SNAKES INTO SNAKE OIL

What Blockchains Are And Why They're Terrible

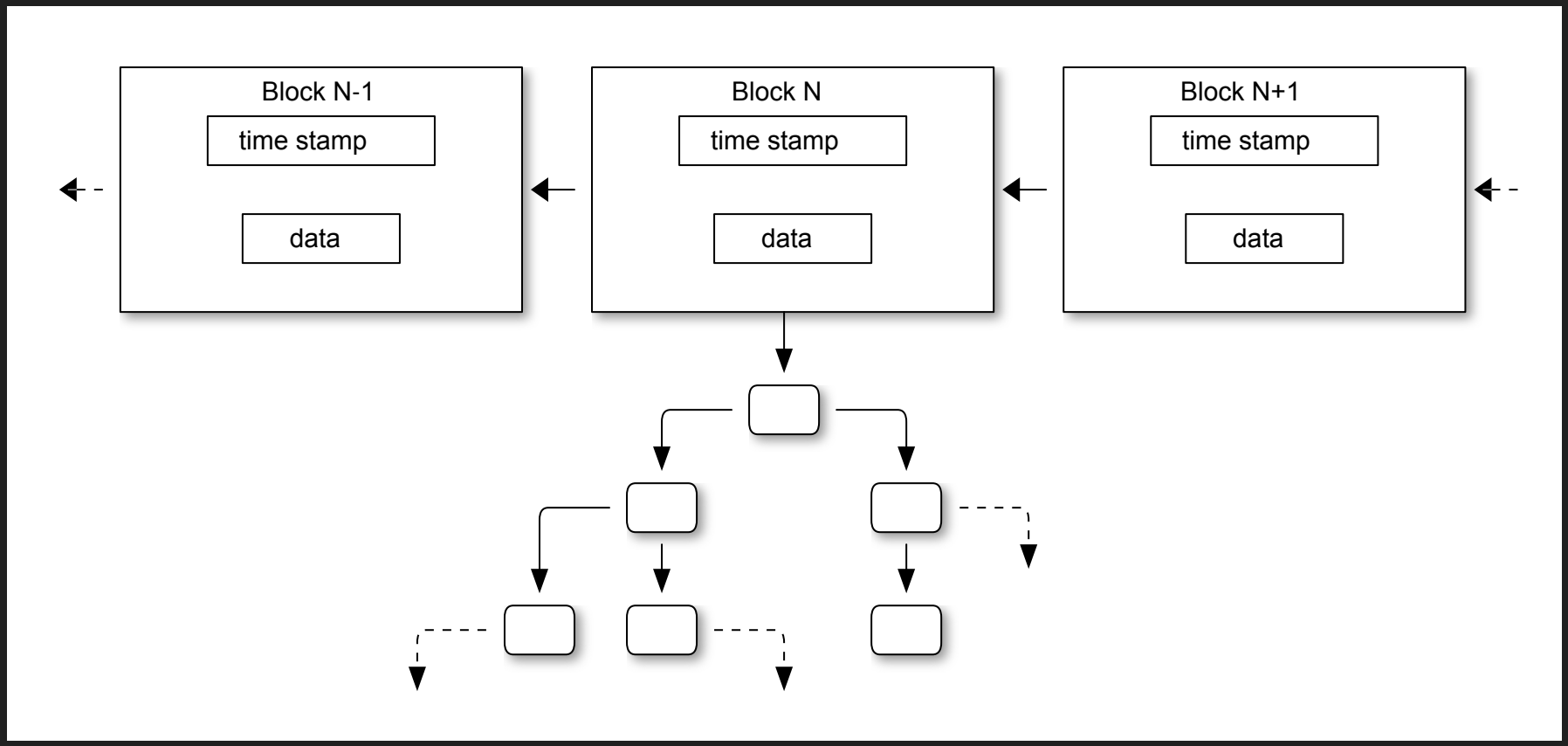
Jez Higgins

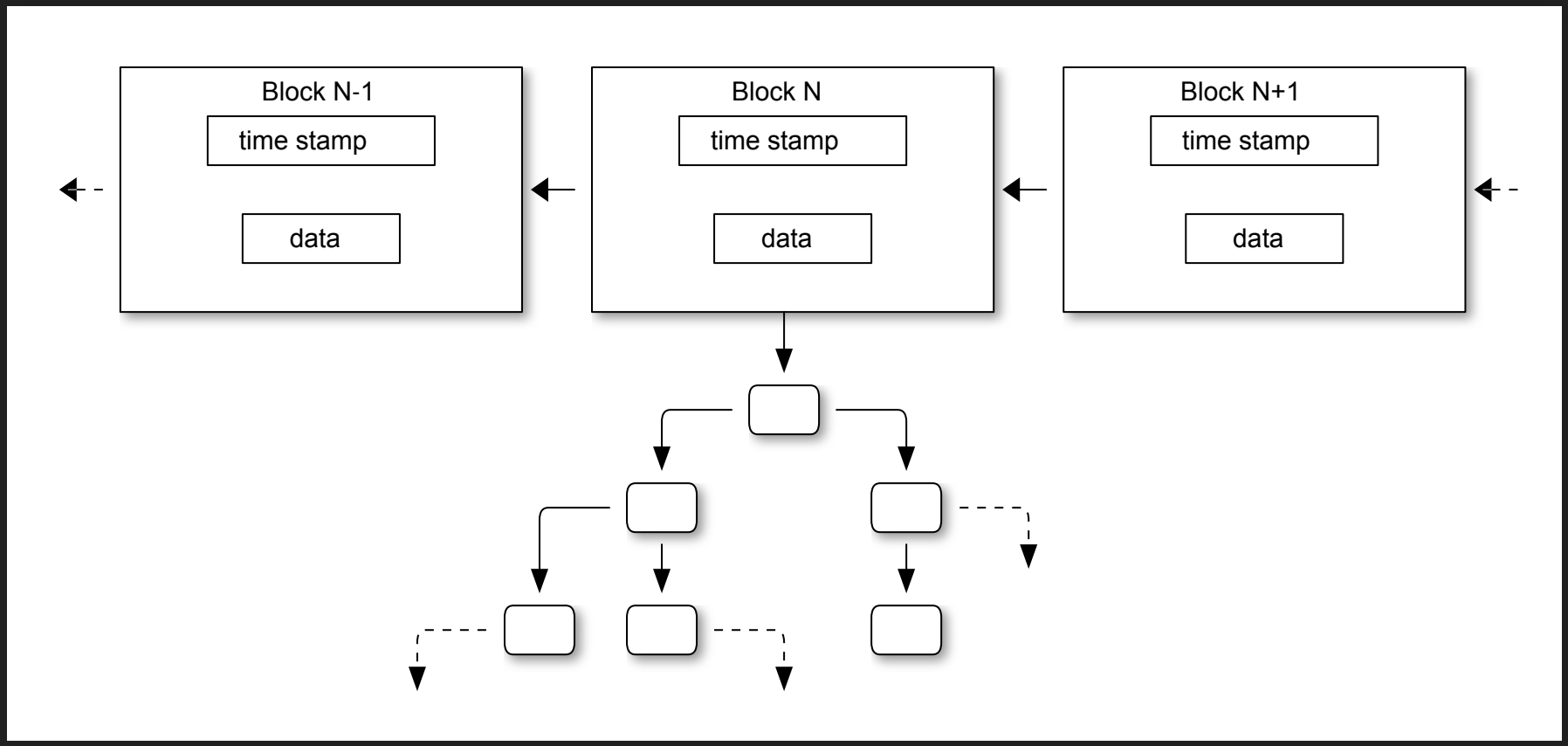
Did I want my name associated on the internet with the words Blockchain and Cryptocurrency?

- What Blockchains Are

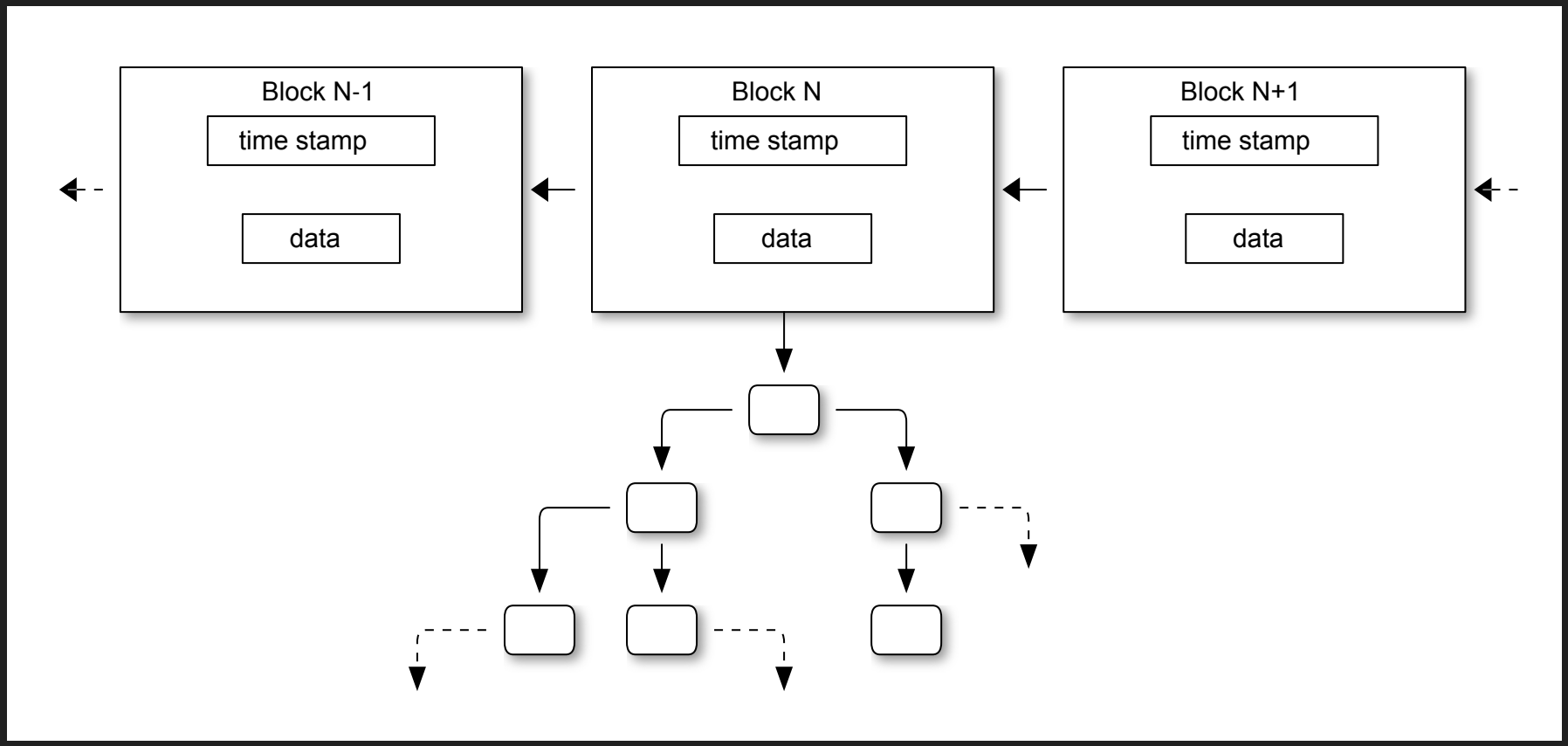
- What Blockchains Are
- Why They’re Terrible

SNAKES INTO SNAKE OIL


Block N-1
time stamp
data
Block N
time stamp
data
Block N+1
time stamp
data

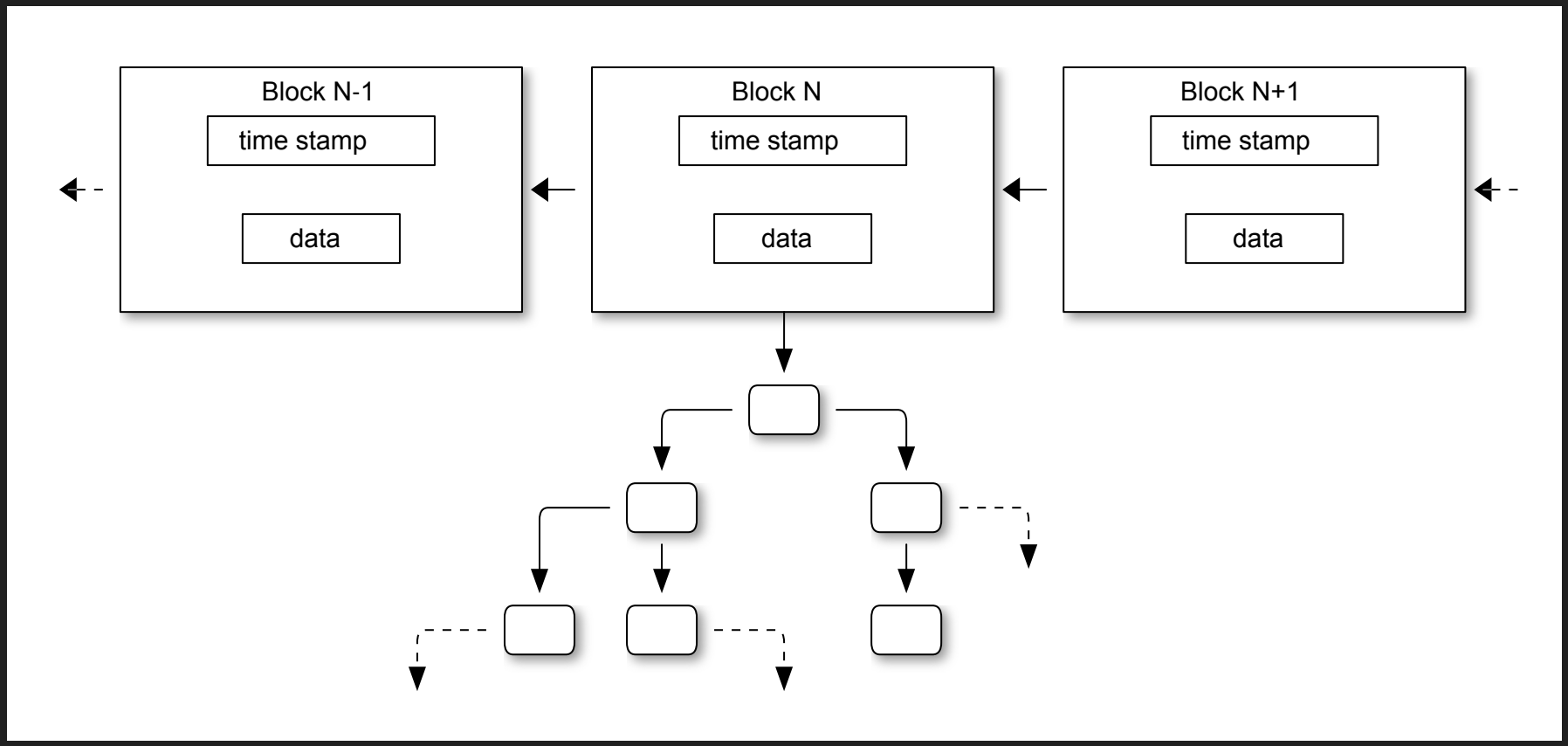

Block N-1
time stamp
data
Block N
time stamp
data
Block N+1
time stamp
data

append only



append only

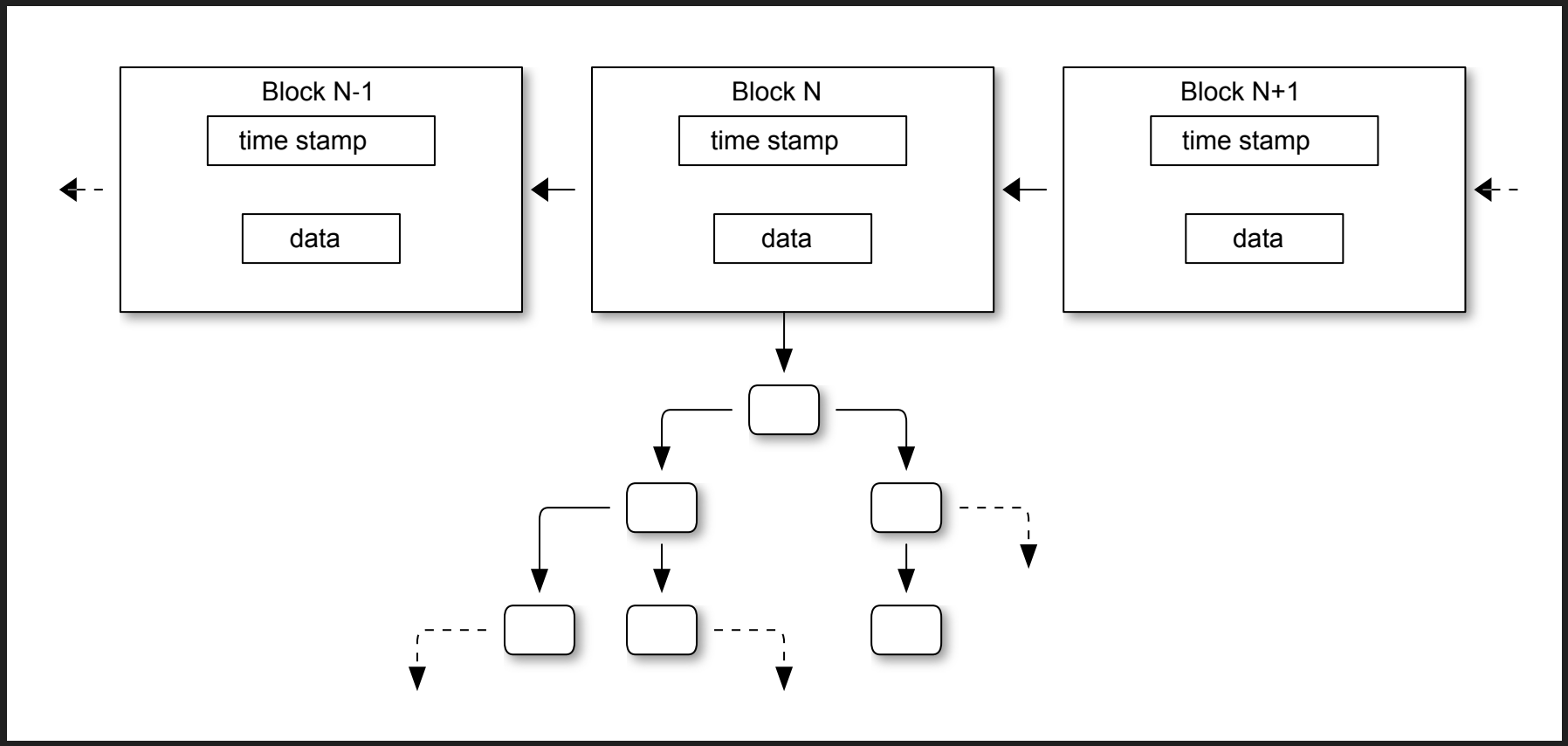
guarantees provenance



append only

guarantees provenance

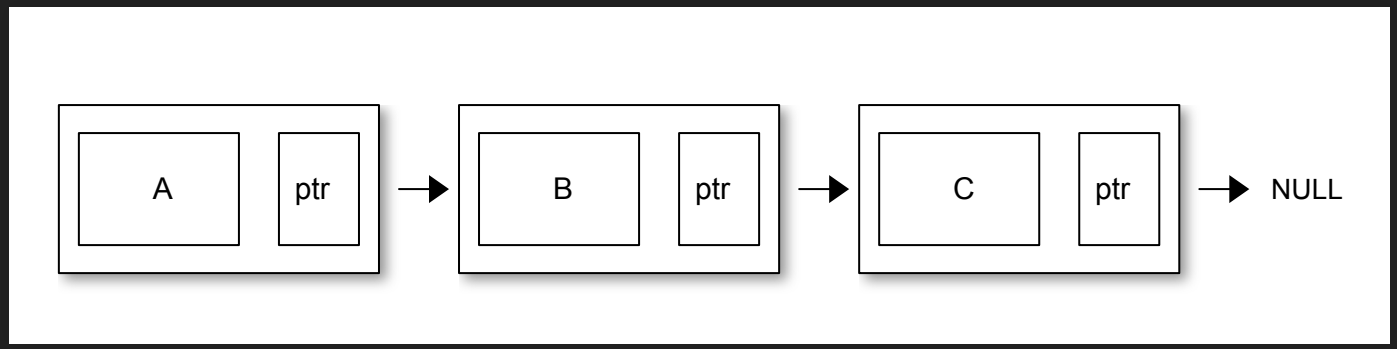
distributed database

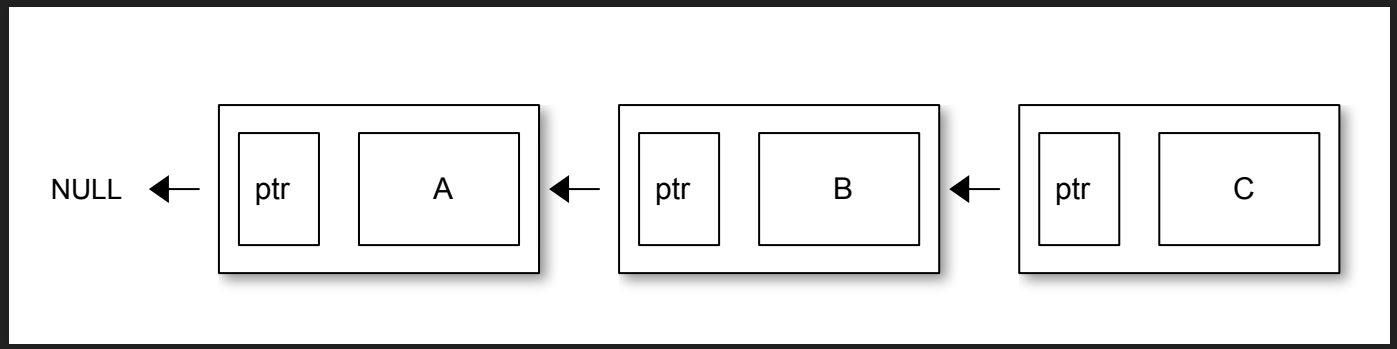


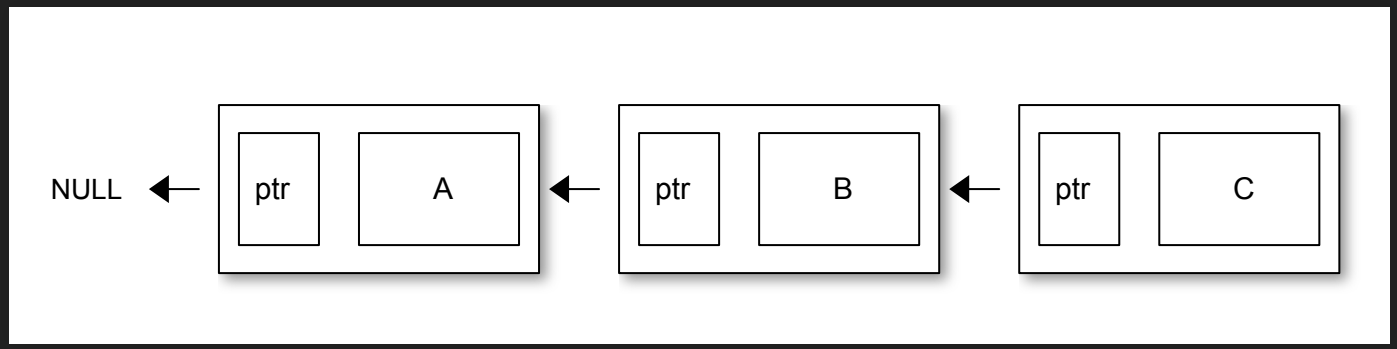
append only
guarantees provenance

distributed database
no central authority

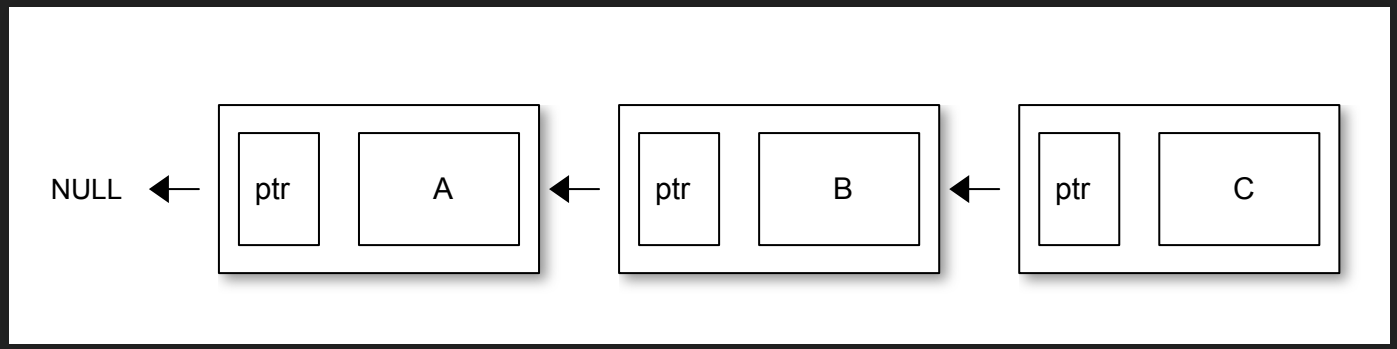
BUILDING A BLOCKCHAIN


A
ptr
B
ptr
C
ptr
NULL

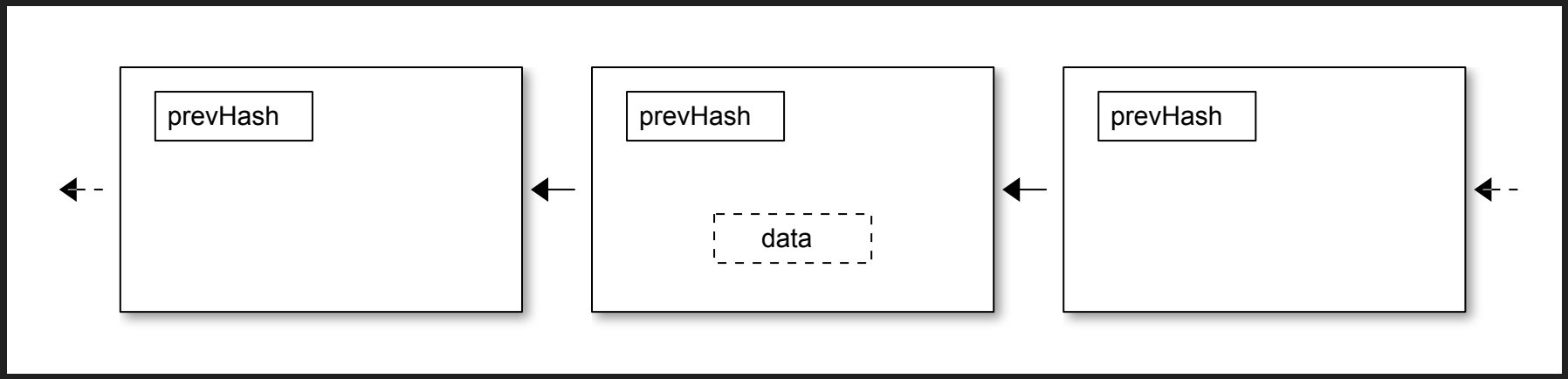

NULL
ptr
A
ptr
B
ptr
C

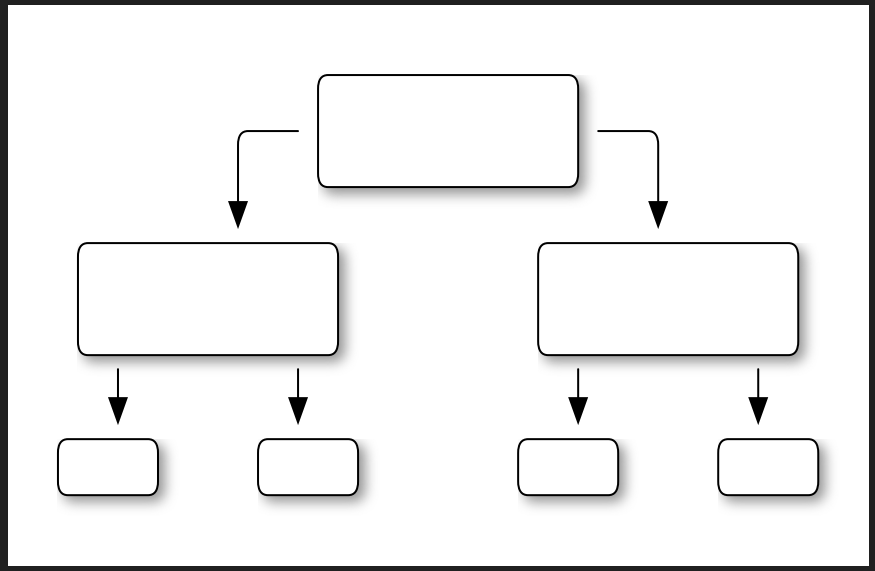


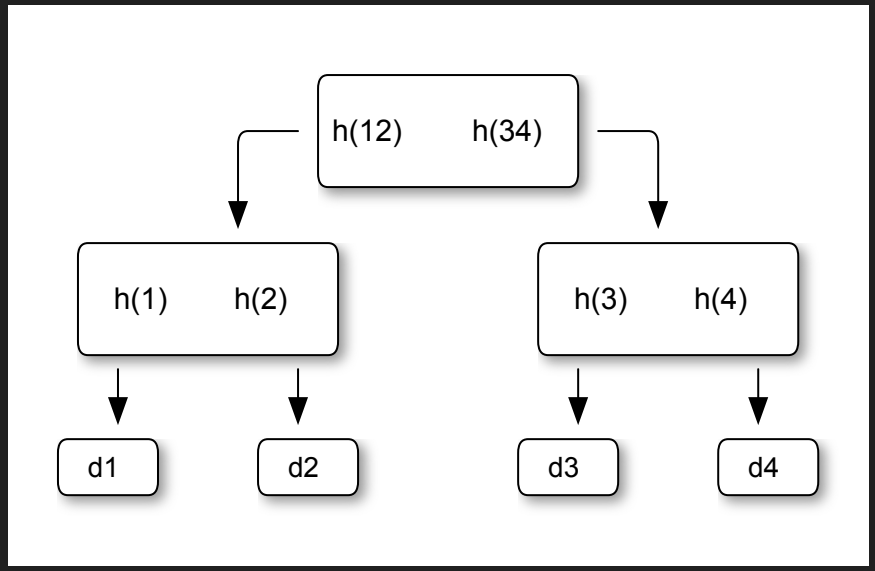
- the block before me is block 742

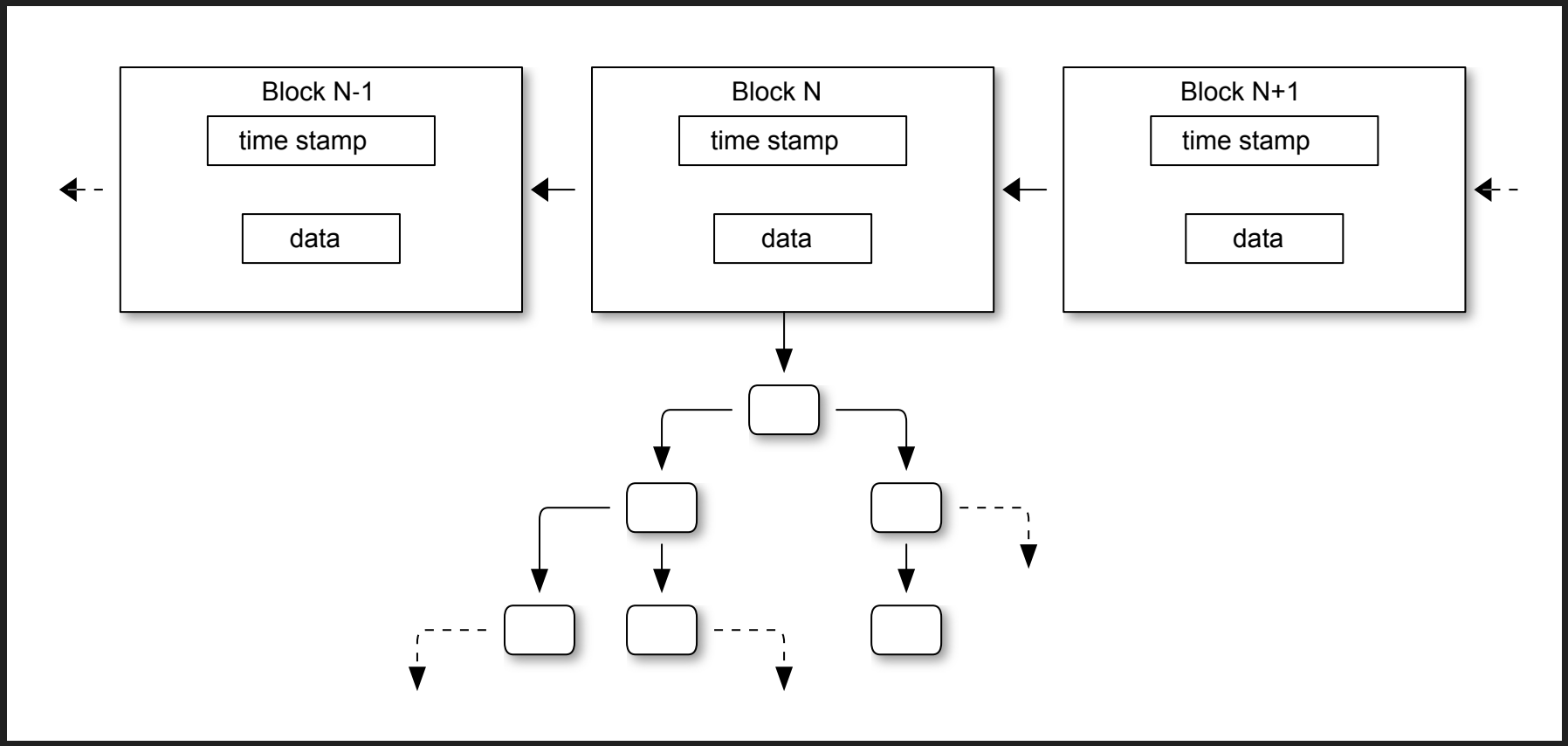


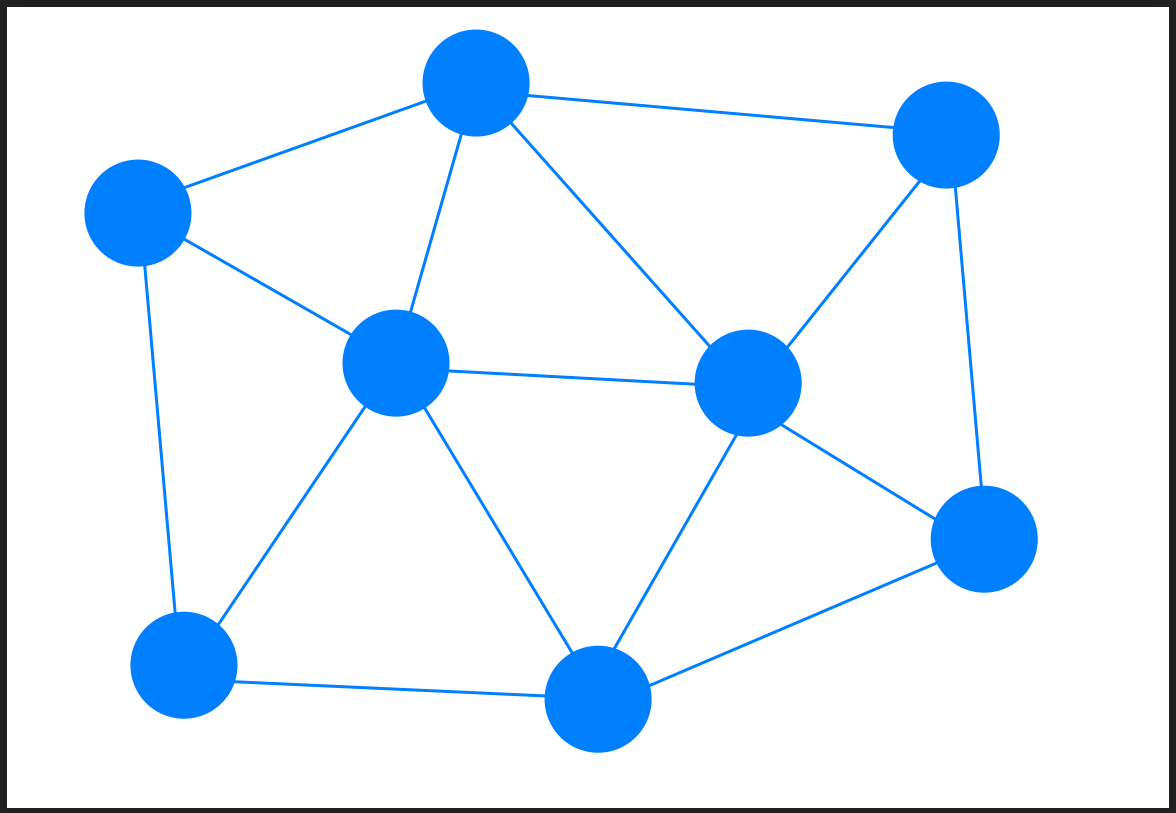
- the block before me is block 742
- and its hash is 0x371291a…

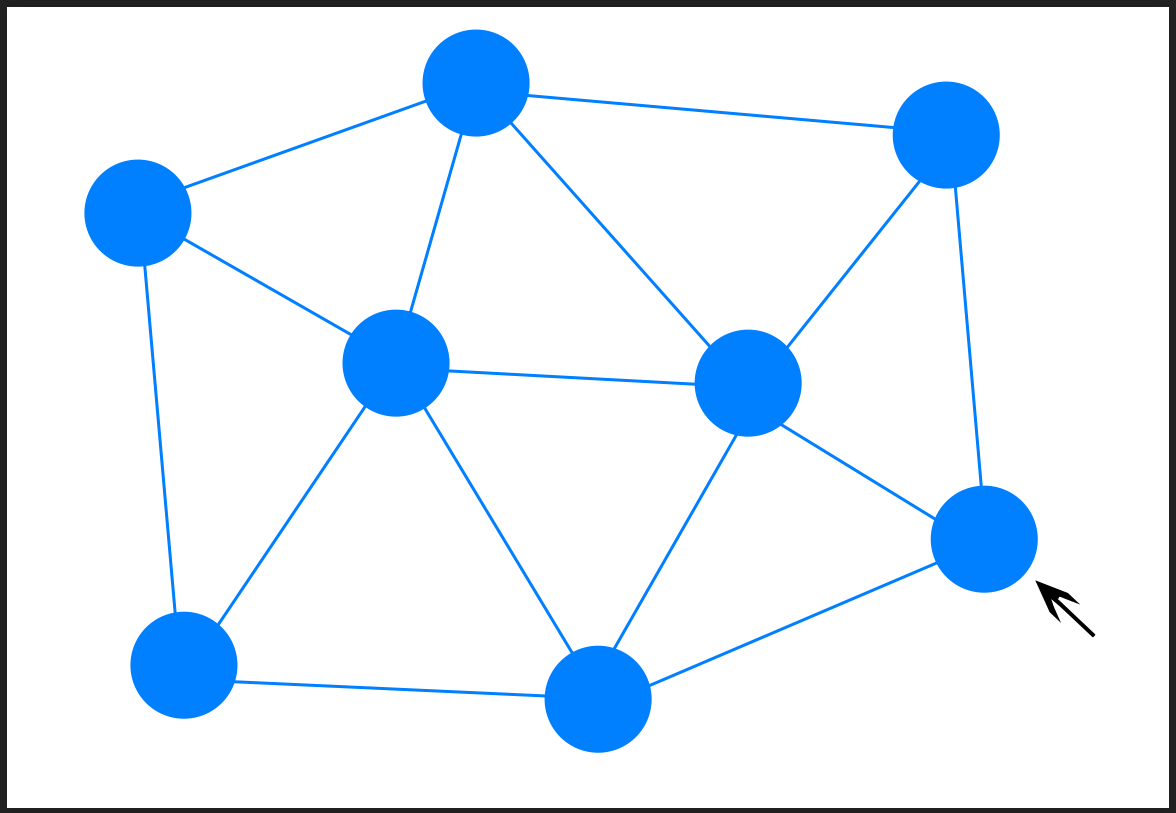

prevHash
prevHash
data
prevHash

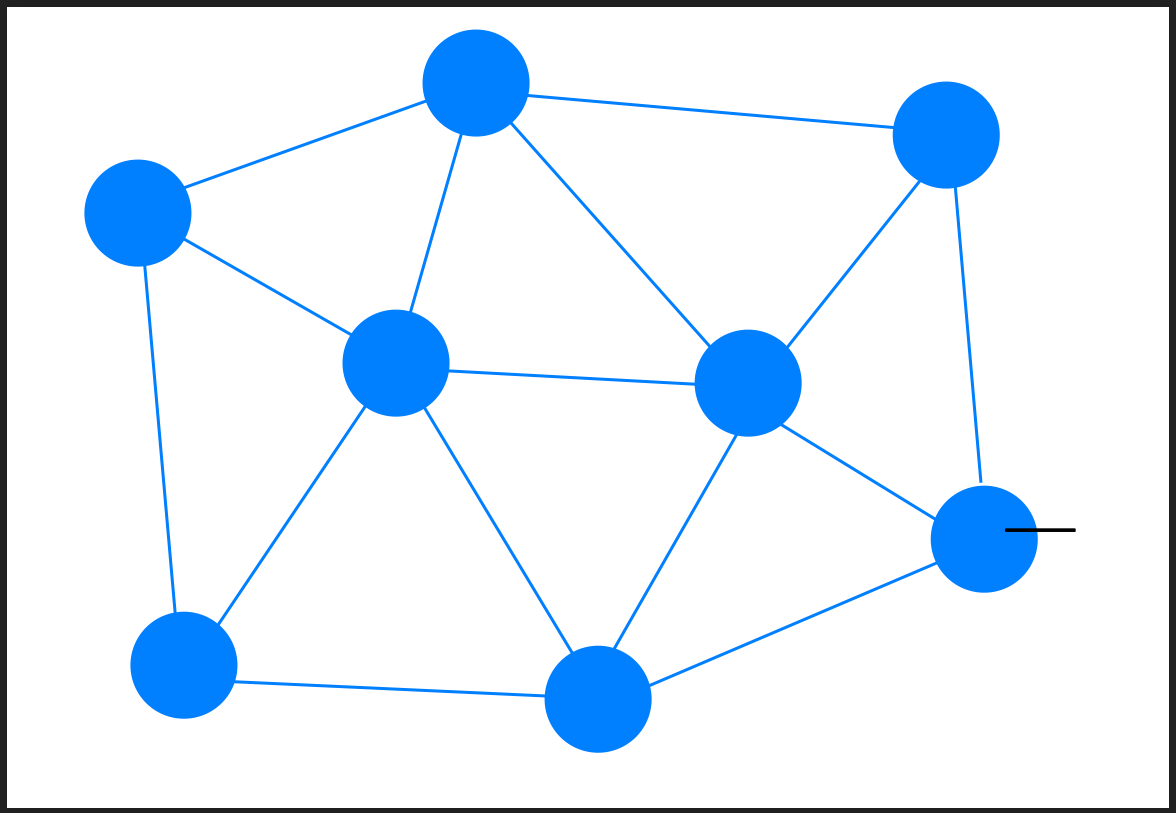


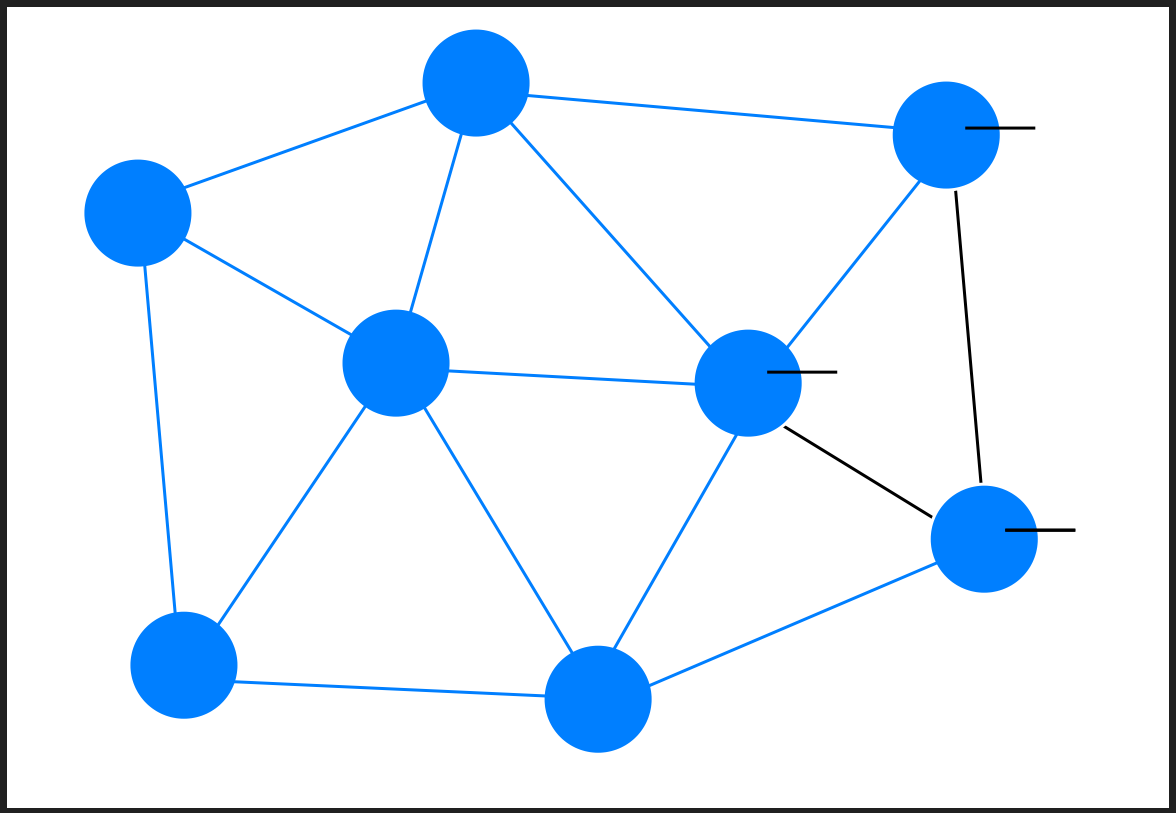

h(12) h(34)
h(1) h(2)
h(3) h(4)
d1
d2
d3
d4

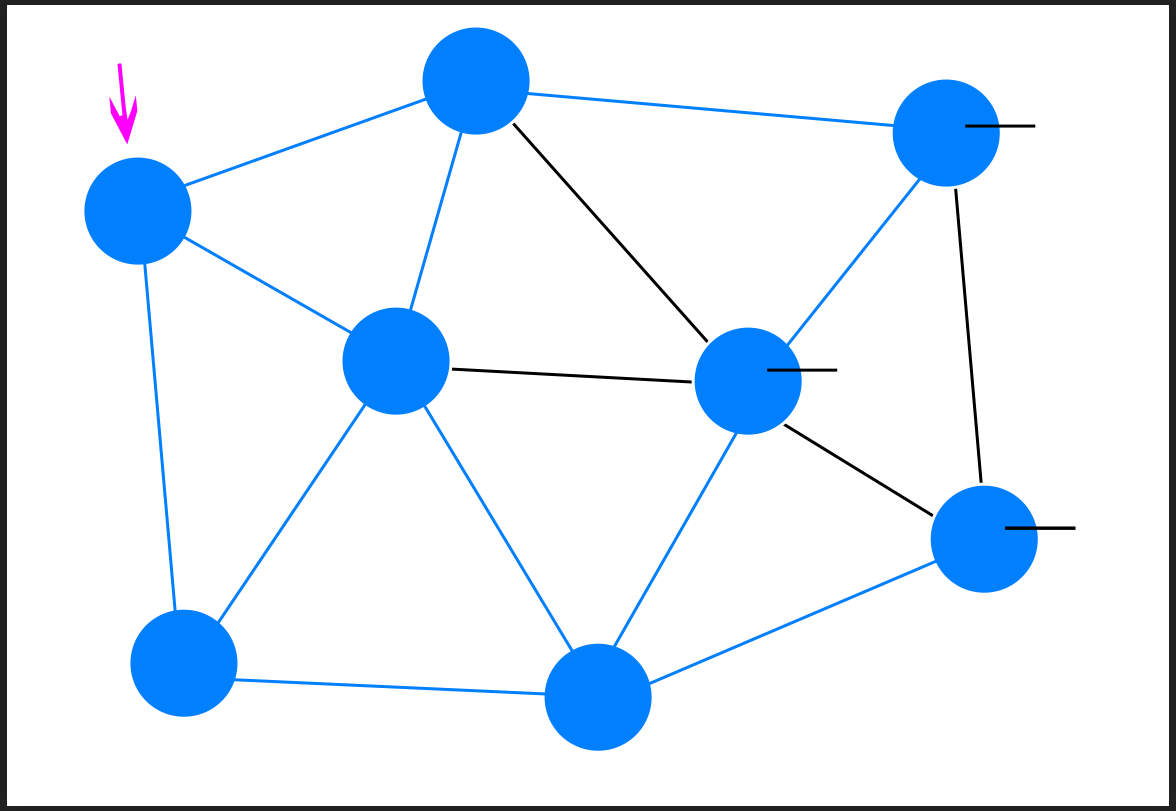

Block N-1
time stamp
data
Block N
time stamp
data
Block N+1
time stamp
data

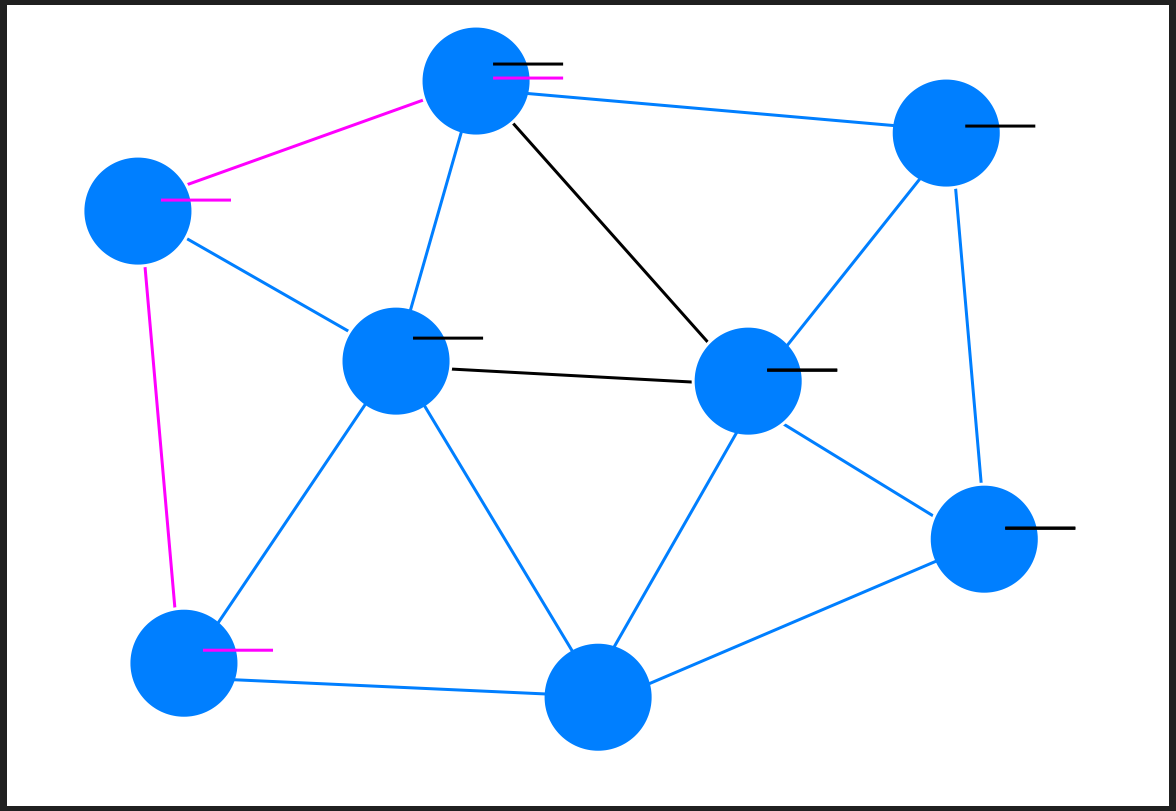


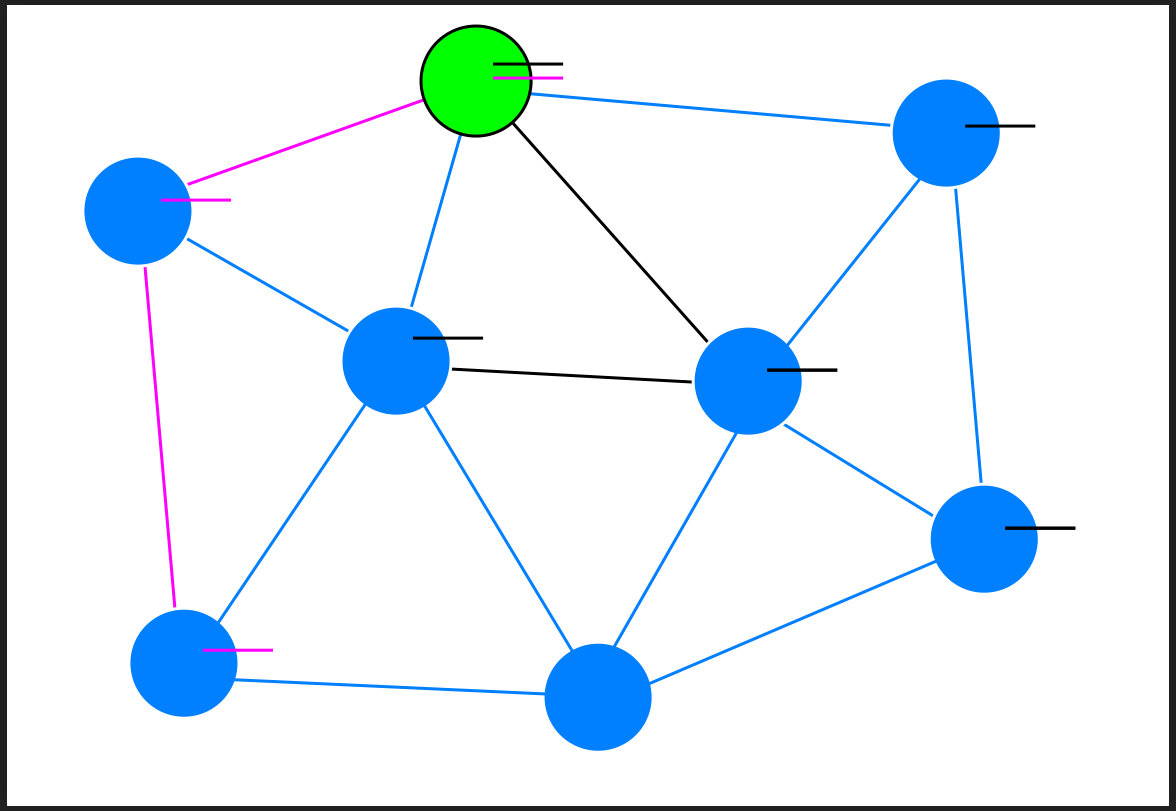


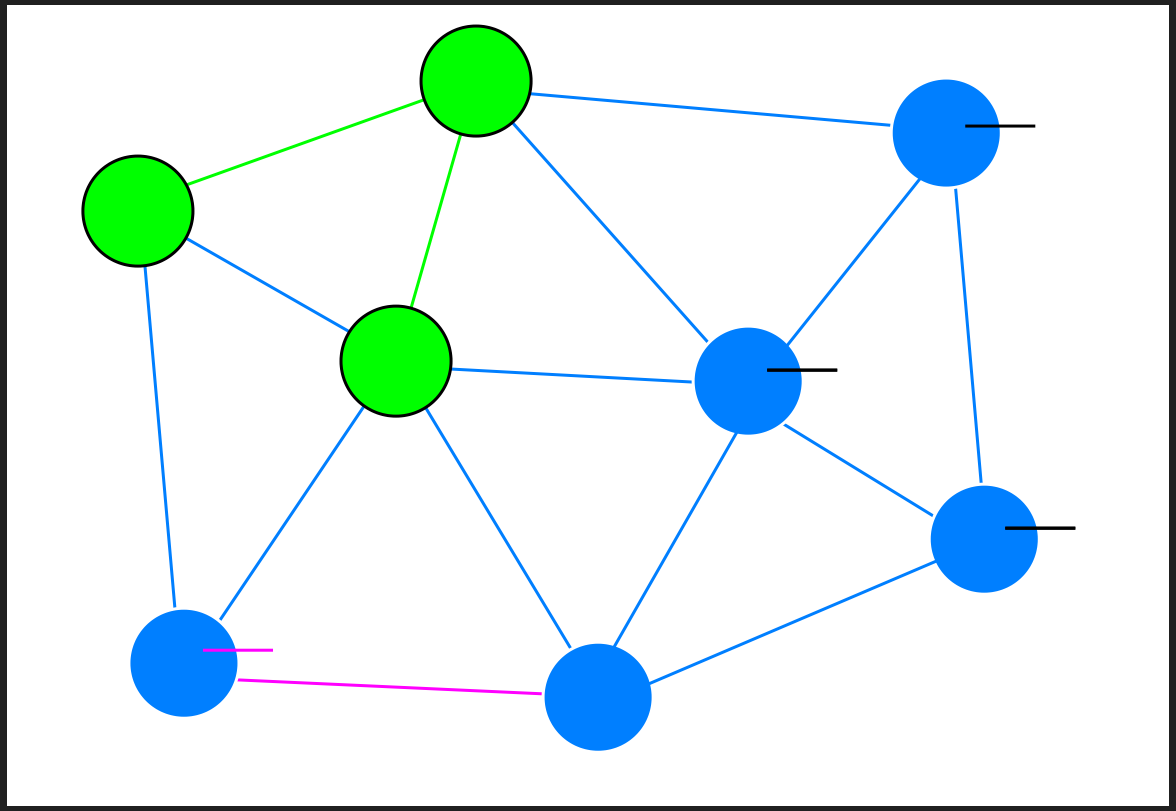


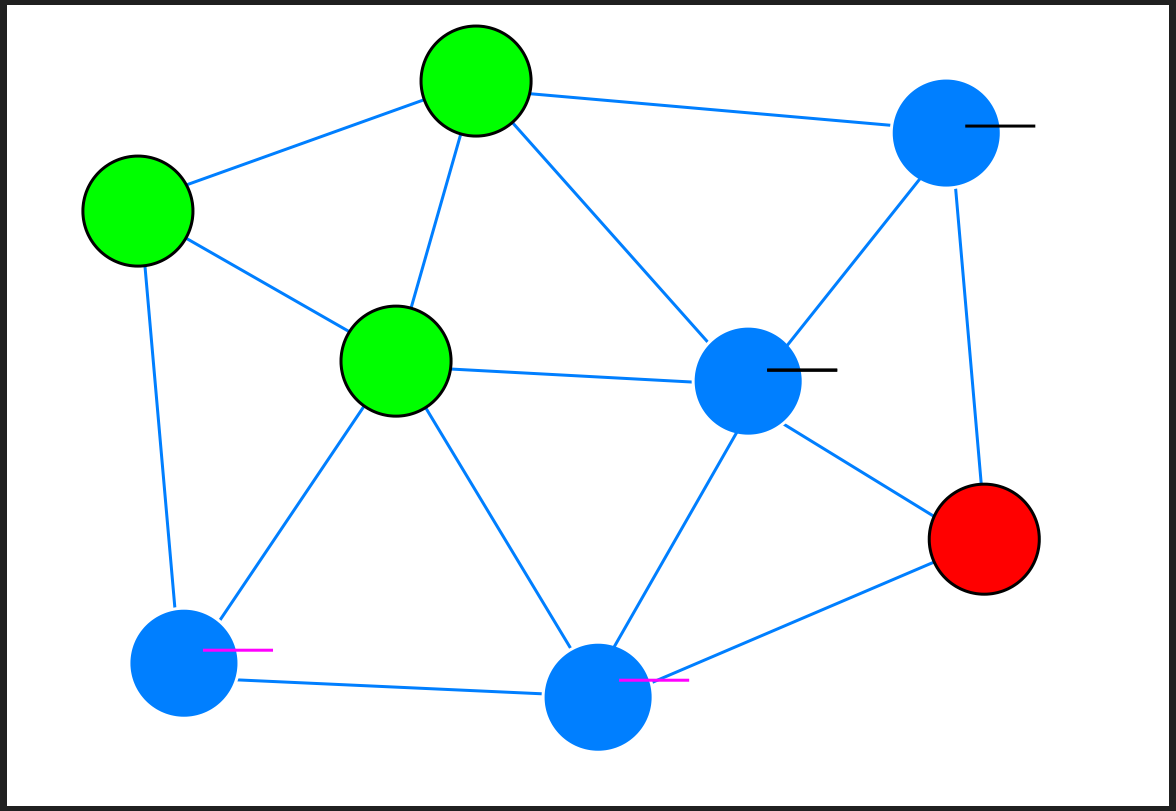


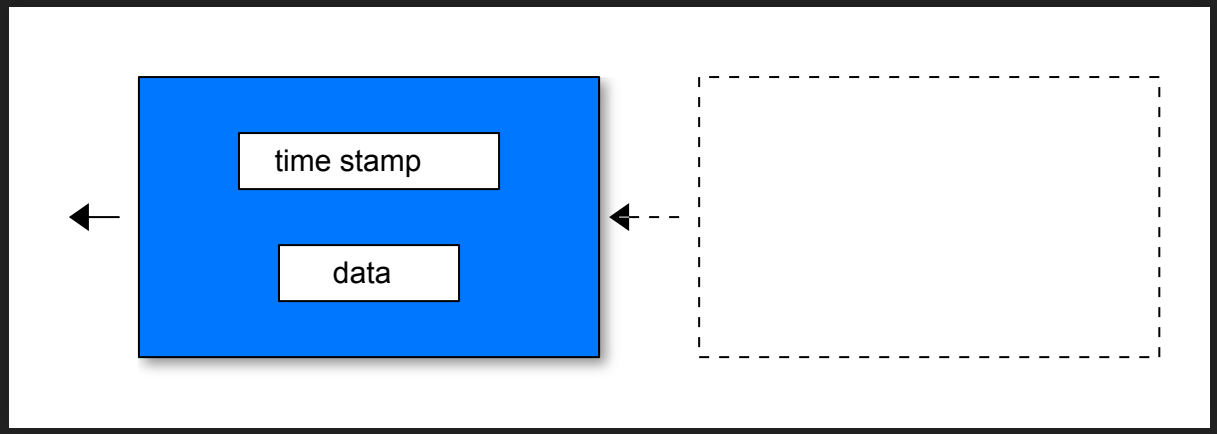


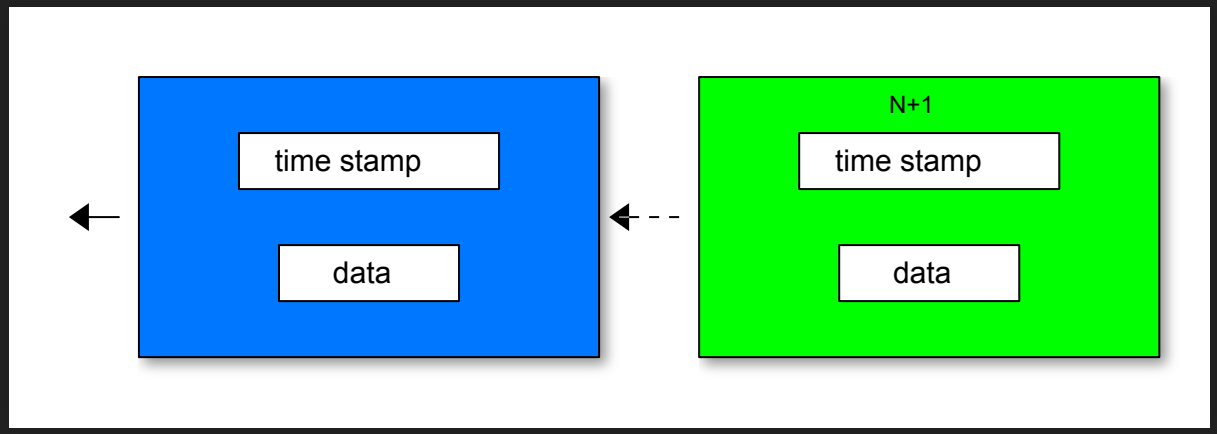


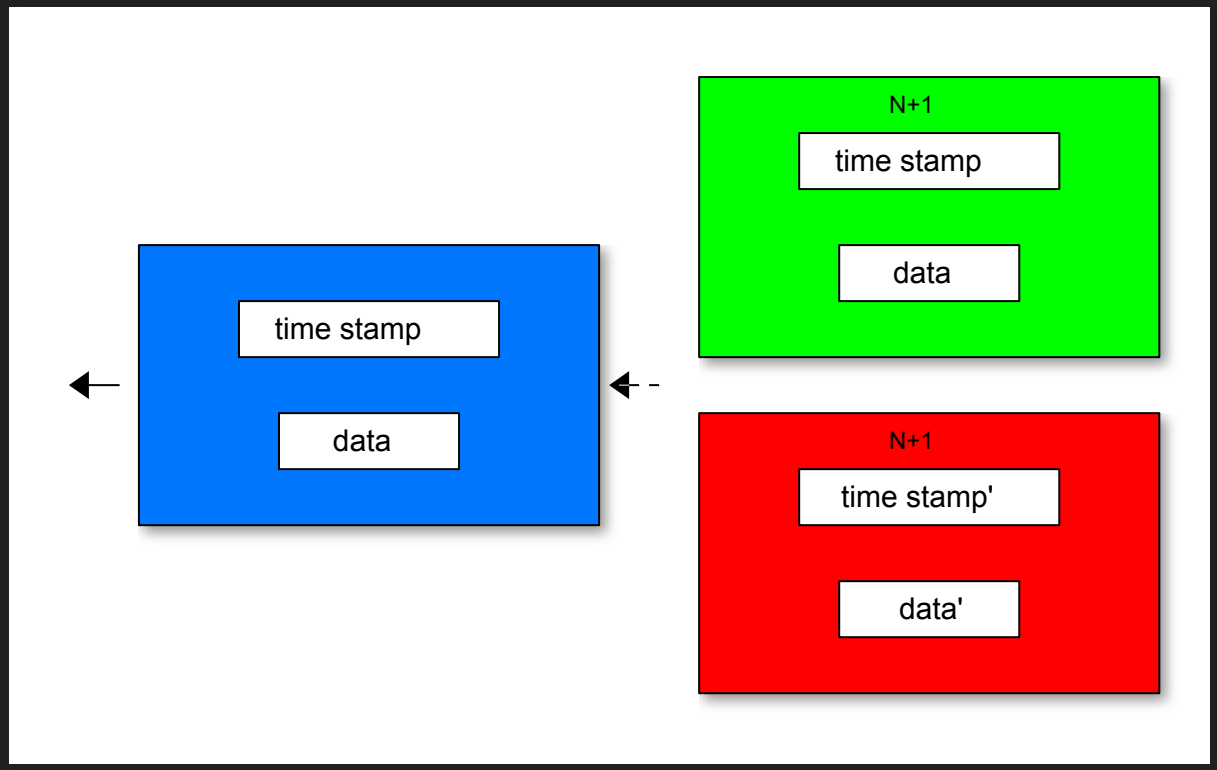


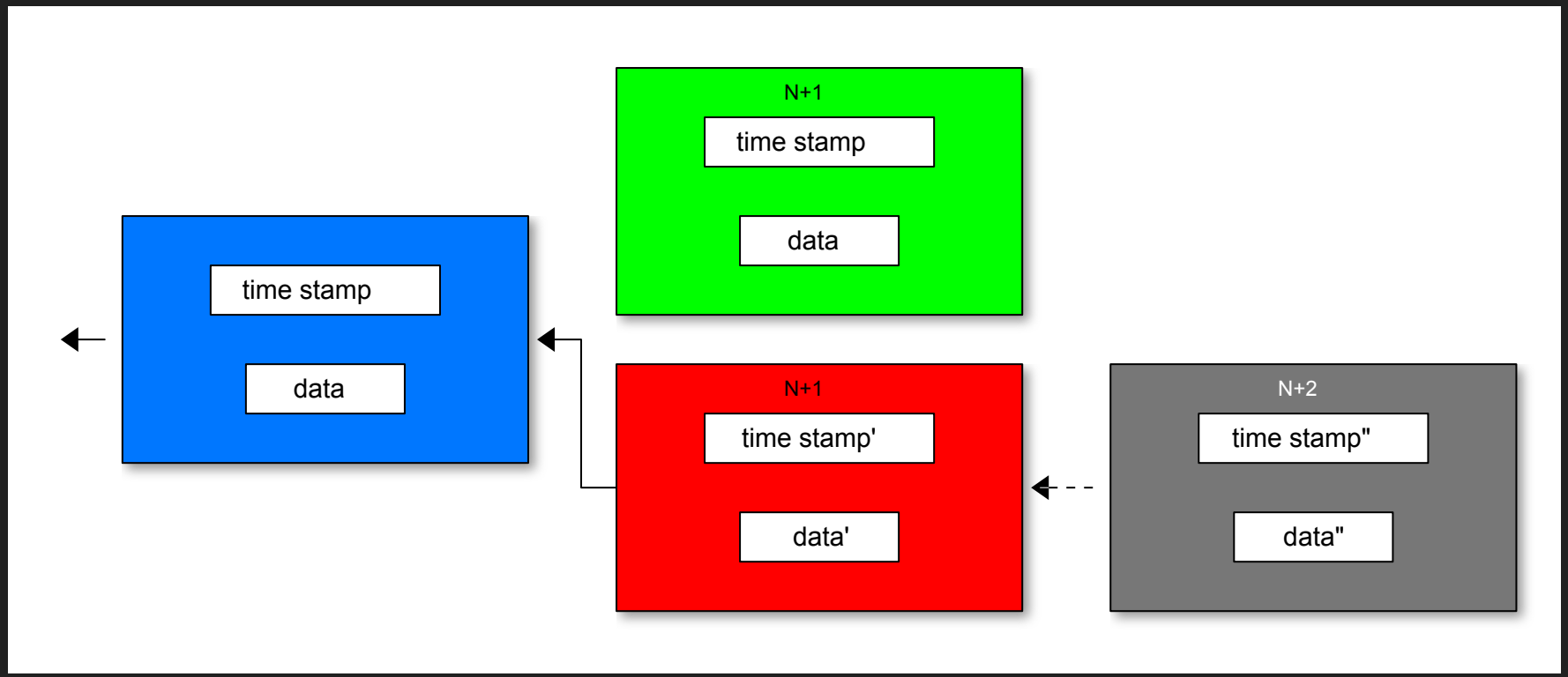


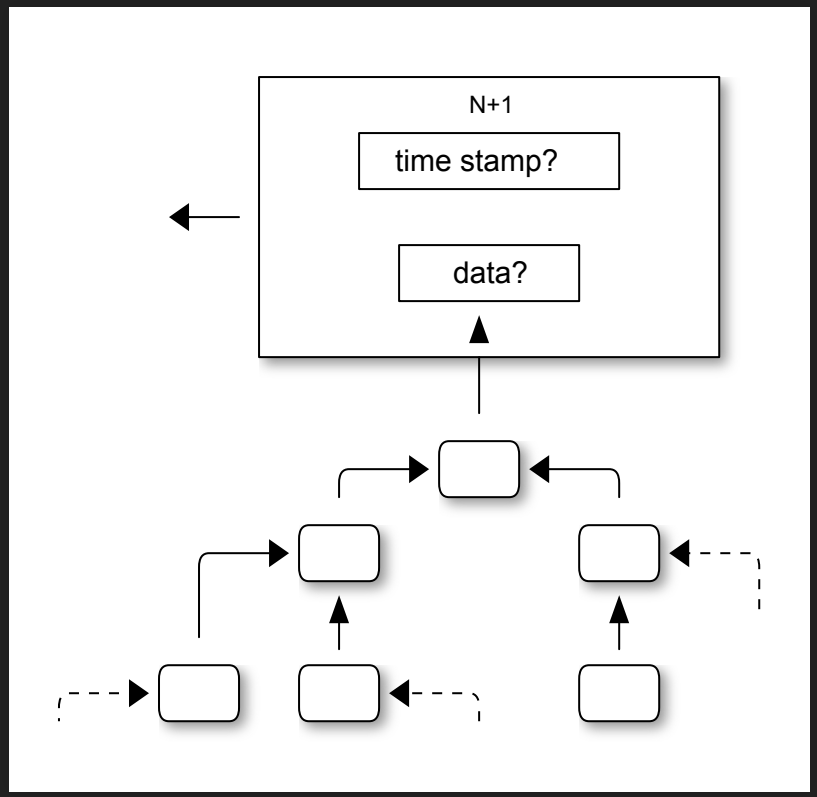


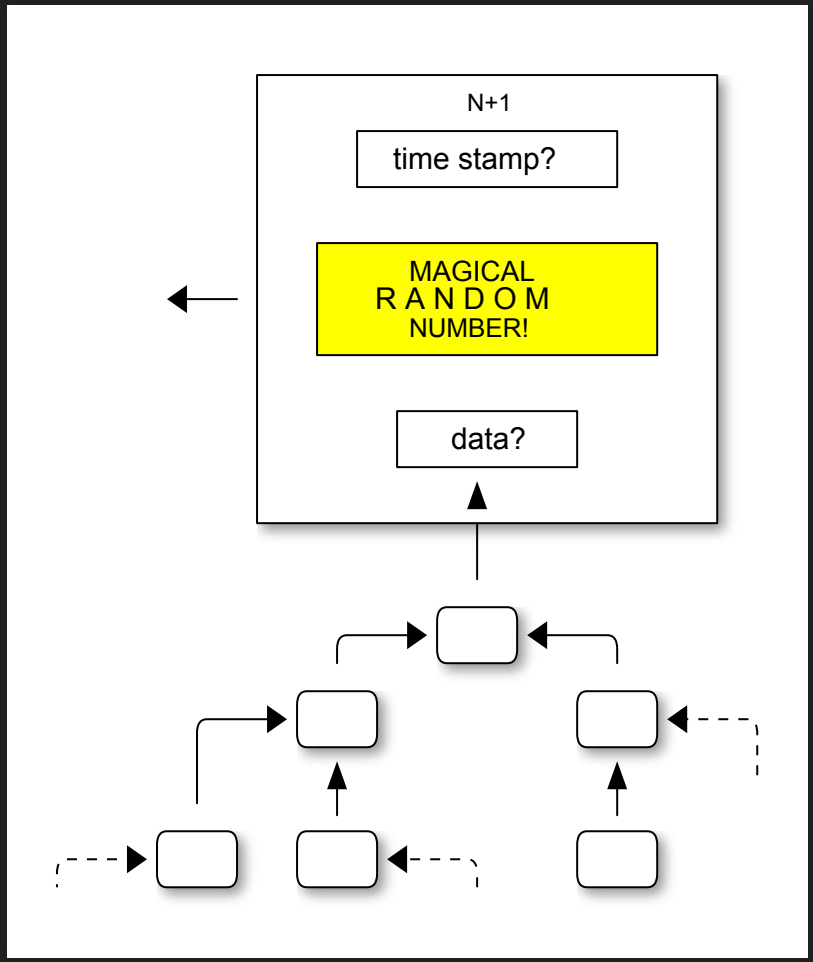

time stamp
data


time stamp
data
N+1
time stamp
data


N+1
time stamp
data
time stamp
data
N+1
time stamp'
data'


N+1
time stamp
data
time stamp
data
N+1
time stamp'
data'
N+2
time stamp"
data"

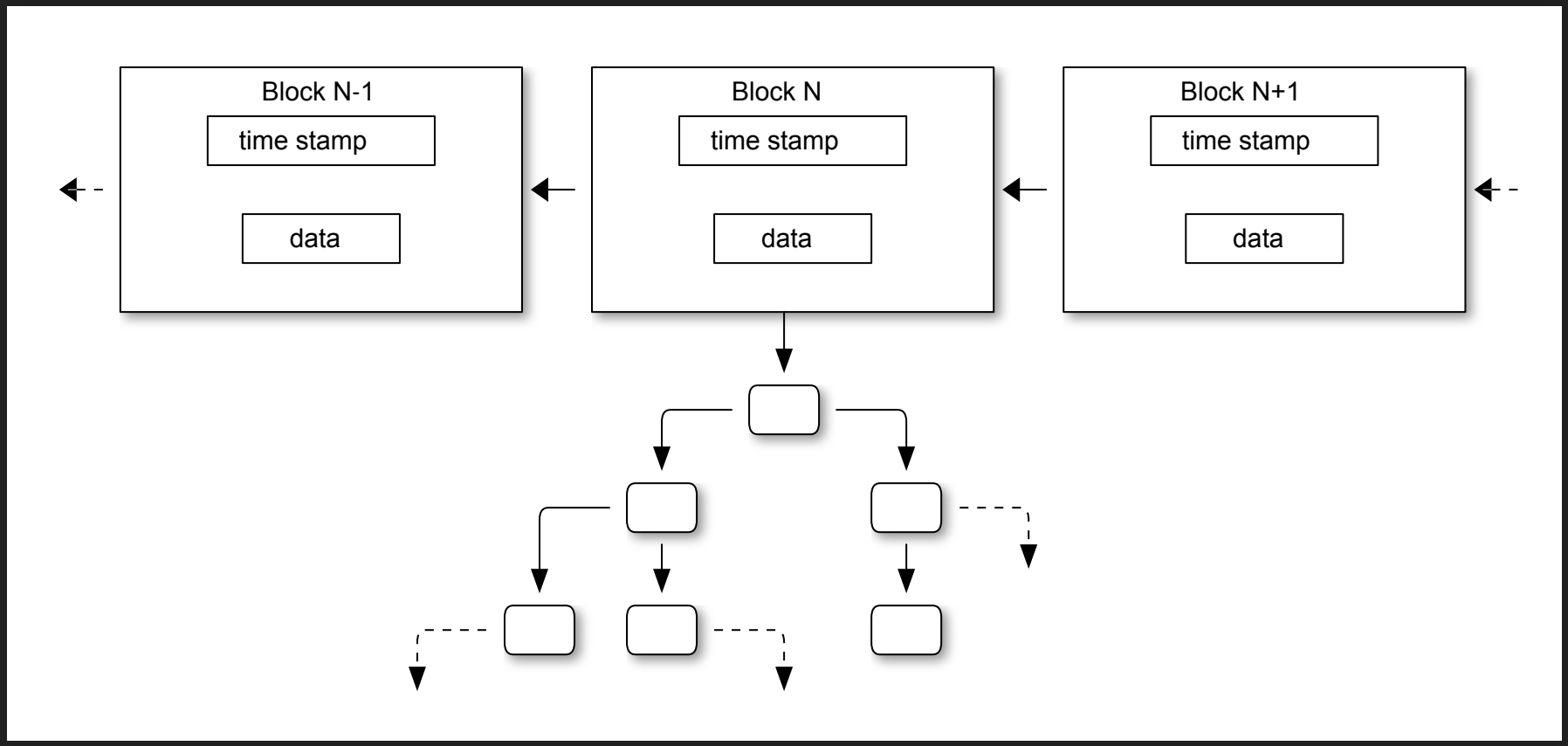

N+1
time stamp?
data?


N+1
time stamp?
MAGICAL
R A N D O M
NUMBER!
data?

HIS
SONY
529

- The Block Reward

- The Block Reward
- Transaction Fees


Block N-1
time stamp
data
Block N
time stamp
data
Block N+1
time stamp
data

Or create your own

at

http://build-a-co.in/

- Proof-of-work

- Proof-of-work
- Proof-of-stake

- Proof-of-work
- Proof-of-stake
- Proof-of-authority

```
{
  "hash": "5a425...",
  "ver": 1,
  "vin_sz": 2,
  "vout_sz": 1,
  "lock_time": 0,
  "size": 404,
  "in": [{
    "prev_out": {
      "hash": "3be4a...",
      "n": 0,
    },
    "scriptSig": "30440..."
  }, {
    "prev_out": {
      "hash": "7508e6...",
      "n": 0,
    },
    "scriptSig": "3f3a4...",
  }],
  "out": [{
    "value": "10.12287097",
    "scriptPubKey":"OP_DUP OP_HASH160 69e02...
        OP_EQUALVERIFY OP_CHECKSIG"
  }]
}
```

```
function store(string key, string payload)
                          external permittedOnly {
  bytes32 previous_key = moveExisting(key);
  bytes32 null_key;

  Payload storage newPayload = registry[key];
  newPayload.payload = payload;
  newPayload.previous_key = previous_key;

  if (previous_key == null_key)
    emit Registration(msg.sender, key, payload);
  else
    emit Update(msg.sender, key, payload);
}
```

THAT’S WHAT BLOCKCHAINS ARE

SNAKES INTO SNAKE OIL

What Blockchains Are And Why They're Terrible

Jez Higgins

… continues after these messages…

What is Bitcoin? (v2)

https://www.youtube.com/watch?v=Gc2en3nHxA4

Ethereum: the World Computer

https://www.youtube.com/watch?v=j23HnORQXvs

SNAKES INTO SNAKE OIL

What Blockchains Are And Why They're Terrible

Jez Higgins

WHY THEY'RE TERRIBLE

MT.GOX
Crypto Rush
QUADRIGACX
BITFINEX
bitfloor

Bitcoin owners told to transfer savings out of Bitpay wallets after private keys stolen

A popular cryptocurrency exchange has warned customers that their Bitcoin could be stolen after hackers managed to create a backdoor in the service.

Bitpay said that customers using earlier versions of the app should "assume" that an attacker had stolen the private keys needed to access their cryptocurrency.

The attacker - or attackers - are understood to have infected a code library used by the service several weeks ago and have been quietly siphoning the keys unbeknown to the owners.

James Howells searches for hard drive with £4m-worth of bitcoins stored

28 November 2013

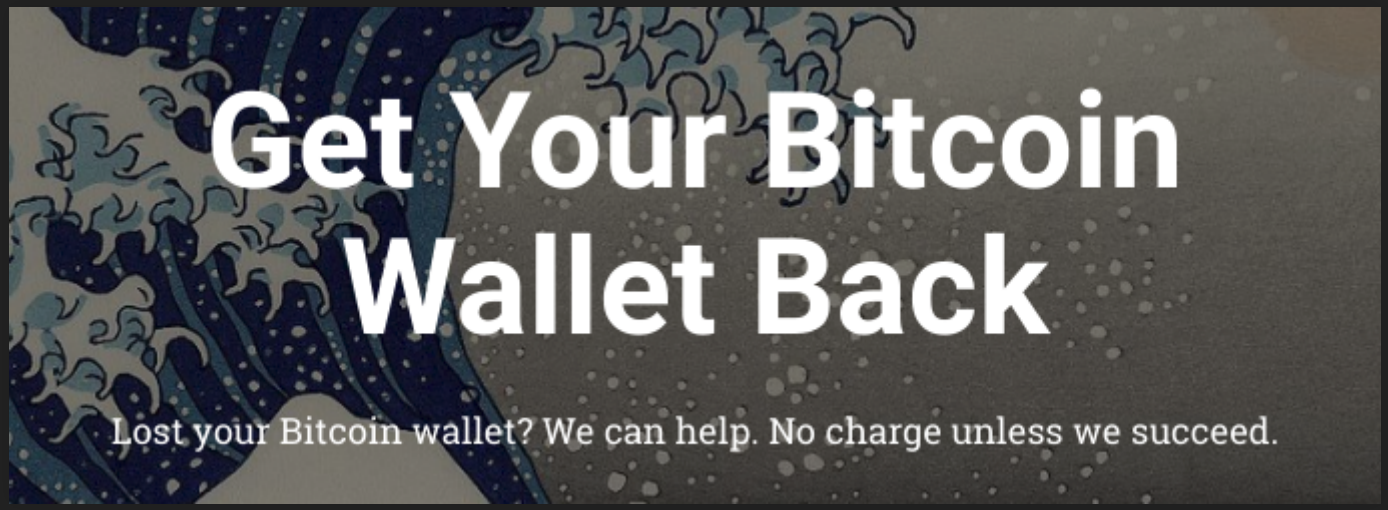
Share

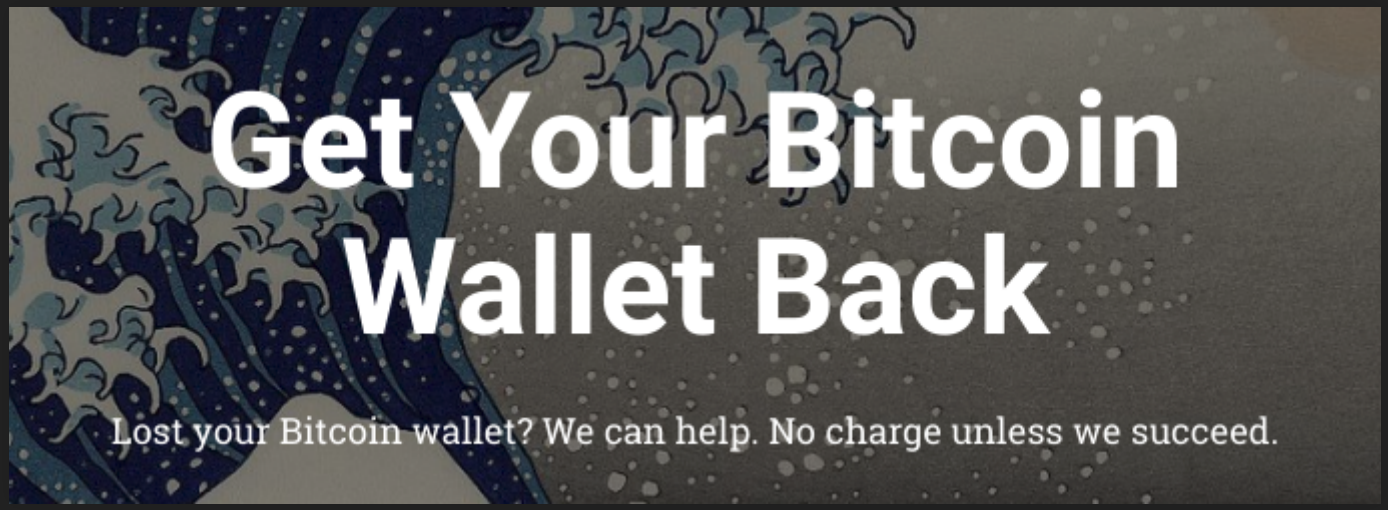
James Howells: "When I went up to the landfill site yesterday my first thought was 'I've got no chance'"

WIRED

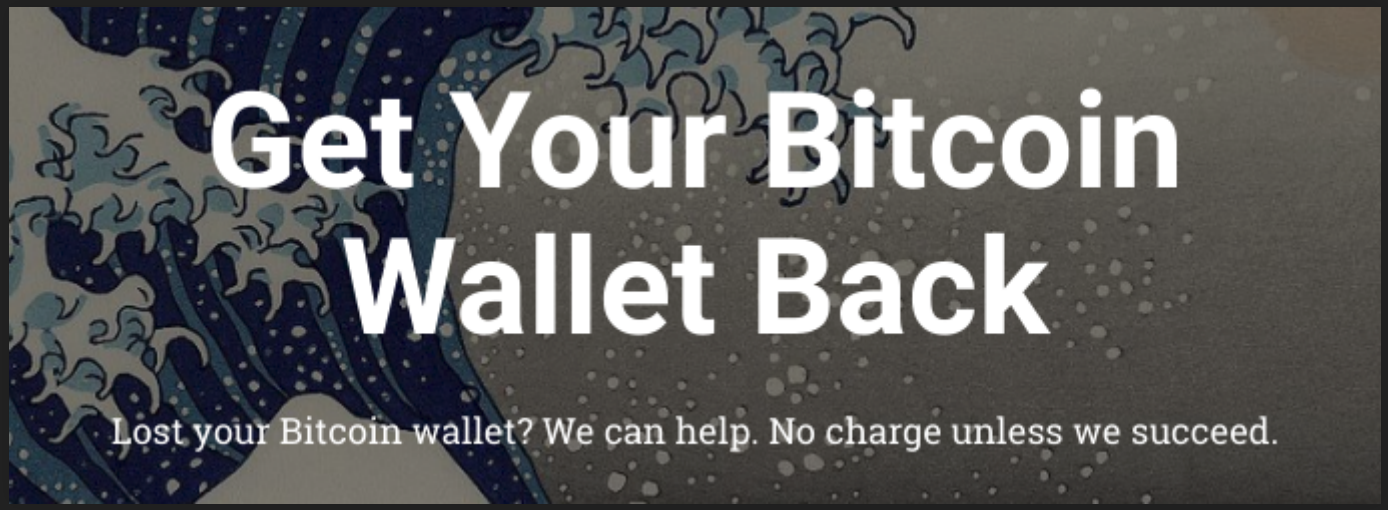
MARK FRAUENFELDER SECURITY 10.29.17 05:00 PM

'I FORGOT MY PIN': AN EPIC TALE OF LOSING $30,000 IN BITCOIN

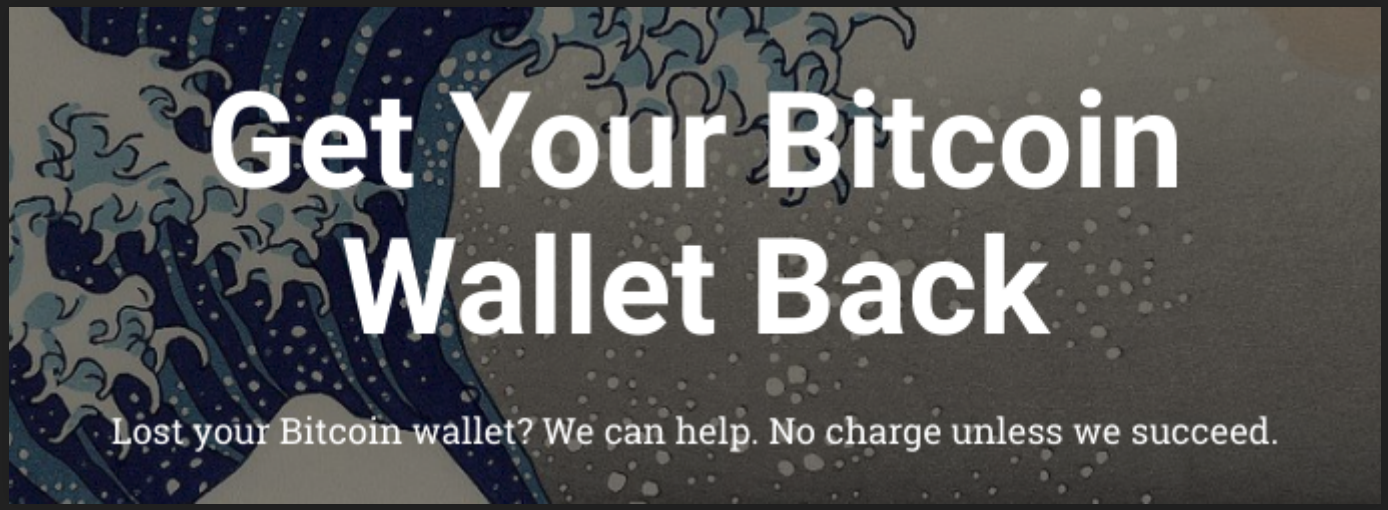

Get Your Bitcoin Wallet Back
Lost your Bitcoin wallet? We can help. No charge unless we succeed.



… typed his recovery words into Notepad to print them out, and promptly had his Bitcoin stolen due to a keylogger …



… printed out his seed words but was missing several due to incorrectly set page margins …



A customer stored his recovery word card in his jeans. The card was destroyed when the jeans had been laundered, which he only discovered months later when updating his wallet firmware.

Accepting Bitcoin as a Small Business – 4 Years In

Posted on February 27, 2019 by Jeff Seymour

As self-confessed Bitcoin enthusiasts here at Seymour Locksmiths we value the importance of decentralised ledger technologies. They have the power to change a lot of things, from financial transactions to unlocking your front door (yep, Bitcoin-powered smart locks are a thing).

In 2014 a large school of thought suggested that the main breakthrough use case for Bitcoin would be peer to peer transactions. That being customers and businesses paying for goods and services directly between one another without having to rely on payment networks such as Visa.

> We decided to put this theory to the test. In September 2014 we officially started accepting Bitcoin for our locksmith services in Worthing, shortly after we also starting accepting Dash and expanded acceptance to our entire service area. Since that point over four years ago and the time of writing, we have not had one customer ask to pay in Bitcoin, Dash or any other cryptocurrency.

Since that point over four years ago and at the time of writing, we have not had one customer ask to pay in BitCoin, Dash or any other cryptocurrency.

> While none of our customers has actually paid a locksmithing invoice with Bitcoin we have had lots of interested people wanting to discuss the subject in depth. Over the years we have noticed a steady uptick in customer awareness of Bitcoin with a huge surge during the bull run and news cycle during mid to late 2017.

While none of our customers has actually paid a locksmithing invoice with Bitcoin we have had lots of interested people wanting to discuss the subject in depth.

MAN WHO 'THREW AWAY' BITCOIN HAUL NOW WORTH OVER $80M WANTS TO DIG UP LANDFILL SITE

"It's a big, expensive and risky project," says James Howells, from Newport

'It's a big, expensive and risky project,' says James Howells, from Newport

By William Suberg MAR 19, 2019

New Report Warns 87 Percent of Cryptocurrency Exchange Volume Is Potentially Suspicious

Almost 90 percent of cryptocurrency exchanges' reported trade volumes may be incorrect, new research from trading analytics platform The Tie warned in a digest released on March 18.

Reporting on figures gathered from 97 exchanges, researchers found that the vast majority of the volume claimed to come from users may not in fact exist.

"In total we estimated that 87% of exchanges reported trading volume was potentially suspicious and that 75% of exchanges had some form of suspicious activity occurring on them," The Tie wrote in social media comments on the findings. The organization added:

> *"If each exchange averaged the volume per visit of CoinbasePro, Gemini, Poloniex, Binance, and Kraken, we would expect the real trading volume among the largest 100 exchanges to equal $2.1 (billion) per day. Currently that number is being reported as $15.9 (billion)."*

Bitcoin Price Goes 20% Up as a Result of Massive Order by Mystery Investor

April 5, 2019

James Howells @howelzy · Mar 29
Newsflash:
The BTC transaction stream is currently blocked.
'Blockstream Inc' denies any involvement.
6
5
45
James Howells @howelzy · Mar 29
Imagine having to pay extortionate transaction fees and still have to wait hours for 1 confirmation.
#BTCProblems
2
2
20

Elon Musk ✓
@elonmusk

Follow

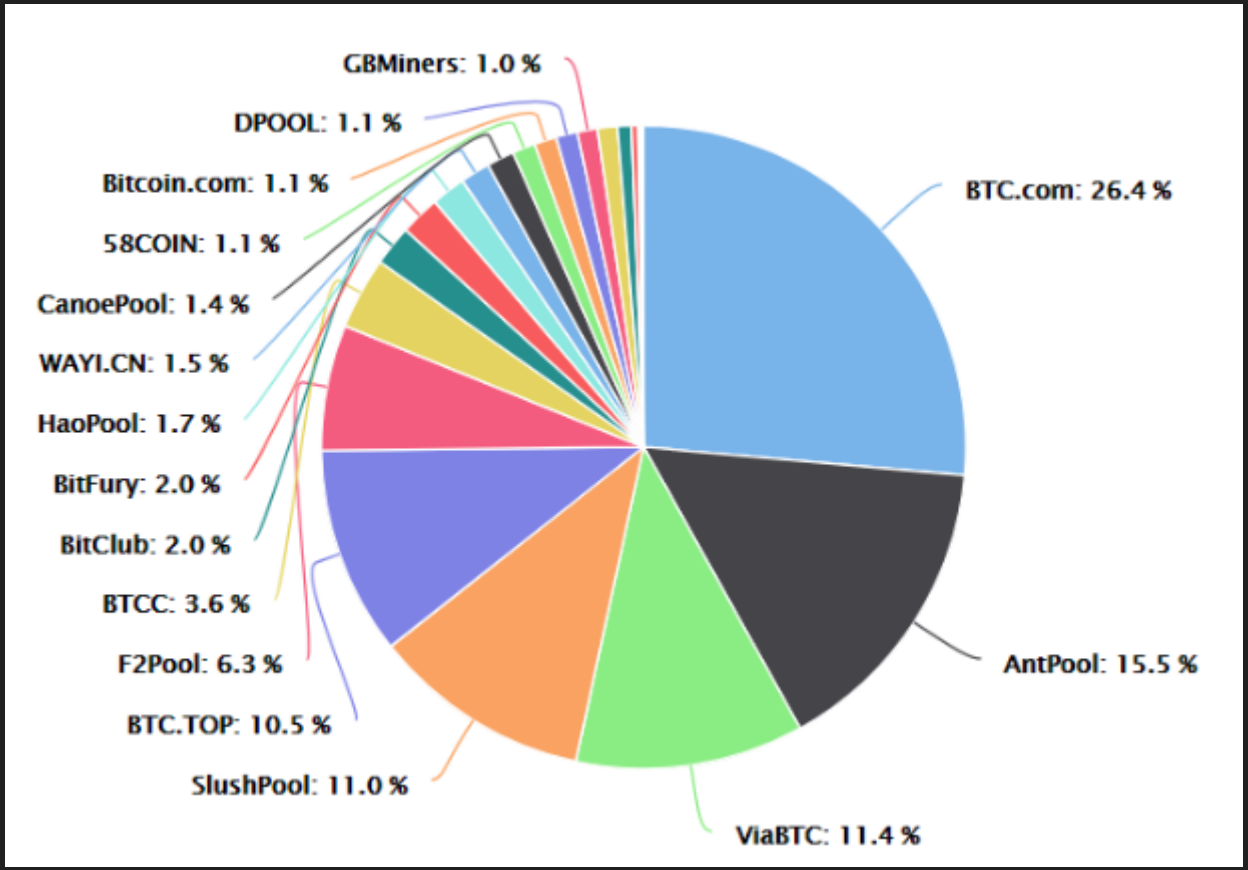
Dogecoin rulz

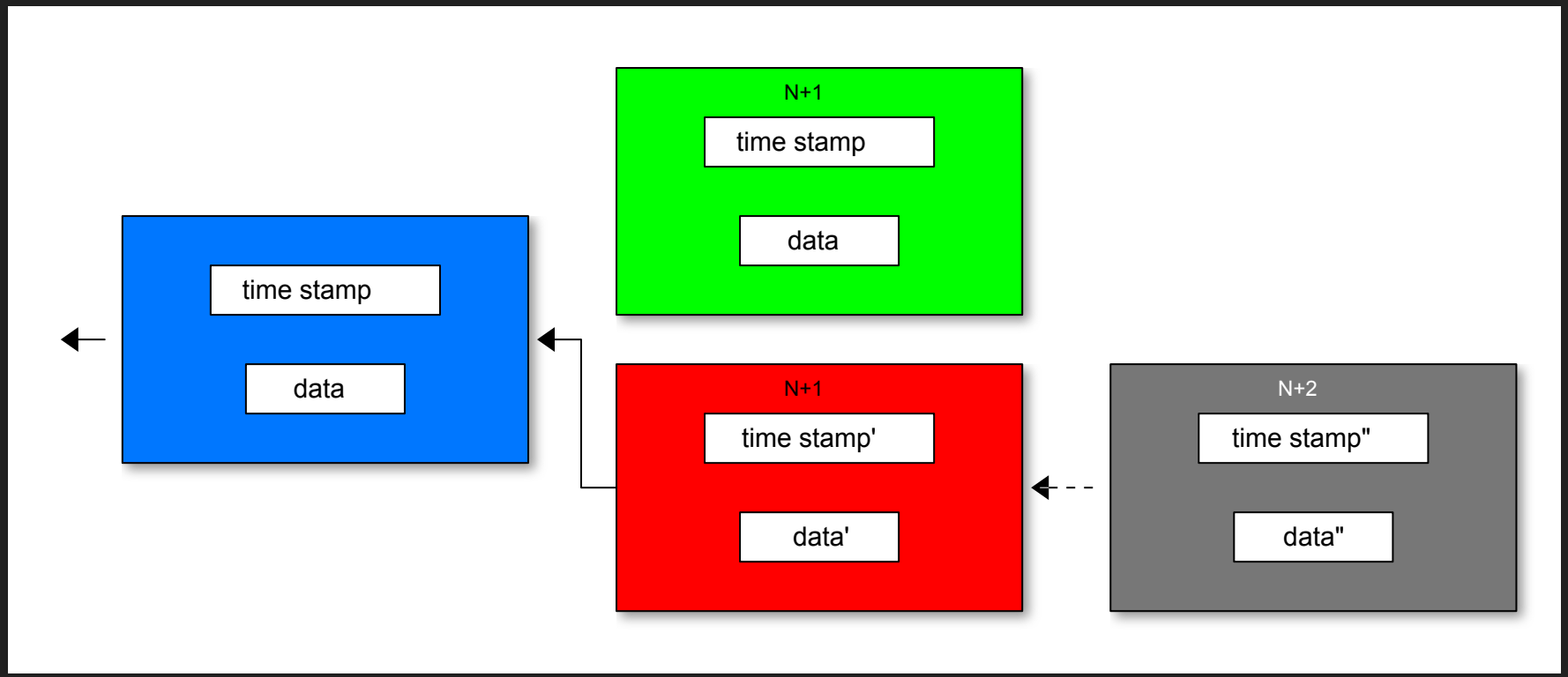
drags cigarette
Doge? I haven't heard that name in years.

9:16 PM - 2 Apr 2019

Dogecoin [DOGE] Skyrockets Overnight with Tesla's Elon Musk Hints His Favorite Coin

Tabassum April 3, 2019 Altcoin News


GBMiners: 1.0 %
DPOOL: 1.1 %
Bitcoin.com: 1.1 %
58COIN: 1.1 %
CanoePool: 1.4 %
WAYI.CN: 1.5 %
HaoPool: 1.7 %
BitFury: 2.0 %
BitClub: 2.0 %
BTCC: 3.6 %
F2Pool: 6.3 %
BTC.TOP: 10.5 %
SlushPool: 11.0 %
ViaBTC: 11.4 %
AntPool: 15.5 %
BTC.com: 26.4 %


N+1
time stamp
data
time stamp
data
N+1
time stamp'
data'
N+2
time stamp"
data"

Bitfly
@etherchain_org
Follow
We can confirm that there was a successful 51% attack on the Ethereum Classic (#ETC) network with multiple 100+ block reorganization. We recommend all services to closely monitored the chain and significantly increase required confirmations.
5:33 PM - 7 Jan 2019

nicehash

NiceHash does not support 51% attacks and we believe such deliberate and harmful actions should be taken very seriously.

NiceHash does not support 51% attacks and we believe such deliberate and harmful actions should be taken very seriously.

NiceHash is giving everyone with smaller and less secure blockchain projects the option to make them more secure by leasing hash power. If you think your network is under attack , you can mitigate such attacks and further secure the network by using NiceHash!
If you want to keep your PoW-based blockchain safe, we highly recommend you periodically lease hash power through NiceHash hash power marketplace. Such activity will always result in making your blockchain more secure.

Cryptocurrencies are not currencies

They are …

Cryptocurrencies are not currencies

They are …

- … difficult to get hold of

Cryptocurrencies are not currencies

They are …

- … difficult to get hold of
- … difficult to keep hold of

Cryptocurrencies are not currencies

They are …

- … difficult to get hold of
- … difficult to keep hold of
- … even more difficult to spend

Cryptocurrencies are not currencies

They are …

- … difficult to get hold of
- … difficult to keep hold of
- … even more difficult to spend
- … probably going to get lost or stolen or just fade away or jam up

Applications on built on Ethereum run exactly as programmed.

Parity Technologies

Powering the decentralised web

July 21, 2017 in Security

Severity: Critical

Product affected: Parity Wallet

Affected implementations: Parity 1.5 or later

Summary: A vulnerability in Parity Wallet's variant of the standard multi-sig contract has been found.

Affected users: Any user with assets in a multi-sig wallet created in Parity Wallet prior to 19/07/17 23:14:56 CEST.

Parity Technologies

Powering the decentralised web

November 08, 2017 in Security

Severity: Critical

Product affected: Parity Wallet (multi-sig wallets)

Summary: A vulnerability in the Parity Wallet library contract of the standard multi-sig contract has been found.

Affected users: Users with assets in a multi-sig wallet created in Parity Wallet that was deployed after 20th July.

Which party will control the House after the 2018 U.S. Midterm Election?

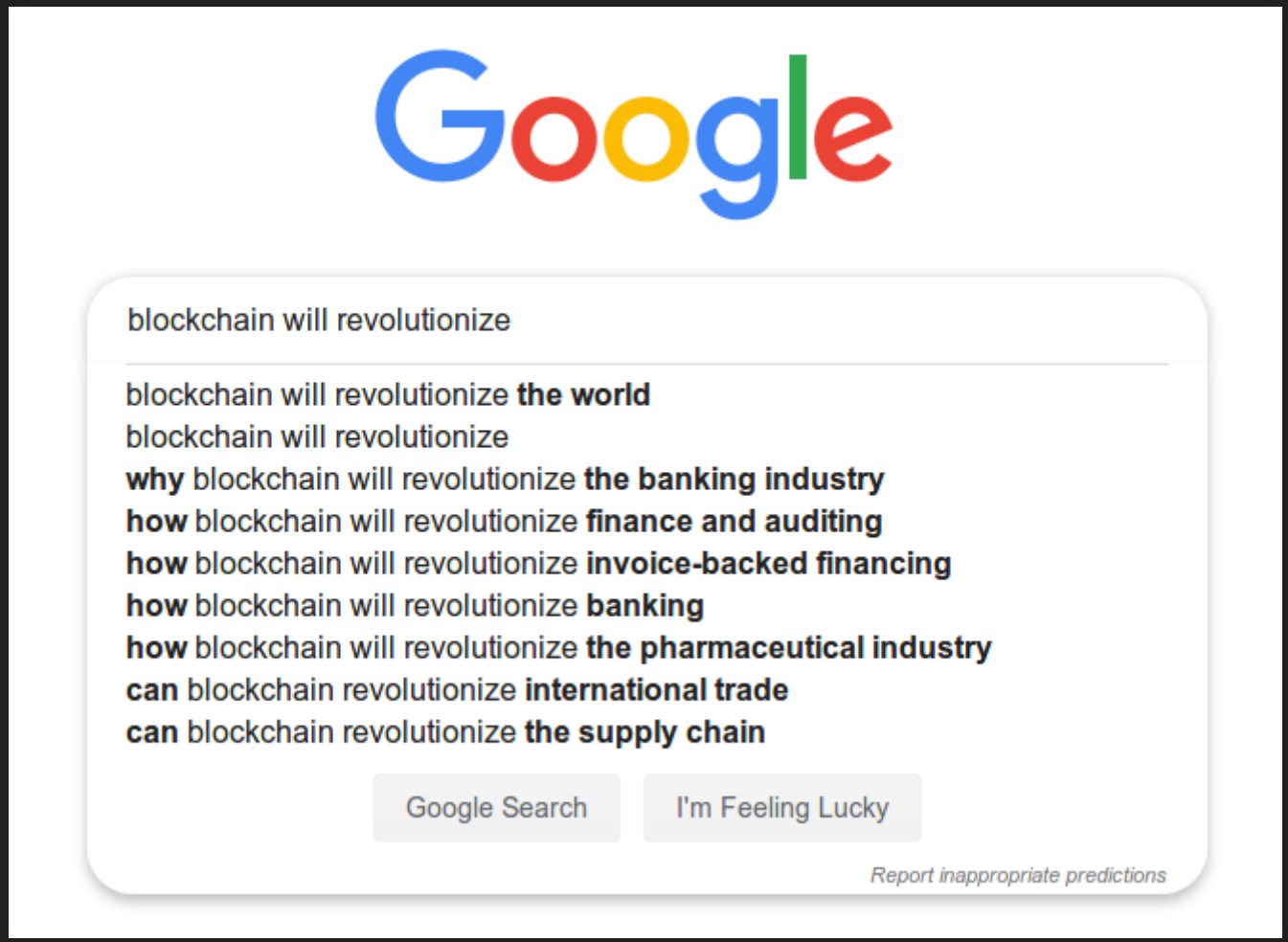
Which party will control the House after the 2018 U.S. Midterm Election?

Which party will control the House after 2018 U.S. Midterm Election?

Market ID: 0xbbbc0a8baa03535e0a680ee2f057162aaaafd570, CATEGORICAL, Predictions.Global, Reporters.Chat

Outcome	Dispute rounds								
Democrats	0	1	2	3	4	5	6	7	8
Republicans	0	1	2	3	4	5	6	7	8
Tied	0	1	2	3	4	5	6	7	8
INVALID	0	1	2	3	4	5	6	7	8

Without any possibility of downtime … or third-party interference

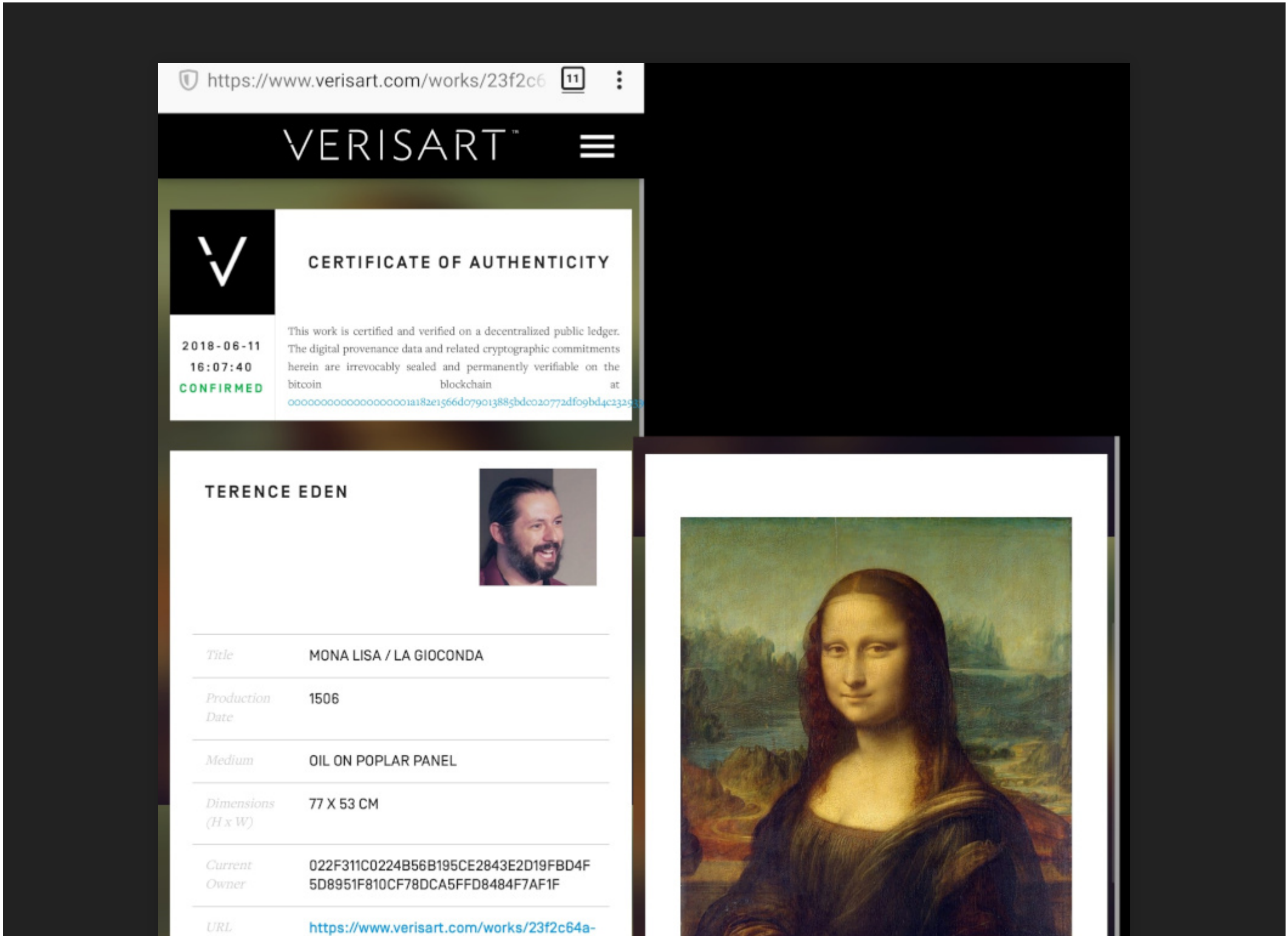

Google
blockchain will revolutionize
blockchain will revolutionize the world
blockchain will revolutionize
why blockchain will revolutionize the banking industry
how blockchain will revolutionize finance and auditing
how blockchain will revolutionize invoice-backed financing
how blockchain will revolutionize banking
how blockchain will revolutionize the pharmaceutical industry
can blockchain revolutionize international trade
can blockchain revolutionize the supply chain
Google Search
I'm Feeling Lucky
Report inappropriate predictions

PIL is already collaborating with IBM on the Tradelens platform

PIL AND IBM COLLABORATE ON BLOCKCHAIN BILL OF LADING PROJECT

Pacific International Lines (PIL) has used an electronic Bill of Lading (e-BL) built on the IBM Blockchain Platform in a real-time pilot tracking shipment of mandarin oranges from China for the Lunar New Year celebrations.

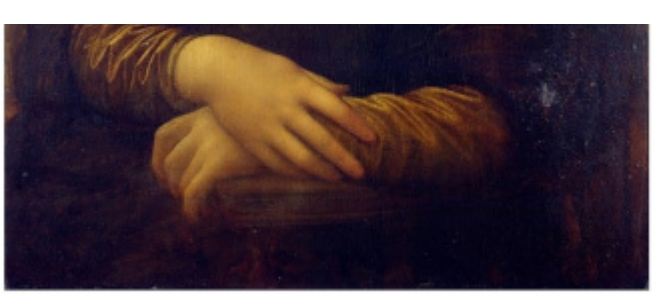
With the use of IBM Blockchain powered e-BL, the trial has produced a significant reduction in the administrative process of transferring the title deed from five to seven days to just one second, claimed the parties.


https://www.verisart.com/works/23f2c6
11
VERISART™
CERTIFICATE OF AUTHENTICITY
2018-06-11
16:07:40
CONFIRMED
This work is certified and verified on a decentralized public ledger. The digital provenance data and related cryptographic commitments herein are irrevocably sealed and permanently verifiable on the bitcoin blockchain at
TERENCE EDEN
Title
MONA LISA / LA GIOCONDA
Production Date
1506
Medium
OIL ON POPLAR PANEL
Dimensions (H x W)
77 X 53 CM
Current Owner
022F311C0224B56B195CE2843E2D19FBD4F
5D8951F810CF78DCA5FFD8484F7AF1F
URL
https://www.verisart.com/works/23f2c64a-

08c6-4a42-8013-84ac8422dffb

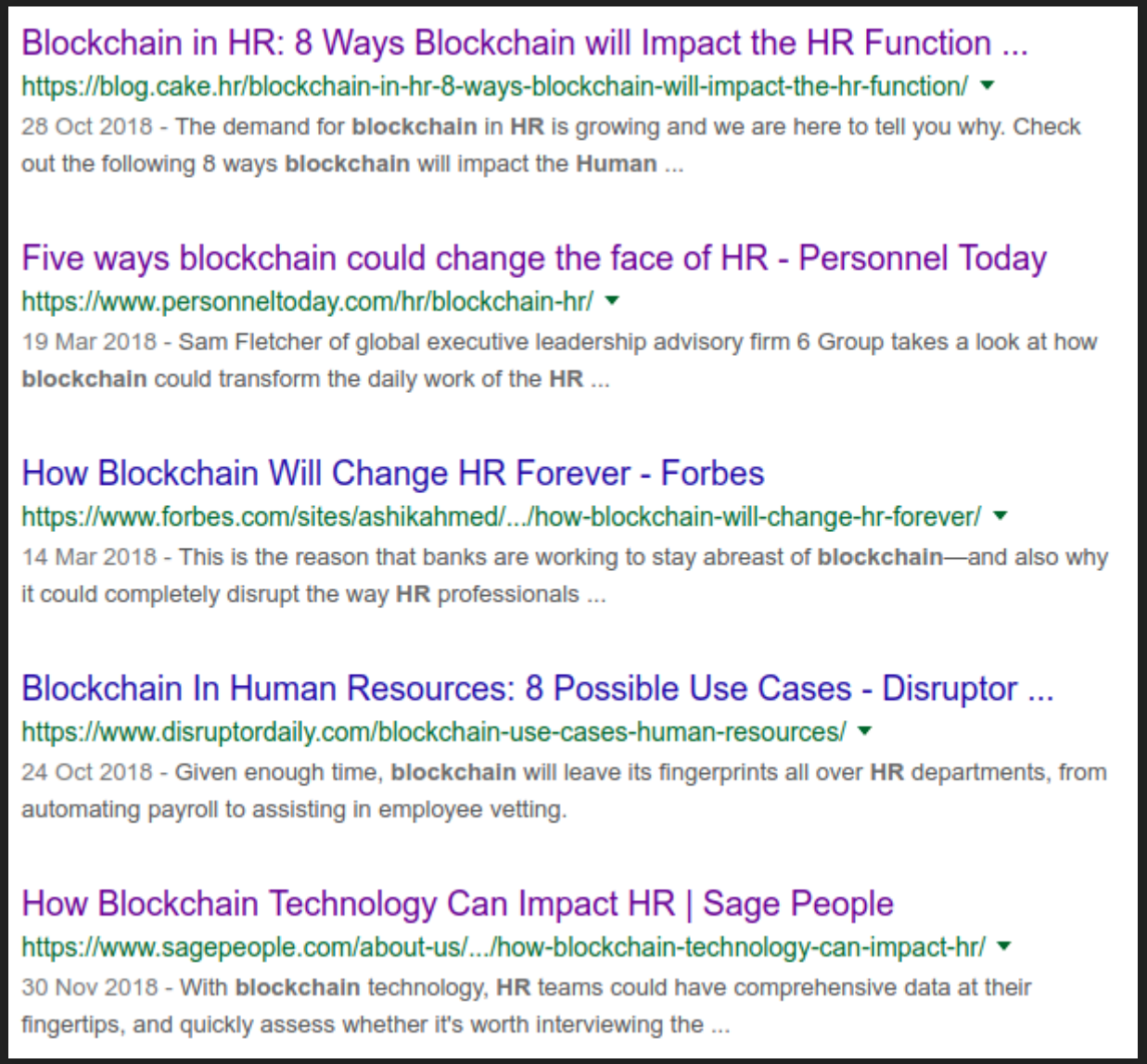
Blockchain Address	0000000000000000001a182e1566d0790138 85bdc020772df09bd4c232933dc8

VERIFIED BY VERISART



Lowland distillery Ailsa Bay has released a travel retail exclusive whisky featuring blockchain technology to ‘ensure authenticity and allow traceability’.

Transparent traceability: Ailsa Bay’s travel retail exclusive uses blockchain data to log its journey


Blockchain in HR: 8 Ways Blockchain will Impact the HR Function ...
https://blog.cake.hr/blockchain-in-hr-8-ways-blockchain-will-impact-the-hr-function/
28 Oct 2018 - The demand for blockchain in HR is growing and we are here to tell you why. Check out the following 8 ways blockchain will impact the Human ...
Five ways blockchain could change the face of HR - Personnel Today
https://www.personneltoday.com/hr/blockchain-hr/
19 Mar 2018 - Sam Fletcher of global executive leadership advisory firm 6 Group takes a look at how blockchain could transform the daily work of the HR ...
How Blockchain Will Change HR Forever - Forbes
https://www.forbes.com/sites/ashikahmed/.../how-blockchain-will-change-hr-forever/
14 Mar 2018 - This is the reason that banks are working to stay abreast of blockchain—and also why it could completely disrupt the way HR professionals ...
Blockchain In Human Resources: 8 Possible Use Cases - Disruptor ...
https://www.disruptordaily.com/blockchain-use-cases-human-resources/
24 Oct 2018 - Given enough time, blockchain will leave its fingerprints all over HR departments, from automating payroll to assisting in employee vetting.
How Blockchain Technology Can Impact HR | Sage People
https://www.sagepeople.com/about-us/.../how-blockchain-technology-can-impact-hr/
30 Nov 2018 - With blockchain technology, HR teams could have comprehensive data at their fingertips, and quickly assess whether it's worth interviewing the ...

Emergent Tech

Blockchain study finds 0.00% success rate and vendors don't call back when asked for evidence

Where is your distributed ledger technology now?

AND THAT'S WHY THEY'RE TERRIBLE

A GLIMMER OF HOPE

The ARCHANGEL project proposes to delivery ***long-term sustainability of digital archives*** *through* ***new technologies*** *that will ensure both the* ***accessibility to and integrity of digial archives***

The National Archives

CHRIS HEATON-HARRIS MP

HOUSE OF COMMONS

LONDON SW1A 0AA

The Rt. Hon Theresa May MP
The Prime Minister
10 Downing Street
London, SW1A 2AA

3rd April 2019

Prime Minister,

It has been an honour to serve in your Government as a Whip and more recently as Parliamentary Under-Secretary at the Department for Exiting the European Union and I thank you for giving me the chance to serve my country in these roles.

In my current job, I've had the responsibility of helping to coordinate our preparations for if we were to leave the European Union without a negotiated deal. As I believe you know, these preparations are well advanced and whilst I would have preferred to leave the European Union with your deal, I truly believe our country would have swiftly overcome any immediate issues of leaving without a deal and gone on to thrive.

It has been a privilege to work with some quite brilliant civil servants in my Department and across your Government. They have moved mountains to prepare our country for leaving the European Union without a negotiated deal. Unfortunately, I do not believe the briefings you have received on these matters recently have reflected all they have achieved or the preparations our European partners have made.

However, I completely understand you do not want to leave the European Union without a negotiated deal and that obviously makes my job in Government irrelevant.

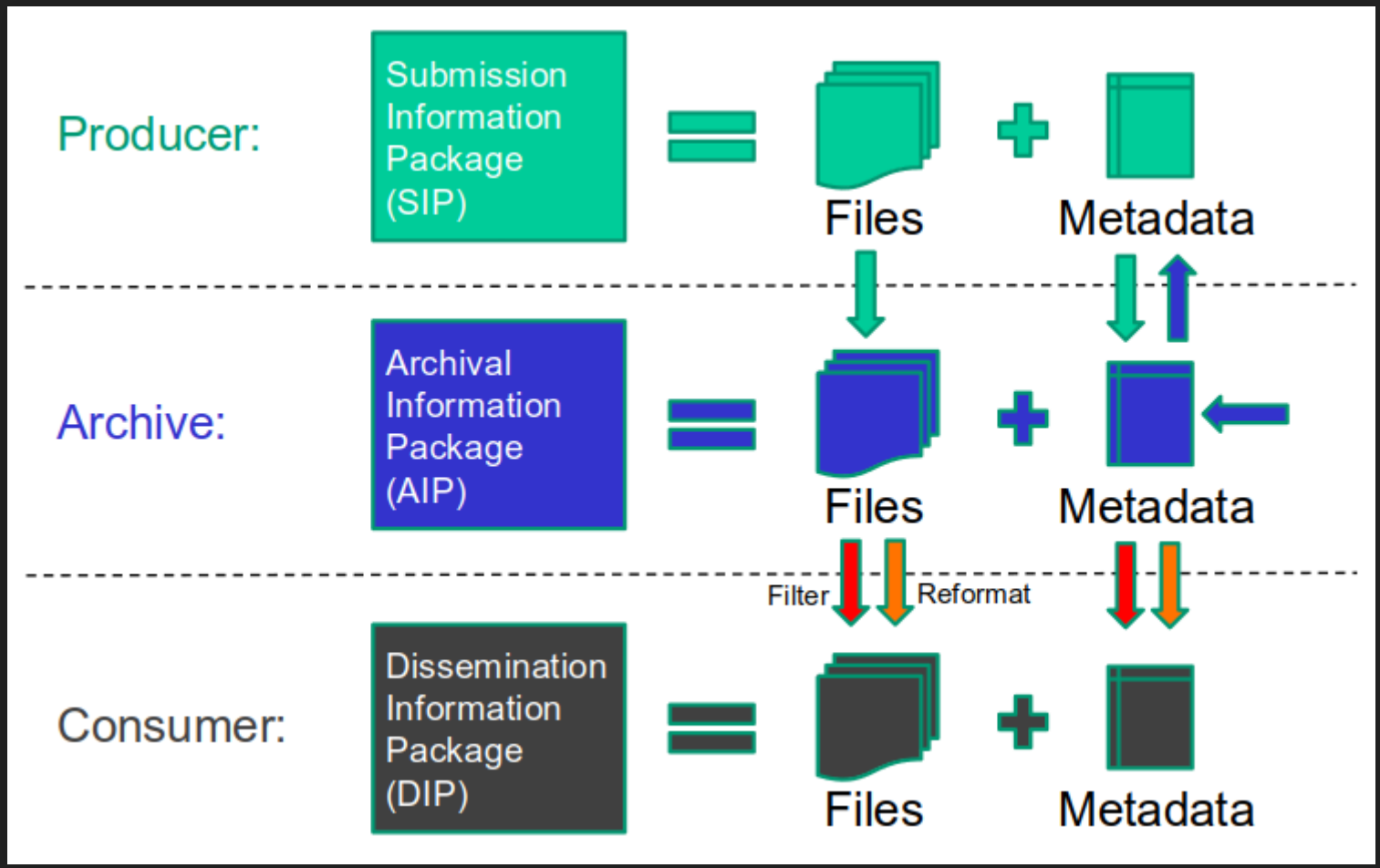
I have constantly voted in Parliament for us to leave the European Union on March 29th, 2019. I truly believe we should have honoured the result of the 2016 Referendum and left on that date. Indeed every time we seek an extension to this process we diminish faith in our political system and the good people, from all political parties, who serve within it. I simply cannot support any further extension to Article 50 and this obviously means I cannot stay in government.

I certainly appreciated the opportunity to serve as a Minister in your Government, but being a backbencher is truly the best job in politics and I now intend to continue to represent and serve my constituents in Daventry to the best of my ability from a seat further back in the House.

Yours sincerely,

CHRIS HEATON-HARRIS MP
MEMBER OF PARLIAMENT FOR DAVENTRY

Tel: 020 7219 7048 Fax: 020 7219 1375
Email: chris.heatonharris.mp@parliament.uk
Website: www.heatonharris.com


Producer:
Submission Information Package (SIP)
Files
Metadata
Archive:
Archival Information Package (AIP)
Files
Metadata
Filter
Reformat
Consumer:
Dissemination Information Package (DIP)
Files
Metadata

THANKS

Jez Higgins

@jezhiggins