The complete

Bitcoin Thief Tutorial

SESSION ID: HTA-R02

Uri Rivner
Head of Cyber Strategy
BioCatch

Etay Maor
PMM Cyber
Trusteer, an IBM Company
The first few things you should know about Bitcoin…

Most people think of Bitcoin in terms of a crazy digital currency whose dollar value has been soaring in recent months.

The only question they have is: should I buy some?

*Let me show you a totally different perspective.*
The first few things you should know about Bitcoin…

Bitcoin is a payment scheme for transferring money:
• To anyone in the world
• In their own currency
• Instantly
• with virtually no commission.

Example: a $50 money transfer to my pal in Hong Kong
The first few things you should know about Bitcoin…

Using Paypal : Owning Paypal
= 
Using Bitcoin : Owning Bitcoin
The first few things you should know about Bitcoin…

Bitcoin works exactly the same whether it’s worth like this:

Bar of Gold

Or like this:

Bar of Soap

You don’t trade in Bitcoins. You trade in bits of Bitcoin. Minimal trade value = Satoshi = 0.00000001 Bitcoin
Remind me…
What is Bitcoin?

Crypto Currency
Vires in Numeris
12m / 21m
Cryptography Mailing List, 2008
Satoshi Nakamoto
Owing a Bitcoin

A bitcoin is just a string of zeroes and ones. So, to steal a Bitcoin, all you need is just to copy them.

Hah! You fell for that one, didn’t you?

The ownership and trade of Bitcoin is one of the most amazing aspects about the protocol. The more you learn about how it’s done, the more you’d think it’s beautiful. As a fraudster you might not care about that, but you should definitely understand the principal of ownership and trade. And no, don’t look for strings of zeroes and ones that you can copy. It’s a bit more complicated than that. Don’t worry, you CAN steal Bitcoins, but it’s not a simple matter of copy and paste.
Step #1: Get a Wallet. It’s free!

In order to own bitcoins, you need a wallet. You have two choices: either

- **Download a Bitcoin wallet** (might take you a while; currently the download is around 15 GB). Or,
- **Subscribe to an eWallet service**.

Once you have a wallet, you also get your Bitcoin address. It’s free and you can get multiple ones. Here’s mine: 1HrxLKBU6xVnwSdqgTjnWs3H3ULDxvaXTG

Essentially it’s your public key.
You don’t have to hide it. The private keys – hell ya!
Lets see a Wallet in action

For your security, please activate at least one MFA Security Device.

CoinJar proactively encourages our customers to be more security-conscious. As your CoinJar balance has exceeded safety threshold, we request you to set up Multi-Factor Authentication to reduce the risk of theft.

Set up MFA Security Devices

This message will disappear once you have taken the required action to protect your account.

Available Balance: $1,000.00
Unconfirmed Balance: $0.00
Incoming Today: $0.00
Outgoing Today: $0.00
Step #2: Getting Bitcoins!

What’s the best way to fill your wallet with Bitcoins?

A. Directly buy Bitcoins from another user
B. Use a local or global Bitcoin exchange
C. Mine bitcoins (more on this later)
D. Steal some bitcoins!
Careful with that QR Code!!
OK – I now own Bitcoins. How can I transact?

Ah. Transacting in Bitcoin is the most fascinating aspect of the crypto currency. There are SO many moving parts!
Validation is Key  (pun intended)

The Bitcoin protocol makes sure that when I send you any Bitcoins, they really were in my possession – i.e. my digital wallet – to begin with, and that I haven’t spent them already. Otherwise I can send the same Bitcoin to several people, and get away with it.

Had Bitcoin been a stock...
But it’s not. So - Who validates Bitcoin transactions?

- The Secret Bitcoin Society  (Nobel Laureates? Famous cryptographers? The Pope?)
- We all are  (and that’s the beauty of it)
Validation by the Masses

Based on Proof of Work principal:
• Make it difficult, but –
• Reward those who go through the trouble

There’s another name for it. Bitcoin Mining.
How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

**WALLETS AND ADDRESSES**

Bob and Alice both have Bitcoin "wallets" on their computers.

Wallets are bags that provide access to multiple Bitcoin addresses.

**Creating a New Address**

Bob creates a new Bitcoin address for Alice to send her payment to.

**Submitting a Payment**

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to this address.

**Public Key Cryptography 101**

When Bob creates a new Bitcoin address, what he's really doing is generating a "cryptographic key pair"—a private key and a public key. If you sign a message with a private key, only someone who knows that private key can verify that the signature is authentic. It is impossible for someone to determine which messages are signed.

**Verifying the Transaction**

Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs the transaction request with the private key of the address she's transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

**Transaction Verified**

As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different sequence of steps, and then redo the work of all the other subsequent miners. Such a feat is nearly impossible.

**Cryptographic Hashes**

A cryptographic hash function takes a block of data and returns a fixed length string called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to extract which initial data set will create a specific hash value.

**Nonces**

To create a different hash value from the same data, Bitcoin uses "nonces." A nonce is just a random number that is added to data prior to hashing. Changing the nonce results in a wildly different hash value.

**The Proof of Work**

Each block includes a "nailbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet, but because it's newly minted bitcoins, it has no value with the required number of leading zeros. So it's failed to generate the required hashes, but what's important is that it's one less hash that needs to be computed and verified by the network.
Follow the yellow brick blockchain

1HrxLKBU6xVnwSdqgTjnWs3H3ULDxvaXTG
Bitcoin Charts

Market Capitalization
Source: blockchain.info

Blockchain Size
Source: blockchain.info

Hash Rate
Source: blockchain.info
Bitcoin: Top B2C Opportunities

- Trojan trigger lists – with popular Bitcoin exchanges
- Phishing for Bitcoin credentials
- RATs for direct wallet access
- Rogue Bitcoin apps
- Using botnets to mine bitcoin: small change…
  - Regular PC with i5 core: 10 MH/S
  - Mid-sized botnet: 5,000 PCs => 50 GH/S => $280/month
Bitcoin: Top B2B Opportunities

- Bitcoin exchanges: sitting ducks!
- Bitcoin mining operations!!
- 51% Attack!!!
- NSA!!!!
A few more interesting things

Signed in successfully.

For your security, please activate at least one MFA Security Device.

CoinJar proactively encourages our customers to be more security-conscious. As your CoinJar balance has exceeded safety threshold, we request you to set up Multi-Factor Authentication to reduce the risk of theft.

Set up MFA Security Devices

This message will disappear once you have taken the required action to protect your account.

Available Balance: $1.0000
Unconfirmed Balance: $0.0000
Incoming Today: $0.0000
Outgoing Today: $0.0000
The Cybercriminal’s Dilemma

A Target? An infrastructure and facilitator?

CATS: ALL YOUR BITCOIN ARE BELONG TO US.
Facilitator for Shady Deals

CannabisUK

Purple Kush

Drivers Licenses

Product | Price | Quantity
---|---|---
20g Purple Kush | 160 EUR | 1
50g Purple Kush | 350 EUR | 1
100g Purple Kush | 650 GBP | 1
Norway Drivers License | 1150 EUR = 2.120 $ | 1

Walther PPK, Kal. 7.65
Ammo, 50 Rounds

40 EUR = 0.074 $
Is Bitcoin Truly Anonymous?

Bitcoin Fog: Secure Bitcoin Anonymization

Bitcoin is not 100% anonymous, we are providing a solution for this: using our service you mix up your bitcoins in our own pool with other users' bitcoins, and get paid back to other accounts from our mixed pool, which, if properly done by you can eliminate any chance of finding your payments and making it impossible to prove any connection between a deposit and a withdraw inside our service.

Login

Username: [blank]
Password: [blank]
Criminal Discussions

◆ What people care about:
  ◆ Discussions around crypto currency
  ◆ Extra fogging
  ◆ Conversation rate
  ◆ Currency volatility
Explaining the News

Bitcoin exchange CEO arrested for money laundering
By Jose Pagliery @Jose_Pagliery January 28, 2014: 10:16 AM ET

Yahoo malware turned PCs into Bitcoin miners
Malicious ads served to Yahoo users were designed to transform computers into a Bitcoin mining operation, according to a security firm.
by Lance Whitney | January 9, 2014 8:25 AM PST
## Bitcoin Mistakes (?)

### Transaction
View information about a bitcoin transaction

<table>
<thead>
<tr>
<th>Summary</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>341 (bytes)</td>
</tr>
<tr>
<td>Received Time</td>
<td>2013-09-17 21:20:13</td>
</tr>
<tr>
<td>Included In Blocks</td>
<td>258546 (2013-09-17 21:23:26 +3 minutes)</td>
</tr>
<tr>
<td>Confirmations</td>
<td>7193 Confirmations</td>
</tr>
</tbody>
</table>

### Inputs and Outputs

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Input</td>
<td>80.99252199 BTC</td>
</tr>
<tr>
<td>Total Output</td>
<td>0.01252199 BTC</td>
</tr>
<tr>
<td>Fees</td>
<td>80.98 BTC</td>
</tr>
<tr>
<td>Estimated BTC Transacted</td>
<td>0 BTC</td>
</tr>
</tbody>
</table>

---

Transaction ID: 258478e8b7a3b78301661e78b4f93a792af878b545442498065ab272eaacfc035

Sender: 1LtjWsKsr2RweDLAmv75oGL7tjVF4wx7W
Recipient: 1CfsAiYaVfk12dnZpZALcRSP9jjWDk26FX

0.01252199 BTC

---
And now… for the LIVE DEMONSTRATION!!!

- This section includes a 20-min demonstration:
  - Logging into Bitcoin exchange account
  - Trojan configuration for the exchange
  - Credentials theft from infected device
  - Unauthorized entry and transferring Bitcoins to fraudster address
  - Confirmation in the blockchain
  - Removing traces
Summary: what have we learned?

- Bitcoin is a New Frontier:
  - Huge opportunity for Phishing and Trojan attacks
  - Exchanges are sitting ducks – hit them first!
  - Don’t bother with Bitcoin botnets
  - eWallets more lucrative than PC wallets
  - Try it at home – it’s fun!
QUESTIONS?

Etay.Maor@Trusteer.com
Uri.Rivner@BioCatch.com

Best use LinkedIn!