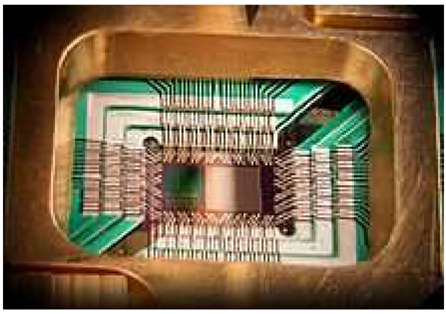
Why is Bitcoin safe against a quantum computer?

As we all know elliptic curve cryptography is vulnerable to a quantum computer. For a conventional computer difficulty of breaking 256-bit key equals 256/2=128 bits. For a quantum computer it's just sqrt(256)=16 bits. Bitcoin address is a hashed public key of 256-bit EC. Hashes are resistant to quantum algos, so while someone keeps his public key unknown it's OK. But when he wants to transfer his money he must reveal the key. Let's assume that an attacker with a quantum computer monitors all transactions. The attacker can pick any key while a transaction awaits to be included into a block. Now imagine that miners choose transactions with higher fees. The attacker can issue other transaction (when he picks the private key) that transfer coins to his address and set a higher fee. Or he could switch his mining rig on and try to find a block himself. With 0.1% of all hashpower he needs only 5 days to solve a block with 50% chance. Quantum computers are just a theoreticall concept. Sad if it's the only frontier... D-Wave Systems, Inc. is a quantum computing company, based in Burnaby, British Columbia. On May 11, 2011, D-Wave System announced *D-Wave One*, labeled "the world's first commercially available quantum computer," and also referred to it as an adiabatic quantum computer using quantum annealing to solve optimization problems operating on an 128 qubit chip-set.[1] The D-Wave One was built on early prototypes such as D-Wave's Orion Quantum Computer. The prototype was a 16-qubit adiabatic quantum computer, demonstrated on February 13, 2007 at the Computer History Museum in Mountain View, California.[2] D-Wave demonstrated what they claimed to be a 28-qubit adiabatic quantum computer on November 12, 2007.[3] The chip was fabricated at NASA's Jet Propulsion Lab's microdevices lab in Pasadena, California.[4]


[37]

Photograph of a chip constructed by D-Wave Systems Inc., designed to operate as a 128-qubit superconducting adiabatic quantum optimization processor, mounted in a sample holder. As of June 2010, it has been published that a D-Wave processor comprises a programmable[5] superconducting integrated circuit with up to 128 pair-wise coupled[6] superconducting flux qubits.[7][8][9] The processor is designed to implement a special-purpose adiabatic quantum optimization algorithm[10][11] as opposed to being operated as a universal gate-model quantum computer. D-Wave maintains a list of peer-reviewed technical publications on their website.[12] D-Wave was founded by Haig Farris (former chair of board), Geordie Rose (CTO and former CEO), Bob Wiens (former CFO), and Alexandre Zagoskin (former VP Research and Chief Scientist). Farris taught an entrepreneurship course at UBC (University of British Columbia), where Rose obtained his Ph.D. and Zagoskin was a postdoctoral fellow. The company name refers to their first qubit designs, which used d-wave superconductors. D-Wave operated as an offshoot from UBC, while maintaining ties with the Department of Physics and Astronomy. It funded academic research in quantum computing, thus building a collaborative network of research scientists. The company collaborated with several universities and institutions, including UBC, IPHT Jena, Université de Sherbrooke, University of Toronto, University of Twente, Chalmers University of Technology, University of Erlangen, and Jet Propulsion Laboratory. These researchers worked with D-Wave scientists and engineers. Some of D-Wave's peer-reviewed technical publications come from this period. Some publications have D-Wave employees as authors, while others include employees of their partners as well or only. As of 2005, these partnerships were no longer listed on D-Wave's website.[13][14] D-Wave operated from various locations in Vancouver, Canada, and laboratory spaces at UBC before moving to its current location in the neighboring suburb of Burnaby.On February 13, 2007, D-Wave demonstrated the Orion system, running three different applications at the Computer History Museum in Mountain View, California. This marked the first public demonstration of, supposedly, a quantum computer and associated service. The first application, an example of pattern matching, performed a search for a similar compound to a known drug within a database of molecules. The next application computed a seating arrangement for an event subject to compatibilities and incompatibilities between guests. The last involved solving a Sudoku puzzle. The processors at the heart of D-Wave's "Orion quantum computing system" are hardware accelerators designed to solve a particular NP-complete problem related to the two dimensional Ising model in a magnetic field.[2] D-Wave terms the device a 16-qubit superconducting adiabaticquantum computer processor.[15][16] According to the company, a conventional front end running an application that requires the solution of an NP-complete problem, such as pattern matching, passes the problem to the Orion system. However, the company does not make the claim its systems can solve NP-complete problems in polynomial time. According to Dr. Geordie Rose, Founder and Chief Technology Officer of D-Wave, NP-complete problems "are probably not exactly solvable, no matter how big, fast or advanced computers get" so the adiabatic quantum computer used by the Orion system is intended to quickly compute an approximate solution.[17]On Tuesday, December 8, 2009 at the Neural Information Processing Systems (NIPS) conference, a Google research team led by Hartmut Neven used D-Wave's processor to train a binary image classifier.On May 11, 2011, D-Wave Systems announced the D-Wave One, an integrated quantum computer system running on a 128 qubit processor. The processor used in the D-Wave One code-named "Rainier", performs a single mathematical operation named Discrete optimization. Rainier uses a process called quantum annealing to solve optimization problems. The D-Wave One is claimed to be the world's first commercially available quantum computer system.[18] May 20, 2011, D-Wave Systems is marketing a $10,000,000 Quantum Computer named "D-Wave One" with a 128-qubit (quantum bit) chipset that performs just a single task—discrete optimization.[19] On May 25, 2011, Lockheed Martin signed a multi-year contract with D-Wave Systems to realize the benefits based upon a quantum annealing processor applied to some of Lockheed's most challenging computation problems. The contract also includes maintenance, associated professional services, and the purchase of the *D-Wave One* Quantum Computer System.[20]In early 2012, D-Wave Systems revealed a 512-qubit code named Vesuvius,[21] which it expects to launch before the end of 2012.[22]In August 2012, a team of Harvard University researchers presented results of the largest protein folding problem solved to date using a quantum computer. The researchers solved instances of a lattice protein folding model, known as the Miyazawa-Jernigan model, on a D-Wave One quantum computer.[23][24]D-Wave was originally criticized by some scientists in the quantum computing field, but this criticism has softened since D-Wave published a paper in the May 12, 2011 edition of *Nature* giving details which critical academics said prove that the company's chips do have some of the quantum mechanical properties needed for quantum computing.[25][26] Prior to the 2011 *Nature* paper, D-Wave was criticized for lacking proof that its computer was in fact a quantum computer. Nevertheless, questions remain due to the lack of conclusive experimental proof of quantum entanglement inside D-Wave devices.[27] In 2007 Umesh Vazirani, a professor at UC Berkeley and one of the founders of quantum complexity theory, made the following criticism:[28] Their claimed speedup over classical algorithms appears to be based on a misunderstanding of a paper my colleagues van Dam, Mosca and I wrote on "The power of adiabatic quantum computing." That speed up unfortunately does not hold in the setting at hand, and therefore

D-Wave's "quantum computer" even if it turns out to be a true quantum computer, and even if it can be scaled to thousands of qubits, would likely not be more powerful than a cell phone. Wim van Dam, a professor at UC Santa Barbara, summarized the scientific community consensus as of 2008 in the journal *Nature*:[29] At the moment it is impossible to say if D-Wave's quantum computer is intrinsically equivalent to a classical computer or not. So until more is known about their error rates, caveat emptor is the least one can say. MIT professor Scott Aaronson, self-described "Chief D-Wave Skeptic", originally said that D-Wave's demonstrations did not prove anything about the workings of the computer. He said that a useful quantum computer would require a huge breakthrough in physics, which has not been published or shared with the physics community.[30] Dr. Aaronson has since updated his views on his blog, announcing that he was "retiring as Chief D-wave Skeptic" in 2011,[31] and reporting his "skeptical but positive" views based on a visit to D-Wave in February 2012.[27][32][33]D-Wave has employed or hired on a contract basis several key members of the scientific community as well as several notable business consultants. A partial list includes: Aspuru-Guzik[34] (Harvard), Dmitri V. Averin (Stony Brook), Seth Lloyd (MIT), Alexandre Zagoskin[35] (Loughborough University),See also AQUA@home, Adiabatic quantum computation, Analog computer, Flux qubit.

References

1. ^ Quantum annealing with manufactured spins(Nature)
2. ^ *a* *b* "Quantum Computing Demo Announcement". 2007-01-19. Retrieved 2007-02-11.
3. ^ D-Wave Systems: News
4. ^ A picture of the demo chip « rose.blog
5. ^ M. W. Johnson et al., "A scalable control system for a superconducting adiabatic quantum optimization processor," Supercond. Sci. Technol. 23, 065004 (2010); preprint available: arXiv:0907.3757
6. ^ R. Harris et al., "Compound Josephson-junction coupler for flux qubits with minimal crosstalk," Phys. Rev. B 80, 052506 (2009); preprint available: arXiv:0904.3784
7. ^ R. Harris et al., "Experimental demonstration of a robust and scalable flux qubit," Phys. Rev. B 81, 134510 (2010); preprint available: arXiv:0909.4321
8. ^ Next Big Future: Robust and Scalable Flux Qubit, [1], September 23, 2009
9. ^ Next Big Future: Dwave Systems Adiabatic Quantum Computer [2], October 23, 2009
10. ^ Edward Farhi et al., "A Quantum Adiabatic Evolution Algorithm Applied to Random Instances of an NP-Complete Problem," Science 92, 5516, p.472 (2001)
11. ^ Next Big Future: Dwave Publishes Experiments Consistents with Quantum Computing and Support Claim of At Least Quantum Annealing, [3], April 09, 2010
12. ^ Publications
13. ^ "D-Wave Systems at the Way Back Machine". 2002-11-23. Archived from the original on 2002-11-23. Retrieved 2007-02-17.

14. ^ "D-Wave Systems at the Way Back Machine". 2005-03-24. Archived from the original on 2005-03-24. Retrieved 2007-02-17.

15. ^ Kaminsky; William M. Kaminsky and Seth Lloyd (2002-11-23). "Scalable Architecture for Adiabatic Quantum Computing of NP-Hard Problems" (PDF). *Quantum Computing & Quantum Bits in Mesoscopic Systems (Kluwer Academic*. arXiv:quant-ph/0211152.

16. ^ Meglicki, Zdzislaw (2008). *Quantum Computing Without Magic: Devices*. MIT Press. pp. 390–391. ISBN 0-262-13506-X.

17. ^ "Yeah but how fast is it? Part 3. OR some thoughts about adiabatic QC". 2006-08-27. Archived from the original on 2006-11-19. Retrieved 2007-02-11.

18. ^ "Learning to program the D-Wave One". Retrieved 11 May 2011.

19. ^ "First Ever Commercial Quantum Computer Now Available for $10 Million". Retrieved 25 May 2011.

20. ^ "Lockheed Martin Signs Contract with D-Wave Systems".Retrieved 2011-05-25

21. ^ D-Wave Defies World of Critics With 'First Quantum Cloud' | Wired Enterprise | Wired.com

22. ^ The black box that could change the world - The Globe and Mail

23. ^ D-Wave quantum computer solves protein folding problem : Nature News Blog

24. ^ D-Wave uses quantum method to solve protein folding problem

25. ^ Quantum annealing with manufactured spins *Nature* 473, 194–198, 12 May 2011

26. ^ The CIA and Jeff Bezos Bet on Quantum Computing *Technology Review* October 4, 2012 by Tom Simonite

27. ^ *a* *b* My visit to D-wave: Beyond the Roast Beef Sandwich 21 February 2012

28. ^ "Shtetl-Optimized: D-Wave Easter Spectacular". 2007-04-07. Retrieved 2007-05-17.

29. ^ "Quantum computing: In the 'death zone'?". 2007-04-07. Retrieved 2008-12-23.

30. ^ "Shtetl-Optimized: The Orion Quantum Computer Anti-Hype FAQ". 2007-02-09. Retrieved 2007-05-17.

31. ^ Quantum-Effect-Demonstrating Beef May 25 2011

32. ^ "Shtetl-Optimized: Thanksgiving Special: D-Wave at MIT". 2007-11-22. Retrieved 2007-12-03.

33. ^ "In Defence of D-Wave".

34. ^ Our sponsors Aspuru-Guzik research group, Harvard University

35. ^ [4]

36. https://bitcointalk.org/index.php?topic=153302.0

37. http://en.wikipedia.org/wiki/D-Wave_Systems