

Bits on Bitcoin

A twist to verifying software releases

Justin Moore

Demo Day - April 5, 2019

Insight Decentralized Consensus '19

The cybersecurity industry is booming!

\$ 3.5 billion industry in 2004

\$ 120 billion industry in 2017

35X in 13 years.

Hackers dropped a secret backdoor in Asus' update software

Zack Whittaker @zackwhittaker · 2 weeks ago

Generate

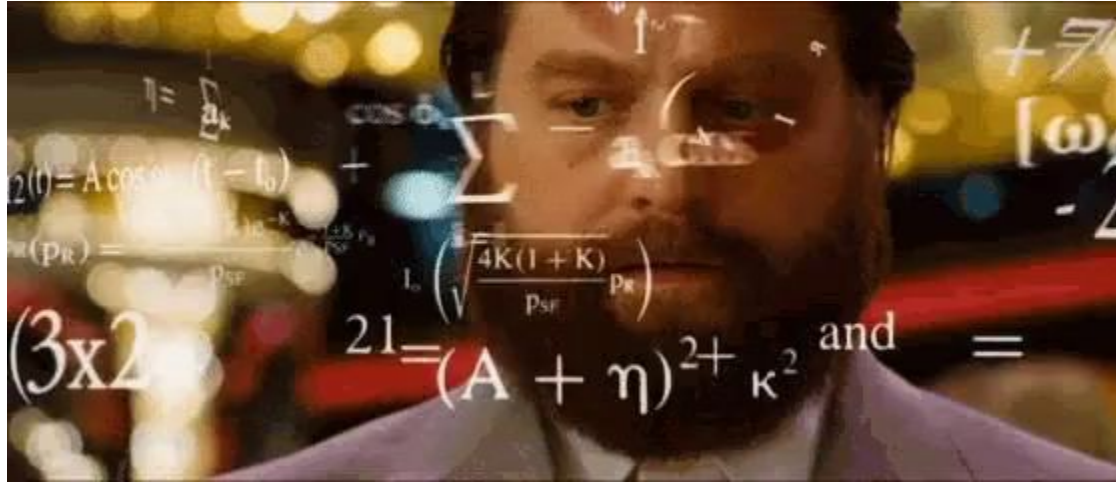


```
...width="16" height="16"></img></div>
...sa name="117" href="#117">117</a>
...title='Generate HTML widget' href=
...height="16"></img></a></div><pre>
...<span class="kw">void</span>&nbsp;<a class="con
...@jdkSopenjdk@6-b14@java$util@Rando
...atic/app/images/1x1.gif" border='0'
...<span class="kw">long</span>&nbsp;<span>
...</span>&nbsp;</pre></div><div class=
...name="ln" class="ln" onmouseover="tr
...],define: ["lnmr" id="lnmr-118" onmouseover="
...on hide:90(118); return false;"><img id="ln
...empty head&nbsp;<span class="mark-700"
...cheduleMark(this);" onmouseout="unsche
...out="unscheduleMark(this);"><a href
...ler" title="long multiplier" class=
...out="unscheduleMark(this);"><a href
...</span></pre></div><div class="li
...name="ln" class="ln" onmouseover="t
...class="lnmr" id="lnmr-119" onmouseover=
...SpilletDialog(119); return false;"><img id="l
```

Hack: How Used a Tiny Infiltrate U.S. Companies

The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources.

Wait, what? Something doesn't add up.



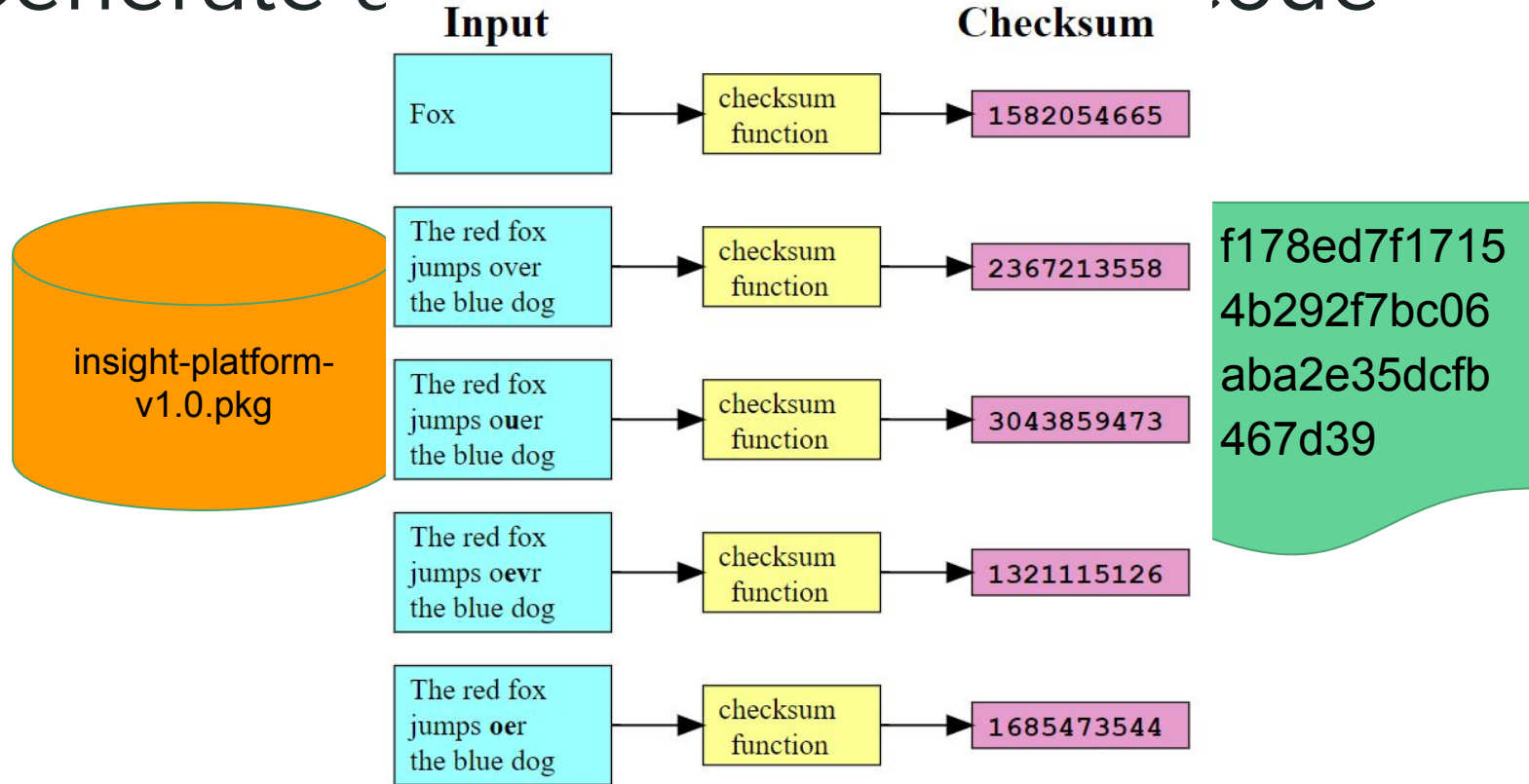
One report predicts as high as \$6 trillion in cybercrime damages by 2021.

Maybe we need to build on a new, secure foundation.



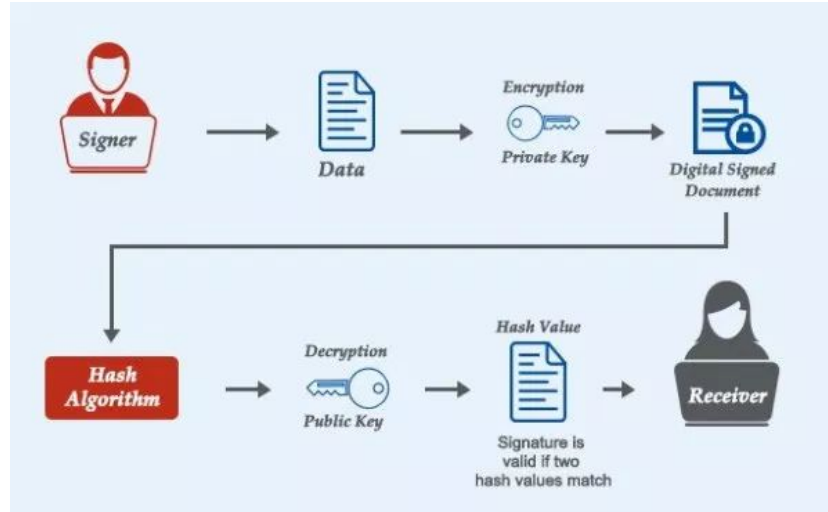
But first,
let's talk about checksums.

Generate a checksum of your code



So this proves data integrity,
but what does it say about data security?

Let's talk about digital signatures



There's nothing wrong with this approach.

... or is there?

How many of you have verified both

- ❑ a checksum
- ❑ a gpg signature

before installing an application?



Right.

So we have this security mechanism, but hardly anyone actually performs these operations.



Demo

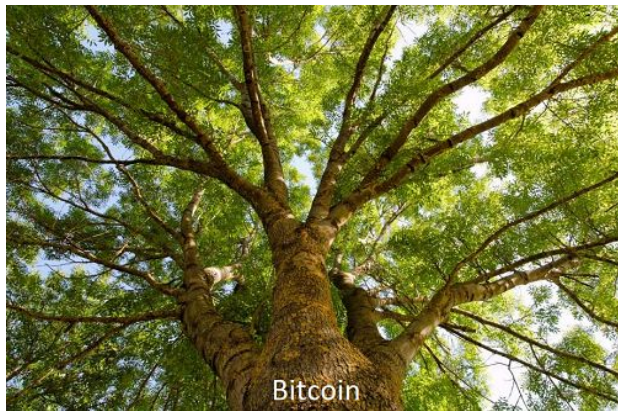
About Me - Justin P. Moore



B.S. Computer Science and Physics



M.S. Astrophysics, Ph.D. Candidate



Step 1:

Create a specific Bitcoin address and load with UTXOs

How about using

1DCSVhKLR6jyaGa7PGaBmXj5NFtZGe39uG

which I mined.

DCSV - Decentralized Consensus Silicon Valley

Step 2:

Developer computes shasum and then pays small fee* to write data to the chain.

*small fee = 550 satoshis (\$0.03 on BTC)
less on other forks

MultiSig

Given most dev teams are $n > 1$ you could imagine releases being multisig transactions requiring m-of-n signatures before becoming official.

Incorporate this into the installation process

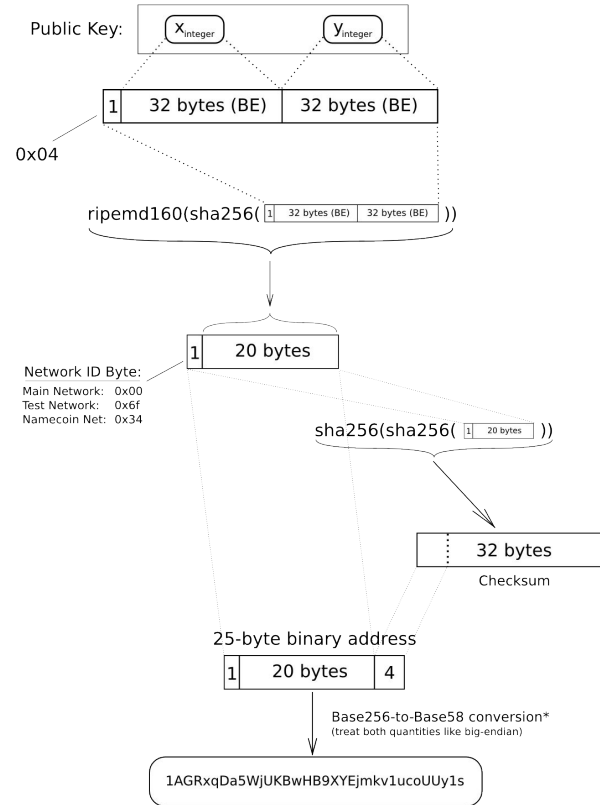
What if the application could check its own signature against what's at a specific location on the chain such that it won't continue installing without that information.

Think of it as an self-integrity check before installing.

Something like this could also potentially be used for software licensing and key management.

Elliptic-Curve Public Key to BTC Address conversion

ECC PK to BTC 1addr



*in a standard base conversion, the 0x00 byte on the left would be irrelevant (like writing '052' instead of just '52'), but in the BTC network the left most zero chars are carried through the conversion. So for every 0x00 byte on the left end of the binary address, we will attach one '1' character to the Base58 address. This is why main-network addresses all start with '1'

Checksum Example



Via Direct Download

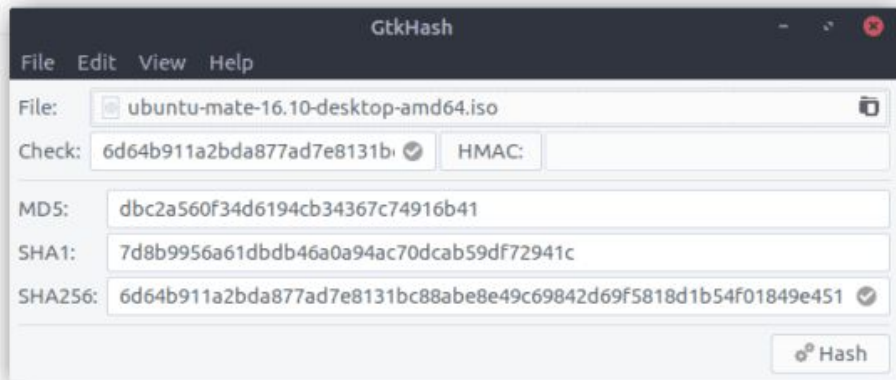
If preferred, you can also download the images over HTTP.

 [ubuntu-mate-16.10-desktop-amd64.iso](#)


Download Size: 1.7 GB

SHA256 Checksum: `6d64b911a2bda877ad7e8131bc88abe8e49c69842d69f5818d1b54f01849e451`

 [How to verify downloads](#)



NodeJS (Checksum + Signature)






HOME | ABOUT | DOWNLOADS | DOCS | GET INVOLVED | SECURITY | NEWS | FOUNDATION

Downloads

Latest LTS Version: **10.15.3** (includes npm 6.4.1)

Download the Node.js source code or a pre-built installer for your platform, and start developing today.

LTS Recommended For Most Users	Current Latest Features	
 Windows Installer node-v10.15.3-x86.msi	 macOS Installer node-v10.15.3.pkg	 Source Code node-v10.15.3.tar.gz

NodeJS

Additional Platforms

SmartOS Binaries

64-bit

Docker Image

Official Node.js Docker Image

Linux on Power Systems

64-bit

Linux on System z

64-bit

AIX on Power Systems

64-bit

- Signed SHASUMS for release files (How to verify)

NodeJS

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

f2f018418b6bfa263ec981f04f3fa5337724edae8d77fc3951cd36667ee720ea
7a5eaa1f69614375a695cc62017248e5dcd15b0b8edf47db5b52997cf992ba
8e3df823a58c7b2de327540ab57a9bcf3f706108fe65c4cde9a073caa68cee
9e97ee69072836bf2a85c4af627ed152574c30c5a32e40fbfcdffa8d9b562e
f690b880cccfb5959436073717b648e4bdc521e3217ab7092d5c03326f6133
c82cd99e01f6e26830f0b3e0465f1f292957ebd69a68c91c03228c2669104359
3d7abbf64bfb07c55168ca0f1c17be12b0d93affe9b6cadd39724649215fab9
72529b6f77d95f9422f6d1c6b88c1f921b00e5500alc3ea05927f1ae3704133d
94432c2944fc78c2d5e82103f73596a060451330839562c04c414067007c5997
6958551264884cd479f15ed8d40673655a283ed3bd8552d04e8531cd3ccdc483
af2106b08f68e0884caa505ea7e695facc5b4cd356f1e08258899e94cc4c5df0
0544b08467384ba3ba462d8907d12cea71ac371f3d118057905dd845be43aad
a2fcc2e1827d7a034f39aad8225b4dd72376ad19f7a7884645a512aeedf4ab5
073e6e2ad4e3a7580d87e5b70b9c1ce785b15e849dfd4f2f846c3039ad1e116c
545caa31bf06b150861ca3a2b1f5112aa92bb855de20fd98f8b7bc3f4c4311d7
6c35b85a7cd4188ab7578354277b2b2ca43eacc864a2a16b3669753ec2369d52
faddbe418064baf2226c2fcbd038c3ef4ae6f936eb952a1138c7ff8cfe862438
f4d0b944618aef2835b500e0cc1c5a013912597f5ce5560cd4bcb534f5270754
c678b8e5a2d652f920c1093e6249b08e4746c2d37a5b9f719d04f3243776fb01
3732ae66ad564c192ff3a4a6e66e0d8922823c128bb8a6766ece87226982ad54
db460a63d057ac015b75bb6a879fcbe2fefaa22afa4b6f6445b9db61ce2270d
4e22d926f054150002055474e452ed6cbb85860aa7dc5422213a2002ed9791d5
9df98cac063229aca443c040fd342a96667891bb8eda821d10aa4d49347d7add
93c881fcd0455a932dd5b506a7a03df27d9f63615c1d3f351ebfa4e20bf1c0d
597a372964252daaba4cb8d8ac57305f79cffeeca579625f0cd6ab85d29ccdda
fc28bbd08b3d9b621c7e0ecd2b42506ca2f356f31f2b64210f413b34cfff31799
46b3d03c96de0b9e7d3a204c67772759283221f5e58ac225df813076a65e2738
e73398cde3e054da7a0a0586aa512a47a24b961b0659be30af01606ca234a9
a921dl4afa63e877087b3f25abd0ab05b63489bffc9ff47acbbee4e1b7494
4ed045aelba046506948b8f90c02716178cb0084f3b56866ac8d2b3591e83235
538c8cc4e0b93facb9d63ed6c55d765ec33a18dd264c6c8b9415ad242521d8e6
525ea4adf5c16607b273db6c0803283c57c4116fce56229ce87c8eb9fodd25
39efb2a884d2f73680b986534eed000017cel6993ea9d695351593fbb9a7bb34
efed715422fcb7032290ec3c7e3b324126e082ee3a87d6ac497f6c97549e478e
38775185b6fc090e7039ea0b3e630f4ab83e5c259d8d94f0f35f04ec12c0e98
1848e05e130dda3c3b53830cb78c4b28c137c7aac0890b70a8c863798c332ed5

-----BEGIN PGP SIGNATURE-----

iQEsBAEBCAAdFiEETtd49TnjY0x3nIfG1wYoSKGrAFwFAlx+rpcACgkQ1wYoSKGr
AFzn6Q/eLpFexv+SahnPg8ChYib9GKqNejKewh9f/DOZ6vSj2N0d35bjoKcK
/p1FRNIdfsZ8ZqhVd4LQeNBxYVgdyRTM7zA6oLuN2wCxjuK0vwn0Zog/LnLnEa15
bLAWdJJs3EmwvHhZnQuj2t1XPQDR+cBosuEArSoulqSgUfw53x4eyJDSNeE77
944xFi7uob828J2wMbM1L5w0MHIRgqs9ptDHEigERGW4fAkKXhpeT9gT9IgFzx
10PQH5oD5z7dZEwo19GfOVZsR0kGf89VVK6y+b/n8Sq4mG6x5LZKL+CecEofCr7
pVileZXVzWQnVbdsTPXHNf/o0AHuCuw==
=X9UW
-----END PGP SIGNATURE-----

node-v10.15.3-aix-ppc64.tar.gz
node-v10.15.3-darwin-x64.tar.gz
node-v10.15.3-darwin-x64.tar.xz
node-v10.15.3-headers.tar.gz
node-v10.15.3-headers.tar.xz
node-v10.15.3-linux-arm64.tar.gz
node-v10.15.3-linux-arm64.tar.xz
node-v10.15.3-linux-armv6l.tar.gz
node-v10.15.3-linux-armv6l.tar.xz
node-v10.15.3-linux-armv7l.tar.gz
node-v10.15.3-linux-armv7l.tar.xz
node-v10.15.3-linux-ppc64le.tar.gz
node-v10.15.3-linux-ppc64le.tar.xz
node-v10.15.3-linux-s390x.tar.gz
node-v10.15.3-linux-s390x.tar.xz
node-v10.15.3-linux-x64.tar.gz
node-v10.15.3-linux-x64.tar.xz
node-v10.15.3.pkg
node-v10.15.3-sunos-x64.tar.gz
node-v10.15.3-sunos-x64.tar.xz
node-v10.15.3.tar.gz
node-v10.15.3.tar.xz
node-v10.15.3-win-x64.7z
node-v10.15.3-win-x64.zip
node-v10.15.3-win-x86.7z
node-v10.15.3-win-x86.zip
node-v10.15.3-x64.msi
node-v10.15.3-x86.msi
win-x64/node.exe
win-x64/node.lib
win-x64/node_pdb.7z
win-x64/node_pdb.zip
win-x86/node.exe
win-x86/node.lib
win-x86/node_pdb.7z
win-x86/node_pdb.zip

NodeJS

Source Code

[node-v10.15.3.tar.gz](#)

Additional Platforms

SmartOS Binaries

64-bit

Docker Image

[Official Node.js Docker Image](#)

Linux on Power Systems

64-bit

Linux on System z

64-bit

AIX on Power Systems

64-bit

- [Signed SHASUMS for release files](#) ([How to verify](#))

NodeJS

Verifying Binaries

Download directories contain a `SHASUMS256.txt` file with SHA checksums for the files.

To download `SHASUMS256.txt` using `curl`:

```
$ curl -O https://nodejs.org/dist/vx.y.z/SHASUMS256.txt
```

To check that a downloaded file matches the checksum, run it through `sha256sum` with a command such as:

```
$ grep node-vx.y.z.tar.gz SHASUMS256.txt | sha256sum -c -
```

For Current and LTS, the GPG detached signature of `SHASUMS256.txt` is in `SHASUMS256.txt.sig`. You can use it with `gpg` to verify the integrity of `SHASUMS256.txt`. You will first need to import [the GPG keys of individuals authorized to create releases](#). To import the keys:

```
$ gpg --keyserver pool.sks-keyservers.net --recv-keys DD8F2338BAE7501E3DD5AC78C273792F7D83545D
```

See the bottom of this README for a full script to import active release keys.

Next, download the `SHASUMS256.txt.sig` for the release:

```
$ curl -O https://nodejs.org/dist/vx.y.z/SHASUMS256.txt.sig
```

Then use `gpg --verify SHASUMS256.txt.sig SHASUMS256.txt` to verify the file's signature.