proceedings

MDPI

Proceedings

Design and Implementation of a Physical Bitcoin Coin †

Alberto Femenias-Hermida [1,*], Cristian R. Munteanu [1,2] and José M. Vázquez-Naya [1,2]

[1] Departamento de Computación, Facultad de Informática, Universidade da Coruña, Grupo RNASA-IMEDIR, Elviña, 15071 A Coruña, Spain; c.munteanu@udc.es (C.R.M.); jose@udc.es (J.M.V.-N.)

[2] Centro de Investigación CITIC, Universidade da Coruña, Elviña, 15071 A Coruña, Spain

[*] Correspondence: alberto.femenias@udc.es

† Presented at the 3rd XoveTIC Conference, A Coruña, Spain, 8–9 October 2020.

Published: 20 August 2020

check for updates

Abstract: One of the major factors hindering the adoption of crypto assets in general, and Bitcoin in particular, is the high level of complexity they present to the common user. Although physical coins are a possible solution, the need to place trust in the manufacturers (so that they throw away the private key) is a big drawback that has hampered their widespread use. The recent boom of the maker movement has brought in a significant number of users with access to 3D printing devices, as well as the supporting electronic and computing resources. We have taken advantage of these capabilities to develop an open source project that interested parties can use to easily print a physical model of a Bitcoin coin, along with the necessary software that allows the creation and validation of keys and addresses.

Keywords: bitcoin; open source coin; 3D printing; cryptographic asset

1. Introduction

To put it in an extremely simplified form, Bitcoin is a public ledger, stored in a single file that is shared with a p2p program, where participants keep their balances in a special form of accounts, called addresses. Each address, which is public, has an associated private key, that confers access to transfer the funds at will. The security of the funds relies in keeping the private keys safely stored and out of the reach of any malicious actor. The many instances were bitcoin owners have lost their funds [1] proves that keeping the private keys safe is a much harder problem than it may initially seem.

A possible solution is the use of a physical bitcoin, which is nothing but an artifact, whose shape and appearance resembles a traditional coin while containing in its interior the private key that gives its owner access to the associated funds. Their two main advantages are—first the use of the coin metaphor makes it very easy for regular users to visualize and identify them as money and second, their physical nature means that we can use the technologies developed over the course of centuries to keep them secure. However, a significant concern associated with physical bitcoin coins is the need to entrust the manufacturer with the disposal of the private key upon creation of each coin. That requires a big leap of faith, which has probably kept physical bitcoins from achieving a much greater level of adoption. In this paper, we present a solution that solves that problem, by allowing end users to create their own physical bitcoins without having to trust any third party.

2. Materials and Methods

We have used Github to make publicly available the results of our work, namely: (a) The software, written in Python (b) The CAD model (created with Autodesk Fusion 360) and (c) All the associated documentation, both for the process of creating the coin, as well as for its ulterior use.

The repository can be accessed at: https://github.com/albertofemenias/bertocoin.

In order to reproduce all the results of this project, the user will need:

(1) An additive 3D printer with PLA filament, such as a Prusa or similar,
(2) A good quality paper printer, such as a generic laser or inkjet printer,
(3) A transparent plastic laminate and a metallic washer.

The software and the 3D models were developed using an incremental process under the Kanban methodology. We rely on the benefits of the open source model to ensure that the design is publicly audited so that the users can trust the design is secure and free of malicious code.

3. Development

After reviewing the state of the art regarding physical bitcoins, we started the project by studying the possibilities of creating a sound design, that could be easily manufactured in an ordinary, maker class 3D printer. Of particular significance is the issue of making a functional seal. The seal is a physical mechanism of the coin with two main properties: (a) the user must manipulate it in order to gain access to the private key of the coin and (b) once the seal has been activated (typically broken) it must be obvious thereafter that the security of the coin has been compromised.

We approached an iterative design with several rounds of trial and error until we finally arrived at a design that we deemed good enough. The final design makes use of a mesh of low-caliber, parallel strands of material that the user must break to access the private key stored internally. The act of breaking the mesh and folding the flap to access the contents of the coin inflicts a permanent and easily visible damage that clearly indicates that the private key has been revealed.

4. Results

Special attention was given to make the software as user-friendly as possible. As a result, it consists of a single Python script that, when run, generates the keys in a secure manner and produces automatically a printable document (in the open source .SVG format) that the user can print using an internet browser. This document (see Figure 1) contains both the private and the public key, and it is designed so that it can be easily cut out and folded, before placing it inside the coin.

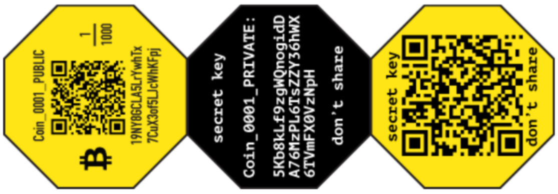

Figure 1. Template with private and public keys.

As for the physical side of the coin, most of the effort was placed on three critical aspects—(a) Making the coin easily recognizable as such. This required finding an appropriate shape, look, weight and size; (b) Designing a workable seal, that makes pretty evident the fact that it has been broken to allow access to the secret key; and c) Guaranteeing the secret is not accessible without breaking the seal. This was ensured in good part by inserting a metallic washer inside the coin that makes the coin 100% opaque. In Figure 2, we can see various aspects of the design and manufacturing of the coin.

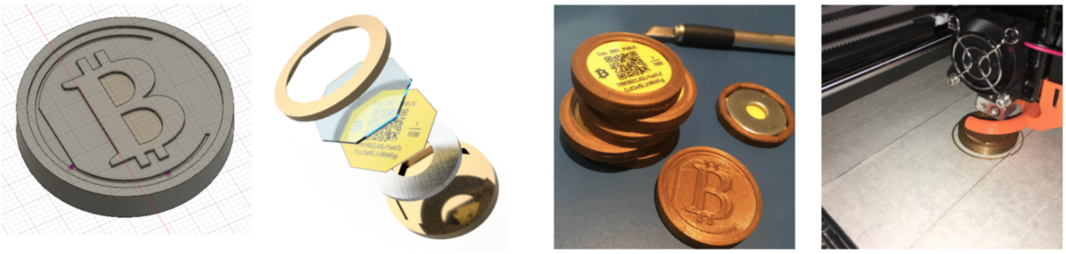

Figure 2. Design and manufacturing of the coin.

5. Discussion and Conclusions

We have created a workable solution to handle bitcoin funds as a coin. The design will surely benefit from public scrutiny, once enough qualified people analyze the code published in the Github repository.

It is critical that the users of these coins understand two key aspects of their security: (a) They must be produced in a non-compromised computer to ensure a fair private key is generated and (b) Upon manufacturing, the coins must be physically kept out of reach of anybody but the legitimate user, since they are essentially 'bearer assets' which means that whoever is in possession of them can access the associated bitcoin funds.

6. Future Work

Upon finishing and testing the design, we identified a line of work for the future that involves embedding electronics within the coin, to improve some of its characteristics. Most notably the incorporation of computing and I/O capabilities in the coin will make it interactive, enabling non-destructive verification of the private key, by building upon the cryptographical properties of the ECC to sign a message with the private key.

Author Contributions: Conceptualization, A.F.-H.; Methodology, A.F.-H., C.R.M. and J.M.V.-N.; Software, A.F.-H.; Investigation, A.F.-H., C.R.M. and J.M.V.-N.; Resources, C.R.M. and J.M.V.-N.; Writing—original draft preparation, A.F.-H.; Writing—review and editing, A.F.-H., C.R.M. and J.M.V.-N.; Supervision, C.R.M. and J.M.V.-N. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Consolidation and Structuring of Competitive Research Units—Competitive Reference Groups (ED431C 2018/49), funded by the Ministry of Education, University and Vocational Training of the Xunta de Galicia endowed with EU FEDER funds.

Conflicts of Interest: The authors declare no conflict of interest.

Reference

1. Eriksson, N. 10 Dramatic Stories of People Who Lost Their Bitcoin Private Keys. *Coinnounce*. Available online: https://coinnounce.com/10-dramatic-stories-of-people-who-lost-their-bitcoin-private-keys/ (accessed on 22 July 2020).