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

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

Adrian Swincoe
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 months, particularly as the underlying technology powering crypto-currencies. In its simplest form, blockchain is a way of recording and verifying transactions in a public ledger. Transactions are grouped together into blocks, which are then added to the chain of existing blocks, creating a permanent and public record of transactions.

Japanese city trials blockchain to replace traditional voting booths

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

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

IBM Blockchain Platform. The complete blockchain for business experience.

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

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

Blockchain success starts here

Colin O’Flynn (Dalhousie University)
THE FIRST PHYSICALLY SECURE CRYPTOCURRENCY VAULT
Always 1000X stronger security and higher performance
Based on AsicVault custom chip, the device incorporates many powerful hardware 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.

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th>ITERATIONS</th>
<th>HARDWARE</th>
</tr>
</thead>
<tbody>
<tr>
<td>AsicVault</td>
<td>2,000,000</td>
<td>AsicVault chip</td>
</tr>
<tr>
<td>Veracrypt</td>
<td>500,000</td>
<td>Server/Desktop CPU</td>
</tr>
<tr>
<td>StableBit encrypted storage</td>
<td>200,000</td>
<td>Server CPU</td>
</tr>
<tr>
<td></td>
<td>SLIM</td>
<td>STANDARD</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Security Levels (Rounds)</td>
<td>1’000’000</td>
<td>2’000’000</td>
</tr>
<tr>
<td>Advanced anti-tamper features, Supercap power</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>Enclosure material</td>
<td>Plastic</td>
<td>Aluminum</td>
</tr>
<tr>
<td>HDD Crypto (USB3.0)</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Price (EUR/month)</td>
<td>9.95</td>
<td>12.50</td>
</tr>
<tr>
<td>Price (EUR)</td>
<td>199</td>
<td>249</td>
</tr>
</tbody>
</table>

Based on AsicVault’s crypto accelerator, channel attacks operations are eliminated. It is one thousand AsicVault. In just a few seconds, 512.
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.

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

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 understandable anger and frustration among researchers. We 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

Oldcastle 8-inch Wall Block
Model #: MPS6 | Store SKU #: 1000150633
Rating: (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
KingChain #4 Straight Link Coil
Chain Bz Spool

$16.98 / each

FREE Pick Up Today
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

Embedded Hardware Blockchain
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

- 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).

Figure 4—Transporting Prisms
Conclusions

Blockchain - Builds up large body of existing work

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.