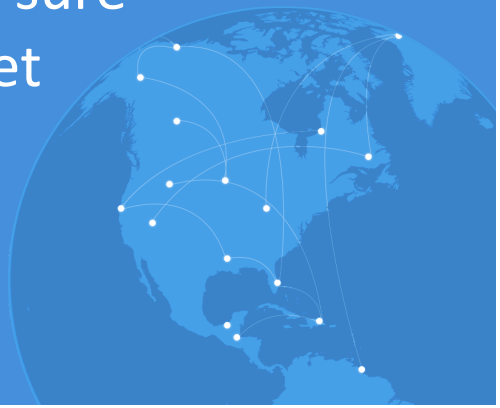
How to Verify a Bitcoin Wallet Address

Introducing Alice and Bob

- Alice and Bob are business partners
- Alice wants to pay Bob via Bitcoin
- Both are familiar with the use of Bitcoin
- However, because Bitcoin transactions are irreversible both are cautious and wish to make sure that the Bitcoin is being sent to the proper wallet address



Goals of the Process

1. Confirm that both Alice and Bob know each others wallet addresses
2. Securely associate an a contact method to to each of their wallet addresses
3. Ensure that they both are able to successfully use the wallets in question

Two Different Ways to Accomplish these Goals

Micro-Transaction to Bob

1. Alice sends Bob a small amount of Bitcoin
2. Alice sends a request for the exact same amount back
3. Bob responds to the request and sends Alice her Bitcoin back
4. Alice finally calls Bob personally to confirm that it was him who sent her back the Bitcoin

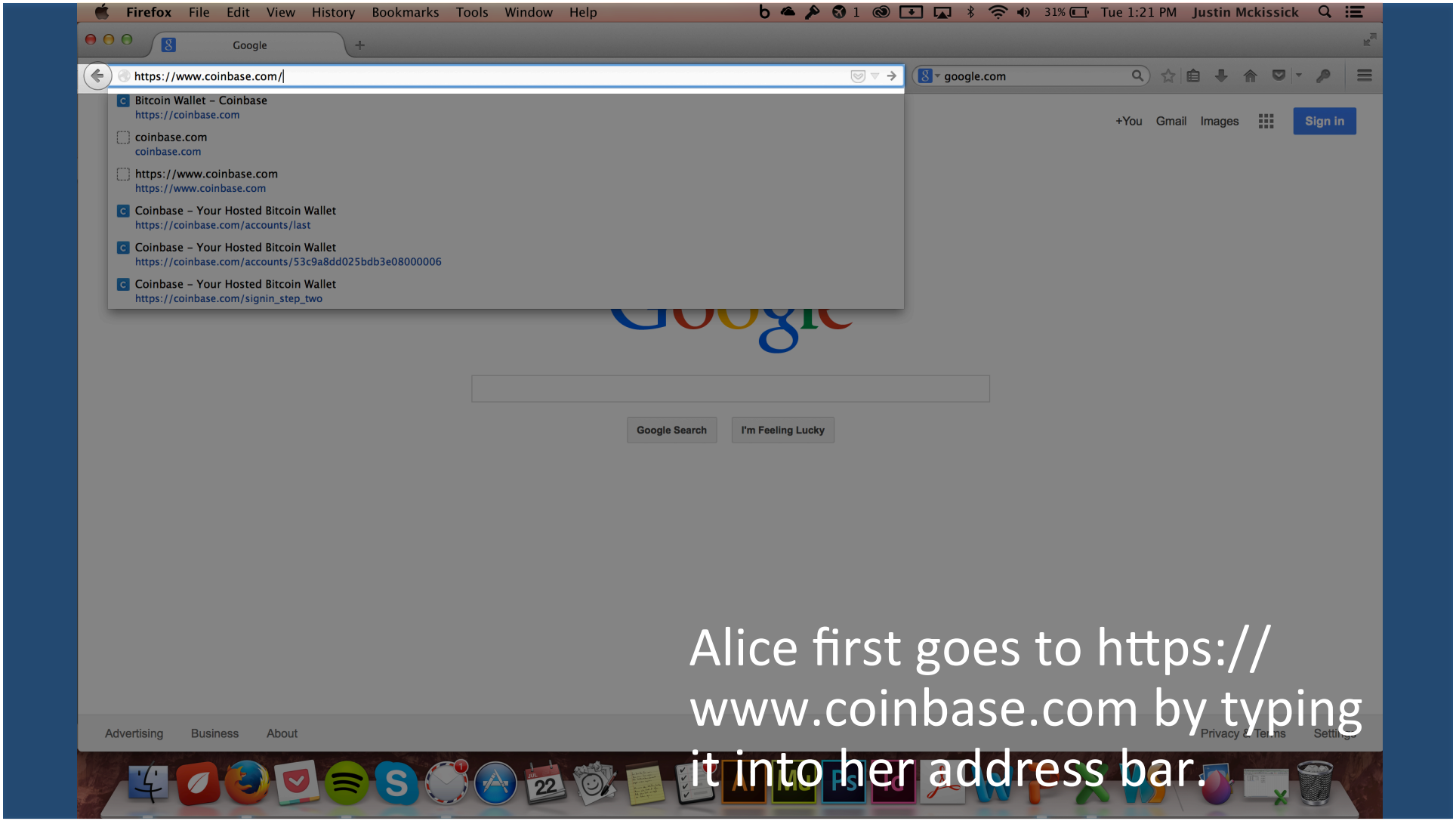
Signed Message from Bob

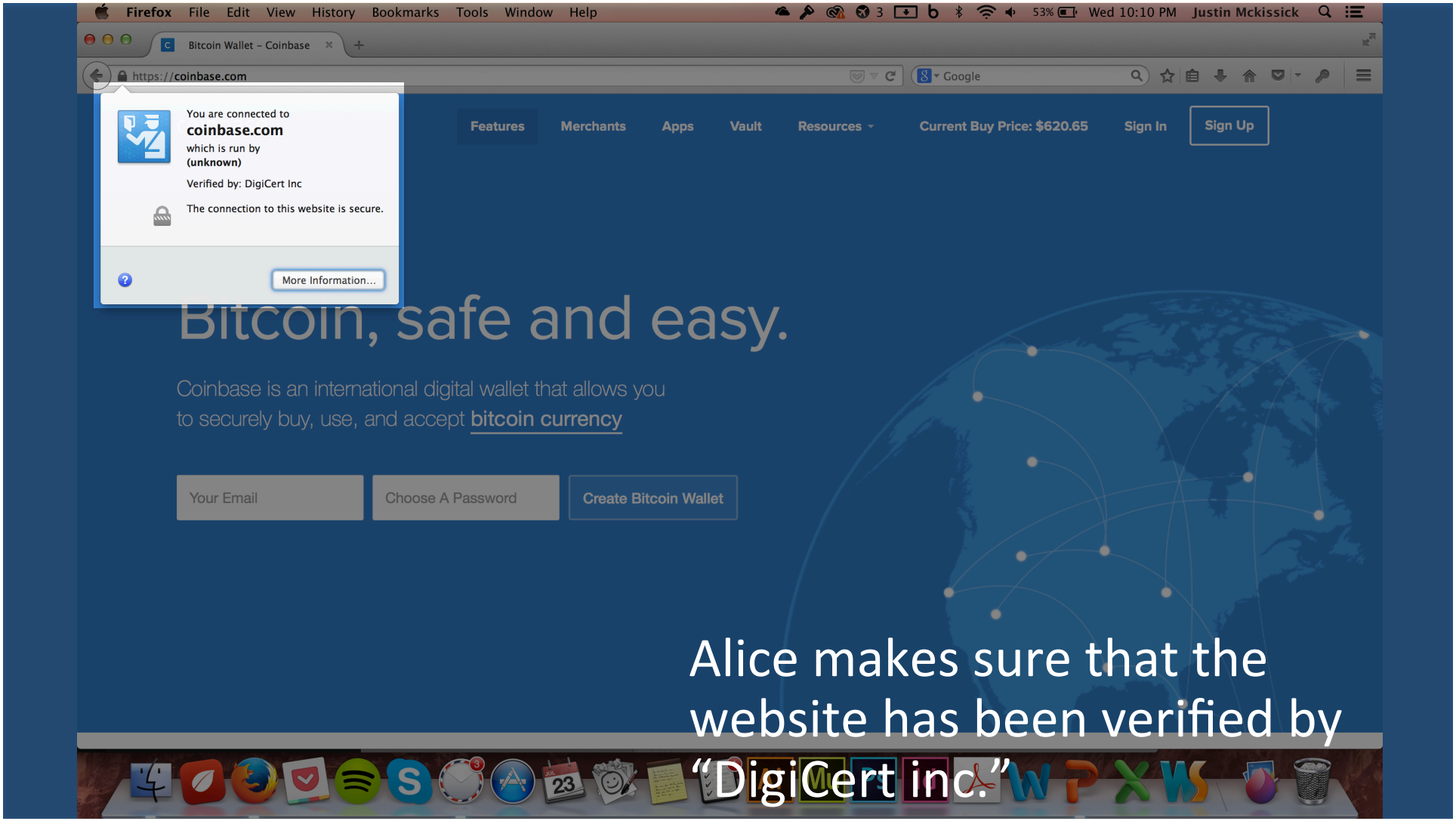
1. Alice sends Bob a email signed with her wallet private key containing her with her email
2. Bob repeats the process with a message sending the same information to Alice
3. They use these signed messages for verification of the addresses to be used

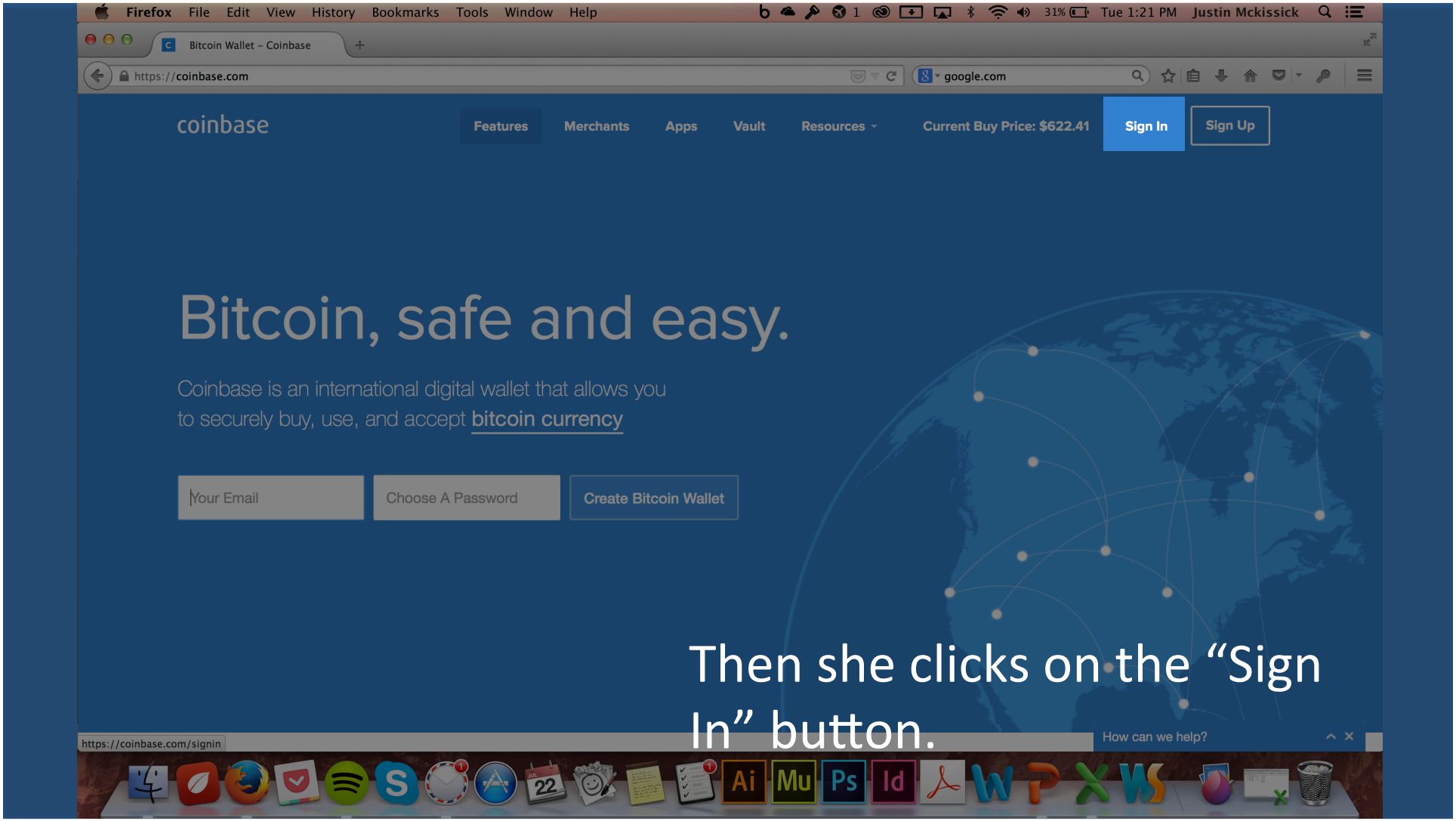
1

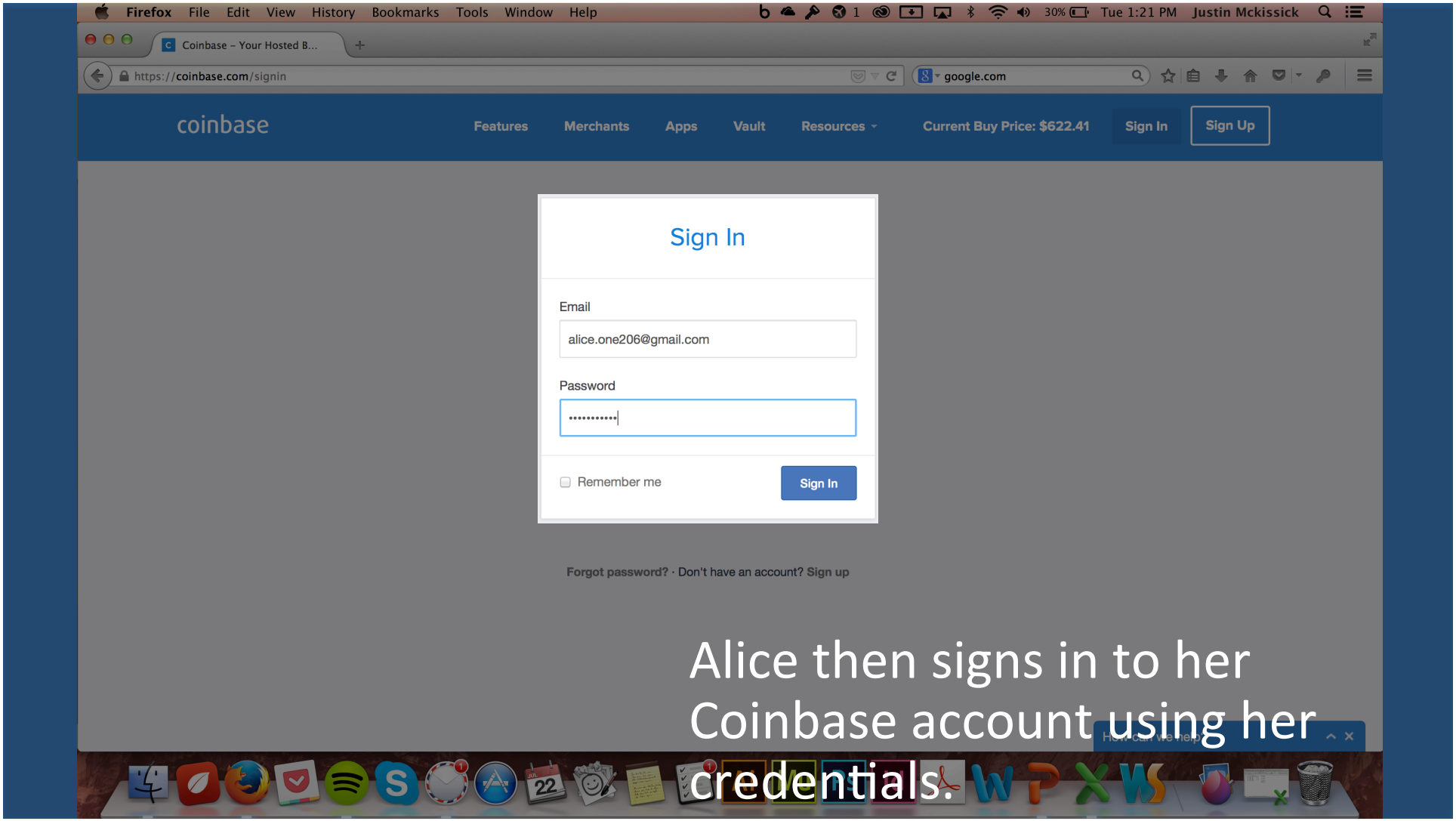
Verifying Addresses via Micro-Transactions

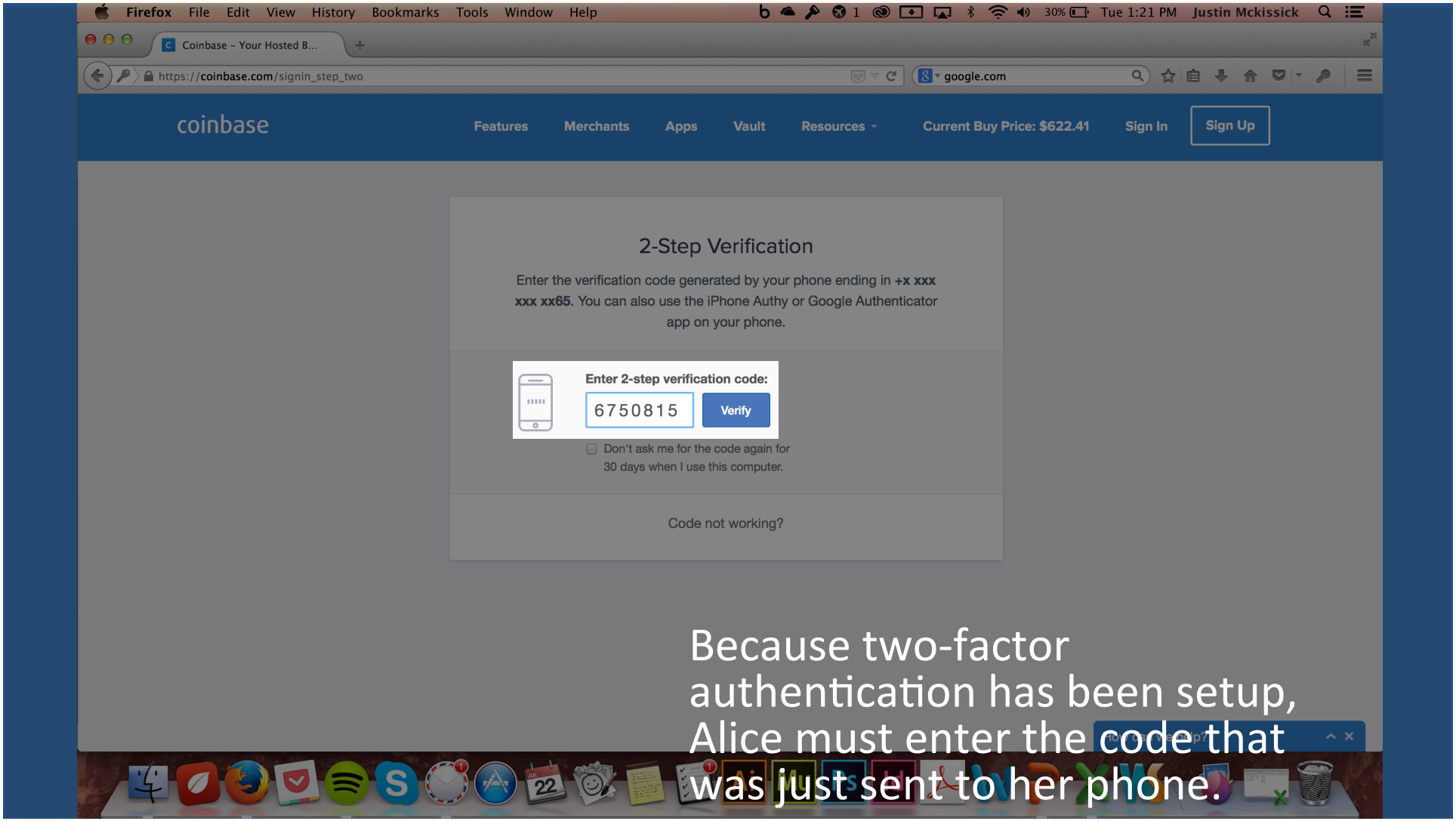
Alice sends Bob a small amount of Bitcoin and then requests it back. Bob responds by sending her the original amount.

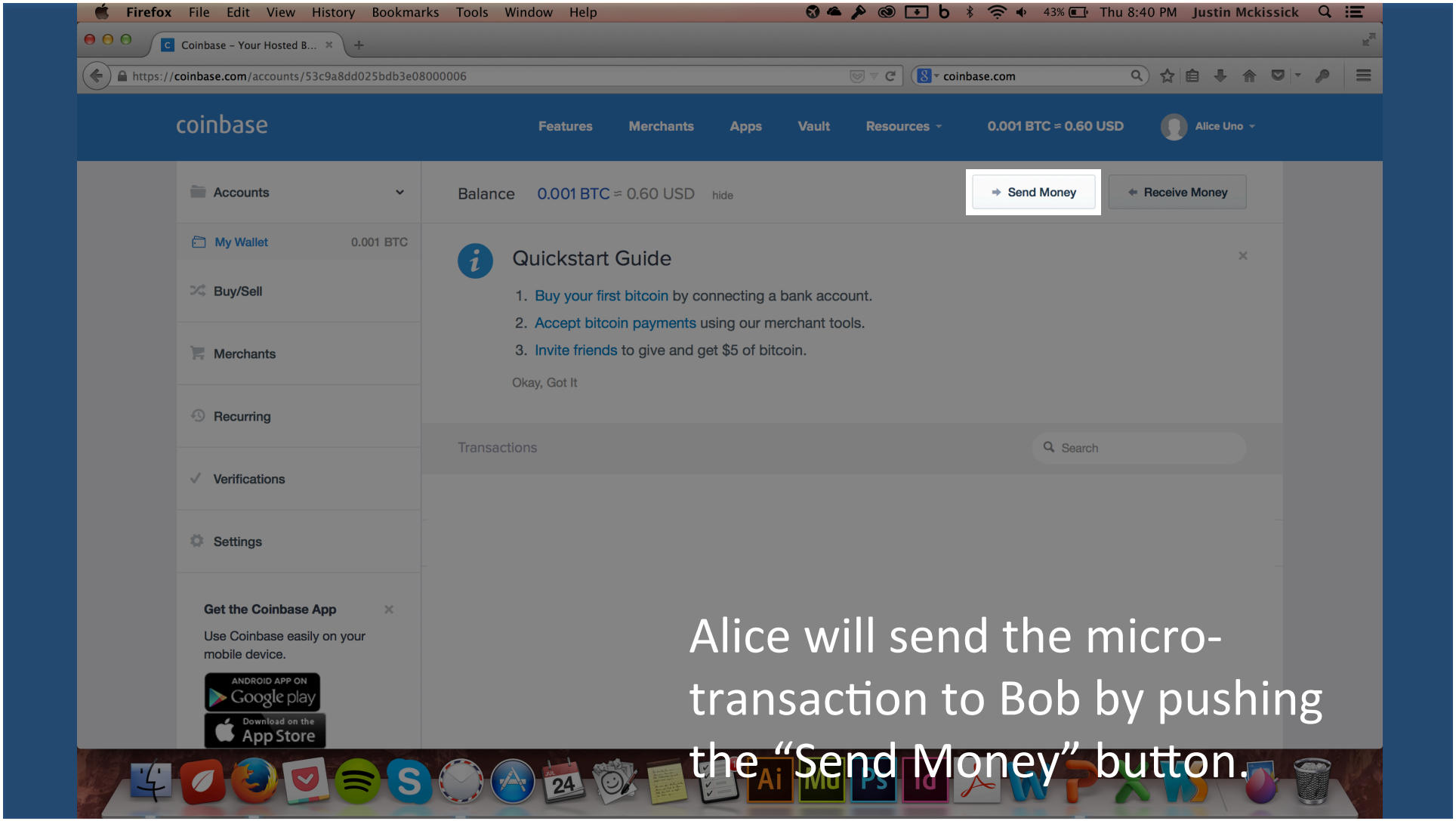

Firefox File Edit View History Bookmarks Tools Window Help
31% Tue 1:21 PM Justin Mckissick
Google
https://www.coinbase.com/
google.com
Bitcoin Wallet – Coinbase
https://coinbase.com
coinbase.com
coinbase.com
https://www.coinbase.com
https://www.coinbase.com
Coinbase – Your Hosted Bitcoin Wallet
https://coinbase.com/accounts/last
Coinbase – Your Hosted Bitcoin Wallet
https://coinbase.com/accounts/53c9a8dd025bdb3e08000006
Coinbase – Your Hosted Bitcoin Wallet
https://coinbase.com/signin_step_two
+You Gmail Images Sign in
Google Search I'm Feeling Lucky
Advertising Business About
Alice first goes to https://www.coinbase.com by typing it into her address bar.

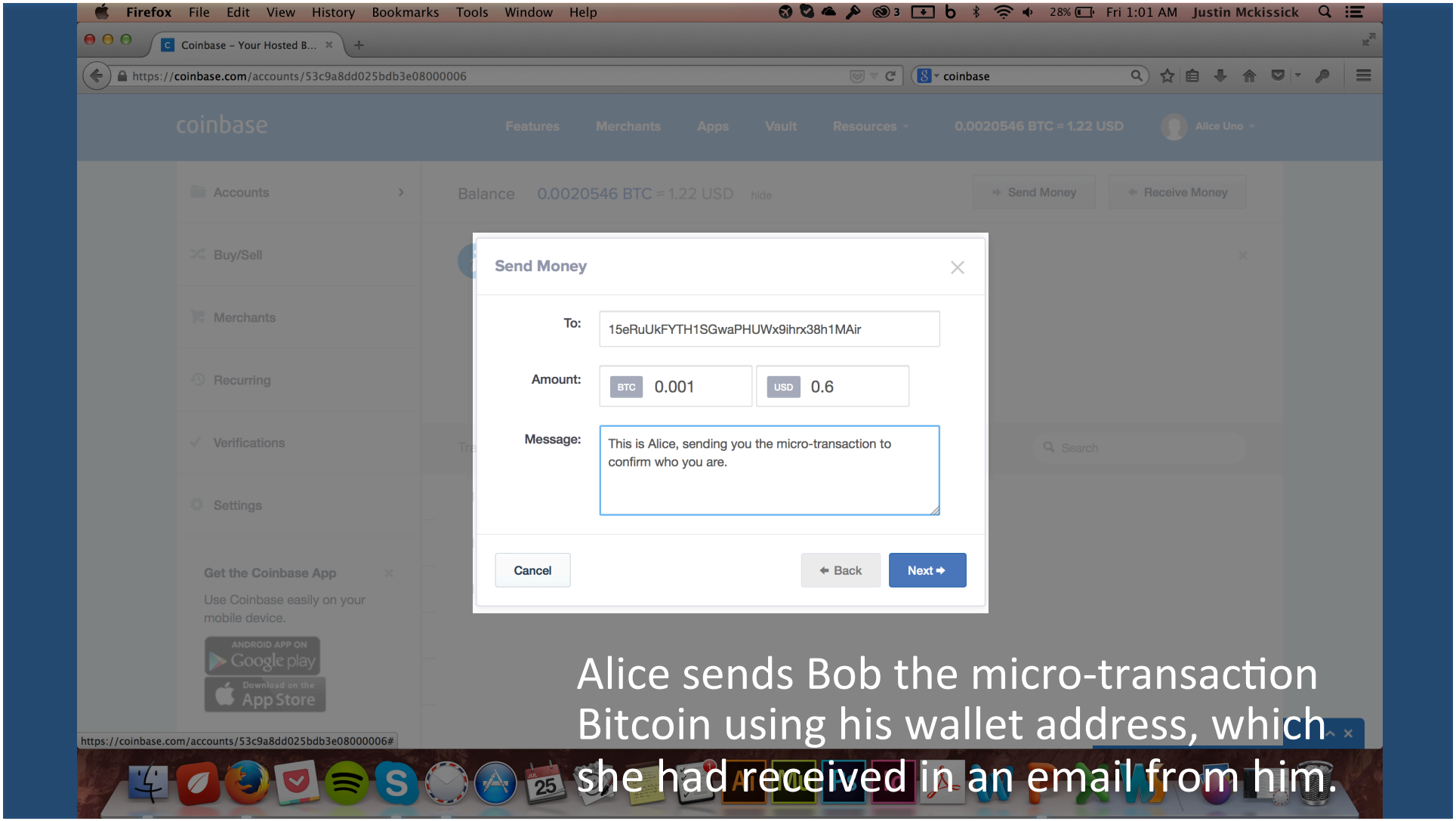

Firefox File Edit View History Bookmarks Tools Window Help
Wed 10:10 PM Justin Mckissick
Bitcoin Wallet – Coinbase
https://coinbase.com
Google
You are connected to
coinbase.com
which is run by
(unknown)
Verified by: DigiCert Inc
The connection to this website is secure.
More Information...
Features
Merchants
Apps
Vault
Resources
Current Buy Price: $620.65
Sign In
Sign Up
Bitcoin, safe and easy.
Coinbase is an international digital wallet that allows you to securely buy, use, and accept bitcoin currency
Your Email
Choose A Password
Create Bitcoin Wallet
Alice makes sure that the website has been verified by "DigiCert inc."


Firefox File Edit View History Bookmarks Tools Window Help
Tue 1:21 PM Justin Mckissick
Bitcoin Wallet – Coinbase
https://coinbase.com
google.com
coinbase
Features Merchants Apps Vault Resources
Current Buy Price: $622.41
Sign In
Sign Up
Bitcoin, safe and easy.
Coinbase is an international digital wallet that allows you to securely buy, use, and accept bitcoin currency
Your Email
Choose A Password
Create Bitcoin Wallet
Then she clicks on the “Sign In” button.
https://coinbase.com/signin
How can we help?

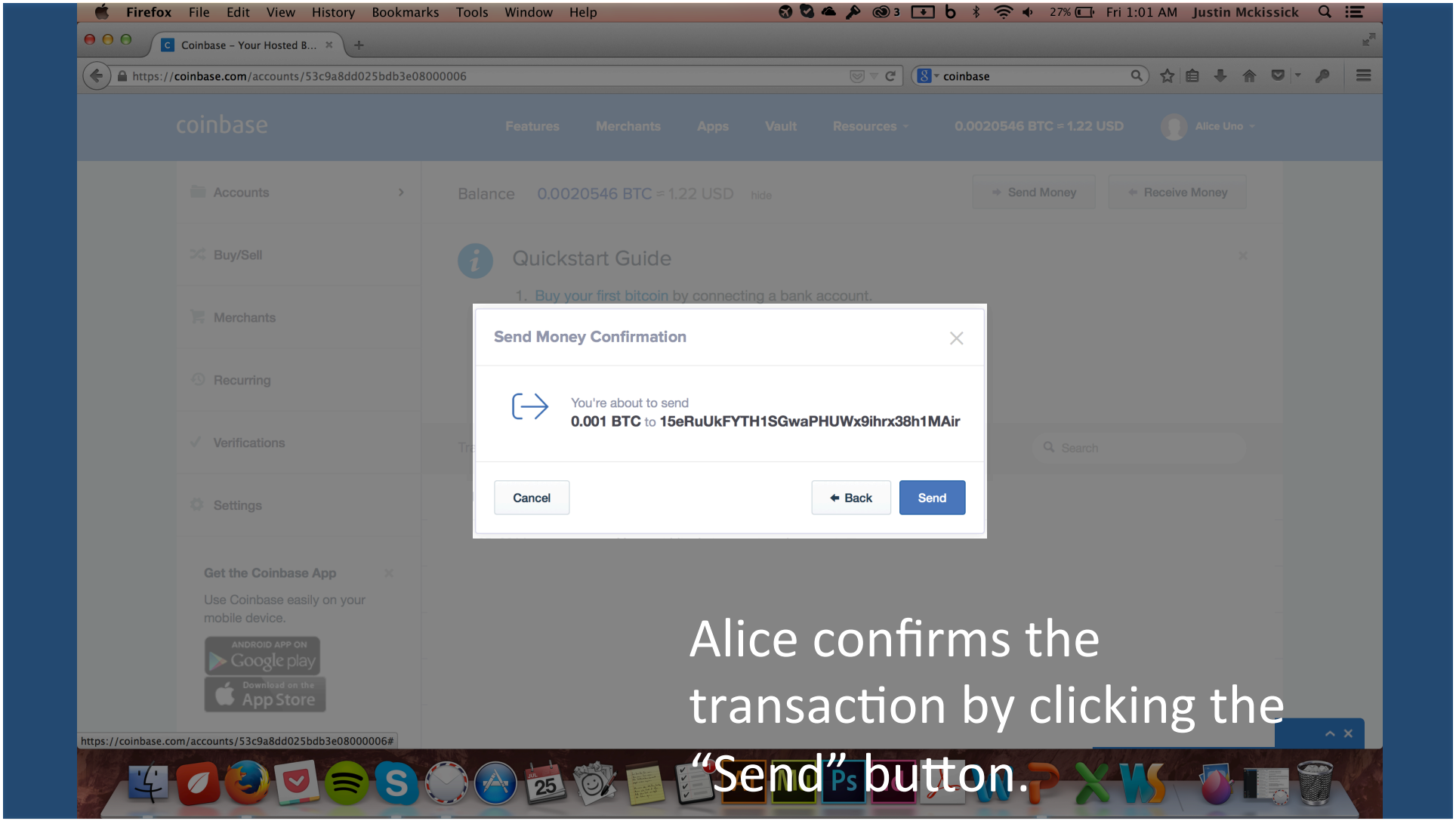

Firefox File Edit View History Bookmarks Tools Window Help
Tue 1:21 PM Justin Mckissick
Coinbase – Your Hosted B...
https://coinbase.com/signin
google.com
coinbase
Features Merchants Apps Vault Resources
Current Buy Price: $622.41
Sign In
Sign Up
Sign In
Email
alice.one206@gmail.com
Password
Remember me
Sign In
Forgot password? · Don't have an account? Sign up
Alice then signs in to her Coinbase account using her credentials.


Firefox File Edit View History Bookmarks Tools Window Help
Tue 1:21 PM Justin Mckissick
Coinbase - Your Hosted B...
https://coinbase.com/signin_step_two
google.com
coinbase
Features Merchants Apps Vault Resources Current Buy Price: $622.41 Sign In Sign Up
2-Step Verification
Enter the verification code generated by your phone ending in +x xxx xxx xx65. You can also use the iPhone Authy or Google Authenticator app on your phone.
Enter 2-step verification code:
6750815
Verify
Don't ask me for the code again for 30 days when I use this computer.
Code not working?
Because two-factor authentication has been setup, Alice must enter the code that was just sent to her phone.

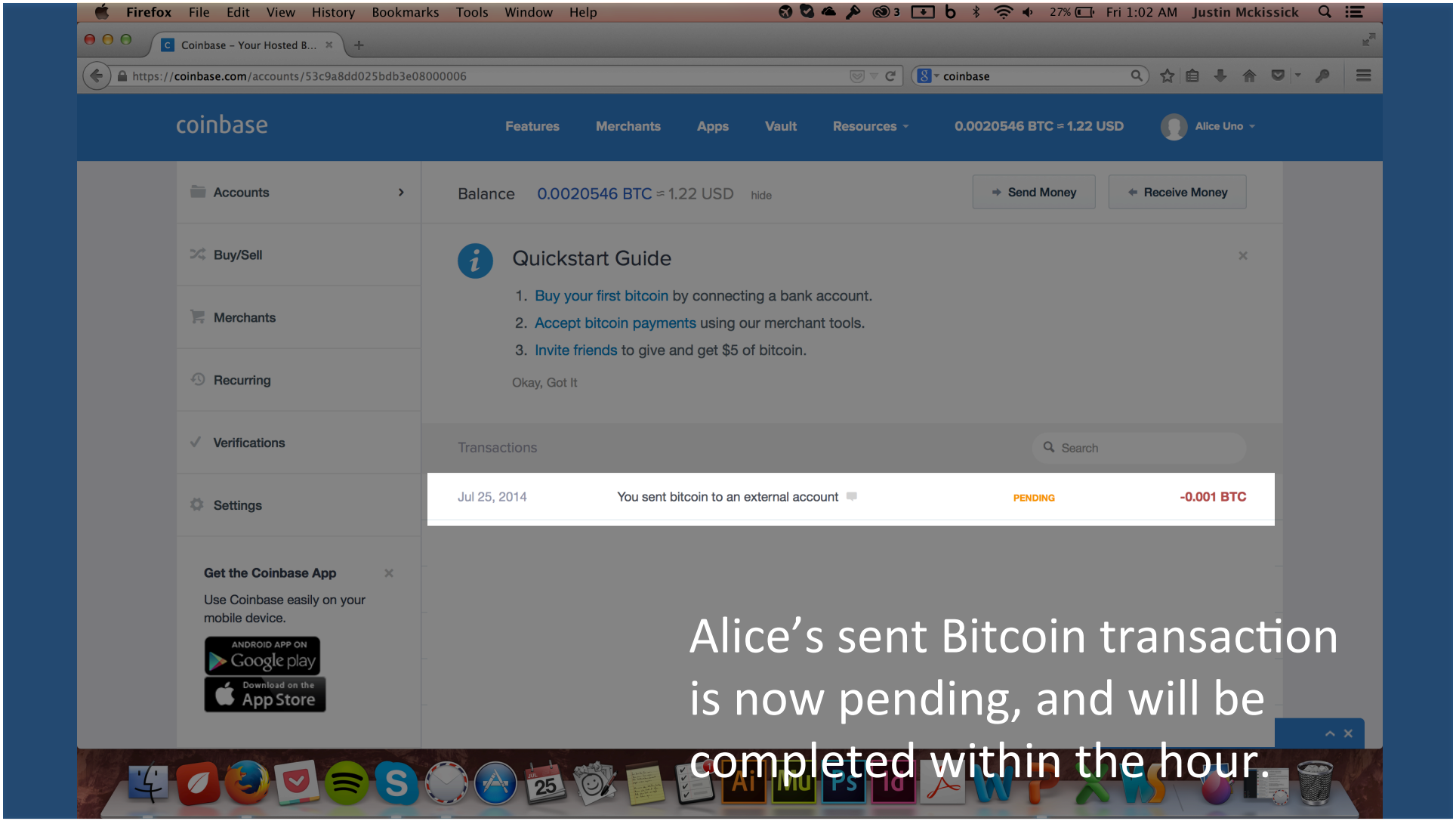

Firefox File Edit View History Bookmarks Tools Window Help
Thu 8:40 PM Justin Mckissick
Coinbase - Your Hosted B...
https://coinbase.com/accounts/53c9a8dd025bdb3e08000006
coinbase.com
coinbase
Features Merchants Apps Vault Resources 0.001 BTC = 0.60 USD Alice Uno
Accounts
My Wallet 0.001 BTC
Buy/Sell
Merchants
Recurring
Verifications
Settings
Balance 0.001 BTC = 0.60 USD hide
Send Money
Receive Money
Quickstart Guide
1. Buy your first bitcoin by connecting a bank account.
2. Accept bitcoin payments using our merchant tools.
3. Invite friends to give and get $5 of bitcoin.
Okay, Got It
Transactions
Search
Get the Coinbase App
Use Coinbase easily on your mobile device.
ANDROID APP ON Google play
Download on the App Store
Alice will send the micro-transaction to Bob by pushing the "Send Money" button.

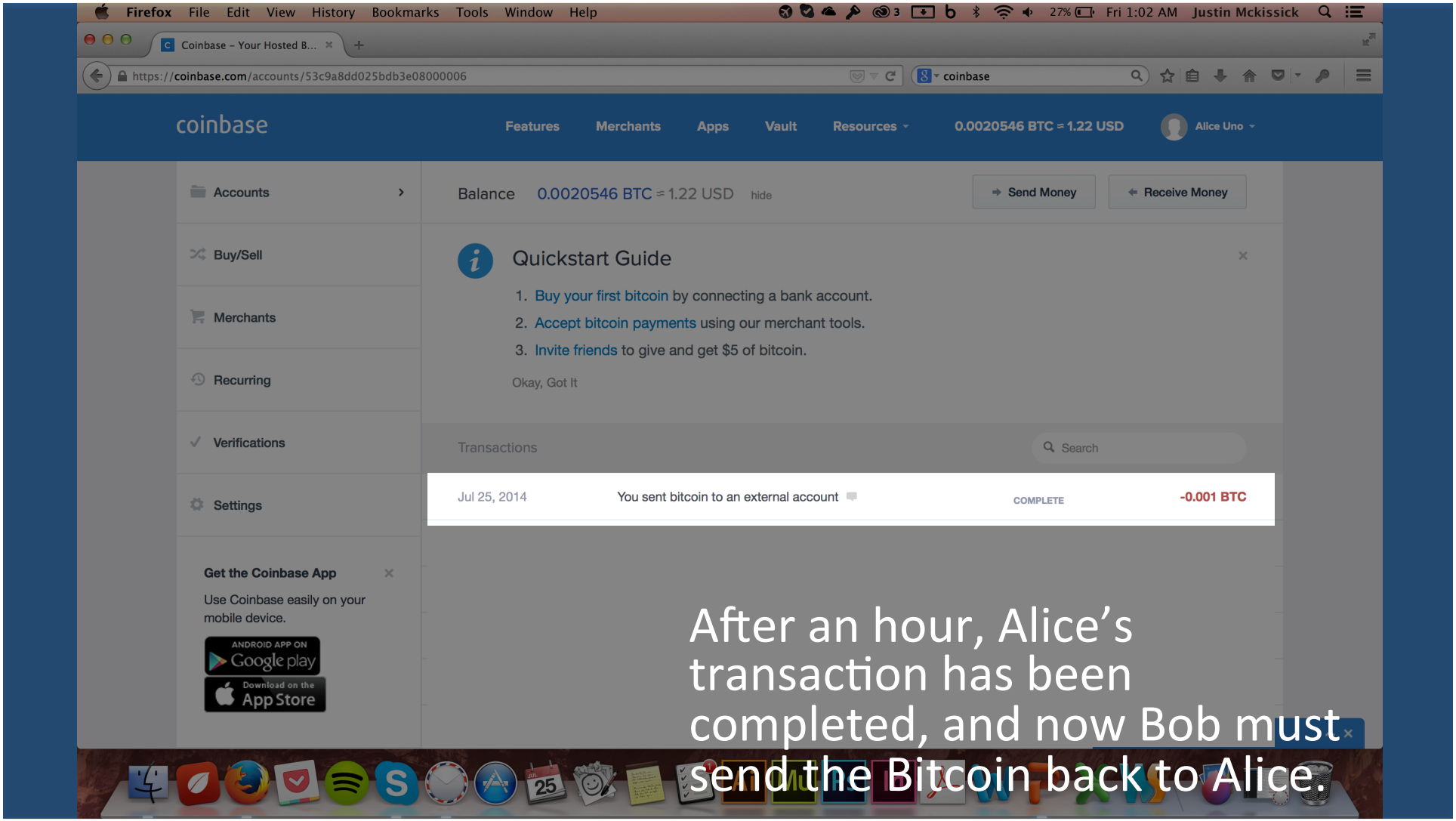


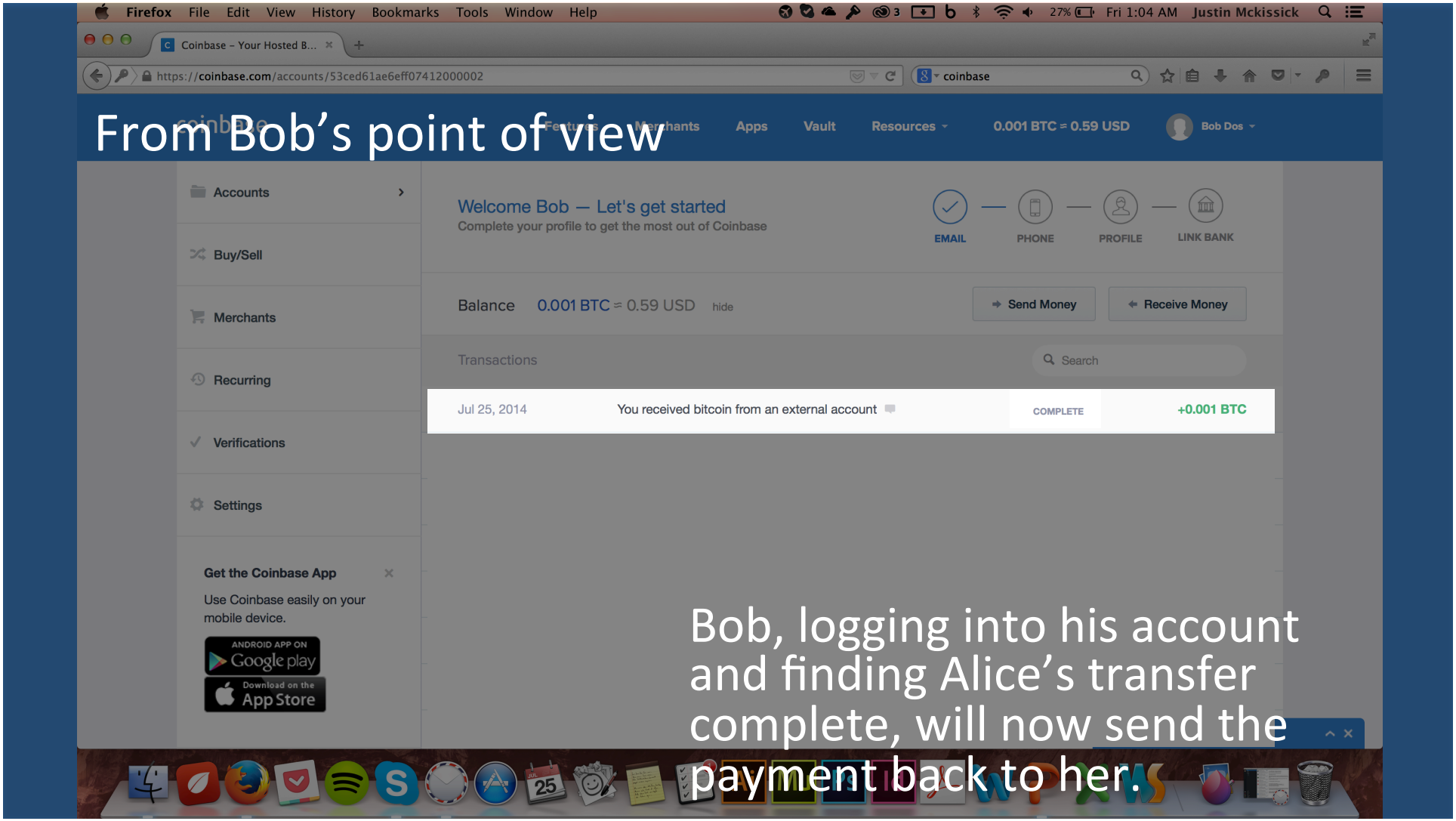
Alice sends Bob the micro-transaction Bitcoin using his wallet address, which she had received in an email from him.

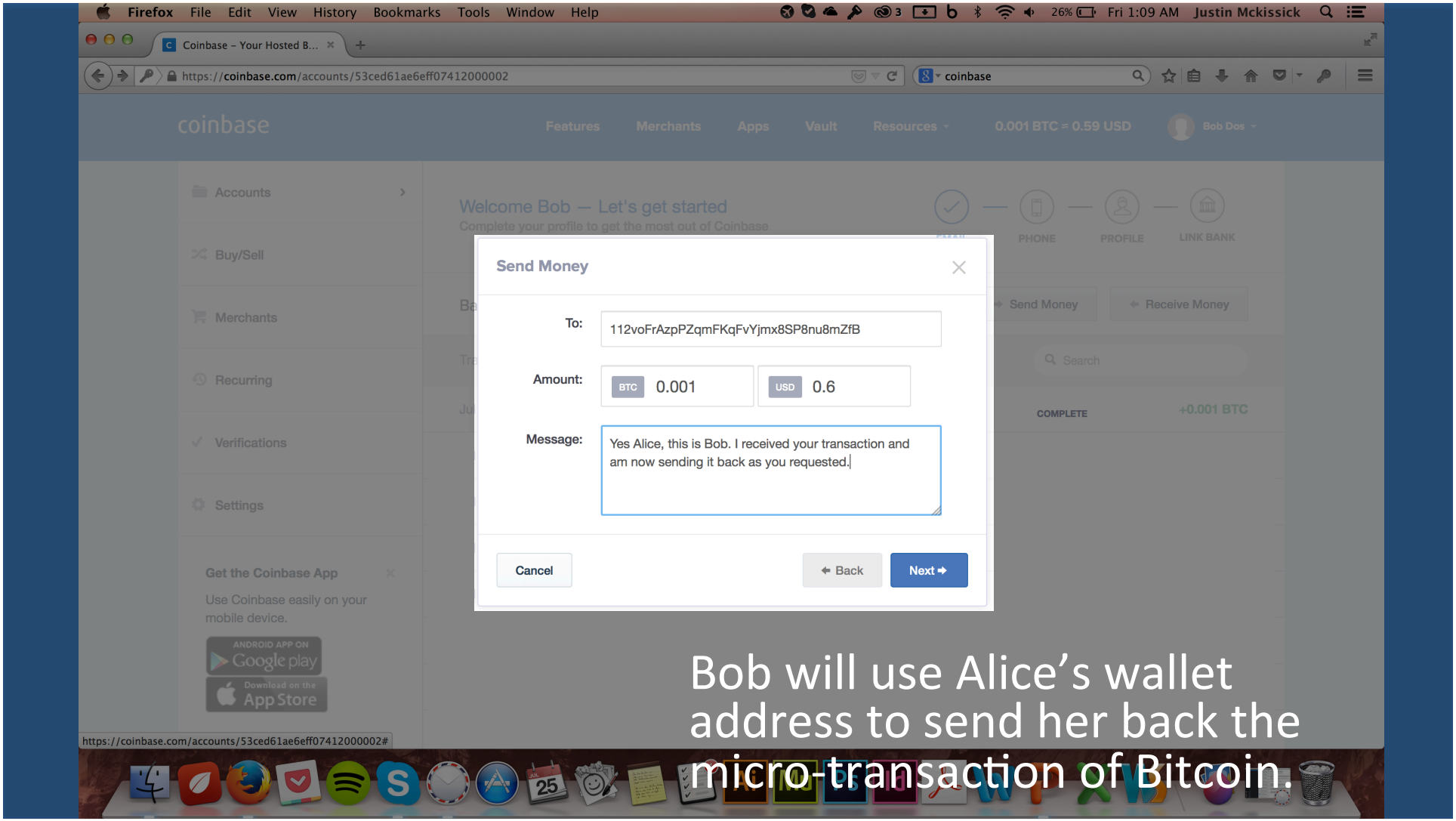


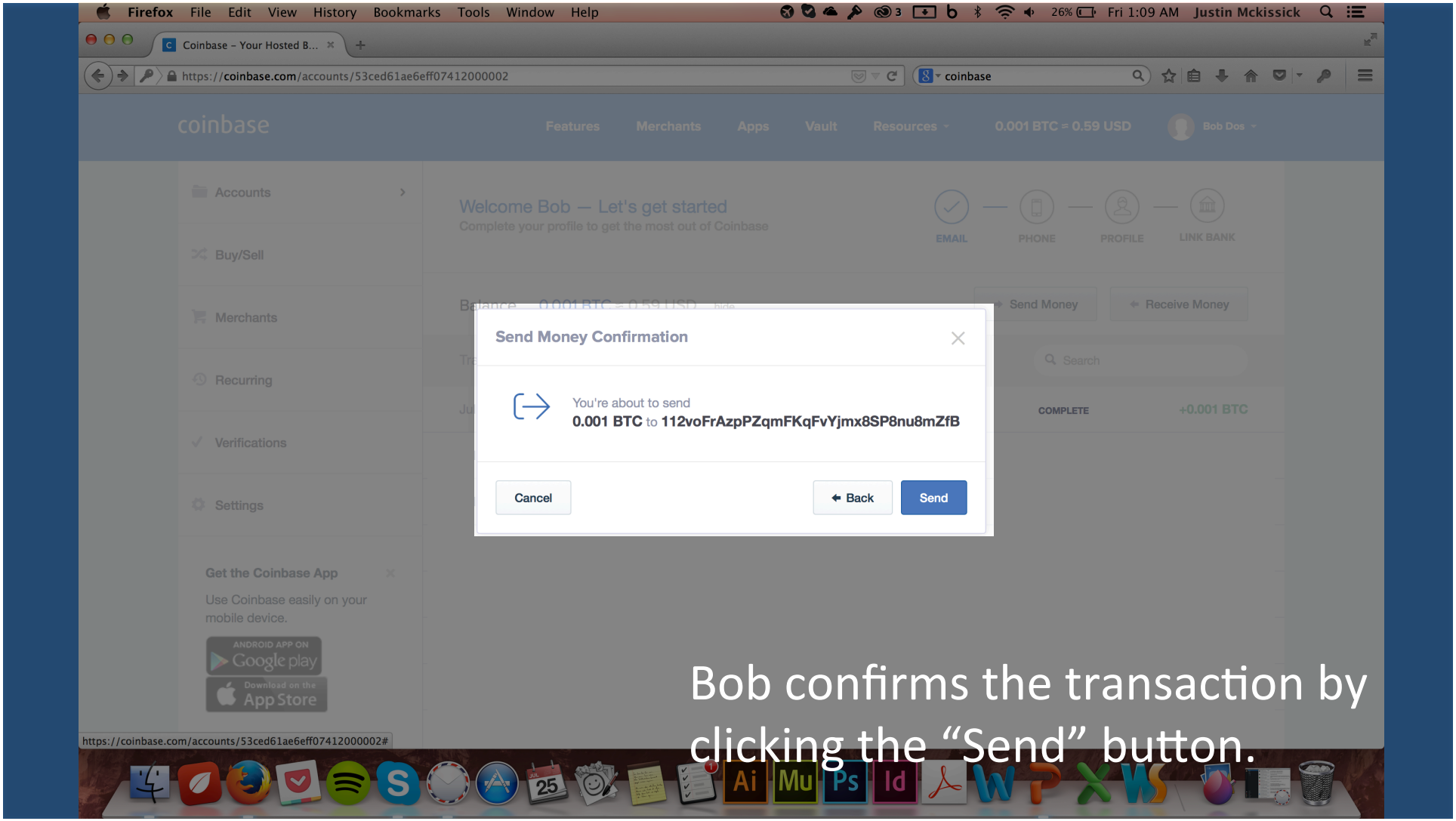
Alice confirms the transaction by clicking the "Send" button.


Firefox File Edit View History Bookmarks Tools Window Help
Fri 1:02 AM Justin Mckissick
Coinbase - Your Hosted B...
https://coinbase.com/accounts/53c9a8dd025bdb3e08000006
coinbase
coinbase
Features Merchants Apps Vault Resources
0.0020546 BTC = 1.22 USD
Alice Uno
Accounts
Buy/Sell
Merchants
Recurring
Verifications
Settings
Balance 0.0020546 BTC = 1.22 USD hide
Send Money
Receive Money
Quickstart Guide
1. Buy your first bitcoin by connecting a bank account.
2. Accept bitcoin payments using our merchant tools.
3. Invite friends to give and get $5 of bitcoin.
Okay, Got It
Transactions
Search
Jul 25, 2014
You sent bitcoin to an external account
PENDING
-0.001 BTC
Get the Coinbase App
Use Coinbase easily on your mobile device.
ANDROID APP ON Google play
Download on the App Store
Alice's sent Bitcoin transaction is now pending, and will be completed within the hour.

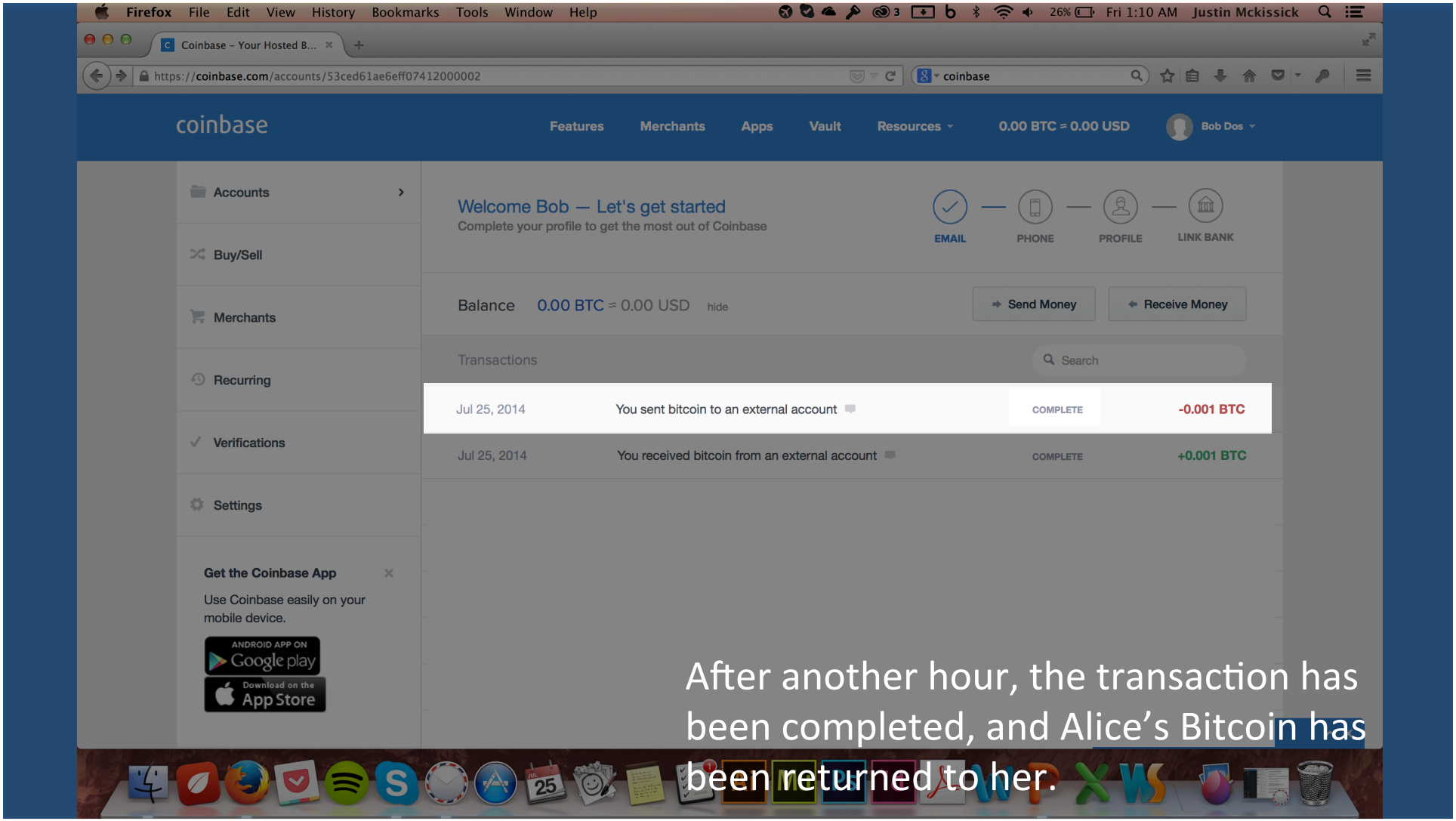

Firefox File Edit View History Bookmarks Tools Window Help
Fri 1:02 AM Justin Mckissick
Coinbase - Your Hosted B...
https://coinbase.com/accounts/53c9a8dd025bdb3e08000006
coinbase
coinbase
Features Merchants Apps Vault Resources
0.0020546 BTC = 1.22 USD
Alice Uno
Accounts
Buy/Sell
Merchants
Recurring
Verifications
Settings
Balance 0.0020546 BTC = 1.22 USD hide
Send Money
Receive Money
Quickstart Guide
1. Buy your first bitcoin by connecting a bank account.
2. Accept bitcoin payments using our merchant tools.
3. Invite friends to give and get $5 of bitcoin.
Okay, Got It
Transactions
Search
Jul 25, 2014
You sent bitcoin to an external account
COMPLETE
-0.001 BTC
Get the Coinbase App
Use Coinbase easily on your mobile device.
ANDROID APP ON Google play
Download on the App Store
After an hour, Alice's transaction has been completed, and now Bob must send the Bitcoin back to Alice.

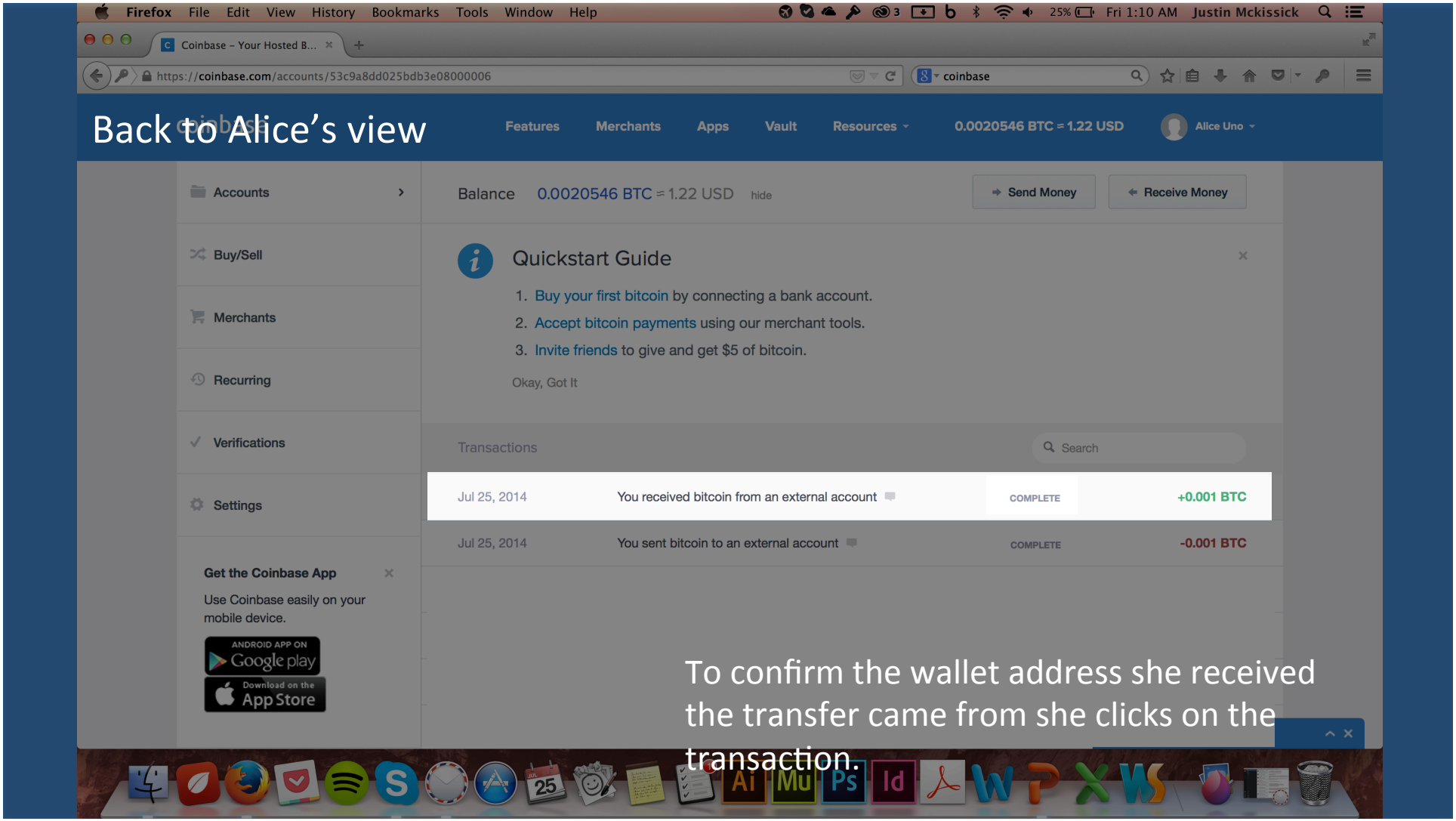

From Bob's point of view
Firefox File Edit View History Bookmarks Tools Window Help
Fri 1:04 AM Justin Mckissick
Coinbase - Your Hosted B...
https://coinbase.com/accounts/53ced61ae6eff07412000002
coinbase
Features Merchants Apps Vault Resources 0.001 BTC = 0.59 USD Bob Dos
Accounts
Buy/Sell
Merchants
Recurring
Verifications
Settings
Get the Coinbase App
Use Coinbase easily on your mobile device.
ANDROID APP ON Google play
Download on the App Store
Welcome Bob — Let's get started
Complete your profile to get the most out of Coinbase
EMAIL PHONE PROFILE LINK BANK
Balance 0.001 BTC = 0.59 USD hide
Send Money
Receive Money
Transactions
Search
Jul 25, 2014
You received bitcoin from an external account
COMPLETE
+0.001 BTC
Bob, logging into his account and finding Alice's transfer complete, will now send the payment back to her.

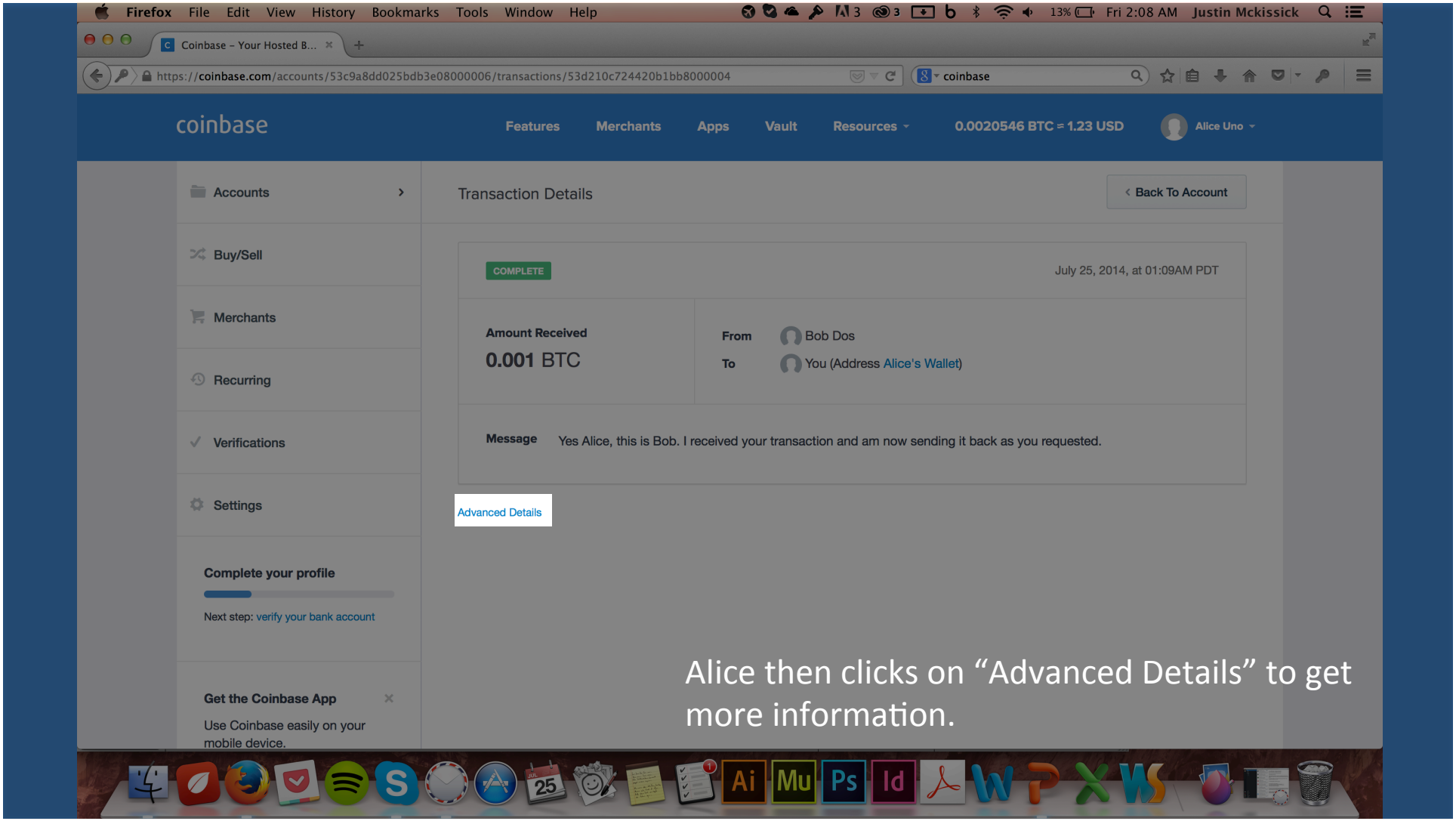

Send Money
To:
112voFrAzpPZqmFKqFvYjmx8SP8nu8mZfB
Amount:
BTC 0.001
USD 0.6
Message:
Yes Alice, this is Bob. I received your transaction and am now sending it back as you requested.
Cancel
Back
Next
Bob will use Alice's wallet address to send her back the micro-transaction of Bitcoin.

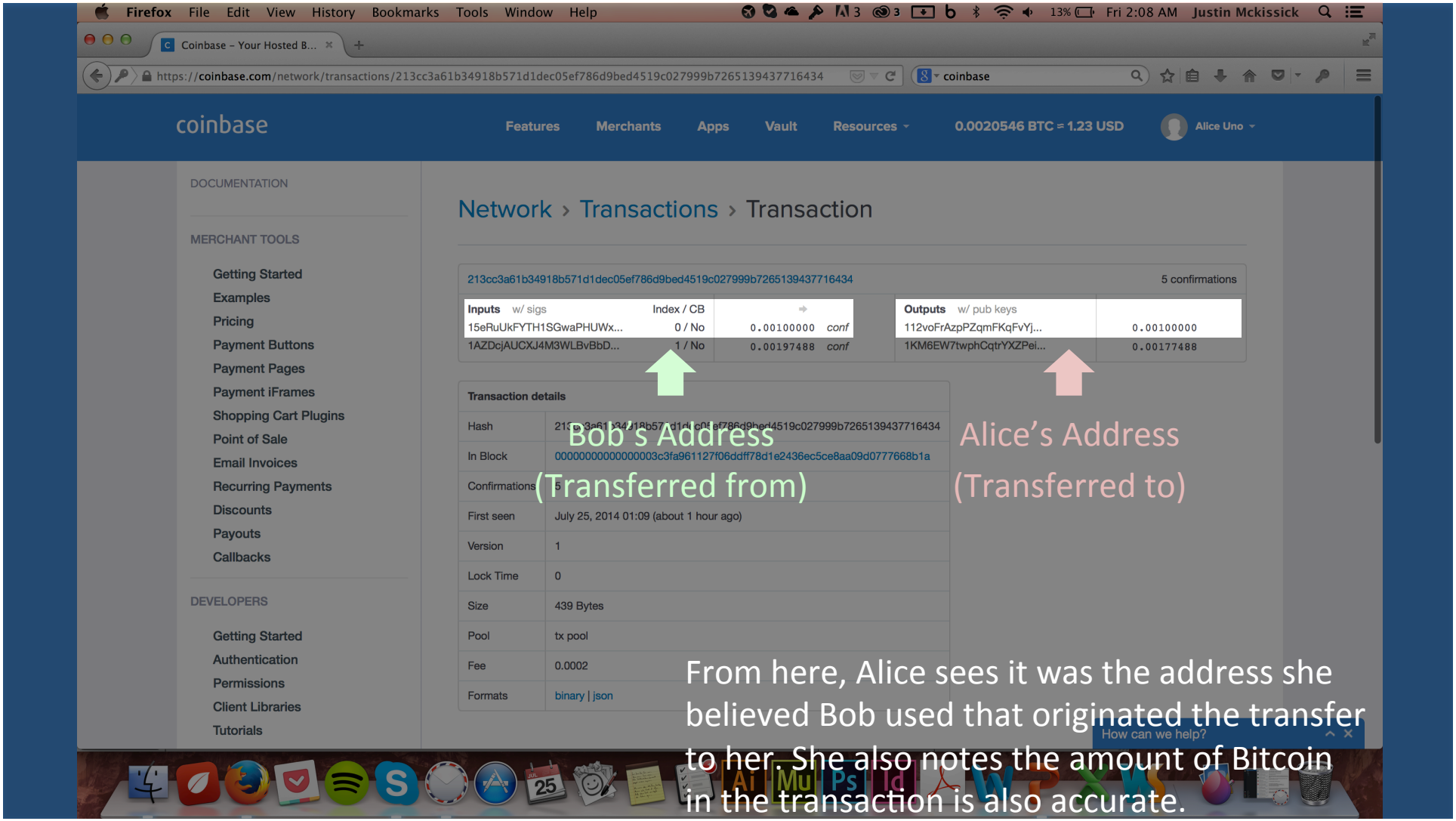


Bob confirms the transaction by clicking the “Send” button.


Firefox File Edit View History Bookmarks Tools Window Help
Fri 1:10 AM Justin Mckissick
Coinbase - Your Hosted B...
https://coinbase.com/accounts/53ced61ae6eff07412000002
coinbase
coinbase
Features Merchants Apps Vault Resources
0.00 BTC ≈ 0.00 USD
Bob Dos
Accounts
Buy/Sell
Merchants
Recurring
Verifications
Settings
Get the Coinbase App
Use Coinbase easily on your mobile device.
ANDROID APP ON Google play
Download on the App Store
Welcome Bob — Let's get started
Complete your profile to get the most out of Coinbase
EMAIL
PHONE
PROFILE
LINK BANK
Balance 0.00 BTC ≈ 0.00 USD hide
Send Money
Receive Money
Transactions
Search
Jul 25, 2014 You sent bitcoin to an external account COMPLETE -0.001 BTC
Jul 25, 2014 You received bitcoin from an external account COMPLETE +0.001 BTC
After another hour, the transaction has been completed, and Alice's Bitcoin has been returned to her.


Back to Alice's view
Features
Merchants
Apps
Vault
Resources
0.0020546 BTC ≈ 1.22 USD
Alice Uno
Accounts
Buy/Sell
Merchants
Recurring
Verifications
Settings
Balance 0.0020546 BTC ≈ 1.22 USD hide
Send Money
Receive Money
Quickstart Guide
1. Buy your first bitcoin by connecting a bank account.
2. Accept bitcoin payments using our merchant tools.
3. Invite friends to give and get $5 of bitcoin.
Okay, Got It
Transactions
Search
Jul 25, 2014 You received bitcoin from an external account COMPLETE +0.001 BTC
Jul 25, 2014 You sent bitcoin to an external account COMPLETE -0.001 BTC
Get the Coinbase App
Use Coinbase easily on your mobile device.
ANDROID APP ON Google play
Download on the App Store
To confirm the wallet address she received the transfer came from she clicks on the transaction.


Firefox File Edit View History Bookmarks Tools Window Help
Fri 2:08 AM Justin Mckissick
Coinbase - Your Hosted B...
https://coinbase.com/accounts/53c9a8dd025bdb3e08000006/transactions/53d210c724420b1bb8000004
coinbase
coinbase
Features Merchants Apps Vault Resources
0.0020546 BTC = 1.23 USD
Alice Uno
Accounts
Buy/Sell
Merchants
Recurring
Verifications
Settings
Complete your profile
Next step: verify your bank account
Get the Coinbase App
Use Coinbase easily on your mobile device.
Transaction Details
Back To Account
COMPLETE
July 25, 2014, at 01:09AM PDT
Amount Received
0.001 BTC
From Bob Dos
To You (Address Alice's Wallet)
Message Yes Alice, this is Bob. I received your transaction and am now sending it back as you requested.
Advanced Details
Alice then clicks on “Advanced Details” to get more information.


Firefox File Edit View History Bookmarks Tools Window Help
Fri 2:08 AM Justin Mckissick
Coinbase - Your Hosted B...
https://coinbase.com/network/transactions/213cc3a61b34918b571d1dec05ef786d9bed4519c027999b7265139437716434
coinbase
Features Merchants Apps Vault Resources 0.0020546 BTC = 1.23 USD Alice Uno
DOCUMENTATION
MERCHANT TOOLS
Getting Started
Examples
Pricing
Payment Buttons
Payment Pages
Payment iFrames
Shopping Cart Plugins
Point of Sale
Email Invoices
Recurring Payments
Discounts
Payouts
Callbacks
DEVELOPERS
Getting Started
Authentication
Permissions
Client Libraries
Tutorials
Network › Transactions › Transaction
213cc3a61b34918b571d1dec05ef786d9bed4519c027999b7265139437716434
5 confirmations
Inputs w/ sigs
Index / CB
15eRuUkFYTH1SGwaPHUWx...
0 / No
0.00100000 conf
1AZDcjAUCXJ4M3WLBvBbD...
1 / No
0.00197488 conf
Outputs w/ pub keys
112voFrAzpPZqmFKqFvYj...
0.00100000
1KM6EW7twphCqtrYXZPei...
0.00177488
Transaction details
Hash
In Block
00000000000000003c3fa961127f06ddff78d1e2436ec5ce8aa09d0777668b1a
Confirmations 5
First seen July 25, 2014 01:09 (about 1 hour ago)
Version 1
Lock Time 0
Size 439 Bytes
Pool tx pool
Fee 0.0002
Formats binary | json
Bob's Address
(Transferred from)
Alice's Address
(Transferred to)
From here, Alice sees it was the address she believed Bob used that originated the transfer to her. She also notes the amount of Bitcoin in the transaction is also accurate.
How can we help?

Alice then calls Bob to make sure that the person who sent her back the Bitcoin was actually him to rule out a compromised email account. Bob confirms that it was indeed him who received her payment and who sent it back to her. Both Alice and Bob now are able to perform larger scale transactions with the confidence that the money will be going to right person.

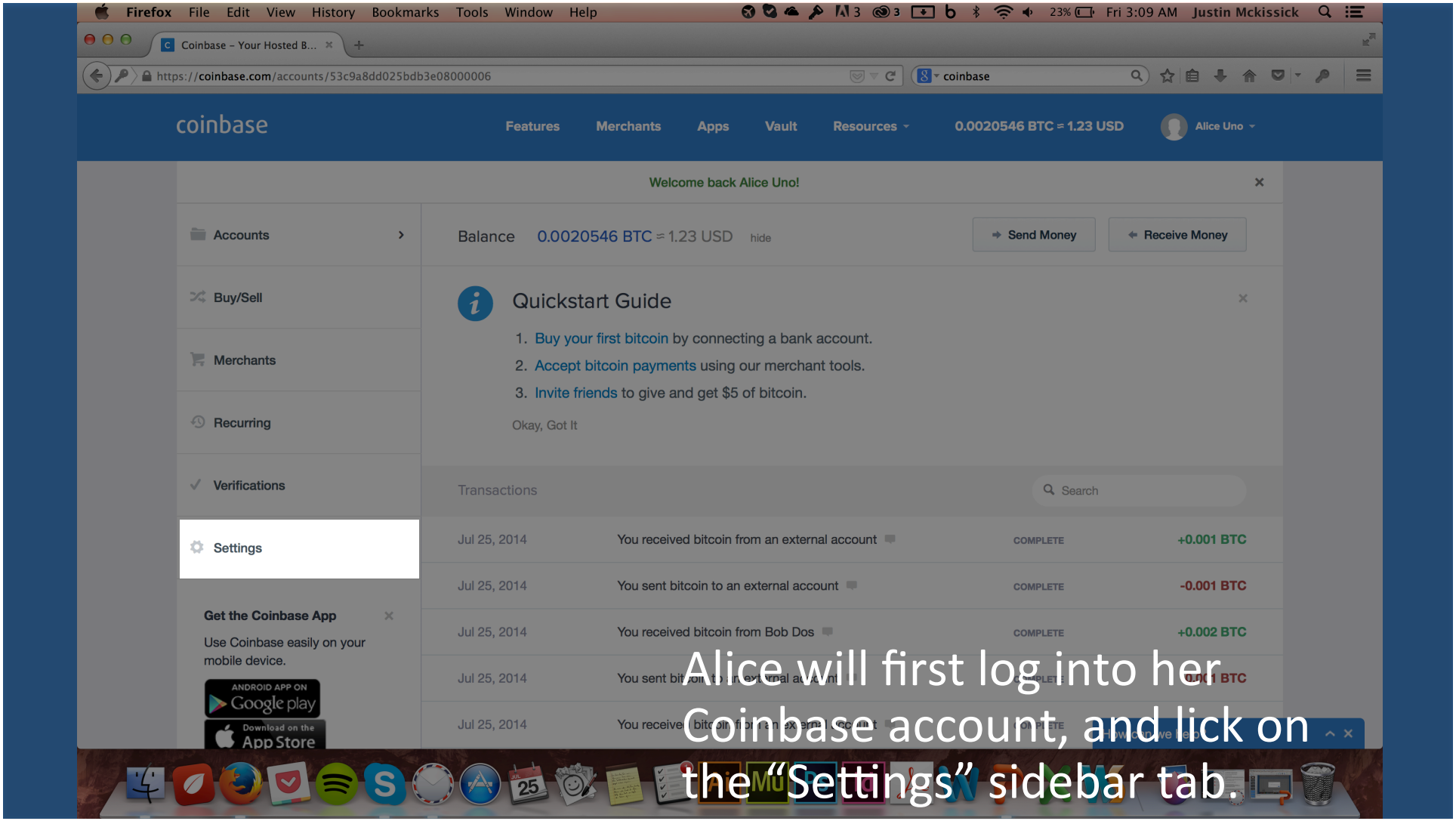
Micro-Transaction Verification Method

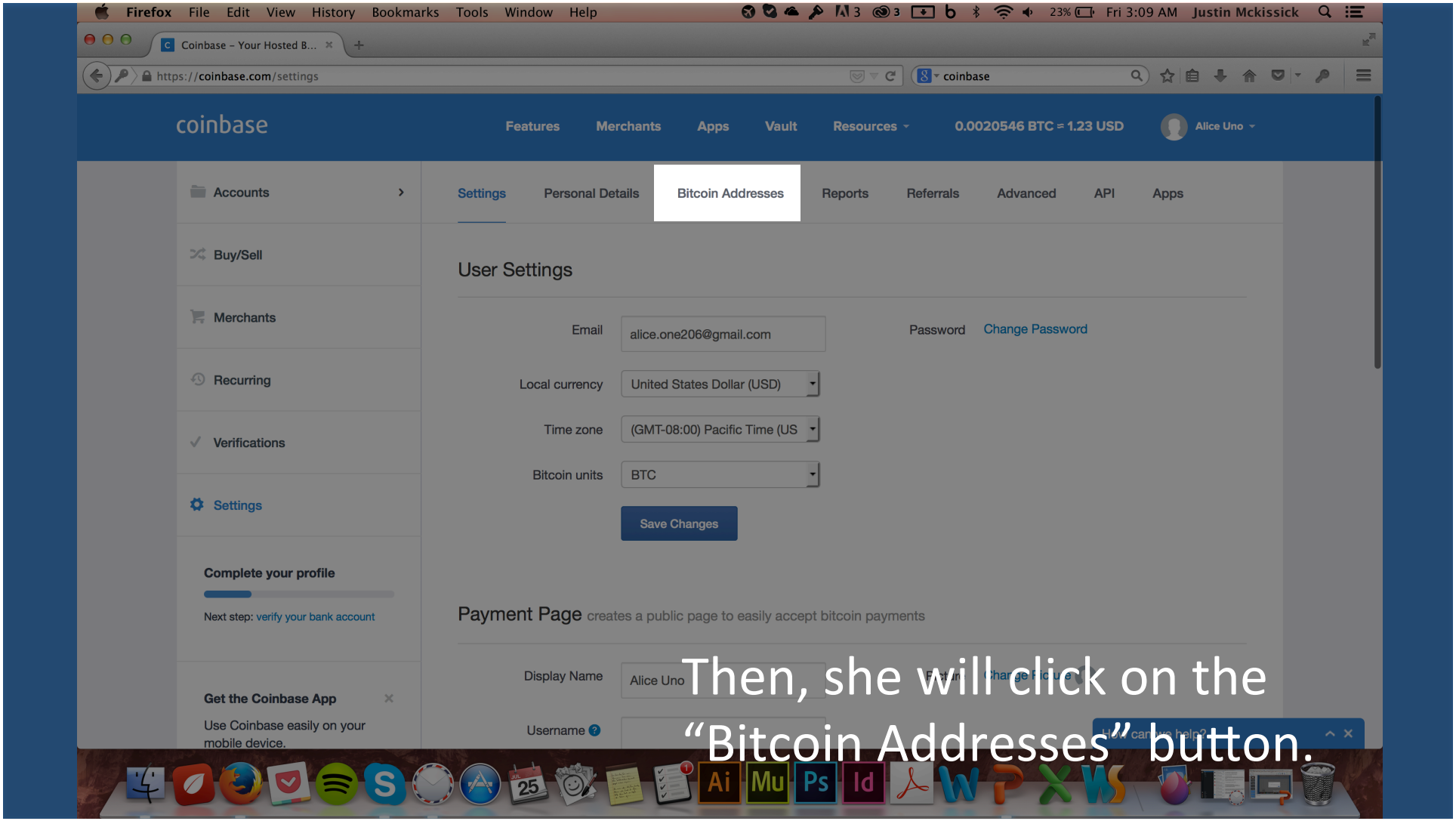
- ✓ Alice and Bob know now for sure they have the correct wallet addresses
- ✓ Both also know that the Bitcoin they send each other will be spendable
- ✓ Both Alice and Bob feel confident to transfer larger amounts of Bitcoin

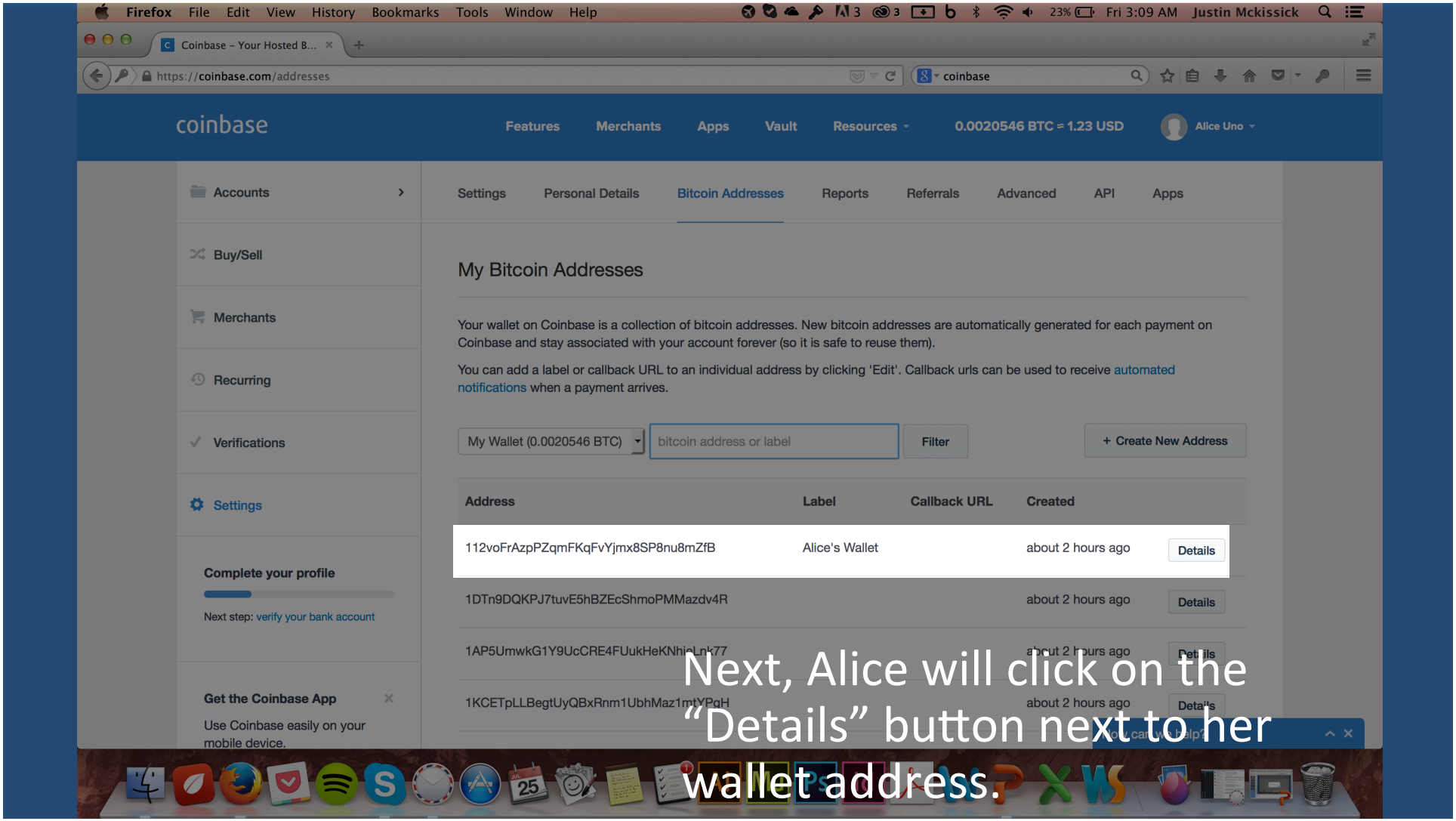
2

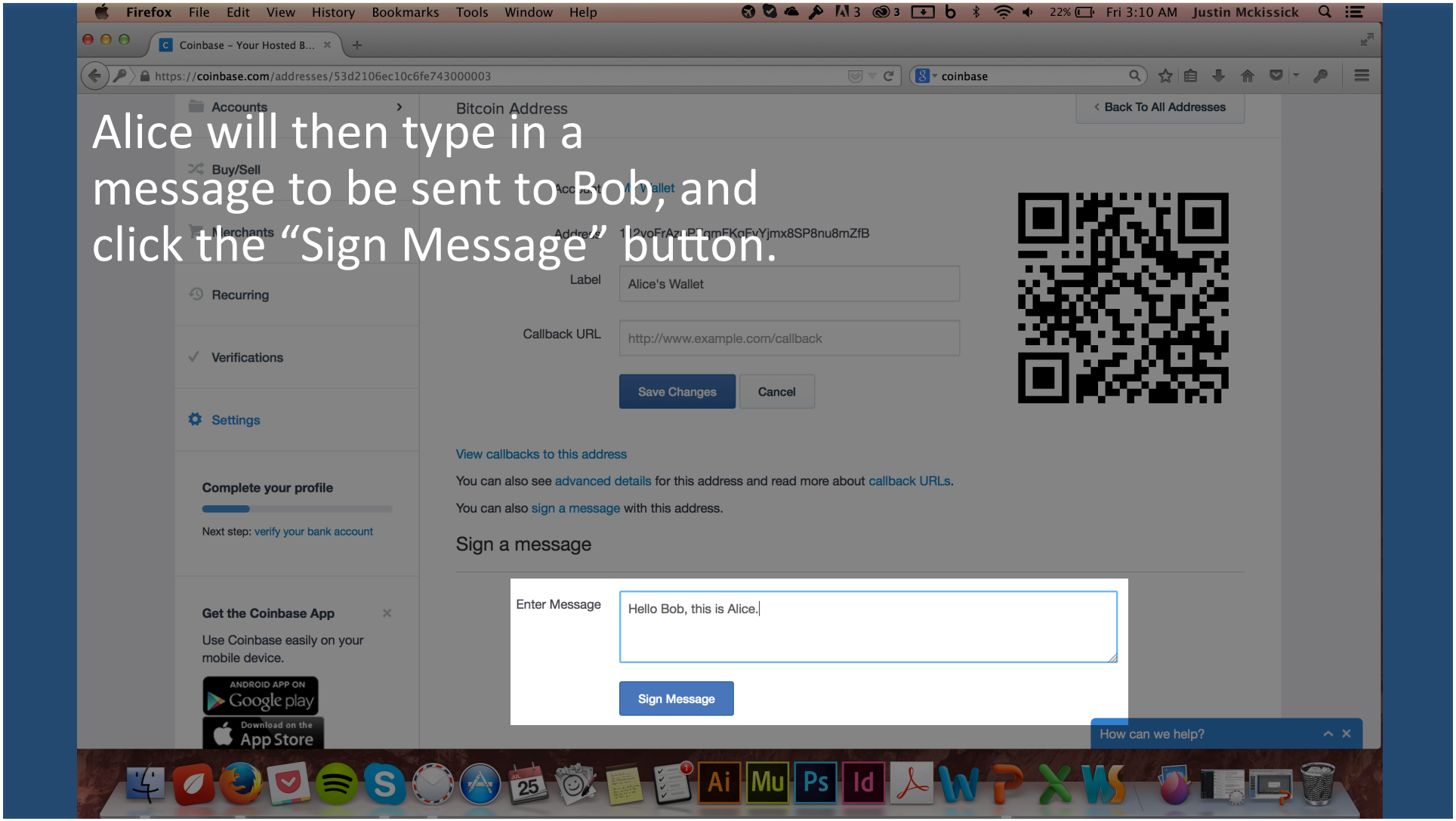
Verifying Addresses via a Signed Message

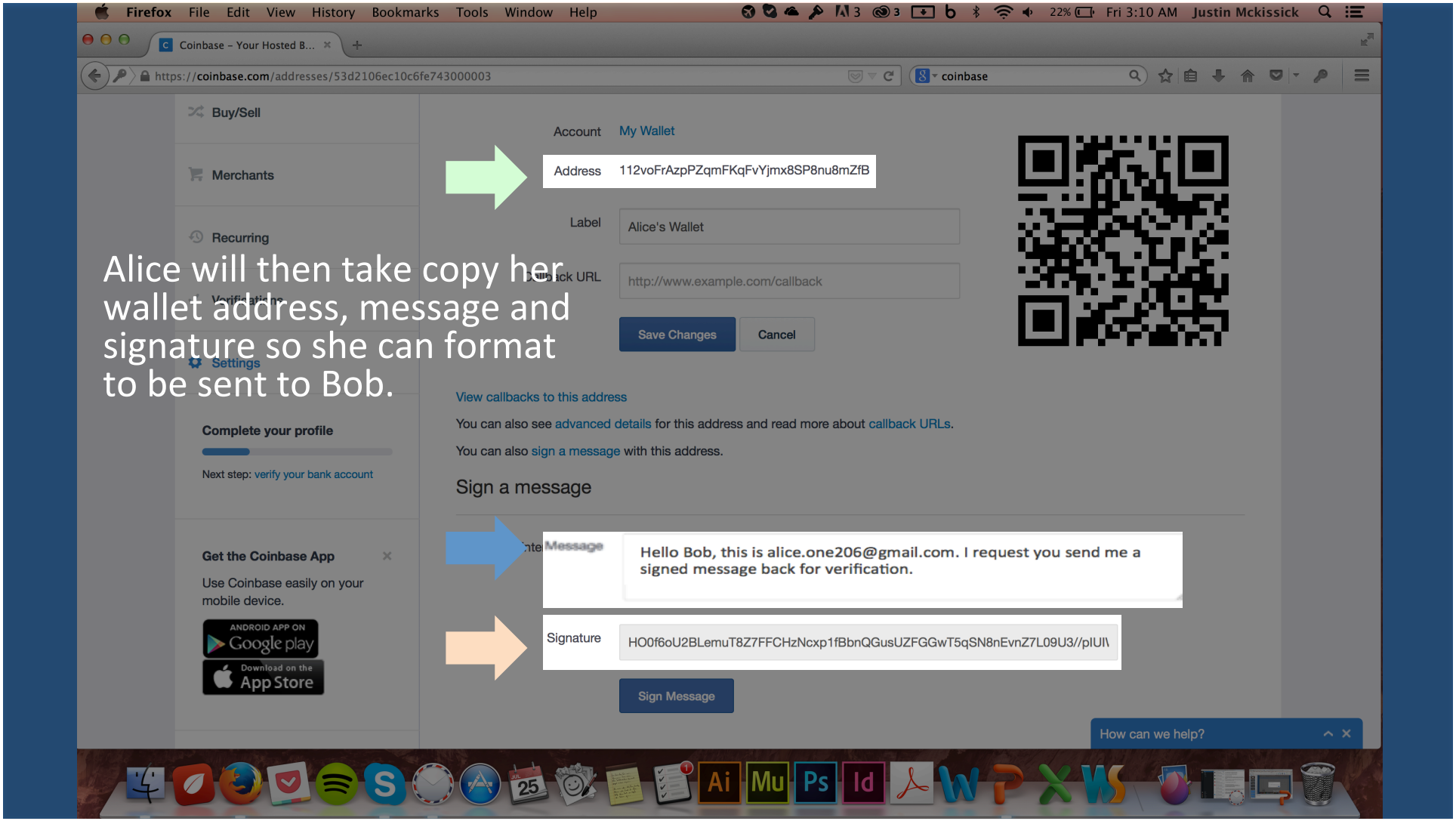
Alice creates a signed message using wallet private key containing her email address and sends it to Bob who then verifies it (and vice versa)


Firefox File Edit View History Bookmarks Tools Window Help
Fri 3:09 AM Justin Mckissick
Coinbase - Your Hosted B...
https://coinbase.com/accounts/53c9a8dd025bdb3e08000006
coinbase
coinbase
Features Merchants Apps Vault Resources
0.0020546 BTC = 1.23 USD
Alice Uno
Welcome back Alice Uno!
Accounts
Buy/Sell
Merchants
Recurring
Verifications
Settings
Balance 0.0020546 BTC = 1.23 USD hide
Send Money
Receive Money
Quickstart Guide
1. Buy your first bitcoin by connecting a bank account.
2. Accept bitcoin payments using our merchant tools.
3. Invite friends to give and get $5 of bitcoin.
Okay, Got It
Transactions
Search
Jul 25, 2014 You received bitcoin from an external account COMPLETE +0.001 BTC
Jul 25, 2014 You sent bitcoin to an external account COMPLETE -0.001 BTC
Jul 25, 2014 You received bitcoin from Bob Dos COMPLETE +0.002 BTC
Get the Coinbase App
Use Coinbase easily on your mobile device.
ANDROID APP ON Google play
Download on the App Store
Alice will first log into her Coinbase account, and lick on the "Settings" sidebar tab.

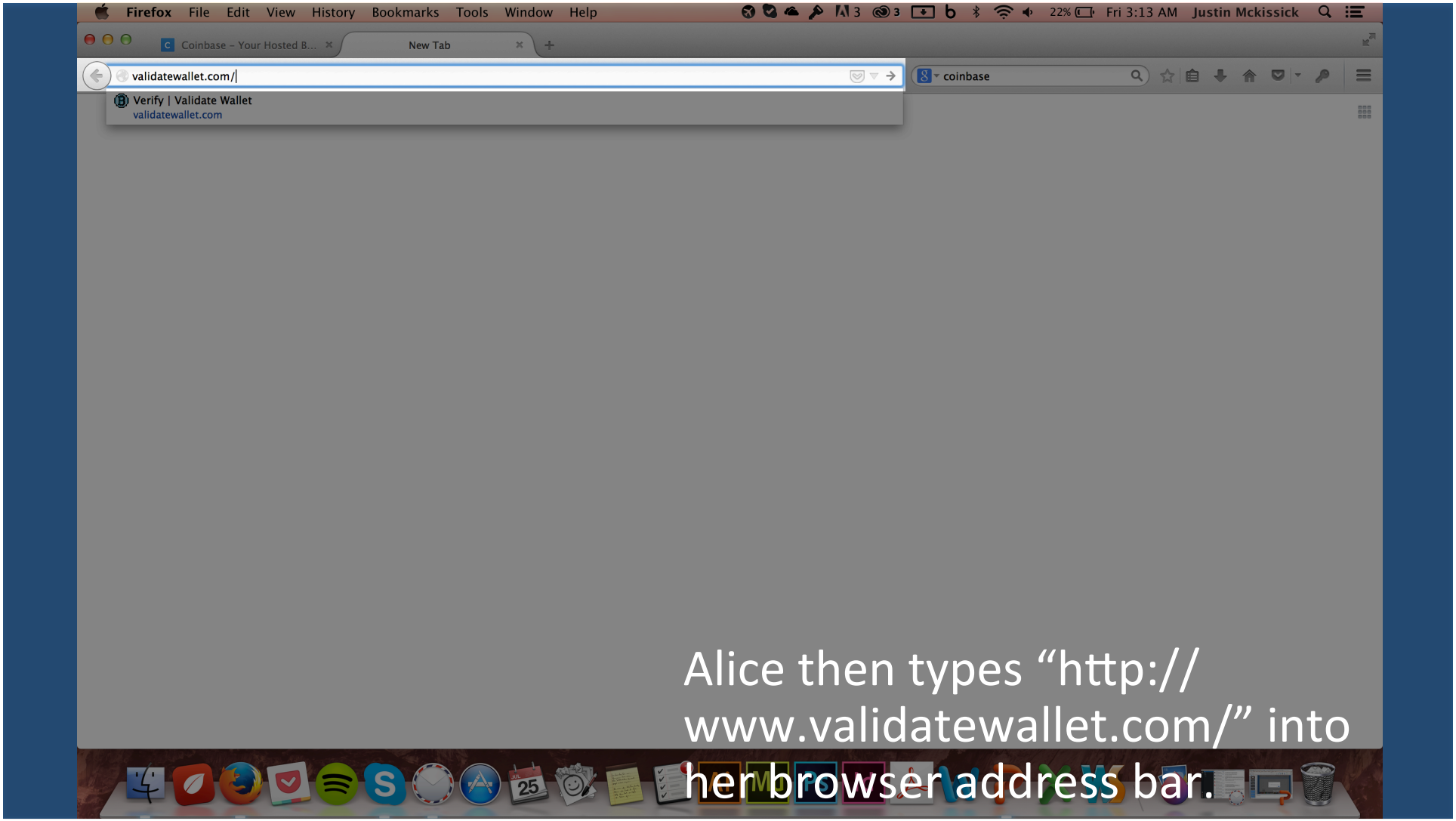

Firefox File Edit View History Bookmarks Tools Window Help
Fri 3:09 AM Justin Mckissick
Coinbase - Your Hosted B...
https://coinbase.com/settings
coinbase
coinbase
Features Merchants Apps Vault Resources
0.0020546 BTC = 1.23 USD
Alice Uno
Accounts
Buy/Sell
Merchants
Recurring
Verifications
Settings
Complete your profile
Next step: verify your bank account
Get the Coinbase App
Use Coinbase easily on your mobile device.
Settings Personal Details Bitcoin Addresses Reports Referrals Advanced API Apps
User Settings
Email alice.one206@gmail.com
Password Change Password
Local currency United States Dollar (USD)
Time zone (GMT-08:00) Pacific Time (US
Bitcoin units BTC
Save Changes
Payment Page creates a public page to easily accept bitcoin payments
Display Name Alice Uno
Username
Then, she will click on the "Bitcoin Addresses" button.

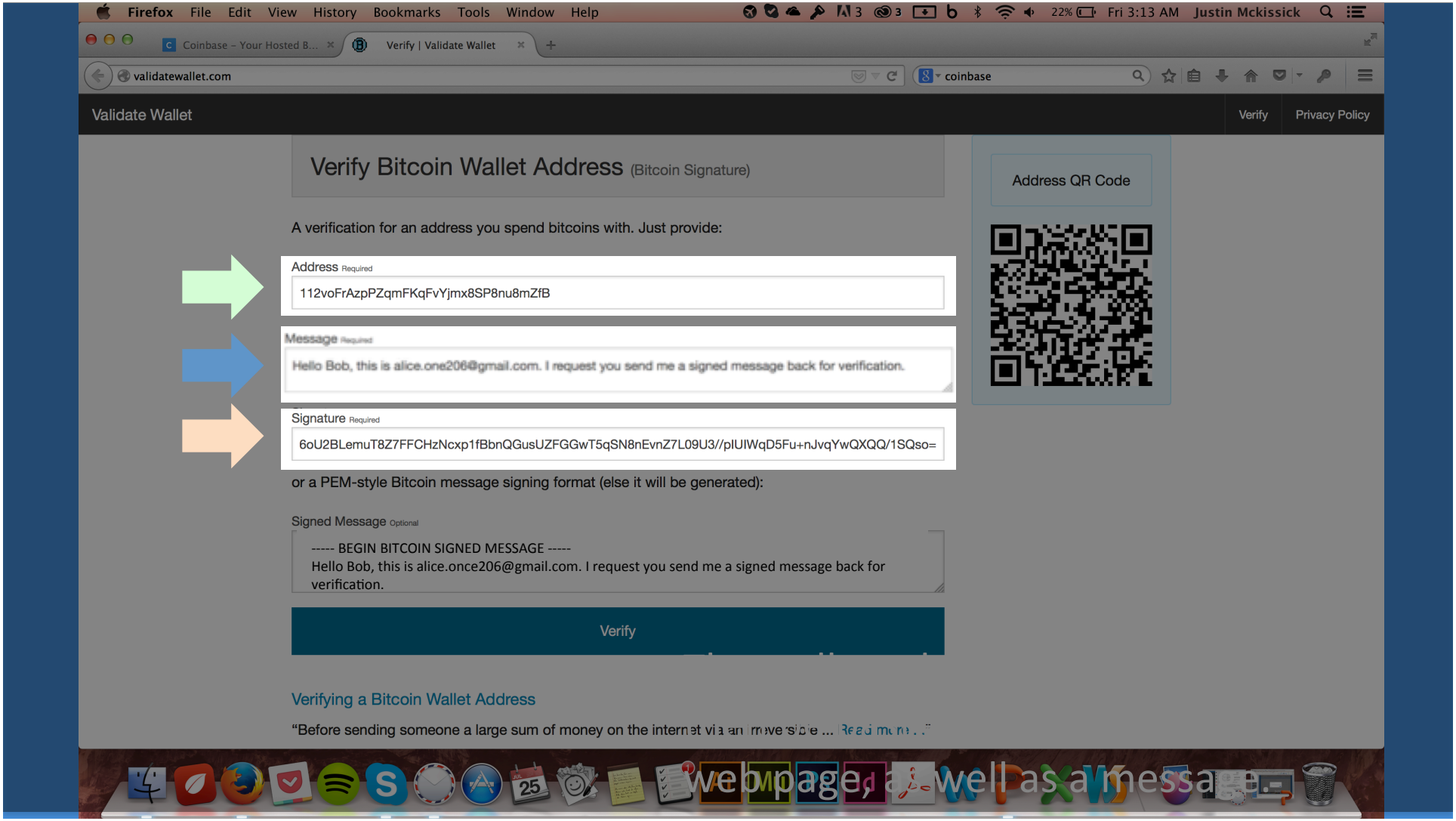

Firefox File Edit View History Bookmarks Tools Window Help
Fri 3:09 AM Justin Mckissick
Coinbase - Your Hosted B...
https://coinbase.com/addresses
coinbase
coinbase
Features Merchants Apps Vault Resources 0.0020546 BTC = 1.23 USD Alice Uno
Accounts
Buy/Sell
Merchants
Recurring
Verifications
Settings
Complete your profile
Next step: verify your bank account
Get the Coinbase App
Use Coinbase easily on your mobile device.
Settings Personal Details Bitcoin Addresses Reports Referrals Advanced API Apps
My Bitcoin Addresses
Your wallet on Coinbase is a collection of bitcoin addresses. New bitcoin addresses are automatically generated for each payment on Coinbase and stay associated with your account forever (so it is safe to reuse them).
You can add a label or callback URL to an individual address by clicking 'Edit'. Callback urls can be used to receive automated notifications when a payment arrives.
My Wallet (0.0020546 BTC)
bitcoin address or label
Filter
+ Create New Address
Address Label Callback URL Created
112voFrAzpPZqmFKqFvYjmx8SP8nu8mZfB Alice's Wallet about 2 hours ago Details
1DTn9DQKPJ7tuvE5hBZEcShmoPMMazdv4R about 2 hours ago Details
1AP5UmwkG1Y9UcCRE4FUukHeKNhiLnk77 about 2 hours ago Details
1KCETpLLBegtUyQBxRnm1UbhMaz1mtYPgH about 2 hours ago Details
Next, Alice will click on the "Details" button next to her wallet address.


Alice will then type in a message to be sent to Bob, and click the “Sign Message” button.
Firefox File Edit View History Bookmarks Tools Window Help
Fri 3:10 AM Justin Mckissick
Coinbase - Your Hosted B...
https://coinbase.com/addresses/53d2106ec10c6fe743000003
coinbase
Accounts
Buy/Sell
Merchants
Recurring
Verifications
Settings
Complete your profile
Next step: verify your bank account
Get the Coinbase App
Use Coinbase easily on your mobile device.
ANDROID APP ON Google play
Download on the App Store
Bitcoin Address
Back To All Addresses
Label
Alice's Wallet
Callback URL
http://www.example.com/callback
Save Changes
Cancel
View callbacks to this address
You can also see advanced details for this address and read more about callback URLs.
You can also sign a message with this address.
Sign a message
Enter Message
Hello Bob, this is Alice.
Sign Message
How can we help?

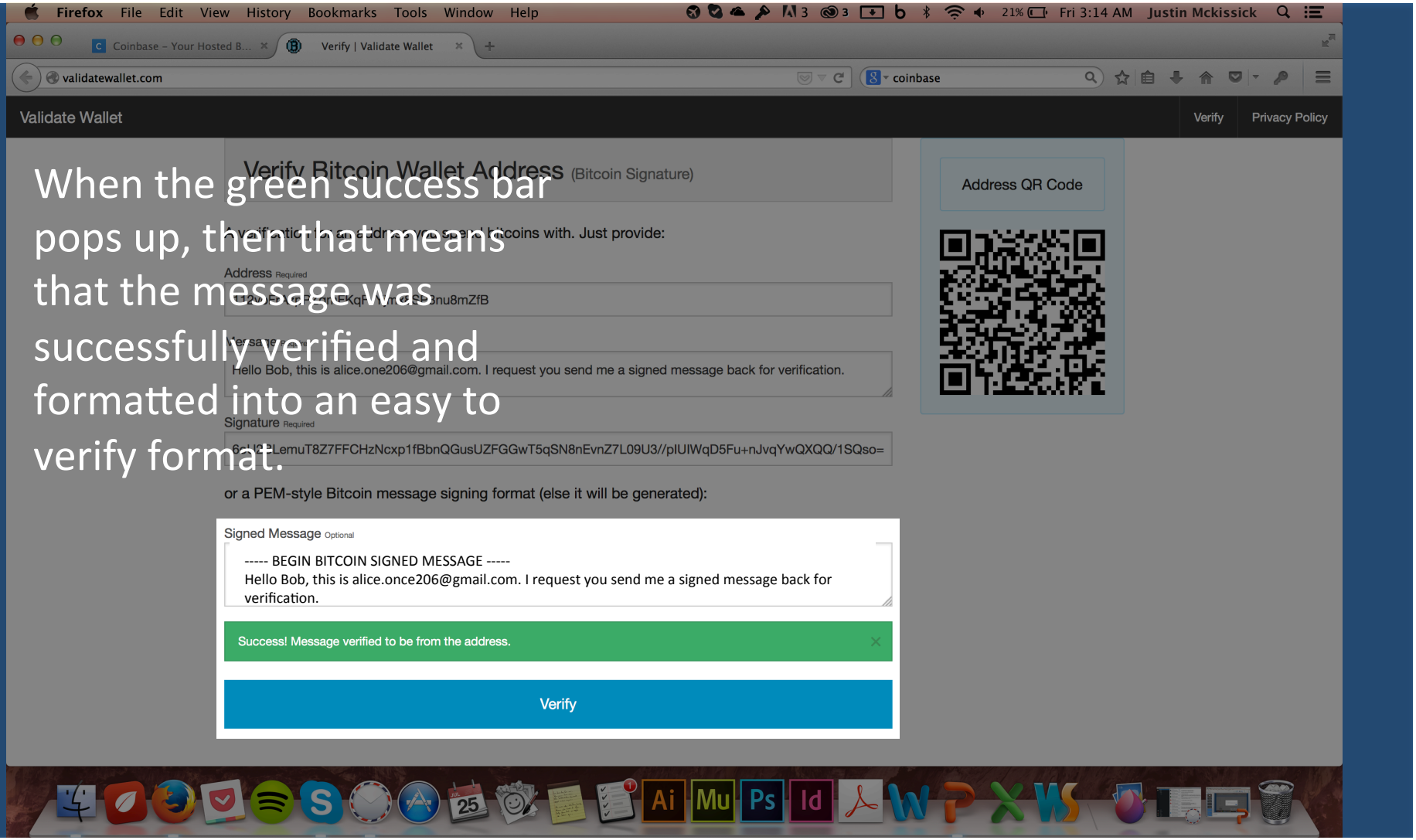


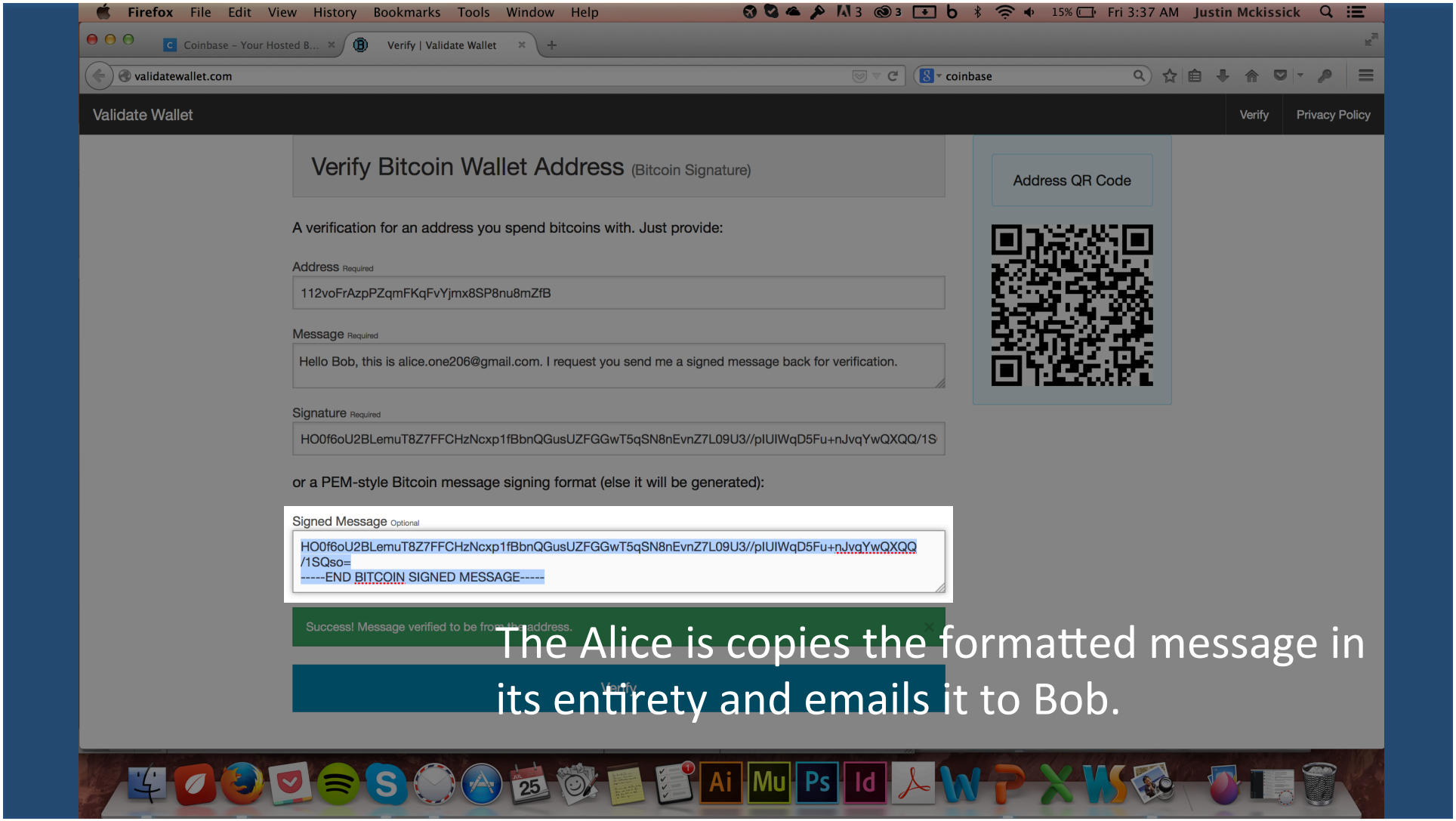
Alice will then take copy her wallet address, message and signature so she can format to be sent to Bob.


Firefox File Edit View History Bookmarks Tools Window Help
22% Fri 3:13 AM Justin Mckissick
Coinbase – Your Hosted B...
New Tab
validatewallet.com/
coinbase
Verify | Validate Wallet
validatewallet.com
Alice then types “http://www.validatewallet.com/” into her browser address bar.

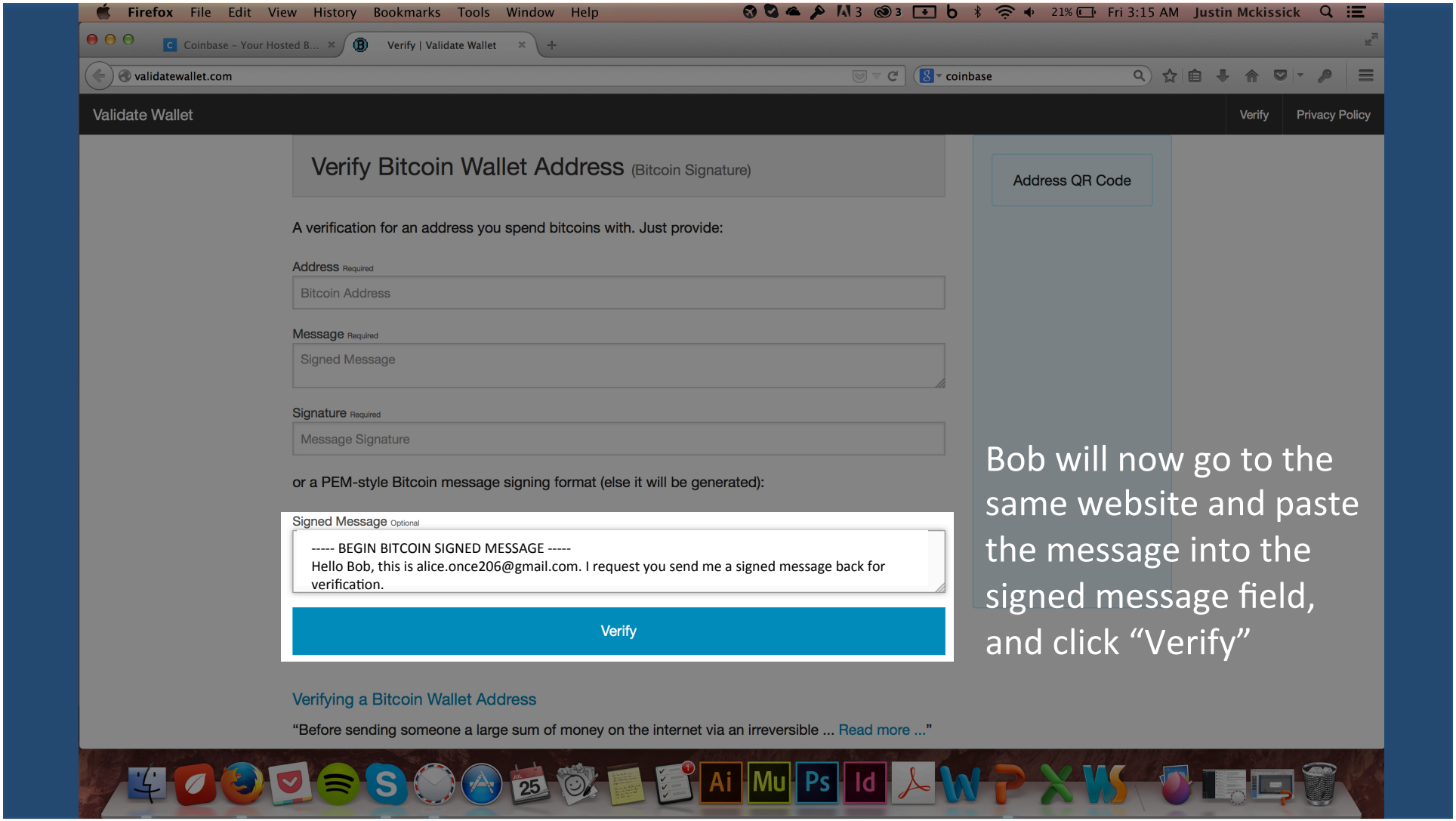

Firefox File Edit View History Bookmarks Tools Window Help
Fri 3:13 AM Justin Mckissick
Coinbase - Your Hosted B...
Verify | Validate Wallet
validatewallet.com
coinbase
Validate Wallet
Verify
Privacy Policy
Verify Bitcoin Wallet Address (Bitcoin Signature)
A verification for an address you spend bitcoins with. Just provide:
Address Required
112voFrAzpPZqmFKqFvYjmx8SP8nu8mZfB
Message Required
Hello Bob, this is alice.one206@gmail.com. I request you send me a signed message back for verification.
Signature Required
6oU2BLemuT8Z7FFCHzNcxp1fBbnQGusUZFGGwT5qSN8nEvnZ7L09U3//pIUIWqD5Fu+nJvqYwQXQQ/1SQso=
or a PEM-style Bitcoin message signing format (else it will be generated):
Signed Message Optional
----- BEGIN BITCOIN SIGNED MESSAGE -----
Hello Bob, this is alice.once206@gmail.com. I request you send me a signed message back for verification.
Verify
Address QR Code
Verifying a Bitcoin Wallet Address
"Before sending someone a large sum of money on the internet via an unknown site ... Read more..."
webpage, as well as a message

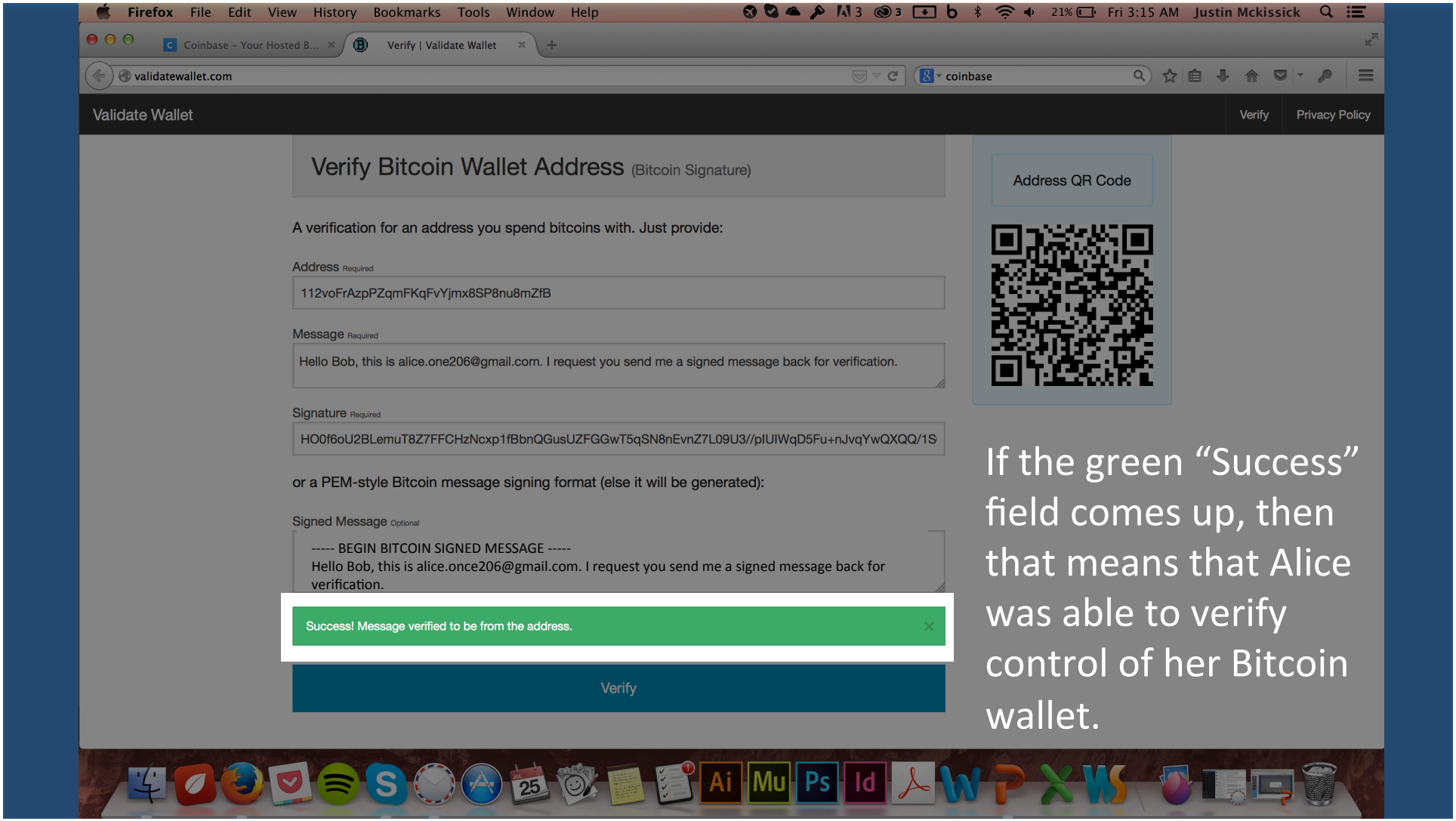
When the green success bar pops up, then that means that the message was successfully verified and formatted into an easy to verify format.





The Alice is copies the formatted message in its entirety and emails it to Bob.


Firefox File Edit View History Bookmarks Tools Window Help
Fri 3:15 AM Justin Mckissick
Coinbase – Your Hosted B...
Verify | Validate Wallet
validatewallet.com
coinbase
Validate Wallet
Verify
Privacy Policy
Verify Bitcoin Wallet Address (Bitcoin Signature)
A verification for an address you spend bitcoins with. Just provide:
Address Required
Bitcoin Address
Message Required
Signed Message
Signature Required
Message Signature
or a PEM-style Bitcoin message signing format (else it will be generated):
Signed Message Optional
----- BEGIN BITCOIN SIGNED MESSAGE -----
Hello Bob, this is alice.once206@gmail.com. I request you send me a signed message back for verification.
Verify
Address QR Code
Verifying a Bitcoin Wallet Address
"Before sending someone a large sum of money on the internet via an irreversible ... Read more ..."
Bob will now go to the same website and paste the message into the signed message field, and click "Verify"


Firefox File Edit View History Bookmarks Tools Window Help
Fri 3:15 AM Justin Mckissick
Coinbase – Your Hosted B...
Verify | Validate Wallet
validatewallet.com
coinbase
Validate Wallet
Verify
Privacy Policy
Verify Bitcoin Wallet Address (Bitcoin Signature)
A verification for an address you spend bitcoins with. Just provide:
Address Required
112voFrAzpPZqmFKqFvYjmx8SP8nu8mZfB
Message Required
Hello Bob, this is alice.one206@gmail.com. I request you send me a signed message back for verification.
Signature Required
HO0f6oU2BLemuT8Z7FFCHzNcxp1fBbnQGusUZFGGwT5qSN8nEvnZ7L09U3//pIUIWqD5Fu+nJvqYwQXQQ/1S
or a PEM-style Bitcoin message signing format (else it will be generated):
Signed Message Optional
----- BEGIN BITCOIN SIGNED MESSAGE -----
Hello Bob, this is alice.once206@gmail.com. I request you send me a signed message back for verification.
Success! Message verified to be from the address.
Verify
Address QR Code
If the green “Success” field comes up, then that means that Alice was able to verify control of her Bitcoin wallet.

"Now that Alice's information has been verified by Bob, Alice must verify Bob's information. This will occur in the exact same process as was just seen, just with Bob and Alice switching places. If both messages are verified, then Alice and Bob can be assured that both accounts are owned by one another."

Signed Message Verification Method

- ✓ Alice and Bob know now for sure they have the correct wallet addresses
- ✓ Both also know that the Bitcoin they send each other will be spendable
- ✓ Both Alice and Bob feel confident to transfer larger amounts of Bitcoin

To Conclude this Tutorial:

Using either method Alice's and Bob have the confidence to transfer Bitcoin in much higher amounts

Both accounts have been proven to be controlled by their respective owners, preventing any confusion or anxiety and ensuring a smooth and safe Bitcoin transfer