A special feature brought to you by Singapore Management University

TACKLING SOCIETAL CHALLENGES

This is a monthly series on SMU research which aims to create significant impact by addressing these five societal challenges: Economies & Financial Markets, Social Fabric & Quality of Life, Boundaries & Borders, Sustainability, Innovation & Technology.

In this issue, SMU researchers offer insights on tackling the societal challenge of advancing innovation & technology.

A potential quantum leap for blockchain applications

Quantum computing could help overcome a problem that has been holding back the power of blockchains

The world of quantum technology – often associated with science fiction such as in the Ant-Man movie in 2015 – was in the spotlight recently after Google computer scientists released a paper in September claiming that a quantum computer had demonstrated "quantum supremacy", which describes the potential of quantum computers to significantly outperform traditional ones.

According to the Google paper, the device was able to perform a calculation in 200 seconds what the scientists claimed would take 10,000 years by the fastest classical computer. However, IBM scientists soon came out to refute this claim, saying that a classical computer could be tuned to perform the calculation in just two days.

While an ordinary or classical computer stores data and performs computations as a series of bits that are either 1 or 0, a quantum version uses qubits, which can be 1 and 0 at the same time. The properties of qubits allow quantum computers to perform billions of calculations simultaneously, far outpacing the fastest classical computers.

According to Associate Professor Paul Griffin from the Singapore Management University (SMU) School of Information Systems, quantum devices make the computations "probabilistic", as opposed to "deterministic". So instead of the deterministic "1+1=2", in the quantum world it would read as "the probability of 1 + the probability of 1 = a probability of 2".

"Obviously, for many applications you do need deterministic answers but there are quite a few applications that are probabilistic in nature and a quantum computer should be much more useful," he said.

"For example, pricing a company stock depends on many events in the industry and markets and there is no deterministic answer to what the correct price is, but there is a most probable price and the trader who is closest to the most probable price will get the most profit."

Associate Professor Paul Griffin

Solving the blockchain trilemma

A recent study by Assoc Prof Griffin argues that quantum computing could be used to solve what is known as the "blockchain trilemma", which refers to the notion that improving all three fundamental attributes of blockchain – decentralisation, scalability, and security – at the same time is not achievable. For example, a larger network is harder to secure, or the more decentralisation there is, the less scalable the network.

A blockchain is essentially a way of keeping records securely on a digital platform. The technology that drives cryptocurrencies such as Bitcoin is finding a growing number of applications across different industries; from logistics to financial services.

According to Assoc Prof Griffin, quantum computing could resolve the blockchain trilemma by introducing highly secure networks. Quantum algorithms could also potentially provide better data privacy for blockchain interoperability, thus improving decentralisation while maintaining scalability. Finally, scalability could be enhanced due to the very high speeds that information can be transferred between quantum computers using quantum networks.

Overcoming these obstacles will address the issue of the interoperability of different blockchains, and lead to greater and safer transfer of information between existing blockchains. Quantum computing could also potentially offer faster performance in searching blockchain transactions. SMU has just begun a collaboration with OneConnect Financial Technology Co Ltd, an associate company of China's insurance giant Ping An Group, to explore these issues and solutions. The research collaboration will focus on studying quantum algorithms that could augment blockchain technology in areas of robust large-scale consensus, efficient on-chain data searching, private record validation, high-speed smart contract processing and interoperability between blockchain networks.

However, there remain several major obstacles to using quantum computing to tackle the blockchain trilemma. Firstly, the current performance of quantum devices is insufficient for more than a Proof of Concept.

"Quantum devices still have insufficient qubits for practical applications, the qubits are fragile and noisy and the methods to transfer data into and out of quantum computers is slow," said Assoc Prof Griffin, referring to the fact that noise can interfere with the quantum state of qubits. The cost of quantum devices also needs to come down significantly so that industry players can afford the hardware, while people will need to learn how to use these advanced computers.

That said, recent breakthroughs point to a brighter future for quantum computing. For instance, there is work done related to the use of silicon devices, which promise to be more robust than the current devices for quantum applications. Meanwhile, the number of qubits is increasing and with less noise, as better noise cancelling is constantly being developed. Said Assoc Prof Griffin: "The future for quantum computing is very exciting."

Scan the QR Code to listen to the podcast on this topic

Enhancing consumer and investor protection in Initial Coin Offerings

The hype over Initial Coin Offerings needs to be accompanied by regulations enhancing the protection of consumers and investors

The emergence of Initial Coin Offerings (ICOs) in recent years has opened up a new, exciting way of financing economic activity.

In a typical ICO, a company or entrepreneur issues cryptocurrencies in the form of "tokens", in exchange for other cryptocurrencies such as Bitcoin or Ethers.

Entrepreneurs can then use the funds received from consumers or investors to finance their businesses.

In a recent study on ICOs from a comparative and interdisciplinary perspective, Assistant Professor Aurelio Gurrea-Martinez from the SMU School of Law argues that more protection mechanisms need to be put in place for the buyers of those tokens that do not meet the prevailing definition of "securities".

In most jurisdictions around the world, including the United States, the United Kingdom, and Singapore, when a token issued meets the definition of "securities" established in the country's securities law – known as a "security token" – the ICO is subject to the same regulatory framework that exists for the issuance of other traditional investment products, such as shares or bonds.

"While the existing regulatory framework for security tokens works reasonably well, the problem comes when the ICO involves the issuance of tokens that are not legally classified as "securities" – that is, when it is a "non-security token".

In those circumstances, the issuance of tokens is subject to neither securities law nor the supervision of the securities regulator," said Asst Prof Gurrea-Martinez.

"My co-author and I propose several measures to protect the buyers of non-security tokens, since these actors are virtually unprotected under current laws. Besides, as the buyers of these tokens are often retail consumers subject to large asymmetries of information and higher risk of opportunism, there is an even stronger case for regulation."

Asst Prof Gurrea-Martinez and his co-author, Nydia Remolina, research associate at the SMU Centre for AI and Data Governance, noted that since many ICOs involve non-security tokens, regulators do not have the opportunity to be aware of their existence nor issuance.

Indeed, in many cases, regulators become aware of these ICOs only when a financial scandal has occurred, by which time, unfortunately, the damage has already been done.

To address this situation, the SMU researchers propose that all ICOs, regardless of the legal nature of the token, should be disclosed to a centralised and public authority in order to reduce the risks of scams.

This would require the entrepreneur to submit a simple, harmonised electronic form providing some basic information about the promoter, the issuance, and the tokens. This will allow authorities to develop a registry of ICOs, making it easier to monitor the entire ICO market, and consequently discourage scammers from launching a fraudulent ICO. "Moreover, as this measure would not imply significant costs to the entrepreneur, it should not harm innovation and firms' access to new funds. Actually, quite the opposite: as it would enhance consumer and investor protection, and therefore confidence, it may facilitate firms' access to finance," explained Asst Prof Gurrea-Martinez.

Assistant Professor Aurelio Gurrea-Martinez

He also argued that, due to the risks of scams and volatility in the ICO market, commercial banks and pension funds should be prohibited from buying tokens. This is to avoid putting at risk the savings of their customers or jeopardising the stability of the financial system if the ICO fails or turns out to be a scam.

The researchers also called for the applicable law of ICOs to be harmonised across different jurisdictions to provide more certainty to entrepreneurs, consumers and investors involved in an ICO in overseas markets.

This would require regulators to come together to establish some common rules to determine the applicable law governing an ICO.

This could be the place of residence or incorporation of the promoter, or the law could be chosen by the entrepreneur and disclosed to the public agency in charge of receiving information about ICOs.

Finally, as many consumers and investors are not aware of the risks involved in an ICO, Asst Prof Gurrea-Martinez proposed that regulators should invest more resources in education and awareness efforts. If they are unable to do so due to the lack of resources or expertise, they could even consider the possibility of prohibiting the purchase of tokens to retail consumers or investors, he added.

"Our proposals seek to promote entrepreneurship, innovation and firms' access to finance by creating more certainty and confidence in the ICO market, while enhancing consumer and investor protection, market integrity, and the stability of the financial system."

Scan the QR Code to listen to the podcast on this topic

For more information on SMU research, visit *https://www.smu.edu.sg/research*