

Fujitsu, Oct. 11, 2016

Proving Bitcoin Solvency

Dan Boneh
Stanford University

Joint work with

Gaby Dagher, Benedikt Bunz, Joe Bonneau, and Jeremy Clark

... but first: Computer Security at Stanford



Alex Aiken

software analysis



Dan Boneh

applied Crypto,
web security



David Dill

verification and
secure Voting



Dawson Engler

static analysis

David Mazières

Op. Systems



Phil Levis

IoT Security



John Mitchell

protocol design,
online ed.



Mendel Rosenblum

VM' s in security



Security events at Stanford

- Annual security workshop
[//forum.stanford.edu/events/2016security.php](http://forum.stanford.edu/events/2016security.php)
 - Security seminar
[//crypto.stanford.edu/seclab/sem.html](http://crypto.stanford.edu/seclab/sem.html)
-
- Computer security courses
[//seclab.stanford.edu/](http://seclab.stanford.edu/)
 - Stanford Advanced Computer Security Certificate
[//scpd.stanford.edu/computerSecurity/](http://scpd.stanford.edu/computerSecurity/)

New Bitcoin course

➤ Courses:

- CS55N (freshmen seminar): ten ideas in computer security

- CS155: Computer Security

- new** • **CS251: Blockchain technologies: Bitcoin and friends**

- CS255: Intro to Crypto

- CS259: Security analysis of network protocols

- CS355: Graduate course in cryptography

➤ Stanford Advanced Computer Security Certificate

<http://scpd.stanford.edu/computerSecurity/>

New Bitcoin course

➤ Courses:

- CS55N (freshmen seminar): ten ideas in computer security

- CS155: Computer Security

- new** • **CS251: Blockchain technologies: Bitcoin and friends**

- CS255: Intro to Crypto


- CS259: Security analysis of network protocols

Try our homeworks and projects








➤ Sta

Online Courses

//www.coursera.org/learn/crypto



The header features a red background. On the left is a small image of a silver padlock. To its right, the text "Stanford University" is in orange and "Cryptography" is in white.

-  Home
-  Problem Sets
-  Video Lectures
-  Lecture Slides
-  Discussion Forums
-  Course Overview
-  Course Syllabus

Latest Updates

Subtitles
Help your fellow students by improving our subtitles and adding translations! You can contribute at [our project page](#).

Course Announcements

[Edit Announcement](#)

Week 3 [lectures](#) and [problem sets](#) are now available. The problem set is due on April 9th. This week there is also an extra credit programming assignment.

Week 2 [lectures](#) and [problem sets](#) are now available. The problem set is due on April 2nd.

About the programming projects: I received many messages from students who want to take the class, but cannot program. As a result, we plan to treat all programming projects as **extra credit**. Everyone who completes all the non-programming problem sets will receive a statement of accomplishment. Students who, in addition, also complete the programming projects will receive a statement saying that they completed the extra credit programming assignments in the course.

Course open to the public

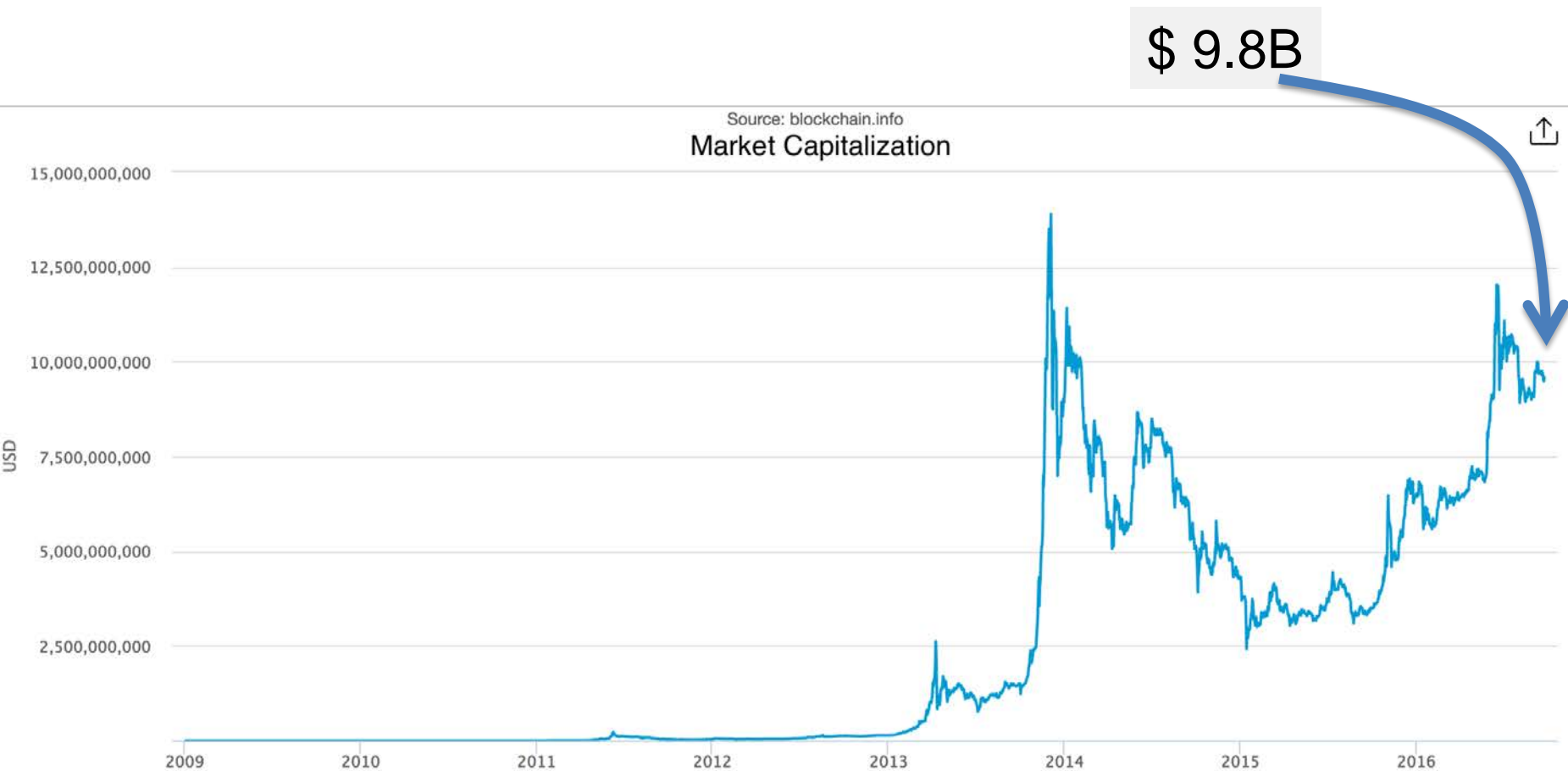
Proving Bitcoin Solvency

Dan Boneh
Stanford University

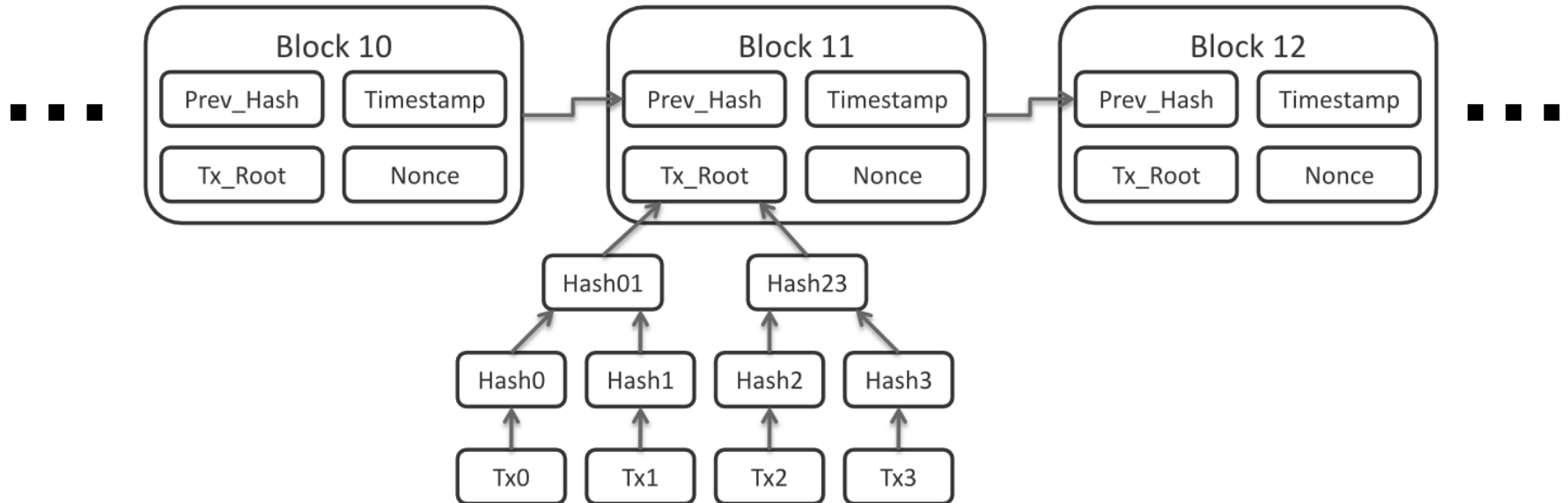
Joint work with

Gaby Dagher, Benedikt Bunz, Joe Bonneau, and Jeremy Clark

Bitcoin: first successful crypto currency



More than a currency: the blockchain



Non-currency applications:

- Document management --- ensuring freshness
- Asset management

Solvency trouble

Technology | Fri Feb 28, 2014 2:30pm EST

Mt. Gox files for bankruptcy, hit with lawsuit

TOKYO | BY YOSHIFUMI TAKEMOTO AND SOPHIE KNIGHT



Solvency trouble



Mt. Gox:
lost roughly US\$450M
Subsequent price
crash

~50% have failed!
[Moore, Christin 2013]

Bitcoin: ensuring solvency

The problem: a Bitcoin “exchange” has:

- ***obligations*** to customers, and
- ***assets*** that it holds (knows secret key for assets)

Goal: prove ***assets*** \geq ***obligations*** (solvency)
without revealing any info about assets or obligations
(i.e., a zero-knowledge proof)



Dagher-Bunz-Bonneau-Clark-Boneh (ACM CCS 2015) :
an efficient zero-knowledge protocol for this problem

Running protocol daily would have detected Mt. Gox troubles early

How?

Sub-protocol 1: create commitment **O** to total obligations:

- Commitment is binding, but reveals nothing about obligations
- Every user is given a secret key that lets it verify that its account balance is (uniquely) included in total sum

Sub-protocol 2: create commitment **A** to total assets:

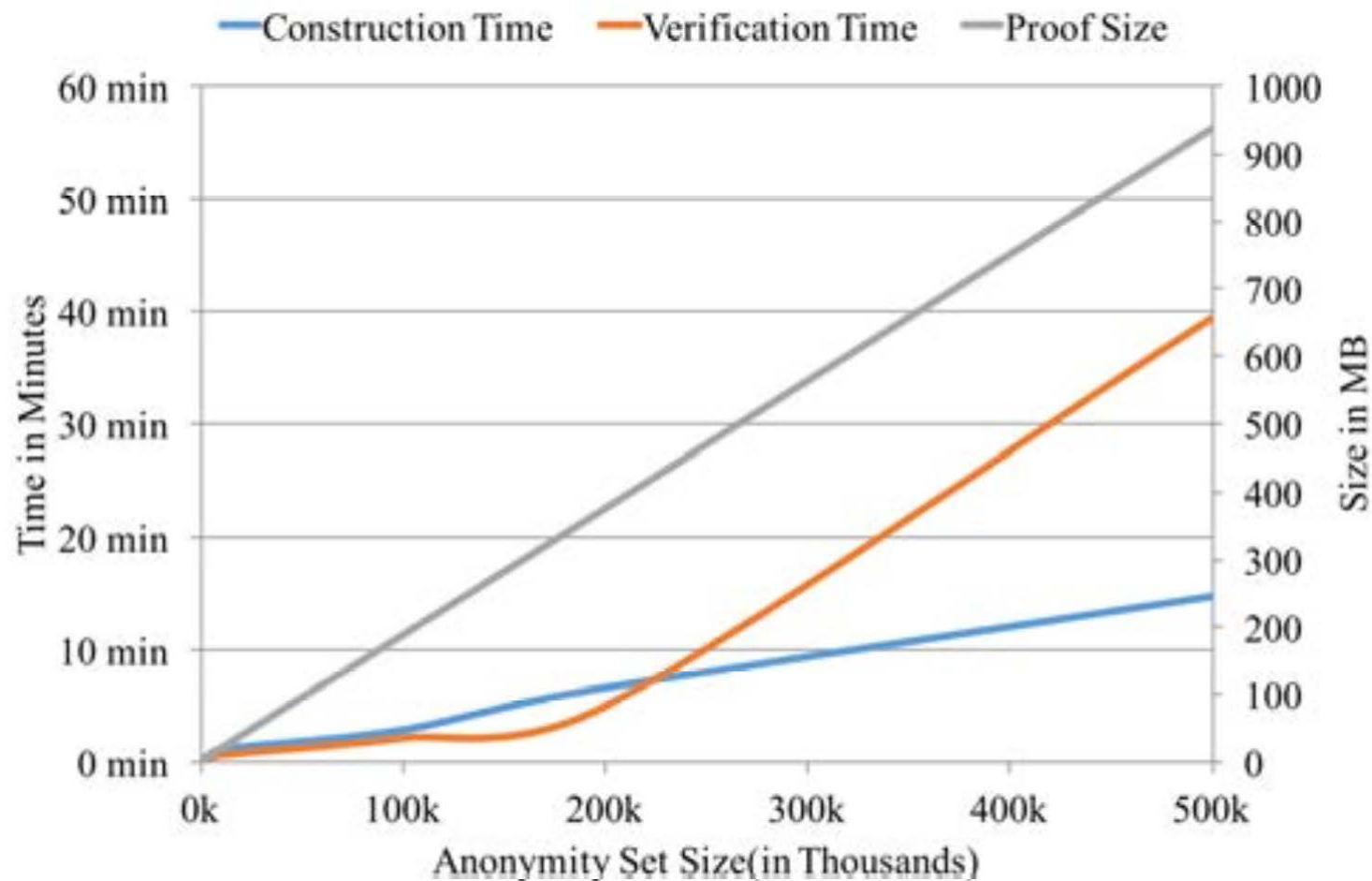
- Let pk_1, \dots, pk_n be public keys (addresses) on the block chain
- The exchange knows **sk** for a **subset** of these addresses
- Exchange proves:

sum of balances for which it knows **sk** is $\text{value}(\mathbf{A})$

nothing is revealed about which addresses the exchange owns

Sub-protocol 3: prove $\text{value}(\mathbf{A}) \geq \text{value}(\mathbf{O})$

Experiments



Deployment

- Open source
- Supporting cold storage:



- An exchange stores the bulk of its assets in cold storage
⇒ cannot use assets in a daily solvency proof
- Solution: valet key (“blinding” of secret key)
sufficient for proof of solvency, but not to spend funds

THE END