量子コンピューティング

2017 年１０月

量子コンピューティングは理論的にはかなり前から可能性があると言われていたが実用化にはほど遠いという認識が多かった。ここへきて、実用化が数年内に入っているという見方が多くなり、注目されている。

例えば MIT Technology Review 誌の「今年の注目技術ベスト１０」では過去に毎年、量子コンピューティングを入れるかどうかが検討されていたがベスト１０の枠からは外されていた。2017 年の「ベスト 10」で初めて取り上げられ、実用化まで「5，6 年」と推測されている。すなわち、数年後には、暗号化、材料科学、製薬研究、人工知能などの研究のやり方がこれにより書き換えられるとの見方もある。

http://bit.ly/2yrndS3

1 大手企業の動向

量子コンピューティングに取り組んでいる大手企業は IBM、Google、Microsoft、Intel であり、IBM と Google が先端とされている。

また、ここへ来て特に注目されている理由の一つは量子コンピュータが人工知能プログラムの実行、複雑なシミュレーションやスケジューリングの問題を処理の処理を極めて速くすること可能性である。

2014 年の時点での各社の量子コンピューティング開発状況のまとめ

Quantum Projects

COMPANY	TECHNOLOGY	WHY IT COULD FAIL
IBM	Makes qubits from superconducting metal circuits.	The error rate of the qubits is too high to operate them together in a useful computer.
Microsoft	Building a new kind of "topological qubit" that in theory should be more reliable than others.	The existence of the subatomic particle used in this qubit remains unproven. Even if it is real, there isn't yet evidence it can be controlled.
Alcatel-Lucent	Inspired by Microsoft's research, it is pursuing a topological qubit based on a different material.	Same as above.
D-Wave Systems	Sells computers based on superconducting chips with 512 qubits.	It's not clear that its chips harness quantum effects. Even if they do, their design is limited to solving a narrow set of mathematical problems.
Google	After experimenting with D-Wave's computers since 2009, it recently opened a lab to build chips like D-Wave's.	Same as above. Plus, Google is trying to adapt technology first developed for a different kind of qubit to the kind used by D-Wave.

MIT Technology Review

出典：http://bit.ly/2wI3ko0

Intel は他社と違い、量子コンピューティングの要素となる Qubits をシリコンを原料として開発する方向を取っている。

http://bit.ly/2hjfMs5

IBM ではごく最近（2017 年 9 月）、量子コンピュータ上で分子をシミュレートするための新しいアプローチを開発したと発表した。これにより、最終的には現在の最も強力なスーパーコンピュータでさえも解決できない化学・電磁気の難題を量子コンピュータが解決できる可能性もあるとしている。

https://bloom.bg/2fcq8pt

2 暗号鍵解読の危険

また、量子コンピューティング実用化による危険もある。一番直近の問題は現在使われている公開鍵による暗号化が、量子コンピューティングによる高速の演算により破られることである。こちらの記事では、量子コンピューティングは、理論上、すべての現代の暗号化を破ることができる。 ブロックチェインも例外ではない。 量子コンピューティングにより暗号化鍵を迅速かつ簡単に分解することができる、警鐘している。また、量子コンピューティングを用いて破られない暗号化作成の研究も進んでいるがどちらが先化の競争となる。

http://bit.ly/2ydr4Bu

3 ベンチャー企業

開発費用がかかり、大手テクノロジーとの競争となる量子コンピューティングでのベンチャー企業は少ないが以下の 2 社が注目される。

D-Wave Systems

https://www.dwavesys.com/

カナダの D-Wave Systems 社は、数年前より、量子アニールと呼ばれる特殊な技術を使用して、量子コンピュータと呼ばれる機械を販売してきた。「量子コンピューターを販売」しているのは同社のみで、また賛否両論がある。懐疑派は同社のアプローチでは、極めて特殊な一部の演算子か出来ないと言っている。Google では同社のコンピュータを 1 台購入、一定の条件においては「量子コンピューティング」と呼べる演算が可能であるという証明をしている。

Rigetti

https://medium.com/rigetti

2013 年設立のベンチャーで、最近までほとんど知られていなかったが、2017 年 6 月に大型（約 60 億円）のベンチャー資金調達を行い、同時にクラウド上で量子コンピューティングのプログラミングのシミュレーションが出来るシステム「Forest」を発表して注目されるようになった。MIT Technology Review 誌の、「先端の企業５０」の 2017 年版に選ばれている。

Forest： http://www.rigetti.com/forest

http://bit.ly/2xj3mEM