Lecture 01
Introduction

Dr. Shujaat Hussain

About me

- Ph.D (Data Science, Health Informatics) – Kyung Hee University, Korea
- Director, Knowledge Discovery and Data Mining (KDD) Lab
- Principal Investigator from NCAI: ”Re-Designing E-recruitment using AI for Temporal Analysis”

Teaching experience

- Undergraduate Courses:
  - Computer Programming, Data Structures, Algorithms, Parallel and Distributed Computing, Introduction to Blockchain and Cryptocurrency
- Graduate Courses:
  - Advance Algorithms, Research Methodology, DS tools and Techniques, Applied Programming

About you

- You are here because?
  - You are passionate to learn about what is the buzz about the Blockchain and cryptocurrencies
  - You are still deciding about the courses; taking most and would drop some later
  - You are thinking this to be an easy course ☺
  - All of the above
  - None of the above
  - The question lacks information to be answered correctly

Some Rules

- *Raise your hand before asking any question and then WAIT for the permission*
- *Never ever miss a class*
- *Never ever "sleep" in the class*
- *Never use mobile phones in the class*

- Above all, whatever you do, please do not disturb others

From our PDC course

1. Were you sleeping in the online classes? Hint: You can choose any option other than the option d.
   a. Yes, at times.
   b. To tell you the truth, yes sir mostly I was sleeping.
   c. No sir, I listened to your calm soothing voice and … Zzz
   d. What kind of question this is, I will email the HoD
2. Did you ever watch the video lectures posted on the classroom? Hint: The option d is the correct option.
   a. Wait, what… There were video lectures uploaded on some classroom (whatever it is)
   b. Sir, the student choosing the option a, should be failed on-spot. Award me A++ grade, I have printed all of them as well
   c. I listen to them every night… Zzz
   d. ☺

Dishonesty, Plagiarism

- Plagiarism in an assignment will result in zero marks in the whole assignments category.

- Plagiarism in the course project will result in zero marks in the project and also the deduction of -75% of the total marks for the assessment from other evaluations. For instance, plagiarism in the course project having 10 absolutes would result in 0 points for the project and -7.5 absolutes would be deducted from scores achieved in other assessment items.

- Plagiarism in the midterm and the final exam would result in a disciplinary case forwarded to the department disciplinary committee.

Dishonesty, Plagiarism

You can fool some of the people all of the time,
and all of the people some of the time,

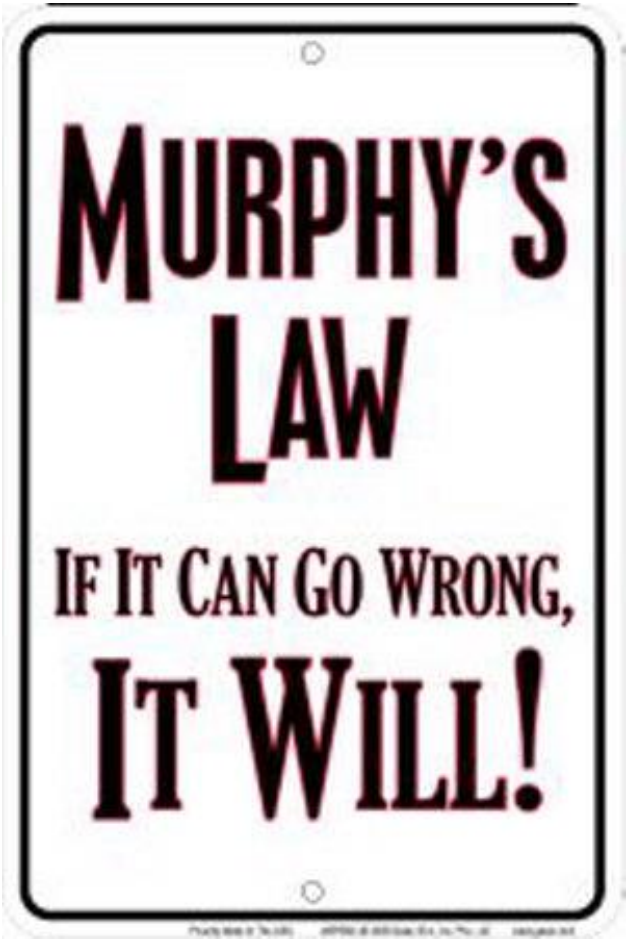
but you can not fool all of the people all of the time.

Abraham Lincoln,
16th president of US (1809 - 1865)

Policy about missed assessment items

- Retake of missed assessment items (other than midterm/ final exam) will not be held.
- One minute (second) late on the deadline is LATE. It is YOUR responsibility to respect the deadlines.

Policy about missed assessment items



Course organization

- We have 2 sections this semester
- Section B are being taught by me and Section A by Dr. Adnan Tariq.

- Course policies, content and grading scheme can be different and the policies in this lecture apply to sections B only.

Some Bonuses (subject to on-campus classed)

- Class participation - 1 absolute for each correctly answered bonus question

Tentative Evaluation Breakdown

Assignments	15
Project (s)	15
Mid-exam	25
Final	45
Total	100

Some of the assessments would be open-book ☺

Absolute grading

Dioyucq

Tentative Course outline

- **PartA - Introduction, Background and Motivation**
  - Introduction, Background, Examples …
- **PartB/C – Building a private Blockchain**
  - Introduction to Golang
  - Network programming, blockchain creation and propagation
- **PartB/C – Core concepts focusing on Bitcoin**
  - Cryptography, Blockchain,
  - Bitcoin nuts and Bolts
  - Mining, Proof of Work and other Concensus approaches
- **PartD – Ethereum, Smart Contracts and Solidity**
  - Ethereum - The world Computer
  - Motivation, Setup, Getting Started and the Hello World
  - Writing Smart Contracts using Solidity

Reference books

- Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction

  Arvind Narayanan, Joseph Bonneau,

  Edward Felten, Andrew Miller, Steven Goldfeder

- Mastering Ethereum

  Andreas M. Antonopoulos Dr. Gavin Wood

  O'Reilly - O'Reilly Media

Do not distribute …

- These slides are not always prepared by me.
- Most of the content comes from the reference book
  - Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction
  - Arvind Narayanan, Joseph Bonneau,
  - Edward Felten, Andrew Miller, Steven Goldfeder

- This lecture however builds upon the bitcoin introduction post by Nik Custodio and slides at www.canton.edu.

Explain Bitcoin Like I'm Five Nik Custodio

- We're sitting on a park bench. It's a great day.
- I have one apple with me. I give it to you.
- You now have one apple and I have zero.

- That was simple, right?

Explain Bitcoin Like I'm Five Nik Custodio

- My apple was physically put into your hand.
- We didn't need a ***third person*** there to help us make the transfer.

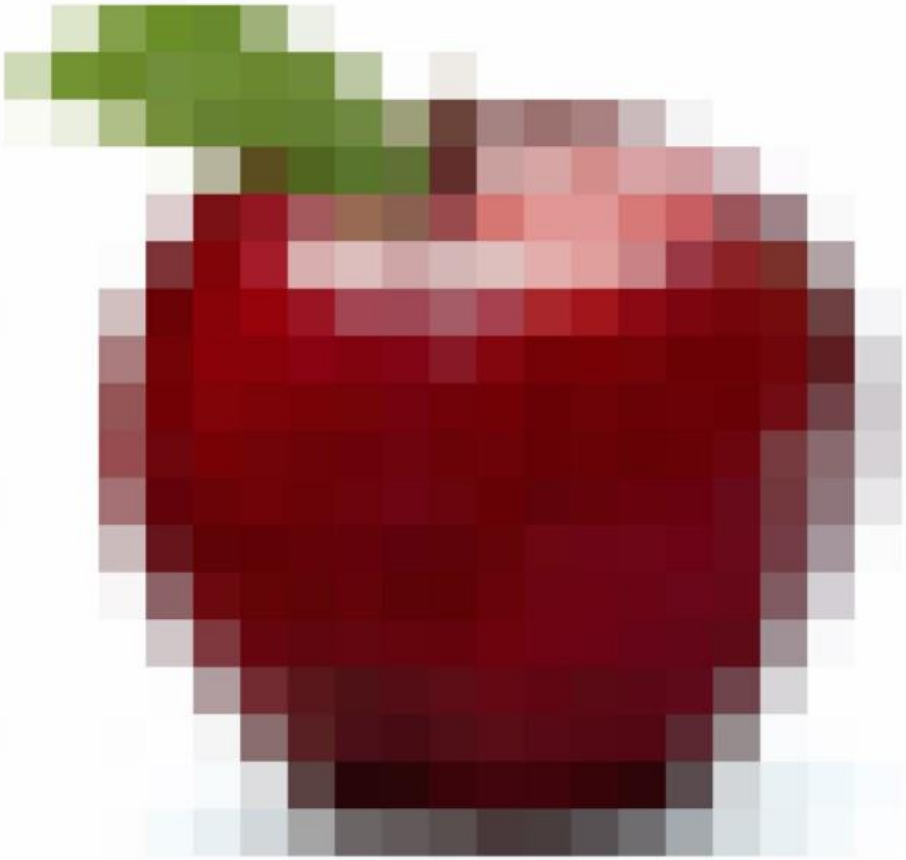
- We didn't need to pull in Uncle Tommy (who's a famous judge) to sit with us on the bench and confirm that the apple went from me to you.

What about the ownership?

- The apple's yours! I can't control it anymore. You have full control over that apple now. You can give it to your friend if you want, and then that friend can give it to his friend. And so on.

- So that's what an in-person exchange looks like. I guess it's really the same, whether I'm giving you a banana, a book, or say a quarter, or a dollar bill….

What about a Digital Apple?



What about a Digital Apple?

- Now say, I have one digital apple. I can give you my digital apple by sending you the image over email or even Whatsapp.

- ***The apple's yours! I can't control it anymore. You have full control over that apple now. Really?***

- How do you know that that digital apple that used to be mine, is now yours, and only yours? Think about it for a second.

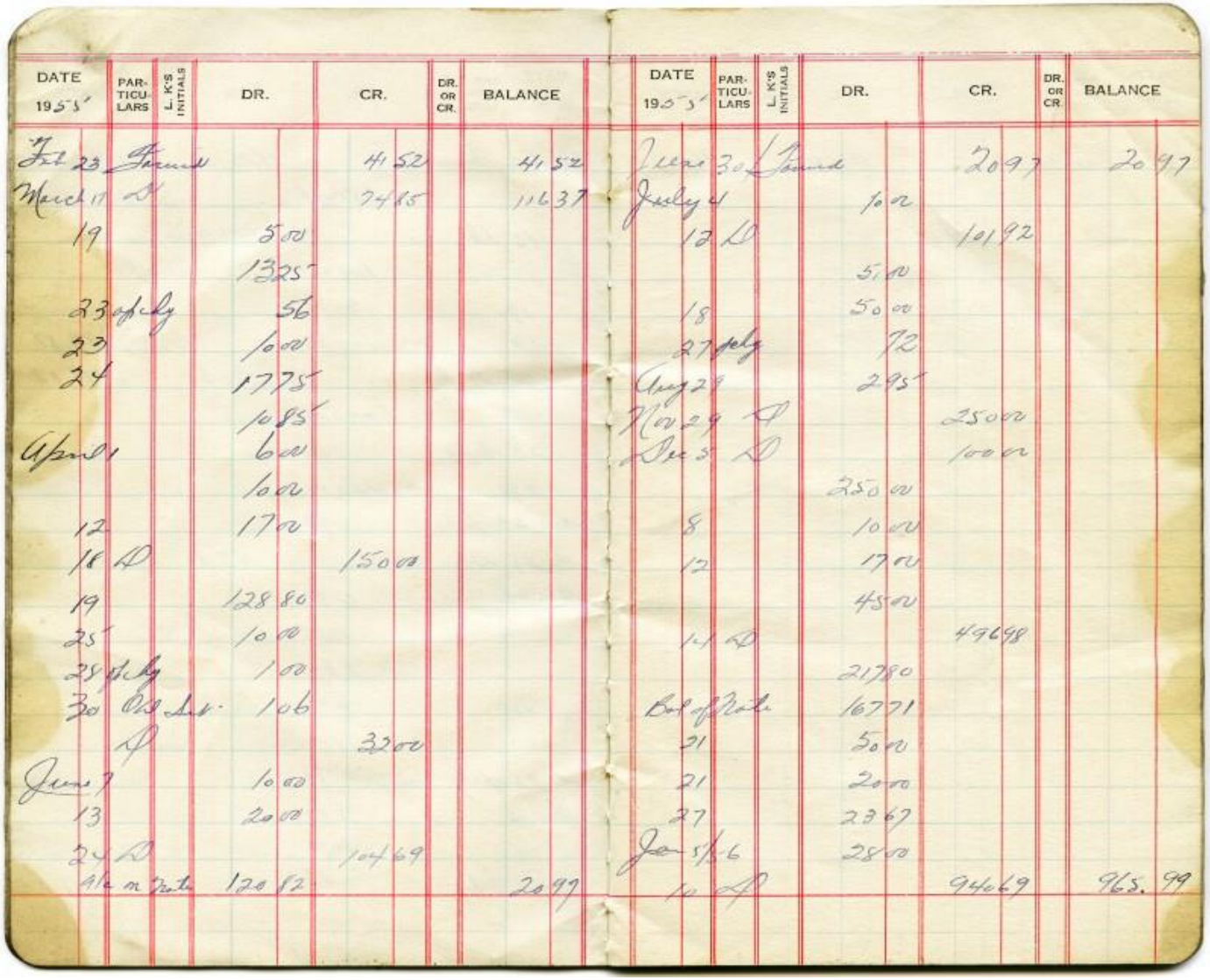
Ownership of a Digital Apple

- It’s more complicated, right? How do you know that I didn’t send that apple to Uncle Tommy as an email attachment first?

- Maybe I made a couple of copies of that digital apple on my computer. Maybe I put it up on the internet and one million people downloaded it.

- There is a name for this problem: it’s called the **double-spending problem.**

One possible solution



Ledgers

- Maybe these digital apples need to be tracked in a ledger. It’s basically a book where you track all transactions — an accounting book.

- This ledger, since it’s digital, needs to live in its own world and have ***someone*** in charge of it.

Centralized Ledgers

- What if that ***someone*** cheats? He could just add a couple of digital apples to his balance whenever he wants!

- Going through that ***someone*** is like pulling in Uncle Tommy (a third-party) for all our park bench transactions.

- How can I just hand over my digital apple to you, like, you know— the usual way?

What else can be done?

- What if we gave this ledger — to everybody?
- Instead of the ledger living on someone’s computer, it’ll live in everybody’s computers.
- All the transactions that have ever happened, from all time, in digital apples will be recorded in it.

Decentralized Ledger

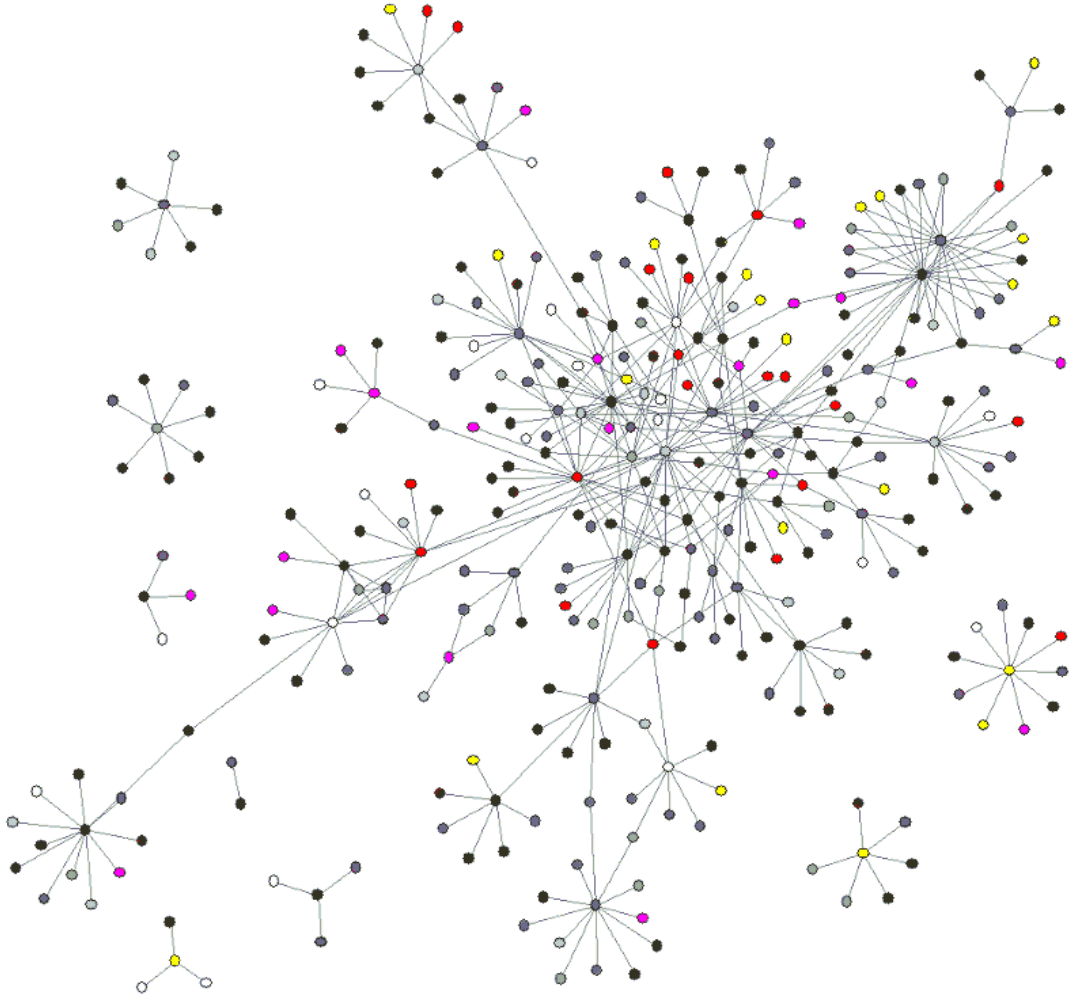
- It’s not controlled by one person, so I know there’s no one that can just decide to give himself more digital apples.
- The rules of the system were already defined at the beginning. And the code and rules are open-source.

Decentralized Ledger

- You could participate in this network too and update the ledger and make sure it all checks out.

- For the trouble, you could get like 25 digital apples as a reward. In fact, that’s the only way to create more digital apples in the system.

Decentralized Ledgers



Bitcoin

- Such a system exists. It's called the Bitcoin protocol. And those digital apples are the "bitcoins" within the system.

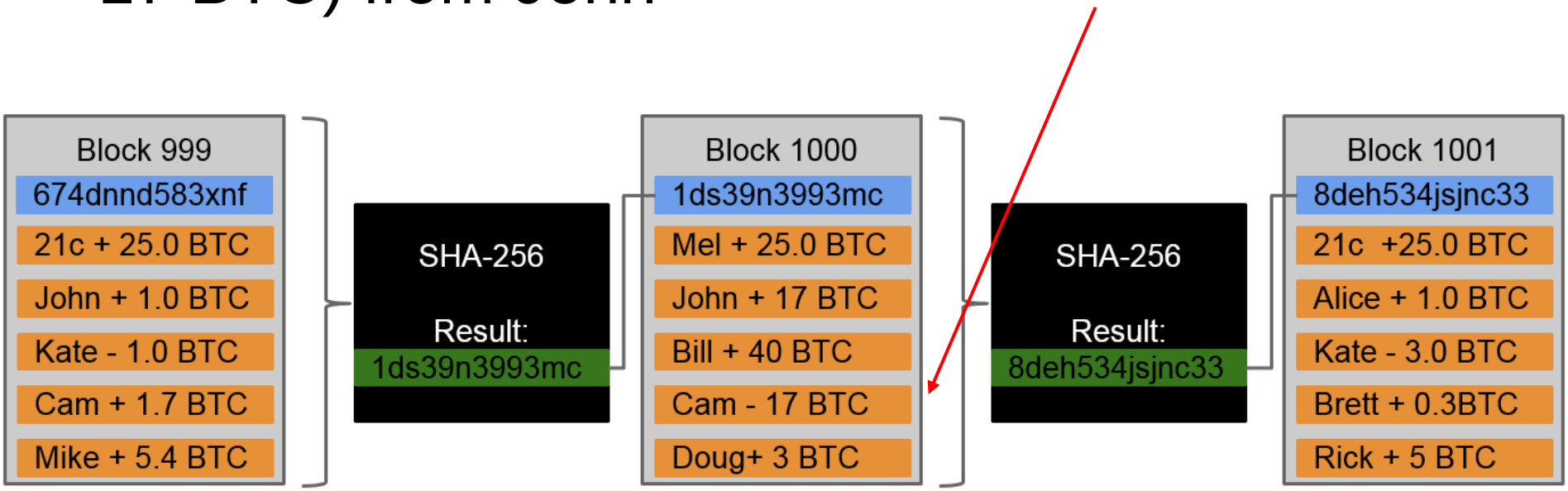
1. It's open source. The total number of apples was defined in the public ledger at the beginning. I know they are limited(scarce).

2. When I make an exchange I now know that digital apple certifiably left my possession and is now completely yours. It will be updated and verified by the public ledger.

3. Because it's a public ledger, I didn't need Uncle Tommy(third-party) to make sure I didn't cheat, or make extra copies for myself, or send apples twice, or thrice…

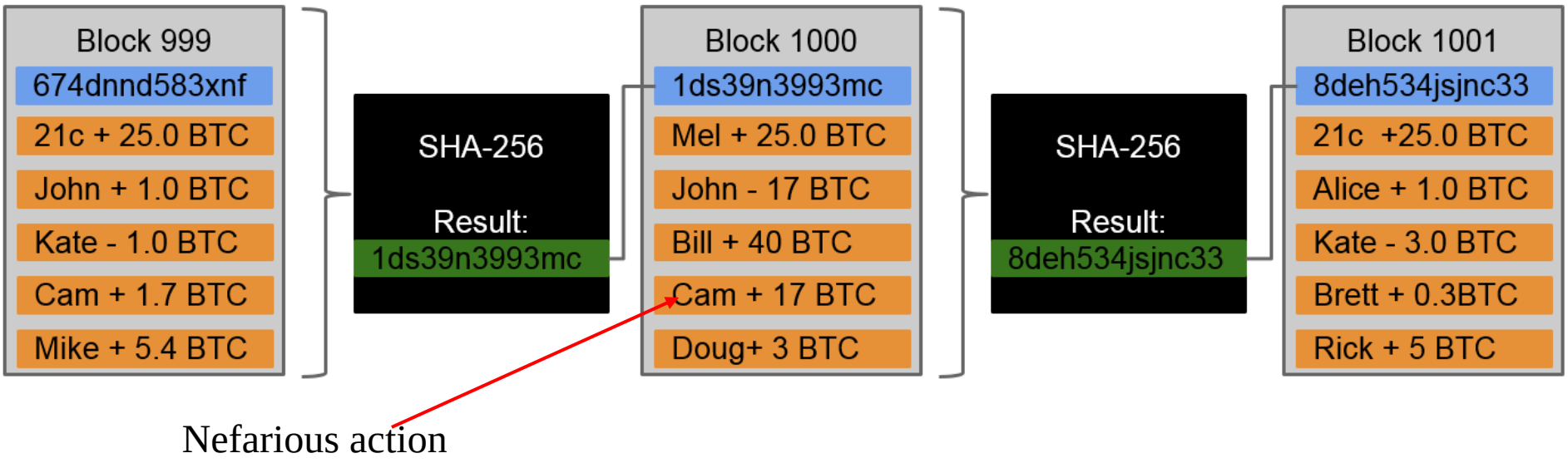
Bitcoin Blockchain

Example: In block 1000, Cam buys a car (for 17 BTC) from John



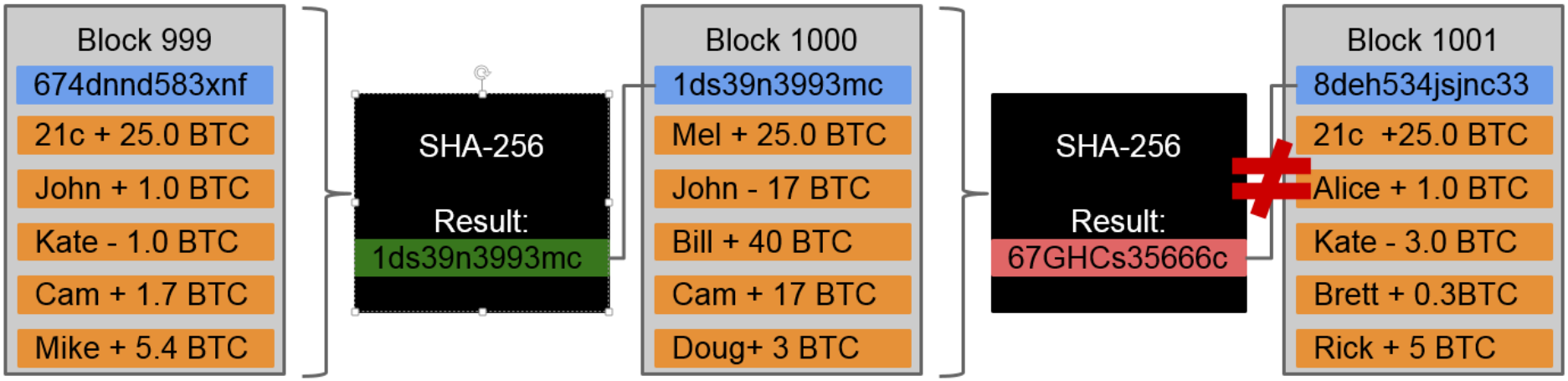
Bitcoin Blockchain

Suppose Cam edits the block on computer and then broadcasts to the network



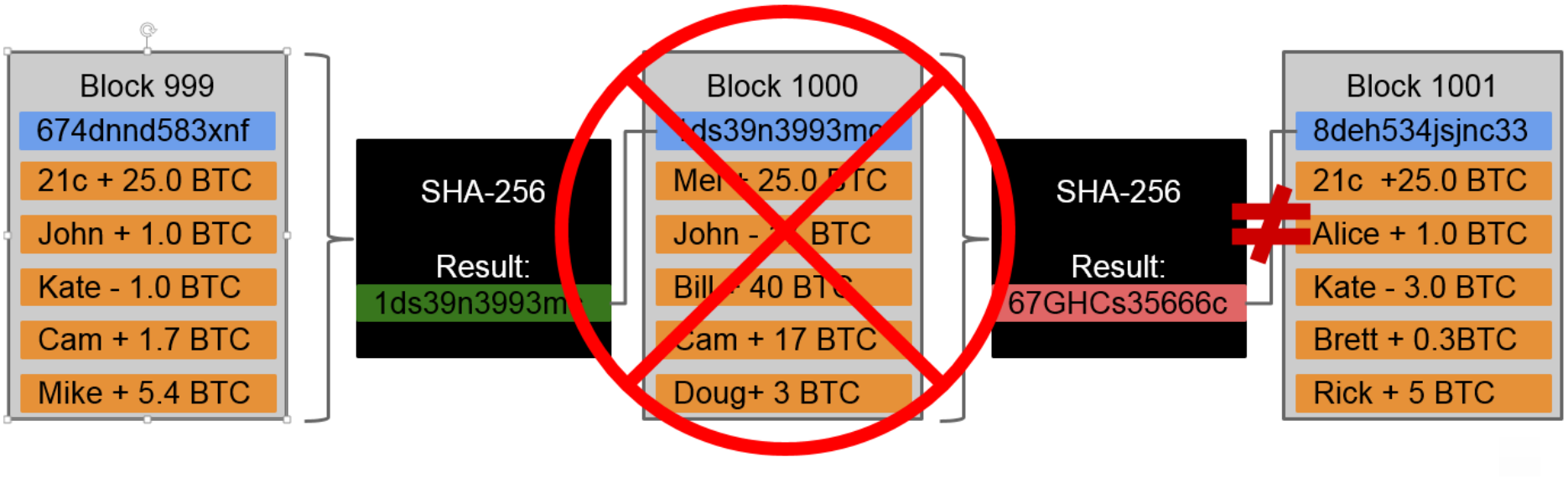
Bitcoin Blockchain

Even making that small change results in a very different block hash. It no longer matches what is stored in block 1001



Bitcoin Blockchain

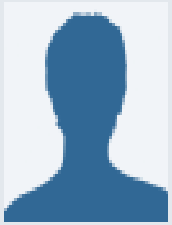
Blockchain clients automatically compute the hash themselves - if no match, they reject the block - Check other peers in the network for correct block



Who developed Bitcoin?

- Satoshi Nakamoto

Satoshi Nakamoto Post



Bitcoin open source implementation of P2P currency

Posted by Satoshi Nakamoto on February 11, 2009 at 22:27

View Discussions

I've developed a new open source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. Give it a try, or take a look at the screenshots and design paper:

Download Bitcoin v0.1 at http://www.bitcoin.org

Dorian NAKAMOTO

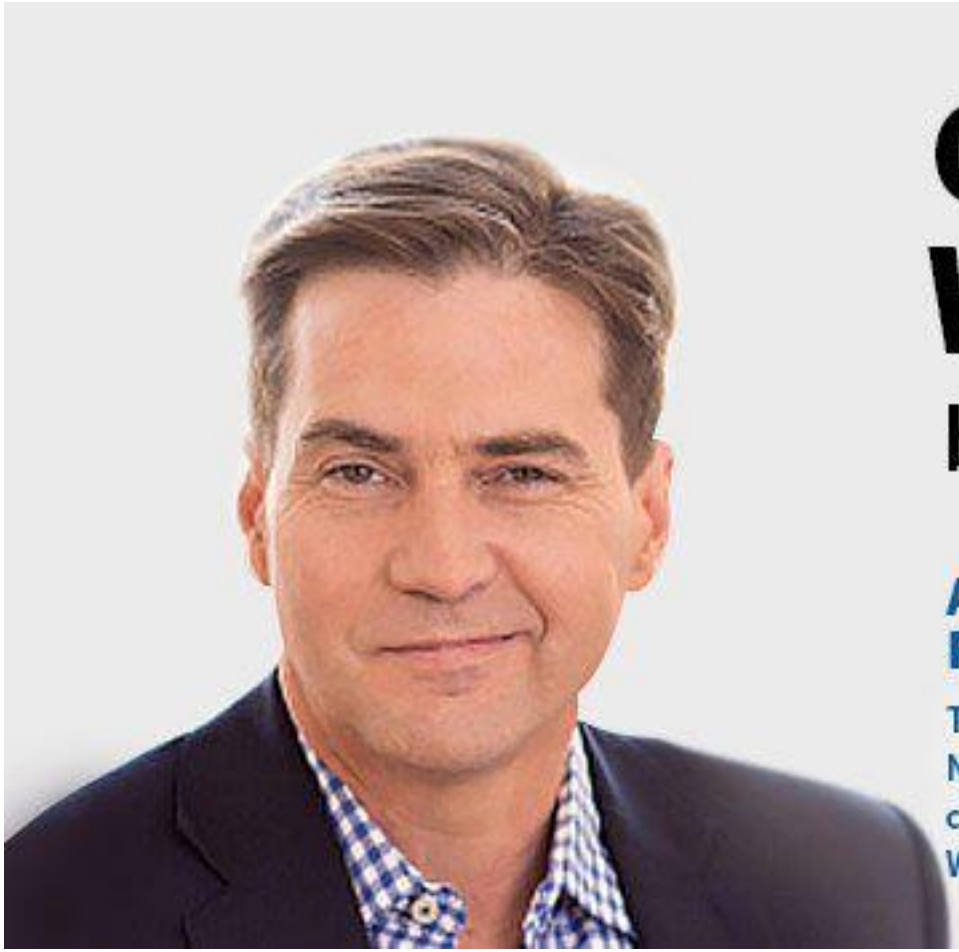
being Satoshi ?

ARGUMENTS FOR

The name and his training as an engineer

ARGUMENTS AGAINST

He aggressively denied it and at the time of his 'outing', had not been working as an engineer for years



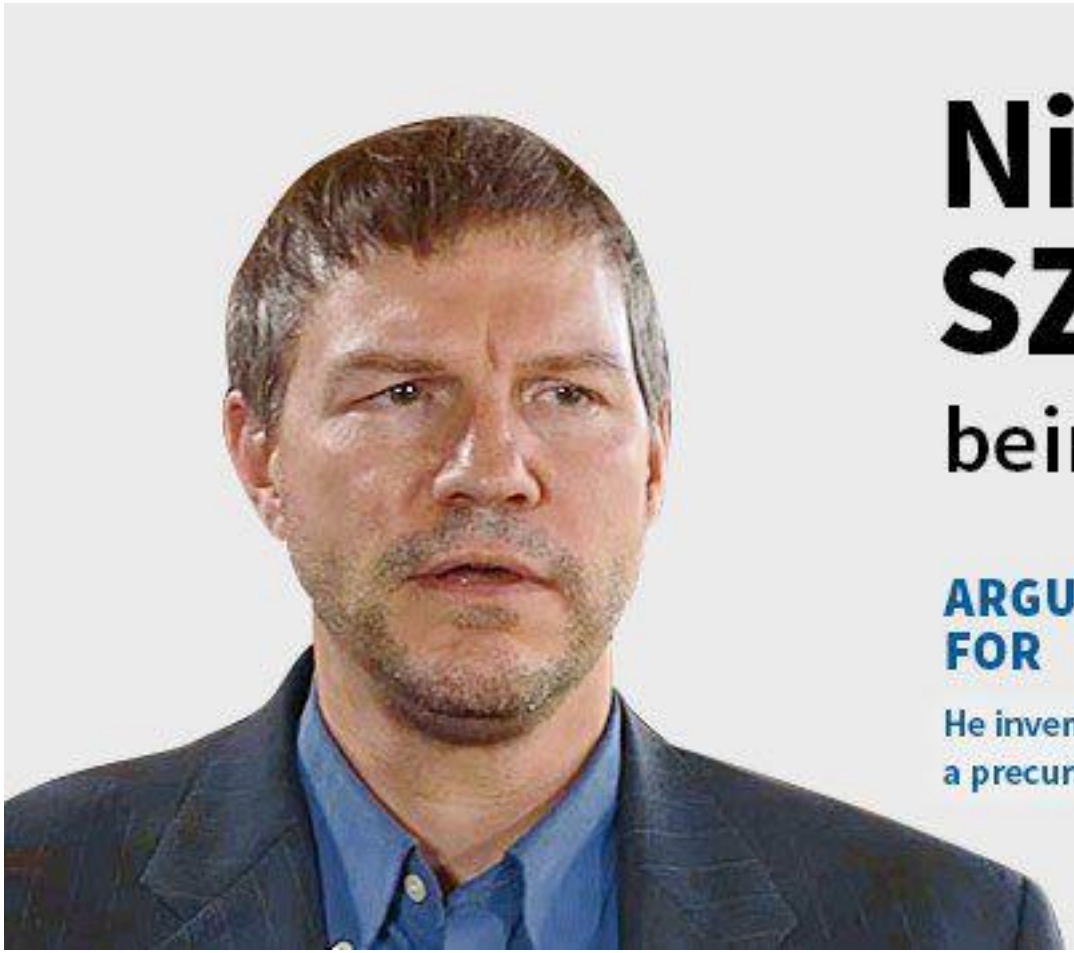
Craig WRIGHT being Satoshi ?

ARGUMENTS FOR

Timestamps of Nakomoto's blog coincide with Wright's blog

ARGUMENTS AGAINST

The PGP keys 'proving' he was founder were backdated, some allege



Nick SZABO being Satoshi ?

ARGUMENTS FOR

He invented Bit Gold, a precursor to Bitcoin

ARGUMENTS AGAINST

No compelling ones. Hm…

Debo Jurgen Etienne Guido claims he is Satoshi Nakamoto in a letter sent to the Florida courthouse. Debo also alleges that Craig Wright's claims are bunk.

How many bitcoins Satoshi owns?

- Estimated to be around 1 million!

First payment made using Bitcoin?

First payment made using Bitcoin

Hanyecz posted posted:

> *I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!*

First payment made using Bitcoin

- Some nine months after the pizza purchase, Bitcoin hit parity with the US dollar, making the two pizzas worth $10,000.

- Current Price: $214million?

Eric Schmidt (Google)

„[bitcoin] is a remarkable cryptographic achievement and the ability to create something which is not duplicable in the digital world has enormous value “ (März 2014)

Jamie Dimon (JPMorgan)

„worse than tulip bulbs “,
„it's a fraud “

(Sept. 2017)

Peter Thiel (Clarium Capital, Palantir, Facebook)

„if bitcoin ends up being the cyber equivalent of gold it has a great potential left “

(Oct. 2017)

Warren Buffett (Berkshire Hathaway)

“with almost certainty [cryptocurrencies] will come to a bad ending”

(Jan. 2018)