01's Post-Quantum Blockchain

June 2018

Background

Since 2017, 01 has been working on its "next technology" because regardless of winning or losing our CAFC appeal it is time to prepare for the next chapter. While we are not a believer of cryptocurrency, we are fascinated by the underlying technology that drives cryptocurrency - blockchain (or to be precise, DLT - Distributed Ledger Technology).

Our discovery

We are excited by its inherent security as well as the natural redundancy duplicating the database in all the nodes. Traditionally "cyber security" is achieved by encrypting data with public/private key mechanism. This is secured because it is very difficult to "reverse engineer" the private key back from its public key using today's technology. The BC technology brings cyber data security to a new level because of its distributed nature as well as the "link mechanism". New block of data certified by the private/public key mechanism is also linked back to the previous block by a hashed value. This makes transactions "saved for life" and "unchangeable". As a result, by combining private/public key encryption mechanism and the BC technology it is a general belief that cyber data is "bullet proof". Hence, the BC technology is proliferating fast worldwide during the last 2 years.

Problems

While the BC is in development there is a "quiet trend of development of a new breed of computer" called the Quantum Computer. The Quantum Computer was first proposed by some scientists such as the famous physicist Richard Feynman in early 1980s. The concept is that instead of silicon based (with only on/off states) it is based on quantum mechanics that "qubit" can contain many different states. Therefore, its computational power is exponentially higher. As of 2018 the Quantum Computer is no longer a fictional item. Companies such as D-wave, IBM, etc. already have working models in their labs. The Quantum Computer's excessive computational power is specifically capable of cracking private/public key encryption mechanism in-use today. This imposes a real threat to basically all cyber security today, including the new BC technology.

Another threat we noticed is that hardware/firmware by Intel and AMD has "backdoor" so that knowledgeable hackers can by-pass encryption and gain direct access to the memory.

R&D performed

We have designed a specific way to solve the above 2 threats. We will develop a "super secure" BC technology as opposed to the standard BC technology. We call this PQBC (Post-Quantum Blockchain). It is important to note that while our PQBC technology is safe against Quantum Computers its infrastructure does not need Quantum Computers to build. In other words, it is implemented on classical computers but can withstand the threat from Quantum Computers.

Applications

Similar to traditional BC, PQBC can be applied to virtually anything that:
1: Needs to store data; and
2: Has multiple writers who don't trust each other

Today, #2 is solved by a TTP (Trusted Third Party) such as a Central Settlement house for stock settlement; or SWIFT in its secure messaging (ISO 20022) for money transfer . E.g. The ASX (Australia Stock Exchange) has just completed their feasibility study less than a month ago that they are moving towards using BC technology provided by Digital Asset (it is not a PQBC technology). Please see the document "ASX paper".

PQBC is a Disruptive Technology (DT) replacing the role of a TTP by charging a small fraction of the fee because PQBC management is far cheaper. PQBC is also a Fundamental Technology (FT) serving brand new markets such as e-voting, plugging identity theft, supply-chain management, etc.

Market size

Market size is huge as either a DT or a FT. For example, a stock exchange with 4m transaction a day represents $200m revenue per year if only $0.2 is charged per transaction. Another example is that SWIFT is handling 12m transactions per day and they are charging 5-10 Eu per transaction. $0.2 per transaction means $400m revenue per year. Note: It is tougher to break the SWIFT-monopoly because they are owned by banks but this serves as a quantifiable market size.

FT potential is less quantifiable since it is new but it is not difficult to foresee a huge market. For example, a government should move its identity database of everything (birth certificate, driver license, health card, etc.) centrally into a PQBC technology so that IDs are represented digitally by, for example, a QR code rather than physically entering an ID, etc.

Go-to-market

Our business model is to charge a per transaction fee on our customers. Our plan is to allow customers to create their transactions on our permissioned PQBC. Alternatively, we can setup a PQBC for our customers if they rather trust their own PQBC. We can also tailor our technology to suit any industry that requires cyber data security.