KAIROS

White Paper

Spring 2018

Vision

Since 2012, Kairos has been creating best in class Artificial Intelligence driven B2B solutions for businesses around the world. We have developed Face Recognition and Human Analytics technologies that consistently deliver valuable business solutions-- defying their reputation as futuristic novelty and gaining the trust and respect of global business culture.

We process millions of faces every month for clients ranging from independent developers to enterprise businesses, and as we continue to grow, we seek to develop new products that will enhance customer experiences while accommodating ever changing markets.

To this end, we recognize the evolution of business transactions through cryptocurrency has opened yet another door for Face Recognition based solutions. The compromise of digital identities occurring in this space calls for identity verification that is advanced and effective, and Kairos is positioned to be a leader in this space through blockchain technology.

Introduction

This white paper delivers an overview of:

1. Past, present, and future.
2. Overview of the market opportunity and the face recognition and emotion detection competitive landscapes.
3. Overview of Kairos technology and architecture.
4. The Kairos Blockchain Protocol™.
5. The Kairos Identity Token™ and the Kairos Identity Wallet™.

Kairos is an established organization with proprietary algorithms, functioning products, Fortune 100 customers and a very experienced team. We've included with this paper a short video which demonstrates our technology and highlights the accuracy with which we are capable of determining human identity and emotion.

Past

In December of 2011 [while participating in the San Francisco based NewMe Accelerator Program] we conceptualized and built a time and attendance product using face recognition. It was a “time clock of the future”; capable of recognizing employees, thereby completely eliminating opportunities for time clock fraud. Businesses adopted the product, and Kairos grew.

Before long, customers began asking if we could isolate the face recognition component of the product for use in other applications. We realized that by exclusively offering the time clock product, we were precluding the company from realizing tremendous growth; so we reordered our focus and our resources to develop a complete platform dedicated to face recognition integration.

By late 2014 we had a Face Recognition product that businesses could integrate into their own software applications.

Present

Kairos is an identity company specializing in Face Recognition. Through computer vision and machine learning, we can recognize faces in videos, photos, and the real-world - making it easier than ever to transform the way businesses interact with people.

We navigate the traditional complexities of face analysis technology and offer a powerful suite of developer tools that any business can integrate with ease. Kairos is a venture-backed organization processing millions of faces every month, and building confidence in face recognition technology over industries and businesses, globally.

Our Products

Kairos' face analysis platform is comprised of three core features:

- **Identity -** used for searching and verifying faces
- **Emotions -** used for measuring sentiment and mood
- **Demographics** - used for gathering demographic data; age, gender, and ethnicity

Collectively branded as 'Human Analytics', these features can be used individually or in combination to gather unique and actionable insights about people as they interact with the world. Key performance indicators, specific to Human Analytics, allow us to truly establish our value to businesses. They serve as the foundation whereby decision makers can visualize and envision ROI.

Customers integrate Kairos into their own software applications using a suite of developer focused API and SDK solutions. The REST-based API is available over the Internet, with data storage provided in the Cloud. Alternatively, offline SDKs provide flexibility for customers

looking for more sophisticated integrations that require stricter control over security, network access and geographies.

Beyond the technology, Kairos was conceived around three guiding principles which serve as our day-to-day compass:

- **Empathy -** The act of listening intently to customers, co-workers, and members of our communities.
- **Design First -** The understanding that design is not superficial, but integral-- and defines our work.
- **Simplicity -** The skill of transforming complicated technologies into user friendly products.

Future

Kairos is building a first of its kind identity standard for using biometrics on the blockchain. And plans to open it up to the whole world. Our design preserves anonymity, while suffocating malicious intent, such as fraud.

The Kairos Identity Token™ and Anonymized Identity

Powered by face biometrics and blockchain technology, Kairos plans to create a method of identity verification which allows the user to remain anonymous-- because we believe to validate a transaction, businesses only need to know that you are you.

The process of verification will begin in the same way that face recognition does-- by establishing feature landmarks (identifiers) and comparing them to those in the image to determine a match. When a match is established, rather than linking back to a person's

actual identity (as in the case of face recognition), our algorithms will create a face template -- a digital identity -- by converting these identifiers into a unique and random string of numbers. Once the template is created, the original image can be discarded.

The Kairos ID Token™ is the specially designed digital asset of this system, and enables users to reduce the risk of face recognition specific identity theft and increase privacy during secure transactions. [Cryptocurrency, for example.]

An Overview of the Market Opportunity

The global face recognition market is expected to grow from USD 4.05 billion in 2017 to USD 7.76 billion by 2022, at a Compound Annual Growth Rate (CAGR) of 13.9% during forecast period (From: Research and Markets, 2017). Most recently, Apple's new iPhone X with it's 'always on' FaceID solution has affected a true inflection point for the technology. Still, behind this explosive growth of the technology comes an even greater, more tangible shift in the world.

Today, we live in an Identity Economy™

The way consumers interact with big-business has fundamentally changed — creating a new paradigm: *The Identity Economy™:*

71%
Consumers prefer personalized advertising

Adlucent: 2016

24bn
Selfies uploaded to Google in 2015

Google: 2016

44bn
Connected cameras by 2022

LDV Capital: 2017

Today, consumers expect on-demand, personalized, frictionless experiences vs. old school transactions. Yet, despite consumers delivering a wealth of identity and preference

intelligence across multiple platforms: **Enterprises risk missing out on $800bn in revenue gains annually*.** This is attributable to poor customer retention, uneven loyalty, subpar service and a lack of awareness.

Kairos: Powering the Identity Economy™

We carry our identity everywhere we go, yet it exists in many different places-- and is often incomplete, inaccurate, and even subject to fraud. Digitally, 'you' are often abstracted as a username and password; in the real world a driver's licence or social security number is your record of existence. But what about the real **you**? The you that likes to spin before work, the you that prefers coffee over tea, the you that feels strongly about managing your privacy.

Kairos understands who customers are and how they feel

Kairos' Human Analytics tools enable Enterprises to capture actionable Human Metrics. Defined, Human Metrics are the measurement of responses to human behavior. Each of our products yields insights that can be used to evaluate business KPIs, and ultimately go a step further and help unlock insights about customers.

For example: *Kairos brings e-commerce advantages to brick and mortar retailers by enabling them to leverage real time data around Human Metrics, which translate into valuable consumer insights.*

Examples of important Key Metrics:

- *Sentiment (How did my customers feel?)*
- *Presence (How many were present?)*
- *Reach (Who is being reached? Age? Gender?)*
- *Engagement (Attentiveness and duration of attention to stimuli?)*

Going one step further, and combining these metrics, results in computational insights and 'formulas' that accurately forecast prospective outcomes:

- *Reach + Sentiment = Preference (What does our audience want?)*
- *Sentiment + Engagement = Selection (Which [X] should we use?)*
- *Presence + Engagement = Loyalty (Has our customer come back?)*
- *Presence + Reach = Identification (Is this our customer?)*
- *Preference + Loyalty = Intention (What will the customer likely do?)*

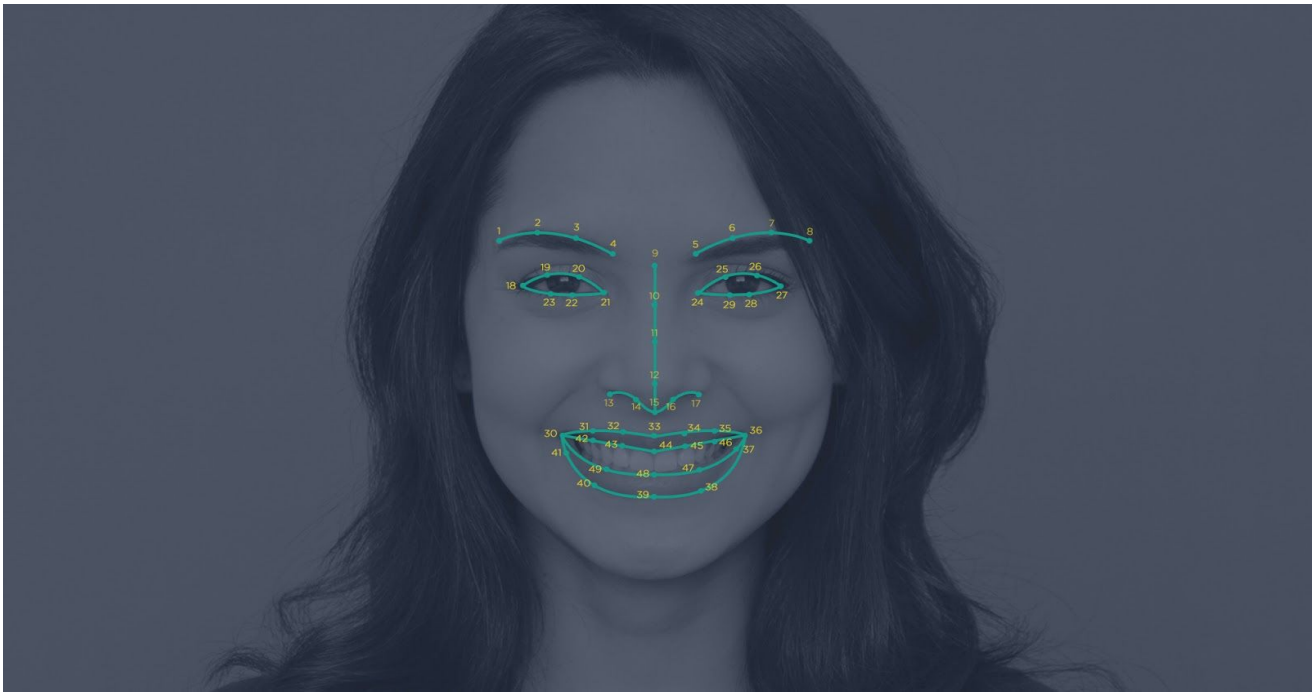
**Drive Revenue With Great Customer Experience': Forrester, 2017*

**Profiting from Personalization: Boston Consulting Group 2017*

Kairos Technology Overview

Kairos' Human Analytics products are powered by state-of-the-art face analysis and machine learning algorithms -- trained on millions of diverse human faces from around the world-- we deliver fast and accurate [real-time] results.

You can analyze any image, video, or stream from most embedded, USB or IP cameras. Kairos software currently measures dozens of unique points on the human face to gather data that includes emotions, expressions, eye blinks, age, and gender.



How it works

First, we scan the image or frame of video looking for all the faces. Next, we look for the feature points on each face i.e: the location of the eyes, eyebrows, nose, and mouth.

Once we locate these feature points we are then able to determine emotional expressions, age, gender, and if people are wearing glasses or blinking. That information is then provided back in the form of various code objects via our APIs and SDKs.

For video, based on the initial finding of feature points-- we are able to keep track of the location of each face per frame. Conversely, competitors need to find feature points in every frame-- which results in compromised accuracy and poor performance as compared to Kairos' proprietary feature-point detection.

This also means we can still measure faces even when they are partially covered, or 'occluded'. So, if someone scratches their nose, for example, it won't affect the results. This advantage also serves in keeping our algorithms fast and their resource consumption low.

Differentiators: Design, Algorithms, Patents, Flexibility, and Security

Design First

Empathy drives strategic and tactical decisions across all aspects of the organization. Understanding and responding to our customer's needs and goals allows us to deliver a service which transcends technology. We take Design incredibly seriously and display leadership in the areas of Affective Computing, HCI, UCD and the Jobs-to-be-Done innovation framework.

Intellectual Property

The Kairos suite of patents and proprietary technology is a distinct competitive advantage.

IMRSV Facial Coding & Emotion Detection Algorithms; Multi-Face Detection; Adaptive Media Content Recommendation Engine U.S. PATENT 61/722,698	**UCF** Video Face Recognition Algorithm U.S. PATENT 14/340,062
Google Predictive Motion Search; Unauthorized Device Usage Prevention (extreme value) GLOBAL PATENTS 11/168,584; 10/212,940; 10/607,009	**Kairos** Auto Enrollment Biometric Time Keeping System U.S. PATENT PENDING

Platform flexibility

Our easy to integrate REST style APIs make using Kairos products seamless on any platform. We're device and hardware agnostic, allowing for solutions that can be delivered both in the cloud and on-premise.

Security

User Privacy is paramount. High level encryption and tokenization are standard practices. We are hosted at Amazon Web Services (AWS) and are a Standard Technology Partner of AWS. We offer 2048 bit SSL encryption for all data in transit and our backups - For more information on AWS, visit their compliance page.

Kairos vs. The Competition: Summary

Kairos is the ONLY company to offer an online & offline integrated Face Recognition Identity, Emotion, and Demographics solution. There are competitors to Kairos in each of the individual areas. None of them have the strength of algorithms that Kairos has which are seen in our speed, match rates, and adaptability.

	Kairos	Amazon	Google	Microsoft	IBM Watson	Face++
Face Detection	✓	✓	✓	✓	✓	✓
Face Recognition (Image)	✓	✓	X	✓	X	✓
Face Recognition (Video)	✓	X	X	X	X	✓
Emotional Depth (%)	✓	X	X	✓	X	X
Emotions Present (Y/N)	✓	✓	✓	✓	X	✓
Age & Gender	✓	✓	X	✓	✓	✓
Multi-face Tracking	✓	✓	✓	✓	✓	✓
SDK (Offline)	✓	X	X	X	X	✓
API (Cloud)	✓	✓	✓	✓	✓	✓
Ethnicity	✓	X	X	X	X	X

A number of players have been taken out of the market in recent years:

Emotient (Apple), Face.com (Facebook), Faciometrics (Facebook), Orbeus (Amazon), Polar Rose (Apple), Looksery (Snapchat), Itseez (Intel), Msqrd (Facebook), Viewdle (Google), PittPatt (Google), Alchemy (IBM), IMRSV (Kairos)

Kairos + Blockchain

The advent of blockchain technology has enabled its users to securely and efficiently store value without it being tied to a physical identity. This ability to represent ownership without divulging the owner's true identity is a powerful characteristic of blockchains that facilitates efficient and private economic activity. However, this also enables malicious users to exploit the pseudo-anonymous nature of these systems.

The only requirement for a user to participate in a blockchain system is to obtain a public/private keypair. Because there is no other form of identity required, malicious activity perpetrated within these systems can be extremely costly to track and respond to in the form of legal or other external actions. A malicious user could be a:

- Hacker
- Fraudulent market participant
- Participant in a transaction for illicit goods or services

This fundamental discrepancy between digital and physical identity creates the perfect opportunity for Kairos to use its industry-leading facial recognition software to optimize and democratize identity management and verification on the blockchain. The concepts proposed in this section will introduce real world accountability to the decentralized, digital economy of tomorrow.

The Kairos [Blockchain] Protocol™

In order to bridge the gap between digital and physical identity, as well as streamline collaboration in the space, industry standards for physical identity verification must be defined. The **Kairos Protocol™ (KP)** defines the standard behavior to be implemented by decentralized applications that wish to leverage the power of Kairos identity verification. The **Kairos Protocol™** consists of the following:

- Smart contracts that implement the **Human Identity Interface™ (HII™)**

- The Kairos API endpoints.

The Human Identity Interface™

The **HII**™ is a smart contract interface that defines the standard by which Kairos and other biometric identity verification providers interact with contracts that implement it.

The goal is to provide the blockchain community not only with an open source, decentralized standard for any physical identity-provider to implement, but also a full suite of open source implementations of this standard for both identity providers and identity-verifying clients.

The HII™ is an interface (similar to ERC20) that, when implemented by a smart contract, provides identity-providers (like Kairos) the ability to interact with that smart contract programmatically and autonomously. The initial implementation of this standard interface targets the Ethereum blockchain, but could be applied in other decentralized systems in the future.

The **Kairos** [**Blockchain**] **Protocol**™ defines functionality to be implemented by decentralized applications that *wish to use Kairos as a physical identity verification provider*. The **HII**™ is a separate standard that defines behavior to be implemented by smart contracts with some form of physical identity verification functionality (i.e. face recognition, voice recognition, fingerprint, retina or iris scan, etc). The HII™ is implemented in any decentralized application that uses a biometric identity provider for physical identity verification.

```
// Interface that allows biometric providers
// to communicate with smart contracts
interface HumanIdentityInterface {
  function verificationOf(bytes16 clientTxGUID)
    public
    returns (
      address sender,
      uint8 confidence,
      bytes32 payload
    );

  // These functions are called by the
  // identityProvider to submit trusted data
```

```
  // to the smart contract

  // providerUserID is typically a user identifier
  // on the provider's internal system
  function register(
    address user,
    bytes16 providerUserID,
    bytes32 template
  );
  function verify(
    address sender,
    uint8 confidence,
    bytes32 payload,
    bytes32 template,
    bytes16 clientTxID
  );

  // events to emit as identity provider changes state of contract
  event Register(address user);
  event Verify(address sender, uint8 confidence, bytes16 clientTxID);
}

// Client app that implements PhysicalIdentityInterface
contract IDToken is PhysicalIdentityInterface, ERC223 {
  struct Verification {
    address sender;
    uint8 confidence;
    bytes32 payload;
    bytes32 template;
    bytes16 clientTxID;
  }

  address private identityProvider;
  mapping(address => bytes16) private registeredUsers;
  mapping(bytes16 => Verification) private verifications;

  // All the ERC223 implementation in here, as well

  function IDToken(address _identityProvider) {
    identityProvider = _identityProvider;
  }

  // ...
}
```

The Kairos Protocol™ Advantage

Decentralized applications that utilize the Kairos Protocol™ greatly reduce costs associated with the process of physical identity verification for their users. Because Ethereum transactions are public and immutable, each transaction that occurs within such applications are necessarily, and transparently, associated with an address tied to a physical identity. This

phenomenon contributes to an economic environment that disincentivizes malicious behavior because a user's true, physical identity is associated with a digital identity on a blockchain, and thus, all the actions associated with the digital identity.

For example, if a decentralized voting platform were to utilize the Kairos Protocol™, it would be cost efficient to build functionality that only allows one vote or ballot entry per user, per voting cycle. Currently, this is a resource heavy undertaking in decentralized voting platforms.

Kairos API

The Kairos API provides access to Kairos' flagship face verification systems. The Kairos API makes Kairos' powerful face comparison technology blockchain-friendly, thereby providing biometric identity verification to any smart contract that implements the Kairos Protocol™. The following outlines the expanded API endpoints:

- `POST /enroll`
  - Parameters
    - New user's Ethereum/ID address as the subject_id
    - Selfie image of user
  - Response
    - Success or failure message response
- `POST /verify`
  - Parameters
    - User's Ethereum/ID address as the subject_id
    - User's comparison selfie image
  - Response
    - Success or failure message with confidence percentage

The Kairos Identity Token™ and The Kairos Identity Wallet™

The Ethereum network allows participants to create exchangeable **tokens** using *smart contracts* that are used as the economic fuel within decentralized applications. The **ID Token**™ is an ERC-223/HII™ standard utility token, that is used to exchange value on the Ethereum blockchain using biometrically verified transactions. The ID Token™ is a first of its kind biometric verification-backed crypto-token because it is the first to implement the HII™.

The **ID Wallet**™ is a client-side wallet dApp that implements the Kairos Protocol™. Users have the ability to store, send, and receive ID Tokens™, as well as issue payment requests to other ID Wallet™ users. Because no existing wallets currently cater to the ID Token™ use cases, it will initially be the primary client interface used for holding and transacting ID Token™. Due to the fact that the ID Wallet™ is available for third-party integrations via an open source SDK, adoption by mobile and traditional web applications is entirely feasible. Projects that would benefit from a biometrically verified token payment system, but don't necessarily have the resources to create their own, are now able to reap the benefits from such a system.

Use Cases for ID Wallet™

Attacks on identity affect more than just the individual, and often times the victim's social network is the next target. A primary use case for the ID Wallet™ is in the context of generic payment requests. When user's Ethereum accounts are compromised, attackers often solicit payment requests under the guise of the exploited user being under some distress. These could easily be mistaken as genuine payment requests by the recipients, and fulfilled, thereby rewarding the attacker. On the other hand, ID Wallet™ users have the ability to force payment request issuers to verify their identity upon the creation of a payment request. This would eliminate an attacker's ability to financially benefit from the social network of a compromised Ethereum account user.

While the ID Wallet™ can greatly diminish the costs associated with malicious payment requests as illustrated above, it can also diminish costs associated with KYC/AML compliance. In the current state of decentralized platforms, it is economically unjustifiable for most of these systems to exist and operate without intrusion due to the high costs associated with KYC/AML compliance. Therefore, there is a high barrier to entry into the decentralized charity space, which is a phenomenon that reduces its benefit to society. If instead, a decentralized charity platform designated the ID Token™ and ID Wallet™ combination as the primary means of economic activity on the platform, it would provide a more cost efficient way for a decentralized charity organization to comply with KYC/AML regulations.

Identity Wallet™ Specifics

The ID Wallet™ includes a biometrically-backed “Payment Request” feature. A payment request is defined as a pending charge to an address, whereas, a payment is defined as the actual transfer of ID Token™.

The wallet has a setting called **Payment Request Identity Verification Required** that allows a payment request recipient to control whether or not a payment request issuer is required to verify her identity upon creation of a payment request. This setting is configured in the wallet, but is set at the address level. If enabled:

- In wallet settings, a user is prompted specify the **Payment Request Confidence Threshold.** This is a minimum required confidence value for any payment requests issued to this address. This value defaults to 90% if not otherwise specified.
- Payment requests to this user contain an amount, a description, and the result of the the issuer’s identity verification attempt, represented by a biometric confidence value.

Otherwise, a payment request to the user is only required to contain an amount and description.

ID Wallet™ Workflows

The following diagrams illustrate how a user initializes the dApp, ‘enrolling’ their biometric data to tie the wallet and their identity together, allowing access to dApp transactional features [Fig.1.], and how a user biometrically verifies a transaction using the dApp [Fig.2.].

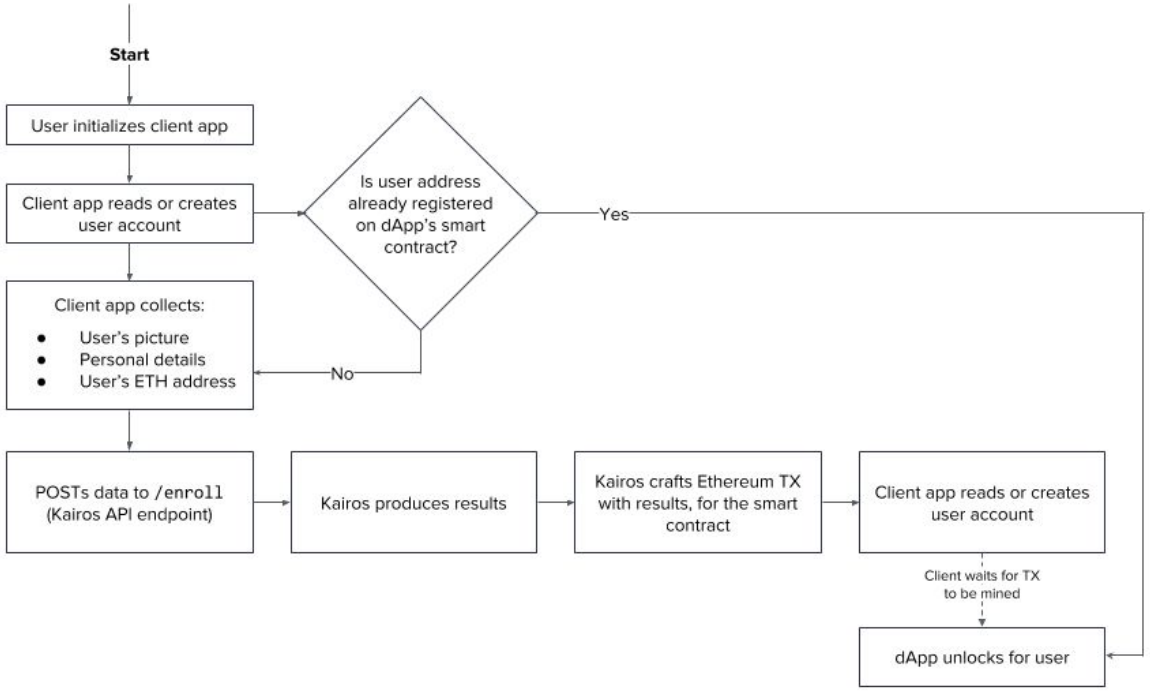


Fig.1. Client dApps that utilize Kairos Face Recognition technology perform user initialization using a standard workflow.

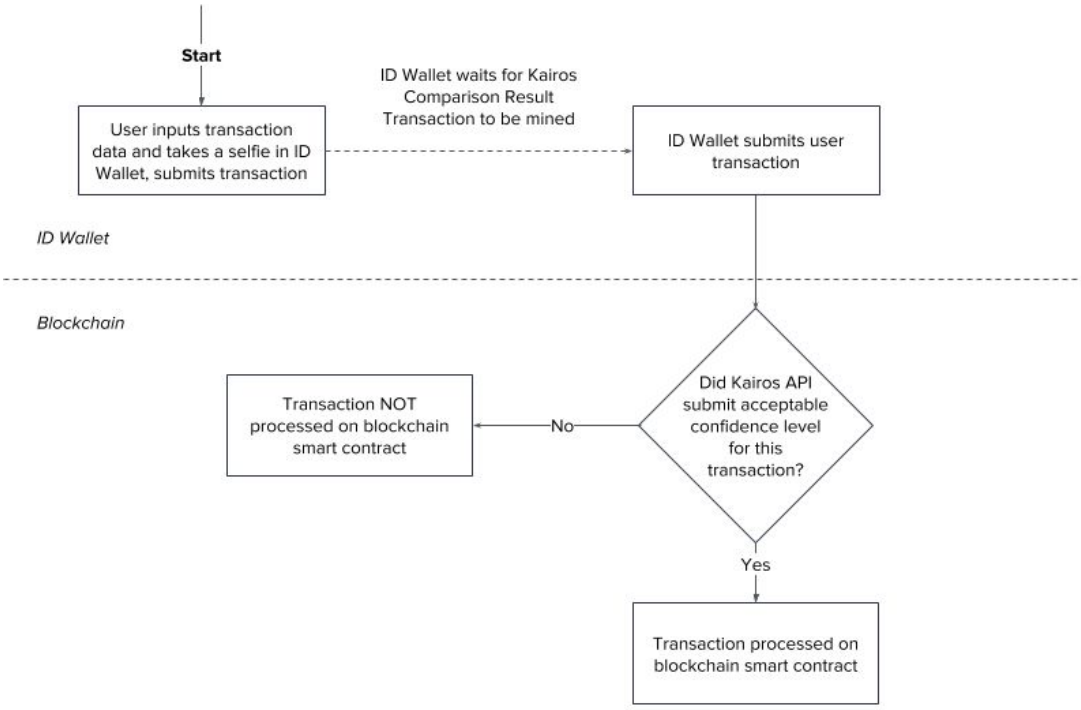


Fig.2. ID Wallet™ biometrically verified transaction workflow

Standard Implementations

Along with defining standard methods for physical identity verification, Kairos will provide standardized, industry-specific implementations of the Kairos Protocol, aside from the ID Wallet™. Some examples of this may be the following:

- A philanthropic decentralized application (dApp) that uses the Kairos Protocol™ for KYC/AML compliance
- A voting platform that uses the Kairos Protocol™ to confirm each participant follows voting rules
- A supply chain dApp that requires “human oracles” (humans who enter data into a blockchain) to use Kairos Protocol™ in order to disincentivize fraudulent data entry and other malicious behavior.

FILE REVISION HISTORY

5.14.2018 → VERSION 2.1 → Remove Finance Info for wider distribution

2.14.2018 → VERSION 2.0 → Updated Finance Info for Publish

2.14.2018 → VERSION 1.7 → Added Kairos Protocol

12.24.2017 → VERSION 1.6 → Added Vesting Schedule Clarification

12.23.2017 → VERSION 1.5 → Charts added, use of proceeds, cap table, formatting changes

12.22.2017 → VERSION 1.4

12.21.2017 → VERSION 1.3 → Copywriter & Editor Additional Edits

12.19.2017 → VERSION 1.2

12.19.2017 → VERSION 1.1 → PUBLIC GO LIVE

12.19.2017 → VERSION 1.0 → Copywriter & Editor Additional Sign-off

12.16.2017 → VERSION 0.9

12.13.2017 → VERSION 0.7

12.13.2017 → VERSION 0.6

11.20.2017 → VERSION 0.5

KAIROS

Kairos' mission is to make it easy for any business to benefit from face analysis, enriching the experience between humans and machines, and being the premier partner for anything to do with facial recognition.