How Blockchain-based Multi-biometrics Revolutionizes KYC for Cryptocurrency and FinTech – and what this means for private traders and exchanges

Geoffrey Yuen
Digital Transaction Limited

1 Introduction

COVID-19 has brought face-to-face customer interactions with to a standstill, traditional banks are starting to allow P2P payments and update client information (e.g. home address) on mobile app. In response and without hesitation, the consumers are accepting this easy-to-use and time-saving mobile banking approach. With the disruptions brought about by the pandemic constantly looming overhead, efforts towards remote interaction will continue and persist in the financial sector, including banks and exchanges, currency and asset exchanges in the post-pandemic era.

Meanwhile, crimes associated with Business Email Compromise (BEC), Synthetic IDs, and identity theft have also been on the rise, which is also rapidly forcing a re-consideration of the traditional approach of Know Your Customer (KYC) and Customer Identification Procedures (CIP) processes in the financial industry.

2 Origin and State of KYC

In 2001, KYC verification was introduced and added to the Patriot Act by the Bush administration after the 9/11 attacks. Required for most regulated services, KYC involves presenting sufficient personal information such as name, proof of address and photo ID to the service provider so to ensure that the client is who they claim to be and is not involved in illicit activity. The goal of KYC is to curb crime and to highlight suspicious behavior as early as possible, stopping the flow of illegally obtained assets and the funding of terrorists. This is known as Anti-Money Laundering (AML). However, according to a study by P.A.ID Strategies in 2018, two-thirds of cryptocurrency exchanges in the US and EU (where KYC is required) fail to comply with these requirements, with many banks only asking for an email address and a phone number. (Yahoo Finance, 2018) And despite the strict AML5 Directive[1] that came into force in 2018, not much has changed ever since.

[1] A new European regulation for Anti-Money Laundering and counter terrorism financing purposes.

In addition, there is widespread criticism on the inefficiency of KYC checks as well as the issue of breach in privacy. For example, due to the lack of standardization, each institution develops their own ineffective variation of KYC/AML, risking a chance of being fined for non-compliance (e.g. Deutsche Bank was fined over $200 million for unacceptable AML protocols in 2017).

3 eKYC for Cryptocurrency Traders

Traders are concerned if they can trade cryptocurrency securely and instantly without delays. Having to make physical visits or endure a delay of 1-2 days for a single transaction due to KYC is simply out of the question. There are many objections to the use of traditional KYC for cryptocurrency on several grounds :

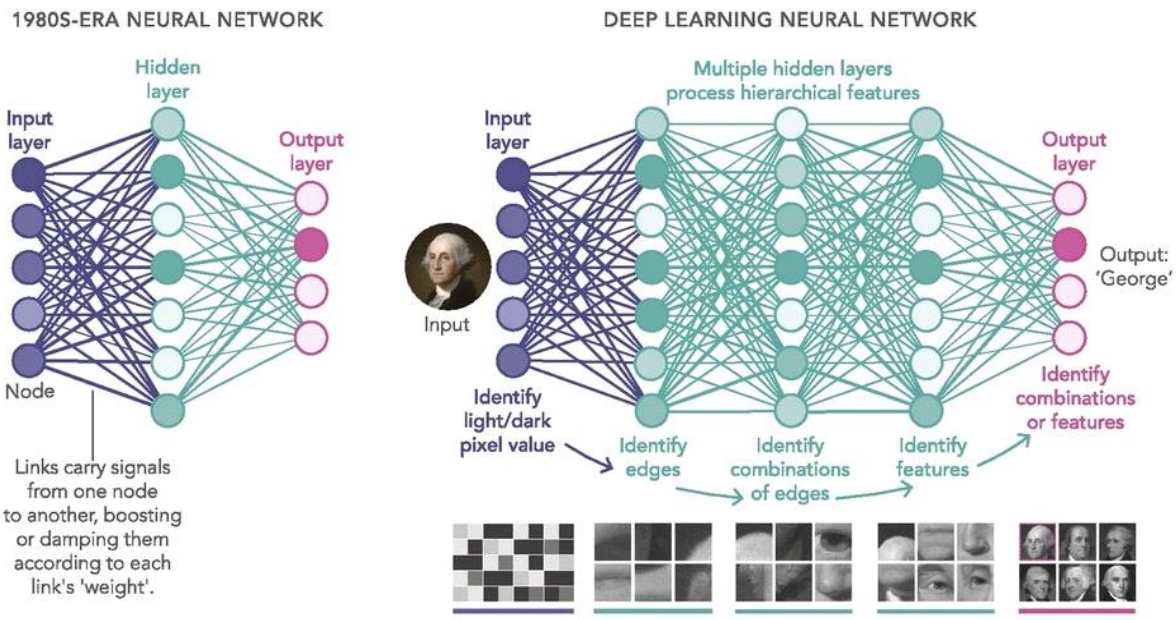
> [1] violation of 'full anonymity' (i.e. neither party needs to disclose their identity when making a bitcoin transaction)
>
> [2] risk of asset loss if passwords and private keys are compromised
>
> [3] personal accounts and information being sold on the dark web by malicious insiders or hackers

Here we shall cover [1] and [2] first; [3] will be addressed in section 6.

An early setback to the use of KYC for cryptocurrency involved thefts of large sums of bitcoin where user passwords were captured through phishing. This reveals the real issue with full anonymity: one cannot prove ownership of crypto asset without revealing their private key since there has never been any verifiable connection between the asset and the owner's unique identity attributes. (Bohannon, 2016) Replacing passwords with biometrics is the obvious and necessary first step because biometrics are unique physical identifiers and cannot easily be forged when used in conjunction with anti-spoofing. Thanks to latest developments in deep learning, both verification accuracy and anti-spoofing reliability have reached commercial standards for deployment.

4 Deep Learning-powered Biometric Authentication

Deep Learning, considered as one of the major technology breakthroughs of the 21st century, is the leading paradigm for solving pattern recognition problems owing to its supreme performance in accuracy and generalization when trained with big data. It has surpassed traditional approaches and human level performance in diverse fields such as computer vision (>96%), Machine reading (88.5%), Machine translation (69.9%), Conversational Q&A (89.4%). (Levy, 2018)



(image 1)

Image 1 illustrates how a deep neural network is trained by data to learn to recognize a person (i.e. George Washington). Connection strengths between successive nodes are adjusted by an optimization algorithm whenever the output is wrong with respect to the inputs. The bottom inset shows how deeper layers to the right learns the higher level representations (i.e. George versus other U.S. presidents).

At Digital Transaction Limited, we have embarked on a mission to develop performant and accurate deep learning biometric identity verification solutions based on learning from small amounts of data, such as a few photos or spoken words from a person. The following table documents our progress as of Q1 2021 for face verification, face anti-spoofing, palmprint and voiceprint verification. These results provide a reliable basis to support authentication in lieu of traditional password security for enterprises as well as mobile internet users.

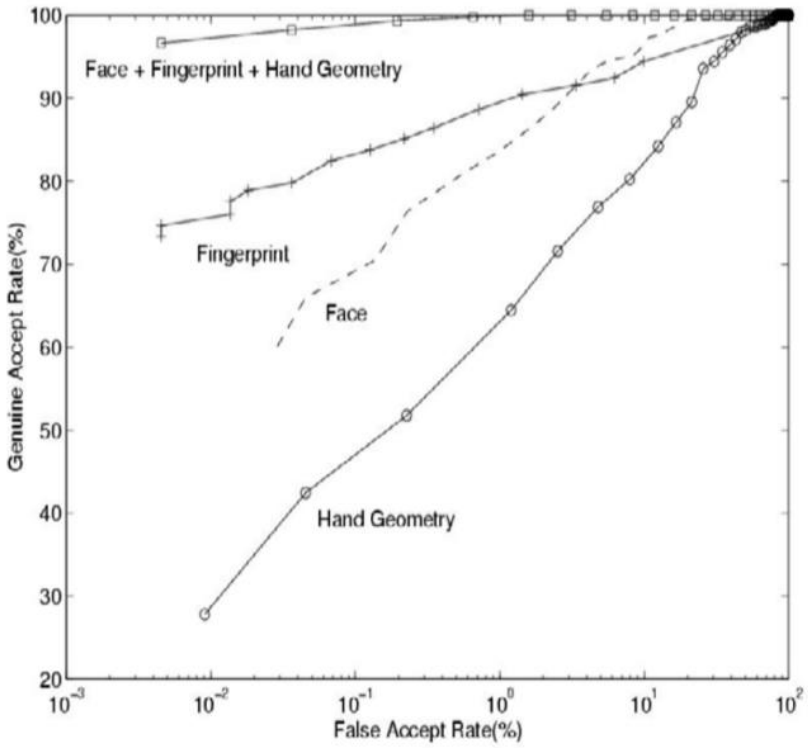
	ACC	EER	FAR	FRR	Public Dataset tested*
Face verification	0.999759	0.000241	0.00003127	0.00045	VISA
Face anti-spoofing	0.997192	0.002818	0.004704	0.000931	Replay Attack
Palm verification	0.9426	0.05740	0.0933	0.0215	Tongji
Voice verification	0.9970	0.02500	-	-	LibriSpeech

(table 1)

* Models trained with multiple datasets, testing performance with public dataset for comparison only.

5 Multi-biometric Authentication for Stronger Security and Flexibility

Elementary probability states that the joint probability of two independent events is simply the product of the individual probabilities. This gives us an opportunity to achieve much higher confidence rates than any single modality. This is illustrated in a research paper from 2004 by combining face, fingerprint and hand geometry data for recognition (top curve) with best performance. (Jain and Ross, 2004)



(image 2)

A familiar imaginary example would be if we were to ask an iPhone user to unlock the phone by passing both the TouchID and the FaceID, then the chance of a false match will become miniscule: 1 in 50,000 for the fingerprint false matching rate multiplied by 1 in 1,000,000 for the face false matching rate gives a chance for a joint false match of 1 in 50 billion. A properly implemented multibiometric solution will always works better than any single biometric for discrimination and false rejection.

In fact, many circumstantial or environmental factors may present challenges to services that rely on single biometric trait in the long run. For examples, a user's face may be deformed beyond recognition from injury, or the voice can be temporarily lost from sickness. Such considerations convince us that a multi-biometric solution for authentication is necessary for the KYC to be highly secure yet flexible. The strengths and weaknesses of single versus multi-biometrics are illustrated in image 3.

(image 3)

6 eKYC with Secure Biometrics Handling for Exchanges

Globally, KYC and AML regulations are becoming stricter. As of Q1 2021, many countries already have, or are putting, such regulations in place for cryptocurrency exchanges, the intensifying regulatory scrutiny is inevitable.

The development in multi-biometric-based eKYC can help cryptocurrency exchanges to automate customer onboarding reliably and quickly, while reducing manual checking of customer personal data to improve privacy and facilitate subsequent AML checks. However, an exchange's additional burden is the secure custody of customer biometrics data with ongoing privacy protection, as theft of customer data and assets can originate from hackers as well as insiders. We maximize the protection of customer biometrics data using the following layers of data abstraction and technologies:

[a] No readable biometrics files (e.g. jpg, wav) are stored in the system; mathematical derivations of biometric data obtained from deep learning, called "embedding vectors", are kept scrambled and encrypted. The scrambling process destroys all correlation to the customer biometrics so the data would be completely useless even if compromised without the original model, encryption key and descrambling method.

[b] Integrated with ParallelChain®[2], the biometrics-derived data inherit the benefits of:

i. immutability for countering identity tampering; and
ii. patent-pending "Ability to Forget" capability allowing sensitive customer data to be purged after usage, in accordance with the EU General Data Protection Regulation (GDPR).

[2] Blockchain infrastructure developed by Digital Transaction Limited.

A widespread opinion in the biometrics industry is that blockchain cannot be used in the safekeeping of biometrics data as blockchain records are made permanent, however, the unique capabilities of ParallelChain® make it both flexible and secure for privacy protection.

[c] It is well known that more than 50% of corporate data breaches originate from insider attacks. Digital Transaction Limited has developed a unique solution PreventiveChain to combat this by using continuous anti-spoofing face recognition. With PreventiveChain, all operator and programmer activities are logged and immutably stored on the ParallelChain® blockchain. This prevents illicit activity of insiders because there is no way to delete the access records to cover one's tracks if customer data or records are improperly accessed or tampered with.

References

1. Bohannon, J. (2016) Why criminals can't hide behind Bitcoin. Available at: https://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin

2. Jain, A. K. and Ross, A. (2004) Multibiometric Systems. Commun. ACM 47, 1 (January 2004), 34–40. DOI: https://doi.org/10.1145/962081.962102

3. Levy, N. (2018) Microsoft claims AI program just as good as human pros in Chinese to English translation. Available at: https://www.geekwire.com/2018/microsoft-claims-ai-program-just-good-human-pros-chinese-english-translation/

4. Yahoo Finance (2018) Bitcoin Prices Fall; Two-thirds of Crypto Exchanges Not KYC Compliant, Study Finds. Available at: https://au.finance.yahoo.com/news/bitcoin-prices-fall-two-thirds-074200560.html?soc_src=social-sh&soc_trk=ma

---

Author Biography:

Dr. Yuen spearheads the efforts of integrating artificial intelligence and emerging technology into the next generation of blockchain technology. Dr. Yuen was Vice President of Emerging Technology at PCCW leveraging on various emerging technologies to establish market advantages with economic payoff. Amongst others he helped contributed to broadband television, e-health and big data business. While building Morningstar's internet infrastructure in Chicago, he created the world's first commercial web service for retirement investment planning. He was a Chief Investigator at the US Naval Research Office Center for Neural Engineering in Nashville Tennessee researching on biologically motivated unsupervised neural network learning and applications in vision, speech and navigation.

Geoff holds a BS in chemistry from Wheaton College and a MS and PhD in biomedical engineering (neuroscience) from Case Western Reserve University.

Published online 2021.06.23