Business Application: Integrating NISQ-era Quantum Random Sampling into Fraud Detection Workflows

By Team 3: Oleg Fonarev, Estelle Inack, Alex Khan, Ziwei Qiu, Yuval Sanders

Technical Explanation

Quantum Random number generation

The ability to make accurate estimations lies at the core of many diverse fields ranging from election polling, finance, artificial intelligence, cryptography and physics. The common denominator of these fields is that a metric is evaluated not on its true population - which in some cases is impossible to obtain exactly due to its nature (e.g. census) or its dimension (e.g. stars or galaxies) - but on a sample population. Thus, in order to accurately represent the probability distribution of this sample population, random numbers generation have been used. However, for practical purposes, most of the applications referenced above are modelled via computer simulations and it is impossible to generate true randomness on CMOS hardware. Pseudo-random number generation is typically the way to go. Though they offer the advantage of reproducibility, the deterministic nature of their generation carries a non-zero risk in application where security and unbiasedness are critical.

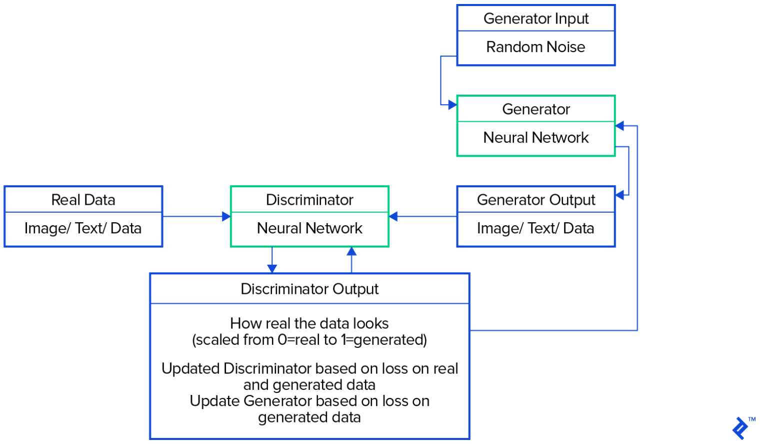
In this project, we address this issue by leveraging the laws of quantum mechanics to generate true random numbers via programmable quantum processors based on trapped ions. The core of our technology lies in the ability of random quantum circuits to generate a large number of random numbers from a probability distribution of an exponential sample space. They do so on time scales that are unrealistic for traditional computers while saving enormous amounts of resources (e.g. space, power consumption) with a guarantee of true randomness similar to the one of dice throwing.

In the following, we highlight how such a quantum sampling could be combined with state-of-art machine learning techniques to solve relevant problems in the finance and health care sectors.

Quantum Random sampling and GANs

Both supervised and unsupervised machine learning algorithms require large sets of training data. With the advance of deep learning algorithms and their integration into business workflows, such as credit card fraud detection, specialized quality data became a scarce commodity. Various techniques, such as data augmentation, are used to work around the data scarcity issue.

Some recent studies suggested that incorporating random noise into various generative adversarial networks (GANs) architectures can be used to extend limited data sets and to improve efficiency of machine learning algorithms.



Model for classical GAN from Toptal

The Google Supremacy experiment inspired us to conceptualize a modified architecture of the above figure by replacing the classical random generator with a programmable random quantum gate circuit model (PRQC). PRQCs can be used to generate random numbers with desired probability distribution and low Kolmogorov complexity more efficiently than available classical algorithms. It can also be argued that PRQC with sufficiently large numbers of qubits and gates are able to generate rich sets of random numbers with desired statistical properties that classical algorithms will never be able to simulate given realistic resource constraints. NISQ-era PRGCs are affected by random quantum noise that may distort a desired probability distribution. However, the latter effect can be mitigated by using GANs workflows and other deep learning techniques.

Real-world use case

As stated in the report by EvolutionQ, Quantum Random Numbers have many applications in protecting high-value assets and critical systems. This includes cybersecurity, lottery and casino for security and trust, manufactured equipment and product tagging and identification, public services or polling fairness and allocation of scarce resources. In addition, the report also identifies Financial and Healthcare services where it is critical to protect private information and prevent fraudulent use.

Fraud Detection

Our proposed technology has many applications in improving machine learning to create more realistic images, voice and videos (Deep Fakes).

It can also be incorporated into fraud detection software which is always struggling against new and innovative methods and patterns not yet discovered. The Quantum Enhanced Fraud Detection provides a unique and new model that will surpass classically trained methods by augmenting them with certified randomness.

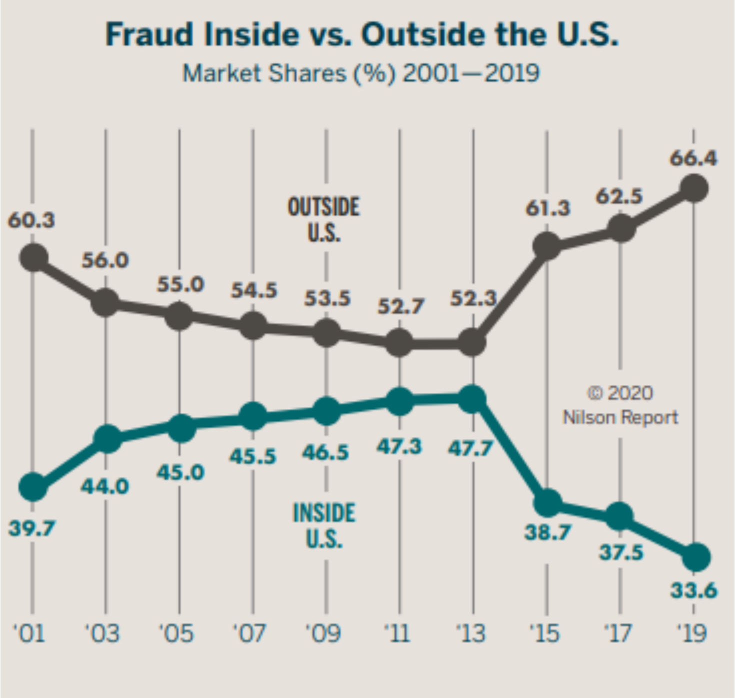
Random patterns or random number generators may help with creating unique and varied learning opportunities for a GAN. Which gives it its strength. We propose that the random numbers generated by random circuits (as used in the Google Supremacy experiment) could be used to achieve better learning opportunities for GAN than done classically.

We also expect that this quantum enhanced learning could be used specifically for the Fraud Detection market. Even though there are many strategies and products for fraud detection as identified in the Gartner Report, our focus will be on two specific verticals: Banks and Health Payers. This allows us to focus our Quantum machine learning efforts based on patterns in these two specific areas. Provide two specific sets of tools for each market that provided better detection of fraud than classically trained GAN products.

Potential customer for this solution

Financial Market and Global Banks:

According to the December 2020 Nilson report global credit card fraud reached $28.65 Billion (up 2.9% from 2018) with the United States market share dropping to 33.6% while that outside the United States reaching 66.4%.



Some banks are not even monitoring or taking an active role in reducing credit card fraud.

In this area our target market is large banks with presence around the world. We select one representative bank from each country to review challenges in working with that market.

We have selected the following 10 Banks as a starting point for research and communications:

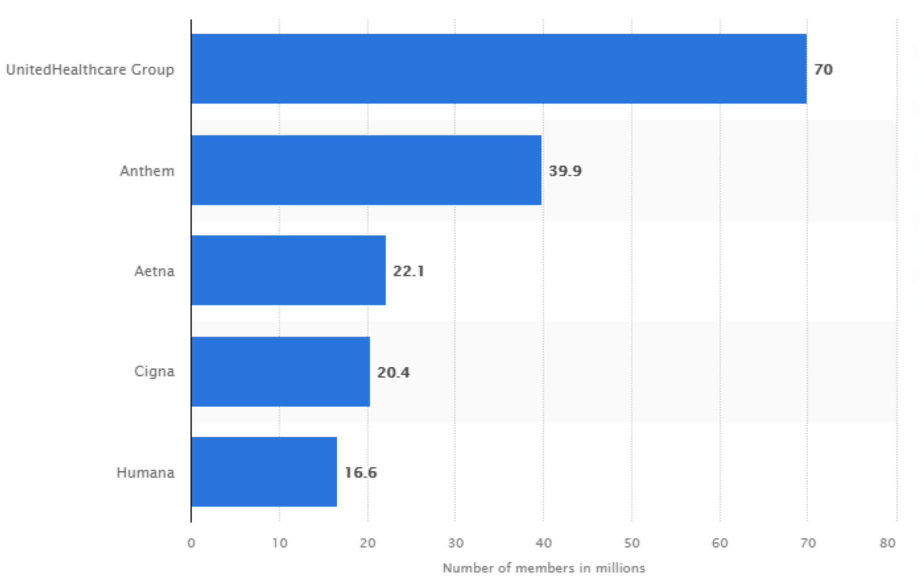
1. Industrial and Commercial Bank of China ($5.1T)
2. Mitsubishi UFJ Financial Group Inc - Japan ($3.4T)
3. JPMorgan Chase & Co -US ($3.4T)
4. BNP Paribas SA - France ($3.0T)
5. Banco Santander SA - Spain ($1.8T)
6. Barclays PLC - UK ($1.8T)
7. Deutsche Bank AG - Germany ($1.6T)
8. Toronto Dominion Bank - Canada ($1.3T)
9. Intense Sanpaolo SpA - Italy ($1.2T)
10. ING Group - Netherlands ($1.1T)

Health Care Market and Insurance Companies

The National Healthcare Anti-Fraud Association report estimates health care fraud at about $68 billion annually (3% of national spending). However there are estimates as high as 10%.

Even though Health Care fraud can happen in many forms and at many locations including at small clinics, payers (insurance companies), and hospitals, we will be targeting the large US based insurance companies and focus on claims fraud. This is an area that is heavily regulated and considerable data is available within the payers.

The largest payer in the United States is CMS.



In the figure above from Statista, the US largest insurance companies are identified. In addition, Kaiser Permanente operates as both an insurer and provider by having its own clinics and hospitals. Thus we identify the following organizations to start our conversations on the capabilities of our quantum enhanced fraud detection.

1. CMS
2. United Healthcare
3. Anthem
4. Aetna
5. Cigna
6. Humana
7. Blue Cross Blue Shield Association and companies