



Kaushal Kumar Singh

The Quantum Resistant Ledger
Core Developer



The Quantum-Resistant Ledger



Agenda

Deploying

Winternitz OTS+ Signatures

in an

**Extended Merkle Signature Scheme
(XMSS)**

for the purpose of

Securing a Blockchain Network

Against

Quantum Computers

Why should I pay attention?



Bitcoin Is Not Quantum-Safe, And How We Can Fix It When Needed

by Vitalik Buterin Jul 30, 2013 11:42 PM EST

coindesk

Blockchain 101

Technology

Markets

Business

actions

The Washington Post
Democracy Dies in Darkness

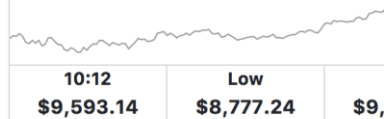
National Security

NSA seeks to build quantum computer that could crack most types of encryption

By Steven Rich and Barton Gellman January 2, 2014 Email the author



BTC/USD



BITCOIN SECURITY OCTOBER 16, 2016 18:58

Quantum Computers Will Destroy Bitcoin, Scientists Warn

MIT
Technology
Review

Business Impact

Quantum Computers Pose Imminent Threat to Bitcoin Security

Quantum Computers Could Jack Your Crypto Private Key in 10 Years, Researchers Say



Agenda

Deploying

Winternitz OTS+ Signatures

in an

Extended Merkle Signature Scheme

(XMSS)

for the purpose of

Securing a Blockchain Network

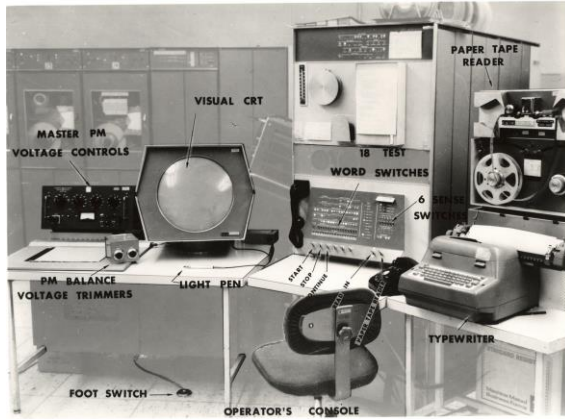
Against

Quantum Computers

What are QCs?

What are Quantum Computers?

Computers exploiting quantum mechanics



Traditional Computer
Circa 1961. PDP-1



Quantum Computer
Circa 2017

0

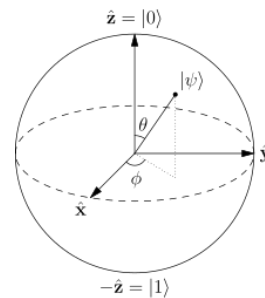
1

Bits

- Can take two possible values - 0 or 1.
- Can be easily linked to one another.

1

Qubits



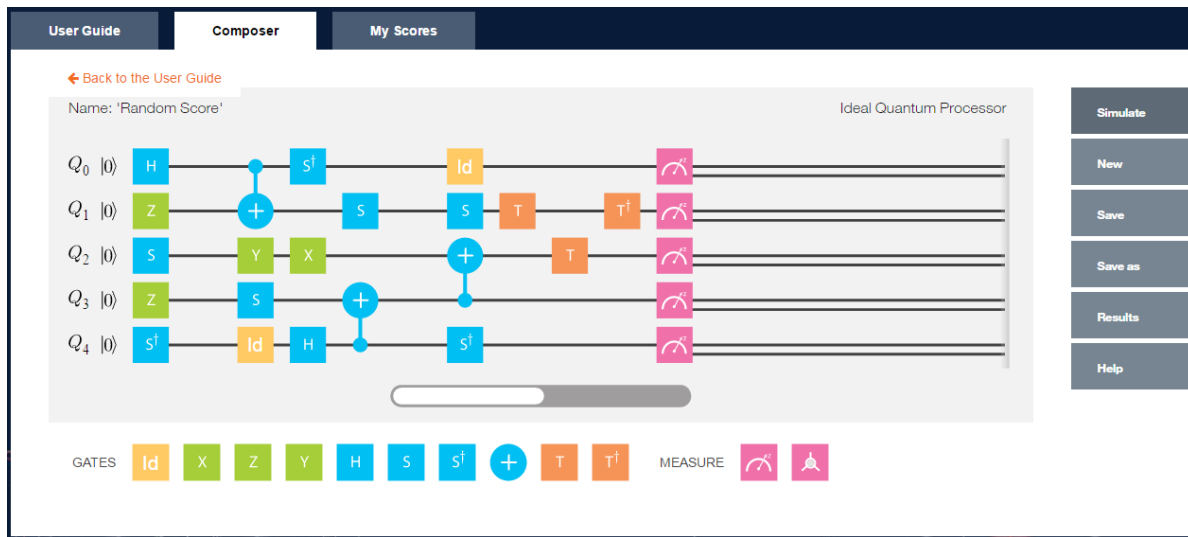
- Can be a **superposition** of both 0 and 1 at the same time.
- Every qubit doubles the amount of positions (1=2, 2=4, 3=8, etc.)
- Difficult to link to one another



What comprises a Quantum Computer?

- Uses **qubits** instead of bits like a traditional computer
- A quantum computer with **n** qubits can be in an arbitrary superposition of up to 2^n different states **simultaneously!**
- Allows for **exponential increase in computational power.** For every qubit added to a system, the amount of alternatives that can be processed in parallel doubles. i.e. 3 qubits can compute 8 values, 4 qubits can compute 16 values *simultaneously*.

When can I use one?



IBM Q Experience

- For researchers & lay people to experiment on quantum computers



Q# from Microsoft

- Not for direct coding of quantum computers
- For writing sub programs that run on a quantum processor, under control of a traditional computer



Agenda

Deploying
Winternitz OTS+ Signatures
in an
Extended Merkle Signature Scheme
(XMSS)
for the purpose of
Securing a Blockchain Network
Against
Quantum Computers

What are QCs?

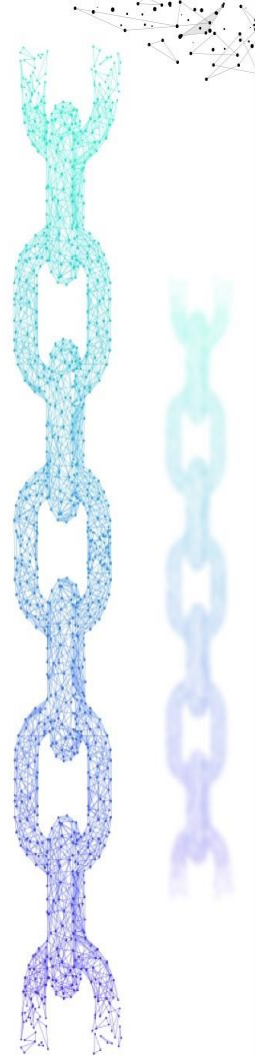
What is the issue?

Cryptography Crash Course!

- *All cryptographic methods are based upon one or more assumptions*
- *More assumptions = more failure points*
- *If the assumption is broken, the crypto is broken*

A history of assumptions

- *Walls were great at defending against medieval siege tech*
- *Assumption: the amount of time to breach them would take so long as to leave the walls functionally secure*



Then there was Dynamite!

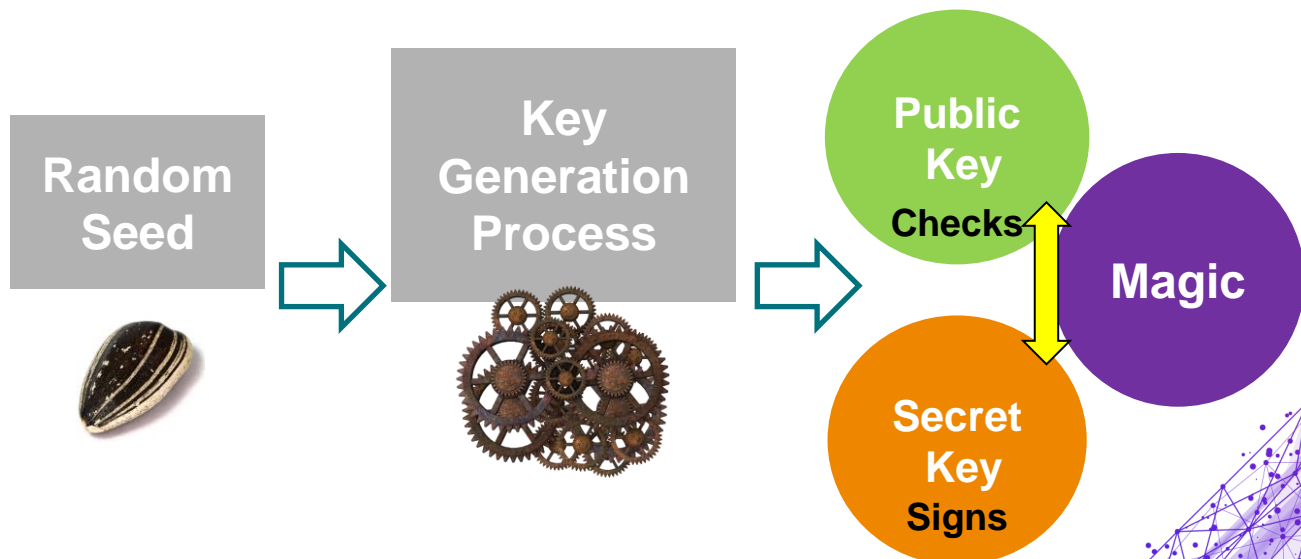
Walls that used to be able to
withstand years of abuse
suddenly could be taken down in
a matter of hours or days



Cryptography Crash Course!

Signatures

- *When Bob wants to prove to the World that he approves something.*



Cryptography Crash Course!

Signatures pt.2

- Bob shows the world his **Public Key**
- Bob uses his **Secret Key** to sign
- Anyone can **Deposit**, only Bob can **Withdraw**



Cryptography Crash Course!

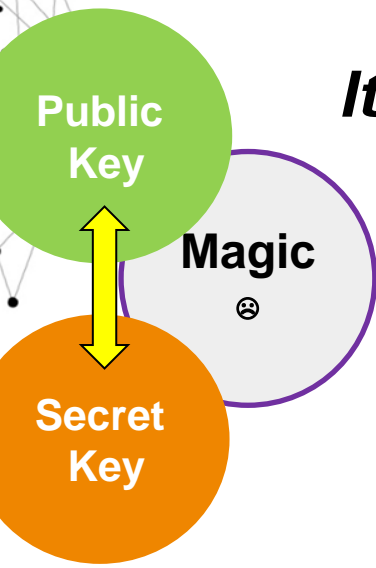
ECDSA

*Used by Bitcoin, Ethereum, and most
cryptocurrencies*

ASSUMPTION

*It is **hard** for computers to factorize large
numbers.*

*It is currently possible to crack ECDSA,
but takes too long to be worth it.*



Cryptography Crash Course!

ECDSA pt.2

Quantum Computers can factorize easily (using Shor's algorithm)

Public
Key

Magic
☹

Secret
Key

Broken assumption

=

Broken cryptography



Agenda

Deploying

Winternitz OTS+ Signatures

in an

**Extended Merkle Signature Scheme
(XMSS)**

for the purpose of

Securing a Blockchain Network

Against

Quantum Computers

What are QCs?

What is the issue?


What can be done?



Post Quantum Cryptography!

A solution to resist both Traditional and Quantum Computers

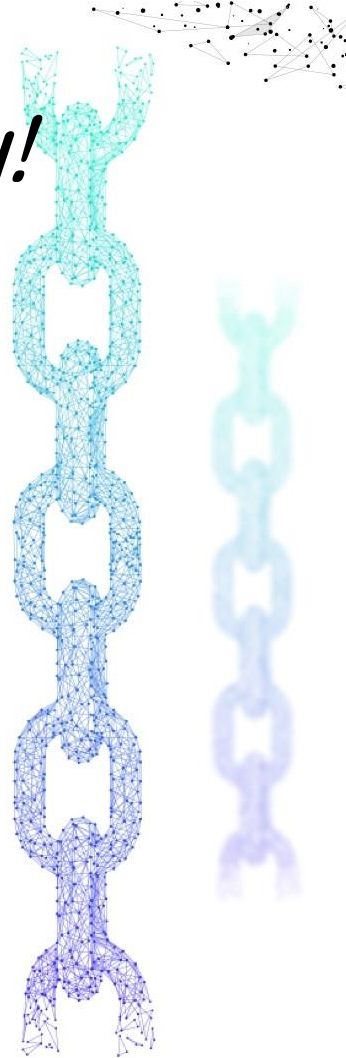
*But also applicable to a **Blockchain***

- *Can't be too slow*
 - *Can't be too large (signature size)*
 - *Must be provably secure*
 - *Minimal failure points (assumptions)*
 - *Has been peer-reviewed & scrutinized*
- 

Post Quantum Cryptography!

Lots of research and many alternatives!

- *Lattice-based cryptography*
- *Multivariate cryptography*
- *Hash-based cryptography*
- *Code-based cryptography*
- *Super-singular elliptic curve isogeny cryptography*



Post Quantum Cryptography!

Lots of research and many alternatives!

- *Lattice-based cryptography*
- *Multivariate cryptography*
- ***Hash-based cryptography***
- *Code-based cryptography*
- *Supersingular elliptic curve isogeny cryptography*



Hash Based Cryptography

One-way functions

- *Like a cake - you cannot determine specific amounts of the individual ingredients post-bake*
- *Also, one cannot un-bake a cake back into its individual ingredients*



Advantages?

- **Simple** *security assumptions (fewer failure points)*
- **Fast** *to compute, hard to crack*
- *Some examples:*
 - *Only rely on the security of one-way functions*
 - *Lamport One Time Signatures (OTS) (1979)*
 - *Winternitz OTS Signatures (1979)*
 - *Developed by Ralph Merkle, inspired by Robert Winternitz*



Winternitz OTS+ = One Time Signature

Quantum Computers struggle with hashes

- *Signatures are relatively small*
- *Keysizes are relatively small*
- *Makes minimal security assumptions (minimal fail points)*

**It is not all rainbows
and unicorns**

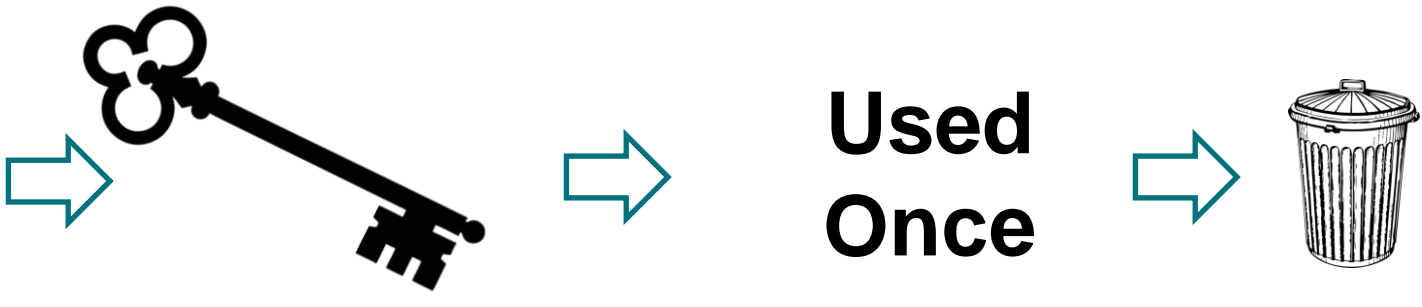


Winternitz OTS+ = One Time

Signature

*Bob can only sign once, and he needs to change his
Public Key **every time!***

*That means changing **wallet addresses** every time!*

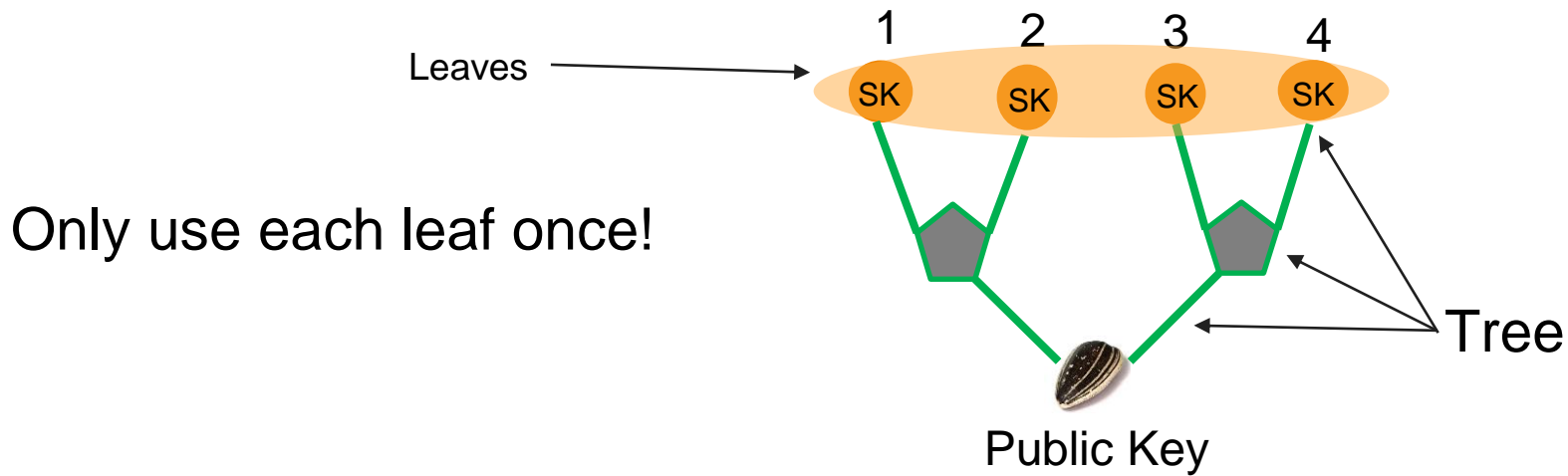


XMSS (Extended Merkle Signature Scheme)

Bob grows a tree full of secret keys!

All are linked to the same Public Key at the root

*BUT! He **must remember** the leaves he has used!*



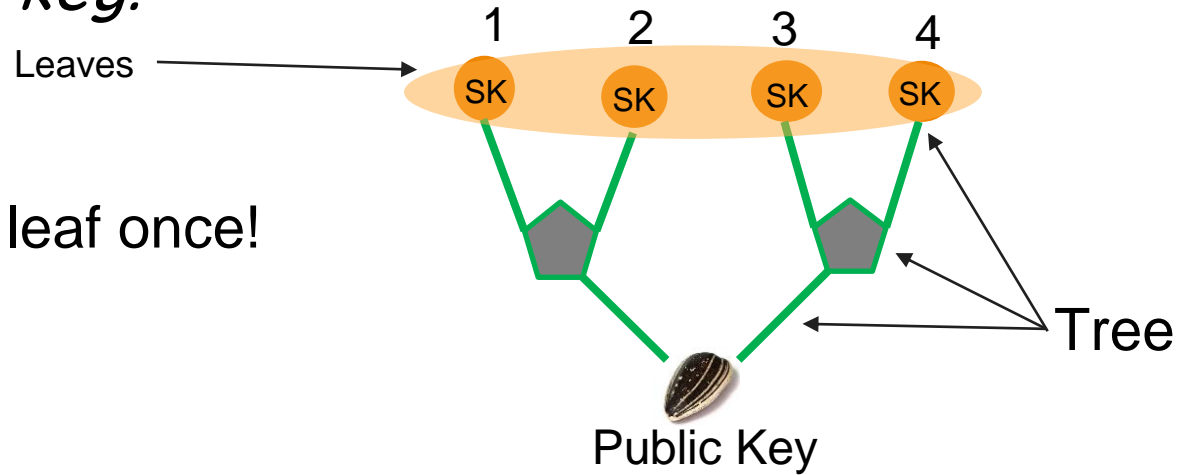
Only use each leaf once!

XMSS (Extended Merkle Signature Scheme)

The Good: *The tree can be VERY high and have many leaves*

The Danger: *Bob **must never** sign twice with the same secret key!*

Only use each leaf once!





Conclusion

- *We don't need to wait for Quantum Supremacy. A single actor could disrupt the cryptocurrency economy*
- *Companies are making a lot of public progress*
- *Government programs have likely made more progress than has been publicized*



Conclusion

- *Upgrading in cryptocurrency is not easy. BTC is an example of political struggles with respect to upgrading*