Intro to Crypto* and Cryptocurrencies, Past and Present

CMSC 23280/ECON 23040, Autumn 2018
Lecture 1

David Cash, Harald Uhlig, Ben Zhao

University of Chicago

*In my lectures, “Crypto” means “Cryptography”!

October 31, 2008

An unusual anonymous email was sent to the metzdowd cryptography list:

Satoshi Nakamoto <satoshi@vistomail.com> Oct 31, 2008, 1:10 PM

to cryptography

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

https://bitcoin.org/bitcoin.pdf

October 31, 2008

An unusual anonymous email was sent to the metzdowd cryptography list:

Satoshi Nakamoto <satoshi@vistomail.com> Oct 31, 2008, 1:10 PM
to cryptography

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

[redacted] Nov 2, 2008, 5:46 PM
to satoshi, cryptography

Satoshi Nakamoto wrote:
> I've been working on a new electronic cash system that's fully
> peer-to-peer, with no trusted third party.
>
> The paper is available at:
> http://www.bitcoin.org/bitcoin.pdf

We very, very much need such a system, but the way I understand your proposal, it does not seem to scale to the required size.

For transferable proof of work tokens to have value, they must have monetary value. To have monetary value, they must be transferred within a very large network - for example a file trading network akin to bittorrent.

[redacted] Nov 3, 2008, 7:32 AM
to cryptography, satoshi

> As long as honest nodes control the most CPU power on the network,
> they can generate the longest chain and outpace any attackers.

But they don't. Bad guys routinely control zombie farms of 100,000 machines or more. People I know who run a blacklist of spam sending zombies tell me they often see a million new zombies a day.

This is the same reason that hashcash can't work on today's Internet -- the good guys have vastly less computational firepower than the bad guys.

I also have my doubts about other issues, but this one is the killer.

January 8, 2009

Bitcoin v0.1 released crypto list ×

Satoshi Nakamoto <satoshi@vistomai… Thu, Jan 8, 2009, 1:27 PM
to cryptography

Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority.

See bitcoin.org for screenshots.

Download link:
http://downloads.sourceforge.net/bitcoin/bitcoin-0.1.0.rar

Windows only for now. Open source C++ code is included.

- Unpack the files into a directory
- Run BITCOIN.EXE
- It automatically connects to other nodes

Note: Do **not** trust anonymous emails asking you to run FILE.EXE…

The early years: 2009-2010

1. Satoshi Nakamoto communicates regularly, involved with software development

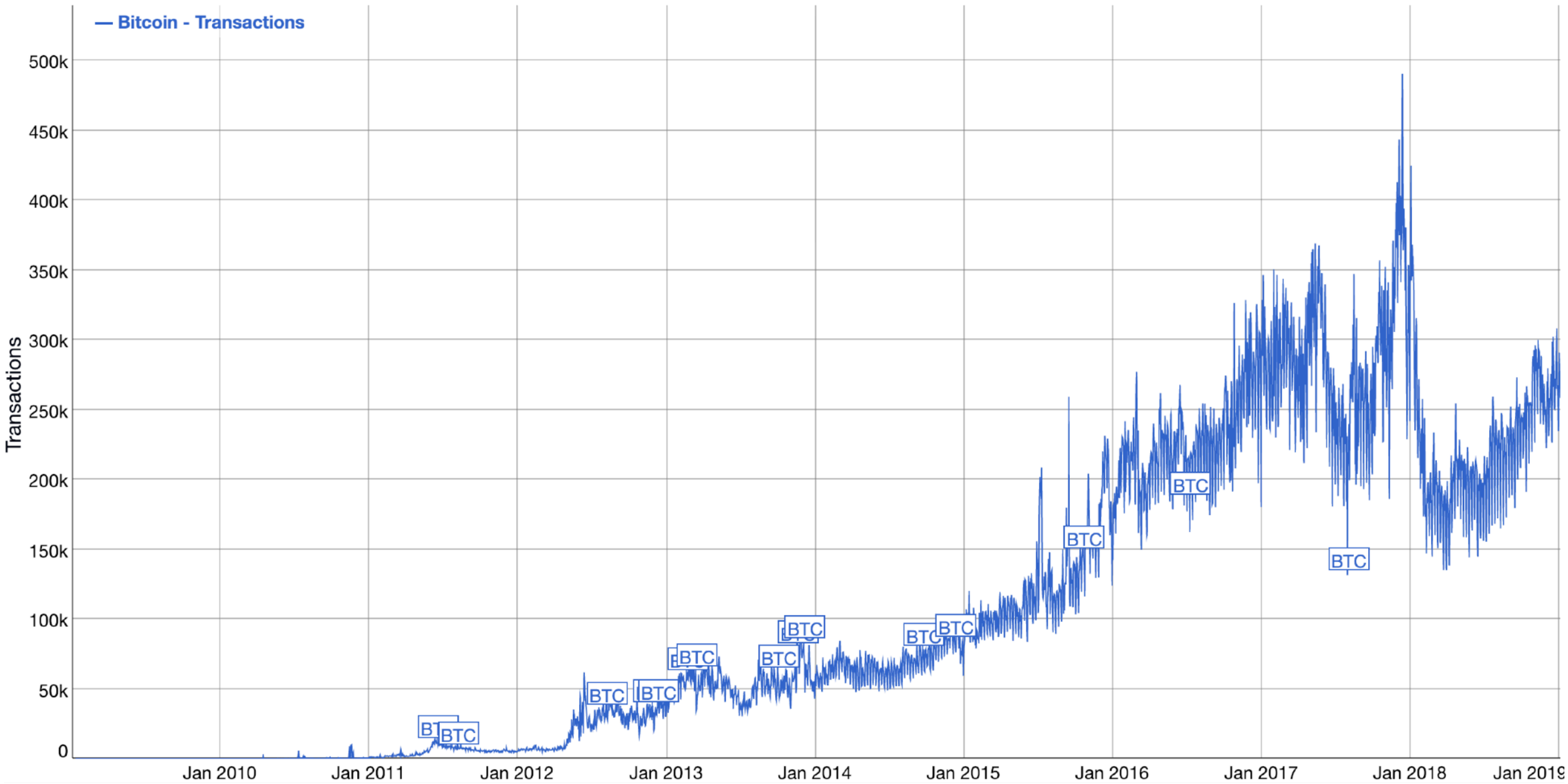
2. May 2010: Laszlo Hanyecz buys two pizzas for 10000 BTC (worth more than $40M today). Bitcoin exchanges start operating around this time.

3. August 2010: Protocol bug lets hacker create 184 billion BTC. Protocol was patched and bugger transaction was “undone” (!).

4. December 2010: Satoshi signs off:

    “I've moved on to other things. It's in good hands with Gavin and everyone.”

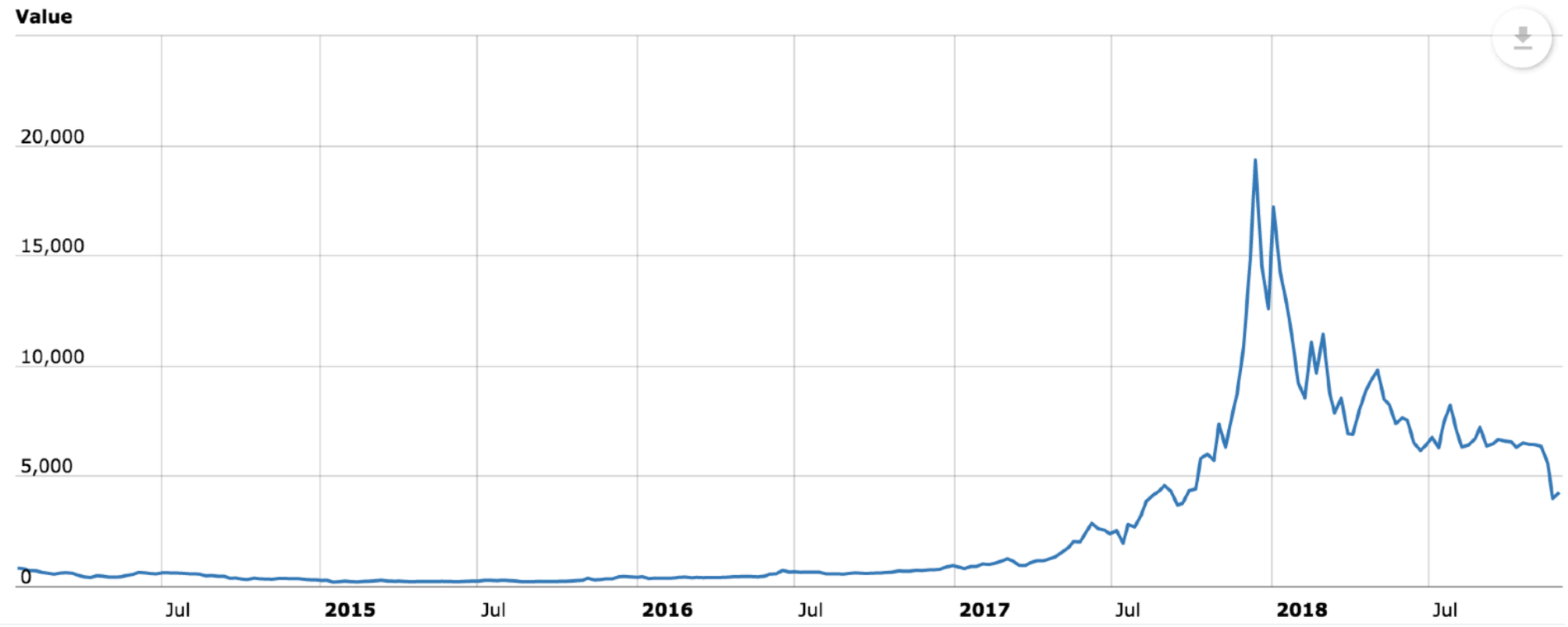
2009-Now: Exponential Volume Growth



Bitcoin Price History

Lately Bitcoin has ~$66 Billion market cap
(Peaked at ~$327 Billion on December 17, 2017)

Bitcoin
Price (USD)



Cryptocurrencies today: Multitudes of “Altcoins”

Hundreds of other currencies built on the ideas of Bitcoin:

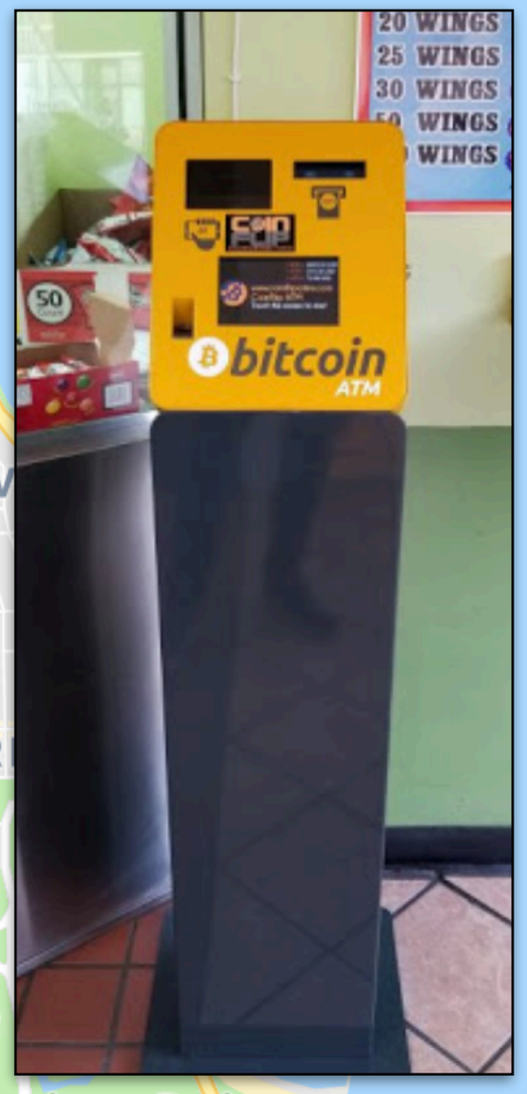
Top 100 Cryptocurrencies by Market Capitalization

Cryptocurrencies ▾ | Exchanges ▾ | Watchlist | USD ▾ | Next 100 → | View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$66,369,974,827	$3,800.64	$4,469,158,173	17,462,825 BTC	-1.05%	
2	Ethereum	$15,652,613,471	$150.22	$2,807,665,353	104,194,631 ETH	1.14%	
3	XRP	$14,462,252,542	$0.354518	$421,058,460	40,794,121,066 XRP *	-1.34%	
4	Bitcoin Cash	$2,791,470,854	$159.07	$198,803,094	17,548,438 BCH	-1.53%	
5	EOS	$2,425,081,974	$2.68	$682,895,317	906,245,118 EOS *	0.24%	
6	Stellar	$2,167,829,141	$0.113127	$83,583,761	19,162,756,352 XLM *	-0.90%	

Ideas underlying Bitcoin are used for hundreds of other “blockchains”

Bitcoin Today



DigitalMint Bitcoin ATM Teller Window

Digital Cash 2 Go - Bitcoin ATM

Digital Cash 2 Go - Bitcoin ATM

DigitalMint Bitcoin ATM

DigitalMint Bitcoin ATM

DigitalMint Bitcoin ATM Teller Window

RockItCoin Bitcoin ATM

RockItCoin Bitcoin ATM

DigitalMint Bitcoin ATM

MetroBTM Bitcoin ATM

DigitalMint Bitcoin ATM

DigitalMint Bitcoin ATM Teller Window

DigitalMint Bitcoin ATM Teller Window

DigitalMint Bitcoin ATM

RockItCoin Bitcoin ATM

CoinFl

OAKLAND

BACK OF THE YARDS

INDIAN V

HYDE PAR

SOUTH SIDE

ENGLEWOOD

GREATER GRAND CROSSING

SOUTH SHORE

Jackson Park

Oak Woods Cemetery

The University of Chicago

W 43rd St

E 43rd St

W 51st St

W Garfield Blvd

E 55th St

W 59th St

E 59th St

W 63rd St

W Marquette Rd

W 71st St

E 75th St

E 67th St

S Western Ave

S Ashland Ave

S Racine Ave

Payne Dr

S Stony Island Ave

1600 E

S Yates Blvd

90

41

Part 1 of this Course: Computer Science

Staff:

Instructors: Ben and David
TAs: Emily Willson and Xi Liang

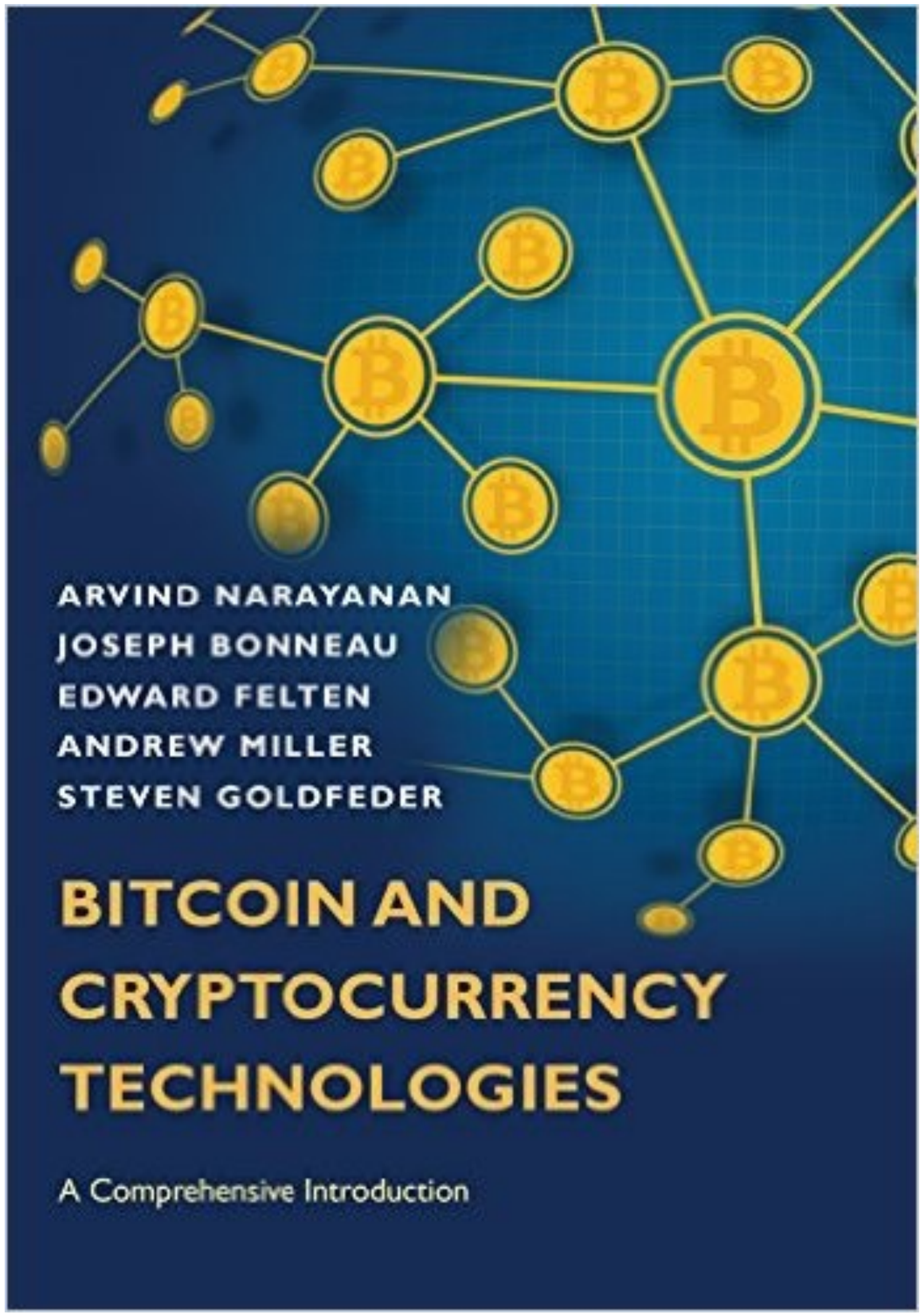
After week 5, you should able to:

1. Understand how popular cryptocurrencies work, and why.
2. Think analytically about the security and privacy issues in cryptocurrencies.
3. Skeptically evaluate cryptocurrency/blockchain hype.
4. Think critically about the societal impacts of cryptocurrencies.

Topics through week 5:

1. Some non-mathematical background in cryptography
2. Cryptocurrencies before blockchain: Ecash
3. How Bitcoin works: Blockchains, transactions, mining
4. How Bitcoin is attacked
5. Alternatives and advanced features of blockchains — Proof-of-work alternatives, smart contracts, zero-knowledge proofs
6. Cryptocurrency communities, exchanges, crime

Textbook



Free PDF at:

http://bitcoinbook.cs.princeton.edu/

Assigned work for Weeks 1-5:

Programming assignments: Hands-on projects building and analyzing your own blockchain. Details soon.

Midterm: Wednesday, Feb 6 (Week 5) in class.

Rest of Lecture 1 Overview

1. The problem of electronic commerce
2. A very brief introduction to cryptography and digital signatures
3. Past digital currencies: eCash and lessons from the 1990's
4. Beginning ledger-based cryptocurrencies

The future of e-commerce in the 80s and 90s

It was clear early on that the Internet was “not secure”.

> *“The use of credit cards and ATM cards is becoming increasingly popular, but those systems lack adequate privacy or security against fraud, resulting in a demand for efficient electronic-money systems to prevent fraud and also to protect user privacy.”*
>
> — Jörg Kienzle and Adrian Perrig in “Digital Money: A divine gift or Satan's malicious tool?” (1996)

> *“Current developments in applying technology are rendering hollow both the remaining safeguards on privacy and the right to access and correct personal data. If these developments continue, their enormous surveillance potential will leave individuals’ lives vulnerable to an unprecedented concentration of scrutiny and authority.”*
>
> — David Chaum in “Numbers Can Be a Better Form of Cash than Paper” (1991)

Early Cryptocurrency: ECash

BLIND SIGNATURES FOR UNTRACEABLE PAYMENTS

David Chaum

Department of Computer Science
University of California
Santa Barbara, CA

INTRODUCTION

Automation of the way we pay for goods and services is already underway, as can be seen by the variety and growth of electronic banking services available to consumers. The ultimate structure of the new electronic payments system may have a substantial impact on personal privacy as well as on the nature and extent of criminal use

STEVEN LEVY BUSINESS 12.01.94 12:00 PM

E-MONEY (THAT'S WHAT I WANT)

SHARE

92

The killer application for electronic networks isn't video-on-demand. It's going to hit you where it really matters - in your wallet. It's not only going to revolutionize the Net, it will change the global economy.

Cryptography underlies Cryptocurrencies

What is cryptography?

Cryptography is about designing and analyzing algorithms that protect information from adversaries.

(but that's just my opinion)


6V
断
45V

nothing

Today 11:11

Can you please come over asap to help me move the couch?

I need to be out of here by 3pm

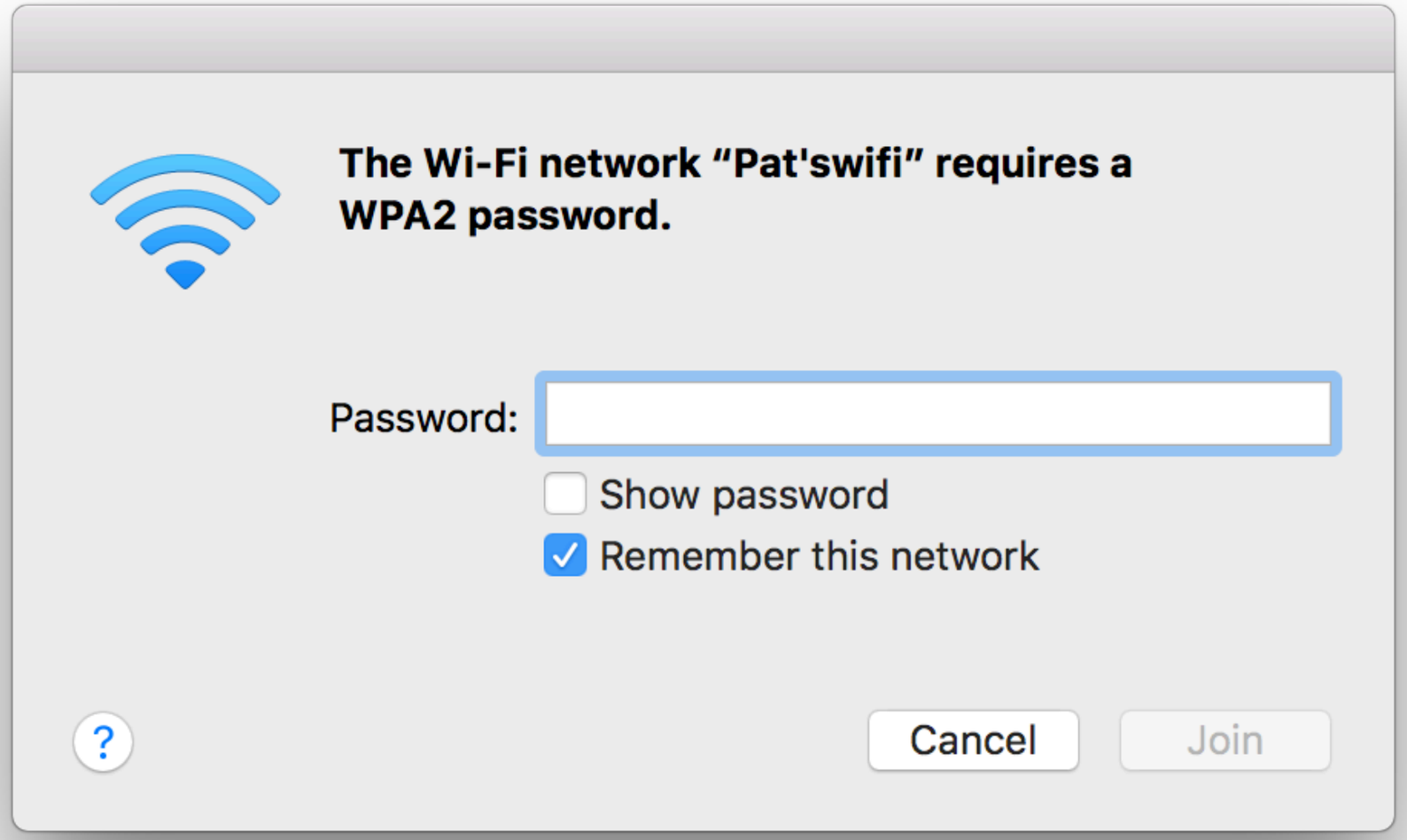
I guess you forgot your phone at home or something

Delivered

Send

iMessage


5100
5100


The Wi-Fi network “Pat'swifi” requires a WPA2 password.
Password:
Show password
Remember this network
?
Cancel
Join

Amazon.com: Online Shopp

https://www.amazon.com

www.amazon.com

Your connection to this site is private.

Details

Permissions | Connection

Chrome verified that Symantec Class 3 Secure Server CA - G4 issued this website's certificate. The server did not supply any Certificate Transparency information.

Certificate Information

Your connection to www.amazon.com is encrypted using a modern cipher suite.

The connection uses TLS 1.2.

The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism.

What do these mean?

Our Main Crypto Tool: Digital Signatures

Digital Signatures are a cryptographic analogue of having people sign their names on contracts.

Three crucial properties:

1. John Hancock can produce that signature.
2. Nobody else can produce that signature perfectly.
3. Everybody can recognize John Hancock's signature

Implies John can't change his mind after signing!

PT7-33

PT5-743

ORINST. P 61238 PERSEPOLIS, IRAN. SEALS AND SEAL IMPRESSIONS.
UPPER: LION STRIKING IBEX, FROM THE APADANA; ACHAEMENIAN?
MIDDLE: TWO LIONS ATTACKING A MOUFLON, FROM THE TREASURY; ACHAEMENIAN.
LOWER: DEITY SEATED AT ALTAR. LION STRIKING ANIMAL, FROM THE GARRISON STREET. LATE ASSYRIAN.

PT5-791

D12

Digital Signatures

A digital signature scheme consists of three algorithms: **`KeyGen`**, **`Sign`**, and **`Verify`**

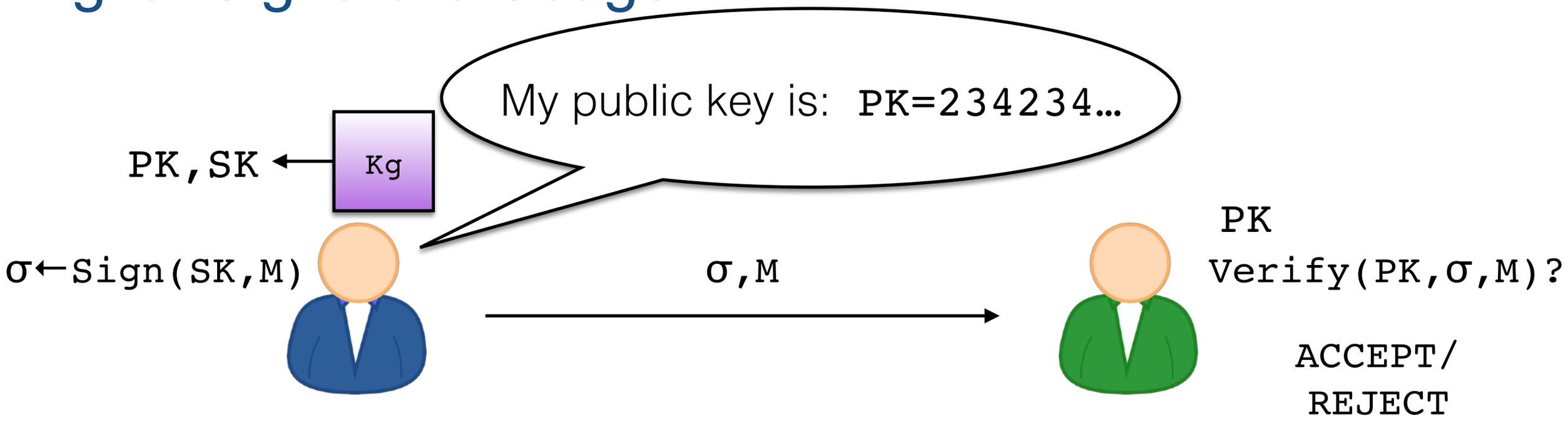
- Key generation algorithm **`KeyGen`**, takes no input and outputs a (random) public-verification-key/secret-signing key pair **`(PK,SK)`**

- Signing algorithm **`Sign`**, takes input the secret key **`SK`** and a message **`M`**, outputs a "signature": **`σ←Sign(SK,M)`**

- Verification algorithm **`Verify`**, takes input the public key **`PK`**, a message **`M`**, a signature **`σ`**, and outputs **`ACCEPT/REJECT`**

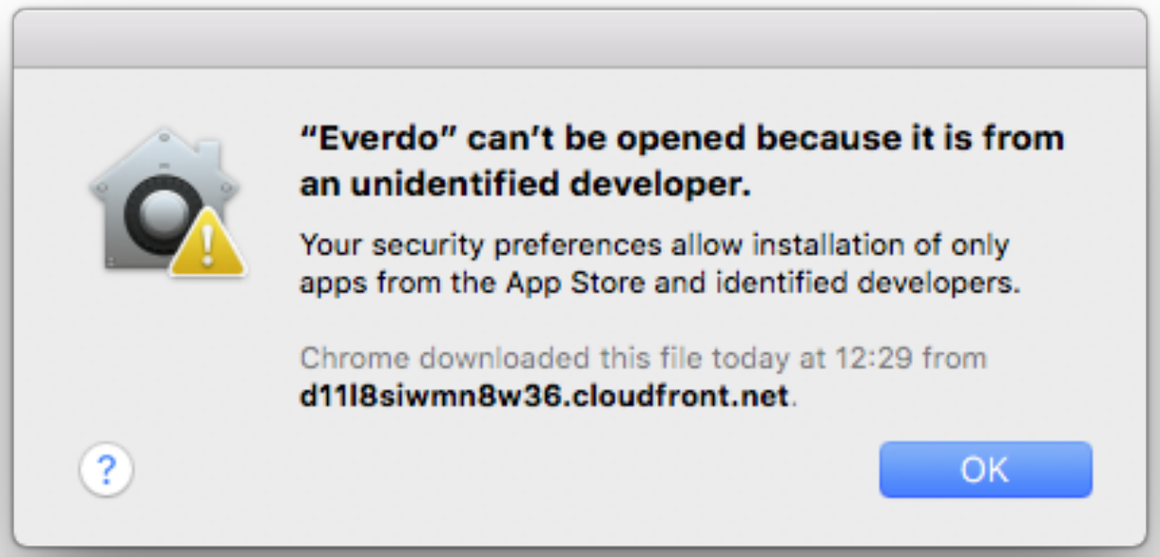
`Verify(PK,M,σ)=ACCEPT/REJECT`

Digital Signature Usage



Common uses of digital signatures:

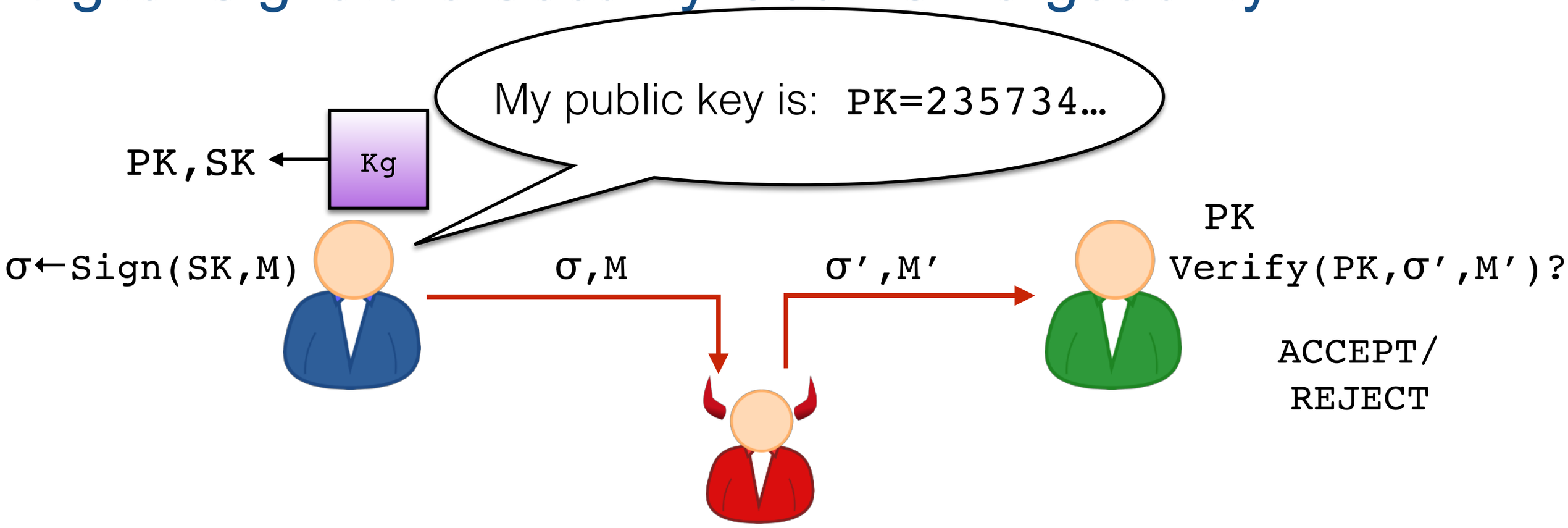
1. Browsers authenticating websites
2. Operating systems authenticating software



Here:

1. $\mathtt{PK}$ is shipped with MacOS
2. Message $\mathtt{M}$ is software you download
3. Signature σ is attached by developer

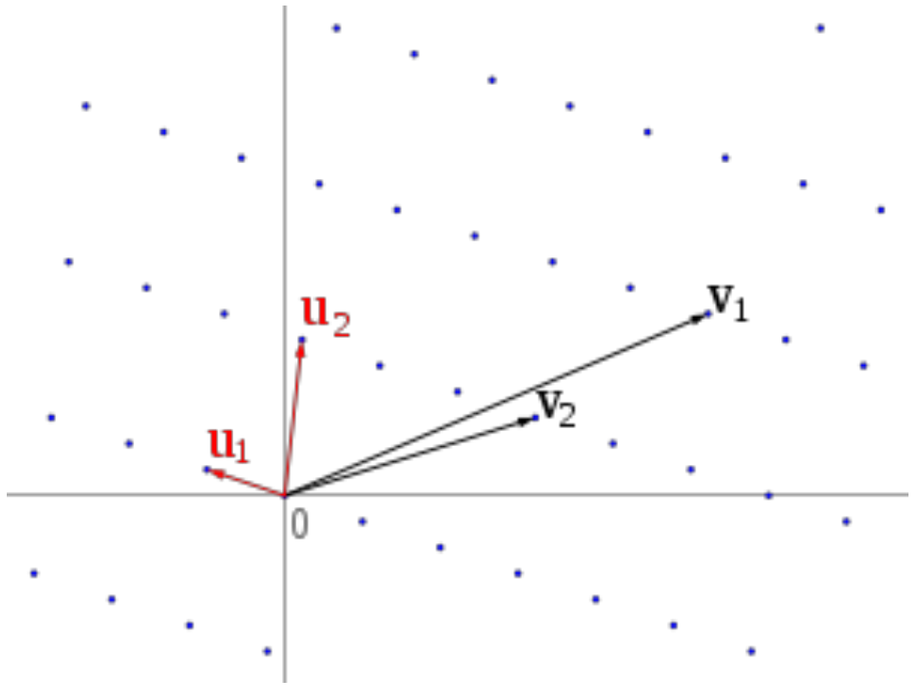
Digital Signature Security Goal: Unforgeability



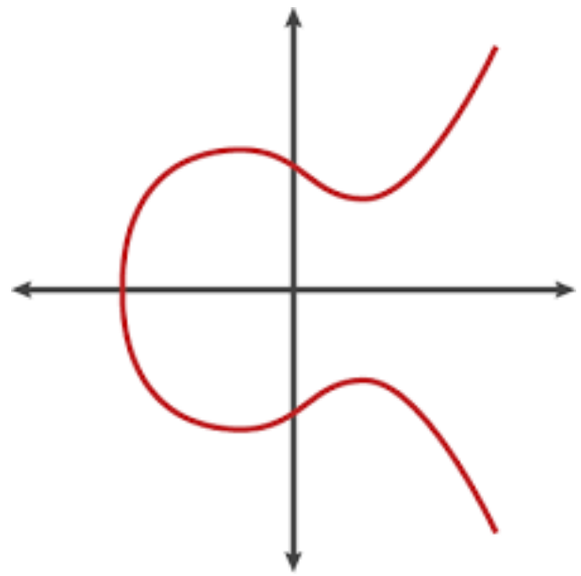
A digital signature scheme is **unforgeable** if it is infeasible for an adversary (who knows `PK`) to fool Bob into accepting `M'` not previously sent by Alice.

Schemes should be unforgeable even for extremely powerful adversaries like governments.

Practical digital signatures all use…



MATH



$$N = pq$$

… which isn't part of this course. 😔

(But is part of CS284/384 if you are interested.)

Some notes about cryptographic security

1. The notion of unforgeability can be made mathematically precise.

2. We cannot <u>prove</u> for sure that any digital signature scheme is unforgeable. Doing so requires resolving the biggest open problem in theoretical CS: P≠NP (and even more in fact).

3. An adversary can always forge with some tiny probability by just guessing a random signature; But this probability will be extremely small.

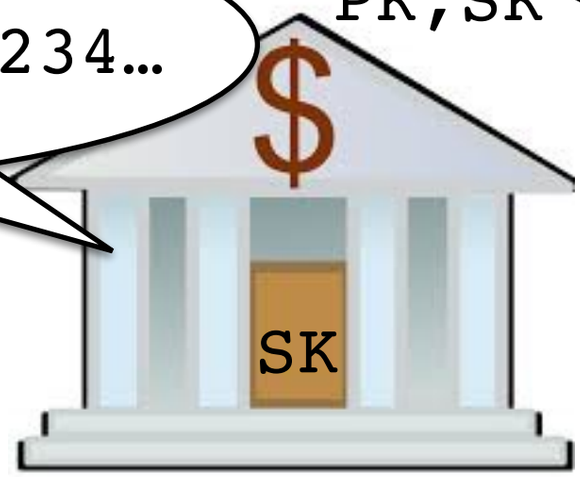
4. A mathematical breakthrough may render all in-use digital signatures insecure. If developed, huge quantum computers can in principle break all in-use digital signatures

<u>Summary</u>: Digital signatures work in practice but security claims come with caveats.

A Basic Cryptocurrency from Digital Signatures

My public key is: PK=814234…

PK,SK ← Kg



Name	Balance
David	~~8~~ 7
Ben	14
Harald	12
Emily	21
Xi	11

Withdraw $1 →

← (N,σ)

(N,σ)

To process a withdrawal:

1. Subtract 1 from David's balance
2. Select next serial number N
3. Compute σ←Sign(SK,N)
4. Give (N,σ) to David

Idea: A "coin" is a serial number N along with a valid signature on N.

A Basic Cryptocurrency from Digital Signatures

My public key is: PK=814234…

Name	Balance
David	~~8~~ 7
Ben	~~14~~ 15
Harald	12
Emily	21
Xi	11

List of spent serial numbers: **N**

(N,σ)

Give $1 to Ben:
(N,σ)

Ok!

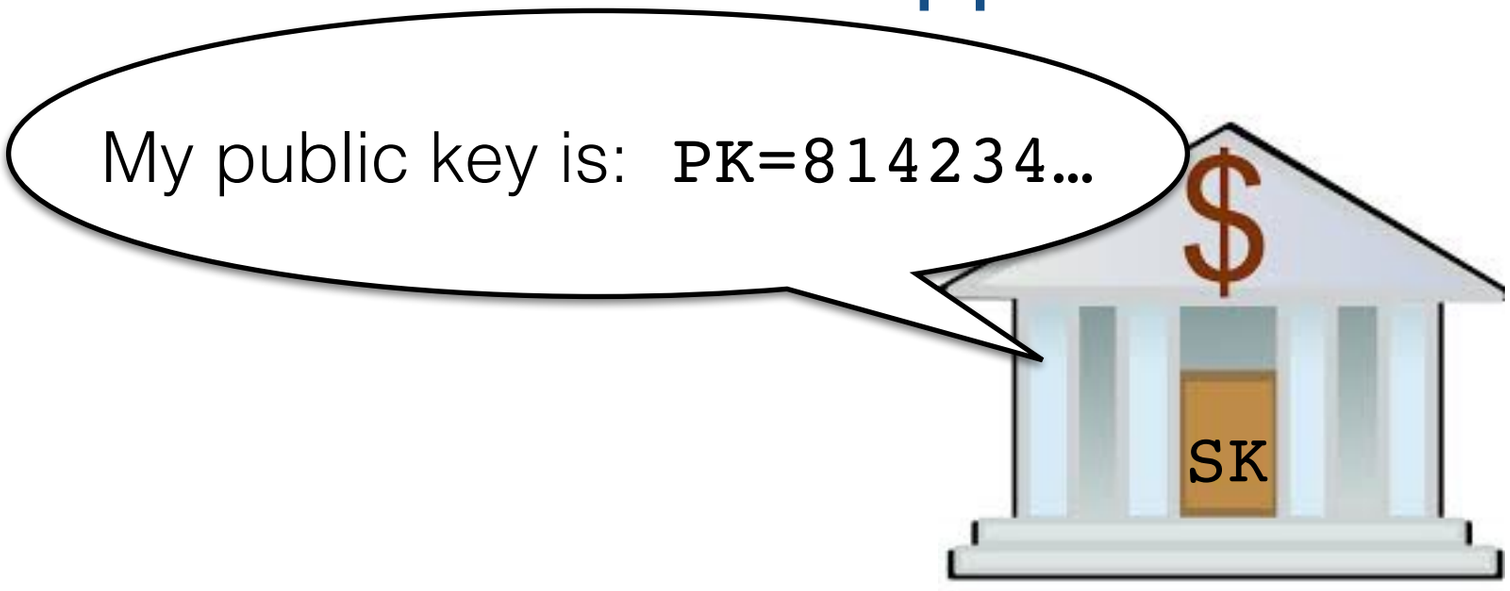
Deposit $1
(N,σ)

To process a deposit:

1. Check that σ is valid
2. Check that N has not been spent previously.
3. Add 1 to Ben's balance
4. Put N on a list of spend serial numbers.

Idea: Putting N on list prevents same coin from being spent twice.

Problems with this approach



Name	Balance
David	~~8~~ 7
Ben	~~14~~ 15
Harald	12
Emily	21
Xi	11

List of spent serial numbers: **N**

1. Clearing a transaction requires speaking to the bank, which is annoying. But otherwise I could double-spend the same coin!
2. Everyone must trust the bank to manage balances correctly.
3. The bank sees every transaction: Withdrawal, Spend, Deposit.
4. If the bank's secret key is stolen then all of the money can be stolen.

A better cryptocurrencies developed in the 1980s

BLIND SIGNATURES FOR UNTRACEABLE PAYMENTS

David Chaum

Department of Computer Science
University of California
Santa Barbara, CA

INTRODUCTION

Automation of the way we pay for goods and services is already underway, as can be seen by the variety and growth of electronic banking services available to consumers. The ultimate structure of the new electronic payments system may have a substantial impact on personal privacy as well as on the nature and extent of criminal use of payments. Ideally a new payments system should address both of

- Several works, many by David Chaum, developed advanced cryptocurrencies
- He and others constructed cryptocurrencies such that:
  1. The bank did not know who was paying who.
  2. Users did not need to contact the bank for each payment.
  3. Double-spending could be caught in creative ways.

DigiCash Inc and ECash's Rise and Fall in the 1990s

(1994)

Attention Internet Shoppers: E-Cash Is Here

By PETER H. LEWIS

Special to The New York Times

CHICAGO, Oct. 18 — The first trials of an international electronic cash system will begin on Wednesday, with a bankroll of one million "cyber bucks" and several hundred volunteers eager to spend them, the system's developer said today.

Digicash Inc., which has offices in Menlo Park, Calif., and Amsterdam, hopes to establish its system as a standard for commercial transactions on the Internet, a global computer network that links millions of users. If the system proves workable in the trials, it is expected to begin commercial operations within months.

The development of an electronic cash system, which eventually would allow buyers and sellers to conduct commercial transactions entirely within the part of cyberspace known as the World Wide Web, is considered critical to the continued business growth of the Internet.

Using credit cards or other means of conventional currency transfer, a consumer would transfer a given amount of E-cash, as electronic cash is rapidly coming to be known, to his or her computer. Then, while shop-

Self-Service Air

By Bloomberg Business News

DAYTON, Ohio, Oct. 18 — AT&T Global Information Solutions and the Datamax Corporation have introduced self-service ticketing kiosks that allow travelers to get their tickets and boarding passes without

15 percent from the cost of each ticket by using the kiosks, Mr. Stellweg said.

To use the system, a customer would make travel arrangements as usual, through travel agents or di-

703 views | Nov 1, 1999, 12:00am

Requiem for a Bright Idea

Julie Pitta BRANDVOICE AdVoice

DAVID CHAUM SAVORED HIS first taste of success two years ago. A brilliant scientist whose specialty is cryptology, he started DigiCash in 1989 to create an on-line currency as secure and private as cash in the physical world. By 1997 he had lured venture backing, snagged the celebrated guru Nicholas Negroponte as chairman and signed a St. Louis bank as his first client. If the cashless society was imminent, he would be among the chief beneficiaries.

Today DigiCash is dead, and Ch

to get enough merchants to acce

to use it, or vice versa," he says.

"As the Web grew, the average level of sophistication of users dropped. It was hard to explain the importance of privacy to them."

— David Chaum, 1999

Enter Bitcoin: A different approach

- Focus on removing the central authority
- Very different privacy and security properties
- Uses a different set of techniques
  - Specifically, no fancy cryptography

Now: We begin breaking down the ideas in Bitcoin.

A Proto-Bitcoin: DCash, The Desert Island Currency

Initialization: Ben, David, and Emily all get `5 DCash coins`

A Proto-Bitcoin: DCash, The Desert Island Currency

Balances are only defined by the transaction history. There is no other conception of money, accounts, etc.

Ben's balance:	TranID	From	To	Amount	
4	1	Ben	Emily	1	✓
4	2	David	Emily	2	✓
1	3	Ben	David	3	✓
1	4	Emily	David	6	✓
1	5	Ben	David	2	✗
	…	…	…	…	

Idea: Transaction history implicitly represents how much money each person has.

Ledger Integrity is Required

TranID	From	To	Amount
1	Ben	Emily	1
2	David	Emily	2
~~3~~	~~Ben~~	~~David~~	~~3~~
4	Emily	David	6
5	Ben	David	1
6	**David**	**Ben**	**8**

Adding/deleting unauthorized transactions amounts to stealing money.

Minting DCash

New DCash coins created via transactions with blank “From:”

TranID	From	To	Amount
1	Ben	Emily	1
2	David	Emily	2
3	Ben	David	3
4	Emily	David	6
5	Ben	David	1
6		Ben	1

Total supply of coins increases!

Digital Signatures for More Secure & Private Ledgers

Initialization: Ben, Emily, and David all generate keys for digital signatures

David's verification key: PK_{david} = 5e7843…
Ben's verification key: PK_{ben} = 88f01e…
Emily's verification key: PK_{emily} = 16823a…

Ben signs transaction row

TranID	From	To	Amount	Signature
1	88f01e…	16823a…	1	91a001…
2	5e7843…	16823a…	2	2c3118…
3	88f01e…	5e7843…	3	7623a6…
4	16823a…	5e7843…	6	987234…
5	88f01e…	5e7843…	1	234b98…

Digital Signatures for More Secure & Private Ledgers

Initialization: Ben, Emily, and David all generate keys for digital signatures

David's verification key: PK_{david} = 5e7843…
Ben's verification key: PK_{ben} = 88f01e…
Emily's verification key: PK_{emily} = 16823a

David signs transaction row, *plus* entire history (prevents reordering)

TranID	From	To	Amount	
1	88f01e…	16823a…	1	91…001…
2	5e7843…	16823a…	2	2c3118…
3	88f01e…	5e7843…	3	7623a6…
4	16823a…	5e7843…	6	987234…
5	88f01e…	5e7843…	1	234b98…

Digital Signatures for More Secure & Private Ledgers

Initialization: Ben, Emily, and David all generate keys for digital signatures

David's verification key: PK_{david} = 5e7843…
Ben's verification key: PK_{ben} = 88f01e…
Emily's verification key: PK_{emily} = 16823a…

TranID	From	To	Amount	Signature
1	88f01e…	16823a…	1	91a001…
2	5e7843…	16823a…	2	2c3118…
3	88f01e…	5e7843…	3	7623a6…
4	16823a…	5e7843…	6	987234…
5	88f01e…	5e7843…	1	234b98…

- Transactions can be added by anyone since signatures can be checked
- Anonymous… sort of

The End

Next time: Decentralizing the ledger