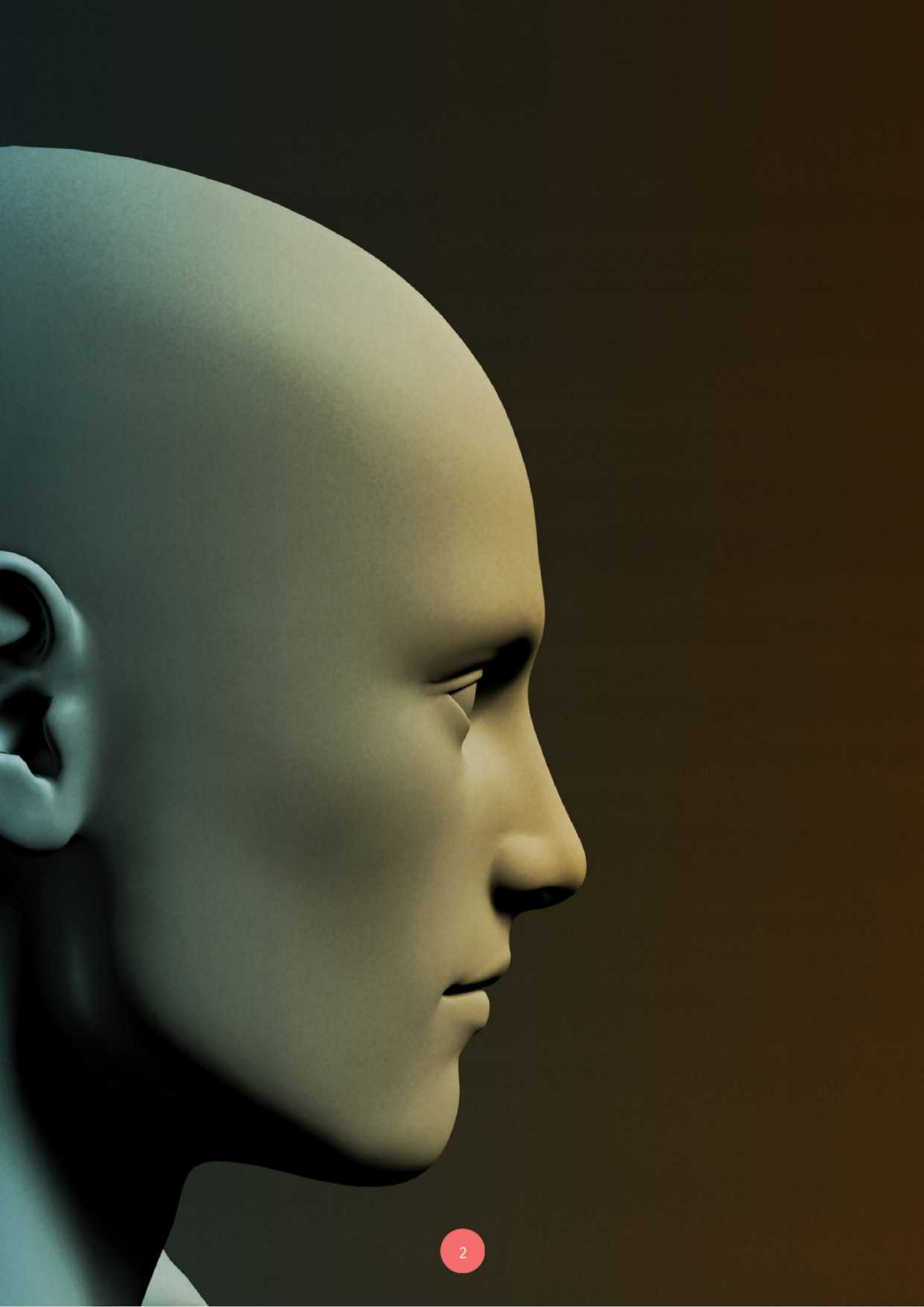

Phaeton
IDENTITY

CONTENTS



INTRODUCTION

With improvements in digital technology, there has been a significant increase in "identity theft". Never before has it been so easy to acquire another person's vital personal details and capitalise on them. According to the Breach Level Index, there are 4,861,553 records stolen every day. Therefore, this problem has created a demand for countermeasures, and blockchain is an efficient and effective way to address a wide range of personal identity security risks.

Besides identity theft, COVID-19 has made the need for health identity an urgent issue. When rushing a patient through an emergency at a hospital, it takes hours to complete forms before a patient can be formally admitted. Hospitals require a patient's health history, including any hereditary illness, their current medication and symptoms, plus details of the relevant health insurance provider. The same information is again required on the new form when visiting another hospital at a later date.

When signing up on multiple online platforms, users have to create a unique username and password each time. With each service, it becomes more difficult for users to remember a combination of usernames and passwords. Maintaining various authentication profiles is quite a challenging task. The current verification process involves three stakeholders, including (a) verifying companies/KYC companies, (b) users and (c) third parties that need to check the identity of the user. The global survey of "Know Your Customer" challenges found that global annual spending on KYC is estimated at US $48million.

Furthermore, it is currently impossible for users to have control over personally identifiable data (PID). For example, they do not know how often their PID has been shared without their consent and where their personal information is stored. Therefore, the existing identity management process requires an innovative change. Using blockchain for identity management allows individuals to own their identity by creating a universal identity to serve multiple purposes. Blockchain offers a solution by providing users with a sense of security that no third party can share their PID without their consent. A blockchain platform can be established to protect an individual's identity from any breaches or theft. Users can be free to create self-sovereign and encrypted digital identities and remove multiple usernames and passwords. This white paper explains how Phaeton has created a unique blockchain identity management system.

WHAT IS IDENTITY MANAGEMENT?

Identity Management, also known as identity and access management (IAM), ensures that only authorised people access the technology to perform their role. It includes policies and technologies that encompass an organisation-wide process. The process identifies, authenticates, and authorises people, groups of people, or software applications through attributes including user access rights and restrictions based on their identities.

Identity Management protects software and data access. It also protects hardware from unauthorised access, such as servers, networks, and storage devices, leading to a ransomware attack. For example, in a governmental setting, the issuing and verification of birth certificates, national id cards, passports or driver's licenses allow citizens to prove their identity and access services from the Government and other organisations.

PROBLEMS WITH CURRENT IDENTITY MANAGEMENT

There are several problems with the current Identity Management. First, most of it is paper based, such as birth certificates that sit idly in Government archives and are subject to loss, theft, or fraud. In contrast, a digital identity reduces bureaucracy and increases the speed of processes within organisations by allowing greater interoperability between departments and other institutions. However, if this digital identity is stored on a centralised server, it becomes a target for hackers. Since 2017 alone, organisations have hacked, leaked or breached more than 600 million personal details such as addresses or credit card numbers. In addition, most of the current identity management systems are weak and outdated.

NEED FOR PORTABLE AND VERIFIABLE IDENTITY

In resolving these problems, identities need to be portable and verifiable anywhere and at any time. Digitisation can allow this but being digital is not enough as Identities also need to be private and secure. Below is a display of some sector examples that suffer these problems of current identity management systems, which include:

- **Government:**
  The lack of interoperability between various government departments takes a toll in the form of excessive bureaucracy. Which, in turn, increases processing times and costs.
- **Healthcare:**
  Fifty per cent of the world's population do not have access to quality healthcare. Moreover, the lack of interoperability between hospitals, clinics, insurance companies, doctors and pharmacies lead to inefficient healthcare and delayed care which frustrates patients.
- **Education:**
  It has been reported that over 1,000,000 fake academic certificates are sold annually. The problem is that the difficulty in verifying the authenticity of these credentials leads to the hiring of unqualified professionals and damage to universities and employment.
- **Businesses:**
  The need to store clients' and employees' data is a source of liability for companies. In addition, a personal data breach may result in huge fines due to General Data Protection Regulation (GDPR) infringement.
- **Banking:**
  With KYC (Know your customer) requirements for financial institutions, correctly identifying the customer to the bank when providing financial services is on the increase.
- **E-commerce:**
  Online shopping has become an integral part of our lives. However, it takes time to fill in information such as name, email, phone number, address, etc. Signing up on multiple e-commerce platforms using a single ID is less time consuming, and blockchain can make it real.


GOVERNMENT
BANKS
HEALTHCARE
SOCIAL MEDIA
TRAVEL
EMPLOYMENT
E-COMMERCE
SUPPLY CHAIN
LEGAL

A PHAETON BLOCKCHAIN IDENTITY SOLUTION

Phaeton Blockchain Identity offers a decentralised and secure solution that gives users total control through a distributed trust model. Our blockchain technology benefits several industries with transparency, security, and trust adding value to our clients. We have the ideal technology to transform the current workings of identity management in a highly secure manner.

Existing identity management systems are neither secure nor reliable. At every point, users are asked to identify themselves through multiple government-authorised IDs, such as driver's licences, passports, proof of address and more. Moreover, sharing multiple IDs with others can lead to privacy concerns and data breaches. Phaeton Identity can pave the way to self-controlled identity through a decentralised network, offering privacy, trust, security, verification and participants endorsing identity documents.

Everyone uses identity documents regularly, shared with third parties without explicit consent and stored at an unknown location. Whether a person is applying for a loan, opening a bank account, entering a hospital, or booking a ticket, identity documents are required. However, government institutions, banks and credit providers are the weakest point in the current identity management system as they are exposed to theft and hacking of data. The blockchain structure eliminates intermediaries allowing citizens to manage their identity independently.

THREE PILLARS OF PHAETON IDENTITY

The three pillars of Phaeton Identity are (1) the Verifiable Credentials protocol, (2) the Decentralised Identifiers protocol and (3) Distributed Ledger Technology (or Blockchain).

1. **Verifiable Credentials:**
   These are statements made by an issuer privately. Verifiable credentials, in essence, allow for the digital watermarking of claims with a combination of public-key cryptography and privacy-preserving techniques to prevent correlation. The result is that not only can physical credentials be safely digitised, but holders of these credentials can also selectively disclose specific information without exposing the actual data. Furthermore, third parties can verify this data without having to call upon the issuer.
2. **Decentralised Identifiers:**
   These are global, unique, and persistent identifiers. The identity owner controls them. They are independent of centralised registries, authorities, or identity providers. When an organisation issues you a Verifiable Credential, they attach their Public DID to that credential. The same Public DID is also stored on the blockchain, an immutable record of data. So, when someone wants to verify the authenticity or validity of the credential, they can check the DID on the blockchain to see who issued it without contacting the issuing party.
3. **Distributed Ledger:**
   The Blockchain acts as a verifiable data registry. It is like a phonebook where anyone can consult to verify the Public DID and its specific organisation. In identity management, a distributed ledger (a "blockchain") enables everyone in the network to have the exact source of verification. It ensures that the credentials are valid and who attested to the validity of the data without revealing the actual data.

NO PERSONAL DATA IS REQUIRED ON PHAETON IDENTITY

Phaeton Identity establishes trust between the parties and guarantees the authenticity of the data and attestations without storing personal data on its blockchain. It is crucial as a distributed ledger is immutable, meaning anything put on the ledger can never be altered or deleted. Thus no personal data should ever be put on the ledger. So, what should be placed on Phaeton Identity?

When using Phaeton Identity, there should only be references and the associated attestation of a user's verified credentials recorded on the ledger. For verification, instead of storing actual private information, the only things stored on the ledger are: (See next page)

1. **Public Decentralised Identifiers (PDI)**
   PDIs are unique identifiers for verifying digital identities and are entirely controlled by the identity owner. Thus, PDIs are independent of centralised registries, authorities, or identity providers.
2. **Credential definitions**
   The tangible proofs of identity or qualification issued by authorities include drivers' licenses, passports, identification cards, credit cards, etc. Hence, credential definitions are merely the definitions of these different credentials to be stored on the ledger.
3. **Proofs of consent**
   These are consent receipts (i.e., proofs of consent) to prove consent saying the data has been received and checks have been executed.
4. **Revocation registries**
   An option for issuers to be able to revoke the claim. The revocation registry tells the rest of the world how the issuer will publish the revocation information.

HOW DOES PHAETON IDENTITY WORK?

To understand how Phaeton Identity works, several technical components and interfaces could be involved in the process, namely:

1. Android/iOS App for individuals.
2. Android/iOS App for third-party companies or verification companies.
3. Inter-Planetary File System (IPFS) to store the user's PII.
4. Microservices programmed using Node.JS.
5. Permissioned Blockchain Component.

These apps will help people to verify and authenticate their identity in real-time.

Step 1: Install a Mobile App
- Users will first have to download the mobile app from an app store to establish their identity.
- After downloading the app on mobile phones, users create their profiles on the app.
- Once their profile is created, the user will get a unique ID number.

Step 2: Uploading documents
- Once the user gets an ID number, they need to upload any issued IDs on the app to be saved in the IPFS plus hashed addresses stored on the blockchain.
- The app will then extract the personal information from these IDs to do self-certification of their details.
- The user will own their data and consent to what information can be shared.

Step 3: Smart contracts generating trust score
- There is a scoring system that determines a person's trustworthiness.
- A smart contract containing the business logic can generate a trust score for a user from their information while creating their identity.

Step 4: Third-party companies requesting access
- Each time a third party requires access to specific details of a person, a notification will be sent to the issuer.
- Once the user allows the third-party access to their details, the third party can use the identifiable information to authenticate the person. Issuers will also be able to trace the purpose for which their PII has been used.

All PII (personally identifiable information) will be stored on the phone backed by IPFS (Inter-Planetary File System) in an encrypted form. As mentioned above, smart contracts can trigger the business rules and generate the trust score for every individual using blockchain identity management.


07.11.e5.56.8e.13
b2.81.65.b2.00.0c
45.78.1d.fe.6f.4f

WHAT ARE THE BENEFITS FOR USERS?

From the user's perspective, there are several benefits of using Phaeton Identity:

- **Unique ID**
  Each user who registers with Phaeton Identity will receive a unique identity number. The ID number consists of all personally identifiable information in an encrypted format stored on their device backed by IPFS. In addition, users can share unique IDs with any third party to authenticate themselves directly through Phaeton Identity.
- **Consent**
  Phaeton Identity will not store any user's information. Moreover, our system uses smart contracts to enable controlled data disclosure. Thus, data manipulation is not possible on our blockchain. Phaeton Identity linked with blockchain is highly secure for identity holders through our unique protocol. No transaction of the user's information can take place without the explicit consent of the user.
- **Decentralised**
  No personal documents of users will be stored in a centralised server. All documents that identify users get stored on their devices backed by IPFS, making them safe from mass data breaches. Phaeton Identity backed by IPFS prevents hackers from stealing user's information. Since the system will be decentralised, there will be no single point of failure (SPOF). Therefore, the absence of SPOF ensures that the system will never be compromised.
- **A universal ecosystem**
  Phaeton Identity does not set any geographical boundaries. So, users can use the platform across borders to verify their identity.

WHERE CAN PHAETON IDENTITY BE USED?

There are many cases where Phaeton Identity can be used. Below are several examples:

- **Opening a bank account**
  Traditionally, when opening a bank account or applying for a loan, you must submit multiple identity documents. To complete the entire manual verification process, it could take weeks for the bank to process. With Phaeton Identity, the process can be quick, saving both time and costs for the user and the bank.
- **International traveler**
  Apart from carrying a passport, a traveler requires additional documents for clearance and security checks. From booking a flight to passing security checks, boarding a flight, or immigrating to a new country, an individual can present a universal blockchain-based identity throughout the entire process. A person with Phaeton Identity would not have to undergo complicated security checks and other procedures.
- **Legal processes**
  When undergoing any legal process, a user may submit various identity documents such as proof of age, occupation and address. With the help of Phaeton Identity, users do not have to carry multiple documents wherever they go. In addition, legal entities and government bodies can verify an individual from a Phaeton Identity. Therefore, a comprehensive background check is no longer required.
- **E-commerce checkout**
  Whenever buyers place an online order, they are asked to complete information like name, email, phone number, address, etc. The process is repeated whenever they sign up on different e-commerce sites, making the whole process time-consuming and cumbersome. Hence, signing up at multiple e-commerce sites with a unique identification number can save users time and effort.
- **Previous employment verification**
  Presently, there is no fixed system to do a background check of employees and their qualifications. Therefore, it is essential to check employee's information written in resumes, previous letters, or reference letters. Validation of the information reported in employee's resumes can be requested directly through Phaeton Identity.
- **Health records**
  COVID-19 has made the need for health identity a critical issue. When a patient is placed in a hospital or visits a new doctor, multiple forms must be completed including the patient's health history, current medication, health insurance provider and more. The same information is again required when visiting another doctor or hospital. With Phaeton Identity, there will be significant time saved, especially in a case of emergency.

Phaeton
Identity

CONTACT:
CHAI SHEPHERD
CHIEF EXECUTIVE OFFICER
E: CHAI.SHEPHERD@QNUCLEON.IO
M: +61 435 217 949