# Embedded Hardware Blockchain: Towards Concrete Security Metrics

Colin O'Flynn

Dalhousie University

*coflynn@dal.ca*

September 8, 2018

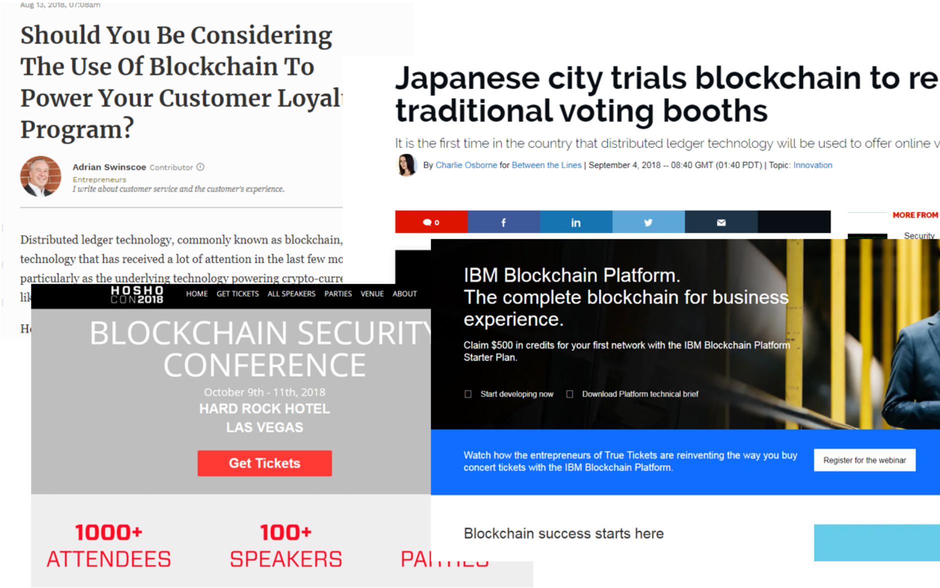
# Overview

1. Motivation

2. Hardware Blockchain Background

3. Embedded Hardware Blockchain Security

# Blockchain is Life



Aug 13, 2018, 07:08am

Should You Be Considering The Use Of Blockchain To Power Your Customer Loyal Program?

Adrian Swinscoe Contributor ⓘ
Entrepreneurs
*I write about customer service and the customer's experience.*

Distributed ledger technology, commonly known as blockchain, technology that has received a lot of attention in the last few mo particularly as the underlying technology powering crypto-curre lik

H

Japanese city trials blockchain to re traditional voting booths

It is the first time in the country that distributed ledger technology will be used to offer online v

By Charlie Osborne for Between the Lines | September 4, 2018 -- 08:40 GMT (01:40 PDT) | Topic: Innovation

BLOCKCHAIN SECURITY CONFERENCE

October 9th - 11th, 2018
HARD ROCK HOTEL
LAS VEGAS

1000+ ATTENDEES

100+ SPEAKERS

PA

IBM Blockchain Platform.
The complete blockchain for business experience.

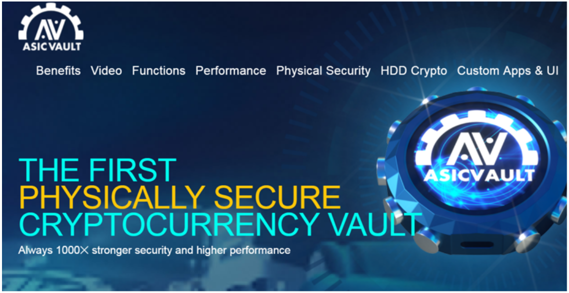
Claim $500 in credits for your first network with the IBM Blockchain Platform Starter Plan.

□ Start developing now □ Download Platform technical brief

Watch how the entrepreneurs of True Tickets are reinventing the way you buy concert tickets with the IBM Blockchain Platform.

Blockchain success starts here

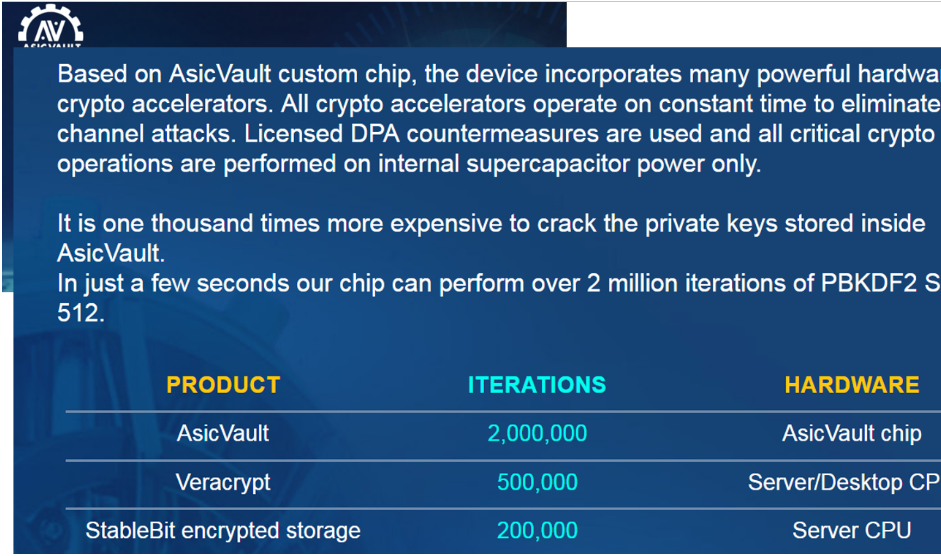
# AsicVault.io



THE FIRST
PHYSICALLY SECURE
CRYPTOCURRENCY VAULT

Always 1000X stronger security and higher performance

# AsicVault.io

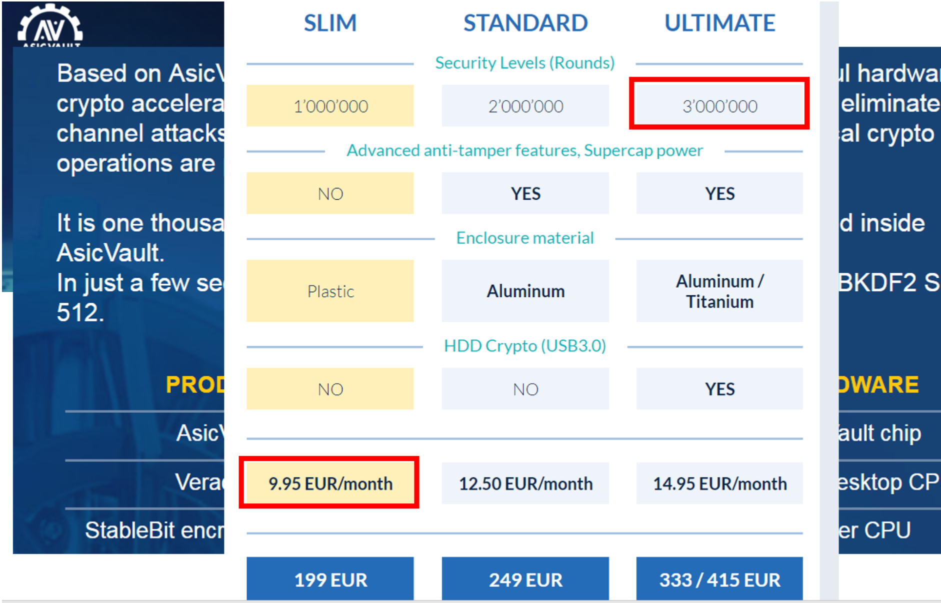


Based on AsicVault custom chip, the device incorporates many powerful hardwa crypto accelerators. All crypto accelerators operate on constant time to eliminate channel attacks. Licensed DPA countermeasures are used and all critical crypto operations are performed on internal supercapacitor power only.

It is one thousand times more expensive to crack the private keys stored inside AsicVault.
In just a few seconds our chip can perform over 2 million iterations of PBKDF2 S 512.

| PRODUCT | ITERATIONS | HARDWARE |
|---|---|---|
| AsicVault | 2,000,000 | AsicVault chip |
| Veracrypt | 500,000 | Server/Desktop CP |
| StableBit encrypted storage | 200,000 | Server CPU |

# AsicVault.io



Based on AsicV
crypto accelera
channel attacks
operations are

It is one thousa
AsicVault.
In just a few se
512.

PROD

AsicV

Verac

StableBit encr

| SLIM | STANDARD | ULTIMATE |
|---|---|---|
| Security Levels (Rounds) | | |
| 1'000'000 | 2'000'000 | 3'000'000 |
| Advanced anti-tamper features, Supercap power | | |
| NO | YES | YES |
| Enclosure material | | |
| Plastic | Aluminum | Aluminum / Titanium |
| HDD Crypto (USB3.0) | | |
| NO | NO | YES |
| 9.95 EUR/month | 12.50 EUR/month | 14.95 EUR/month |
| 199 EUR | 249 EUR | 333 / 415 EUR |

l hardwa
eliminate
al crypto

d inside

BKDF2 S

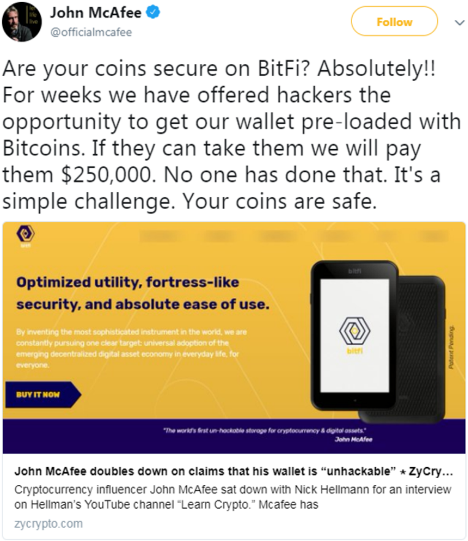
DWARE

ault chip

esktop CP

er CPU

# "Unhackable", by John McAfee

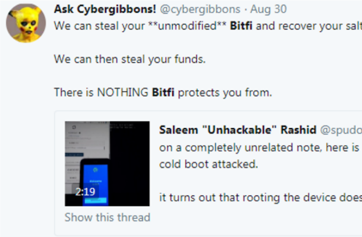


John McAfee @officialmcafee

Are your coins secure on BitFi? Absolutely!! For weeks we have offered hackers the opportunity to get our wallet pre-loaded with Bitcoins. If they can take them we will pay them $250,000. No one has done that. It's a simple challenge. Your coins are safe.

Optimized utility, fortress-like security, and absolute ease of use.
By inventing the most sophisticated instrument in the world, we are constantly pursuing one clear target: universal adoption of the emerging decentralized digital asset economy in everyday life, for everyone.
BUY IT NOW
bitfi
Patent Pending
"The world's first un-hackable storage for cryptocurrency & digital assets."
John McAfee

**John McAfee doubles down on claims that his wallet is "unhackable" ⋆ ZyCry...**
Cryptocurrency influencer John McAfee sat down with Nick Hellmann for an interview on Hellman's YouTube channel "Learn Crypto." Mcafee has
zycrypto.com



**Ask Cybergibbons!** @cybergibbons · Aug 30
We can steal your **unmodified** **Bitfi** and recover your salt

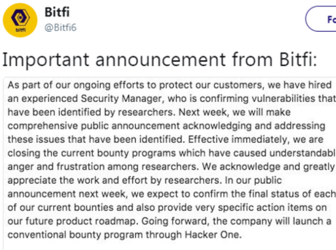
We can then steal your funds.

There is NOTHING **Bitfi** protects you from.

**Saleem "Unhackable" Rashid** @spudo
on a completely unrelated note, here is cold boot attacked.

it turns out that rooting the device does

Show this thread



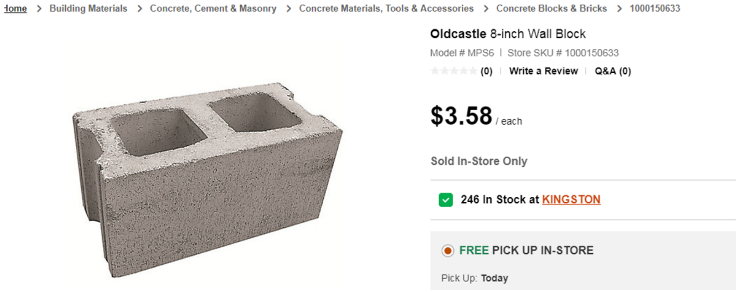
Bitfi
@Bitfi6

Important announcement from Bitfi:

As part of our ongoing efforts to protect our customers, we have hired an experienced Security Manager, who is confirming vulnerabilities that have been identified by researchers. Next week, we will make comprehensive public announcement acknowledging and addressing these issues that have been identified. Effective immediately, we are closing the current bounty programs which have caused understandabl anger and frustration among researchers. We acknowledge and greatly appreciate the work and effort by researchers. In our public announcement next week, we expect to confirm the final status of each of our current bounties and also provide very specific action items on our future product roadmap. Going forward, the company will launch a conventional bounty program through Hacker One.

# Hardware Blockchain Background

# Part 1: Block



Home > Building Materials > Concrete, Cement & Masonry > Concrete Materials, Tools & Accessories > Concrete Blocks & Bricks > 1000150633

**Oldcastle** 8-inch Wall Block

Model # MPS6 | Store SKU # 1000150633

☆☆☆☆☆ (0) | Write a Review | Q&A (0)

**$3.58** / each

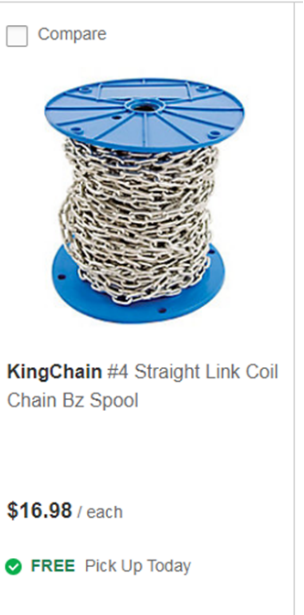
Sold In-Store Only

✓ 246 In Stock at KINGSTON

● FREE PICK UP IN-STORE

Pick Up: Today

# Part 2: Chain



□ Compare

**KingChain** #4 Straight Link Coil Chain Bz Spool

**$16.98** / each

✓ **FREE** Pick Up Today

# Blockchain 101: Example in Voting Machine Security

VOTE
Insert the Blue PEB to load a ballot for a voter.
DO NOT Confirm a vote for any voter.
**When closing the polls at 7:30 PM**

# Blockchain 101: History

- *May 11, 2008*: First concrete implementation by Homer Simpson.
- *October 31, 2008*: Satoshi Nakamoto releases computer-based version.

# Embedded Blockchain

# Embedded Blockchain: Concrete Implementation

# Blockchain Security Threats

# Existing Strength Testing

- Considerable existing body of knowledge around compressive strength of concrete masonry units (CMU).
- Chain testing in both load strength and hardness.
- Testing done in laboratory environment.

# Real-Life Considerations

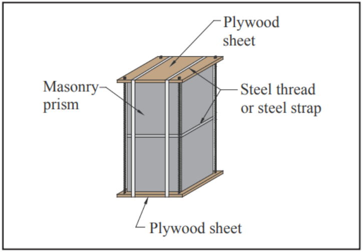


**Figure 4—Transporting Prisms**

- Attacks during transport are large risk, installed device may have been compromised in transport.
- Issues such as incorrect salt usage weaken both block & chain (concrete curing, excessive corrosion).
- New and novel attacks rarely considered in existing literature (liquid nitrogen, hammer drill, etc).

# Conclusions

## Blockchain - Builds up large body of existing work

Usage of Blockchain proposed by H. Simpson in 2008, made popular by S. Nakamoto with computer based version.

## Embedded Blockchain Security

We can use existing research on block and chain strength, which scale well to embedded sized block and chains.

## Security Threats - More Work Needed

Existing metrics poorly capture risk of threats such as in-transport attack and salt problems.