Blockchains and Cryptography

James Davenport
masjhd@bath.ac.uk

University of Bath

30 April 2024

Basics

"A blockchain is a distributed ledger with growing lists of records (blocks) that are securely linked together via cryptographic hashes" [Wikipedia/many]
Bitcoin uses SHA-256 as the cryptographic hash. This is part of the SHA-2 family, designed in 2001. While generally obsoleted by SHA-3 (2012) there are no known successful attacks on SHA-2. Furthermore, it is generally believed that there aren't good quantum attacks on SHA-2 [ADMG+16].
Hence it makes sense to believe in the integrity of the chain of blocks (which doesn't necessarily guarantee confidentiality or availability!).
From this point, we'll focus on public permissionless blockchains, as in most cryptocurrencies.

public permissionless blockchains

If they are public, can't anyone join? Needs some proof of those who validate the blockchain (consensus protocol).

Proof of work (Bitcoin etc.) To add a block, The validator (miner) need to have solved a hard (lots of CPU) problem. Bitcoin uses SHA-256, but this is a separate use.

Again, this is believed quantum safe, in terms of *generating* the proof of work, but I need "identity" to continue to have it.

Proof of stake (Ethereum since 2022) The validator most prove possession of a certain amount of the currency, generally via a smart contract. This relies on "identity".

Hence "identity" is key to all known serious cryptocurrency schemes

Who are the participants

How do I prove I'm the Joe Shark with 100 bitcoin in an account? Or the Ugly Miner with a proof of work, or ....
The answer is public key cryptography, which is a slight misnomer (JHD prefers *asymmetric cryptography*).

Private Key Which I use to generate signatures

Public Key (paired with private key) which anyone can use to verify my signature

Examples RSA [Coc73, RSA78] based on difficulty of factoring suitable large numbers.

ECDSA which tends to be used today.

All such schemes are vulnerable to quantum computers.

Post-Quantum Cryptography

The U.S. NIST is running a competition to choose quantum-proof algorithms, and has selected some (`https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022`). However, this is not easy.

Signatures are larger (10×–100×), and signatures have to fit in blocks.

The implications for practice/performance are not clear.

The implications for a mixed economy are not clear.

But I will need to transfer from old (unsafe) signatures to new ones, so a mixed economy will be necessary for a transition.

See for example `https://cointelegraph.com/learn/post-quantum-threats-to-proof-of-work-cryptocurrencies`.

Q&A

When will quantum actually become a threat?

A–JHD I don't answer that sort of question.

Insists

JHD There are two views.

1. "Quantum Computing is the Technology of the Future, always was and always will be". I have some sympathy with this view.
2. No serious person expects to see quantum computers *of this scale* in less than 10 years. But we are looking at a major transition programme of at least five years to get safe, and the research is only part-done..

Bibliography I

M. Amy, O. Di Matteo, V. Gheorghiu, M. Mosca, A. Parent, and J. Schanck.
Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3.
International Conference on Selected Areas in Cryptography, pages 317–337, 2016.

C.C. Cocks.
A Note on Non-Secret Encryption.
`http://www.cesg.gov.uk/publications/media/notense.pdf`, 1973.

R.L. Rivest, A. Shamir, and L. Adleman.
A Method for Obtaining Digital Signatures and Public Key Cryptosystems.
Comm. ACM, 21:120–126, 1978.