. The organization has plans to initiate its own validators and migrate to a dedicated Avalanche Subnet after the public sale. This move adds an extra layer of security, reducing dependency on external validators.

To further strengthen data protection and prevent loss, Authon adopts a two-pronged approach for data storage. Primary data is stored on the blockchain, while the decentralized IPFS network serves as a secondary backup storage mechanism. This dual-storage strategy ensures data longevity and accessibility, even in the unlikely event of blockchain failure.

Authon's architecture and forward-thinking strategies ensure the platform's resilience, security, and ongoing operational capability, irrespective of external market conditions or technological hiccups.

How It Works



2.1 Technology

2.1.1 Smart Contract

The underpinning foundation of Authon lies within its Avalanche Smart Contracts. These multi-functional contracts are responsible for an array of operations, including storing certificates, validating user authenticity, and regulating team token unlocks and donations.

Institutions willing to lock a specific amount of $AUTH can create and upload certificates to the primary "Main Contract." This privilege may enable them to issue and digitize various documents for their students or customers via Authon, potentially facilitating an easier transition to digital asset management.

Moreover, individuals or Small-to-Midsize Businesses (SMBs) can lock a modest amount of $AUTH to establish personal spaces.

At the core of this secure system, the smart contract stores the hashed representations of uploaded assets and categorizes the data into four main information types:

1. Cryptographic IPFS hash of the asset
2. Issuer Information
3. End User
4. Metadata

Notably, Authon employs public and private key cryptography, utilizing hashed biometric data to secure these digital assets. The result is a unique, encrypted blockchain identity that the wallet owner can securely share with any party.

Each asset's hash corresponds to its IPFS address on the Interplanetary Decentralized File System, thereby ensuring data traceability and integrity. While the data resides on the blockchain, it remains completely secure and confidential, accessible only by its authorized owner.

A unique feature of the Main Contract is its flexibility in invocation. It can be triggered not only through a Web3 DApp but also via an Open Source SDK. This flexibility enhances Authon's adaptability and compatibility, allowing for more seamless and efficient asset management on the blockchain.

2.1.2 IPFS Storage

IPFS allows users to host and receive content in a manner similar to how BitTorrent functions. As opposed to a centrally located server, IPFS is built around a decentralized system of user-operators who hold a portion of the overall data, creating a resilient system of file storage and sharing. Any user in the network can serve a file by its content address, and other peers in the network can locate and request that content from any node which includes it using a distributed hash table (DHT).

The smart contract stores the actual binary and metadata of the assets one the IPFS network, providing a cost-effective solution as well as increased redundancy in the case of a failure in the blockchain network.

The organization behind Authon (the founding body) also aims to fund its own IPFS nodes to potentially enhance availability, optimize latency, and improve redundancy.

2.1.3 Web3 DApp

Authon is launched with its own DApp from day one, which is actually a combination of two seperate web / mobile applications.

2.1.3.1 Validator

The mobile and web distributed application named the “Validator” is a free-to-use, non-wallet dependent application that allows anyone, be it an Authon user or not, to validate any asset that has been verified and uploaded to the Authon network. This is a disruptive and novel approach which allows non-blockchain internet users to be actually onboarded on a Web3 project directly.

Using a website that has zero centralized backend requirements or a mobile application that interacts with the Avalanche network directly without any intermediaries, the validator allows any mobile or web user to authenticate assets just by visiting a URL or scanning of a QRcode.

The validator application verifies the authenticity of the asset as well as provides metadata such as the date, the issuer institution, and the IPFS hash of the original document itself.

2.1.3.2 Issuer

This is the key application that allows small to middle-sized businesses or institutions to issue digital assets on the Authon network. The steps required for a digital asset to be issued on Authon are as follows:

1. The user must have an Avalanche compatible wallet (like Metamask)
2. Wallet must have a balance of $AUTH for the staking operation.
3. A copy of the asset must be uploaded.
4. The user must choose the handle of the end-user that the asset has been issued to..
5. If the user does not exist, the program will create an entity with the handle, and the issuer will be presented with additional input fields for the identification (name & surname)
6. Any other metadata the issuer wants to insert must be entered into the wizard
7. The blockchain notarization is complete

2.1.4 Biometric Blockchain Identity and Key Recovery

Building upon the solid foundation of Avalanche Smart Contracts and IPFS Storage, Authon extends its identity protection and verification strategy with the incorporation of biometric data, turning your body into the key to your digital identity.

2.1.4.1 Storing the Private Key

Every individual user on Authon possesses a unique identity wallet, the private key of which is stored as a biometric hash - a cryptographic representation of personal biometric information such as facial biometry or fingerprints. This private key grants access to a user's digital identity and all associated documents on Authon's decentralized network.

Alternatively, the private key could also be represented as a seed phrase consisting of three distinct words. Regardless of the chosen method, the primary principle remains that only the rightful owner of the identity - the individual whose biometric data matches the stored hash or who knows the unique seed phrase - can unlock and manage their digital identity.

2.1.4.2 Key Recovery using Shamir's Secret Sharing

Understanding that the loss or compromise of a private key could lead to an irreversible lockout, Authon incorporates Shamir's Secret Sharing algorithm for secure key recovery. With this system, the private key (biometric hash or seed phrase) is divided into multiple parts, each securely stored in isolation.

To recover the key, at least two out of the three methods (biometric hash or seed phrase parts) are required. This multi-factor approach ensures that even in the event of a single method being compromised, the private key and hence the digital identity remains secure and recoverable.

By utilizing the strength of biometrics and the resilience of Shamir's Secret Sharing, Authon provides users a secure and user-friendly way of managing their blockchain identity, simultaneously maintaining the integrity and security of the stored data. This system effectively merges the physical and digital world, embodying the saying: Your body is the key.

2.1.5 Transfer of Identity and Financial Assets

Authon not only provides a secure system for storing and validating digital identity but also enables a user-friendly process for transferring this digital identity and any associated financial assets. The platform has been designed to incorporate safeguards against potential misuses and frauds while offering flexibility for the wallet owner.

2.1.5.1 Designating Inheritors

Each wallet owner has the capability to designate up to three inheritors for their digital identity and associated assets. The wallet owner can specify the percentage of assets each inheritor is entitled to, allowing for a personalized distribution of wealth. This asset division can be adjusted at any time by the wallet owner, ensuring continuous control and flexibility over personal assets.

2.1.5.2 Triggering Inheritance Process

The inheritance process can be initiated by at least two of the three designated inheritors. This requirement ensures multiple points of verification before the transfer process begins and prevents any single inheritor from unilaterally initiating the process.

2.1.5.3 Waiting Period and Fraud Prevention

Upon triggering the inheritance process, there is a waiting period of 60 days before the assets are transferred. This time window serves as a security measure and allows the wallet owner to object to the process if they believe it has been triggered under fraudulent circumstances.

In the event of an objection, the process is immediately frozen, securing the wallet owner's digital identity and assets until the situation is resolved. This provision ensures that the wallet owner's rights are prioritized, and any unauthorized attempts at asset transfer can be effectively halted.

Through these mechanisms, Authon provides a secure, flexible, and user-centric approach to managing and transferring digital identities and associated assets, protecting users in life and beyond.

2.1.6 Open Source SDK

The key to the widespread adoption of Authon's innovative blockchain solution lies in the Open Source Software Development Kit (SDK). This powerful feature promotes seamless integration with existing Web2 applications and automation software, extensively utilized by billions across the globe.

Blockchain implementation has traditionally been hindered by a talent deficit in software development and a fundamental divergence in software architecture and engineering principles. Authon addresses this challenge head-on by offering a middleware solution written in Golang. This solution functions as an effective interface between the Authon smart contract and the conventional web/desktop applications that institutions and ed-tech companies worldwide currently rely on.

To operationalize the SDK, the issuer's wallet private key should be defined in an .env file. From there, the Authon SDK begins serving a REST API, making the issuance of assets on the blockchain as straightforward as uploading a file via an HTTP POST request. Crucially, this operation maintains stringent security measures. The private key is never exposed to the internet since the SDK operates locally. Moreover, the SDK supports OAuth for an added layer of security, enhancing protection of sensitive user data, including biometric information.

With its foundation as a Golang HTTP server, the SDK can be reverse-proxied behind Nginx/Apache or any other web server, ensuring flexible and seamless integration.

The Authon SDK also showcases horizontal scalability, capable of accommodating substantial workloads. It can manage use cases requiring thousands of parallel requests, thus delivering robust and resilient service even under high-demand scenarios. Through these features, the Open Source SDK epitomizes the promise of Authon: secure, scalable, and user-focused blockchain solutions.

2.2 Tokenomics

2.2.1 Auth Token Overview

$AUTH, short for "Authon", is the utility token that powers the tokenomics behind the platform. It is fixed in supply with a total of 100.000.000 tokens minted at the beginning. Unlike the substantial amount of tokens currently in circulation, $AUTH has liquidity from day one, being used in every asset issuance transaction on the network.

The liquidity of the token facilitates instant tradability on DEXs and exchanges, increasing its utility in the Authon ecosystem. The token is designed to be unlike other tokens and $AUTH isn't aligned with BTC. The value of $AUTH is more linked to its activity level on the Authon service. This allows the demand for the token to be independent of general cryptocurrency trends, social media manipulation, and other financial / geopolitical factors.

As the network grows and more organizations start issuing Authon verified assets, the utility-based demand and value in fiat pairs is expected to increase parabolically.

2.2.2 Token Utility

2.2.2.1 Use Case

2.2.2.1.1 Transactions

Every issuance transaction on Authon requires a transaction fee paid in $AUTH & a gas fee paid in the native token of Avalanche; $avax. The fees paid are the responsibility of the issuer, not the end-user whom the digital asset is being verified for. The web3 Dapp and the SDK automatically handle the fees simultaneously in a single transaction.

2.2.2.1.2 Locking

The locking model differs from normal Web3 projects as it doesn't only have financial benefits but also practical ones. To be an issuer on the Authon network, the entity has to lock amounts detailed in the table below:

Type	**Staking Amount**
Issuer	10,000 $AUTH
Individual	0.1 $USD

Issuers and Individuals have two differences:

1. Individuals can do asset verifications only for themselves, not others
2. Issuers are the only ones who can develop their own distributed applications & do asset bounding / verification for other Authon users.

2.2.2.2 Fees

The transaction fees on Authon are not fixed $AUTH amounts. As seen in previous examples where gas fee surges related to token value gains affected big or small players alike (for eg. Ethereum), the expected increase in the value of $AUTH would normally make token issuance a very expensive process in the long run.

To overcome this, the transaction fees are based on a fiat currency ($USD). This makes the price of using Authon predictable and allows other business models to be based on the network. The transaction fees in $AUTH are calculated as illustrated below:

$$e = 0.1 \div \left(\frac{\sum_{0 \leqslant i < 100}^{n} a_i}{n} + \left(\frac{\sum_{0 \leqslant i < 100}^{n} a_i}{n} \right) \times 0.02 \right)$$

e = fee
n = number of last 100 transactions
a = $AUTH/$USD trades in DEX's and exchanges
0.1 = the fiat value of the transaction

Fee calculation formula can be summarized as follows:

1. Last 100 trades are pulled from exchanges
2. Mean average of the $AUTH / $USD pair in those trades + a %2 slippage is added
3. And the $AUTH required is calculated conforming the value in $AUTH to match 0.1 $USD

Examples of transaction cost in $AUTH:

1. $AUTH / $USD: $0.20 = 0.4901 $AUTH
2. $AUTH / $USD: $10 = 0.0098 $AUTH

2.2.3 Distribution

The token distribution is detailed below, all the assets belonging to the team and the founders are locked in the Smart Contract, there is also a release schedule with details on authon.org.

Distribution	**Percentage**	**$AUTH**	**Initial Price**
Private Sale	15%	15,000,000	$0.1
Public Sale	35%	35,000,000	$0.15
Founders	30%	30,000,000	-
Team	12%	12,000,000	-
NPO Giveaways	5%	5,000,000	-
Airdrop	3%	3,000,000	-

2.2.4 Exclusive Owner Benefits

2.2.4.1 Early Utilizers

Public sale early utilizers are incentivized by the enhanced utility of the tokens after the platform launches. The intrinsic value of $AUTH comes from its essential role in the Authon ecosystem, ensuring smooth operation from day one.

Initial adopters of the Private Sale are only a fraction of the utilizers yet to register. The demand for the token is expected to increase significantly as more and more institutions are onboarded to validate and verify their assets. Notarization is one of the most substantial benefits of blockchain technology.

The reward program will also ensure that the early utilizers are deposited with $AUTH tokens in airdrops, and the team has other perks to be announced for the platform's early supporters.

2.2.4.2 Token Utilizers

The token utilizers are the backbone of Authon, as the entire tokenomy is built around high liquidity & an ever-increasing count of TPS. Every issuance action on Authon requires a deposit of $AUTH, thereby causing the number of tokens in circulation to decrease, but the demand for $AUTH by the issuers to increase, which creates a stable & thriving tokenomy that awards both early and long term users.

2.2.5 Token Specifications

$AUTH is an ERC-20 token created by its parent smart-contract. It runs on the Avalanche C-Chain and implements the Ethereum standards

2.2.6 Sale Process

There are two stages of sales:

1. Private Sale

   The participants, selected by the Authon team, are all strategic partners comprising edu-tech powerhouses, e-learning startups, institutions, and investment funds. These partners acquire $AUTH tokens for the primary purpose of utilizing the Authon platform's services. The initial allocation of $AUTH tokens corresponds to a value of $0.1 per $AUTH/$USD pair.

2. Public Sale

   The public sale will last for 30 days, progressing in 10 phases, each phase lasting for 3 days. With each new phase, the allocation of $AUTH tokens will adjust by $0.005, starting at a value of $0.15 per $AUTH/$USD pair at the beginning of the sale and ending at a value of $0.20. This public sale allows a broader audience to obtain $AUTH tokens, thereby enabling them to utilize the comprehensive services offered on the Authon platform.

2.3 Market

2.3.1 E-Learning

2.3.1.1 Current Statistics

E-Learning, or electronic learning, has established itself as a crucial pillar in the modern educational landscape. Not confined to the boundaries of conventional classrooms, E-Learning leverages electronic technologies to facilitate access to educational curriculum outside of a traditional classroom. The implementation ranges from compact disks (CDs), computer-based training (CBT) to highly sophisticated web-based applications and software. E-learning has been adopted by a diverse array of sectors, including but not limited to Information Technology, healthcare, marine, retail, financial services, and telecommunications. These sectors harness E-learning solutions for effective employee training, communication, and efficient dissemination of information.

There are numerous factors contributing to the exponential growth of E-learning in both the academic and corporate world. These include rapid advancements in internet technologies, the introduction of high-speed internet access, bandwidth expansion, the launch of 5G networks, and innovative E-learning service offerings. In addition to these technological enhancements, factors like the rapid proliferation of smartphones and tablets and the increased use of these devices in the educational context, supported by the digital lifestyles of consumers, are playing a crucial role in shaping E-learning's landscape. The cost-effectiveness of E-learning, favorable government initiatives promoting the use of technology in education, and the burgeoning trend of BYOD (Bring Your Own Device) in enterprises are also integral to this growth narrative.

According to reports, the E-Learning global market was valued at around US$315 billion in 2021. However, the future looks even more promising, with the market projected to reach a revised size of US$630 Billion by 2028, translating to an impressive CAGR (Compound Annual Growth Rate) of 10.3% over the analysis period.

2.3.1.2 Future Growth

Looking into the future, the E-Learning market is slated for substantial growth across various regions. In the U.S., the E-Learning market is projected to continue its growth trajectory, estimated at around US$90 Billion in 2021. China, the world's second-largest economy, shows promising signs of market expansion, with predictions stating it will reach a market size of US$105 Billion by the year 2026.

In Europe, a region known for its emphasis on quality education and advanced infrastructure, the E-Learning market is estimated at around US$ 75 billion in 2019 and expected to grow at a CAGR of 8% by 2026. This growth will be driven by various factors, including cultural dynamics, smartphone penetration, internet connectivity, and innovative learning methods.

Meanwhile, the Asia-Pacific region is also projected to contribute significantly to the global E-learning market, with its market size estimated to be around $35 billion in 2019 and expected to grow at a CAGR of 11% from 2020 to 2026. The increase in smartphone usage, high-speed internet connectivity, and an ever-expanding digital user base are the key drivers of this growth.

2.3.2 Digital Identities

2.3.2.1 Current Statistics

In parallel with the developments in E-learning, the digital world has been grappling with the significant problem of identity theft. In 2021 alone, the total loss due to identity theft in the US economy was a staggering $204 billion. The issue is not just confined to a single region; about 52% of companies globally have suffered the repercussions of identity theft. The types of attacks are wide-ranging and include phishing attacks, impersonation, and the creation of product reviews by fake accounts. The impacts of these actions are profound and extend beyond monetary losses, affecting the reputation and credibility of the entities involved.

2.3.2.2 Future Growth

Amid these growing challenges, the market for solutions to identity theft is projected to expand significantly. According to the World Economic Forum, the value of solutions dealing with identity theft could reach up to $1 trillion. This growth is not limited to direct measures addressing identity theft. Still, it also encompasses the integration of secure and efficient practices in various sectors, including the rapidly growing E-learning market. The development and deployment of advanced security measures, innovative authentication methods, and stringent data protection regulations are among the major factors propelling this growth.

3.3 Future Plans

3.3.1 Verify with AuthID

Authon platform as described in the Introduction section of the paper, is a new, secure & redundant way of storing information bound to an identity. The current version of “the first edition publication date of the paper” details use cases where the assets are individually verified. We should add the fact that AuthID is actually a verified identity that can be used to authenticate with any platform whether it runs on a blockchain or a centralized traditional application.

Following the launch, the Authon founders will use the funding to work on bringing **"AuthID - OpenID on Blockchain"** live and running. An identity provider running on blockchain will not only be an efficient way for solving yet another real world problem using blockchain but also is likely to promote mass adoption of non-users.

A key aspect about AuthID is the fact that users are owners of their own personal data, therefore a much more secure alternative to currently popular identity providers like Google, Facebook Connect & Twitter.

The liquidity generative properties of $AUTH for an OpenID implementation running on blockchain are immense and the fact that the users can actually profit from their data instead of giving it for free to centralized tech conglomerates.

It is planned that full implementation will be ready 6 months after the end of the public sale. The final product will include a Javascript SDK & libraries for all major backend programming languages.

AuthID will provide an ecosystem where you own your data, authenticate your identity with a single click, and share what scopes you want. In the fully-functioning final phase, the end-users will be the sole owners and controllers of their personal data.

3.3.1.1 Digital Identities

Identity is a socially constructed and contextual concept. We have supported people having multiple identities inside their societies. These identities range from student IDs, customer numbers, and government IDs to passports and other official documents. We have even more identifiers in the digital world, as we have different personas in different online services like shopping, gaming, social media, and banks.

The problem is that we go around the web and try to manage hundreds of these divided identifiers like a username and password, a domain name, or a user ID. Although widely used protocols like HTTPS, SSL, and TLS are wrongly believed to be indicators of security, they are, in fact, tools for making sure that the data transferred between the client and the server is secured and can't be accessed by the middle-man.

3.3.1.2 Problems Around Centralized ID

The chaos of managing identities this way has helped new standards to emerge like SAML, OAuth2, and OpenID. However, these standards have been adopted by big and small tech companies alike, where the big ones have positioned themselves as third-party identity providers, and the small ones have been using the identity providers for faster user onboarding, user experience, and cost. The new standards helped big tech companies to become the middleman in all our interactions when we go around the web and use their social login infrastructures. As a result, they have even more control over your digital self, browsing habits, and personal data, which enables companies to profit from that data.

It is safe to say that the current internet provides us with no digital identifiers that we really own right now. SSO services lock you up in their ecosystem and prevent you from figuratively owning your digital identity. However, AuthID provides a way to solve yet another real-world problem using blockchain.

3.3.1.3 The Missing 8th Layer of the Internet- Identity Layer

The current internet is made of seven (7) layers and missing a key component: the Identity Layer. Authon believes in an 8th abstract identity layer for empowering individuals to take control of their privacy. A new way to authenticate and authorize the user, enabled by blockchain, where you are the sole administrator of your own digital identity and are completely in control of how your personal data is shared and with whom.

It is envisioned that the core of this new emerging 8th layer is the decentralized identifier. (DID). It really is a long self-generated string that is generated on the client side.

3.3.1.4 Decentralized Identifiers

The blockchain technology provides a solution to the online identity problem by enabling DIDs to be permanent, cryptographically verifiable decentralized identifiers that resolve to data on the Authon network, either public or encrypted.

DIDs represent real-world identities like passport numbers and email addresses with legal and practical implications. They serve as identifiers for your digital identities. DIDs are under the control of the holder, independent, unique global ids that don’t require a centralized registration authority database.

3.3.1.5 Verifiable Credentials

Currently things like university degrees, online training certifications, information on your driver’s license, professional licenses, etc. are shown to a verifier in paper form. Therefore, there are lots of ways to fake it as we have mentioned in the previous sections of the paper. The fact that the current systems allow for such fraudulent behavior creates a vast industry and costs for verifying these documents.

Verifiable credentials used by AuthID will allow information to be efficiently shared between parties in a controlled manner while ensuring the integrity of the information and allowing the recipient to more effectively evaluate the trustworthiness of the information being shared.

Your digital wallet is the pointer and the key to where your credentials and keys are stored. The credentials can be issued by yourself but most of them will come from other issuers. Examples might be your employer, loyalty card, passport etc. To prove your identity, it should either be verified by the third party issuing it or the AYCDAO.

3.3.1.6 Use Case

The first use case for AuthID will be the federated login feature which enables individuals with an SSO that does not rely on centralized institutions. This will greatly benefit protecting the privacy of individuals using SSOs as there will be no intermediary institutions that profit from their online activities.

An example scenario: Alice wants to use her social login account to log in to other websites. She is concerned about her privacy because of incidents with companies like Cambridge Analytica, and considers how her personal information might be used with the intent that she has not consented to. She is not as comfortable with sharing information with big tech companies as she used to; she is privacy aware...

Alice wants to use the seamless experience of SSO but without making a trade-off by losing her online privacy.

Alice uses AuthID to create a new account when signing up for a new website that creates a public DID. Alice exchanges cryptographic keys with the website, and whenever Alice returns to the website the keypairs allow her to be uniquely known to the service. Alice’s wallet manages her keys and presents a single interface for all the login information required by the other websites that she is using.

3.3.2 AYCDAO

The solution that will allow all products, whether they are on blockchain or are centralized is AYCDAO, short for “Auth Your Customer Decentralized Autonomous Organization”.

There are real-life cases where personal data verification is not secure enough. Moreover, the KYC costs have been growing exponentially because of the inefficiencies in the process. AYCDAO aims to optimize the KYC & due-diligence processes, therefore, creating cost savings for the economic enterprises.

The use cases include tasks such as verification of official government-issued documents like ID's or passports. Authon is planning to solve this problem by creating a DAO under an NPO, in which their members will be verifying official documents (AI / Software assisted) and earning $AUTH for each verification transaction. There will be a modest staking amount to ensure that the DAO is not spammed. The votes required to verify official documents would have to be 3 and the right to vote will be randomly distributed based on properties of the document like language or profession.

This is not only a very affordable way for companies to KYC in a lightning-fast and efficient way but also a new way of working for freelancers all around the globe.

3.3.3 AuthID Card

The plans described in 3.3.1 Verify with AuthID & 3.3.2 AYCDAO will eventually allow the creation of an hardware ledger that will allow the verification services of Authon to be used in real-life scenarios globally and in a much more secure & faster way than other types of official identification.

This paper will be updated as concepts and development regarding the AuthID Card evolve and require necessary upgrades.

Glossary

Apache The Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0. Apache is developed and maintained by an open community of developers under the auspices of the Apache Software Foundation.

API API stands for application programming interface, which is a set of definitions and protocols for building and integrating application software.

Availability Availability refers to a property of software, that it is there and ready to carry out its task when you need it to be.

BitTorrent BitTorrent is a communication protocol for peer-to-peer file sharing, which enables users to distribute data and electronic files over the Internet in a decentralized manner. To send or receive files, users use a BitTorrent client on their Internet-connected computer.

BTC Bitcoin is a decentralized digital currency that can be transferred on the peer-to-peer bitcoin network. Bitcoin transactions are verified by network nodes through cryptography and recorded in a public distributed ledger called a blockchain.

C-Chain The Contract Chain is the default smart contract blockchain on Avalanche and enables the creation of any Ethereum-compatible smart contracts.

CAGR Compound annual growth rate, or CAGR, is the mean annual growth rate of an investment over a specified period of time longer than one year.

DAO A decentralized autonomous organization (DAO), sometimes called a decentralized autonomous corporation (DAC), is an organization constructed by rules encoded as a computer program that is often transparent, controlled by the organization's members and not influenced by a central government

DApp Dapps (Decentralized Applications) are the apps that run on the blockchain.

DEX Decentralized crypto exchanges (DEXs) are blockchain-based apps that coordinate large-scale trading of crypto assets between many users. They do that entirely through automated algorithms, instead of the conventional approach of acting as financial intermediary between buyers and sellers.

DHT A distributed hash table is a distributed system that provides a lookup service similar to a hash table: key-value pairs are stored in a DHT, and any participating node can efficiently retrieve the value associated with a given key.

DID Decentralized identifiers (DIDs) are a new type of identifier that enables verifiable, decentralized digital identity. A DID refers to any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID. In contrast to typical, federated identifiers, DIDs have been designed so that they may be decoupled from centralized registries, identity providers, and certificate authorities.

ERC-20 (Ethereum Request for Comments 20), proposed by Fabian Vogelsteller in November 2015, is a Token Standard that implements an API for tokens within Smart Contracts.

Ethereum Ethereum is the community-run technology powering the cryptocurrency ether (ETH) and thousands of decentralized applications.

EVM The Ethereum Virtual Machine (EVM) is what defines the rules for computing a new valid state from block to block. The EVM is a powerful, sandboxed virtual stack embedded within each full Ethereum node, responsible for executing contract bytecode.

Fiat Fiat money is a government-issued currency that is not backed by a commodity such as gold. Fiat money gives central banks greater control over the economy because they can control how much money is printed. Most modern paper currencies, such as the U.S. dollar, are fiat currencies.

Gas Gas refers to the fee, or pricing value, required to successfully conduct a transaction or execute a contract on an Ethereum compatible blockchain platform.

Golang Go (also called Golang or Go language) is an open source programming language used for general purpose. Go was developed by Google engineers to create dependable and efficient software.

Hash A hash function is any function that can be used to map data of arbitrary size to fixed-size values. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes.

HTTP The Hypertext Transfer Protocol (HTTP) is the foundation of the World Wide Web, and is used to load web pages using hypertext links.

HTTPS HTTPS (Hypertext Transfer Protocol Secure) is a secure version of the HTTP protocol that uses the SSL/TLS protocol for encryption and authentication. HTTPS is specified by RFC 2818 (May 2000) and uses port 443 by default instead of HTTP’s port 80.

IPFS The InterPlanetary File System (IPFS) is a protocol and peer-to-peer network for storing and sharing data in a distributed file system.

KYC Know Your Customer (KYC) refers to the process of verifying the identity of your customers, either before or during the time that they start doing business with you.

Latency Network latency, sometimes called lag, is the term used to describe delays in communication over a network.

Metadata Metadata is "data that provides information about other data", but not the content of the data, such as the text of a message or the image itself.

Middleware Middleware is software that lies between an operating system and the applications running on it. Essentially functioning as hidden translation layer, middleware enables communication and data management for distributed applications.

Miner Mining is the process that Bitcoin and several other cryptocurrencies use to generate new coins and verify new transactions.

Minting Minting crypto is the process of generating new coins by authenticating data, creating new blocks, and recording the information onto the blockchain through a “proof of stake” protocol.

Nakamoto The Nakamoto Consensus is a set of rules that verifies the authenticity of a blockchain network, using a combination of the proof-of-work consensus algorithm on a Byzantine Fault Tolerance (BFT) peer-to-peer network.

NFT NFTs are individual tokens with valuable information stored in them. Because they hold a value primarily set by the market and demand, they can be bought and sold just like other physical types of art.

Nginx NGINX is open source software for web serving, reverse proxying, caching, load balancing, media streaming, and more. It started out as a web server designed for maximum performance and stability.

NPO A nonprofit organization (NPO) is one that is not driven by profit but by dedication to a given cause that is the target of all income beyond what it takes to run the organization.

OAuth OAuth is a standard that apps can use to provide client applications with “secure delegated access”. OAuth works over HTTPS and authorizes devices, APIs, servers, and applications with access tokens rather than credentials.

Open Source Open-source software is computer software that is released under a license in which the copyright holder grants users the rights to use, study, change, and distribute the software and its source code to anyone and for any purpose. Open-source software may be developed in a collaborative public manner.

OpenID OpenID allows you to use an existing account to sign in to multiple websites, without needing to create new passwords. You may choose to associate information with your OpenID that can be shared with the websites you visit, such as a name or email address. With OpenID, you control how much of that information is shared with the websites you visit.

P2P Peer-to-peer computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes.

POS Proof-of-stake protocols are a class of consensus mechanisms for blockchains that work by selecting validators in proportion to their quantity of holdings in the associated cryptocurrency. This is done to avoid the computational cost of proof-of-work schemes.

POST POST is a request method supported by HTTP used by the World Wide Web. By design, the POST request method requests that a web server accept the data enclosed in the body of the request message, most likely for storing it. It is often used when uploading a file or when submitting a completed web form.

Redundancy Data redundancy occurs when the same piece of data is stored in two or more separate places and is a common occurrence in many businesses.

REST Representational state transfer is a software architectural style that was created to guide the design and development of the architecture for the World Wide Web. REST defines a set of constraints for how the architecture of an Internet-scale distributed hypermedia system, such as the Web, should behave.

SAML Security Assertion Markup Language (SAML) is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP). What that jargon means is that you can use one set of credentials to log into many different websites.

SDK A software development toolkit (SDK) is a set of software tools and programs provided by hardware and software vendors that developers can use to build applications for specific platforms.

Smart Contract A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. The code controls the execution, and transactions are trackable and irreversible.

SMB Small and medium-sized enterprises or small and medium-sized businesses are businesses whose personnel numbers fall below certain limits.

SSL SSL, or Secure Sockets Layer, is an encryption-based Internet security protocol. It was first developed by Netscape in 1995 for the purpose of ensuring privacy, authentication, and data integrity in Internet communications. SSL is the predecessor to the modern TLS encryption used today.

SSO Single sign-on (SSO) is an authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials.

Subnet A subnet, or subnetwork, is a smaller network within a larger one.Subnets make networks more efficient by simplifying routes from one computer or server to another.

Tether Tether is a stablecoin cryptocurrency that is hosted on the Ethereum and Bitcoin blockchains, among others. Its tokens are issued by the Hong Kong company Tether Limited, which in turn is controlled by the owners of Bitfinex.

TLS SSL, more commonly called TLS, is a protocol for encrypting Internet traffic and verifying server identity. Any website with an HTTPS web address uses SSL/TLS.

Token Unlock Vesting period, also called token lockup period, refers to a period of time in which the tokens which are distributed before the actual product launch are prevented from being sold for a specific period of time. In most cases, tokens are transferable immediately upon receipt, but this is not the case with all projects.

TPS Transactions per second (TPS) is a computer software and hardware measurement that represents the number of transactions completed in one second by an information system.

USDT Tether (often called by its symbol USDT) is a stablecoin cryptocurrency that is hosted on the Ethereum and Bitcoin blockchains, among others

Validator A validator is an entity that participates in the consensus of a blockchain protocol.

Web3 Web3 is an idea for a new iteration of the World Wide Web based on blockchain technology, which incorporates concepts such as decentralization and token-based economics.