Digital assets
The security problem

Digital assets need quantum safe security

Blockchain has vast transformational potential, but flaws in security will hold it back.

The cryptography securing blockchains is compromised, making all data and value vulnerable. NIST is urging the world to migrate as soon as possible. But the proposed "Post Quantum Algorithms" are not suitable for blockchain, causing huge latency and block size problems, for only a short-lived cryptographic fix.

The technology must change to survive.

Arqit can upgrade existing blockchains with encryption that is permanently quantum safe, lightweight, and flexible.

This transforms the opportunities for enterprise and government adoption of blockchain.

Introduction

This paper discusses the threat to blockchain systems based on the vulnerabilities of the cryptography it uses. Public key infrastructure ("PKI"), the system of managing certification used by most online systems is already vulnerable to all manner of cyber threats. The public key cryptography ("PKC") underpinning it, and which most blockchains use is definitively compromised by quantum attack.

The technology world is currently being urged by government to migrate as quickly as possible from PKC. The signature schemes being proposed, so called "Post Quantum Algorithms" are fundamentally unsuited to blockchain because of their vast complexity. They seriously frustrate the ability of blockchains to scale securely, and there is very little public discussion on this problem. But there *is* an alternative.

Arqit initially targeted its utterly transformational encryption product, QuantumCloud™ at the telecoms, defence and enterprise markets to great success. Some Arqit founders have deep heritage in the emergence of early blockchain systems, and we have high conviction that the technology has an important role to play in digital transformation. But the encryption problem must be solved first. Arqit has a solution which is computationally secure, trustless, lightweight and energy efficient.

This paper should be read in conjunction with a paper analysing the computational threat to blockchain[i] published recently by Surrey University. (https://eprint.iacr.org/2021/967) and an Arqit article which discusses the rate of innovation in quantum computing technology.

About Arqit

Arqit was founded in 2017 by a group of former government and financial services cryptographers, physicists and engineers to address the looming problem in the collapse of all encryption as we know it. Our innovations exceeded our early expectations, we created a transformational system to deliver computationally secure and trustless symmetric encryptions keys to any device, anywhere with no extra hardware. Prior to product launch in 2021, dozens of major government and corporate customers have engaged with the Arqit product launch this year.

The QuantumCloud™ Platform-as-a-Service product uses quantum satellites to create identical copies of root source keys in data centres around the globe. Then a lightweight software agent or SDK, which can work as well on an IoT sensor as a battleship, borrows some of the root source key data in a process where participating edge or end point devices agree new symmetric keys in a manner which can be described as trustless and computationally secure. Keys do not exist until the moment they are needed, they can be used once and discarded.

This is a dramatic step forward in countering the weaknesses of PKI and PKC today, and also protecting the world against future quantum attack. Arqit has only been publicly known for a few weeks after inventing in private for four years, but already has a significant cohort of customers using its software in defence, telecoms, process automation and financial services. The product is ultimately available to all accredited

companies, and all uses cases. But these early vertical markets have embraced the product quickly. To these markets, Arqit now intends to add a new focus on blockchain.

Digital Transformation held back by security flaws

We are living through a global mass digitisation of almost every aspect of our society. It is possible that blockchain technology will become a truly mainstream feature of this trend. To quote BCG:

> *Blockchain is a potent and versatile emerging technology that is only starting to live up to its billing. Best known for its use in cryptocurrency, blockchain—a distributed database that fosters trust and lowers transaction costs—has the potential to change how organizations operate. Already, the technology is used in a variety of business- and public-sector applications, such as tracking and tracing items in supply chains, automating customs clearances, and facilitating financial transactions. And many more applications await development.*

The technology offers an opportunity to greatly increase liquidity into global capital markets, through faster transactions. Today's non-digital assets, once tokenised, become liquid assets that can be traded globally. The future of money is digital and this links to so many other areas such as supply chains. Many countries are closely investigating Central Bank Digital Currencies, and Arqit has one such customer.

However, there is a problem. Blockchain systems are not quantum safe. A paper published recently by Surrey University[1] explained the certainty with which all blockchain systems are compromised, posing an existential threat to the value of all cryptocurrencies and to the very possibility of the adoption of Digital Assets at government and enterprise level. There also remain unanswered questions over regulatory requirements and conflicting confidentiality/privacy requirements necessary to be successfully adopted at scale by enterprise and government users. Open source permissionless ledgers have great and enduring applications which have been embraced by a significant proportion of the world population, but we need another layer of technology to reassure enterprise and government users of long-term security effectiveness and compliance.

Today's blockchain systems

The underpinning technologies used for blockchain systems are mainly:

1) Digital signatures (locks assets to pseudo-identities)
2) Hash chaining (links blocks together and preserves immutability of blocks)
3) Merkle trees (detects and prevents tampering with any value within the blockchain)
4) In addition, for some systems, public key infrastructures (PKI) such as x509 certificates are used to enable identification and authentication of participant nodes.

Today's blockchains were designed using non-quantum safe digital signatures. Quantum computers using Shor's algorithm can derive a private key from the public key[2].The use of Elliptic Curve cryptography for signatures and the move by Bitcoin core to Schnorr signatures does nothing to protect against a quantum-enabled adversary. Both are based upon a mathematical hard problem that uses discrete logarithms to thwart a conventional computer yet will be broken on a quantum computer using Shor's algorithm.[3]

The greatest risk with non-quantum safe digital signatures occurs during the time a transaction is waiting in the unprocessed transactions buffer. The public key and a signed message are provided as part of the transaction. A quantum adversary can derive a private key from the public key in the transaction and create a new transaction with a forged signature to steal the asset.[4] All this needs to be achieved before the transaction is locked into a block. Once it is locked into a block, it is safe.

Hash-based schemes (constructions of cryptographic primitives based on the security of hash functions) are currently not seen as vulnerable to a quantum computer adversary however NIST in their report http://dx.doi.org/10.6028/NIST.IR.8105NISTIR 8105 Report on Post-Quantum Cryptography - Table 1 - Impact of Quantum Computing on Common Cryptographic Algorithms recommends a best practice of increasing the hash function output to provide protection from Quantum computer attack. Current hash-based schemes enable extensible output functions, which can deliver output of the size requested. This makes hash-based chaining schemes to secure blocks and Patricia Merkle Trees safe against a quantum adversary.

The few blockchains that have implemented a quantum-resistant signature scheme use a stateful hash-based system. This has limited applications, as there are a limited number of signatures before the wallet is inaccessible, plus keys are one time use only. Consequently, careful consideration is required when setting up the wallet, both in terms of how many keys you need, as well as when you may need to migrate to another wallet. This also makes “smart contracts” impractical using such schemes.

Some blockchain systems make extensive use of x509 certificates for use in identification of participant nodes and enabling the setting up of channels and sharing of data between these identified nodes. The x509 certificate currently uses non quantum safe digital signatures. The communications protocol TLS that consumes these certificates to prove identity, needs to be upgraded or replaced to make this quantum resistant.[5] For example, failure to upgrade to a quantum safe x509 certificate can result in spoofing of nodes. For systems where channel security acts as a means of preventing data going to non-interacting parties, this poses a significant security risk. The recent Kaseya cyberattack involved the abuse of PKI through the improper acquisition and use of a certificate, and there are many similar examples. Network node identity attacks, such as flawed identity allocation may result in non-unique and indistinguishable nodes, resulting in security problems and render the system unable to run.[6]

Upgrading digital signatures

The upgrade of blockchain digital signatures to a quantum safe version is a fundamental requirement to protect against a quantum computer enabled adversary. Signature schemes can and have been replaced on blockchain and DLT systems successfully. An example of this in blockchain is the recent acceptance and rollout of Schnorr-based signatures in the TAPROOT upgrade to Bitcoin core. Corda introduced a quantum resistant experimental signature scheme BPSS back in 2018. Both these migrations were achieved by a soft fork with new transaction signature types being introduced into the core code base.

Why not simply choose a new quantum resistant or safe digital signature scheme and implement this? The table below illustrates the problem (sizes are in bytes):

Signature Scheme	Security Claim	Public key size	Private Key Size	Signature size
ECDSA (Today's signature scheme)	-	64	32	72
Bitcoin TAPROOT Schnorr signatures	-	32	32	64
HMAC (Symmetric)	AES256	-	32	32
FALCON (NIST Finalist)	AES256	1793	2305	1330
Dilithium (NIST Finalist)	AES256	2592	4864	4595
Rainbow (NIST Finalist)	AES256	1,885,400	1,375,700	204
GeMMS (NIST Alternate)	AES192	1,237,964	24	53
Picnic3-Full (NIST Alternate)	AES192	49	73	71,179
Sphincs+ 256f Simple (NIST Alternate)	AES256	64	128	49,856

Note, none of the currently proposed NIST candidate digital signature post quantum algorithms provide a practical solution for blockchain and DLT systems. Key sizes are impractical for this use case. The only quantum safe digital signature that meets the strength and size criteria, is a symmetric HMAC signature, the signature size is half the current size of the current blockchain signature schemes.

Additionally, the computational burden placed on endpoint devices is significantly higher. For example, the NIST candidate, Dilithium signature scheme, (which is the lowest number of cycles of the NIST candidates) consumes 418,157 CPU (average) cycles per signature measured. While the HMAC signature consumes 1,300 cycles on ARM M4, assuming average transaction size of 861 bytes P2SH for Bitcoin.

Thus, the Dilithium PQA signature scheme consumes 321 times as many CPU processing cycles as HMAC. This is a huge increase in processing and power consumption, resulting in latency and the need for larger processors and power supplies. Given that the future hyperconnected world is based on ubiquitous IoT sensors, which need to be tiny and cheap, PQAs are fundamentally wrong for the world and for any form of blockchain sensitive to latency and power limitations.

The challenge with using a symmetric-based signature is identification of the signer when multiple parties have the signing key. This is resolved by including within a signed message, a public identity and a ratchetted key derivation signature.

Public keys need to be stored on the blockchain and transmitted with each transaction, alongside the signed transaction. The public key stored on a blockchain is a hash of the public key in order to prevent

an adversary having access to the public key from the blockchain. This reduces the public key size stored through the use of the hash function. However, the public key needs to be transmitted with each transaction, along with the signature of the transaction. Therefore, the size of public keys and in particular signatures, is a critical aspect for blockchain.

The reason for this is they directly impact both the storage requirement for each transaction and block, as well as the number of transactions that can be processed in each block, given a fixed block size. Blocks and transactions need to be communicated to participating nodes, while size impacts latency and transmission times. Block sizes are carefully chosen to ensure response and throughput for a blockchain, so any increase in block size will negatively impact overall system performance.

The size of transactions also impacts the costs of transactions for end users. The recent move by bitcoin core to TAPROOT was primarily driven to reduce the size of multi-signatures and as a by-product, enhance privacy. With TAPROOT Schnorr, signatures aggregate multiple signatures into one signature. Size of signatures matters acutely for blockchain systems users. Ironically, this also removes a key quantum defence for Bitcoin's core system, namely enforcing multiple signatures to increase the number of signatures a quantum adversary needs to crack for each transaction. This is also true for privacy coins, where privacy comes at the price of not using multi-signatures.

Private signing keys need to be held off-chain securely by the owner. Today, these are typically held in a hardware wallet or an online custodial wallet. Wallet security is perhaps the weakest link in the chain today and needs to be addressed to protect against a quantum adversary. However, the technology used is essentially symmetric-based and so can be extended relatively easily.

The growing gap between regulation and privacy

As the digital asset marketplace evolves towards the mainstream, the size, scale, and impact of digitising assets has become an issue for regulators around the world.

The Financial Action Task Force Travel Rule, officially accepted by FATF[7] on 21 June 2019, describes the compliance obligations financial institutions in 37 member countries worldwide must apply. The Travel Rule is an update to existing FATF Recommendation 16 on cross-border and domestic bank transfers.

According to the Travel Rule of Recommendation 16, all digital fund transfers creators and beneficiaries should exchange descriptive information. The rule applies to all Virtual Asset Service Provider (VASPs), financial institutions, and mandatory organisations.

As part of FATF Recommendation 16, virtual asset transfers must provide information such as the name, account number, physical address, national ID number, customer ID number, date, and location of the creators and beneficiaries.

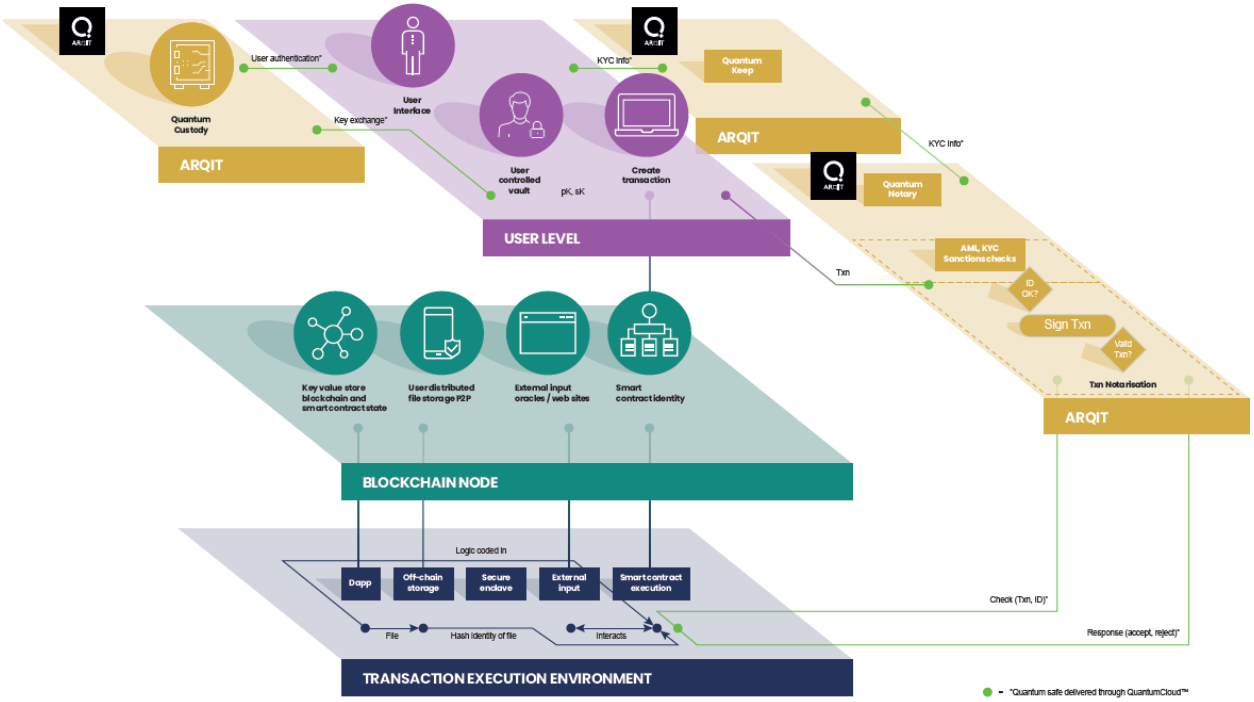
Recent regulations on requirements to use digital asset custodial services have created a need to demonstrate brokers compliance with use of "qualified custodian" for digital asset custody. This is an extension of existing broker dealer regulations to the digital assets. It can be seen as a pre-cursor to enable the introduction of issued digital currency by either central banks or banks. Rules for special-purpose broker dealers have been recently published by the Securities and Exchange Commission (SEC).[8]

Securing digital assets keys is a critical activity but doing so in a non-quantum safe manner does not deliver a long-term store of value benefit.

Making blockchain quantum safe

Updating an existing blockchain's digital signatures to use the proposed NIST Post Quantum Cryptography[9] digital signature algorithms is not a practical solution for today's systems.

An alternative means of making an existing blockchain or DLT system quantum safe is to add an extra layer of quantum safe security. This can be achieved by adding a digital notary service, an additional step in the unlocking process for a new type of transaction on a blockchain or DLT system. We call this Quantum Notary.



QuantumCloud™ as an authority can operate the quantum notary, but optionally the notary code can be given to any customer or group of members to operate. Therefore, a government or enterprise customer does not need to trust Arqit for the operation of the notary. Equally in a decentralised scheme of many mutually distrusting but co-operating counterparties, the Quantum Notary can be decentralised.

A Notary service can only operate/work if it has the ability to notarise based upon strong authentication of the device/user. Notaries exist in one form or another on every DLT network. Privacy is assured in that the customer still has their private key, which the notary will never see, or any details of the transaction. The notary is only holding a checksum of the payload and authentication of the device/user and providing true/force to the recipient's challenge.

Arqit will also provide a quantum safe digital asset custody service to independently hold the private keys for the user. This enables both regulatory compliance and perhaps more crucially is a pre-requisite for any digital asset issuance such as Central Bank Digital Currency (CBDC) or Bank Issued Digital Currency (BIDC).

Arqit has built a system to sit on top of the Quantum Blockchain, called Quantum Money. This product is suitable for either CBDC or BIDC, or simply as a Fiat multicurrency payment system. The first large scale customer is developing this project with Arqit at the moment.

Simpler, stronger encryption for blockchain

By enhancing Blockchain and DLT platforms with Symmetric encryption, we assure long term security, enabling long term business use cases and guaranteed security assurance beyond the lifetime of current PKC based blockchain systems. Through quantum secure deployment of symmetric keys to both blockchain nodes and wallets, it is possible also to address the conflicting need for privacy of transactions and the transparency needed to check them.

A blockchain or DLT system using symmetric keys can enable practical encryption of data at rest on the blockchain.This enables users and smart contracts on blockchains to securely communicate between themselves and both encrypt and decrypt transactions they are authorized to participate in. This makes blockchain and DLT systems significantly more useful to business.

Building an eco-friendly blockchain and DLT system

The origins of blockchain technology with the proof of work (PoW) consensus algorithm has perhaps, understandably, made people aware of the carbon footprint of blockchain technologies.

Most modern blockchain systems are moving away from PoW consensus algorithms to alternative, more carbon-efficient consensus algorithms such as Proof of Stake (PoS). This can dramatically reduce carbon emissions for a blockchain. However, through use of symmetric encryption keys on a blockchain we can also radically reduce the carbon cost.

Simply put, symmetric encryption algorithms are far more efficient than asymmetric algorithms. In the context of blockchain systems, the one constant encryption and decryption operation is the digital signature. Using a symmetric digital signature such as HMAC, this is significantly more efficient than today's digital signature. When compared against the NIST candidate digital signatures the difference is orders of magnitude better. Typical Post Quantum Algorithms are less efficient in terms of CPU processing cycles by 1,488 times. Arqit's key exchange process stands to generate significant energy savings. Furthermore, Arqit's Quantum Blockchain incorporates a patented technology which measures the energy efficiency of every participating node.

Conclusions

The adoption of digital assets at scale is now in full flow in the financial services market, with others likely to follow. But all blockchain is compromised by quantum attack, and the proposed PQA solutions are not viable. Investing for the medium term in technology which is either fundamentally insecure or will become unusable is not strategy that supports successful global adoption.

There is an answer, and to understand how easy it is to apply it, get in touch.

References

[1] "Assessment of Quantum Threat To Bitcoin and Derived Cryptocurrencies," [Online]. Available: https://eprint.iacr.org/2021/967.

[2] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *Society for Industrial & Applied Mathematics (SIAM),* p. 1484–1509, 1997.

[3] H. Reich, "Youtube - How Quantum Computers Break Encryption | Shor's Algorithm Explained," 1 May 2019. [Online]. Available: https://www.youtube.com/watch?v=lvTqbM5Dq4Q. [Accessed 5 7 2021].

[4] I. Barmes and B. Bosch, "Quantum computers and the Bitcoin blockchain," 1 1 2020. [Online]. Available: https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html. [Accessed 5 7 2021].

[5] E. (. T. S. Institute), "Quantum Safe Cryptography," 1 6 2015. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf. [Accessed 5 7 2021].

[6] I. T. U. (ITU), "ITU-T X.1401 Security threats to distributed ledger technology," International Telecommnunications Union, 29 11 2019. [Online]. Available: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1401-201911-I!!PDF-E&type=items. [Accessed 5 7 2021].

[7] F. A. T. F. (FATF), "Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs," Financial Action Task Force, 2021.

[8] S. a. E. C. (SEC), "SEC Issues Statement and Requests Comment Regarding the Custody of Digital Asset Securities by Special Purpose Broker-Dealers," Securities and Exchange Commission (SEC), 23 12 2020. [Online]. Available: https://www.sec.gov/news/press-release/2020-340. [Accessed 5 7 2021].

[9] "NIST Post Quantum Cryptography," National Institute of Technology (NIST), 5 k7 2021. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography. [Accessed 5 7 2021].