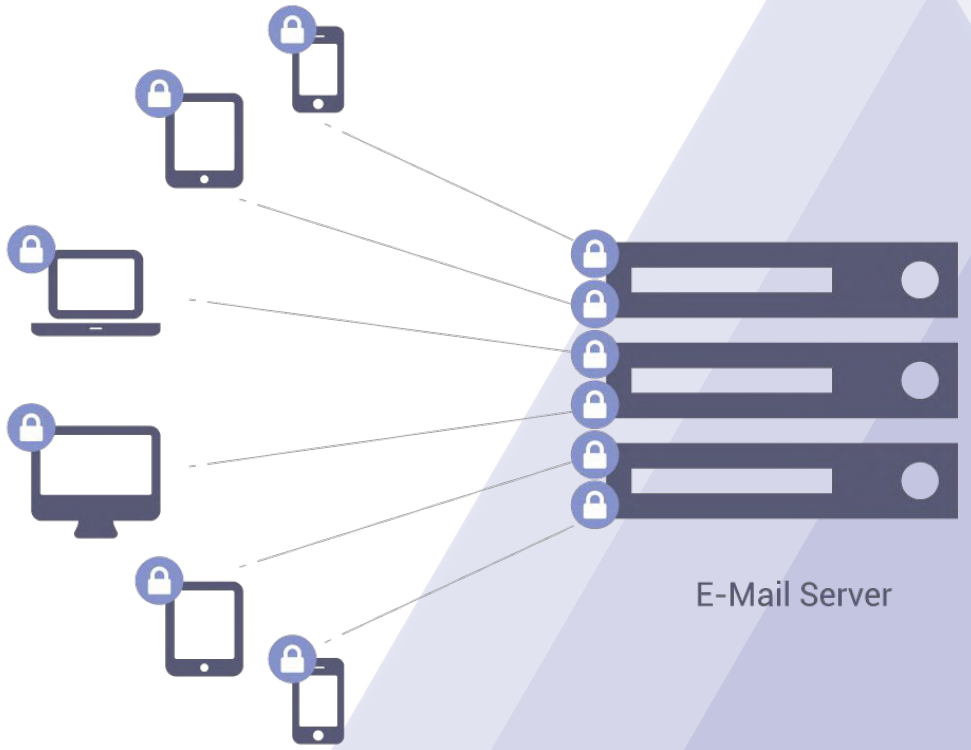
Securing ProtonMail:

Building a Web App that Doesn't Trust the Server

Daniel Huigens

What do we want to achieve?

- Allow you to trust that we can’t read your email
- Without trusting the server

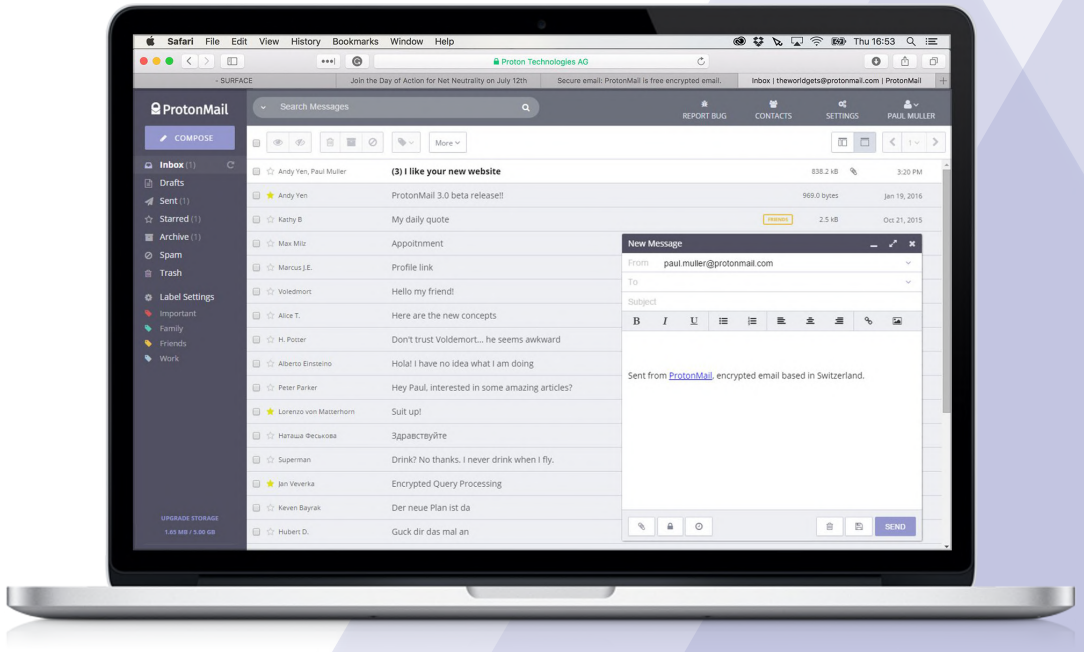


How does our web app work?

Normal web app	Our web app
Trust source code coming from the server	**?**
Send password to the server	Use **Secure Remote Password** protocol
Trust data coming from the server	**?**
Send data to the server **unencrypted**	Send data to the server **signed and encrypted** using OpenPGP

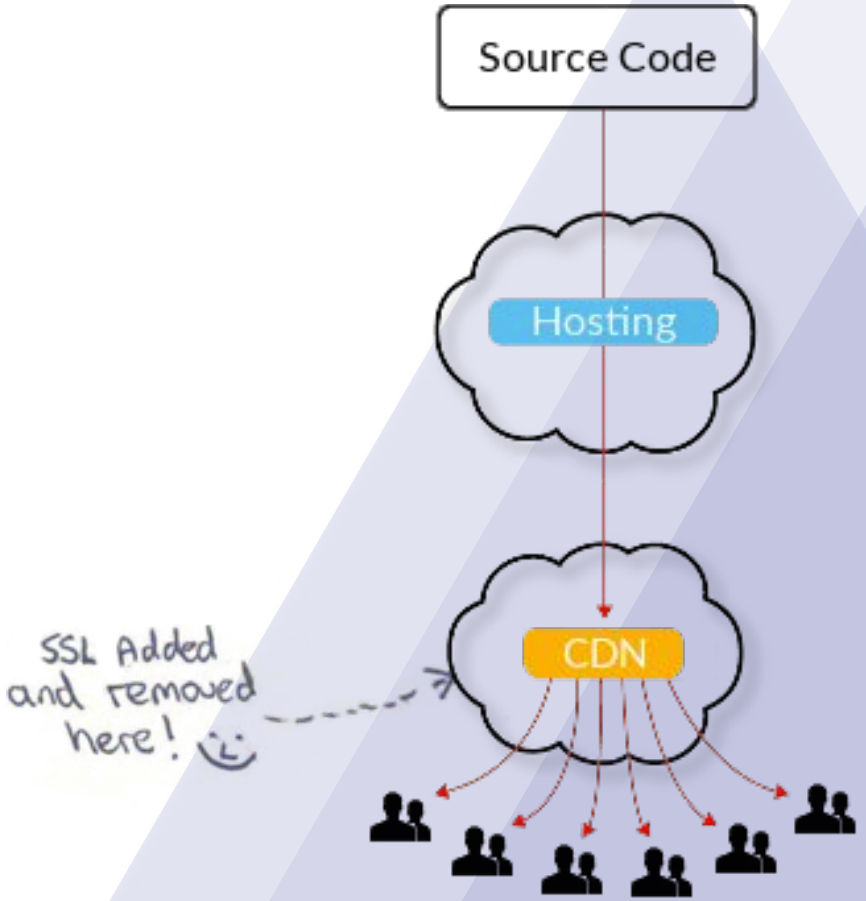
The JavaScript trust problem (I)

- HTML, CSS and JavaScript are sent to the browser each time
- The browser does what the server says
- Server says: send me the password



The JavaScript trust problem (II)

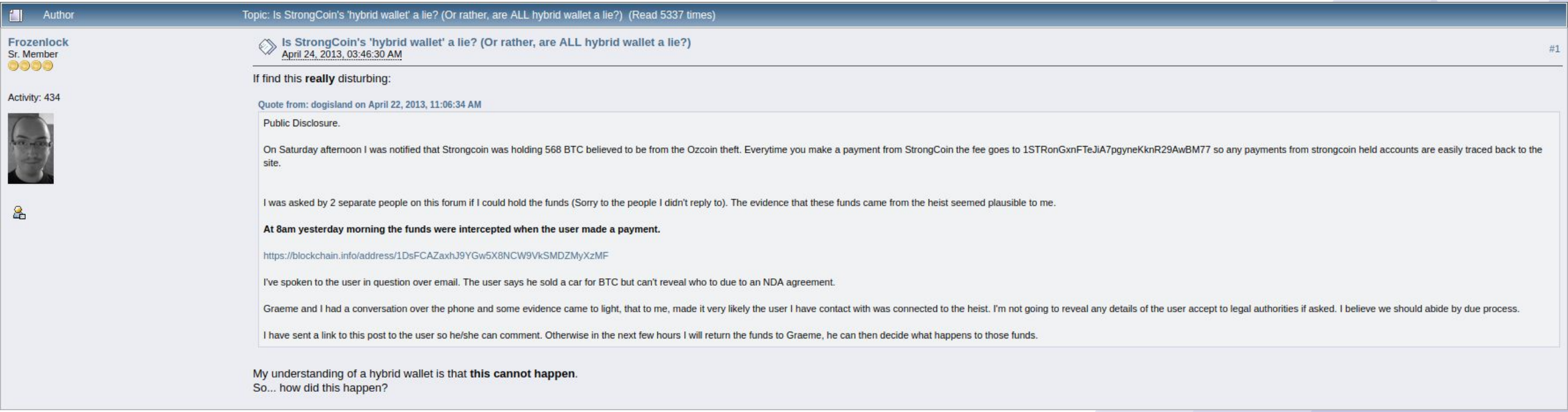
- Could be hacked or rogue:
  - Employee
  - Hosting
  - Content Delivery Network (if used)
  - National Security Agencies
  - Corporate Network



OzCoin Hacked, Stolen Funds Seized and Returned by StrongCoin

Apr 24, 2013 4:55 PM by Vitalik Buterin

“the funds were intercepted when the user made a payment ”



Author | Topic: Is StrongCoin's 'hybrid wallet' a lie? (Or rather, are ALL hybrid wallet a lie?) (Read 5337 times)

Frozenlock
Sr. Member

Activity: 434

Is StrongCoin's 'hybrid wallet' a lie? (Or rather, are ALL hybrid wallet a lie?)
April 24, 2013, 03:46:30 AM #1

If find this **really** disturbing:

Quote from: dogisland on April 22, 2013, 11:06:34 AM

Public Disclosure.

On Saturday afternoon I was notified that Strongcoin was holding 568 BTC believed to be from the Ozcoin theft. Everytime you make a payment from StrongCoin the fee goes to 1STRonGxnFTeJiA7pgyneKknR29AwBM77 so any payments from strongcoin held accounts are easily traced back to the site.

I was asked by 2 separate people on this forum if I could hold the funds (Sorry to the people I didn't reply to). The evidence that these funds came from the heist seemed plausible to me.

At 8am yesterday morning the funds were intercepted when the user made a payment.

https://blockchain.info/address/1DsFCAZaxhJ9YGw5X8NCW9VkSMDZMyXzMF

I've spoken to the user in question over email. The user says he sold a car for BTC but can't reveal who to due to an NDA agreement.

Graeme and I had a conversation over the phone and some evidence came to light, that to me, made it very likely the user I have contact with was connected to the heist. I'm not going to reveal any details of the user accept to legal authorities if asked. I believe we should abide by due process.

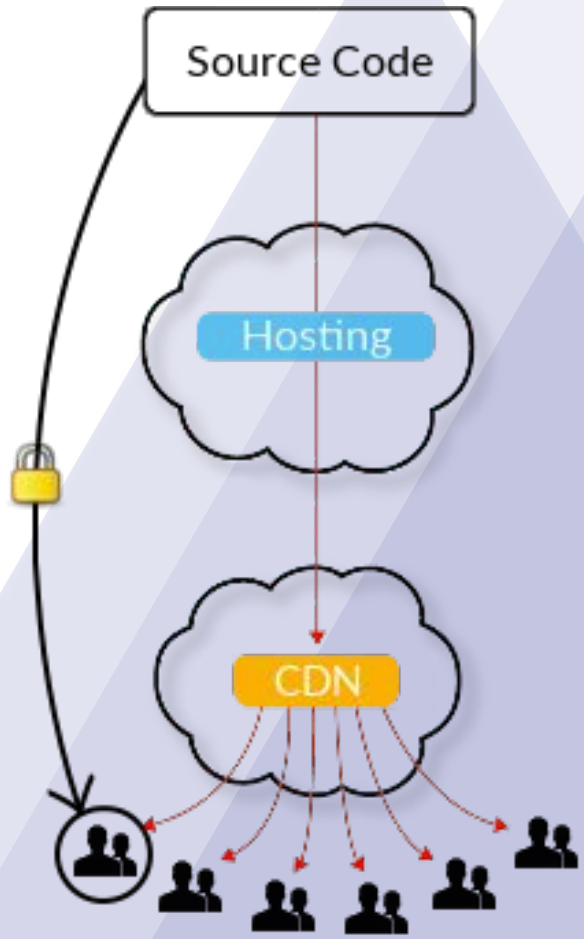
I have sent a link to this post to the user so he/she can comment. Otherwise in the next few hours I will return the funds to Graeme, he can then decide what happens to those funds.

My understanding of a hybrid wallet is that **this cannot happen**.
So... how did this happen?

“how did this happen? ”

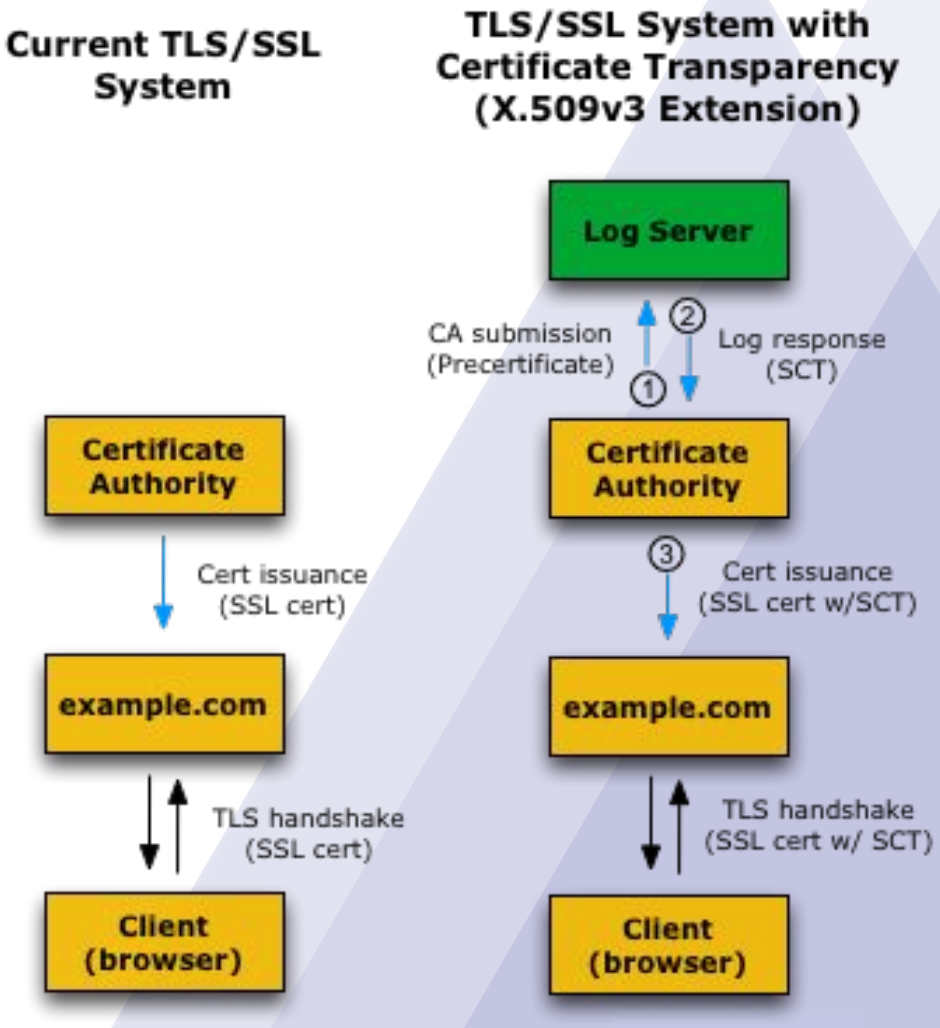
Source Code Transparency

- Hash the code at the source
- Publish it somewhere
- Verify that everyone gets the same code



Certificate Transparency

- Append-only log server
- Gives you Signed Certificate Timestamp
- Promises to publish the Certificate in the Log

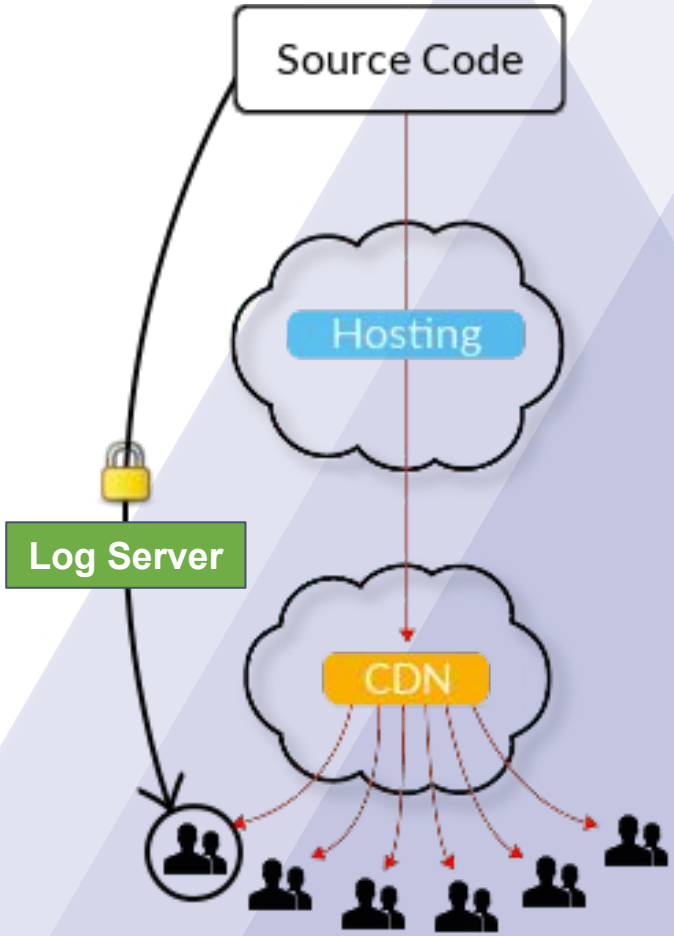


Service Workers

- Sit “between web app and server”
- Can read and block responses
- Can even detect updates to the Service Worker itself

All together now

- Certificate goes in the Log Server
- Able to verify that there's only one certificate
- Hash goes in the certificate
- ⇒ Everyone sees the same code



How will our web app work?

Normal web app	Our web app
Trust source code coming from the server	**Verify source code** coming from the server
Send password to the server	Use **Secure Remote Password** protocol
Trust data coming from the server	**?**
Send data to the server **unencrypted**	Send data to the server **signed and encrypted** using OpenPGP

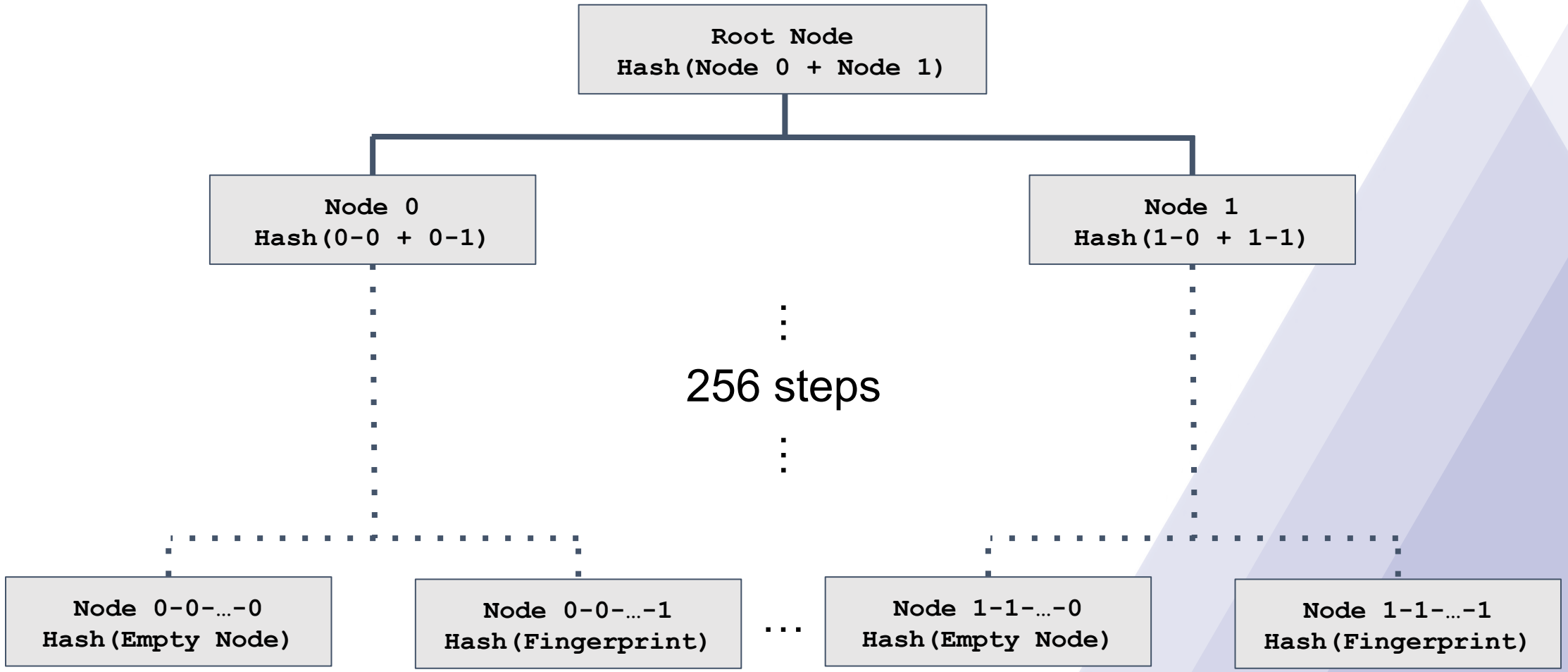
Key distribution solutions

- In-person exchange / verification
- Key Signing parties
- Web of Trust

Key Transparency

- Publish all keys
- Make sure that everyone sees the same keys
- Everyone checks their own key
- ⇒ All keys can be trusted

Merkle tree



[0-0-…-1, proof] == VerifiableRandomFunction(EmailAddress)

How will our web app work?

Normal web app	Our web app
Trust source code coming from the server	**Verify source code** coming from the server
Send password to the server	Use **Secure Remote Password** protocol
Trust data coming from the server	**Verify data** coming from the server
Send data to the server **unencrypted**	Send data to the server **signed and encrypted** using OpenPGP

Thanks! Questions?

Contact Us!

Daniel Huigens
Cryptography Engineer
d.huigens@protonmail.com
PGP Key ID: `F7D8FA8EC9D526EC`

ProtonMail

protonmail.com

news.ycombinator.com/user?id=protonmail

reddit.com/r/ProtonMail