CS1699: Blockchain Technology And Cryptocurrency

1. History & Overview

Bill Laboon

From The Beginning…

The Billnited States of Billmerica
1
1
#00000001
ONE
BILL
BUCK
1
This signifies that one (1) Bill Buck is on retainer at the Bank of Bill.
1

- You want to create your own currency
- What characteristics should it have?

For more information on the history of money and Bitcoin, see The Bitcoin Standard by Saifedean Ammous

Properties of Money

- Durability.
- Portability.
- Divisibility.
- Uniformity.
- Limited supply.
- Acceptability.

Credit vs Cash

- Credit: Debt-based system
- Cash: “External” medium of exchange
- Benefits and drawbacks to each - no perfect solution

Reality

- Different societies used different mechanisms
- For cash, a variety of physical objects were found which met this need
- Silver, gold, cowrie shells, wampum, glass beads, Federal Reserve Notes acted as “cash”
- Difficult to translate this into digital form
    - Why?

FirstVirtual

- Basically an escrow account - you would give them your credit card information, they would purchase things “for” you from different sites
- Never caught on - merchants had to wait 90 days for every transaction to be cleared!

SET Architecture

- Allowed you to encrypt your credit card number and send an encrypted version through an intermediary
- Seller cannot see your actual credit card information - buyer, seller, and intermediary would come to an agreement by each coming up with an encrypted version
- Did not succeed because every user needed to get a certificate - a boring, technical, arduous process in the '90s

Digital Credit to Digital Cash

- Cash needs to be bootstrapped, but…
  - Has no risk of default (assuming that the underlying currency is sound!)
  - Credit is by its nature not anonymous, very trackable
  - With credit, you must be online (checking with a centralized authority) or willing to deal with swindlers!

Chaumian Ecash

- First serious digital money proposal
- In 1983, cryptographer David Chaum had an idea - blind signatures
- A blind signature allowed someone to sign a document and prove their ownership while at the same time hiding the information in the document
- You could "prove" that you owned some money (stored at a bank) by signing a transaction (credit-based)
- Anonymous but still required centralization
- Commercialized as DigiCash - tried out at a single bank, later company went bankrupt

Reference: http://blog.koehntopp.de/uploads/Chaum.BlindSigForPayment.1982.PDF

The Double-Spend Issue

- Alice has an ecash note, serial 0x86A54399B01738
- She buys a hot dog from hot dog vendor Bob with the note. Bob does not have access to the Internet from his hot dog stand.
- She then goes over to Carol's ice cream shop and pays with the same note.
- How can we prevent a "double-spend", i.e., how can Bob and Carol know that the note is legitimate?

The Double-Spend Issue

- They can’t!
- Chaumian ecash avoids double-spend by determining AFTER the fact (Chaum-Fiat-Nour scheme)
- Your identity is safe UNLESS multiple parties try to redeem your note, in which case you are fingered as the culprit… but this is done after you have eaten your hot dog and ice cream

Anonymity

- Buyers were anonymous, merchants were not
- They had to check in with the centralized bank server to determine validity of notes

Money For “Nothing”

- Chaumian ecash, despite its name, was pseudo-debt - to get the money, you bought it from the bank, and it represented a claim on the bank’s assets
- Similar ideas: Liberty Reserve, Digigold, e-Gold, the nascent currency in Neal Stephenson’s *Cryptonomicon* - represent a claim on some other asset (e.g., gold)

Scarcity

- Recall our fifth property of money - it must be of limited supply, you must work to get it
- Computers can do computation work
- So we can we use computation as the backing for our currency?

Computational Backing

- This was the idea behind Dwork and Naor's paper (1992), later expanded into a commercial product with Adam Back's Hashcash
- Alice sends Bob an email. Before Bob can see it, his computer asks Alice's computer to solve a math problem which would take a few seconds to solve (think of a CAPTCHA for computers) and send him the answer
- Answer is specific to that email, thus rate-limiting and avoiding spam - user (computer) has to do "work" to get something (successful delivery of mail)
- "Bitcoin is Hashcash extended with inflation control" -Adam Back

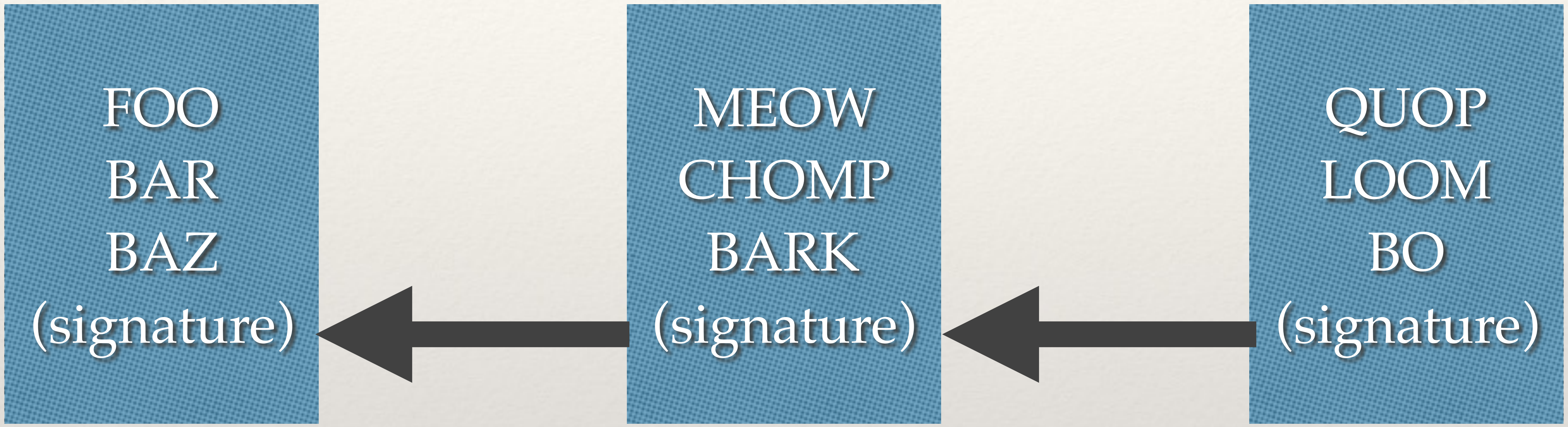
Pricing via Processing or Combatting Junk Mail, Dwork, Cynthia and Moni Naor. https://dl.acm.org/citation.cfm?id=705669

Ledgers

- How to determine the order / timestamp of documents in a decentralized manner?
- If we know Document d_1 was written before d_2, and d_2 before d_3, etc., we can have a good idea of when a document was written (and definitely know the order)
- How to enforce order? Links to previous document!
- This makes a *chain* of documents…

How to Timestamp a Digital Document. Haber, Stuart and Scott Stornetta. https://www.anf.es/pdf/Haber_Stornetta.pdf (1991)

Linked Timestamping



FOO
BAR
BAZ
(signature)

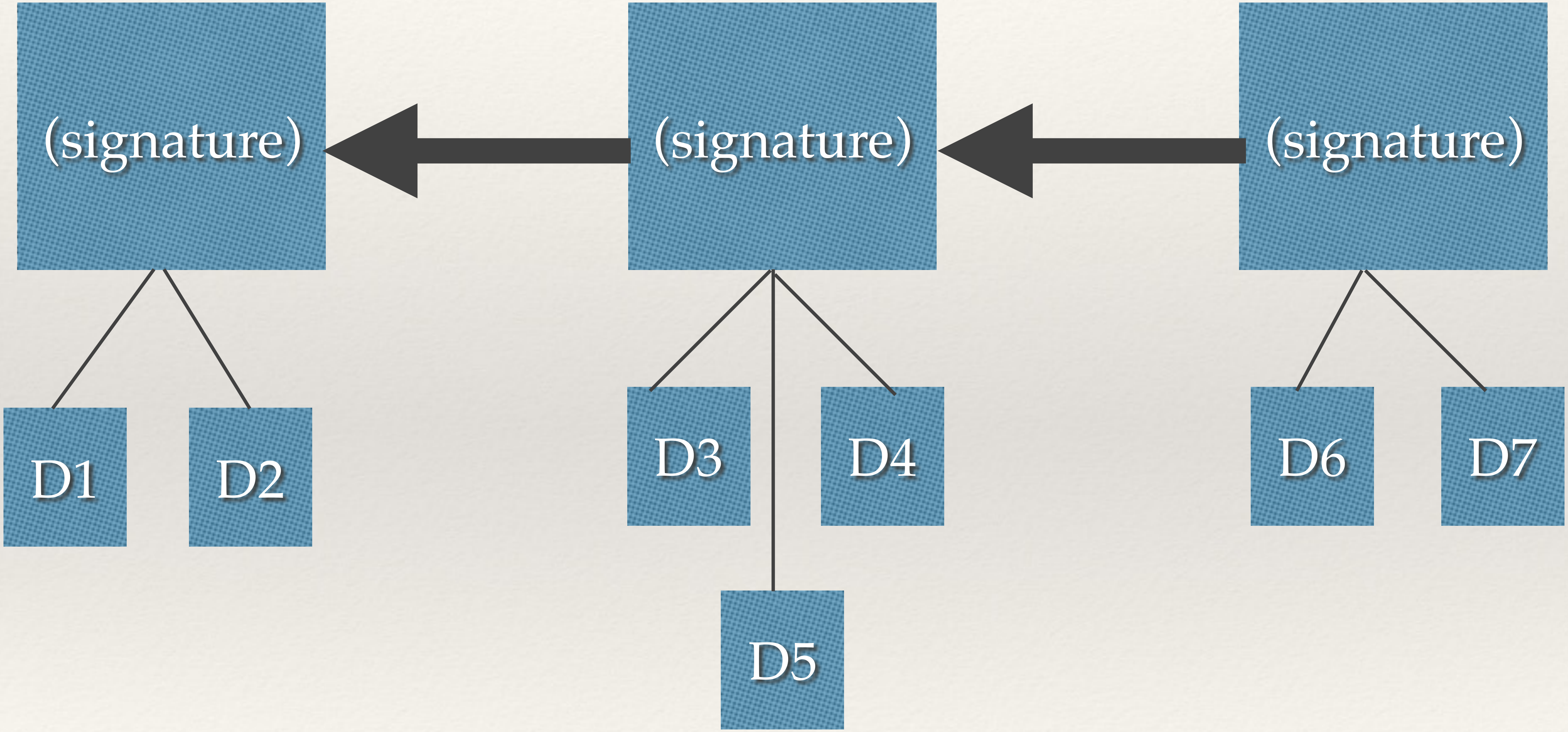
MEOW
CHOMP
BARK
(signature)

QUOP
LOOM
BO
(signature)

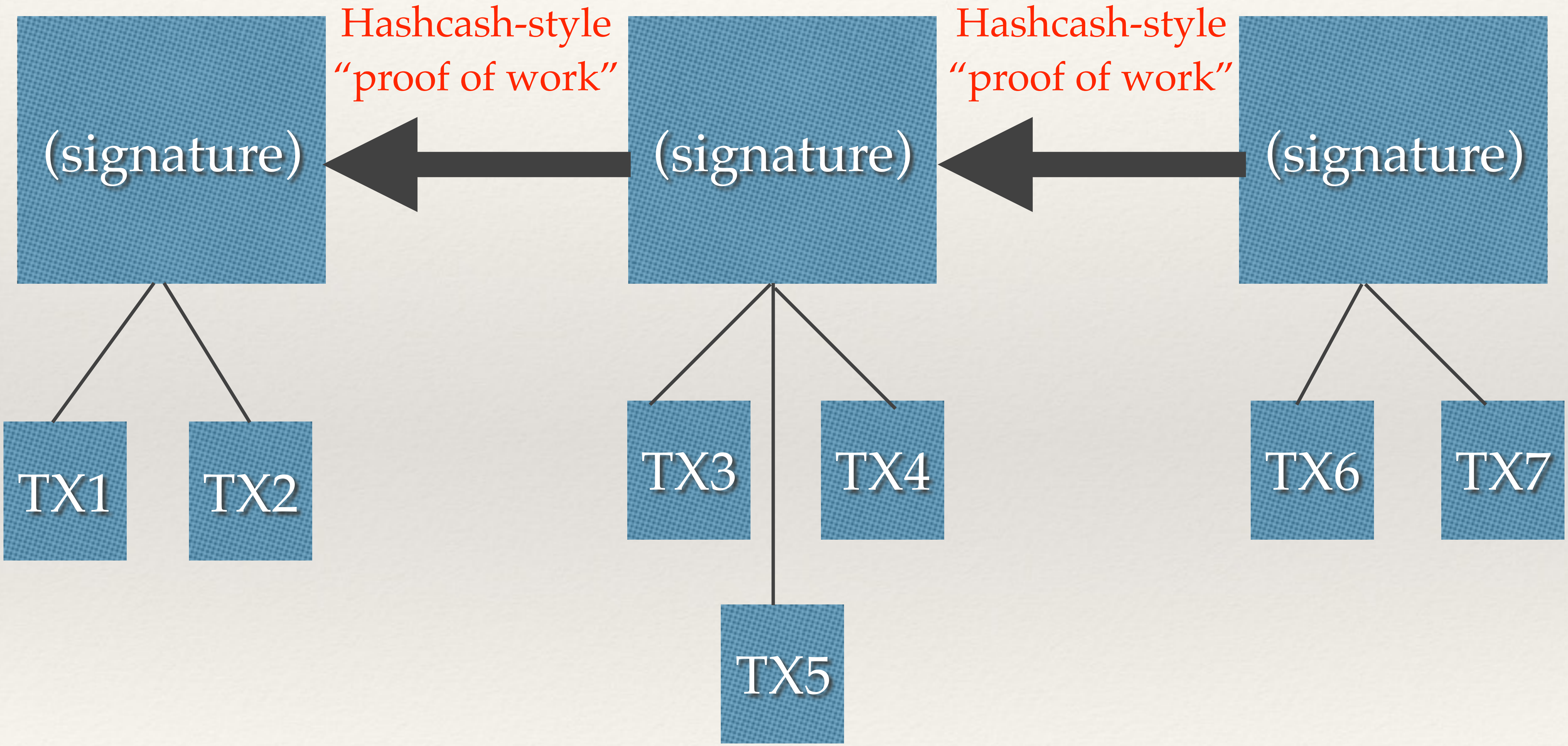
Efficiency of Linked Timestamps

- Turns out this is very inefficient for large number of documents, and we also usually don’t need that much granularity
- Improvement: collect documents into groups (“blocks”) and only have the signature link going from block to block
- In other words, a “block chain”

A "Block Chain"



Bitcoin-style "Blockchain"


(signature)
Hashcash-style "proof of work"
(signature)
Hashcash-style "proof of work"
(signature)
TX1
TX2
TX3
TX4
TX5
TX6
TX7

The Bitcoin Genesis Block

```
01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E
67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA
4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C
01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D
01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F
4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C
6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20
73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66
6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05
2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27
19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6
79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4
F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 5
8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00
```

```
..EThe Times 03/
Jan/2009 Chancel
lor on brink of
second bailout f
or banksÿÿÿÿ..ò.
```

Resolving the Double-Spend Issue?

- If we assume that this computationally difficult blockchain is the ground truth, no longer a need for a centralized server or source of truth
- Several proposals using this scheme: bitgold (Wei Dai), b-money (Nick Szabo)
- In both schemes, computational challenges directly map to created money, and no way to determine what happens if users disagree on blocks

Resolving the Double-Spend Issue!

- With Bitcoin, creating the link to a previous block (and generating a new one via a complex computational challenge) creates money
- In case of conflict, chain with most work behind it wins (originally it was the longest chain, this has since been modified)
- This is what miners are doing and what they are rewarded for
- Key modification that allowed Bitcoin to solve previous digital money problems

Satoshi Nakomoto

- Bitcoin was created by the pseudonymous “Satoshi Nakomoto”
- Note that Satoshi is a male Japanese name, but there is no evidence that they are a male, female, or possibly a collective
- Satoshi interacted with people online for several years, then went dark entirely
- Many theories on his true identity
- Writings collected in “The Book of Satoshi”, edited by Phil Champagne

“Bitcoin: A Peer-to-Peer Electronic Cash System”, by Nakomoto, Satoshi. https://bitcoin.org/bitcoin.pdf

Mining Challenge

- Take my name “Bill Laboon” and convert each letter (ignore spaces and capitalization) into its equivalent numeric value (A=1, B=2…Z=26)
- For each entry, square it and add four (e.g., A = 1^2 + 4 = 5, B = 2^2 + 4 = 8, etc.)
- Sum up all of entries
- Add one to the number, write it down on a piece of paper and hand it to me
- First person to hand me the correct result wins