MORGAN CREEK
DIGITAL
ALTERNATIVE THINKING ABOUT INVESTMENTS

Welcome to Morgan Creek Digital's digital asset update. It is comprised of a thought piece from our team. We hope you find this content interesting. Please let us know if you have any comments or questions or if you would like to speak to a member of the [Morgan Creek Digital team](#).

Mind-Bending Quantum Breakthroughs and Implications

In case you missed it, here is the headline, *Quantinuum unveiled a 56-Qubit Quantum Computer, achieving performance breakthroughs*.[1]

Summary[2]: Quantinuum has introduced the H2-1 model, the first quantum computer in the industry with 56 trapped-ion qubits, setting a new standard for cross-entropy measures. Quantinuum leverages a Random Circuit Sampling (RCS) technique that outperformed Google's previous 2019 findings by a factor of 100. Further, at 30,000x power savings over traditional supercomputers, the H2-1's increased fidelity puts current supercomputers and quantum systems to the test.

Quantum computing is a field that leverages the principles of quantum mechanics to process information in a manner that fundamentally challenges classical computing. The primary goal of this newsletter is to simplify quantum mechanics and describe its potential implications in emerging technologies. Let's first review some general quantum fundamentals and mechanics.

Wave-Particle Duality: Recall your middle-school science class relating to the properties of particles. Electrons and photons have both wave-like and particle-like properties, often referred to as duality. This describes the state in which particles create an interference pattern when not observed but behave like particles when observed.[3] For example, in the popular “double slit” experiment, light waves that pass through two slits, interfere and reduce the bright and dark bands displayed on the screen.

Quantization: This describes the process of mapping continuous infinite values to a smaller set of discrete values.[4] For example, the energy levels of electrons in an atom can only occupy discrete or specific levels of energy.

Superposition: Until it is measured, a quantum system can exist in several states at once. A qubit, for instance, can be in any “superposition” of 0, 1, or any other state.[5] This allows for parallel processing capabilities.

Entanglement: No matter how far apart two particles are, once they entangle, their states are dependent on one another.[6] The condition of one particle is instantly impacted by the measurement of another, challenging traditional ideas of locality and causality.

Uncertainty Principle: This concept, which was developed by Werner Heisenberg, asserts that some pairings of physical attributes, such as momentum and location, cannot be measured simultaneously and with arbitrarily high precision. There is an inverse relationship between the paired properties, as the more precise one property is measured the less the other property can be known.

Wave-function: An object's or system's quantum state is represented by its wave-function (denominated as the Greek letter psi, ψ). Wave-function has all of the system's information (like time, position, momentum, spin, etc)and can be used to determine the likelihood of different outcomes or a probabilistic description of a system.[7]

Measurement Problem: A quantum system's wavefunction collapses to a single eigenstate, a definite state of a quantum system that occurs as an observer predicts the result of a measurement.[8] This collapse is probabilistic, meaning the result cannot be predicted with certainty but only in terms of probabilities.

Key Takeaways: The quantum bit, or qubit, is the fundamental component of quantum computing. Qubits can exist in a state of 0, 1, or any quantum superposition of these states, in contrast to classical bits, which are binary and can only exist in one of two states (0 or 1). This implies that a qubit, which derives from the concept of superposition, can exist in more than one state at once, and unlocks a quantum computer's ability to process enormous amounts of data at once. Recall that entanglement is the process in which qubits become intertwined in such a way that the state of one directly influences the state of another, regardless of how far away they are. This interconnectedness also allows quantum computers to perform incredibly complex computations at a far faster pace compared to classical computers.

Quantum gates, manipulate qubits through unitary transformations, or linear transformations that change a vector's direction while preserving its attributes (like length).[9] Quantum gates such as the Hadamard, CNOT, and Pauli-X execute operations leveraging properties of superpositions and entangled qubits, in contrast to classical *logic gates* that process bits using simple binary operations (like AND, OR, and NOT).[10] In short, these gates modify quantum states in ways that result in intricate transformations that are necessary for quantum algorithms.

Quantum and Cryptography

Algorithms like *Shor's algorithm*, which can factor large numbers exponentially faster and compute discrete logarithms in polynomial time, can potentially break some of the most well-known classical algorithms, like RSA and ECC (Elliptic Curve Cryptography), which rely on the difficulty of factoring large numbers.[11] This potential threat also presents an opportunity for the creation of quantum-resistant encryption techniques. For example, lattice-based cryptography, which depends on the difficulty of issues like the Learning With Errors (LWE) problem[12], is thought to be immune to quantum assaults at this time.[13] Similar to this, hash-based cryptography creates secure signatures using hash functions, which are also said to be quantum-resistant as it is difficult for quantum computers or any actor to reverse hash functions. The hardness of decoding random linear codes serves as the foundation for code-based cryptography, which is another intriguing option for protecting data from quantum threats.[14] In the end, we believe quantum computing should improve general security by spearheading the development and application of these novel cryptographic methods.

Quantum Key Distribution (QKD) is an example of quantum cryptographic protocols that leverage the principles of quantum mechanics to ensure the secure exchange of keys.[15] Because of the characteristics of quantum states—such as the no-cloning theorem[16] and the disruption of quantum states upon measurement—any attempt to eavesdrop on the key exchange in QKD can be identified. This security could potentially guarantee that the conversation will be private even if a bad actor is trying to listen.[17] Furthermore, Quantum Random Number Generation (QRNG) used to produce random numbers essential to cryptographic keys, leverages the intrinsic unpredictability of the quantum processes.[18] Combining classical and quantum cryptographic techniques can create hybrid systems that leverage the strengths of both worlds. Robust security can be achieved by securely exchanging keys using QKD and utilizing traditional symmetric encryption methods like AES.

Quantum and Artificial Intelligence

Deep neural network training, especially those that use machine learning, demand significant amounts of processing power to complete. Due to the inherent parallelism in quantum computing, quantum machine learning algorithms may be able to greatly speed up these processes. Quantum versions of principal component analysis, support vector machines, and other fundamental AI algorithms, for instance, might run more quickly on quantum hardware and handle massive datasets more quickly while also improving pattern recognition.[19]

Conclusion

Quantum computing has enormous potential, but there are still a lot of technological obstacles to overcome. Because of their great fragility, quantum states are prone to decoherence, which is the disintegration of superposition states and a loss of quantum coherence as a result of interactions with the environment. This fragility makes it difficult to sustain stable quantum states long enough to complete computations. Large-scale qubit quantum computer construction also poses formidable engineering obstacles. Techniques for scaling higher qubit counts while preserving coherence, could allow for quantum to realize its potential in impacting a wide array of scientific and technological fields, creating potential investment opportunities.

Click Here to listen to the latest episode of Digital Currents

Podcast feed: subscribe to *Digital Currents* in your favorite podcast app, and follow us on Apple Podcasts, or Spotify

[1] https://www.quantinuum.com/news/quantinuum-launches-industry-first-trapped-ion-56-qubit-quantum-computer-that-challenges-the-worlds-best-supercomputers

[2] https://www.datacenterdynamics.com/en/news/quantinuum-upgrades-h2-quantum-computer-from-32-to-56-qubits/

[3] https://www.thoughtco.com/wave-particle-duality-2699037

[4] https://www.sciencedirect.com/science/article/abs/pii/S0039368122001339#:~:text=In%20physics%20the%20word%20%E2%80%9Cquantization,from%20classical%20theory%2C%20in%20particular.

[5] https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-superposition#:~:text=When%20an%20electron%20is%20in,in%20two%20places%20at%20once.

[6] https://www.quantum-inspire.com/kbase/superposition-and-entanglement/

[7] https://byjus.com/physics/wave-function/#:~:text=What%20is%20Wave%20Function%3F,Greek%20letter%20called%20psi%2C%20%F0%9D%9A%BF.

[8] https://www.scientificamerican.com/article/quantum-theorys-measurement-problem-may-be-a-poison-pill-for-objective-reality/

[9] https://www.nist.gov/physics/introduction-new-quantum-revolution/quantum-logic-gates

[10] Ibid.

[11] https://www.quera.com/glossary/shors-algorithm

[12] The Learning With Errors (LWE) problem is a mathematical challenge where you try to uncover a hidden secret number from several math problems, each with a small random error added to their answers. The difficulty in solving this problem makes it a key tool in creating secure cryptographic systems, as it is hard for attackers to reverse-engineer the secret number.

[13] https://www.redhat.com/en/blog/post-quantum-cryptography-lattice-based-cryptography#:~:text=Lattice%2Dbased%20cryptographic%20systems%20are,combinations%20are%20called%20a%20lattice.

[14] https://www.cs.princeton.edu/techreports/2008/845.pdf

[15] https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/#:~:text=Quantum%20key%20distribution%20utilizes%20the,over%20a%20dedicated%20communications%20link.

[16] According to the no-cloning theorem, perfect duplicates of any unknown quantum state cannot be produced. This theory guarantees that any attempt to intercept and clone quantum carriers will include detectable flaws, which has significant implications for quantum key distribution.

[17] https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/#:~:text=Quantum%20key%20distribution%20utilizes%20the,over%20a%20dedicated%20communications%20link.

[18] https://camacholab.byu.edu/qrng

[19] https://www.linkedin.com/pulse/impact-quantum-computing-machine-learning-exploring-inbuiltdata-a8pxc/

intended that they will. This document is for informational purposes only and should not be distributed.

Risk Summary
Interests in the Morgan Creek Digital Fund IV, LP ("Fund") are speculative and involve a significant degree of risk. Cryptocurrencies and related businesses have limited performance histories, can be extremely volatile, and are not subject to many of the regulatory oversights over which other investable assets are subject. An investment in the Fund is suitable only for sophisticated investors and requires the financial ability and willingness to accept the high risks and limited liquidity inherent in the Units.

There can be no assurance that the Fund will be successful or that losses will not be incurred by the Fund. Each investor in the Fund must have the ability to bear the risk of loss of their entire investment and must be prepared to bear such risks for an extended period of time. Investors are strongly urged to consult with their professional advisors and to carefully review the risk prior to investing.

Performance Disclosures
There can be no assurance that the investment objectives of any fund managed by Morgan Creek Capital Management, LLC will be achieved. Past performance is not indicative of the performance that any fund managed by Morgan Creek will achieve in the future. Although Morgan Creek Capital Management, LLC has been presented with co-investment opportunities in the past, there can be no assurance that Morgan Creek will be presented with similar opportunities in the future. Further, there can be no assurance that co-investment opportunities will be available in the future.