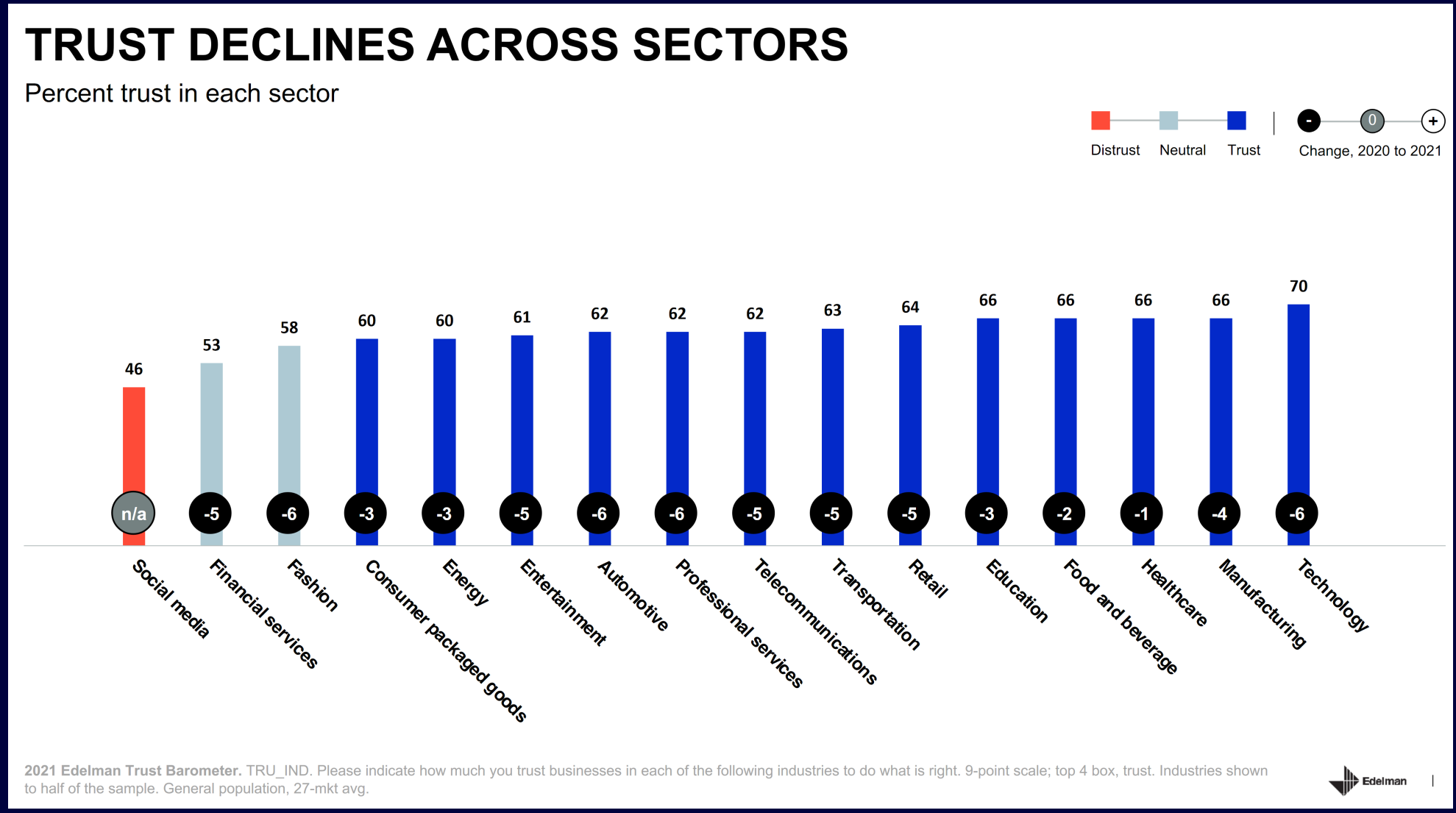
Love, Trust, and Crypto

Raghavendra Rau, University of Cambridge

The major economic transformations over time

Era	When	Technology	Trust
Pre-Industrial revolution	Before 1750		Local trust
Industrial revolution	1750-1840	Mechanization, steam power, weaving looms	Local authorities
Revolution 2.0	1840-1920	Mass production, assembly lines, electrical energy	Intermediaries
Revolution 3.0	1960-2008	Automation, electronics and computers	System
Today	2008-	Internet of Things, Networks	?

Banks are near the bottom of the trust tables



Trust in Industries 2021 (Edelman Trust Barometer)

What do we know about crypto?

Complicated jargon: Distributed ledger technology, blockchains, consensus protocols, smart contracts, shared databases, blah, blah, blah

Difficult to understand how it works

Difficult to understand why it is important

The relation between blockchain and crypto

Crypto is a general phrase that applies to a lot of transactions:

Money – cryptocurrencies

Contracts – Smart contracts or Decentralized Finance

The underlying technology is based on a blockchain

Blockchains: The big picture

The users want to be anonymous – use cryptography to protect anonymity

The data is unstructured – use hashes to represent the data

The data needs to be indelible – no one can alter the data without everyone finding out – use proof-of-work to validate data.

Start with a bank ledger

You pay some money to your friend in the same bank as you. How does the bank record this?

The bank makes a ledger entry. Each ledger entry contains some information:

- The originating person (+ Account number)
- The destination person (+ Account number)
- The transaction detail (How much money is being transferred)

This is linked to your bank accounts. Another entry is made in each account:

- The starting balance
- How much is transferred
- The ending balance

Ledger entries and account balances

A simple ledger entry might be

Mr Black writes a cheque to transfer 5 bitcoin (BTC) from his account to Ms Green

Here Mr Black is the originator

Ms Green is the destination

The ledger entry might look like

Origin	Destination	Amount
Mr. Black	Ms Green	5 BTC

And the account might look like

Date	Starting balance	Amount CR/DR	Ending balance
14 Nov	10 BTC	5 BTC (DR)	5BTC

Problems?

Perhaps your bank manager (who keeps the records) diverts the money to her own account, so she falsifies the transaction.

Origin	Destination	Amount
Mr. Black	~~Ms Green~~ Ms. Red	5 BTC

Perhaps Mr. Black does not have enough money in his account in the first place – so the cheque bounces.

Or perhaps Mr. Black sends the money to Ms. Green but then turns around and spends the same cash to buy a coffee – so he double spends.

Or perhaps Mr. Black does not want everyone (or even his bank manager) to know he needed to send funds to Ms. Green – he wants to be anonymous.

How does a blockchain help?

No one has control of the ledger, so Ms. Red cannot divert the money to her own account.

In general, no one can falsify anything on the chain – even though no one person is responsible for the ledger.

There is no way for Mr. Black to spend the same money twice.

And best of all, everyone's identity can be kept completely secret.

Key points

The blockchain is a way to store data when you do not trust your counterparty

Trust is ensured by technology

If you trust your counterparty, you do not need a blockchain

If you do not need to store data, you do not need a blockchain

Types of blockchains

If everyone is allowed to read entries, it is a public blockchain, otherwise private.

If everyone is allowed to write entries, it is a permissionless blockchain; otherwise it is permissioned.

Can anyone read the entries in the ledger?		Can anyone write in the ledger?	
Yes	No	Yes	No
Public	Private	Permissionless	Permissioned

Type of counterparties			
Known			Unknown
Trusted	Untrusted		
	Need to let outsiders check the data later	No need to let outsiders look at the data	
No need for a blockchain	Public permissioned blockchain	Private permissioned blockchain	Permissionless blockchain

Bottom line: Blockchains need to solve 3 problems

1. No falsification
2. No double-spending
3. Anonymity

They do this using three technologies:

- Cryptography
- Hashing
- Mining.

Solving problems of love through blockchains

Romeo and Juliet want to send letters to each other. What problems do they face?

- They need to be sure that no one else can read their letters.
- They need to be sure that the letter is indubitably coming from only the two of them (not forged by Juliet's cousin, Tybalt)
- Even if someone else gets the letter, the sender should be secret
- The letter is not garbled during sending.
- They need to be sure that Romeo (or Juliet) is not writing the same letter to 5 other girls (boys).

Love and crypto: Problem 1

No one else should be able to read the letters.

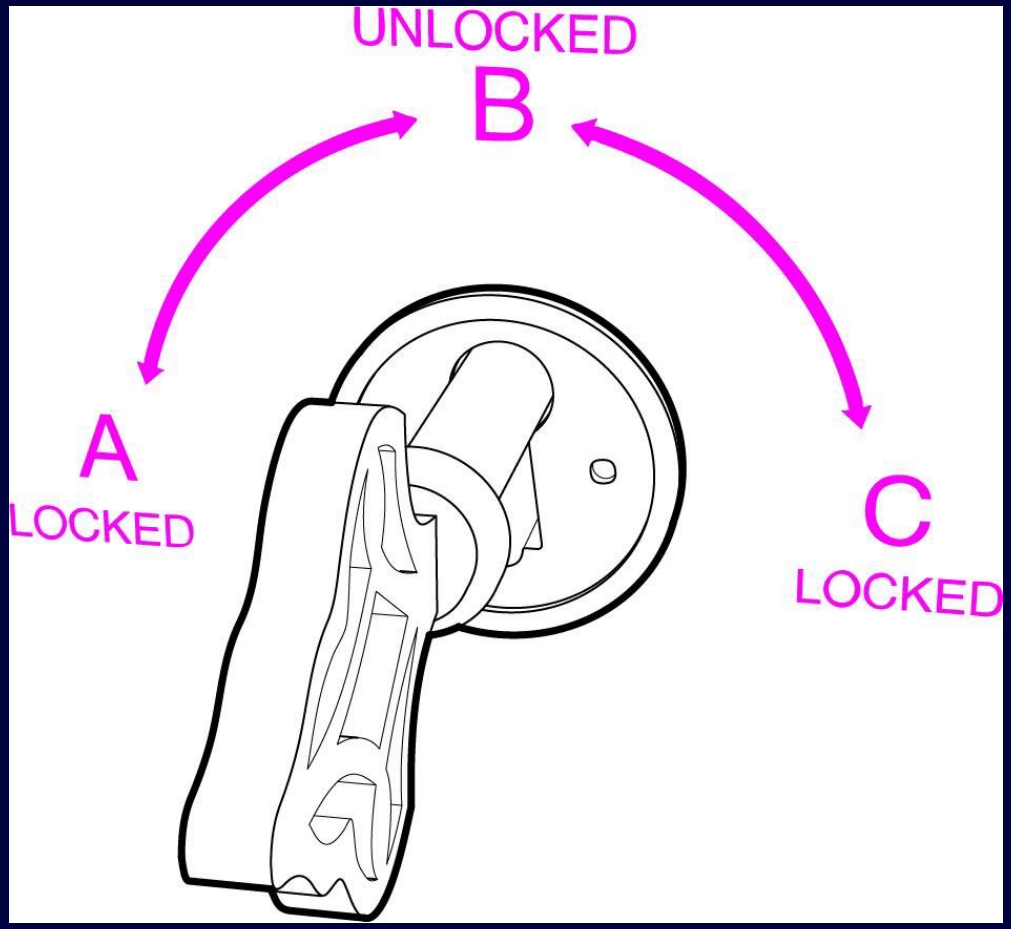
Enter Juliet’s lockbox

What is so special about this lockbox?

Love and crypto: Problem 1

No one else should be able to read the letters.

Why two keys? Asymmetric key cryptography

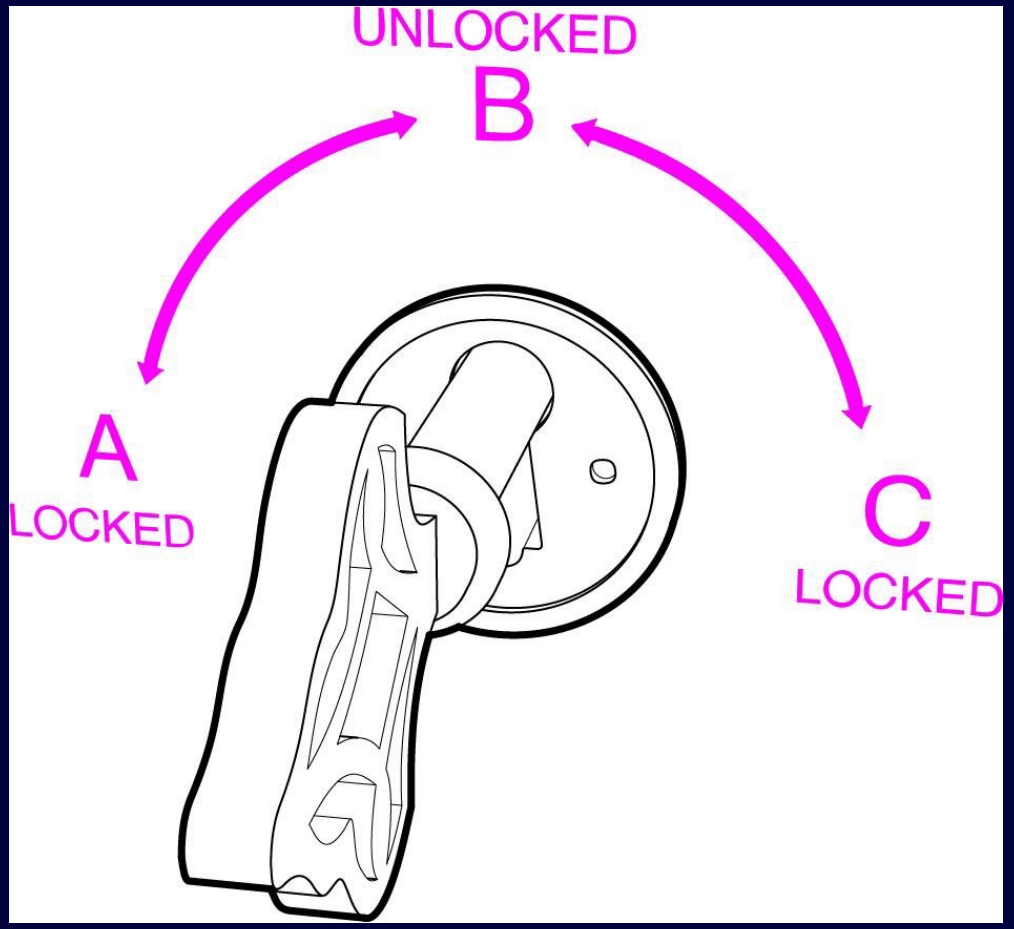


Source: Vryonis, P., 2013, Explaining public-key cryptography to non-geeks

Love and crypto: Problem 2

You need to be sure that the letter comes from Juliet (or Romeo)

Digital signatures



Source: Vryonis, P., 2013, Explaining public-key cryptography to non-geeks

Love and crypto: Problem 3

Even if someone does intercept the letter, he should not know the identity of the sender.

How on earth do you make such keys?

Mathematics:

- What is 17959 times 33851?
- Is 643712231 prime?

PS 17959 times 33851 is 607930109

643712231 is not prime. 643712231 = 20261 × 31771 ... but both of those ARE prime

RSA Algorithm

The public key consists of two numbers where one number is multiplication of two large prime numbers.

The private key is also derived from the same two prime numbers.

If somebody can factorize the large number, the private key is compromised.

Encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially.

Solving problems of love through blockchains

Romeo and Juliet want to send letters to each other. What problems do they face?

- They need to be sure that no one else can read their letters.
- They need to be sure that the letter is indubitably coming from only the two of them (not forged by Juliet's cousin, Tybalt)
- Even if someone else gets the letter, the sender should be secret
- The letter is not garbled during sending.
- They need to be sure that Romeo (or Juliet) is not writing the same letter to 5 other girls (boys).

Love and crypto: Problem 4

- The letter is not garbled during sending.

Solution: Hashing: Construct a summary of the letter.

The summary should have three characteristics:

1. Regardless of the length of the original data, the hashed summary always has the same length
2. A particular data input will always result in the same hash
3. Two different data inputs cannot result in the same hash – the no collision property

What on earth is hashing? It sounds vaguely illegal

Enter Hans Peter Luhn: January 1954 U.S. patent on a “Computer for Verifying Numbers”.

Specifically: Credit card numbers and Social Security numbers

What was the patent for?

Start with a 10-digit number.

- *Double every second digit*
- *If any result is 10 or greater, add up the digits of that result to get a single-digit number (for example, “16” becomes 1 + 6 = 7)*
- *Add up all 10 digits of the new number*
- *Multiply by 9*
- *Take the last digit of that result*

This recipe produces a single-digit “check” number. In Luhn’s original formulation, a 0 indicated the original number was valid.
In later versions, the check was simply appended to the original number as a final digit

Take your credit card

Is the number 3476 096921 02916 valid?

- Take the last digit 6. That is our check digit.

3476 096921 02916

- Take the rest of the sequence

3476 096921 0291

- Double every other digit starting from the right

3,8,7,12,0,18,6,18,2,2,0,4,9,2

Take your credit card

Is the number 3476 096921 02916 valid?

- Sum the double digits

3,8,7,12,0,18,6,18,2,2,0,4,9,2

becomes

3,8,7,3,0,9,6,9,2,2,0,4,9,2

- Add all the digits together

3+8+7+3+0+9+6+9+2+2+0+4+9+2 = 64

Multiply by 9: 64 × 9 = 576

Take your credit card

Is the number 3476 096921 02916 valid?

- Sum the double digits

3,8,7,12,0,18,6,18,2,2,0,4,9,2

becomes

3,8,7,3,0,9,6,9,2,2,0,4,9,2

- Add all the digits together

3+8+7+3+0+9+6+9+2+2+0+4+9+2 = 64

Multiply by 9: 64 × 9 = 576 <- Does the last digit match the check digit?

Hashing constructs a summary of any field

Consider a word: **adam**

Let us give each letter a numeric value:

a = 1, b = 2, and so on.

Obviously A and a will have different values and we will need to give values to the commas, periods, dashes, numbers themselves and all the other special symbols. But to make it easy for us, let us assume that there are only small letters in our text.

Then **adam = 1 4 1 13**

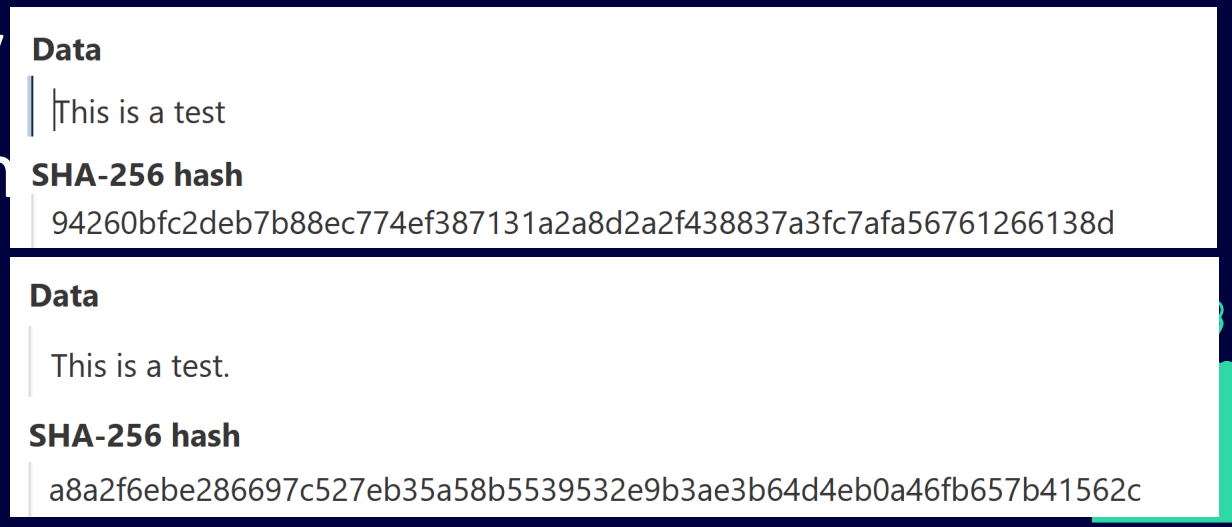
Hashing constructs a summary of any field

Set the maximum length of the hash. Let us suppose this is 10.

adam only takes 4 characters, so we add 1 bit, pad out the remaining length by zeros, and add the number of characters at the end. So adam becomes 1 4 1 13 1 0 0 0 4

We can handle longer phrases by

fragments that are never more th



Love and crypto: Problem 5

- They need to be sure that Romeo (or Juliet) is not writing the same letter to 5 other girls (boys).

Love and crypto: Problem 5

- But who verifies the transaction?

- The miners

- What do the miners do?

- The system sets an allowable solution to a problem
  - The solution must have 3 leading zeros (for example).
- The miners try to hash a set of transactions so that their hash fits that pattern.

Love and crypto: Problem 5

- Let's look at a set of transactions

From	To	Amount	Details
Alice	Maya	1 BTC	For movie
Bob	Gregoire	0.2 BTC	For coffee
Lucas	Bryan	0.9 BTC	For pizza
Alice	Vincent	0.005 BTC	For haircut
Rashid	Tania	1 BTC	For dogwalking

Hash this block (set of transactions)

Add a trial number (nonce)

Hash again

Does it fit the network rule?

Required number of leading zeros

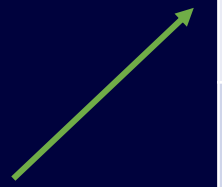
Yes! Broadcast to everyone; earn fee

No … Start again

Love and crypto: Problem 5a

- But wait! Suppose a nefarious miner comes along later and alters a transaction?

From	To	Amount	Details
Alice	Maya	100 BTC	For movie
Bob	Gregoire	0.2 BTC	For coffee
Lucas	Bryan	0.9 BTC	For pizza
Alice	Vincent	0.005 BTC	For haircut
Rashid	Tania	1 BTC	For dogwalking



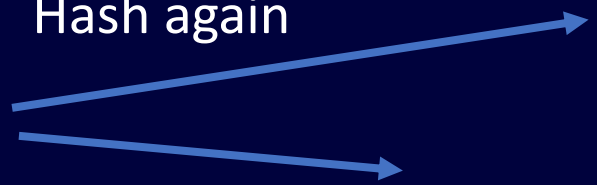
Hash this block (set of transactions)

Add a trial number (nonce)

Does it fit the network rule?

Required number of leading zeros

Hash again



Yes! Broadcast to everyone; earn fee

No … Start again

Love and crypto: Problem 5a: Preventing cheating

- Chain the blocks

From	To	Amount	Details
Alice	Maya	1 BTC	For movie
Bob	Gregoire	0.2 BTC	For coffee
Lucas	Bryan	0.9 BTC	For pizza
Alice	Vincent	0.005 BTC	For haircut
Rashid	Tania	1 BTC	For dogwalking

Hash this block + Header

ADD HEADER FROM PREVIOUS BLOCK

Add a trial number (nonce)

Hash again

Does it fit the network rule?

Yes! Broadcast to everyone; earn fee

No … Start again

Required number of leading zeros

Love, trust, and crypto

Romeo and Juliet send letters to each other. What problems have they solved?

Cryptography:

- They are sure that no one else can read their letters.
- They are sure that the letter is indubitably coming from only the two of them (not forged by Juliet's cousin, Tybalt)
- Even if someone else gets the letter, the sender is secret

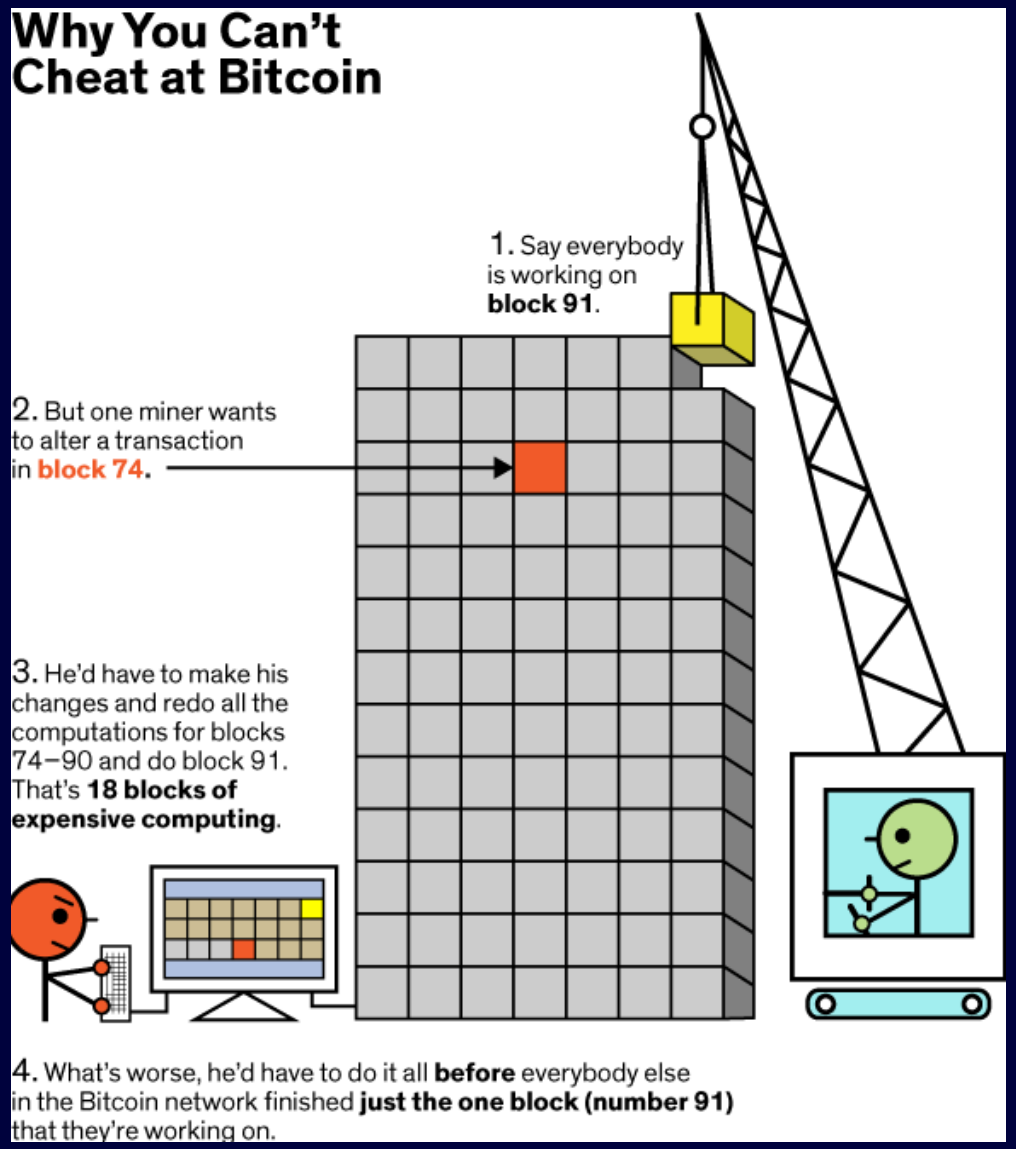
Hashing

- The letter is not garbled during sending.

Mining and verification

- They are sure that Romeo (or Juliet) is not writing the same letter to 5 other girls (boys).

Love and crypto: Mining



Bottom line: Blockchains solve 3 problems

1. No falsification
2. No double-spending
3. Anonymity

They do this using three technologies:

- Cryptography
- Hashing
- Mining.

FOR THE LOVE OF LEARNING SINCE 1597