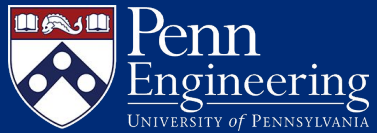
Introduction to Blockchain

Web3 Builders workshop series #1

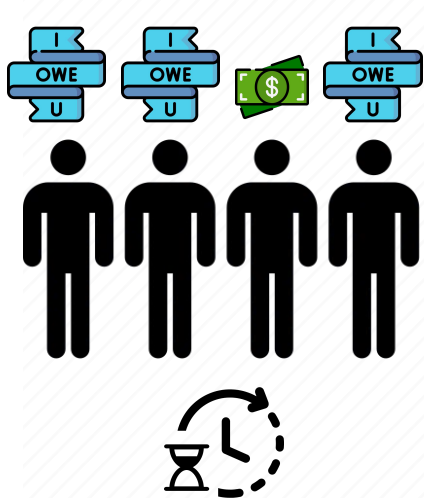


Disclaimer

- This workshop series is **not** designed to teach you everything about blockchain, but it serves as a starting point for you to do your own research
- We will not be going into too much details, but feel free to discuss more about it with us after the main workshop!
- Feel free to interrupt us anytime you want
- Enjoy :)

Once upon a time before Splitwise was a thing…

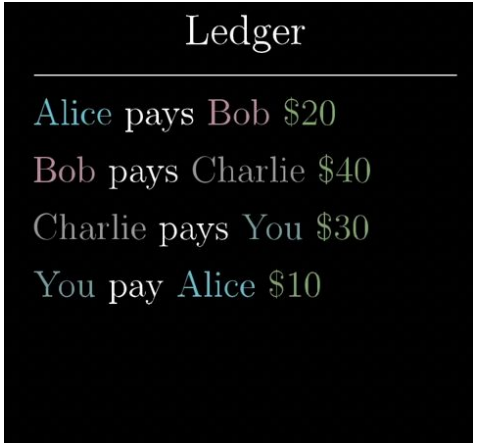
- Four friends, Alice, Bob, Charlie, and Dylan often eat out together
- Only one of the friends gets the bill and everyone else owes them money (credit)
- Friends don’t want to have to deal with cash everytime they eat out
- At the end of a period of time, friends come together and settle the debit/credit
- Is there a system that we can employ to make this happen?



Penn Engineering University of Pennsylvania
Wharton University of Pennsylvania

The ledger

- Instead of settling who owes who however much money after each meal and dealing with cash, friends kept a log of debits and credits (a log of transactions).
- This log of transactions is called **the ledger**.
- By tracing through the records of the ledger, we can calculate how much debits and credits each friend has at the current time.
- Friends with credits owe friends with debits money
- Sum of debits == sum of credits
- Only deal with cash at the end when friends want to settle



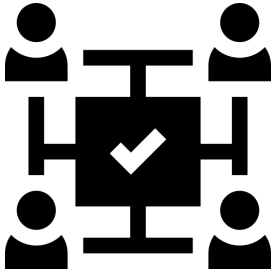
Required properties of the ledger for it to work

Non-invertibility

- Confirmed transaction records are **immutable** and cannot be modified or deleted
- Transaction history is also **immutable**

Non-repudiation

- Whoever created a confirmed transaction **cannot deny** that they were the creator of the transaction
- People cannot effectively pretend as anyone else without their consent



Consensus

- There must be **only one** version of the ledger that is **agreed and accepted** by everyone

Penn Engineering
University of Pennsylvania

Wharton
University of Pennsylvania

What is a blockchain?

- Persistence: Append only (no deletions)
- Sequential order
- Consensus: Same data visible to all
- Liveness: Blocks are added continuously
- Created in a distributed manner
- No need for a trusted party

if trusted party exists ⇒ no need for a blockchain lol

What is all the excitement about?

(1) Basic application:

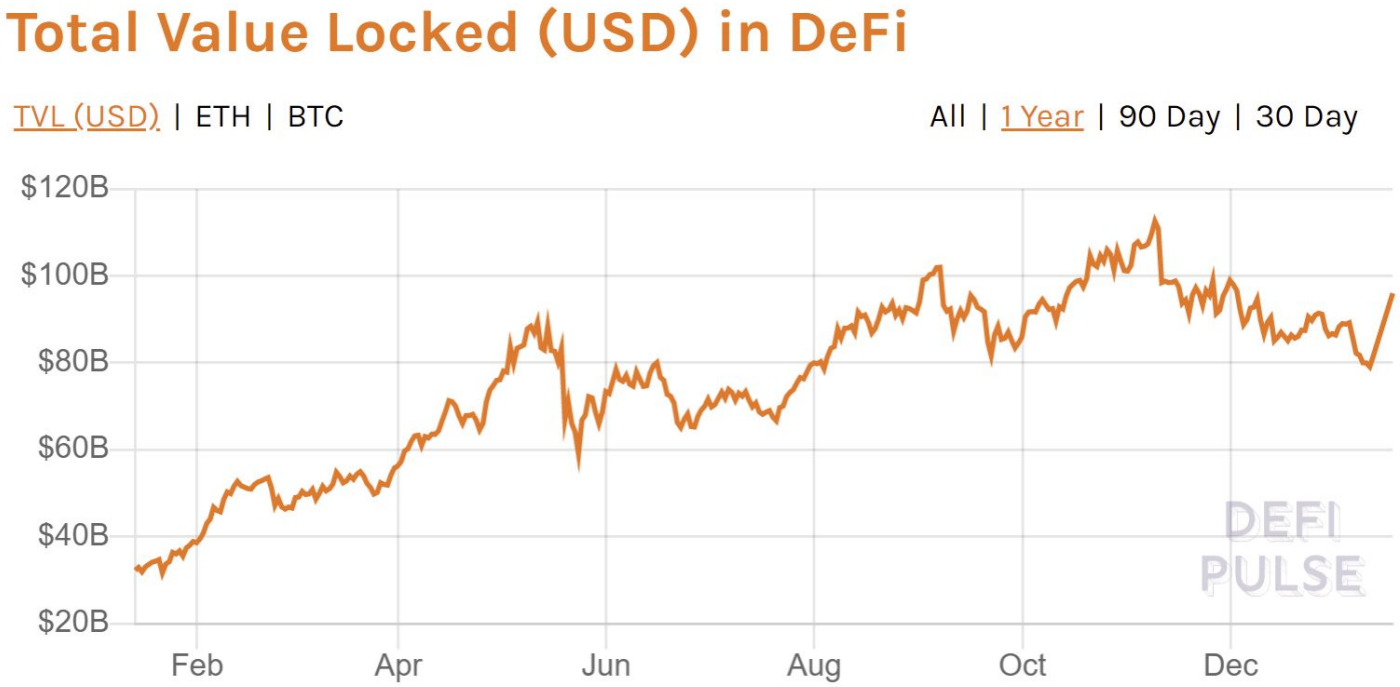
- a **digital currency** (stored value)
  - Current largest: Bitcoin (2009), Ethereum (2015)
- Global: accessible to anyone with an Internet connection

What is all the excitement about?

(2) Beyond stored value:

- decentralized applications (**DApps**)
- **DeFi**: financial instruments managed by public programs
  - examples: stablecoins, lending, exchanges, …
- **NFT**: art, game assets, ….
- Decentralized organizations (**DAOs**): decentralized governance
- DAOs for investment, for donations, for collecting art, etc.

Assets managed by DAPPs



Penn Engineering University of Pennsylvania

Wharton University of Pennsylvania

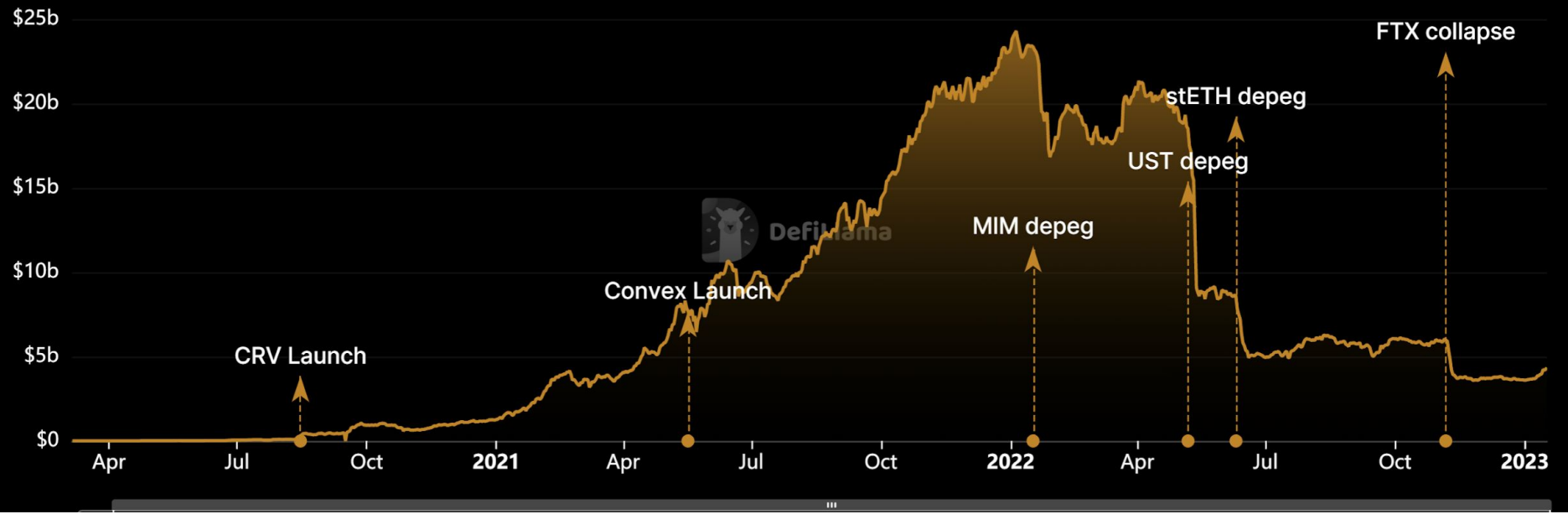
Include in TVL (optional)

Staking

$545.88m

USD ETH

Hide Events Show MCap Chart



Transaction volume

	24h volume Sep. 2021	24h volume Jan 2023
Bitcoin • BTC	$[illegible]B	23B
Ethereum • ETH	$[illegible]B	7B
Cardano • ADA	$[illegible]B	380M

Penn Engineering University of Pennsylvania

Wharton University of Pennsylvania

Central Bank Digital Currency (CBDC)

Penn Engineering University of Pennsylvania

Wharton University of Pennsylvania

When poll is active, respond at **PollEv.com/intelchen259**

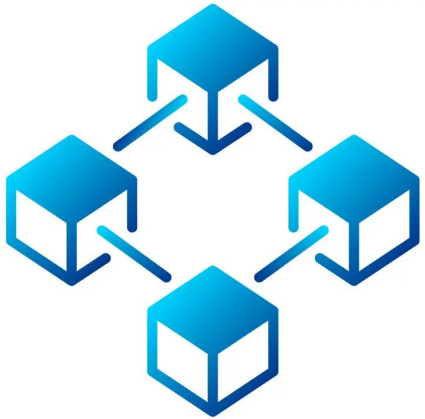
Text **INTELCHEN259** to **22333** once to join

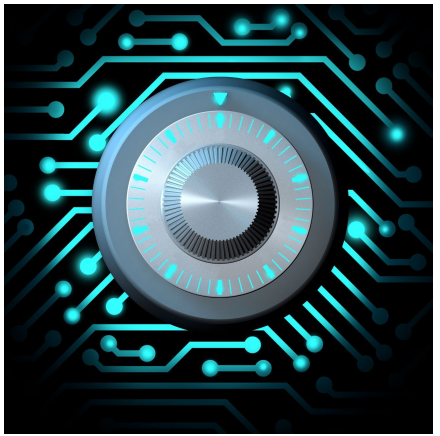
What is blockchain

Penn Engineering
University of Pennsylvania

Wharton
University of Pennsylvania

Blockchain ≠ Bitcoin ≠ Crypto ≠ Web3.0





Penn Engineering
University of Pennsylvania

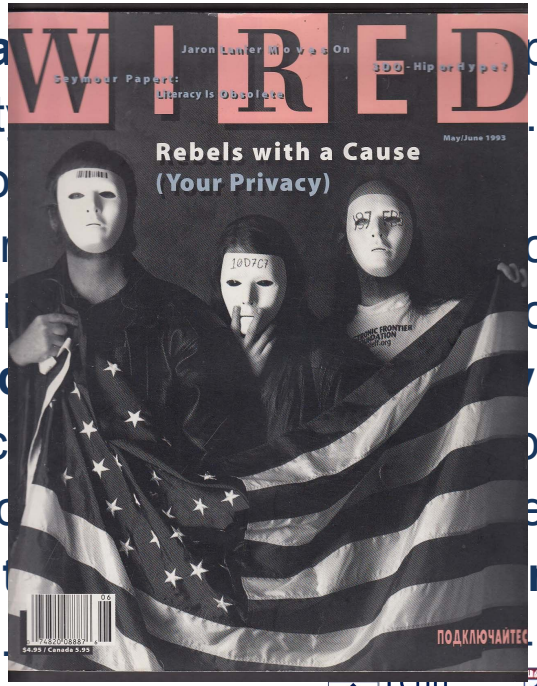
Wharton
University of Pennsylvania

The Origin of Blockchain

Origin of the Philosophy

"p to
c
a
n
r out
e
i ia
extensive re-routing of encrypted packets…" -1988 Timothy C. May

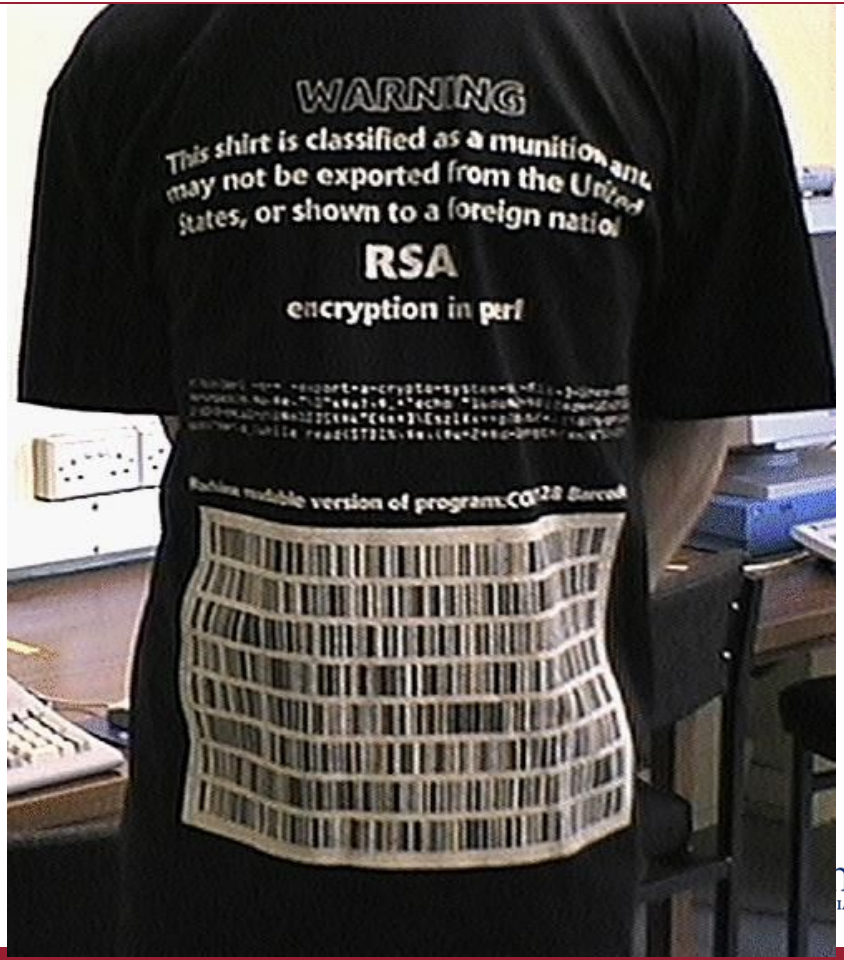
"**Priva** pen
societ . We
canno
corpor celess
organi cy ... We
must **c** if we
expec unks
write c eone has
to **writ** **rivacy**,
and ... 1993 Eric Hughes



Penn Engineering
University of Pennsylvania
Wharton
University of Pennsylvania

Key Beliefs

1. Privacy of Communications
2. Anonymity and pseudonymity
3. Privacy and self-revelation
4. Censorship and monitoring
5. Digitization of trade
6. Redefine property rights



Technology + Philosophy = Application

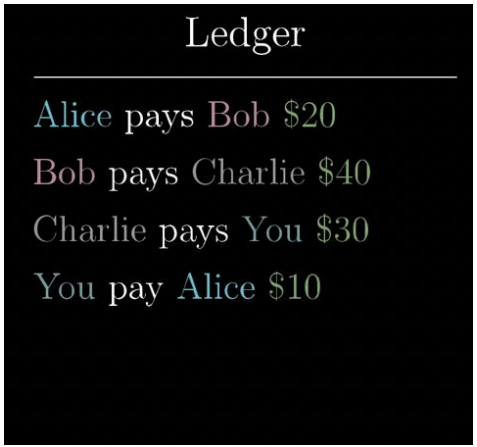
- 1989 Digicash (anonymous money transfer thru banks)
- 1996 E-Gold (digital currency backed by gold)
- 1997 Hashcash (proof of work)
- 1998 B-money (proof of work + digital currency + decentralized)
- 1998 BitGold (proof of work + digital currency + decentralized + “chaining”)
- **…. Bitcoin!!**

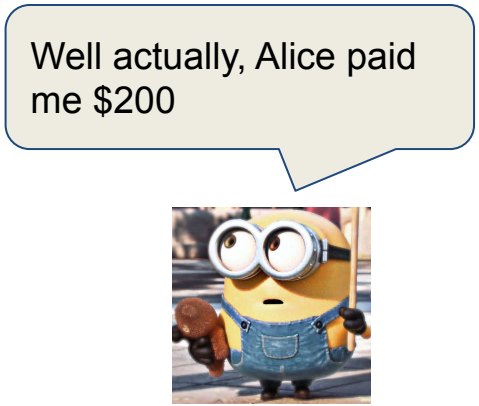
Back to Alice and friends

How do we achieve immutability

Problem:

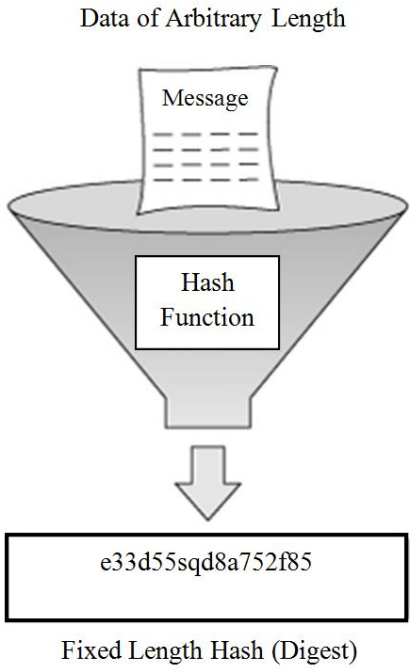
You have a ledger and a friend group. People will add transactions to this ledger. How do you prevent people from changing the content of the record book?





Bob

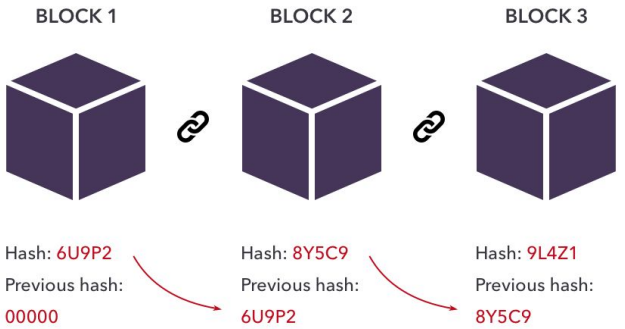
Hash



https://www.figma.com/proto/sqewqjemMFsBjXDkZRhOb6/W3B-Animations?page-id=0%3A1&node-id=1%3A3&viewport=713%2C471%2C0.1&scaling=contain&starting-point-node-id=1%3A3&show-proto-sidebar=1

Hash Chain

https://www.figma.com/proto/sqewqjemMFsBjXDkZRhOb6/W3B-Animations?page-id=0%3A1&node-id=1%3A2017&viewport=713%2C471%2C0.1&scaling=contain&starting-point-node-id=1%3A2017&show-proto-sidebar=1



Penn Engineering University of Pennsylvania
Wharton University of Pennsylvania

Origin of the Technology

Ittai Abraham @ittaia

The longest running blockchain started in 1995 and is still running strong today. Current hash circled in red. Based on Stuart Haber and W. Scott Stornetta

6:13 PM - 22 Aug 2018

Penn Engineering
University of Pennsylvania

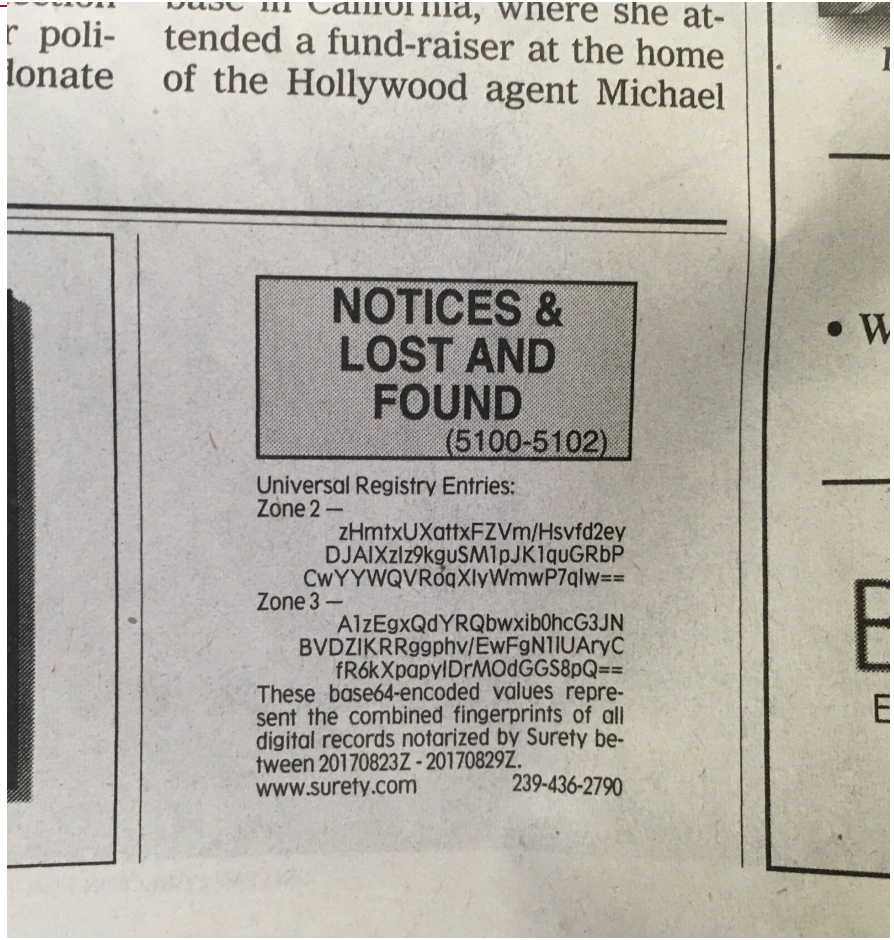
Wharton
University of Pennsylvania

from the White House.

After Mr. Trump publicly exploded against Mr. Rosenstein this month, Mr. Sessions called Donald F. McGahn II, the White

NOTICES & LOST AND FOUND
(5100-5102)

Universal Registry Entries:
Zone 2—
HiCeghjtkivSiQqu5xPlmp9oc
pkGr/HOrnw5HMAOWk3JO8bT
kRkyS2pNTaVpCrhqClpmEQ==
Zone 3—
uaXUfpKmgPUWOlSMSW+KMq
nq84HWrVRdABwrT6lpnYXzdQ2
+HqQYlwBT88LuZsNkuUJFVA==
These base64-encoded values represent the combined fingerprints of all digital records notarized by Surety between 20180411Z - 20180417Z.
www.surety.com 239-436-2790



poli-
lonate

tended a fund-raiser at the home of the Hollywood agent Michael

NOTICES & LOST AND FOUND
(5100-5102)

Universal Registry Entries:
Zone 2 —
zHmtxUXattxFZVm/Hsvfd2ey
DJAIXzlz9kguSM1pJK1quGRbP
CwYYWQVRoqXlyWmwP7qlw==
Zone 3 —
A1zEgxQdYRQbwxib0hcG3JN
BVDZIKRRggphv/EwFgN1IUAryC
fR6kXpapyIDrMOdGGS8pQ==
These base64-encoded values represent the combined fingerprints of all digital records notarized by Surety between 20170823Z - 20170829Z.
www.surety.com 239-436-2790

How to we achieve non-repudiation?

Problem: can you deny the validity of a confirmed transaction signed by you? (this is bad)

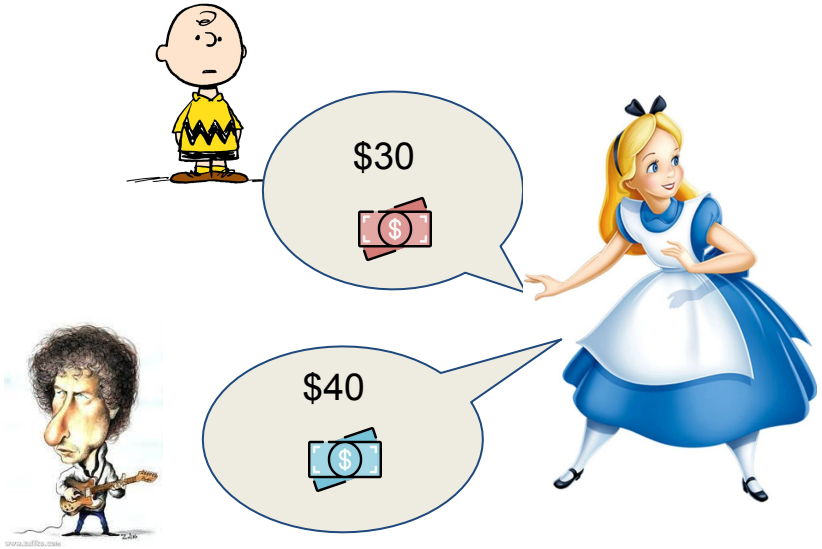
How can you make sure no one can pretend to be you and you can’t pretend to be other people?

Public private key cryptography

1. Everyone have an un-forgeable stamp
2. They protect it with their life, no one except themselves can use it

How do we get consensus

Problem: Alice told two friends two different versions of a valid transaction



$30

If alice can pay both?

If alice can only pay one?

PoW

Essentially majority voting

but each vote you need to solve a cryptographic puzzle (supposedly no cheating)

It's really hard to cheat for a single party

<hashing challenge> (look up SHA256 ONLINE)

1. Find a hash with 1 leading 0.
2. Find a hash with 2 leading 0.

Why does this also contribute to immunity(non-invertibility)?

PoW

At time T, Alice has $30 in her ledger account, yet she told B and C that she wants to transfer them $30 and $20 each.

1. Can’t spend both. The one received by the Ledger later will get rejected due to lack of funds
2. Can’t go back to reconstruct the entire history of blockchain to add more funds
   a. Easy to detect that the hash has changed
   b. (PoW) In turn need to recompute the cryptographic puzzle in each block
3. If some of Alice’s friend believes one truth, and some the other, they get together and vote by majority -> 51% attack

How a blockchain works - Animated

https://www.figma.com/proto/r34qLPnbRKEhyDXgmWzb52/CIS-2330-Animations?page-id=0%3A1&node-id=1%3A2&viewport=854%2C491%2C0.27&scaling=contain&starting-point-node-id=1%3A2&show-proto-sidebar=1

Optional Activity: Classroom Blockchain

Extra resources

https://www.youtube.com/watch?v=bBC-nXj3Ng4

Join Web3 Builders to learn more about blockchain

Penn Engineering
University of Pennsylvania

Wharton
University of Pennsylvania