Technical Analysis of bitcoin.com contracts between Roger Ver and OKCoin

by J. Maurice

Background

I am a freelance IT security consultant in Tokyo, having prior experience performing various forensic investigations into hacking, cryptographic, and other IT security incidents. I was asked to perform a technical/forensic analysis of the digital contracts between Roger Ver and OKCoin regarding the management agreement of the bitcoin.com domain name, and these are my findings and conclusions.

Analysis

The following documents were presented to me for cryptographic analysis:

1) “Bitcoin.com_v7 (final) (Signed).pdf” (MD5: 4e4e5cd9c2b62bbbf9b62580f561f19c)

   This is a simple 2-page mostly text PDF document composed in TextEdit, with an image of Roger Ver’s hand-written signature at the bottom. The file contains a cryptographic signature created by Adobe Acrobat, the hand-written signature is timestamped “2014.12.15 10:34:43 -04’00’” and the PDF Metadata also shows a last modified timestamp of the same exact timestamp.

   The cryptographic signature was verified to be valid using freely available PDF software and Roger Ver’s PDF certificate at https://www.rogerver.com/CertExchangeRogerVer.fdf -- the SHA1 fingerprint of this certificate is “F1FC552BF7579A8D33519DFDB6848C4FFB54D645”.

   I have confirmed in-person that the above-named PDF signing certificate does in-fact belong to Roger Ver, and I have observed other PDF documents signed by Roger Ver with this same key in the same way.

2) “Decrypted GPG signed contract from CZ.txt” (MD5: 248a7eaa0daae2b6eb0ef8aa16da953c)

   This file contains the decrypted multipart/x-mimegpg content of a GPG email from Changpeng Zhao at OKCoin to Roger Ver. The file contains a cryptographic signature created by GPGTools, and the timestamp of the GPG signature is Tue 16 Dec 2014 12:31:17 AM JST (approximately 1 hour after Roger’s signed timestamp, after calculating time zone difference). The PDF Metadata shows a timestamp of 2014/12/16 00:28:36.

   The cryptographic signature was verified to be valid using freely available “mimegpg” utility from sqwebmail, freely available GNU GPG software, and the GPG public key for Changpeng Zhao <cz@okcoin.com> available for download from public GPG keyservers with fingerprint 2B96 B48E 93A8 C5B9 0F82 7FD1 C30C DAD2 062D D960.

   I have confirmed in-person that the above-named GPG signing key does in-fact belong to Changpeng Zhao, and I have observed other emails signed by CZ with this same key in the same way.

3) “Bitcoin.com_v7 (final) (counter-signed).pdf” (MD5: b8f69d5b85acb1ecd0a015e31f5044ca)

This file is the PDF document attachment extracted from the email content of Document #2 above. The contents of this PDF document are identical to the contents of Document #1, except this PDF has an image of Changpeng Zhao's hand-written signature added.

This document was digitally signed by Changpeng Zhao as part of Document #2 from which it was extracted.

4) "Bitcoin.com_v8.pdf" (MD5: 5debc6a50d54cb75a41e39da8b6bea5d)

This is a PDF document almost identical to document #1, but with an additional provision added at the bottom of the contract: "OKCoin may cancel the contract by givin Roger 6 months advanced notice." The word "givin" is incorrectly spelled in this provision.

There are no cryptographic signatures present in the document, from what I can find. The hand-written signature is timestamped "2014.12.15 10:34:43 -04'00'" in this document, exactly the same as Document #1, down to the same minute and second.

5) "5175722026199499148.jpg" (MD5: aa91019dfde7b23e183134b696149f4e)

This is a JPEG image, with EXIF data indicating it was modified using "Photoshop 3.0" - the JPEG is a photo of the last page of Document #4, printed out, with a hand-drawn signature added under OKCoin's signature line.

Findings

Judging from the various metadata, email headers, and digitally signed timestamps, the following timeline of events can be inferred from the analysis of Documents #1, #2, and #3:

2014/12/15 23:33:49
Roger exports the PDF from his TextEdit application (Document #1)
2014/12/15 23:34:43
Roger digitally signs Document #1 using Adobe Acrobat X, emails to CZ
2014/12/16 00:28:36
CZ adds his hand-drawn signature to Document #1 using RunePDF, creating Document #3
2014/12/16 00:31:17
CZ sends a GPG signed email (Document #2) to Roger, with Document #3 attached

Unlike the other documents, Documents #4 and #5 contain no cryptographic signatures or other evidence of discussion or agreement between the parties, so they do not seem to fit into this timeline of events. Moreover, the timestamp of Roger's hand-written signature in Document #3 is identical to the one in Document #1, so either he signed both of them within 1 second, or one of them is a forgery.

Conclusions

The contract documents are identical in substance, except for the additional provision added in Documents #4 and #5.

The strong cryptographic evidence, counter-signed by both parties, as well as the corresponding timestamps, makes it clear that the signed contents of Documents #1 and #3 were indeed agreed to by both parties.

However, because of the identical timestamps in the hand-drawn signature images, I can conclude that Document #4 was produced by someone who copied Document #1 after Roger signed it, and modified the PDF to contain the additional provision allowing OKCoin to cancel the contract after “givin” 6 months notice to Roger. The hand-signed Document #5 cannot be verified, as there are no cryptographic signatures present.

There was no evidence presented that indicates either party discussed or agreed to the additional provision in Documents #4 and #5, and strong cryptographic evidence to the contrary, proving that the parties agreed to the contract terms in Document #1 that did not contain this provision.