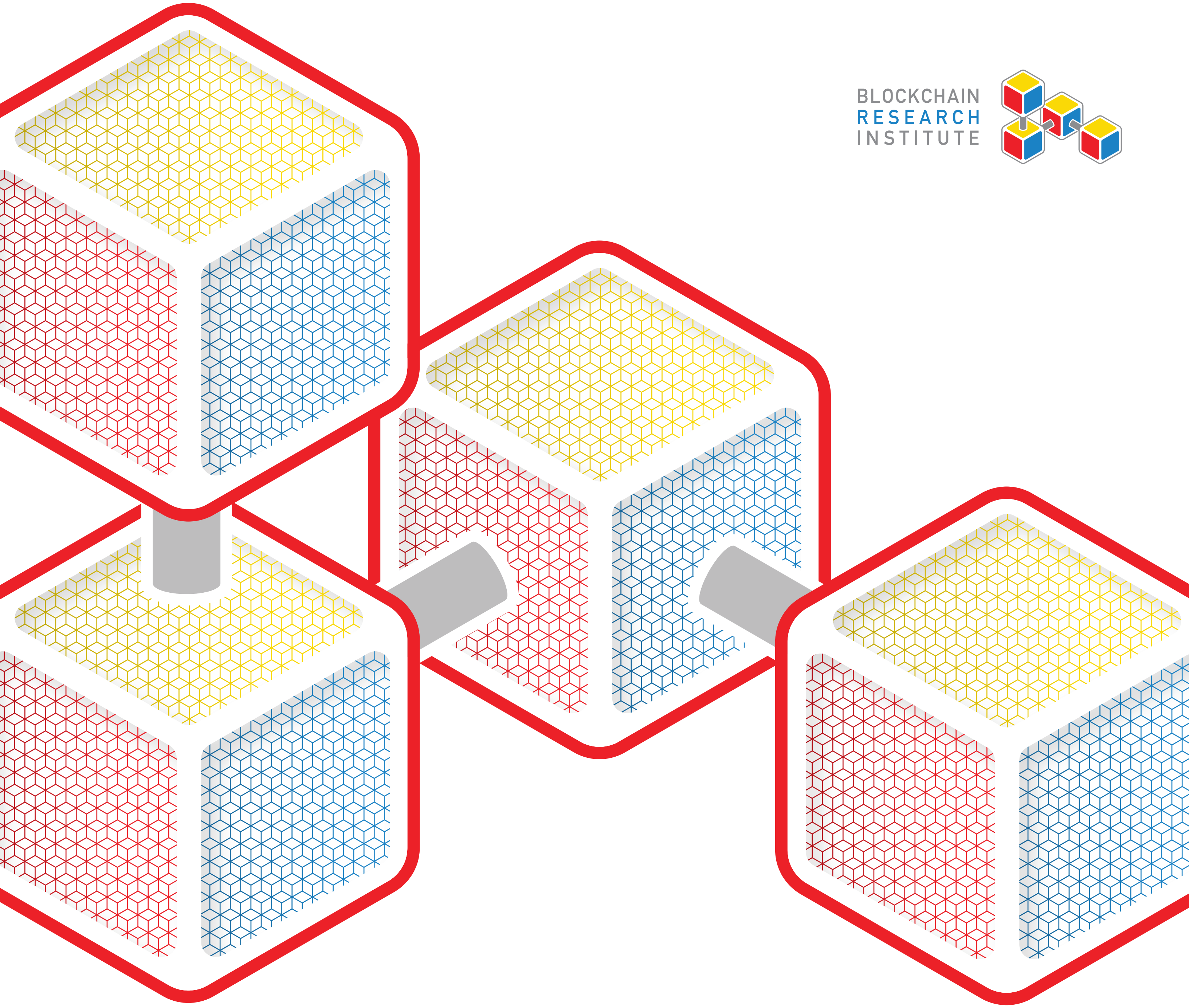


QUANTUM-PROOFING THE BLOCKCHAIN

Vlad Gheorghiu, Sergey Gorbunov, Michele Mosca, and Bill Munson

University of Waterloo

November 2017

A BLOCKCHAIN RESEARCH INSTITUTE BIG IDEA WHITEPAPER

Realizing the new promise of the digital economy

In 1994, Don Tapscott coined the phrase, “the digital economy,” with his book of that title. It discussed how the Web and the Internet of information would bring important changes in business and society. Today the Internet of value creates profound new possibilities.

In 2017, Don and Alex Tapscott launched the Blockchain Research Institute to help realize the new promise of the digital economy. We research the strategic implications of blockchain technology and produce practical insights to contribute global blockchain knowledge and help our members navigate this revolution.

Our findings, conclusions, and recommendations are initially proprietary to our members and ultimately released to the public in support of our mission. To find out more, please visit www.blockchainresearchinstitute.org.

BY NC ND **Blockchain Research Institute, 2018**

Except where otherwise noted, this work is copyrighted 2018 by the Blockchain Research Institute and licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Public License. To view a copy of this license, send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA, or visit creativecommons.org/licenses/by-nc-nd/4.0/legalcode.

This document represents the views of its author(s), not necessarily those of Blockchain Research Institute or the Tapscott Group. This material is for informational purposes only; it is neither investment advice nor managerial consulting. Use of this material does not create or constitute any kind of business relationship with the Blockchain Research Institute or the Tapscott Group, and neither the Blockchain Research Institute nor the Tapscott Group is liable for the actions of persons or organizations relying on this material.

Users of this material may copy and distribute it as is under the terms of this Creative Commons license and cite it in their work. This document may contain material (photographs, figures, and tables) used with a third party’s permission or under a different Creative Commons license; and users should cite those elements separately. Otherwise, we suggest the following citation:

> Vlad Gheorghiu, Sergey Gorbunov, Michele Mosca, and Bill Munson, “Quantum-Proofing the Blockchain,” foreword by Don Tapscott, Blockchain Research Institute, 23 Nov. 2017.

To request permission for remixing, transforming, building upon the material, or distributing any derivative of this material for any purpose, please contact the Blockchain Research Institute, www.blockchainresearchinstitute.org/contact-us, and put “Permission request” in subject line. Thank you for your interest!

Contents

Foreword

In *Blockchain Revolution*, Alex Tapscott and I wrote about the quantum threat: "Looming in the distance is quantum computing, the cryptographer's Y2K problem. It combines quantum mechanics and theoretical computation to solve problems—such as cryptographic algorithms—vastly faster than today's computers." According to Steve Omohundro, an expert in artificial intelligence, "Quantum computers, in theory, can factor very large numbers very rapidly and efficiently, and most of the public key cryptography systems are based on tasks like that. And so if they turn out to be real, then the whole cryptography infrastructure of the world is going to have to change dramatically."[1]

We have not yet reached *quantum supremacy*, the point at which a quantum machine is able to perform a computational task beyond what any classical computer is capable of performing. But Google has contended that we could reach this milestone within five years.[2]

The quantum race is on. According to *The Economist*, China is leading the pack in patent applications for quantum cryptography and quantum key distribution, and the United States is leading in quantum computing and quantum sensors.[3] Given that cryptography underpins blockchain technology and the very cybersecurity of our institutions and infrastructure, we believe this topic is too big to ignore.

A project this ambitious required a research team, and so we recruited four stars from the University of Waterloo—Vlad Gheorghiu, Sergey Gorbunov, Michele Mosca, and Bill Munson. They brought their expertise in computer science, theoretical physics, cybersecurity policy, and two areas of mathematics—*optimization*, which works with the management problems of business and government, and *combinatorics*, which combines discrete structures in modeling the physical world. More companies are hiring this kind of talent.

They explain how quantum computing is a real threat to modern cryptography: there's a one-in-seven chance that a quantum computer will be commercially available by 2026. That's less than a decade away! By 2031, the odds become one in two. Their research is a call to action. Some of their explanations are technically complicated, but we think it imprudent to oversimplify these issues: we need a level of detail for precision. Our members need to understand their options for quantum-proofing existing blockchains and designing quantum-resistant blockchain networks.

DON TAPSCOTT
Co-Founder and Executive Chairman
Blockchain Research Institute

© 2017 BLOCKCHAIN RESEARCH INSTITUTE

Idea in brief

» The arrival of powerful quantum computers will shatter currently deployed public key cryptography and weaken symmetric-key cryptography, thereby undermining the cybersecurity that protects our systems and infrastructure. The digital signature scheme used in blockchain technology to authenticate transactions is completely vulnerable.

» The problem of quantum-proofing the blockchain can be divided into two scenarios. The first scenario refers to quantum-proofing new blockchains, that is, designing quantum-resistant blockchains from scratch, whereas the second refers to quantum-proofing existing blockchains (such as the Bitcoin network).

» Perhaps the cost-effective way of making the blockchain resistant against quantum attacks is to replace the currently deployed digital signature schemes (based on RSA or EC-DSA) with post-quantum ones, which derive their security from the difficulty of certain mathematical problems; hence, they offer what is often called *computational security*.

» Quantum computation is highly susceptible to environmental noise, and so it needs quantum error correcting codes to function properly. Hence, such a realistic quantum implementation would not pose a threat unless we make significant progress in the fault tolerance quantum error correction or new quantum computing architectures come into play.

» Post-quantum digital signature schemes offer security against a quantum adversary, at the expense of much larger public/private key sizes or signature sizes, which may pose serious scalability challenges. Reducing both the signature sizes and the public/private key sizes is paramount to designing a robust and efficient quantum-resistant blockchain.

© 2017 BLOCKCHAIN RESEARCH INSTITUTE

Introduction to the quantum threat

We appear to be at the cusp of what some have called the *blockchain revolution*.[4] The blockchain is a permissionless decentralized distributed ledger of transactions (not necessarily financial) across a peer-to-peer computer network, in which the network collectively establishes trust without a central authority. This capability has profound implications, as society has always strived for distributed trust.

We must begin preparing for the quantum revolution, when computers using qubits rather than conventional bits can solve exceedingly difficult mathematical problems astronomically faster than today's computers.

Soon enough, we will be at the cusp of what we might call the *quantum revolution*. Scientists and engineers around the world are working to build the first viable computer that uses quantum bits (or 'qubits') rather than conventional bits to solve exceedingly difficult mathematical problems astronomically faster than today's computers can. The arrival of phenomenally powerful quantum computing will shatter currently deployed public key cryptography and weaken symmetric-key cryptography, thereby undermining the cybersecurity that protects our infrastructure and systems.

Unfortunately, we cannot assume that blockchains, with their strong reliance on public key cryptography, are immune from this existential threat. The security of the blockchain is based on modern cryptographic protocols.[5] For instance, the authenticity of a transaction is based on public key cryptographic digital signatures, and the validation and further immutability of the data is based on symmetric-key cryptography (hash functions). The currently deployed public key infrastructure is vulnerable against quantum attacks, being based on the hardness of computational problems such as factoring or computing a discrete logarithm, which can all be broken by a quantum computer.

Therefore, blockchain community must act to ensure that the technology can withstand quantum-powered cyberattacks. This means assessing the potential impact of quantum computing on the encryption that protects the elements of a blockchain system, and then designing and implementing the measures needed to mitigate the quantum threat by deploying cryptography designed to resist quantum attacks.

Blockchain community must act to ensure that the technology can withstand quantum-powered cyberattacks.

A story from the year 2030

It's the year 2030. Some vast global company runs its entire operation on the blockchain. Its customers (and all its robots) participate in part of the blockchain network: they negotiate by smart contract for products and services and pay in cryptocurrency on the blockchain.[6] The level of trust in the company is significantly higher than it was back in 2017, because the integrity of each transaction is now intrinsic and guaranteed on the blockchain.

© 2017 BLOCKCHAIN RESEARCH INSTITUTE

In another corner of the world, a group has assembled and is about to deploy the first fault-tolerant universal quantum computer.[7] For the first time outside the lab, a computer will be able to factor 2048-bit RSA numbers.[8] The first prototype is expected to hit the markets in fewer than six months. Unfortunately, our massive global company has never considered quantum computing as a serious risk; its CEO dismissed warnings as scientific mumbo-jumbo with no real implications for business operations any time soon—if ever.

Unfortunately, our massive global company never considered quantum computing as a serious risk; its CEO dismissed warnings as scientific mumbo-jumbo with no real implications for business operations.

Now imagine that some of the nodes (i.e., participants, be they human or thing) in the company's blockchain are on the list of customers waiting for access to quantum computers, and ready to be using them in less than a year. Some of these nodes will not let moral—or even legal—code prevent them from making a great deal of money very quickly. Maybe these ne'er-do-wells will use the quantum computer to alter, whenever possible, the transactions sent for validation and misdirect funds by replacing the intended destination address with their own.

Mounting such an attack is impossible without a quantum computer, as digital signatures—unforgeable using classical (non-quantum) computers—protect the authenticity of the data. However, the universal fault-tolerant quantum machine will enable our ne'er-do-well nodes to forge the digital signature in a matter of minutes, fewer than the 10 minutes needed on average for the network to validate a block. The attacking nodes then broadcast the altered transaction, which looks perfectly valid to other nodes; they will not know that some of the money went straight into the attackers' digital wallets instead of returning to the original sender's.

Blockchain is meant to be public and immutable and should maintain its integrity and security features for many decades. However, with a quantum computer, one can potentially rewrite history: forge a transaction that happened 10 years ago, and efficiently compute a new longest-path chain to overwrite the entire history for last 10 years. We will analyze the severity of such an attack later.

With a quantum computer, we can potentially rewrite history: forge a transaction that happened 10 years ago and compute a new longest-path chain to overwrite what transpired over the last 10 years.

Returning to our story, as time passes, more and more attacks of the sort just described take place. Public trust in the company is at an all-time low. Clients are already re-investing their assets in more secure companies that employ quantum-resistant blockchains as their underlying business model.[9] Within a year, the company goes bankrupt.

Does this scenario seem far-fetched? Sixty years ago, most people believed that the automated computing machine would never be useful outside big corporations, and a personal computer was totally unimaginable. Nowadays we each have more processing power in our smartphone than the total computing power available in the world fifty years ago.

Quantum computers are a real threat to modern cryptography. Even if one is not available today, the chance that a quantum computer will be available by 2026 is estimated to be one in seven, and the chance

© 2017 BLOCKCHAIN RESEARCH INSTITUTE

of one's being available by 2031 increases to an ominous one in two.[10] Given that cryptography underpins our cybersecurity, we think even one in seven is too large a chance to ignore.

Let's return to 2030, where an organization (say, a foreign government or large corporation) has access to the first general purpose quantum computer, and no one else in the world is aware of it. The computer is powerful enough to break RSA or ECC keys in a matter of seconds or a few minutes by running Shor's algorithm. For the current blockchain technology, such a scenario is catastrophic.

Even if a quantum computer is not available today, the chance that one will be by 2026 is estimated to be one in seven, and the chance increases to an ominous one in two by 2031.

Why? Suppose that the above organization maliciously targets a bank that uses the Bitcoin blockchain as its underlying payment system. Each client of the bank has a wallet, which consists of pairs of public keys/secret keys, where the public key is derived from the secret key, but the secret key is impossible to recover from the public key alone.[11] Similarly, the bank has a wallet that consists of many such public key/secret (or private) key pairs. Each time the bank wants to send money (in this case, bitcoin) to a client, the bank uses the hash of the public key of the respective client as the address of the wallet the money will go to, then signs a transaction of the form "I, the Bank X, sent 10 bitcoins to the client Y identified by the address Z." The bank signs the transaction with one of its secret keys, then broadcasts to the blockchain network, which will validate it within 10 minutes.[12]

However, the private key of the bank is broken within seconds or a few minutes by the malicious organization using a quantum computer. Then the latter can install a new wallet, load the compromised key in it, and then make payments pretending to be the bank. Since this new wallet is identical to the wallet of the original bank, no one will be able to see the difference in transactions and will assume transactions are valid and should be included in the blockchain. The malicious organization now can tap into and redirect all the bank's payments to its own wallet(s).

This is only one example of how the security of the current Bitcoin blockchain becomes obsolete against a quantum adversary. We mentioned before that quantum computers can not only break the current public key cryptography based on RSA or ECC using Shor's algorithm but also speed up attacks against hash functions by running the Grover's search algorithm. The speed-up of the latter is less dramatic, being only quadratically faster than any brute-force classical algorithm. Nevertheless, such an attack can still create havoc in the blockchain.

Quantum computers can not only break the current public key cryptography but also speed up attacks against hash functions by running the Grover's search algorithm.

For example, let's suppose that a whole chain of transactions was already validated and added to the blockchain. Suppose, too, that our malicious organization goes "back in time" to a certain point on the blockchain and forks the chain at that point in time, then starts modifying all the transactions in the chain sequentially and validating them on the fly so that the funds (bitcoin) are redirected to its wallet. The malicious organization will most likely be able to validate each transaction faster than some other mining pools because it is able to perform the proof of work significantly faster.

Eventually, the malicious organization is able to "catch up" with the current honest fork in the blockchain and then extend its malicious fork further. Ultimately, the network agrees that the new malicious fork is longer than the existing honest fork and collectively agrees to switch to the new fork—and a whole long chain of transactions is compromised at once.

Endangered will be many applications such as financial institutions that use private blockchains to validate transactions among themselves or Internet of Things systems that use the blockchain for micropayments.

The above examples only scratch the surface of how malicious users can use quantum computers against unaware public blockchain networks.[13] There will probably be even more clever attacks, which we will only become aware of when or after they have happened, as cybersecurity history shows us. Endangered will be many applications, ranging from financial institutions that use blockchain as a ledger to validate transactions among themselves, to Internet of Things (IoT) systems that use the blockchain for micropayments or to record state information such as users' health to the blockchain.[14]

The issue: Blockchain is not entirely quantum-safe

Today's blockchain is not quantum-safe, at least not entirely. A blockchain transaction consists of two steps: the transaction *per se*, followed by a validation of multiple transactions grouped together in a block by the blockchain network. The transaction itself can be anything. For simplicity, let's assume it is a financial transaction where Alice agrees to pay Bob 100 units. Such a transaction is time-stamped and digitally signed by Alice, who broadcasts it to the network, which collectively agrees that indeed Alice agreed to pay Bob 100 units. How can the network guarantee that it was Alice herself who sent the message to Bob, and not Bob trying to get rich quick?

Here's where public key cryptography comes into play. Alice's digital wallet consists of one or more so-called public key/private key pairs. Each private key directly corresponds to the public key; the public key and the private key are mathematically linked. However, recovering the private key from the public key alone is computationally infeasible with today's technology.[15] Alice uses her private key (known only to her) to digitally sign a transaction and then broadcasts the corresponding public key to the network. The network can verify that it was indeed Alice who used her public key to send the transaction. No one else could have signed the message.

What kind of digital signature schemes do we use in practice? The most popular are RSA-based signatures (Rivest-Shamir-Adelman), the DSA (digital signature algorithm), and EC-DSA (elliptic-curve digital signature algorithm), which is the scheme used in the Bitcoin blockchain today.[16]

© 2017 BLOCKCHAIN RESEARCH INSTITUTE

RSA-based signatures derive their security from the difficulty of factoring a product of two very large primes, each in the range of hundreds to thousands of bits long, depending on the particular scheme. If we're given such a large number, then extracting its factors seems like an exponentially difficult computational problem.

The latter two schemes are based on a completely different difficult problem: solving the discrete logarithm problem in a large Abelian group (i.e., a group where the result of applying the group operation to two group elements does not depend on the order in which they appear).[17] Simply put, if we're given an element of a group—let's call it g, of the form $g = b^k$, where b is another known element of the same group and k is an unknown integer—the problem is to find k.

With EC-DSA, the group itself consists of points on an elliptic curve, and the group operations follow some rules.[18] Both the factoring and the discrete-log problem are instances of a more general class of problems called the *hidden subgroup problem* (HSP) over a finitely generated (Abelian) group. Classical computers find the HSP problem intractable, and its intractability underpins our current public key infrastructure.

In 1994, Peter Shor realized that a universal quantum computer could factor and find discrete logarithms in polynomial time, that is, could solve those problems efficiently.[19] Hence, any public key cryptosystem based on these problems (or the HSP) is not secure against a quantum adversary. In our case, the digital signature scheme used in the blockchain to authenticate transactions is completely vulnerable: anyone with a powerful enough quantum computer can impersonate Alice and redirect some of the assets from a transaction to his/her own pocket (digital wallet) without the network's realizing that an attack took place. This is because the attacker can recover the private key from the public key with the help of the quantum computer and then alter the transaction and forge the signature using the respective private key, which will appear to the network as a perfectly legitimate transaction, because only Alice could have been able to sign the transaction correctly.

Quantum computers pose a very serious threat to the blockchain: a user's wallet would be safe only as long as the user did not spend from it. If the user only collected assets and never had to sign a transaction, an adversary would have no way of figuring out the private key.

Therefore, quantum computers pose a very serious threat to the blockchain: a user's wallet would be safe only as long as the user did not spend from it. In other words, as long as users only collect assets into their wallets and never broadcast their public keys, an adversary has no way of learning about their private keys.[20] Users broadcast their public keys only when they need to sign a transaction, that is, when they want to spend. If someone impersonates the user at that stage, then the user can irreversibly lose the money associated with that public/private key pair.

What about the second stage, the validation by the network? After transactions are grouped into a block, the block must be validated by entire network. Only when the majority of network nodes agrees on the block, is it added to the blockchain, that is, linked to the previous block via a hash of the latter. Often the validation scheme is based on a proof-of-work principle (although other schemes

© 2017 BLOCKCHAIN RESEARCH INSTITUTE

exist), which requires the nodes of the network to solve a hard computational problem or a puzzle, such as inverting a hash function on a subdomain. The node that first solves the puzzle often receives some reward (such as newly minted bitcoins according to the Bitcoin protocol), and so nodes have an incentive to participate in the validation process.

The best-known attack against hash functions is based on brute force.

Could an attacker try to double-spend some assets by broadcasting two transactions in which the attacker spent the same asset with both Bob and Charlie? Only if the attacker could take over the network and attempt to validate both transactions. However, to do so, the attacker would have to solve the proof-of-work problem faster than the rest of the combined network. Otherwise, the rest of the network will come up with a solution before the attacker, and the blockchain validates the transactions that belong to the longest chain, which in this case will belong the honest users.

Fortunately, quantum computers pose a less serious threat to hash functions and symmetric-key cryptography in general.[21] The best-known attack against hash functions is based on brute force, that is, the attacker searches for preimages of the hash until the required validation condition is achieved. Because such a search is completely unstructured, all a quantum computer can offer over a classical computer is a quadratic speed-up.[22]

Therefore, quantum computers indeed threaten hash functions, but we could easily make the proof-of-work puzzle harder so that even a quantum computer could not solve it fast enough. However, users with more computational power (which may include quantum computers) in the network have higher chances of winning the puzzle and, hence, always concentrate power. Therefore, an asymmetric distribution of fast computational machines (i.e., fast machines such as quantum computers available only to a restricted number of users) pose a significant threat to the network. We should take this into account when designing quantum-resistant blockchains.

Analysis of our options

An abstract model of the blockchain

The blockchain is a distributed ledger of trust in which consensus is obtained collectively by the network without any need for a centralized authority. The blockchain consists of blocks of transactions, each linked to its parent via some linking mechanism such as a hash of the previous block header. Only when the network validates a block, is it appended to the blockchain (Figure 1).

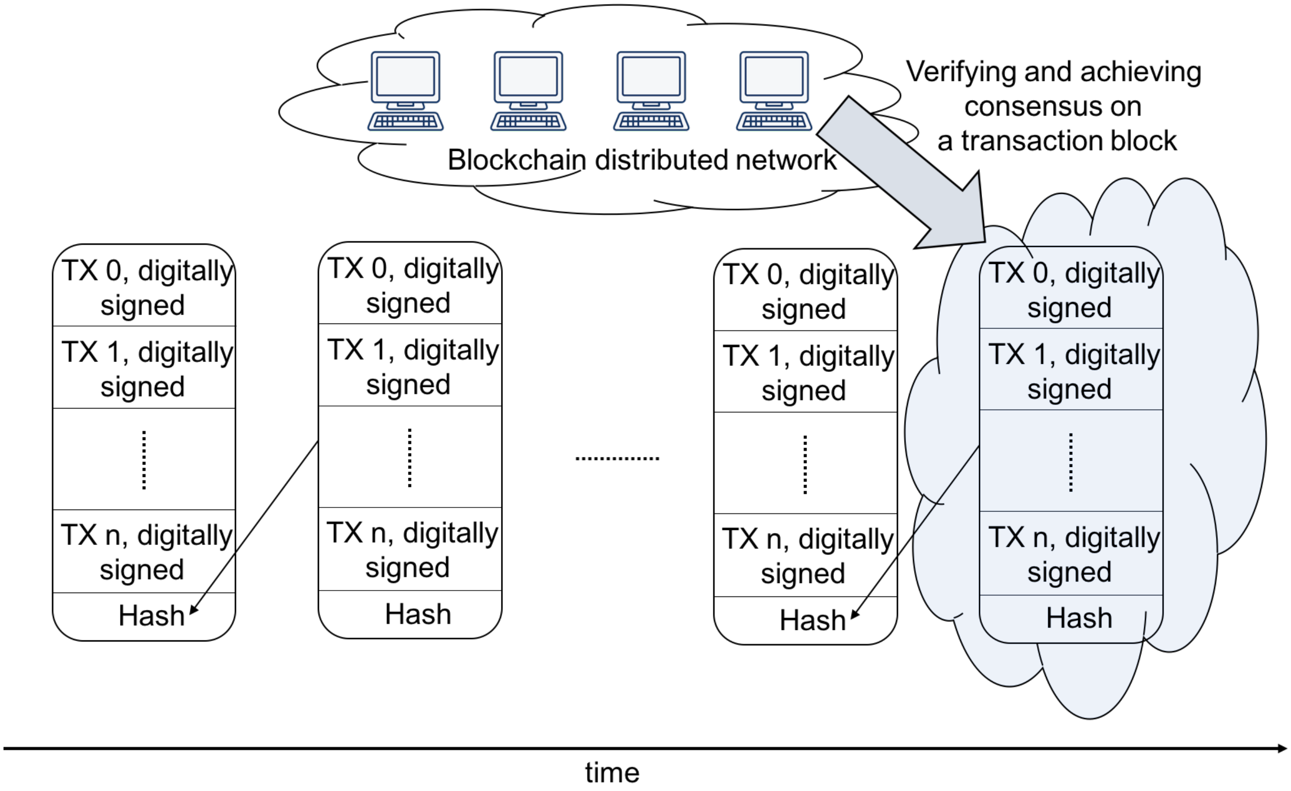
The best-known consensus mechanisms are:

1. Proof of work (PoW), in which only the network node that first solves a computationally hard problem can validate the transaction
2. Proof of stake (PoS), in which the nodes with more at stake (e.g., holding more cryptocurrency) are more likely to be chosen as validators
3. Proof of storage or proof of time, in which the nodes that have more computational resources available to the network, such as disk space or central processing unit time, are more likely to be chosen as validators

All of the consensus mechanisms above prevent the problem of double spending. Whereas PoW is considered cryptographically secure, it has a major disadvantage, namely, that it requires significant thermodynamic work and time.[23] The other consensus mechanisms, such as fault-tolerant Byzantine agreement (e.g., Algorand, Tendermint, and Hyperledger), avoid the PoW problem.[24] However, we are not yet entirely clear how cryptographically secure those protocols are, and we know even less about whether we can make them quantum-resistant.

Figure 1: Blockchain schematic model

Each block is "linked" to the previous block via the hash of the latter, i.e., each block contains a hash of the previous block (depicted here by the arrow pointing back to the previous block).


Blockchain distributed network
Verifying and achieving consensus on a transaction block
TX 0, digitally signed
TX 1, digitally signed
TX n, digitally signed
Hash
time

© 2017 BLOCKCHAIN RESEARCH INSTITUTE

From a higher level, we can see the blockchain as consisting of layers:

1. The cryptographic building blocks (e.g., hash functions, public key exchange, symmetric cryptography)

2. Algorithmic primitives (e.g., Merkle trees, cryptographic puzzles, global clocks)

3. Consensus protocols (e.g., PoW, fault-tolerant Byzantine agreement)

4. Additional non-default security properties (e.g., Zcash blockchains use a variant of zero-knowledge proofs called zk-SNARKs—zero knowledge Succinct Non-interactive ARguments of Knowledge—to provide transaction anonymity. Zk-SNARKs are not quantum-safe, and so 30 years of blockchain data could suddenly become de-anonymized once a quantum computer appears)

Zk-SNARKs are not quantum-safe, and so 30 years of blockchain data could suddenly become de-anonymized once a quantum computer appeared.

Here we focus on the cryptographic building blocks only, and mostly on the PoW-based blockchains. At this stage, we cannot assume that the more advanced algorithms or protocols within the blockchain are quantum-safe.

Ways of patching the blockchain

Given the importance of the information and relationships protected by blockchains, and the consequent certainty that blockchains will frequently be targeted for cyberattack by malicious actors, we would be prudent to introduce quantum-resistance by design and ensure the most reliable forms are utilized for the most critical and vulnerable assets.

The most important security objectives of the blockchain are unforgeability and the impossibility of double spending. Currently, the problem of quantum-proofing the blockchain can be divided into two scenarios. The first scenario refers to quantum-proofing new blockchains, that is, designing quantum-resistant blockchains from scratch, whereas the second refers to quantum-proofing existing blockchains (such as the Bitcoin network). The first scenario is considerably simpler than the second.

The most important security objectives of the blockchain are unforgeability and the impossibility of double spending.

In the analysis below, we will consider that quantum computers are either available to everyone (we will call this *symmetric adversaries*), or available only to a very few (which we will call *asymmetric quantum adversaries*). Table 1 depicts the possible combinations of types of blockchains and flavors of quantum adversaries.

© 2017 BLOCKCHAIN RESEARCH INSTITUTE

Table 1: Possible combinations of quantum adversaries

Symmetric quantum adversaries/ existing blockchains	Symmetric quantum adversaries/ new blockchains
Asymetric quantum adversaries/ existing blockchains	Asymmetric quantum adversaries/ new blockchains

Designing quantum-resistant blockchains from scratch

Designing quantum-resistant blockchains from scratch is relatively straightforward: we can apply post-quantum cryptographic schemes and quantum cryptography.

Using post-quantum cryptographic schemes

The most obvious, and perhaps cost-effective, way of making the blockchain resistant against quantum attacks is to replace the currently deployed digital signature schemes, which are based on RSA or EC-DSA, with post-quantum ones. Post-quantum cryptographic schemes derive their security from the difficulty of certain mathematical problems; hence, they offer what is often called *computational security*.

Examples of post-quantum schemes are lattice-based schemes (learning with errors, LWE), super singular isogenies schemes, multivariate-polynomial schemes, code-based schemes, or Merkle tree-based signatures.[25] All of these protocols are designed to be resistant against quantum attacks, and until now no one has been able to find an attack that destroys any of these schemes. However, such robust schemes come with a performance cost because of their slightly (or sometimes considerably) larger key sizes and significant decrease in computational speed, necessitating a trade-off of efficiency for security.

Around the world, cryptographic researchers are studying quantum-resistant algorithms; but, in the absence of international standards, their work may yield competing, under-tested proprietary cryptosystems.

Unfortunately, industry and government have been slow to act on widespread awareness of the quantum threat until recently. At the present time, cryptographic researchers around the world are increasing their focus on studying quantum-resistant algorithms; but, in the absence of international standards, the result may be a confusing plethora of competing, under-tested proprietary cryptosystems.

Fortunately, in 2016, the US National Institute for Standards and Technology (NIST) began a multi-year standardization project to identify candidate quantum-resistant cryptosystems.[26] This calls for submissions due November 2017, followed by a three- to five-year public review, followed by a one- to two-year standardization phase—leading to NIST standards between 2021 and 2024. These standardized algorithms will provide a more focused and manageable suite of alternatives for organizations to consider incorporating into their systems. However, it will likely be too soon to pick an ultimate winner (or winners), and so cryptographic agility remains critical.

Quantum key distribution is a method for using an untrusted quantum channel to establish symmetric keys through an untrusted, but authenticated, communication channel.

Blockchains using quantum cryptography

In principle, we may use a number of quantum cryptographic tools to make blockchains more secure. Quantum random number generators (QRNGs) are likely the most practical tools in the short term.[27] They avoid the cryptanalytic risks associated with pseudo-random number generators, and promise a more fundamental and more reliable source of randomness than conventional entropy-based random number generators.[28]

Also, quantum key distribution (QKD) systems are increasingly commercially available (though still in their early days).[29] QKD is a method for using an untrusted quantum channel to establish symmetric keys through an untrusted, but authenticated, communication channel. This is what is often achieved today using public key based key agreement authenticated by public key signatures, and can be achieved in the future using post-quantum public key schemes.

The advantage of establishing keys using QKD compared to post-quantum schemes for key establishment is that QKD's security does not rely on computational assumptions (i.e., it is "information theoretically" secure), and thus is resilient to cryptanalysis. Post-quantum schemes, in contrast, are based on computational assumptions, and thus come with some risk of future cryptanalysis. However, QKD requires specialized hardware (such as lasers, fiber optics, etc.) to run, and we are many years away from a global QKD network.

In practice, we don't know for sure how helpful QKD will be in improving the security of blockchains in the future. In a recent proposal for a QKD-based blockchain, the authors described a blockchain scheme in which the authentication is achieved via a QKD network among the participants, and the consensus is obtained via a Byzantine agreement-like protocol.[30] The practical usefulness of such a scheme is not yet clear.

Various quantum tools, such as quantum authentication, quantum money, and quantum fingerprints, may someday help to reduce the threat of cryptanalysis.

There are also various quantum tools, such as quantum authentication, quantum money, and quantum fingerprints, that may someday help further to reduce the threat of cryptanalysis.[31] We might also consider a fully quantum blockchain, that is, based on a distributed architecture in which the nodes are quantum computers, all linked via quantum communication channels (see Jogenfors).[32] For our purposes here, we note simply that these schemes generally require quantum computation and communication tools that will not be available, especially not for practical use, for many years to come.

Flavors of quantum adversaries

Asymmetric quantum adversaries

As with the development of classical computers, we expect quantum computers to be available initially to very few entities such as governments, large research institutions, and large corporations—in other words, we expect an asymmetric distribution of quantum adversaries.

Let's consider the impact that such a quantum computer will have on a PoW-based blockchain in which hash functions are used to enforce the immutability of transactions. We assume that the system uses quantum-resistant digital signatures to ensure the authenticity of transactions. The question is, how much damage can an isolated quantum computer (or a small number of quantum computers) do to such a network?

First, we note that the only vulnerability may be in the PoW component of the blockchain and not in the digital signature itself (if a quantum-safe signature scheme is used). Therefore, a quantum adversary cannot impersonate someone else and try to spend her/his money. The only viable attack is against the PoW system based on hash functions, where the quantum adversary may try to validate transactions faster than the rest of the combined blockchain network. If it succeeds on average, then it can double-spend without the network's awareness.

To make this example more concrete, let's look at the current Bitcoin network. The combined difficulty of the proof of work is continuously adjusted (on average increased) over time so that, on average, a solution (hence, a validation) is found every 10 minutes. This adjustment is needed because new and improved hardware is injected into the network as time passes. Figure 2 shows the increasing combined hash rate of the entire Bitcoin network between September 2016 and August 2017. In August 2017, the network performed approximately 7×10^{18} hashes per second, which means approximately 4.2×10^{21} hashes on average every 10 minutes.[33]

Therefore, to succeed, a quantum adversary must search a space of 4.2×10^{21} hash preimages in a time that is significantly smaller than 10 minutes.[34] The best such attack is via Grover's algorithm, which can potentially offer a quadratic speed-up in terms of time. An ideal quantum computer (i.e., with no need for error correction) will therefore be able to perform such a search in $\sqrt{4.2 \times 10^{21}} \approx 6.5 \times 10^{10}$ time steps. Assuming, very optimistically, a 1GHz quantum machine (i.e., a quantum computer that performs 10^9 operations per second), this search will be performed in about a minute.

Thus, the PoW system is highly vulnerable to such idealized quantum machines, as the latter can not only validate much faster than the rest of the network, but also rewrite history by creating a fork in

© 2017 BLOCKCHAIN RESEARCH INSTITUTE

time, adding new bogus transactions to the chain, and validating each block fast enough that the new chain eventually becomes the valid one that all network participants accept.

The proof-of-work system is highly vulnerable to such quantum adversaries because they can not only validate much faster than the rest of the network, but also rewrite history.

However, in reality, quantum computation is highly susceptible to environmental noise and it needs quantum error correcting codes to function properly. Quantum error correction introduces significant computational overhead because of the need for redundant encoding of information.[35] Optimistically, we assumed a quantum computer operating at a 1Gz frequency and physical components with error rates smaller than 10^{-5} (which is again a very optimistic approach). With those numbers, we computed that approximately 2.2×10^{14} steps would be required to perform the attack, all of which would take approximately two and a half days.

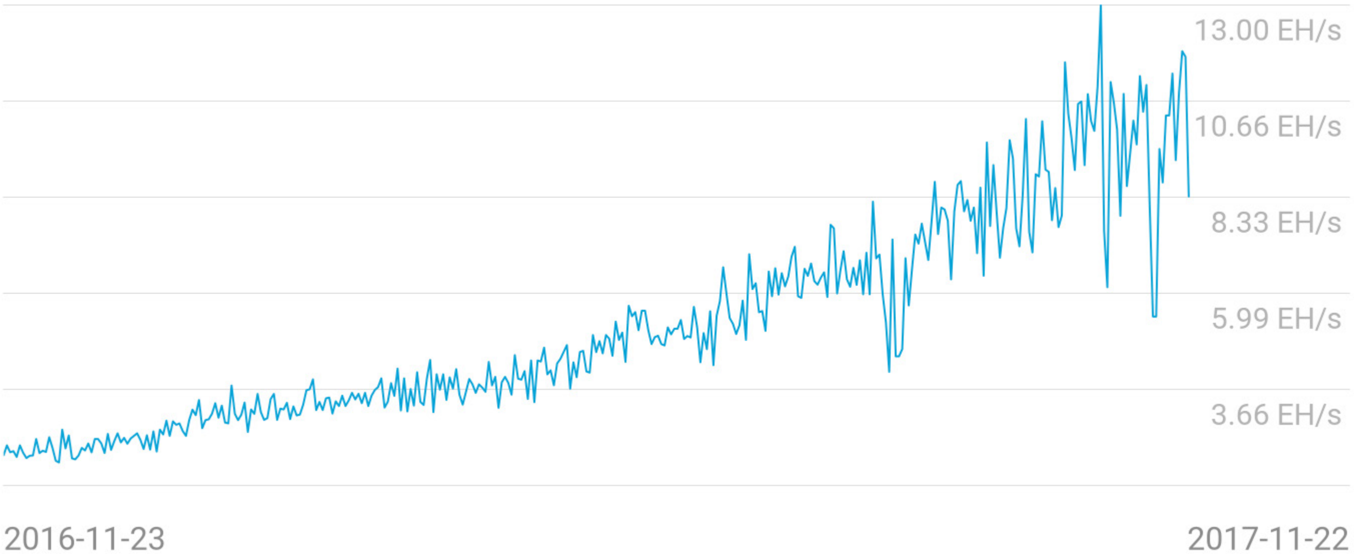
Hence, such a realistic quantum implementation would not pose a threat unless we make significant progress in the fault tolerance quantum error correction or new quantum computing architectures come into play. We do not know yet what the future holds, including the potential of new cryptanalytic attacks.

Note that searching via Grover's algorithm cannot be parallelized efficiently.[36] In other words, the best we can do is to split the searching space in chunks and use a separate quantum computer for every chunk. Hence, if K quantum computers are used in parallel to search a space of size N, the running time will be proportional to

$$\sqrt{\frac{N}{K}} \text{ and not } \frac{\sqrt{N}}{K}$$

as one may have expected. In the fault tolerant example above, an adversary will need approximately 33,000 ($\approx 2^{15}$) fully fault tolerant quantum computers to reduce the searching time to 10 minutes.

Figure 2: Bitcoin's network hash rate over 12 months



Source: blockchain.info/charts/hash-rate.

© 2017 BLOCKCHAIN RESEARCH INSTITUTE

Symmetric quantum adversaries

In this case, the whole protocol can assume the existence of widespread quantum computation, including the availability of such quantum machines to the majority of computing nodes (or mining farms). Hence, on average, there will be no outside computing power that can be significantly faster than the rest of the network. Therefore, we conclude here that the blockchain is secure against generic quantum attacks on the hash function.

Patching existing blockchains against quantum attacks may be significantly harder than designing quantum-safe blockchains from scratch.

Quantum-proofing existing blockchains

Patching existing blockchains against quantum attacks may be significantly harder than designing quantum-safe blockchains from scratch. The first step is to replace the vulnerable cryptographic primitives with quantum-resistant ones. For example, in the Bitcoin network, we would need to replace the digital signature scheme with a quantum-resistant scheme and use the latter to sign new transactions. This approach would provide security for future transactions.

The problem, however, is what would happen with old transactions? Let's assume that a wallet spent some cryptocurrency from an address. Because the address is a hash of the public key associated with that wallet, the public key has been publicly revealed and a quantum adversary can recover the corresponding secret key. If the wallet still has some cryptocurrency associated with that address, a quantum adversary can impersonate the wallet's owner and spend the rest of the funds.

A solution to this problem: never reuse a public key or make sure that there are absolutely no more funds available to an address for which the public key has been revealed. If quantum-safe digital signatures are introduced into the blockchain before quantum computers become a reality, then the network can ask every user to perform a *self-transfer* transaction in which the user transfers all funds associated with his or her old (non-quantum-safe) public keys to an address that corresponds to the user's quantum-safe public key.

A solution to this problem: never reuse a public key or make sure that there are absolutely no more funds available to an address for which the public key has been revealed.

The discussion of symmetric versus asymmetric quantum adversaries follows the same line as our flavors of quantum adversaries. In the worst-case scenario, an asymmetric quantum adversary is able to solve the cryptographic puzzle significantly faster than the rest of the network. Although this scenario is highly unlikely based on current assumptions, we cannot rule it out as impossible. Therefore, we need to take precautions.

For example, we could consider transactions longer than a fixed number L of blocks to be completely immutable, and modify the blockchain protocol such that blocks longer than L are not allowed to be forked and mined anymore. Although this option somewhat fixes the problem of rewriting history older than L blocks, it does not address the quantum adversary's ability to validate pending transactions much faster than the entire network and, therefore, to take control over the network. There is no obvious solution to this last problem, and we need significantly more research. We could design variable-difficulty cryptographic puzzles that a quantum computer could not solve faster. Of course, no one should be able to solve such puzzles by searching, because Grover's algorithm would provide a speed-up.

In the worst-case scenario, an asymmetric quantum adversary is able to solve the cryptographic puzzle significantly faster than the rest of the network.

Performance analysis

According to one acknowledged expert, one of the main technical difficulties in implementing a post-quantum blockchain resides in the overhead introduced by the post-quantum digital-signature schemes to be used.[37] For example, the Bitcoin protocol uses EC-DSA for transaction authentication, the average size of which is equal to 71 bytes. In contrast, post-quantum digital signature schemes are at least six times larger (Table 2) or much worse and significantly slower computationally than the current ones deployed such as EC-DSA. The constraints introduced by post-quantum digital signature schemes may pose serious scalability challenges for quantum-resistant blockchains.

For example, supersingular isogenies post-quantum schemes, which are very promising for public key encryption in terms of the shortness of their key sizes (about half a kilobyte), are currently inadequate as digital signatures schemes in space-constrained environments such as blockchains, because the corresponding signature size is around 140 kilobytes (in contrast to 71 bytes for EC-DSA).[38]

Table 2: Post-quantum key sizes and signature sizes at 128-bit security level

All sizes are in bytes.

Post-quantum scheme	Public-key size	Private-key size	Signature size
Hash-based	1,056	1,088	41,000
Code-based	192,192	1,400,288	370
Lattice-based	7,168	2,048	5,120
Ring-LWE-based	7,168	4,608	3,488
Multivariate-based	99,100	74,000	424
Isogeny-based	768	48	141,312
Isogeny-based (compressed)	336	48	122,880

See Y. Yoo, R. Azarderakhsh, A. Jalali, D. Jao and V. Soukharev, "A Post-Quantum Digital Signature Scheme Based on Supersingular Isogenies," Cryptology ePrint Archive, 2017, p. 186.

On the other hand, code-based and multivariate-based digital signatures have short sizes, but their corresponding public/private keys used for signature generation and verification are relatively large. Hence, for those two schemes, the size of a hypothetical block in a PoW blockchain will probably be around seven times larger than the current size of the Bitcoin blockchain. However, the required PKI will require significant more storage, as the corresponding public/private keys are significantly larger than the current EC-DSA keys. Moreover, multivariate-based schemes have a relatively large number of opponents because their security is less convincing than other schemes.

The next candidate on the list is the LWE-based digital signature scheme, which suffers from a slightly larger key (3-5 kilobytes). The schemes are provably secure asymptotically via hard-problem reduction arguments.[39] There are no such tight security proofs for real-world parameters, but the cryptographic community has not yet found any flaws or security issues with the scheme. The public/private key sizes are also reasonable in size; hence, LWE seems to be a viable candidate for quantum-resistant blockchains.

The hash-based schemes are the most trusted ones in terms of security and have relatively small public/private keys. However, the corresponding signature size is over 40 kilobytes long, which is problematic in a very space-constrained environment such as the blockchain.

Lamport one-time based signatures are another potential candidate.[40] Their public key size is 16 kilobytes, the corresponding secret key size is 16 kilobytes as well, and their signature size is eight kilobytes. Slightly more efficient schemes (in terms of signature size) such as the Winternitz one-time signature scheme are also viable.[41] Winternitz signature compression reduces the size of the private key and public key by slightly less than a factor of the two times the chunk size (in bits⟩ and half that factor for the signature. The computation time increases by slightly more than a factor of two times the chunk size (in bits). Those schemes are *one time*, that is, they are secure as long as keys are not reused when signing new transactions.

In conclusion, post-quantum digital signature schemes offer security against a quantum adversary, at the cost of much larger public/private key sizes or signature sizes. We need significantly more research in the area of post-quantum digital signatures.[42] Reducing *both* the signature sizes *and* the public/private key sizes is paramount in a robust and efficient quantum-resistant blockchain.

We need significantly more research in the area of post-quantum digital signatures.

© 2017 BLOCKCHAIN RESEARCH INSTITUTE

Q&A: What four experts say about blockchain security

During our research, we interviewed a number of blockchain experts on the security of current and future blockchain protocols against quantum adversaries. We asked them about the challenges and defects that organizations may need to address when implementing quantum-resistant ledgers.

Dr. Manfred Lochter, Federal Office for Information (BSI), Germany

Question. *How do you see breaking EC-DSA within 10 minutes?*

Answer. Do not use EC-DSA if quantum computers exist! If not, look at what kind of attack it is and how it scales, perhaps increase the security parameter.[43]

Q. *Do you believe that quantum computers will affect the security proof-of-work systems based on hash inversion?*

A. Hashes are the least of the problem in a proof-of-work system, but it depends on the type of blockchain. For example, there may be serious issues with time-stamping blockchains, in which collision resistance is of paramount importance. If a quantum computer finds a collision, it can attack the system.

Q. *How often do current wallets reuse keys?*

A. Wallets are indeed an issue. There are wallets out there that use deterministic algorithms for generating key sequences. Moreover, the number of public key collisions out there is larger than expected, mainly because of poor wallet implementations.[44]

"Do not use EC-DSA if quantum computers exist!"

DR. MANFRED LOCHTER
Federal Office for Information
Germany

Dr. Ghassan Karame, Chief Security Researcher, NEC Labs, Germany

Question. *How do you see quantum threat affecting the blockchain? How serious is this threat perceived?*

Answer. The threat is not only particular to the blockchain—it applies to all systems. I do not see blockchain as an exception. … What we know is that there are lots of inactive addresses currently in the blockchain, in the sense that if in 10 years someone can break those keys, then he/she can get lots of money. There is currently also a considerable number of coins that are dormant [Satoshi's coins].[45]

"The [quantum] threat is not only particular to the blockchain—it applies to all systems."

DR. GHASSAN KARAME
Chief Security Researcher
NEC Labs

Q. *What is the most vulnerable part of the blockchain implementations as of today?*

A. Many attacks are on the network layer implementation. It is very weak in most blockchains [because of the attempt] to optimize for

© 2017 BLOCKCHAIN RESEARCH INSTITUTE

"Many attacks are on the network layer implementation. It is very weak in most blockchains."

DR. GHASSAN KARAME
Chief Security Researcher
NEC Labs

scalability and losing security features in the process. … This is one of the weakest links of the existing implementations. … When there are users involved, the user becomes the bottleneck in security, for example, the private keys are not always properly managed.

Q. *How often do wallets reuse keys or use a deterministic algorithm to generate a key sequence? Can you comment on current wallet security issues?*

A. Bitcoin should give you a new address by default when collecting change (unless one manually alters the code). The issue is that this is not good enough. There are implementation issues as well.

Q. *Do you think a quantum-safe blockchain is useful as of today?*

A. Yes, it may make sense. Hashes are quantum-resistant, but currently the standard dilemma in the community is how to come up with a proper key-management solution for the digital signature part of the blockchain. This is a problem even for the current EC-DSA key management infrastructure. … I think we should have quantum-safe blockchains in mind.

Dr. Nadia Diakun-Thibault, North Carolina State University

Question. *What is your opinion about quantum computing attacks on the blockchain infrastructure?*

Answer. Currently, blockchain notwithstanding, we may have some quantum capabilities today, is safe at SHA-256, which is what Bitcoin blockchain uses. … The problem is humans are involved, and they may not secure the system well, may not follow all security rules, or may inject human error. … More research is needed in areas in which the blockchain is indeed vulnerable, such as digital signatures, smart contracts, or security rules and security applications in cloud computing.[46]

Q. *How common is it for wallets to have implementation security problems/major software flaws? Major catastrophes?*

"The problem is humans are involved, and they may not secure the system well, may not follow all security rules, or may inject human error."

DR. NADIA DIAKUN-THIBAULT
North Carolina State University

A. That is where the problem really is. Wallets, exchanges, accounts may be in the cloud; they are not necessarily secure. Cloud providers don't know all that goes on in the cloud. Mining can be done in the cloud. What assurance can the cloud provider give that security measures are fully applied? Most security problems are at the provider's/user's/wallet's end.

Q. *Is there any Canadian government official position or advice regarding quantum threats to the blockchain or regulating the blockchain?*

A. At this time, none that I know of. In my view, it's an area many will be very reluctant to comment on. Government can regulate use, but not with respect to blockchain itself—there are no standards. I

© 2017 BLOCKCHAIN RESEARCH INSTITUTE

"Most security problems are at the provider's, user's, or wallet's end."

DR. NADIA DIAKUN-THIBAULT
North Carolina State University

do not think we can "regulate" blockchain; one could say it would be akin to regulating a "database." Government can stipulate where it would be appropriate to use blockchain, whether it would be permissioned or permissionless, who the participants are, security requirements, compliance measures, et cetera. These are reasonable expectations.

Dr. David Jao, Centre for Applied Cryptographic Research, University of Waterloo

Question. *What is the most challenging part in building a quantum-resistant ledger?*

Answer. Definitely the digital signatures. Post-quantum signature schemes are still way larger than EC-DSA, and simply plugging a post-quantum replacement may work fine for relatively small blockchains, but will create major scalability issues for large blockchains such as the Bitcoin. The cryptographic community needs more research in the area of post-quantum digital signatures.[47]

Conclusions and recommendations

Post-quantum solutions are not yet fully standardized, so making a strong recommendation at this time is exceedingly difficult. However, what we can definitely recommend now is to build agile blockchain protocols, in which the digital signature scheme is modular so that it can easily be switched out and replaced by a quantum-resistant one. While stateful hash-based signatures are attractive from a security perspective, there are also practical advantages for stateless schemes (which also include stateless hash-based signatures), for example, digital signatures based on the hardness of lattice problems, such as LWE, or code-based digital signature schemes. [48] Remember, there is currently no quantum-resistant digital signature scheme that offers *both* short signatures *and* short key sizes.

Regulating the blockchain would be like regulating a database.

Our recommendation is to be agile and design a quantum-resistant blockchain in which changing the digital signature scheme should be a fully integrated part of the code base. For example, assume a common application programming interface (API) for digital signatures, and design the protocol with the ability to change the signature on the fly, whenever needed.

We also highly recommend a careful design of the end-user blockchain architecture, such as the digital wallet infrastructure. Remember, the end-user infrastructure is the most vulnerable link in the cryptographic chain. Making it secure is therefore of paramount importance.

A far more difficult problem is how to patch a blockchain system based on proof of work. If quantum computers are widely available, then we can modify the network protocol so that it assumes everyone is using quantum searching to find the preimages of hash functions. However, if only a small minority of users has access to quantum computers, then how to avoid an attack is unclear, when all transactions in a chain are modified sequentially. Likely, there will always be an asymmetry in the blockchain network, and those very few users with access to quantum computers will eventually be able to compromise long chains.

There is currently no quantum-resistant digital signature scheme that offers both short signatures and short key sizes.

One brute-force solution is simply to modify the blockchain protocol such that forks longer than a specified length should not be accepted for mining anymore. This solution only partially addresses the issue: while it guarantees the integrity of past transactions beyond a specified number of steps, it does not prevent malicious users from validating transactions faster than everyone else and basically taking over the network.

We hope these issues raise awareness in the blockchain research community so that it can develop novel protection schemes. Currently, we do not see hash inversion as a very serious security issue, at least not in the near term and medium term. The first generations of quantum computers will most likely suffer from significant overhead because of error-correction. Remember, in this case, Grover will not really speed things up enough so that hash inversion becomes a security issue. However, 25 years from now, we may have powerful enough asymmetric quantum adversaries who will be able to find hash preimages much faster than a large majority of the network. Currently we lack a full solution to this problem, except the aforementioned brute-force patch.

To conclude, the most stringent requirement in designing a quantum-resistant blockchain is the authentication part. Current digital signature schemes are vulnerable and must be either replaced in current blockchains or implemented from the very beginning in new quantum-resistant ledgers designed from scratch.

In designing a quantum-resistant blockchain, the most stringent requirement is the authentication part. We must either replace current digital signature schemes or else design and implement new quantum-resistant ledgers from scratch.

None of the existing post-quantum digital signature schemes satisfies all the requirements of a distributed ledger system, namely small size and efficiency. We hope that future research in the area will bring smaller and more efficient schemes. Until then, we recommend maintaining agility in the architectural design and building ledgers in which changing the digital signature scheme should be relatively easy (i.e., built into the protocol or via straightforward update patches).[49]

The Open Quantum Safe platform is a collaborative open source effort that developers can leverage for testing and benchmarking various quantum-resistant key exchange and signature schemes in blockchain applications.[50] We hope our research will motivate fruitful collaborations among blockchain experts, cryptographers, and software developers in designing the quantum-resistant ledger of the future.

About the authors

Vlad Gheorghiu is a researcher at evolutionQ Inc. and a postdoctoral fellow at the Institute for Quantum Computing at the University of Waterloo, where he is also affiliated with the Department of Combinatorics and Optimization. His interests lie in quantum computing and quantum-safe cryptography.

Sergey Gorbunov is an assistant professor in the Department of Computer Science at the University of Waterloo. He works in cryptography and is building secure protocols and systems.

Michele Mosca is the CEO of evolutionQ Inc. and a founder and professor at the Institute for Quantum Computing at the University of Waterloo, where he is affiliated with Department of Combinatorics and Optimization. He is a member of the Perimeter Institute for Theoretical Physics as well as the Canadian Institute for Advanced Research. His area of research ranges from quantum algorithms to quantum-safe cryptography.

Bill Munson is director of research and policy analysis of Quantum-Safe Canada at the University of Waterloo, with a focus on cybersecurity. He is also a research associate at Institute for Quantum Computing.

Acknowledgments

The authors thank all the interviewees for dedicating valuable time and expertise to speaking with us. We also thank John Schanck for very useful discussions regarding blockchain and quantum-resistant cryptography.

Disclosures

Michele Mosca is a project leader of Open Quantum Safe.

About the Blockchain Research Institute

Co-founded in 2017 by Don and Alex Tapscott, the Blockchain Research Institute is a knowledge network organized to help realize the new promise of the digital economy. It builds on their yearlong investigation of distributed ledger technology, which culminated in the publication of their critically acclaimed book, *Blockchain Revolution* (Portfolio|Penguin).

Our syndicated research program, which is funded by major corporations and government agencies, aims to fill a large gap in the global understanding of blockchain technology and its strategic implications for business, government, and society.

Our global team of blockchain experts is dedicated to exploring, understanding, documenting, and informing leaders of the market opportunities and implementation challenges of this nascent technology.

Research areas include financial services, manufacturing, retail, energy and resources, technology, media, telecommunications, healthcare, and government as well as the management of organizations, the transformation of the corporation, and the regulation of innovation. We also explore blockchain's potential role in the Internet of Things, robotics and autonomous machines, artificial intelligence, and other emerging technologies.

Our findings are initially proprietary to our members and are ultimately released under a Creative Commons license to help achieve our mission. To find out more, please visit www.blockchainresearchinstitute.org.

Leadership team

Don Tapscott – Co-Founder and Executive Chairman
Alex Tapscott – Co-Founder
Joan Bigham – Managing Director
Kirsten Sandberg – Editor-in-Chief
Jane Ricciardelli – Chief Marketing Officer
Hilary Carter – Director of Research
Jenna Pilgrim – Director of Business Development
Maryantonett Flumian – Director of Client Experiences
Luke Bradley – Director of Communications

© 2017 BLOCKCHAIN RESEARCH INSTITUTE

Notes

1. Steve Omohundro, interviewed by Don Tapscott and Kirsten Sandberg, 28 May 2015.
2. Masoud Mohseni, Peter Read, Hartmut Neven, et al., Google's Quantum AI Laboratory, "Commercialize quantum technologies in five years," *Nature*, www.nature.com, Macmillan Publishers Limited, 3 March 2017. www.nature.com/news/commercialize-quantum-technologies-in-five-years-1.21583, accessed 18 Nov. 2017.
3. Jason Palmer "Quantum technology is beginning to come into its own," Technology Quarterly: Here, There and Everywhere, *The Economist*, 9 March 2017. www.economist.com/news/essays/21717782-quantum-technology-beginning-come-its-own, accessed 18 Nov. 2017.
4. Don Tapscott and Alex Tapscott, *Blockchain Revolution* (New York: Penguin Random House LLC, 2016).
5. Jonathan Kats and Yehuda Lindell, *Introduction to Modern Cryptography* (Boca Raton, FL: CRC Press, 2015); and Ghassan O. Karame and Elli Androulaki, *Bitcoin and Blockchain Security* (Boston and London: Artech House, 2017).
6. In general, smart contracts are arbitrary complex programs that may rely on security of cryptographic protocols used outside of blockchains. The conditions that trigger payments then rely on the security of those protocols. For instance, users implement smart contracts for auctions that rely on bidders properly holding/executing certain bids/payments, perhaps using cryptographic keys that are completely external to the blockchain.
7. A universal quantum computer is a quantum computer that can be programmed or configured to implement reliably an arbitrary quantum algorithm or program. The known powerful quantum attacks on cryptography require such a fault-tolerant device capable of universal operations.
8. N-bit RSA numbers are semi-primes (the products of two large primes) having size $\sim 2^{N/2}$ used in RSA-based public key schemes. R. L. Rivest, A. Shamir and L. Adleman, "*A method for obtaining digital signatures and public key cryptosystems*," *Communications of the ACM*, vol. 21 (1978): 120-126; NIST, "Digital Signature Standard (DSS)," Federal Information Processing Standards, Gaithersburg, 2013.
9. "Quantum-resistant" or "quantum-safe" means designed to be safe against quantum attacks. This requires using cryptographic tools known or believed to be resilient to quantum attacks.
10. Michele Mosca, "Cybersecurity in an era with quantum computers: will we be ready?" *Cryptology ePrint Archive: Report 2015/1075*, Waterloo, ON, 2015.
11. Technically, by *impossible*, we mean computationally hard, i.e., the running time of any known classical algorithm for key recovery (breaking) is exponential in the length of the key.
12. The 10 minutes required on average for validation of a block applies to the current Bitcoin blockchain, where the agreement protocol is based on proof of work. There are other blockchain agreement protocols in which the validation is done via other agreement schemes, and which may be significantly faster, at the (possible) cost of less understood security assumptions.
13. Companies can also deploy so-called *private* blockchains, i.e., blockchains that are visible only from the interior of the company, with no outside exposure whatsoever. However, their use is still debatable. In this paper, we focus our attention only on *public* blockchains, i.e. blockchains visible in principle to everyone.
14. By *Internet of Things*, we mean sensors and other small devices that are connected to the Internet and collect and/or transmit data via the network.
15. Technically, by *infeasible*, we mean computationally hard, i.e., the running time of any known classical algorithm for key recovery (breaking) is exponential in the length of the key.
16. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM* 21 (1978): 120-126; NIST, "Digital Signature Standard (DSS)," Federal Information Processing Standards, Gaithersburg, 2013.
17. Eric W. Weisstein, "Abelian Group," *MathWorld: A Wolfram Web Resource*, n.d. mathworld.wolfram.com/AbelianGroup.html, accessed 2 Nov. 2017.
18. Kats and Lindell, *Introduction to Modern Cryptography*, 2015.
19. Peter W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing* (1997): 1484-1509.

20. User wallets do not reveal directly the public keys they contain, but only "addresses," which are obtained from the public key via a series of hash function applications. Therefore, the public key is not directly visible to the network, but only its hash, which is believed to be resistant against a quantum attack. The public key must be broadcasted only when the user wants to spend money from her/his wallet, so the network can verify that indeed the money belongs to the respective user. Only at this stage is the public key fully revealed and thus potentially open to attack from a quantum computer.

21. Matthew Amy, Olivia Di Matteo, Vlad Gheorghiu, Michele Mosca, Alex Parent, and John Schanck, "Estimating the cost of generic quantum preimage attacks on SHA-2 and SHA-3," arXiv:1603.09383 [quant-ph], *Selected Areas of Cryptography*, 2016.

22. A quadratic speed-up is nonetheless remarkable. Imagine trying to find a particular book in a library of 1,000,000 books shelved randomly. Any human or conventional machine would need an order of 1,000,000 time steps (i.e., the intervals between events such as the browsing of each book one by one). A quantum computer could perform the same search quadratically faster, in only 1,000 time steps. Lov Grover discovered this scheme in 1994, and so we know it as Grover's quantum search algorithm. See Lov K. Grover, "Quantum Mechanics Helps in Searching for a Needle in a Haystack." *Physical Review Letters* (1997): 325-328.

23. It is estimated that the total power consumption in the Bitcoin network might surpass that of a small country like Denmark by 2020. See Vice Motherboard, "Bitcoin Could Consume as Much Electricity as Denmark by 2020," 29 Mar 2016. motherboard.vice.com/en_us/article/aek3za/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020.

24. Jing Chen and Silvio Micali, "Algorand," arXiv:1607.01341 [cs.CR], 2016; Tendermint, tendermint.com; and Hyperledger, www.hyperledger.org.

25. Oded Regev, "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography," Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing (New York: Association for Computing Machinery, 2005): 84-93; David Jao and Luca De Feo, "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies," Bo-Yin Yang, editor, *Post-Quantum Cryptography*, Lecture Notes in Computer Science (Berlin, Heidelberg: Springer, 2011): 19-34; and Tsutomu Matsumoto and Hideki Imai, "Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption," Barstow D. et al., eds., *Advances in Cryptology, EUROCRYPT 1988*, Lecture Notes in Computer Science (Berlin, Heidelberg: Springer, 1988): 419-453; and Robert J. McEliece, "A Public key Cryptosystem Based On Algebraic Coding Theory," *DSN Progress Report* (La Cañada Flintridge: Jet Propulsion Laboratory, 1978): 114-116.

26. NIST, "Post-Quantum Crypto Standardization - Call for Proposals Announcement," 15 Dec. 2016. csrc.nist.gov/groups/ST/post-quantum-crypto/cfp-announce-dec2016.html.

27. Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin, "Quantum random number generators," *Reviews of Modern Physics*, vol. 89, no. 1 (American Physical Society, 2017): 015004.

28. A cryptographically-secure pseudo-random number generator uses an initial seed to generate deterministically the list of pseudo-random numbers. If an adversary has somehow access to the seed, she/he can faithfully reproduce the whole list of numbers, hence compromising cryptographic security.

29. Charles H. Bennett and Gilles Brassard, "Public Key Distribution and Coin Tossing," *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (New York: IEEE Press, 1984): 175-179.

30. E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, A. S. Trushechkin, R. R. Yunusov, Y. V. Kurochkin, A. I. Lvovsky and A. K. Fedorov, "Quantum-secured blockchain," arXiv:1705.09258 [quant-ph], Moscow, Calgary, Orsay, 2017.

31. Anne Broadbent and Christian Schaffner, "Quantum cryptography beyond quantum key distribution," *Designs, Codes and Cryptography*, vol. 78, no. 1 (2016): 351-382.

32. Jonathan Jogenfors, "Quantum Bitcoin: An Anonymous and Distributed Currency Secured by the No-Cloning Theorem of Quantum Mechanics," arXiv:1604.01383 [quant-ph], Linköping, Sweden, 2016.

33. The number 4.2×10^{21} as a power of 2 is approximately equal to $2^{71.8}$. In cryptography, the number in the exponent of the number of steps an adversary needs to perform in order to attack the system is called the security parameter. In other words, we can say that as of August 2017, the proof-of-work system of the Bitcoin network offers approximately 71.8 bits of security.

34. A *preimage* is the inverse image of a hash.

35. The overhead is polynomial in the logarithm of the number of logical qubits and logical gates used in the computation and highly depends on which quantum error correcting code is used. As of today, the most promising quantum error correcting code is called the *surface code* and it is based on topological error correction. For a comprehensive introduction, see Austin G. Fowler et al., "Surface codes: Towards practical large-scale quantum computation," *Physical Review* A, vol. 86, no. 3 (2012): 032324.

36. Christof Zalka, "Grover's quantum searching algorithm is optimal," *Physical Review A*, vol. 60, no. 4 (1999): 2746.

37. Dr. David Jao, professor, faculty of mathematics at the University of Waterloo, and member of the Centre for Applied Cryptographic Research at the University of Waterloo, 2017.

38. Jao and Feo, "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies," 2011.

39. An *asymptote* is "a straight line that continually approaches a given curve but does not meet it at any finite distance." *Oxford Dictionaries*, Oxford University Press, 2017. en.oxforddictionaries.com/definition/us/asymptote, accessed 16 Nov. 2017.

40. Leslie Lamport, "Constructing digital signatures from a one-way function," *Technical Report SRI-CSL-98*, SRI International Computer Science Laboratory, 1979.

41. Ralph C. Merkle, "A Digital Signature Based on a Conventional Encryption Function," C. Pomerance, ed., *Advances in Cryptology - CRYPTO '87*, Lecture Notes in Computer Science (Berlin, Heidelberg: Springer, 1987): 369-378; and C. Dods, N. P. Smart, and M. Stam, "Hash Based Digital Signature Schemes," *Proceedings of the 10th International Conference on Cryptography and Coding* (Berlin, Heidelberg: Springer-Verlag, 2005): 96-115.

42. Dr. David Jao, interviewed by Vlad Gheorghiu, 7 Sept. 2017.

43. Dr. Manfred Lochter, Bundesamt für Sicherheit in der Informationstechnik, interviewed by Vlad Gheorghiu, 16 Sept. 2017.

44. Public key collisions are a major security flaw. If wallet B, newly added to the blockchain, happens to have the same address as an existing wallet A (i.e., having a public/private key collision or having a different public key that by chance hashes to the same address as the address of A), then B will be able to spend all of the A's currency (and vice-versa). Those issues appear whenever the random number generators used to generate the key pairs are not cryptographically secure, are poorly implemented, or are used inadequately (e.g., by reusing seeds).

45. Dr. Ghassan Karame, interviewed by Vlad Gheorghiu, 27 Sept. 2017.

46. Dr. Nadia Diakun-Thibault, interviewed by Vlad Gheorghiu, 25 Sept. 2017.

47. Dr. David Jao, interviewed by Vlad Gheorghiu, 7 Sept. 2017.

48. *Stateful* means that the protocol or server depends on the previous state of the application or process to function properly. As their name implies, *stateless* signatures do not need a server to keep track of a current state.

49. Johannes Buchmann, Erik Dahmen, and Andreas Hulsing, "XMSS - A Practical Forward Secure Signature Scheme based on Minimal Security Assumptions," Cryptology ePrint Archive (Nov. 2011): 484.

50. "Open Quantum Safe," 2017. openquantumsafe.org.

BLOCKCHAIN RESEARCH INSTITUTE

blockchainresearchinstitute.org