UNIKEYS

WHITE PAPER

V1.6

Our objective is to empower people to seamlessly and safely adopt cryptocurrencies into their lives.

Written by
Alexandre Tabbakh

CONTENTS

UNIKEYS

UNIKEYS ECOSYSTEM SUMMARY

Unikeys introduces a frictionless user experience incentivizing individuals, merchants, SMEs and larger enterprises whether they are banked or unbanked, to feel comfortable interacting within blockchain powered ecosystems.

At Unikeys we believe hardware wallets are meant to be highly transportable, safe and easy to use. Unikeys' UKey smart hardware wallet card is making it possible to take secure cryptocurrency payments anywhere. The use of a biometric protection on the UKey card improves the reliability of identification and establishes the most secure way to store and spend cryptocurrencies. Unikeys is a universal provider of cryptocurrency and blockchain payment solutions, enabling seamless transactions as well as creating new opportunities.

Key elements

Smart Hardware Wallet

The UKey smart hardware wallet card is ISO/IEC 7810 & 14443 compliant and has passed all the required tests. It has exactly the same dimensions as your banking card.

Security

The secure biometric authentication allows users to use their fingerprint to safely enjoy the convenience of contactless payments. The UKey card's secure element dynamically calculates and ciphers the card information.

NFC

The UKey card removes the need for USBs. Having the possibility to use the encrypted NFC feature empowers you to design your own contactless payment experience.

EMV

The EMV chip allows you to safely cash in and cash out at affiliated cryptocurrency ATMs. Embedded into the UKey Card, the EMV chip technology is effective in combating counterfeit fraud with its dynamic authentication capabilities.

Universal

The combination of features embedded into the UKey card enables anyone to spend cryptocurrencies anytime, anywhere. Unikeys empowers people to enjoy a solution that fits well into users' life and doesn't require additional infrastructure.

Unikeys Reader

Create your own merchant experience with the Unikeys Reader. EMV and NFC technologies are embedded into the UKey cards to create an effortless acceptance.

Payment Processing

Unikeys allows merchants to easily and safely accept payments in cryptocurrencies. Online through the merchant API or on-site, the payment processor offers the possibility to set up tailor made allocations of cryptocurrencies.

Enterprise Friendly

Every blockchain and distributed ledger networks have their own characteristics. Unikeys has the ability to provide white label solutions on demand, for any cryptocurrency and token powered ecosystems.

BACKGROUND

Unikeys was born from the emergence of security challenges related to the storage of confidential data in cryptocurrency ecosystems and the still unsecure process of contactless payments by card. The rise of cryptocurrencies and blockchain powered solutions are posing a real challenge in terms of adoption. As cryptocurrencies gain popularity, the blockchain industry confronts issues about how users conduct blockchain transactions securely. This has led to an increasing trend for users to hold their own private keys in a secure but accessible manner.

Given our increasingly mobile-centric world an obvious path is to leverage mobile devices to hold confidential data and conduct blockchain transactions. Today many of these mobile applications are only authenticated through passwords leaving a potential security gap. Easy to use multi-factor authentication processes around blockchain transactions are a strong solution to tighten the security and privacy around mobile applications and solving pain points for consumers and merchants.

While powerful institutions playing the role of intermediaries into the current financial ecosystem need to rethink themselves to propose better services, Bitcoin and other cryptocurrencies allowed us to truly envision a world where transacting becomes significantly cheap and easy. We need to maintain this trend and work towards more secure and user-friendly tools to strengthen those abilities.

Unikeys is committed to putting users' first as well as fostering a strong relationship with its community. The team is made of cryptocurrency, fintech and hardware professionals joining forces to build products and services that make a difference and encourage a wider use of cryptocurrencies.

The fruit of Unikeys' work began with the challenge of designing a smart hardware wallet card that would include a dedicated private biometrics layer of protection. The Unikeys team has spent a consequent amount of time testing and expanding the capabilities of its solutions with its partners before deciding to reach back its results to the world.

INTRODUCTION

For adoption to rise, we need acceptance, for acceptance we need trust, for trust we need security and user experience.

The cryptocurrency ecosystem and blockchain powered infrastructure have proven to be here to grow and rise, however certain problems subsist and could impact its reputation. The reason why the adoption of cryptocurrencies increased in the last years happens to be its ease of exchange. Currently this advantage is being challenged due to several factors among which the user experience, and the security frameworks around private key storages. The security standards around cryptocurrency wallets are not only affecting the user experience but also the confidence and trust towards the blockchain ecosystem as a whole.

Unikeys wants to participate in establishing robust security standards in the cryptocurrency ecosystem by making use of game-changing tools in the most professional manner. The Unikeys team is aiming to offer an experience facilitating both the experience of the user who is incentivized to use a highly secure device for daily transactions, and the merchant who does not go through a cumbersome and costly process to accept and embrace cryptocurrency payments.

Biometric technology has rapidly appeared to become a go-to solution for improving digital security and has been adopted by a wide variety of industries, including banking where payment cards using fingerprints for authentication are currently being tested on the market. The estimated value of the biometrics market in 2020 is around US$25.31billion. Collection of biometrics data on national scales like in India, achieved through the rapid progress of Aadhaar, the world's largest biometric ID system with over 1.19 billion enrolled members (as of 30 November 2017) are boosting initiatives taken towards the utilization of biometrics data at different levels. Biometrically powered demonetization is becoming a reality.

A biometrically protected hardware wallet card is a key enabler, not only for exercising a wide range of rights but also for accessing financial empowerment and essential services.

1. The Cryptocurrency Ecosystem: User Experience & Security

1.1. A Problem of Security and Confidence

The risk of a major hack is still one of the biggest risks faced by the global crypto community. Since the Mt. Gox hack in 2014, when $460 million of user's funds were stolen, cryptocurrency enthusiasts have started to become more cautious with the storage of their private keys. An increasing number of cryptocurrency holders have been turning to paper and hardware wallets in order not to become one of those individual who lost their funds sometimes with no way to claim them. In fact, a significant part of investors do not yet fully understand the risks they may be facing by leaving their cryptocurrency assets on centralized exchanges. The level of responsibility systematically granted to exchanges for storing our private keys is not sustainable, especially in a young and fast-changing ecosystem like the cryptocurrency one where myriad of startups are supposed to provide highly secured exchange and storage services.

If a cryptocurrency holder owns and protects his keys, he really owns and controls his cryptocurrencies, if he does not hold his keys, nor back them up, and leaves them on exchanges, he technically does not fully control and own his cryptocurrencies. The danger with any new technologies that are on the path of democratization is the lack or absence of understanding especially from new adopters and enthusiasts attracted by the FOMO (fear of missing out). New cryptocurrency holders encounter difficulties understanding the range of solutions available to control their private keys. Everyone should understand the risks involved when somebody else or another entity is controlling our keys in custodial wallets.

The contactless credit card protocol in use today is insecure. Reliance on NFC's short range has led to poor security standards in the contactless credit card protocol. The current protocol assumes the ability to receive a solicitation and implies the cardholder's intent to purchase. The use of NFC has been standardized more generally in EMV's contactless specifications for payment systems. However, the protocol in use today by contactless credit cards is not efficiently addressing fundamental security issues. Cards are transmitting sensitive information without protection or encryption (credit card number, expiration date, etc.). The number of security vulnerabilities is significantly high and increases not only the risk of being victim of frauds, but also represents an extremely high refunding cost for financial institutions.

Passwords are the most common form of authentication used to control access to information, ranging from the personal identification numbers in use for automatic teller machines, credit cards and voice mail systems to the more complex alphanumeric passwords that protect access to files, computers, and network servers. Passwords are not strong enough but are widely used because they are simple, inexpensive, and convenient mechanisms to use and implement. At the same time, passwords are also recognized as being a poor form of protection difficult to manage. A single local computer network may have hundreds or thousands of password-protected accounts and only one needs to be compromised to give an attacker an entree to the local system or network.

Nowadays organizations are increasingly moving from password-centric to strong authentication solutions. The future of digital security is into biometrics authentication relying in the attributes personal to every individual and where myriad of passwords are not required anymore. Biometrics enables organizations to securely authenticate identified users and gain one of the most crucial elements of any business relationship – trust.

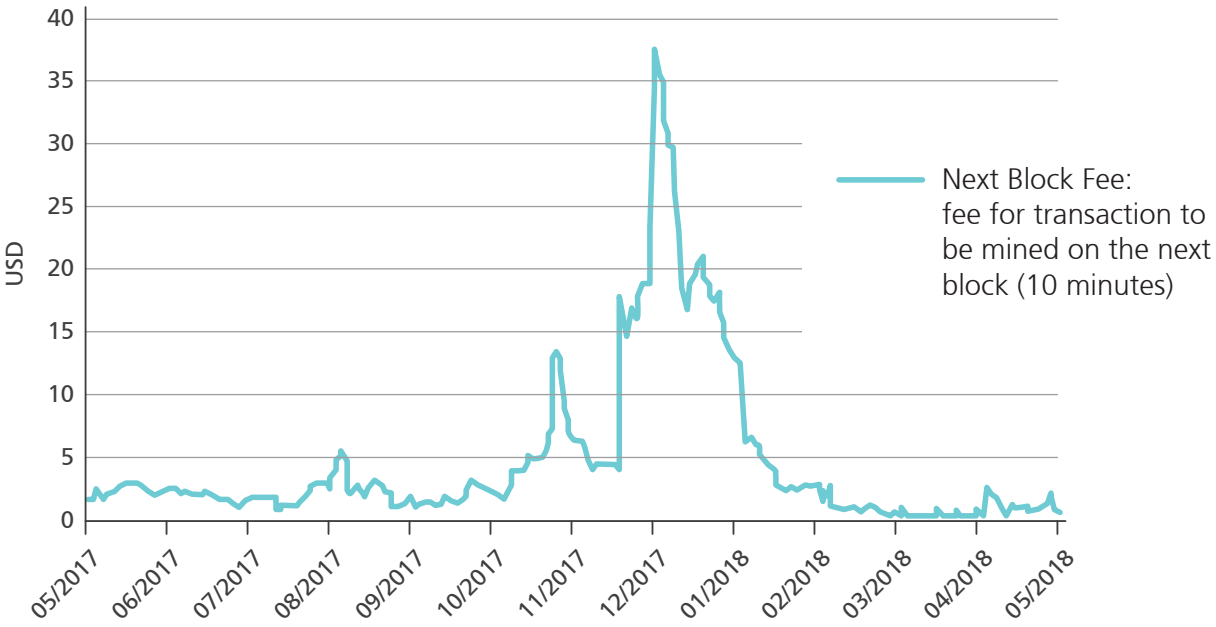
1.2. Scalability and Daily Utilization

Bitcoin, Ethereum and other cryptocurrencies have recently struggled with growing transaction volumes. Bitcoin is for instance processing from 3 to 7 transactions per second, in contrast to more than 2,000 transactions the VISA network completes every second. The negative effects following a high traffic on the blockchain are the drastic increase of transaction fees as well as slower transaction confirmations due to the cap in block size e.g.1MB on the Bitcoin blockchain.

One of the solutions to increase the ability for blockchains to handle higher transaction throughput and avoid blockchain congestions is to increase the size of its blocks. This approach that consists in increasing the memory cap of the blockchain through hard forks is partially solving the problems but may open to a centralization of the network. On-chain scaling which seems like an interesting way to increase capacity and speed may be postponing the resolution of the issues to a later date.

Off-chain transactions and the creation of payment channels between parties seem to be a highly reliable option for cryptocurrency scaling. A payment channel is defined as a class of techniques designed to allow users to make multiple cryptocurrency transactions without committing all of the transactions to the blockchain. In a typical payment channel, only two transactions are added to the blockchain but an unlimited or nearly unlimited number of payments can be made between the participants. The first implementations of off-chain payment channels architectures were made out of Bitcoin (Lightning Network) and Ethereum (Raiden Network). The user experience around payment channels represents a serious challenge since an optimized implementation must allow individuals, merchants and enterprises to easily create new channels and perform high frequency transactions. More details about Unikeys' vision and implementations around payment channels are introduced in the second part of the white paper and in the technical paper.

Bitcoin transactions fees history (May 2017 - May 2018)



1.3. Cryptocurrency and the Current Cards Available on the Market

The current crypto-fiat card providers are relying on VISA and MasterCard networks through the services of third party payment providers issuing debit cards. **In January 2018, VISA decided to abruptly suspend the license of WaveCrest,** a member of both the Visa and Mastercard networks which specializes in providing payment solutions. The event affected several crypto-fiat card providers and a global panic emerged from users who did not receive any warning and suddenly ended up holding deactivated and worthless cards with no way to spend their funds. Being directly exposed and dependent of such networks bring back centralization on the map and weaken the independence of those projects.

This situation is proper to any ecosystems relying on external third parties messaging system or platform owned and governed by external parties. The SWIFT interbank messaging network extensively being used by financial institutions was victim of significant hacks that not only impacted banks, but also central banks, which seriously questions the robustness of our current financial infrastructures.

Crypto-fiat cards have for now caught the attention of a limited part of the crypto community. A game-changing implementation can come through the creation of cards that connect every cryptocurrency holders together and provides new value added services compared to traditional circuits. For merchants and consumers, the 2%-3% fees some of the current crypto-fiat card providers are requiring make the card not better than those already in use.

Traditional cards are not safe as some might think. Today with simple credit card readers available online, thieves can get access to private data and credit card numbers. Intercepting private data from the radio chip inside, copying and cloning is possible without difficulties. We seriously need to be concerned about it and start acting now. Chips with unencrypted forms are highly vulnerable to attacks. With certain devices, the data can be caught from 15 meters away. Unikeys aims to be the leading reference and supplier of smart hardware wallet cards.

1.4. The Emergence of Cryptocurrency Hardware Wallets

Hardware wallets providers have seen their demand boomed in 2017 with certain providers seeing their orders reaching 1 million devices. This phenomenal success is due to two main factors:

- First the number of cryptocurrency holders has exponentially increased in 2017 with an increase of around 50% of the number of blockchain connected wallets worldwide.
- The second reason tarnishes the cryptocurrency ecosystem and lies into the increasing lack of confidence towards centralized cryptocurrency exchanges, sometimes victims of hacks where attackers target private key storages and infrastructures vulnerabilities, leaving users with no way to recover their funds.

A private key is a long stream of numbers and letters that acts as the password to the cryptocurrency wallet and should always be kept secret and safe. The purpose of using hardware wallets is to secure and isolate cryptographic secrets e.g. private keys, from computers or smartphones, which are vulnerable to hacks, in order to protect cryptocurrencies from being stolen.

The wallets core function is the creation, storage and use of the private key. **Hot storage wallets** refer to any form of cryptocurrency wallet that is connected to the Internet. Hot wallets may sometimes seem relevant since they do not require a user to use different transportable devices and hardware wallets to perform a daily transaction; however they represent the least secure technique of private key storage. Web wallets for instance are insecure since the users don't have a direct access to the private keys, which forces users to rely on a third party. Desktop Web wallets store the private key into the computer and are also targets for hackers as they are vulnerable to virus and other malwares. Mobile wallets offer low security and low privacy given the potential association to phone number localization.

Cold storage wallets refer to any type of wallet that is independent of any internet connections (paper wallets, brain wallets or hardware wallets), like physical devices which safely store and isolate private keys. Most hardware wallets provide a seed backup to protect users from unfortunate oversights and losses. The user experience of backing up the private key is still cumbersome, however it is highly recommended to back up the private key knowing how trivial it can be to lose access to a wallet and the cryptocurrencies stored inside. Private keys and passphrases should ideally not just be stored into computers. Currently, cryptocurrency holders tend to secure mnemonic and other secrets recovery tools by printing out their secrets on a piece of paper or saving them into USB drives. Everything happens on the device. If you lose your device, you can still recover your private key using your back up and secret phrases.

The potential dangers for cryptocurrency holders when relying on exchanges are not only problems of hot wallet exposures but also a problem related to the governance of those entities. Exchanges that are not decentralized have proven to be sometimes powerless in front of internal hacks or external attacks. Even if certain participants emphasize on their governance and try to increase transparency, hardware wallets are a strong safeguard solution. The questions a cryptocurrency holder wants to ask him/herself when having to decide whether purchasing and storing his or her private data on hardware a wallet is required are: how much do I currently trust centralised exchanges for storing my cryptocurrencies and private keys? How much do I value my privacy and personal data?

An individual or corporate who wishes to store Bitcoin and other cryptocurrencies securely for the long-term should think of securing its exposure and invest in the most advanced and convenient hardware wallet.

1.5. Biometrics Protection, the New Standard for Security, Conveniency and Privacy

The integration of biometrics, particularly fingerprinting, into financial services has recently started to become a promising trend towards solutions that can address the security issues encountered by the financial industry on identification and authentication of their customers. **A fingerprint is a person's most unique biological identifier as there are no two people who can have the exact same fingerprint pattern.**

Most of the developments in the applications of biometrics are driven by the rise of highly advanced hardware technologies, specifically more sophisticated sensors and scanners, which are integrated into smartphones, wearables, and other innovative devices.

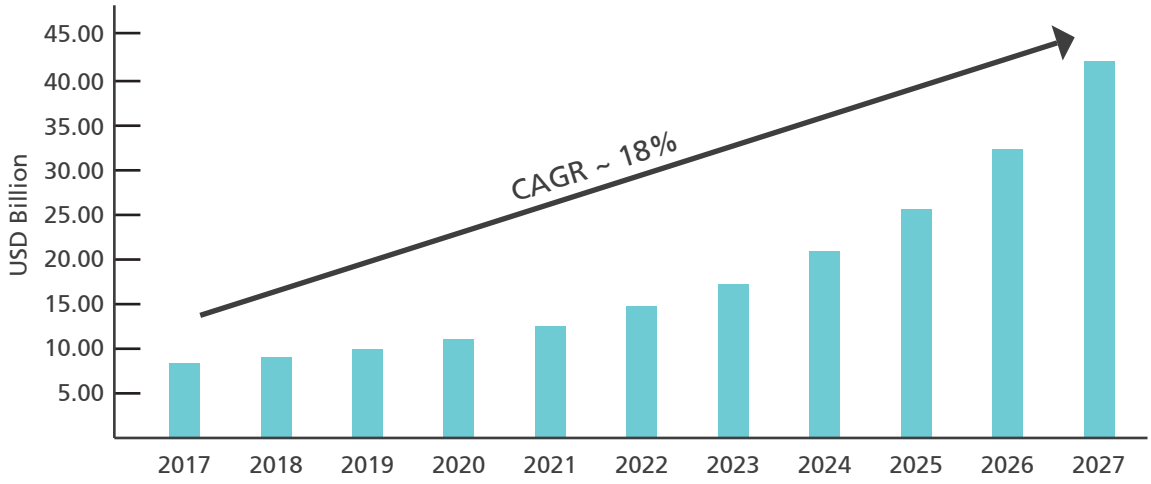
According to Goode Intelligence, 350 million customers used biometrics for payments during 2015. Here are some of its key forecasts in the biometrics space by 2020:

- 1 billion users of biometrics-enabled devices for financial services.
- Over $5.6 trillion of payments secured by biometrics.
- Over 622 million downloads for banking apps that employ biometrics for customer authentication and transaction verification.
- Nearly 160 million wearable devices that support biometrics for banking.

According to recent studies conducted by Frost & Sullivan, the market for electronic identification card should continue to grow and diversify in the coming years. Most European countries have introduced these technologies for identity check, payment or digital signature. According to the Contactless Smart Card Market Research Report (HCR Reports) , **the global contactless smart card market is predicted to reach $25 billion by 2025**.

Smart cards will be extensively used to enable and promote secure payment transactions and cashless payments, thereby enabling cost savings for merchants and offering convenience to consumers.

Global Smart Card Market Size 2017-2027
(USD Billion)



Two-thirds of all adults are comfortable using biometric authentication today, and 87% would consider using it in the future, according to a global study by IBM. "The IBM Security: Future of Identity Study" also found that younger adults are more likely to use biometrics and multi-factor authentication to improve their personal security as they put less effort into traditional password hygiene.

There is no such thing as weak fingerprints. As part of a multi-factor authentication system, biometrics can vastly reduce the chances of hackers breaking into users' accounts.

2. Unikeys

2.1 Objectives

Unikeys designs and creates innovative hardware wallets enabling biometrically triggered wireless transactions, with an end-to-end solution allowing individuals and merchants to secure and facilitate their access to cryptocurrencies. Unikeys is meant to help everyone joining the cryptocurrency revolution.

The proposed solution improves accessibility to essential financial services:

- Secured value storage.
- Convenient cashless payments relying on blockchain and payment channels infrastructures.
- Straightforward cross-border transfers.
- Optimized cryptocurrency acceptance and payment processing solutions for merchants.
- Fingerprint-based identification and protection.

Unikeys targets several groups of users and solve different industry problems.

The number of cryptocurrency holders is increasing at a staggering path. Initially orientated towards the opportunity to cheaply and securely transact in a peer-to-peer manner, the cryptocurrency holders now have various types of objectives: means of payment, utility value, store value and speculation. The community keeps on growing but the ecosystem needs the right tools to trigger a wider acceptance into our societies and at different levels e.g. individuals, enterprises, financial institutions, central banks etc.

Individuals, merchants and other SMEs are currently bearing very high and opaque money transfer costs. Building the most convenient and secure framework to welcome individuals and institutional participants to adopt and transact with cryptocurrencies is entirely part of Unikeys' objectives.

Apart from a very few cashless and crypto-friendly countries where various daily transactions can be performed in cryptocurrencies, it is still very challenging to be able to spend cryptocurrencies on everyday purchases. Unikeys, its ecosystem and the UKey cards are specifically designed to encourage and strengthen the adoption of cryptocurrencies in mainstream payments.

Hardware Wallet Smart Card - The UKey biometrics card is capable of facilitating and securing cryptocurrency payments via **NFC and EMV chips technology**. The UKey Hardware wallet holds the private keys locked away and are protected not by an access PIN but instead by the user's own biometrics information, making it more convenient for day-to-day transactions. The UKey card is built to be compatible with all major cryptocurrencies including first, BTC, ETH, XRP, LTC and BCH (ERC20 tokens will be available on the midterm for consumers but are already available on demand for white label solutions). The UKey card simplifies the payment experience and reduces the time it takes to complete everyday transactions. Cash top-up at the merchants counter and affiliated ATMs will also be feasible.

The Unikeys Mobile App can be used to send, receive and exchange cryptocurrencies: BTC, ETH, XRP, LTC and BCH. Unikeys also wants to connect and facilitate accesses to Ethereum ERC20 tokens whether they are native Ethereum tokens, or tokenized assets. On the midterm, Unikeys is committed to implement payment channels feature in order to provide a frictionless experience when interacting on-chain, and off-chain using channels. The Unikeys team is testing different implementations and is currently developing the first smart hardware wallet based payment channels transaction (Part 2: Unikeys-Payment Channels).

The Unikeys Merchant Ecosystem

- **The Unikeys Merchant App** is designed to be convenient to plug in for merchants who can accept UKey cards powered transactions. The Merchant App can be used with a dedicated merchant API and proposes customizable features which include payment functions, fund transfer, bill payment, prepaid top up, and customizable loyalty management solutions for merchants. **The cost of utilization is lower than the market fees standards, with 0.5%-0.75% transaction fees**. Unikeys will also maintain a midterm focus on testing and adding payment channels features into the Merchant App in order to allow individuals and merchants to efficiently interact using channels.
- **The Unikeys Reader** - Every small, medium and large businesses must have the opportunity to accept cryptocurrency payments smoothly. The Unikeys Reader has been developed to be compatible with all smartphones and tablets that have Bluetooth and an Internet connection, running operating systems iOS, as well as Android. The Unikeys Reader is quick to set up and easy to use, empowering merchants to safely accept contactless payments thanks to the UKey card NFC feature. The device is very easy to transport and can adapt to any environment whether it is a street shop or a brick and mortar store. It has a long lasting battery life, with a stable Bluetooth connection. The Unikeys Reader can be set up in minutes with a few steps to follow in order to pair the device with the smartphone or tablet using Bluetooth.
- **The Payment Processor** - Merchant processing needs to be effortless. An essential development step that blockchain ecosystems and the payment applications built on top of it need to go through is improving user experience and offering the flexibility for merchants to accept and exchange cryptocurrencies into fiat currencies on demand. Unikeys allows merchants to easily and safely accept payments in cryptocurrencies and receive funds directly into their bank accounts, settled in US Dollars, Euros, Japanese Yen and HK Dollars.

Crypto Gift Card - The purpose of the Crypto Gift Card is to make cryptocurrencies accessible and easy. The Crypto Gift Card simply stores an amount of cryptocurrency on a secured card equipped with the NFC feature and allows anyone to physically donate the card or digitally transfer the cryptocurrencies loaded into the card at any time.

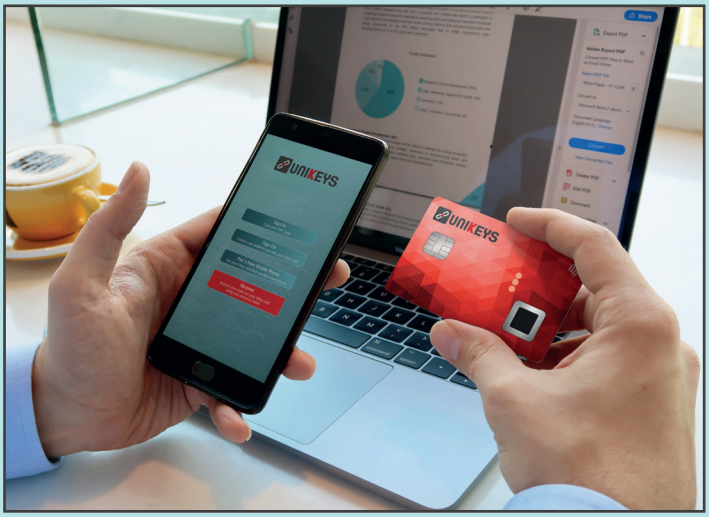
2.2 The UKey Biometric Hardware Wallet Card

The Unikeys team closely works with its smart card designing partner to run a highly secure operating system with a secure element. With the goal of creating alternatives and empower any users to rely on a universal device that can easily and safely be used, Unikeys has developed a solution that unlocks the potential of cryptocurrencies and bridges the gap between enterprises, merchants and the whole cryptocurrency universe.

Biometric authentication in relation to card applications has traditionally focused on external fingerprint readers communicating with the card through a communication interface. The biometric system is usually either residing in a POS (Point of sales) or ATM (Automatic Teller Machine). These systems have security risks associated with them, but more importantly they involve the transmission of sensitive biometric data either internally or even externally between the terminal and the card. **A biometric system on the card eliminates all concerns relating to privacy of biometric data, since the data never leaves the card**.

Unikeys is developing solutions with a focus on user's direct ownership and control over their personal data when interacting into cryptocurrency and blockchain powered environments. **The UKey biometric card** enables the authentication of a card owner by comparing the fingerprint read by the sensor to the fingerprint recorded inside the protected template of the card. The card has 2 main modes of operation:

- **The NFC/RFID mode**
  The NFC mode currently enables the utilization of the UKey biometrics card with the following devices: Android NFC equipped mobile phone or tablet, Unikeys Reader, and also Apple NFC equipped mobile phone or tablet (once Apple's iOS unveils a wider NFC access). The NFC feature technically enables the UKey card to communicate with any terminal or devices equipped with an NFC reader interface, which facilitates further deployments.
- **The EMV chip**
  EMV is a payment method based upon a technical standard for smart payment cards and for payment terminals and automated teller machines (ATM). EMV equipped cards store their data on integrated circuits.



Smart & User Friendly Technology:

1. Open the Unikeys Wallet
2. Place thumb on the sensor
3. Place the UKey Card behind your phone to authenticate and sign your transaction.

The UKey card offers the possibility to store 2 fingerprints. The private keys are isolated inside the card and can only be utilized to sign transactions through an accurate fingerprint authentication. Even if the user's phone gets hacked, the hacker won't be able to retrieve the private keys.

Once the enrolment has been performed and the fingerprints are recorded into the card, pressing the finger on the biometrics sensor will allow the authention and generate encrypted messages through the NFC and the EMV chip. **The biometrics authentication operation takes less than a second** and offer an efficient onboarding process for users. Private and sensitive data are encrypted and only available when the fingerprint authentication occurs. **Out of this period the card does not and cannot transmit signatures**. From now, reduction of fraud and theft can move on a different level since stolen cards become unusable and worthless.

The signal diodes on the card inform the user about the operating state of the card. The card is non rechargable and can be used up to 4000 times.

The 3FA (3 factor authentication) process proposed by Unikeys: What I have (UKey card), What I know (Optional Pin Code), What I am (Biometrics Data) creates a strong chain of authentication for transaction.

The UKey card is a Bitcoin, Ethereum, Ripple Litecoin and Bitcoin Cash and hardware wallet, built on highly robust security features for storing cryptographic assets and securing seamless digital payments on site or online. Light and robust, the UKey multi-cryptocurrency hardware wallet can be carried anywhere and used at any time to trigger transactions thanks to its convenient design.

A smart card includes a plurality of application circuits that are each related to at least one application service securely contained within the card. The biometric circuit is used for authenticating the user so as to generate the activation authorization. The UKey card provides an alternative solution for securing the data stored into a card.

Format
ISO 17839
ISO 7810 ID-1 bank card format

Operational temperature
10°C to 50°C

NFC/RFID Frequencies
13.56 MHz

Contactless Protocols
ISO 14443

Contact Protocols
ISO 7816

OS
Global Platform

Certification
EMV Co & EAL 6+

Reading System
Touch fingerprint sensors

MoC Algorithm
Precise Biometrics
& On Demand

Autonomy
> 4000 uses

2.3. An Enterprise Level Hardware Wallet

Businesses in every industry are aiming to differentiate themselves by providing their clients with a customized experience adapted to their business. At the same time, one of the most efficient paths to design customization is to grant customers the right to choose the way they want to transact. Spending cryptocurrencies needs to become easier, providing flexibility to customers in making their payments, it must also make merchants and other businesses comfortable with regulation. **The Unikeys team is sensitive to legislations, regulations and global industry standards**.

The most common concern with biometric authentication is about the data collection process and the data utilization. A key issue with regards to privacy and the spread of personal information is dealt throughout the devices Unikeys manufactures. Unikeys ensures that the biometrical information of the users never leaves the cards as authentication takes place into the card with no need for external third party based verification. This eliminates the potential for identity theft.

Key standards, certification norms and bodies include:

- **ISO/IEC 7810** is an international standard that defines the physical characteristics for identification cards. The standard defines four card sizes: ID-1, ID-2, ID-3 and ID000.
- **The CNIL** (Commission Nationale de l'Informatique et des Libertés) is an independent French administrative authority whose mission is to ensure that data privacy law is applied to the collection, storage, and use of personal data.
- The UKey card also comes compliant with the **Haifa Center of Law & Technology** under the title 'Privacy in the Digital Environment' which proposed a new definition for the right to privacy.
- **The General Data Protection Regulation (GDPR)** is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). The regulation is enforceable throughout the European Union from May 2018 and is closely observed by other regulators worldwide. The EU data privacy law defines biometric data as "special categories of personal data" and prohibits its "processing", thereby protecting people from having their information shared with third parties without their consent.

Individuals and institutions want secure and convenient payment solutions for themselves and their own users. They also want to make sure regulation is respected and the technology they are using is following the most updated standards. A strong key advantage of Unikeys' hardware is that users' biometric data is solely protected inside the card, enabling trust and privacy.

2.4. The Unikeys Wallet

The Unikeys Wallet offers an all-in-one payment solution allowing users to store, spend, receive and exchange various cryptocurrencies: BTC, ETH, XRP, LTC and BCH. Other essential services such as real time fiat currency value, account balances, transaction history and exchange rates are also included.

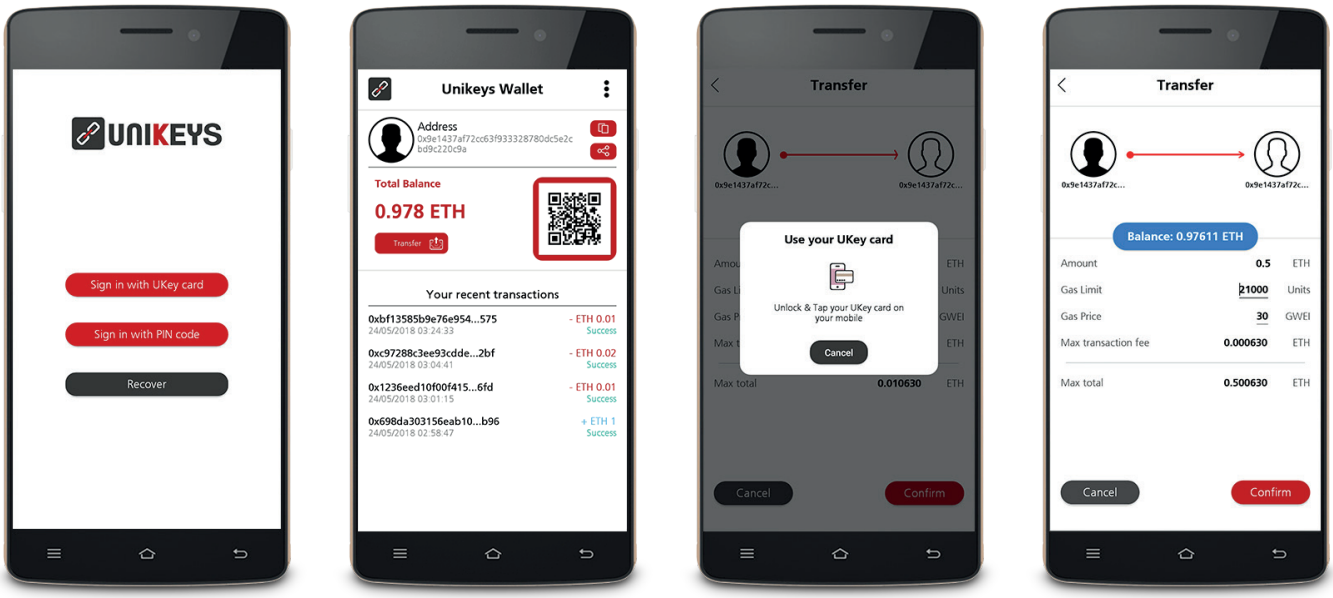
The Unikeys Wallet offers the opportunity for users to perform exchanges using real-time exchange rates. The possibility to add a three factor authentication process gives the users the flexibility of adjusting extra protection layers.

Unikeys has been able to demonstrate the functionality and mechanisms for how the UKey cards can be integrated into the next generation of blockchain wallet and payment services, demonstrate security models for use and revocation of UKey cards and build practical scalable solution suitable for further developments.

2.4.1. Working Pilot Ethereum

The purpose of the Unikeys Ethereum based pilot is to showcase a turnkey solution for the UKey card to secure the private key and interact securely with a mobile wallet application. The proof of concept is relying on Ethereum and allows users to sign up, generate an Ethereum wallet with a key pair (BIP32), back up the private keys with 24 recovery words (BIP39) and use the UKey card to store and biometrically secure the private key. Every single communication between the UKey card (triggered by the fingerprint authentication) and the mobile app are ciphered thanks to an AES algorithm and OTP functions available and embedded into the card.

Having the possibility to back up the private key and write down one or several secrets means being in possession of the key e.g. Mnemonic phrases or recoverable keywords solution. Even in the case of theft or damage to the UKey hardware wallet, a user can restore his or her wallet and tokens with the recovery solutions.



Screenshots from the Unikeys Ethereum App
(For more information or a demo, please contact the Unikeys team)

2.5. The Merchant Ecosystem

The Unikeys Merchant Ecosystem aims to make the adoption of cryptocurrencies by merchants easy and affordable. In order to achieve this goal, Unikeys provides payment and analytics tools that fit the different needs of merchants regardless of their business size and market characteristic.

2.5.1. Merchant App

A merchant can download and install the Merchant App available on both android and iOS powered smartphones and tablets. The Merchant App allows the merchant to sell products and services in exchange of cryptocurrency payments. Signing up is easy. A KYC has to be performed on the Unikeys website before getting started. Merchants need to provide a proof of identity and a utility bill at a minimum. Once the application is approved, merchants can have access to the merchant package they have chosen.

A merchant simply needs a smartphone to start accepting cryptocurrency payment with the Merchant App.

Unikeys proposes two packages for merchants in order to enjoy business tools and complementary merchant services. The Essential package is dedicated for small merchants looking for attracting new type of consumers and diversifying their payment solutions at a limited cost. The Plus Package is dedicated to medium and large merchants who anticipate a higher turnover and need advanced analytics tools as well as additional payment processing services.

	Essential	Plus
Package Target Price	Free	The target price will be set strategically and published on the website.
Monthly Fee	Free	49$
Unikeys Reader	Non included	Included
Merchant App iOS / Android	Yes	Yes
Fee per transaction	0.75%	0.5%
Product Inventory management	No	Yes
Sales Analytics	Yes	Yes
Employee management	No	Yes
Analytics per location & per employee	No	Yes
Wireless printer for receipt included	No	Yes
Support	Full support Phone - Email - Tickets	Full support Phone - Email - Tickets Account manager
Receipt by email	Yes	Yes
Access/validation with UKey card	Yes	Yes
UKey card included	No	Yes
Accept cryptocurrency payments	Yes (BTC, ETH, XRP LTC, BCH)	Yes (BTC, ETH, XRP LTC, BCH)
Cryptocurrency real time conversion	Yes	Yes
Cryptocurrency and fiat wallet	Yes	Yes
Transfer fiat to bank account	No	Yes
Automatic fiat transfer	Yes	Yes
Split payment into cryptocurrency & Fiat	No	Yes
Plugins to accept cryptocurrency payment for ecommerce	Yes	Yes

2.5.2. Unikeys Reader

A merchant has the option to start accepting cryptocurrency payments with the Unikeys Reader. Beforehand, he or she needs to setup and pair the device. When starting the Unikeys Reader, a QR code will be generated to link the reader with the merchant Unikeys account. Once logged into the merchant account, the merchant will see that a new API token has been created for his account. The consumers are now able to check out with cryptocurrencies by biometrically authenticating and tapping the UKey card on the Unikeys Reader.

The Unikeys team believes the adoption of cryptocurrencies by merchants has to offer real advantages, both logistically and financially. The cost of the Unikeys Reader will be set strategically in order to remain competitive for small and larger merchants. The cost of utilization is much lower than the market fees standards (0.5% to 0.75% per transactions).

The merchant can enter transaction details or scan the barcode before the transaction is displayed on the screen of the Unikeys Reader with the actual cryptocurrency conversion rate. A QR code is also displayed. The customer has the possibility to double check the details of the transaction by scanning the QR code with the Unikeys Mobile App. The consumer can then validate the payment either by tapping the UKey card on the Unikeys Reader, or using their Unikeys Mobile App.

Unikeys Reader

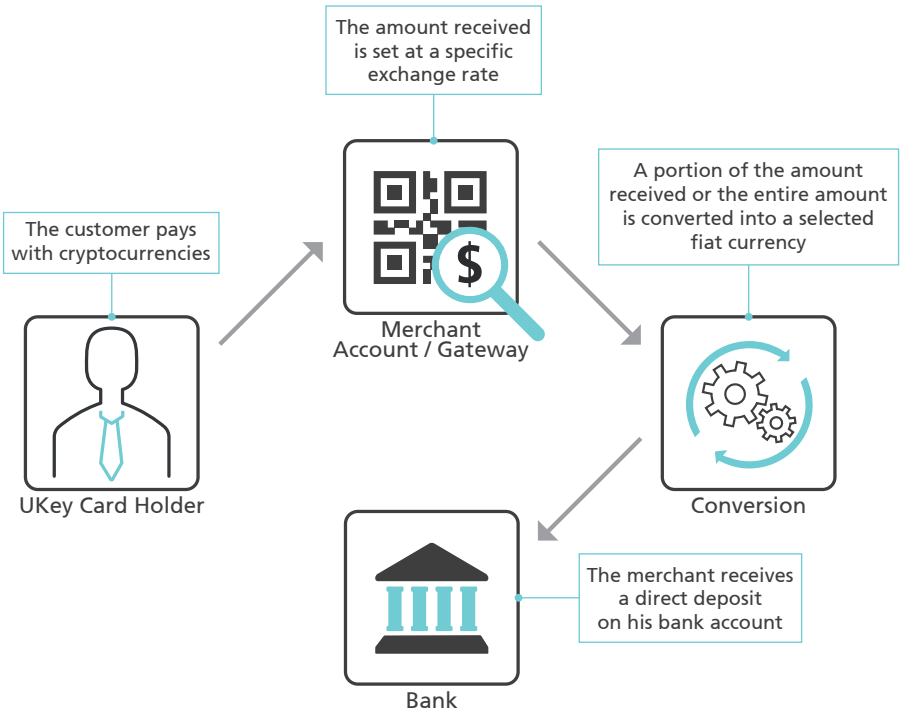
2.5.3. Payment Processor

Speed and ease of transaction between any parties are the main reasons for blockchain to potentially have a disruptive effect on the payment processing industry. Incumbents manage to make traditional payments very fast and frictionless, something that cryptocurrency payment solutions are currently struggling with. The challenge for Unikeys is to provide a payment journey that positively reshapes merchants' relationship towards cryptocurrencies.

Credit cards require to pay around 2%-3% in processing fees on every transaction. Relying on the Unikeys merchant ecosystem payment processor allows to receive direct bank deposits in the merchant's own currency and protects sensitive personal information at the same time for 0.5% to 0.75% transaction fee.

Unikeys offers a hardware wallet acceptance service which enables small and medium businesses as well as larger enterprises to safely and conveniently accept cryptocurrency payments.

Payment Processor Workflow



2.6. Payment Channels

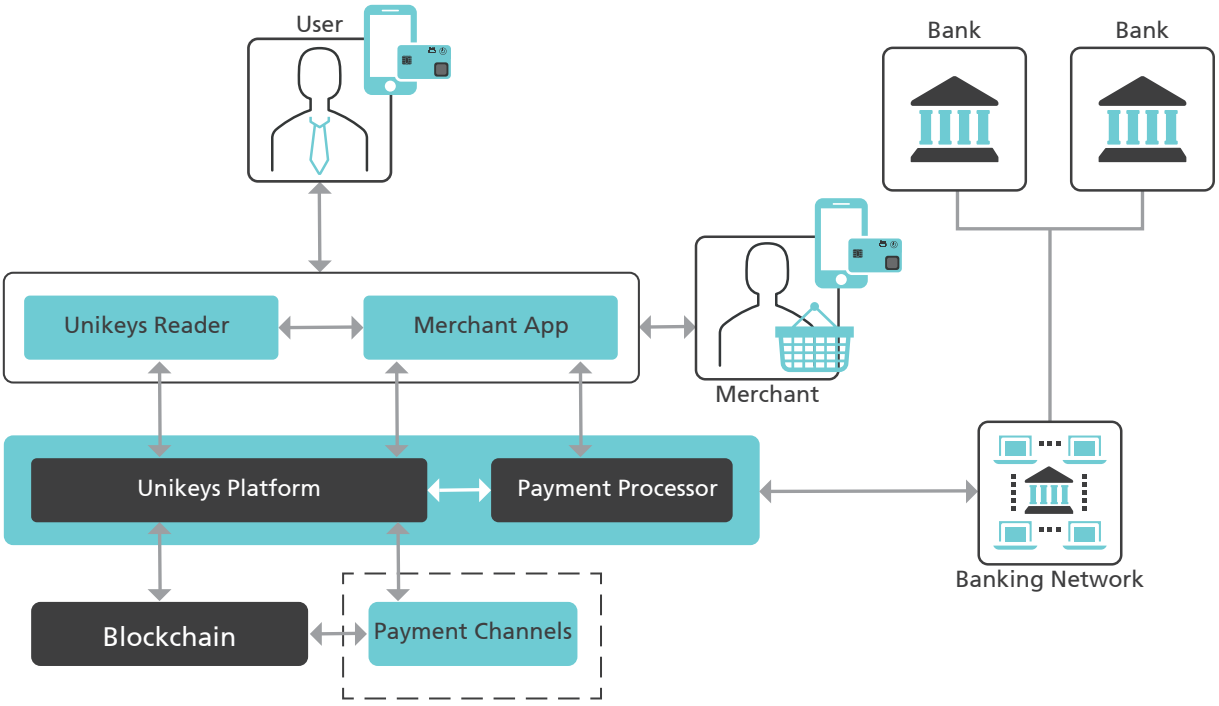
Unikeys believes every one of us into the cryptocurrency community should participate and coordinate actions to come up with the most optimized and complete implementation for wider scalability. In order to make a contribution, the Unikeys team has decided to have a particular focus on testing and developing solutions that democratize the utilization of payments channels.

Even though lightning network (Bitcoin second layer) or Raiden Network (Ethereum second layer) are still at an early implementation stage, Unikeys strongly believes the adoption of such networks will have a strong impact on the public approach towards cryptocurrencies. Decreasing the congestion of blockchain networks could remove one of the main burdens for a mainstream cryptocurrency adoption, generate essential cryptocurrency transaction needs and offer the possibility to instantly exchange and send cryptocurrencies to merchants in everyday life, almost without a fee.

Bidirectional payment channels allow network participants to pay each other off-chain and only broadcast net positions to the network based on their transacting rules. A channel can stay open indefinitely and two users can exchange as many payments as they want. The process works like an escrow function that only releases funds held in a particular cryptocurrency address after some conditions are met. When a certain amount of time has elapsed or when one of the party wishes to close a channel, the channel broadcasts the final state of the pair's transactions to the blockchain, incurring another transaction fee. Because they don't rely on the blockchain, payment channels based transactions can be completed at very high internet speeds. Small payments between parties are not added to the blockchain, but still benefits from the security of the blockchain.

The payment channels infrastructure includes extra cryptographic features that allow users to safely send payments not only through their direct connections but also across their extended networks.

Unikeys Payment Solution



2.6.1. Working Pilot Payment Channels

Unikeys has successfully implemented the first smart hardware wallet payment channels transaction worldwide. For the pilot, Ethereum transactions are performed using Sprites State Channels. The working pilot relies on a merchant website where goods can be purchased, an Android app, as well as a blockchain backend with the payment channels infrastructure. The setup is the following:

- The user has been issued a UKey card.
- The card already has a payment channel setup with a payment provider (here Unikeys), and the merchant also has a payment channel with the same provider.
- The user buys a top-up card.
- The user utilizes the Android app to scan the QR code located on the top-up card in order to fund the channel with ETH.
- The user visits the merchant website to purchase goods.
- Once the user authenticates using the UKey card, the card gets the hash value through NFC.
- The signature is calculated inside the card using the private key and the ECDSA algorithm.
- The card emits the signed transaction through NFC.
- The payment and settlement are made instantly.

2.7. White Label Strategy

The utilization of blockchain and distributed ledger ecosystems will move our approach towards assets beyond money. Land titles, invoices, commodities, loyalty rewards, and other type of assets will be seen under a different and more transparent angle throughout the blockchain paradigm shift. New networks will be designed, new cryptocurrencies and tokens emerge, while users will more and more rely on cryptographic keys to execute transactions. The techniques and processes adopted for securing them will be crucial for keeping security breaches out of reach.

Unikeys, its team and partners are engaged to provide a sustainable progress to the service of users as well as design and operate devices and systems reflecting their needs. Each ecosystem has its own characteristics and needs, that's why developing **dedicated digital strategies** is required to demonstrate agility to customers coming from different industries, potentially using different type of blockchains, cryptocurrencies and tokens.

Financial institutions, loyalty program makers, governments, NGOs and closed loop ecosystems have already started to test and implement blockchain and distributed ledger powered ecosystems. Several major institutions have also announced their intention of proposing blockchain based remittances solutions to remain relevant and competitive. Unikeys will dedicate a **Business Development Engineering Team** to provide professional solutions in line with the need of enterprises. The UKey card will be specifically redesigned depending of the need and characteristics of institutions wishing to implement hardware wallet distribution strategies. Leveraging on existing and new partnerships will help Unikeys create synergies between community members.

The Unikeys authentication solutions with the UKey card allow individuals and private companies to:

- **Conduct business securely** and efficiently as well as open new market opportunities with innovative products that enable secure data access while protecting confidential data identities for employees, customers and business partners.
- **Reduce risk** with strong authentication solutions that prevent fraud and data theft and enable compliance to industry regulations.
- **Expand options** with a flexible range of strong, innovative and simple to use OTP technologies that are easy to integrate, manage and use.

2.8. Financial & Social Inclusion

2 billion people worldwide do not have a bank account or access to a financial institution, and less than a quarter of adults have an account with a formal financial institution in Africa. Those people cannot participate to the economic growth of their regions and develop businesses.

Blockchain technology and cryptocurrencies are one way for lesser-developed countries to jump intermediate stages and catch up on the unfair impact the globalization might have had on certain areas of the world. By encouraging and sponsoring initiatives moving towards a demonetized, accessible and inclusion friendly world, Unikeys wants to maintain a strong focus on the development of financial and social empowerment implementations that can offer unbanked and underserved with highly secure and affordable ways of authenticating, identifying and transacting.

Unlike traditional inert bank cards, the UKey card is an autonomous piece of technology with embedded intelligence that can be activated through the simple use of a fingerprint. The universality of the UKey card can empower low-income and unbanked populations to access financial services that were inaccessible until now.

Commodity trading in western Africa is one of the major drivers of economic growth and represents a major source of revenue for people who live from the different activities surrounding the industry.

For example, in Ivory Coast, the world's largest producer of cocoa and the third largest in coffee, exporters transfer an amount X to their cooperatives' partners who work with commercial agents' intermediaries, called "Pisteurs". Those intermediaries receive very high amounts in order to purchase raw commodities at the plantations. More than 3.000 billion of FCFA ($5.64 billion) went through the hands of the planters in 2016. The losses through poor accounting and corruption reached 100 billion FCFA ($188 millions). The time spent to reconcile and perform cash transactions represents an impediment to business development and allows for fraud to seep in, as funds and salaries are unsecurely transferred.

Here are the different sectors where Unikeys intends to play an important role:

- **Agriculture:** Financial services (payment of goods and services, withdrawal and transfer of money) to producers, and cooperatives. Offering convenient microfinancing and microlending ecosystems to unbanked and underbanked.
- **Energy and Water:** Invoice payments (fixed meters, prepaid, solar kits, etc.). Customer management and billing for water distribution.
- **Public Administration, Education:** In developing and emerging countries where identity registries are not yet efficient or sometimes inexistent, the UKey card represents a very safe and universally applicable solution for identification and authentication of students and employees.
- **NGO:** Biometrically identify refugees and settle their entitlement payments. Offer a more transparent traceability in the distribution and collection of goods and funds.

2.9. A Know How Made in France

For Unikeys to be positioned among the safest methods of storing crypto-assets, relying on a highly professional chain of fabrication from A to Z is essential. The exclusive hardware partner of Unikeys, IDEMIA, is a French multinational company, specializing in security and identity solutions. With 13,000 employees around the world, IDEMIA serves clients in 180 countries and has for instance produced 800 million payment cards produced in 2018.

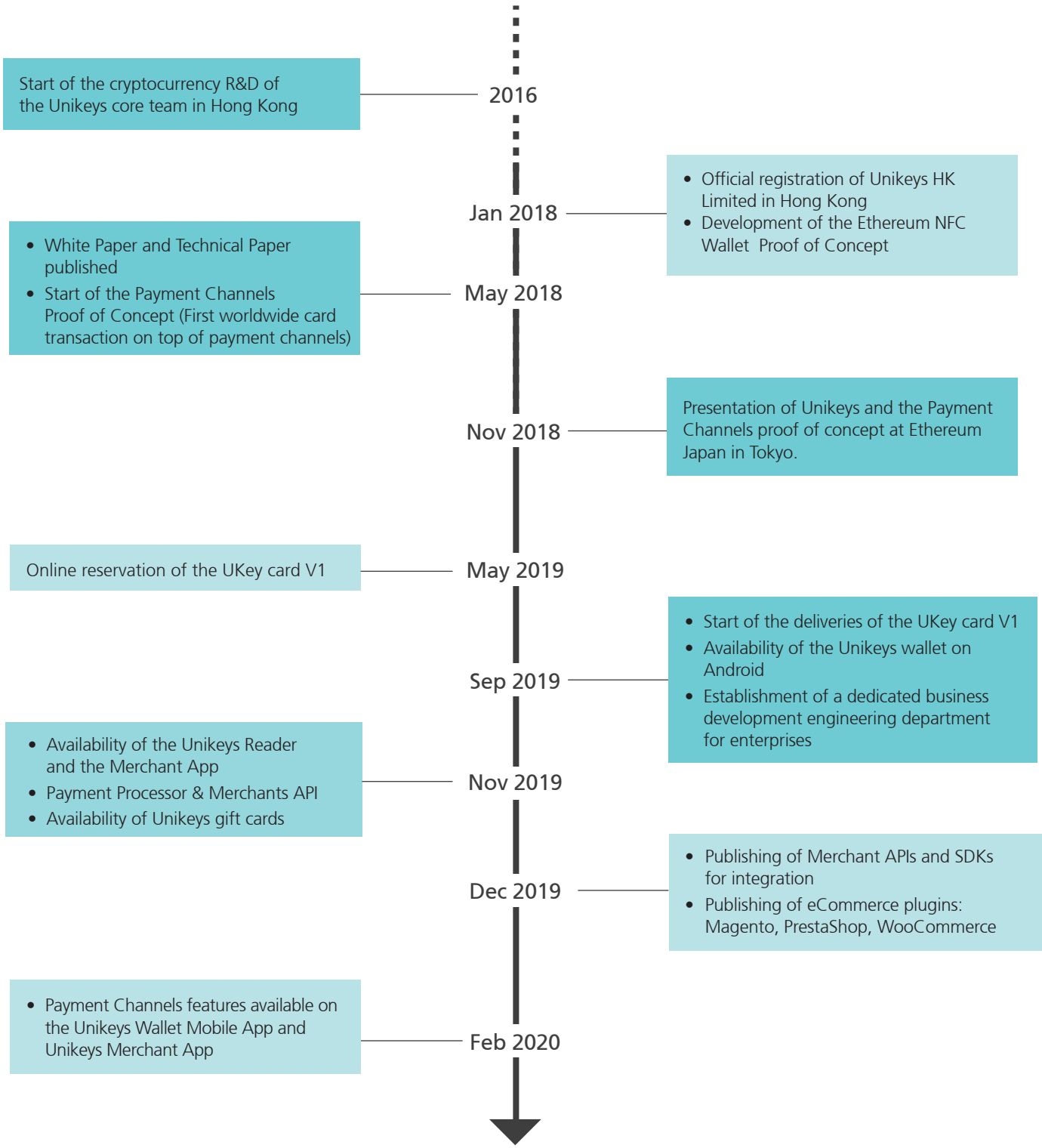
IDEMIA has developed cutting-edge technologies and services leveraging artificial intelligence, biometrics and cryptography. This makes IDEMIA a major technological player in the fields of authentication or security of payments and a significantly strong partner for Unikeys.

The partnership offers a high level of security and provides Unikeys with a significantly large scope for expansion. The R&D team of IDEMIA, the exclusive partner of Unikeys is one of the most important and advanced in the world in card manufacturing industry, biometrics and more generally augmented identity. The smart card designer and manufacturer IDEMIA is being recognized as a precursor and leader in the conception of interactive electronic circuits for biometric cards.

The UKey card provides a foolproof method of storing cryptocurrencies. However new technologiesand intrusional techniques are constantly progressing. For these reasons, Unikeys has built a dedicated stress test framework managed in coordination with its team, its community, and its partners in France and Hong Kong in order to test and challenge the resiliency of the card. Those tests are considered with the highest attention to make sure all devices are following the most updated standards of security.

One of the indisputable advantages of Unikeys lies into its exclusive, strong and transparent connection with its smart card manufacturer IDEMIA. Unikeys has the ability to rely on a growing team with offices in Paris and Hong Kong, to be able to perform testing, researches and new implementations.

ROADMAP


2016
Start of the cryptocurrency R&D of the Unikeys core team in Hong Kong
Jan 2018
Official registration of Unikeys HK Limited in Hong Kong
Development of the Ethereum NFC Wallet Proof of Concept
May 2018
White Paper and Technical Paper published
Start of the Payment Channels Proof of Concept (First worldwide card transaction on top of payment channels)
Nov 2018
Presentation of Unikeys and the Payment Channels proof of concept at Ethereum Japan in Tokyo.
May 2019
Online reservation of the UKey card V1
Sep 2019
Start of the deliveries of the UKey card V1
Availability of the Unikeys wallet on Android
Establishment of a dedicated business development engineering department for enterprises
Nov 2019
Availability of the Unikeys Reader and the Merchant App
Payment Processor & Merchants API
Availability of Unikeys gift cards
Dec 2019
Publishing of Merchant APIs and SDKs for integration
Publishing of eCommerce plugins: Magento, PrestaShop, WooCommerce
Feb 2020
Payment Channels features available on the Unikeys Wallet Mobile App and Unikeys Merchant App

CONCLUSION

While the cryptocurrency dynamics are being challenged, the Unikeys team has spent a consequent amount of time to test and build highly advanced products and solutions to increase security and user experience for the cryptocurrency community, merchants and the enterprise world. The high security combination of biometric fingerprint, NFC and chip technology provide a universal solution for any cryptocurrency and blockchain based ecosystems.

The real value of efficiency is to create new opportunities and make things that were previously cumbersome and unthinkable possible. The Unikeys team is devoted to create and develop products and services that bring people together and reshape the way we interact. The "One for all and all in one" solution is giving Unikeys a unique advantage to take an active role in driving blockchain and cryptocurrency standards forward. Unikeys aims to inspire and encourage as much ecosystems as possible to reshape and enhance security and user experience through the development of users' centered ecosystems.

Unikeys is committed to build sustainable relationships with its partners and community as well as shape a truly accessible crypto world where opacity and doubts are raised. Cryptocurrencies and blockchain networks have led to the creation of new services and payment solutions, the time came to support this trend towards highly accessible and secure standards.

SOURCES:

The Global Biometrics and Mobility Report
http://www.acuity-mi.com/GBMR_Report.php

IBM Future of Identity Study
https://www-03.ibm.com/press/us/en/pressrelease/53646.wss

Counting the uncounted: 1.1 billion people without IDs
http://blogs.worldbank.org/ic4d/counting-uncounted-11-billion-people-without-ids

The Biometric Future of Banking
https://thefinancialbrand.com/61449/biometric-banking-password-trends/

WIREX, TenX, Bitwala, See Cards Frozen, European Banks Refuse to Play with Cryptocurrencies
https://cryptovest.com/news/wirex-tenx-bitwala-see-cards-fro-zen-european-banks-refuse-to-play-with-cryptocurrencies/

Bangladesh Bank Attackers Hacked SWIFT Software
https://www.bankinfosecurity.com/report-swift-hacked-by-bangladesh-bank-attackers-a-9061

EMV Contactless Communication Protocol Specification
https://www.emvco.com/wpcontent/uploads/2017/04/D_EMV_Contact-less_Communication_Protocol_v2.6_20160301114325655.pdf

Contactless Smart Card Market Research Report - Global Forecast to 2027
https://www.marketresearchfuture.com/reports/contactless-smart-card-market-1022

My Vision For SegWit And Lightning Networks On Litecoin And Bitcoin
https://segwit.org/my-vision-for-segwit-and-lightning-net-works-on-litecoin-and-bitcoin-cf95a7ab656b

Bitcoin Transaction Fees
https://bitcoinfees.info/

Payment channels
https://en.bitcoin.it/wiki/Payment_channels

Michael Roland, Josef Langer, and Josef Scharinger. Relay attacks on secure element-enabled mobile devices
https://hal.inria.fr/hal-01518227/document

Crypto Credit Cards & The WaveCrest Fiasco
https://www.financemagnates.com/thought-leadership/crypto-credit-cards-wavecrest-fiasco/

Smart Cards Market Size to Reach $15.4 Billion By 2025
https://www.grandviewresearch.com/press-release/global-smart-card-market

Global Biometric Market to Reach USD 25.31 Billion By 2020 - Estimation & Forecast Report 2015-2020
http://www.marketwired.com/press-release/global-biometric-market-reach-usd-2531-billion-by-2020-estimation-forecast-report-2015-2103248.htm

The world's 2 billion unbanked, in 6 charts
http://uk.businessinsider.com/the-worlds-unbanked-population-in-6-charts-2017-8/#the-vast-majority-94-of-adults-in-oecd-high-income-countries-said-they-had-a-bank-account-in-2014-while-only-54-of-those-in-developing-countries-did-the-middle-east-had-the-lowest-proportion-of-account-holders-with-only-14-on-average-1

Singapore Bank Claims First Regional Use of Blockchain Tech for Remittance
https://www.ccn.com/singapore-bank-claims-first-regional-use-blockchain-tech-payments/c

Lightning Network Main net
https://lnmainnet.gaben.win/

The Haifa Center of Law and Technology Publication Series, Privacy in the Digital Environment.
http://weblaw.haifa.ac.il/he/Research/ResearchCenters/techlaw/DocLib/Privacy_eng.pdf

Biometrics for Banking; Market & Technology Analysis, Adoption Strategies & Forecasts 2015-2020
https://www.goodeintelligence.com/report/biometrics-for-banking-market-technology-analysis-adoption-strategies-forecasts-2015-2020/