QUANTUM CYBER

BLOCKCHAIN IOT

QUANTUM CYBER

BLOCKCHAIN IOT

Secure https://unsplash.com/search/photos/quantum-computer

quantum computer

Home

Laptop | Computer | Keyboard | Technology | Macbook | Screen | Monitor | Deskto

Quantum computer pictures

1,111 free quantum computer pictures

1.1k Photos 0 Collections 6 Users

Sorry, this product is no longer available!

See larger image

100 pcs lot Lava pendants Energy quantum scalar pendant energy card and Resist radiation JHE0151

Price: **US $263.72 - 341.67** / Lot (US $2.64 - 3.42 / Piece) Reference Currency

100 Pieces / Lot

Wholesale Price (Lot):	1 +	3 +	15 +	16 +	32 +
	US $341.67	US $334.70	US $317.96	US $314.75	US $313.17

Quantity: 1 Lot

Shipping Cost: **US $0.95** to Switzerland Via China Post Air Mail

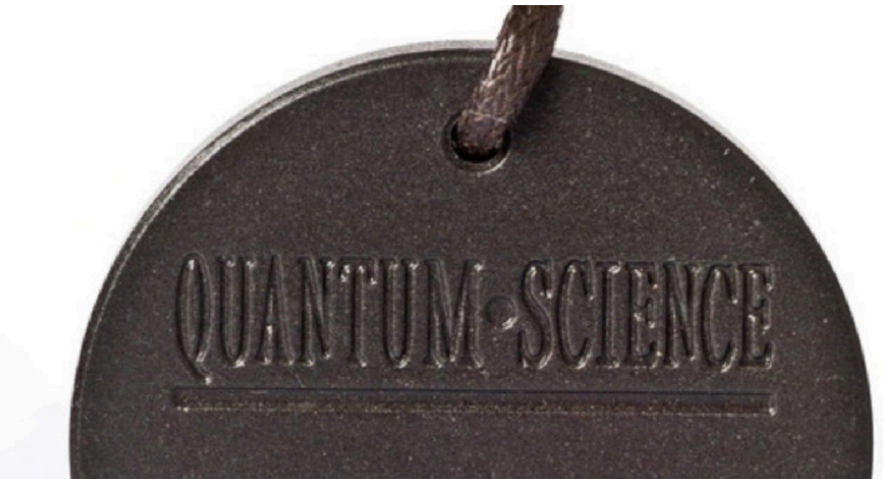
Estimated delivery time: Dec 26 and Jan 5, ships out within 7 business days ?

Total Cost: US $342.62

Item sold out Add to Favorite Items (0)

Health Benefits:

1. Reduces inflammation.
2. Promotes unclamping of cells.
3. Enhances immune and endocrine systems.
4. Helps to protect DNA from damage.
5. Improves stamina, endurance and strength.
6. Alleviates soreness, aches and pains, and improves flexibility.
7. Helps to retard the ageing process.
8. Helps to fight cancer cells.
9. Has the ability to destroy viruses and bacteria.
10. Enhances cellular nutrition and detoxification.
11. Enhances cellular permeability.
12. Increases energy.
13. Strengthens the body's biofield preventing electro-magnetic waves from affecting one's health.
14. Increases focus and concentration.
15. Improves blood Circulation.
16. Energizes block cells and reduces "stickiness".



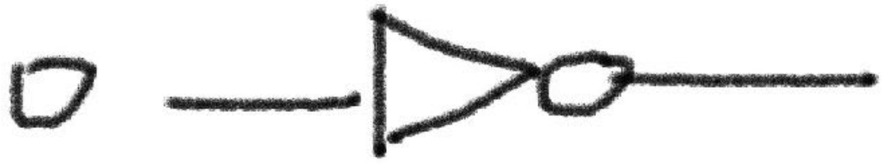
QUBIT

$$\alpha|0\rangle + \beta|1\rangle \equiv \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$\alpha, \beta \in \mathbb{C}$

= "AMPLITUDES"

$\simeq$ QUANTUM PROBABILITIES

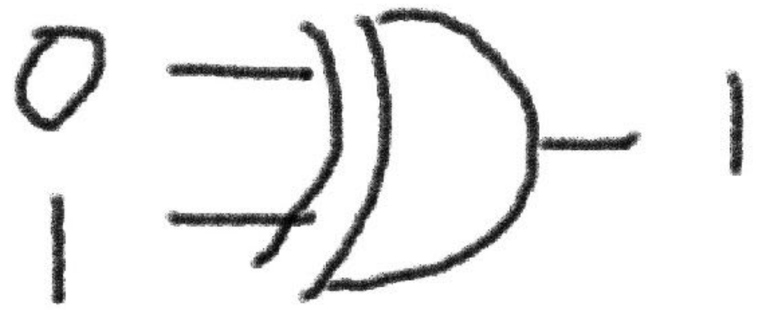


CLASSIC

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{—H—} \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}$$

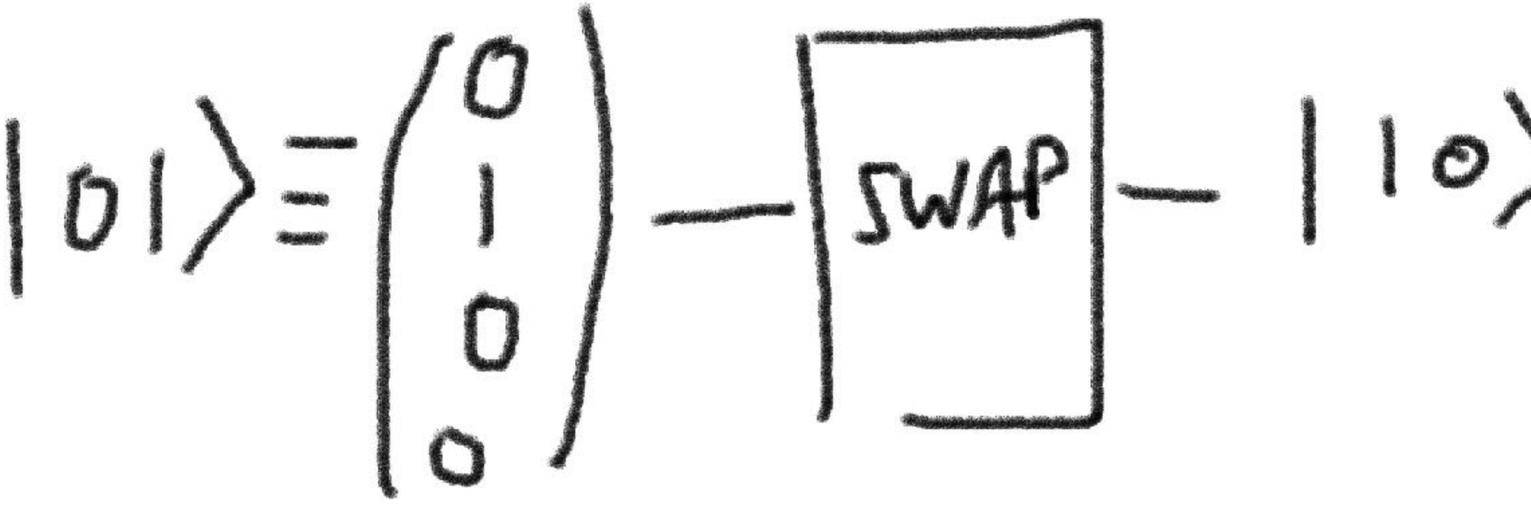
QUANTUM

↪ 2 Numbers



CLASSIC

2 BITS



QUANTUM 2 QUBITS

→ 4 numbers to simulate

2-QUBIT GATE

$\simeq$ 4x4 matrix

$$\boxed{\text{SWAP}} \simeq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

N QUBITS

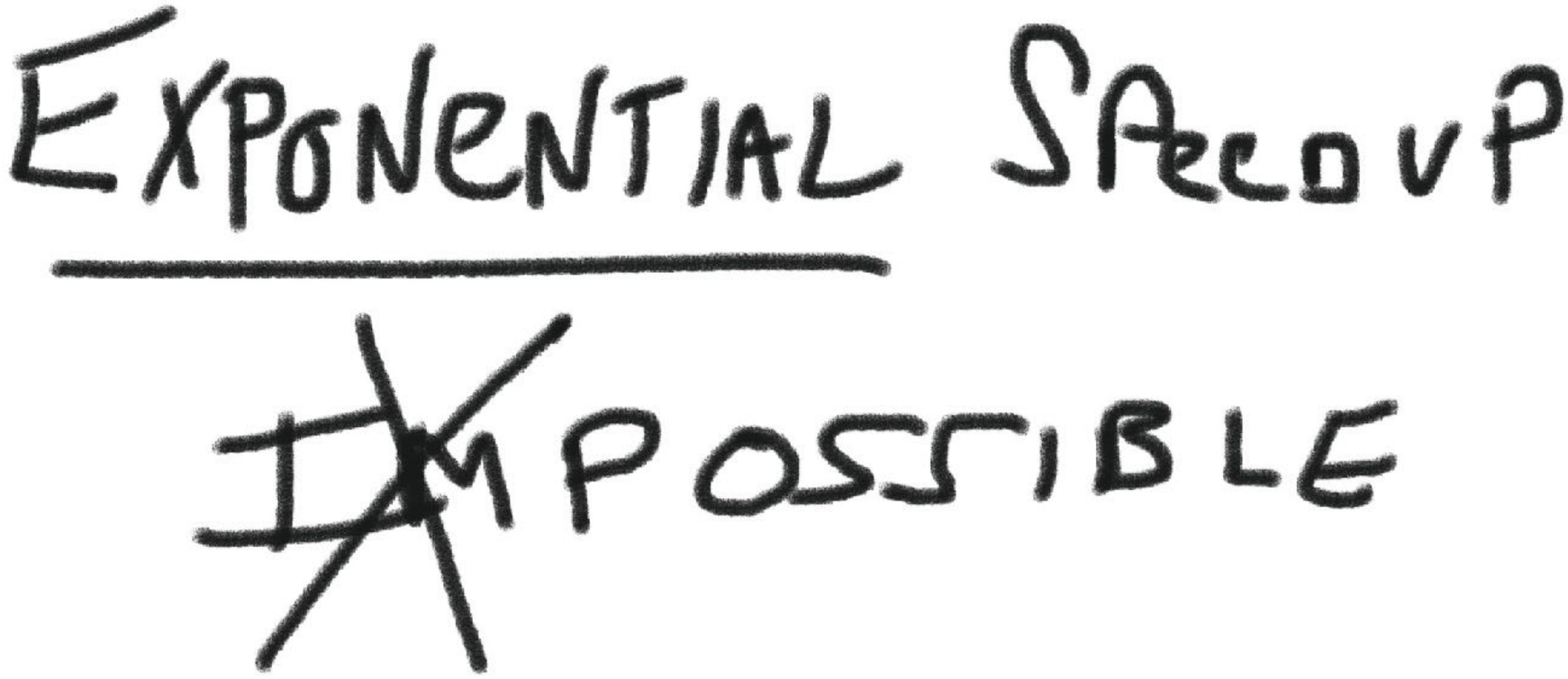
$\rightarrow$ $\int$ state $\sim$ 2^N numbers

Gate $\sim$ 2^{2N} numbers

$\Rightarrow$ CAN'T SIMULATE CLASSICALLY FOR $N \gtrsim 50$

Quantum Circuits can solve certain problems faster

Ex $O(2^{n/2}) \rightarrow O(n)$


EXPONENTIAL SPEEDUP
IMPOSSIBLE

QC IS NOT

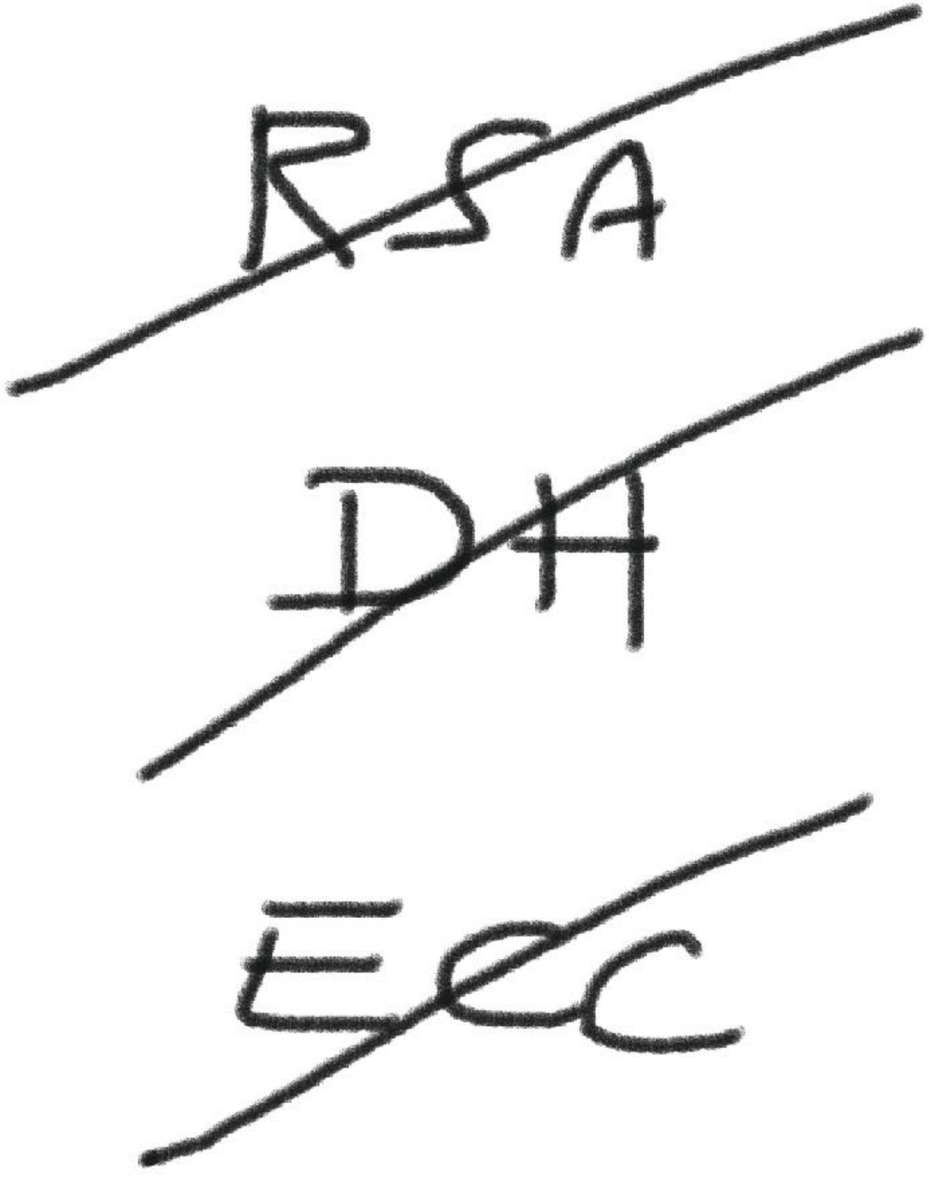
- SUPERFAST COMPUTER
- FREE PARALLELISM
- SOLVING NP-HARD POS

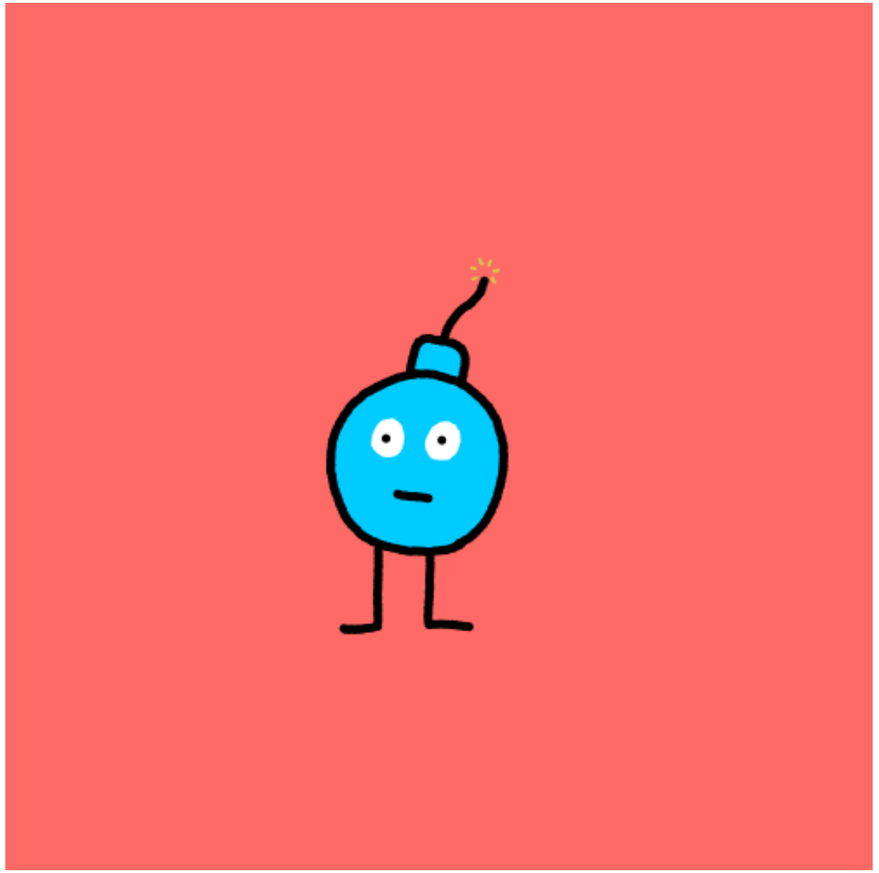
SHOR

$N = pq \longrightarrow (p, q)$

$x^d \bmod p \longrightarrow d$

in $O(m^5)$


RSA
DH
ECC

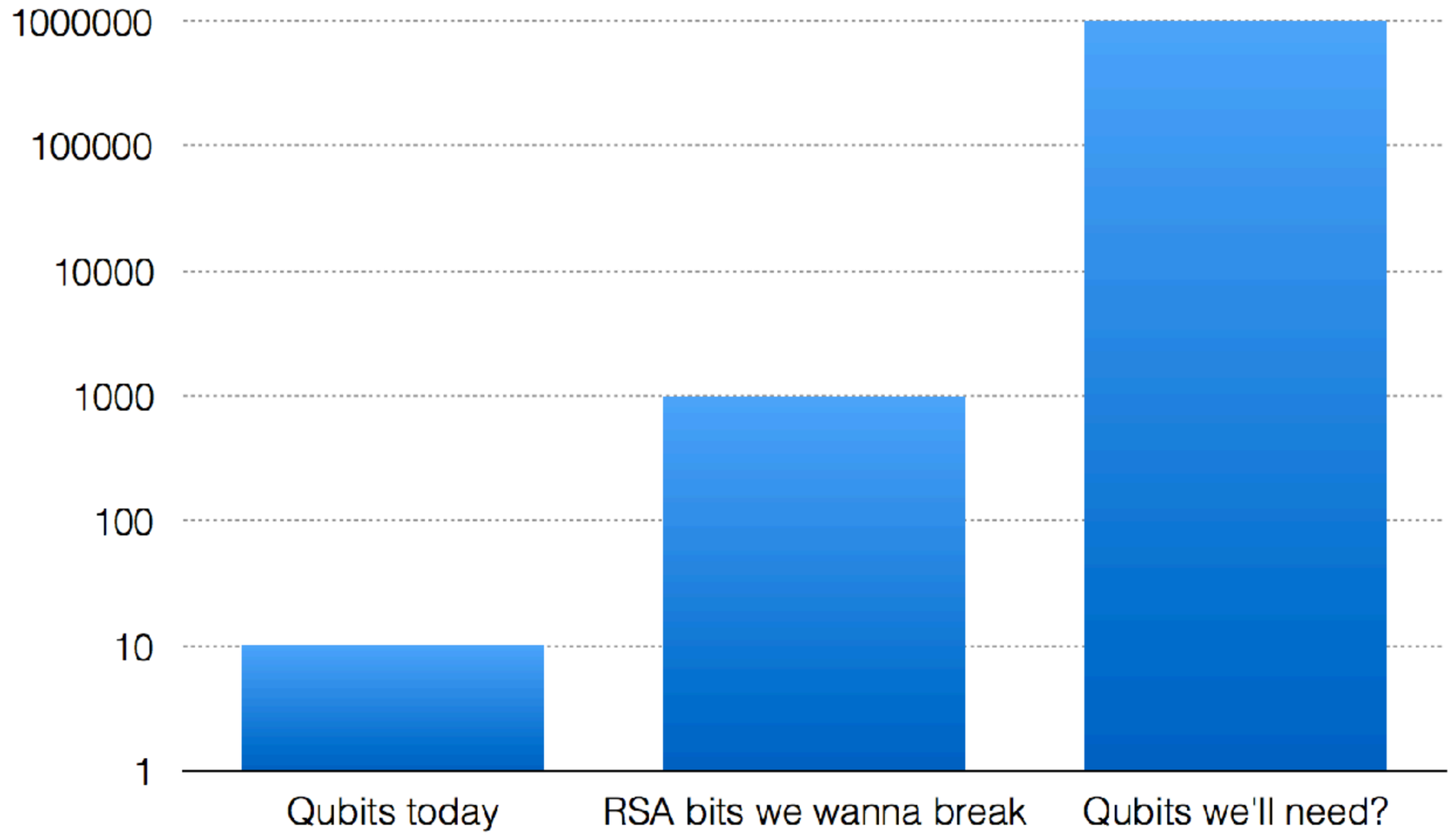


Designing a Million-Qubit Quantum Computer Using Resource Performance Simulator

Muhammad Ahsan, Rodney Van Meter, Jungsang Kim

(Submitted on 2 Dec 2015)

The optimal design of a fault-tolerant quantum computer involves finding an appropriate balance between the burden of large-scale integration of noisy components and the load of improving the reliability of hardware technology. This balance can be evaluated by quantitatively modeling the execution of quantum logic operations on a realistic quantum hardware containing limited computational resources. In this work, we report a complete performance simulation software tool capable of (1) searching the hardware design space by varying resource architecture and technology parameters, (2) synthesizing and scheduling fault-tolerant quantum algorithm within the hardware constraints, (3) quantifying the performance metrics such as the execution time and the failure probability of the algorithm, and (4) analyzing the breakdown of these metrics to highlight the performance bottlenecks and visualizing resource utilization to evaluate the adequacy of the chosen design. Using this tool we investigate a vast design space for implementing key building blocks of Shor's algorithm to factor a 1,024-bit number with a baseline budget of 1.5 million qubits. We show that a trapped-ion quantum computer designed with twice as many qubits and one-tenth of the baseline infidelity of the communication channel can factor a 2,048-bit integer in less than five months.

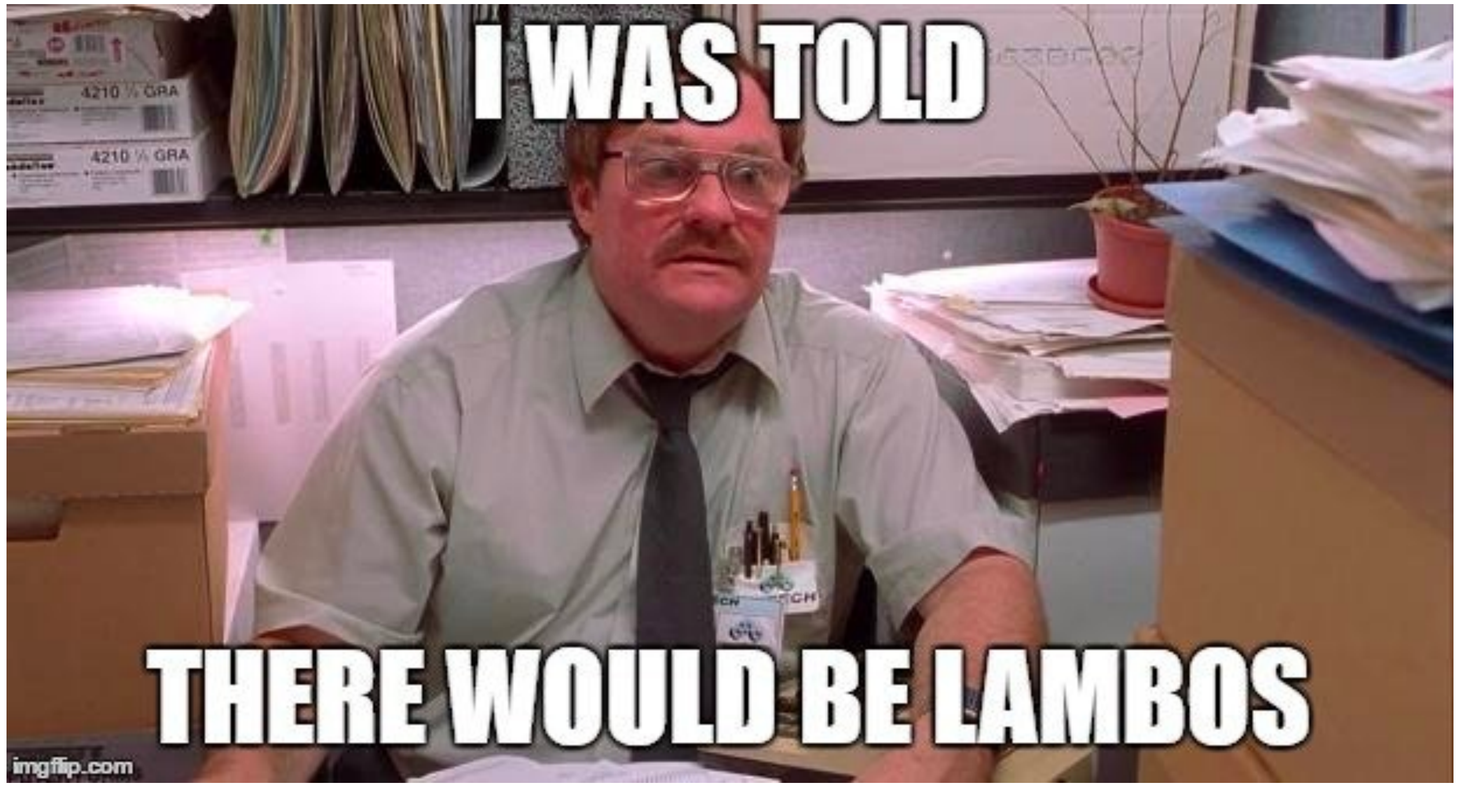

1000000
100000
10000
1000
100
10
1
Qubits today
RSA bits we wanna break
Qubits we'll need?

(log scale)

Where are these used?

QUANTUM CYBER

BLOCKCHAIN IOT


I WAS TOLD
THERE WOULD BE LAMBOS
imgflip.com

Mandatory slide: Bitcoin’s blockchain

- **Database** recording all transactions
- Guaranteed **immutable**, thanks to a *proof-of-work* system
- **Distributed**: transactions validated by a network of peers
- **Decentralized**: thanks to a *consensus protocol*

Mandatory slide: Bitcoin’s blockchain

- **Database** recording all transactions
- Guaranteed **immutable**, thanks to a *proof-of-work* system
- **Distributed**: transactions validated by a network of peers
- **DECENTRALIZED**: thanks to a *consensus protocol*

Blockchain accounts security

"Public-key money":

- Public key ~ recipient's account number
- Private key needed to access/spend money received, by issuing a **digital signature** (typically 256-bit ECDSA)

Blockchain accounts security

"Public-key money":

- Public key ~ recipient's account number
- Private key needed to access/spend money received, by issuing a **digital signature** (typically 256-bit ECDSA)

BROKEN BY SHOR'S QUANTUM ALGORITHM

Blockchain mining security

“Decentralized lottery”:

- Proof-of-work (PoW): slightly less strong because of quantum search, but hash-based scheme essentially ok
- Proof-of-state (PoS): no crypto computations specific to PoS

Blockchain mining security

“Decentralized lottery”:

- Proof-of-work (PoW): slightly less strong because of quantum search, but hash-based scheme essentially ok
- Proof-of-state (PoS): no crypto computations specific to PoS

BUT: both need secure digital signatures

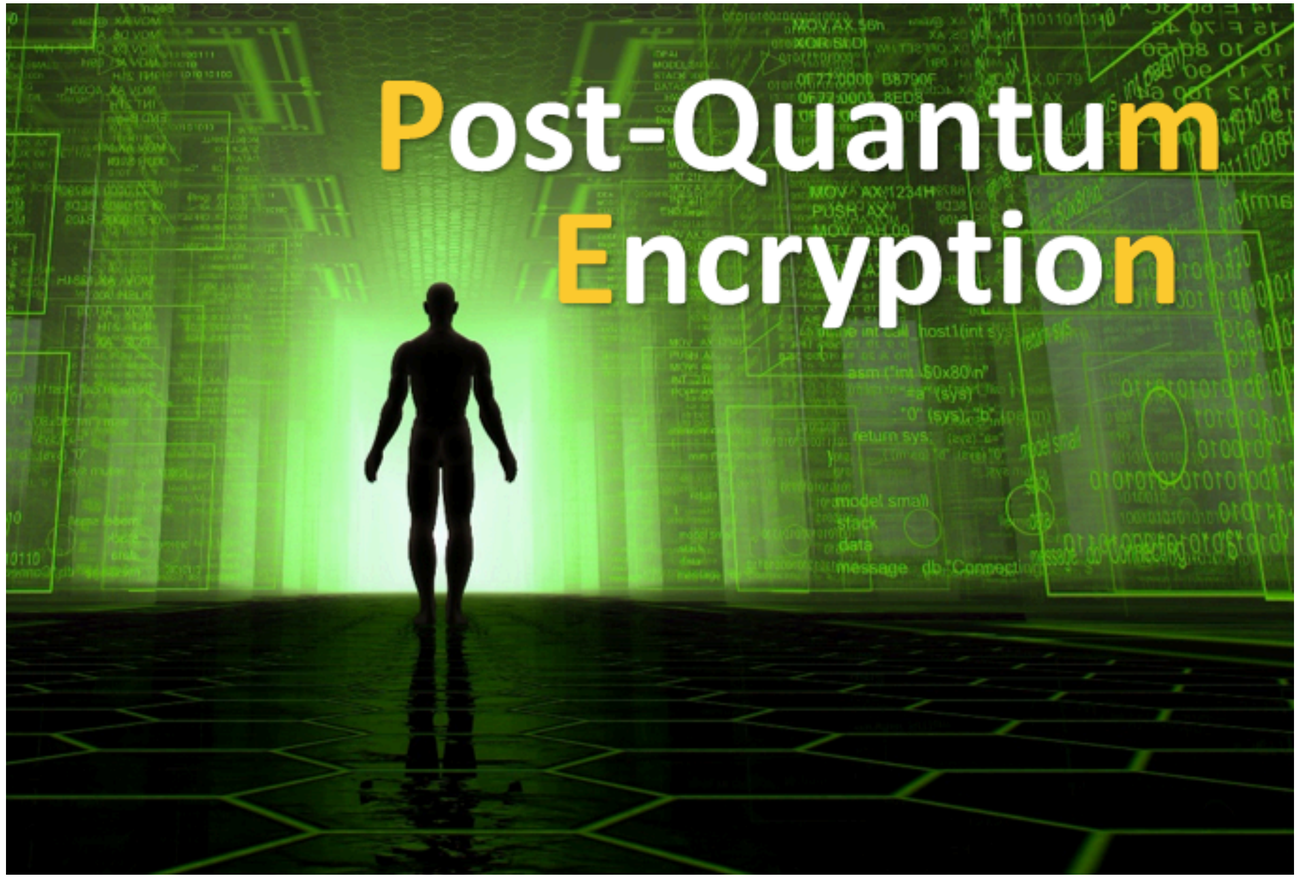
Blockchain mining security

“Decentralized lottery”:

- Proof-of-work (PoW): slightly less strong because of quantum search, but hash-based scheme essentially ok
- Proof-of-state (PoS): no crypto computations specific to PoS

BUT: both need secure digital signatures

BROKEN BY SHOR’S QUANTUM ALGORITHM


Post-Quantum
Encryption

POST-QUANTUM

≃ NOT IN BQP

⇒ RSA IS NOT P-Q

AES IS

POST-QUANTUM CRYPTO IS AN INSURANCE

(Against an unlikely event)

Risk Management

WHY CARE?

WHY CARE?

National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

Commercial National Security Algorithm Suite and Quantum Computing FAQ

WHY CARE?

Q: Given the range of algorithm options and sizes to choose from, which is best?
A: CNSS Advisory Memorandum 02-15 alerts NSS developers and operators of the need to transition to quantum resistant algorithms in the future and permits greater flexibility in algorithm choice today than was allowed under the existing CNSSP-15. This flexibility avoids making systems that do not already comply with CNSSP-15 first do an upgrade to comply with

NIST's PQ Contest

POST-QUANTUM CRYPTO PROJECT

NEWS -- August 2, 2016: The National Institute of Standards and Technology (NIST) is requesting comments on a new process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Please see the Post-Quantum Cryptography Standardization menu at left.

Fall 2016	Formal Call for Proposals
Nov 2017	Deadline for submissions
Early 2018	Workshop - Submitter's Presentations
3-5 years	Analysis Phase - NIST will report findings *1-2 workshops during this phase*
2 years later	Draft Standards ready

NIST's PQ Contest

5 MAIN FAMILIES OF PQ CRYPTO

- CODE - BASED
- HASH - BASED
- LATTICE - BASED
- MULTIVARIATE
- ISOGENY - BASED

HASH-BASED CRYPTO

ONE-TIME SIGNATURES

$K_0 \longrightarrow H(K_0)$

$K_1 \longrightarrow H(K_1)$

Secret key Public key

N keys for N bits

Keys used only once

Where is this used?

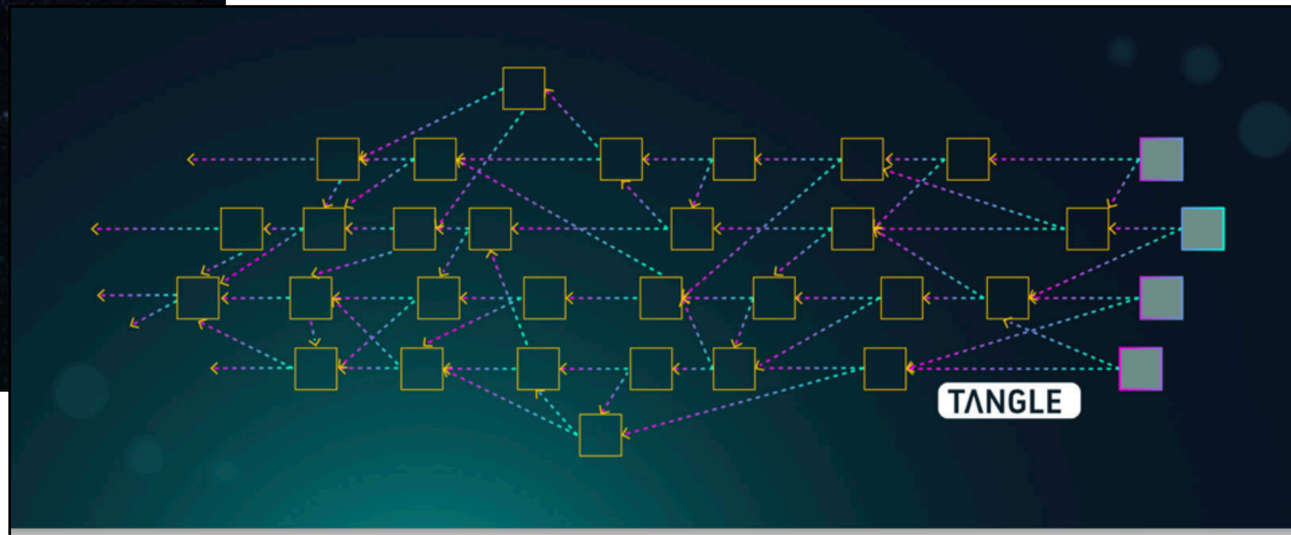
QUANTUM CYBER

BLOCKCHAIN IOT

IOTA

THE BACKBONE OF IOT IS HERE

Scalable, Decentralized, Modular, No Fees



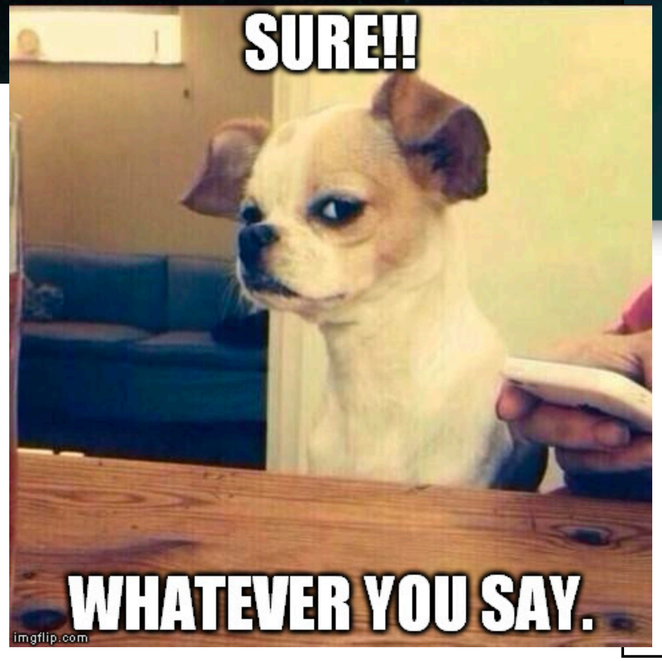
No Block / No Chain

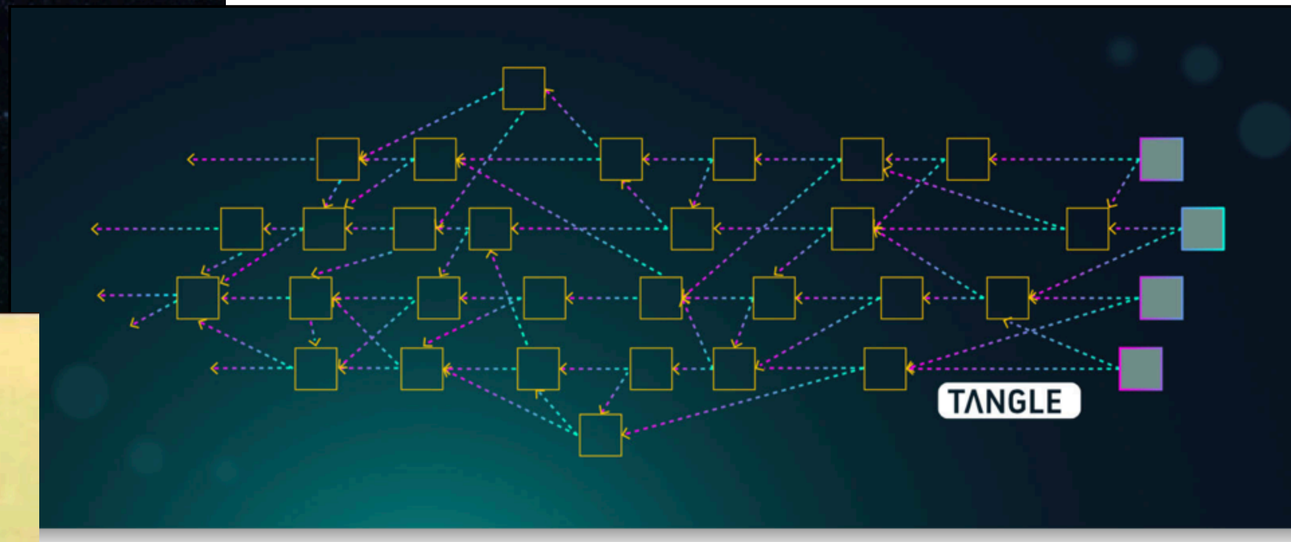
- A new Distributed Ledger Architecture
- Designed for the Internet of Things
- Novel Machine to Machine interactions

IOTA

THE BACKBONE OF IOT IS HERE

Scalable, Decentralized, Modular, No Fees





No Block / No Chain

- A new Distributed Ledger Architecture
- Designed for the Internet of Things
- Novel Machine to Machine interactions

IOTA's signature scheme

TL;DR:

- **Customer algorithm** to hash the message
- **Hash-based one-time signature** to sign the hash

IOTA's signature scheme

TL;DR:

- **Customer algorithm** to hash the message
- **Hash-based one-time signature** to sign the hash

SECURE AGAINST QUANTUM COMPUTERS

IOTA's signature scheme

TL;DR:

- **Customer algorithm** to hash the message
- **Hash-based one-time signature** to sign the hash

SECURE AGAINST QUANTUM COMPUTERS

SECURE AGAINST CLASSICAL COMPUTERS?

IOTA Vulnerability Report: Cryptanalysis of the Curl Hash Function Enabling Practical Signature Forgery Attacks on the IOTA Cryptocurrency

By Ethan Heilman (Boston University, Paragon Foundation, Commonwealth Crypto), Neha Narula (MIT Media Lab), Thaddeus Dryja (MIT Media Lab, Lightning Network Dev), Madars Virza (MIT Media Lab, Zcash)

Team contact e-mail: curl@mit.edu

Summary: We present attacks on the cryptography used in the IOTA blockchain including under certain conditions the ability to forge signatures. We have developed practical attacks on IOTA's cryptographic hash function Curl, allowing us to quickly generate short colliding messages. These collisions work even for messages of the same length. Exploiting these weaknesses in Curl, we break the EU-CMA security of the IOTA signature scheme. Finally we show that in a chosen message setting we can forge signatures of valid spending transactions (called bundles in IOTA). We present and demonstrate a practical attack (achievable in a few minutes) whereby an attacker could forge a signature on an IOTA payment, and potentially use this forged signature to steal funds from another IOTA user. This report provides example demonstrations of these vulnerabilities but does not detail the exact cryptanalytic process to generate the collisions. A later publication will provide an in-depth study of our cryptanalysis of Curl.

A cryptographic disaster, but hard to exploit realistically…

More blockchain and IoT...

Forbes

Tech / #BigData

JAN 28, 2018 @ 12:28 AM 20,367

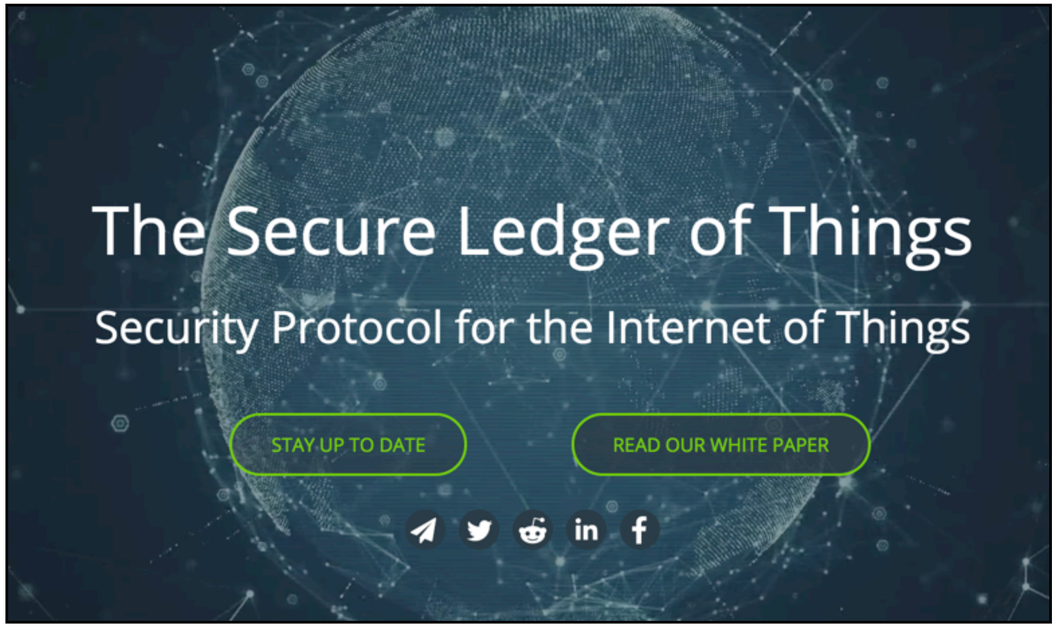
Blockchain And The Internet Of Things: 4 Important Benefits Of Combining These Two Mega Trends

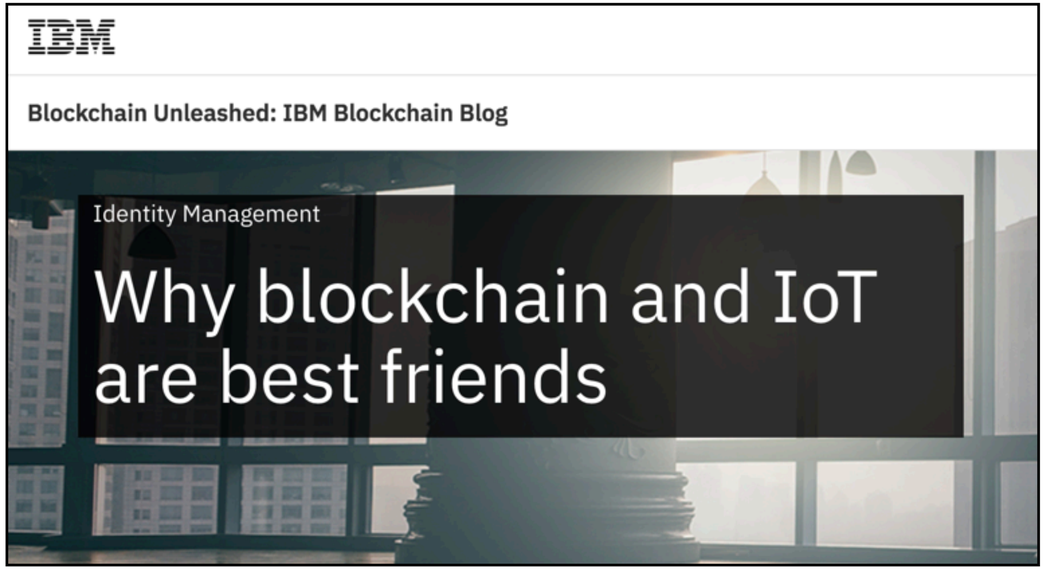
New report: The Internet of Things and blockchain tech are made for each other

IoT devices are constantly talking about themselves, and shared ledger technologies just love to record it all, permanently.

Barry Levine on January 10, 2018 at 10:00 am

More blockchain and IoT…





Forbes

Tech / #BigData

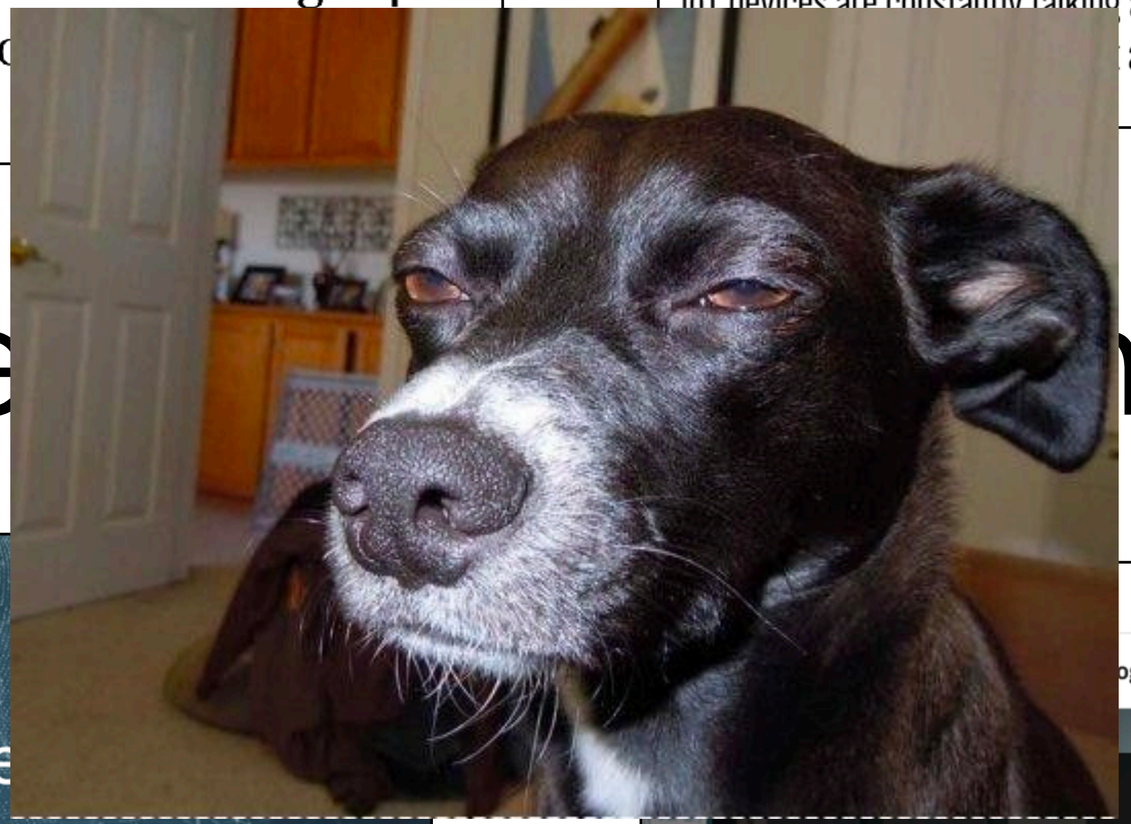
JAN 28, 2018 @ 12:28 AM 20,367

Blockchain And The Internet Of Things: 4 Important Benefits Of Co
Mega Trends

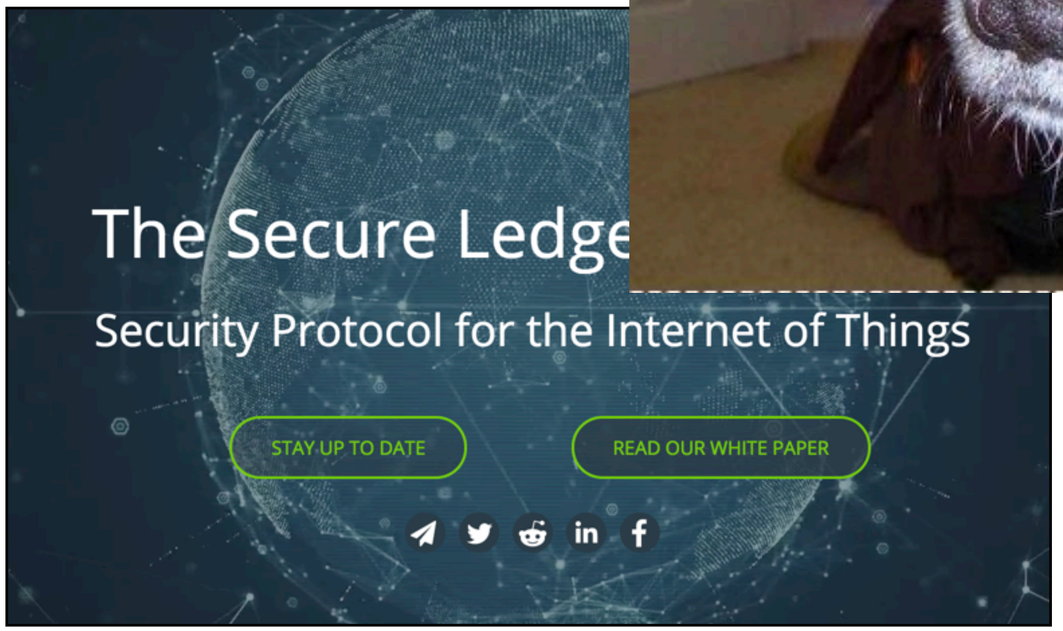
New report: The Internet of Things and blockchain tech are made for each other

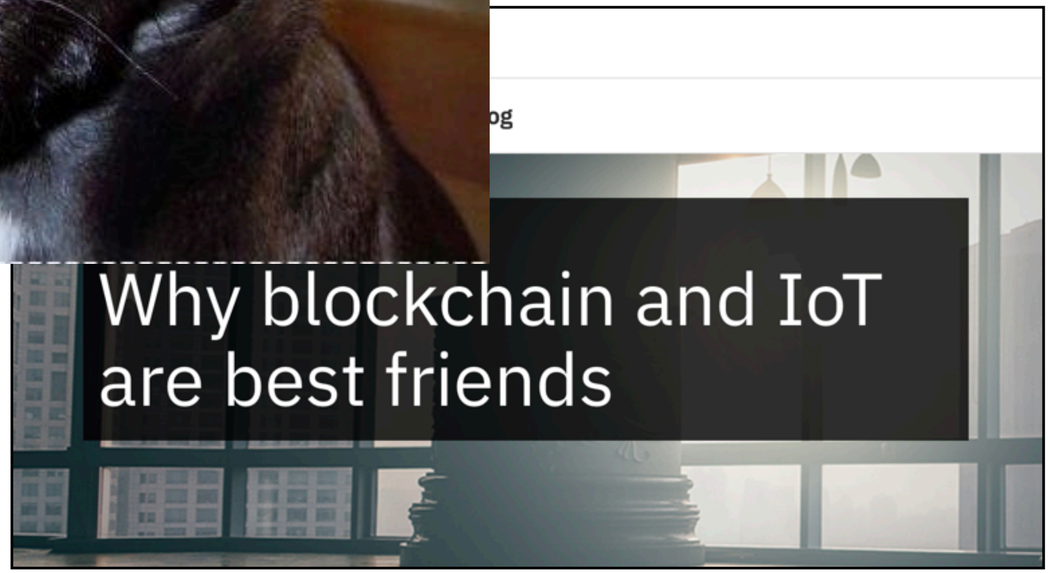
IoT devices are constantly talking about themselves, and shared ledger
all, permanently.

More



nd IoT...





What about the security of (non-IoT) blockchains?

QUANTUM CYBER

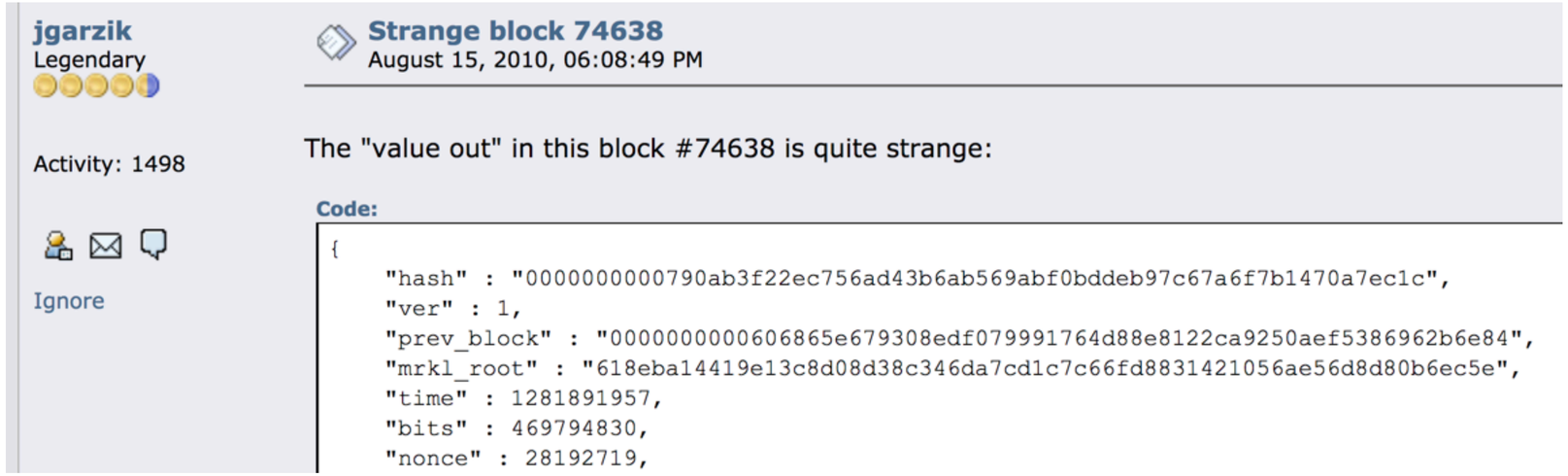
BLOCKCHAIN IOT

I did many **security audits** of blockchain applications…

Wallets, consensus protocols, crypto components, etc.

Not always as bad as imagined, but not as strong as it should be…

Bitcoin worst bug



jgarzik
Legendary

Activity: 1498

Ignore

Strange block 74638
August 15, 2010, 06:08:49 PM

The "value out" in this block #74638 is quite strange:

Code:


```
{
    "hash" : "0000000000790ab3f22ec756ad43b6ab569abf0bddeb97c67a6f7b1470a7ec1c",
    "ver" : 1,
    "prev_block" : "000000000606865e679308edf079991764d88e8122ca9250aef5386962b6e84",
    "mrkl_root" : "618eba14419e13c8d08d38c346da7cd1c7c66fd8831421056ae56d8d80b6ec5e",
    "time" : 1281891957,
    "bits" : 469794830,
    "nonce" : 28192719,
```


- The sum of a transaction's outputs overflowed the integer
- Transaction check validated the (negative) sum
- **184,467,440,737.09551616** bitcoins were created…

Bitcoin worst bug

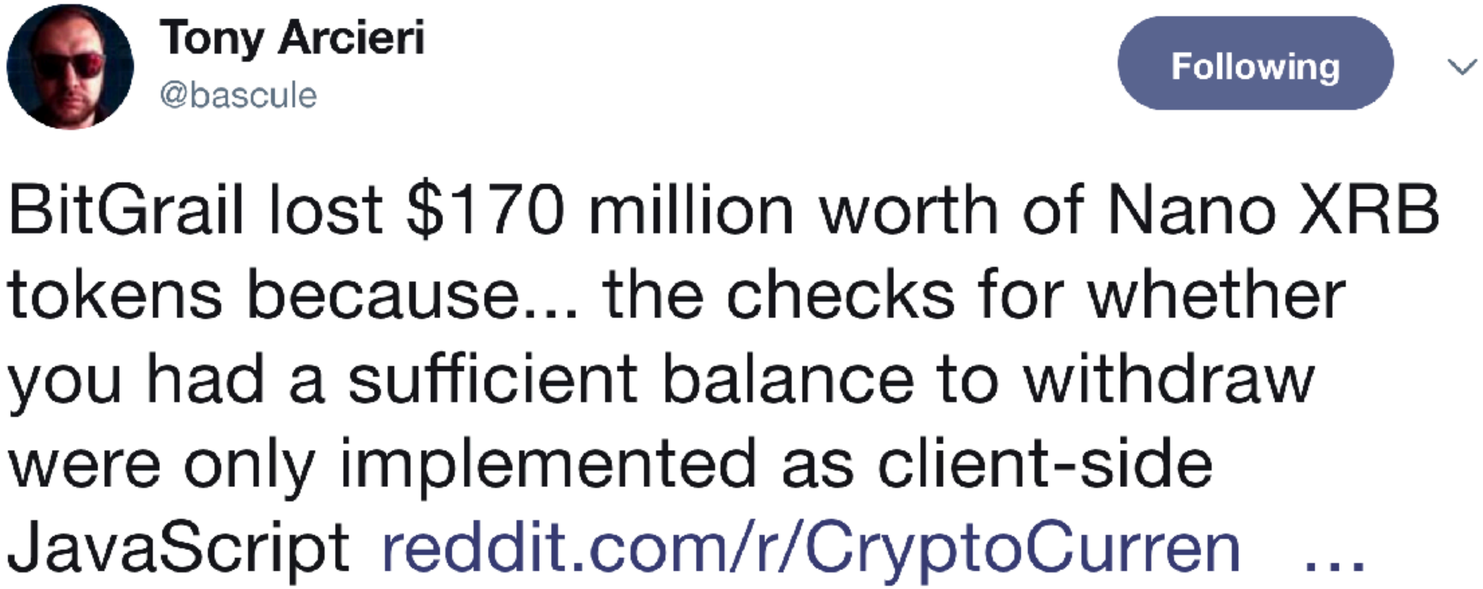
```
1009  +
1010  +            // Check for negative or overflow input values
1011  +            if (txPrev.vout[prevout.n].nValue < 0)
1012  +                return error("ConnectInputs() : txin.nValue negative");
1013  +            if (txPrev.vout[prevout.n].nValue > MAX_MONEY)
1014  +                return error("ConnectInputs() : txin.nValue too high");
1015  +            if (nValueIn > MAX_MONEY)
1016  +                return error("ConnectInputs() : txin total too high");
```

- Soft fork de facto invalidated the transaction
- Patched in 0.3.10
- CVE-2010-5139

Account hijacking (Lisk)

- Lisk ~ Ethereum with contracts in JS and PoS instead of PoW
- Addresses only 64-bit long, derived from a passphrase…
- Can steal accounts' funds by brute forcing a preimage

Client-side validation (Bitgrail)



QUANTUM CYBER

BLOCKCHAIN IOT

QUANTUM CYBER

BLOCKCHAIN IOT

MACHINE LEARNING

I CYBER

BLOCKCHAIN IOT

MACHINE LEARNING

Forbes

Tech / #IfIOnlyKnew

FEB 8, 2018 @ 09:46 PM 13,288

Blockchain, AI, Machine Learning And IOE Will Make You Money in 2018

CYBER

Samantha Radocchia Follow

Co-Founder at Chronicled // Blockchain // Forbes 30 Under 30

Oct 24, 2017 · 4 min read

Here's How IoT, Blockchain, And Machine Learning Are Working Together To Seriously Innovate Supply Chain Management

BLOCKCHA

MACHINE LEARNING

CYBER

Forbes

Tech / #IfIOnlyKnew

FEB 8, 2018 @ 09:46 PM 13,288

Blockchain, AI, Machine Learning And IOE Will Make You Money in 2018

Samantha Radocchia Follow

Co-Founder at Chronicled // Blockchain // Forbes 30 Under 30

Oct 24, 2017 · 4 min read

Here's How IoT, Blockchain, And Machine Learning Are Working Together To Seriously Innovate Supply Chain Management

March 15, 2018

BIG DATA POWERING BLOCKCHAIN WITH MACHINE LEARNING TO REVOLUTIONIZE THE TRANSPORTATION AND LOGISTICS INDUSTRY

by Matt Spillar

We're excited to announce that we'll be hosting an upcoming webinar with Trimble Inc on April 3rd!

MACHINE LEARNING

CYBER

Forbes

Tech / #IfIOnlyKnew

FEB 8, 2018 @ 09:46 PM 13,288

Blockchain, AI, Machine Learning And IOE Will Make You Money in 2018

Samantha Radocchia Follow

Co-Founder at Chronicled // Blockchain // Forbes 30 Under 30

Oct 24, 2017 · 4 min read

Here's How IoT, Blockchain, And Machine Learning Are Working Together To Seriously Innovate Supply Chain Management

March 15, 2018

BIG DATA POWERING BLOCKCHAIN WITH MACHINE LEARNING TO REVOLUTIONIZE THE TRANSPORTATION AND LOGISTICS INDUSTRY

by Matt Spillar

We're excited to announce that we'll be hosting an upcoming webinar with Trimble Inc on April 3rd!

MACHINE LE

Blockchain, AI, and Quantum Computing make for a perfect Dunkirk style 2018

Featured in

TECHNOLOGY +

“But what’s the message of your talk??”
—Philipp Jovanovic

Thank you!

Thank you!

Join my ICO! :-p
#JPcoin