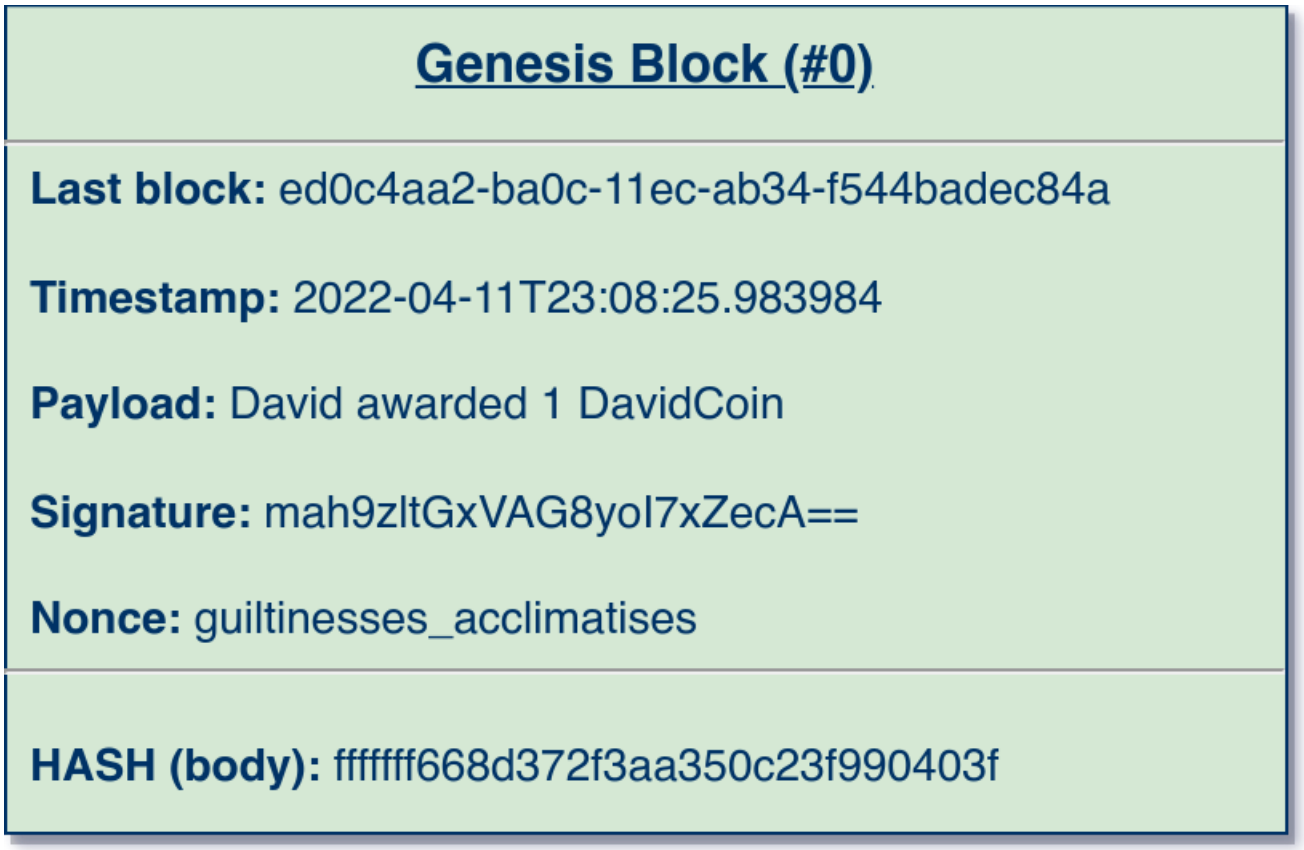
Blockchain, cryptocurrency, NFTs, and dystopianism.

dmertz@atlantistech.com
mertz@gnosis.cx
http://gnosis.cx/cleaning
http://gnosis.cx/regex

GPG 1672C26BB3B3555C794F4AC5BF4561E50EC5166B
BTC 1GaxnVtRegebBDUknHL6ZPRLeAa8yfnFQE
ETH 0x300833A83e37a5374d01DfF395988ba287a6d0e1

Encrypting Tulips in the Modern Prestige Society

Creating a Blockchain (Genesis Block)



Encrypting Tulips in the Modern Prestige Society

Creating a Blockchain (Rules, part 1)

Genesis Block (#0)
Last block: ed0c4aa2-ba0c-11ec-ab34-f544badec84a
Timestamp: 2022-04-11T23:08:25.983984
Payload: David awarded 1 DavidCoin
Signature: mah9zltGxVAG8yol7xZecA==
Nonce: guiltinesses_acclimatises
HASH (body): ffffff668d372f3aa350c23f990403f

The payload block follows a predefined grammar.

"Sentences" include:

- <Identity> **awarded** <amount>
- <Identity> **transfers to** <identity> <amount>

Identity and amount follow some defined sub-grammar.

One payload might contain multiple sentences.

Creating a Blockchain (Rules, part 2)

Genesis Block (#0)
Last block: ed0c4aa2-ba0c-11ec-ab34-f544badec84a
Timestamp: 2022-04-11T23:08:25.983984
Payload: David awarded 1 DavidCoin
Signature: mah9zltGxVAG8yoI7xZecA==
Nonce: guiltinesses_acclimatises
HASH (body): ffffff668d372f3aa350c23f990403f

Last block is usually the hash of the prior block, but in the genesis block it is simply a random UUID.

Timestamp is a coordinated time, such as UTC.

The title is convenient for humans, but does not change anything about the working of the blockchain.

Creating a Blockchain (Rules, part 3)

Genesis Block (#0)

Last block: ed0c4aa2-ba0c-11ec-ab34-f544badec84a

Timestamp: 2022-04-11T23:08:25.983984

Payload: David awarded 1 DavidCoin

Signature: mah9zltGxVAG8yoI7xZecA==

Nonce: guiltinesses_acclimatises

HASH (body): ffffff668d372f3aa350c23f990403f

Signature is proof that a given entity "claims credit" for the prior elements of the body.

```
>>> sign(
 'ed0c4aa2-ba0c-11ec-ab34-f544badec84a',
 '2022-04-11T23:08:25.983984',
 'David awarded 1 DavidCoin',
 david_privkey)


'mah9zltGxVAG8yoI7xZecA=='
```

Encrypting Tulips in the Modern Prestige Society

Creating a Blockchain (Rules, part 4)

Genesis Block (#0)

Last block: ed0c4aa2-ba0c-11ec-ab34-f544badec84a

Timestamp: 2022-04-11T23:08:25.983984

Payload: David awarded 1 DavidCoin

Signature: mah9zltGxVAG8yoI7xZecA==

Nonce: guiltinesses_acclimatises

HASH (body): fffffff668d372f3aa350c23f990403f

₿ uses "proof-of-work." The actor signing this block is required to perform an expensive computation.

```
>>> find_nonce(
 'ed0c4aa2-ba0c-11ec-ab34-f544badec84a',
 '2022-04-11T23:08:25.983984',
 'David awarded 1 DavidCoin',
 'mah9zltGxVAG8yoI7xZecA==')

('fffffff668d372f3aa350c23f990403f',
 'guiltinesses_acclimatises')
```

A valid nonce has the special property that it creates a hash which starts with 7 'f' characters when hex encoded.

Encrypting Tulips in the Modern Prestige Society

Creating a Blockchain (Rules, part 5)

Genesis Block (#0)

Last block: ed0c4aa2-ba0c-11ec-ab34-f544badec84a

Timestamp: 2022-04-11T23:08:25.983984

Payload: David awarded 1 DavidCoin

Signature: mah9zltGxVAG8yoI7xZecA==

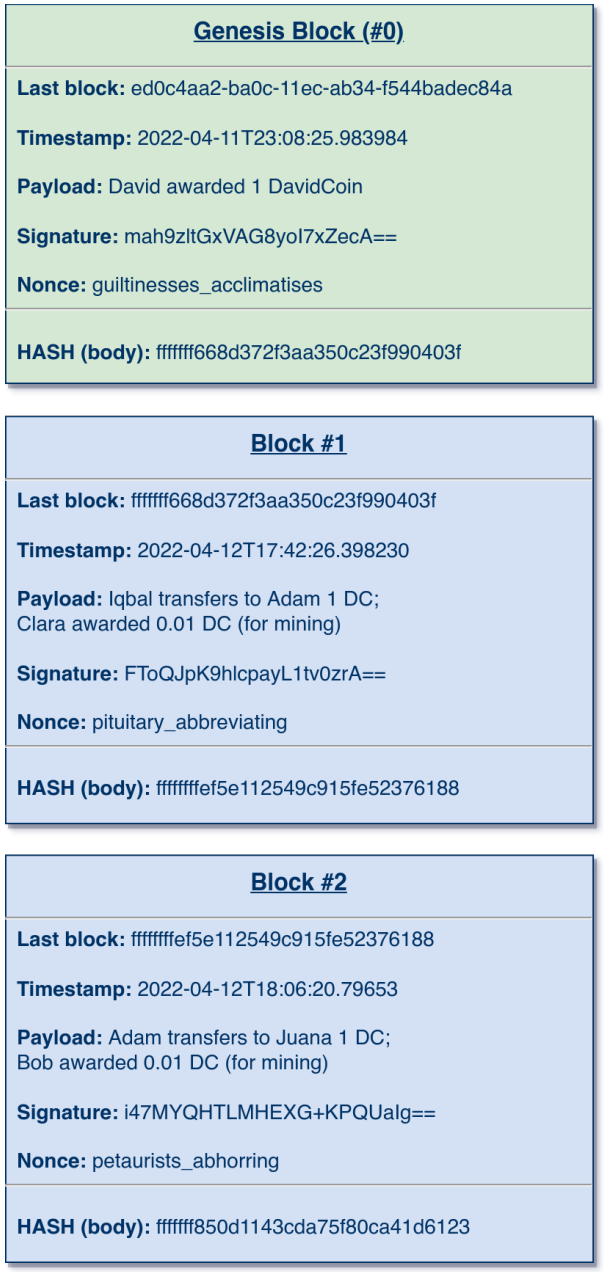
Nonce: guiltinesses_acclimatises

HASH (body): fffffff668d372f3aa350c23f990403f

Validating a block in ₿ is cheap, unlike creating a valid block which is relatively expensive

```
def validate_block(
    last_block: str,
    timestamp: str,
    payload: str,
    signature: str,
    nonce: str):
    s = "\n".join([
        last_block, timestamp, payload,
        signature, nonce])
    return md5(s.encode())\
        .hexdigest()\
        .startswith('fffffff')
```

Encrypting Tulips in the Modern Prestige Society



Adding Entries to the Ledger

Each block can be validated as before.

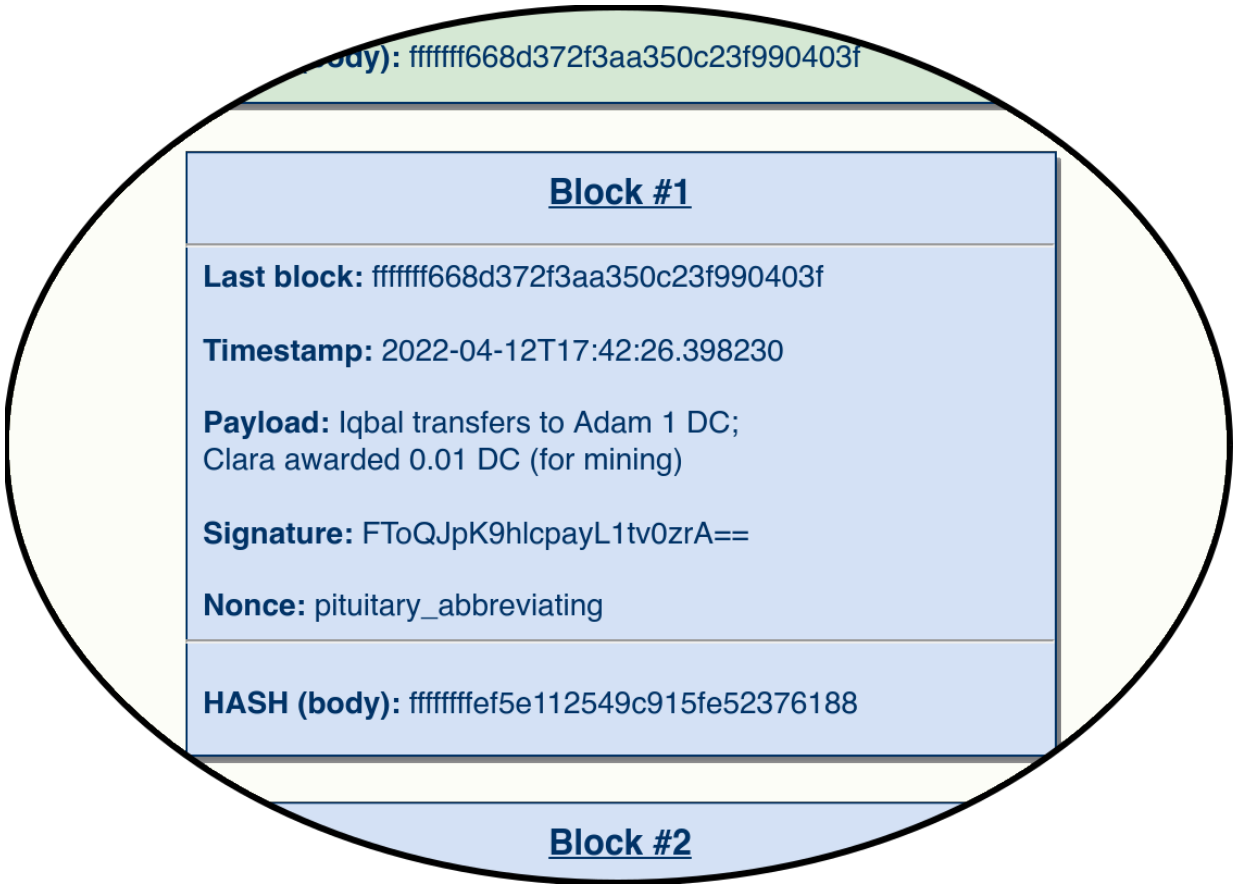
Blocks form a singly-linked list, with each subsequent block referencing its prior block via a hash of a body.

The result is a completely linear ledger of sentences, whose verbs express some fictive action (such as “transfers” or “awarded”

Often use of the ledger is encouraged by awarding some small amount to the actors performing the *expensive* construction of a valid block.

Encrypting Tulips in the Modern Prestige Society

Adding Entries to the Ledger



When a block is added it often includes a "mining fee" as part of the block.

In the example, Clara both signed the block (cheap) and generated a suitable nonce (expensive).

One constraint is that timestamps must be ordered, but this is less important than the proof-of-work and hash link.

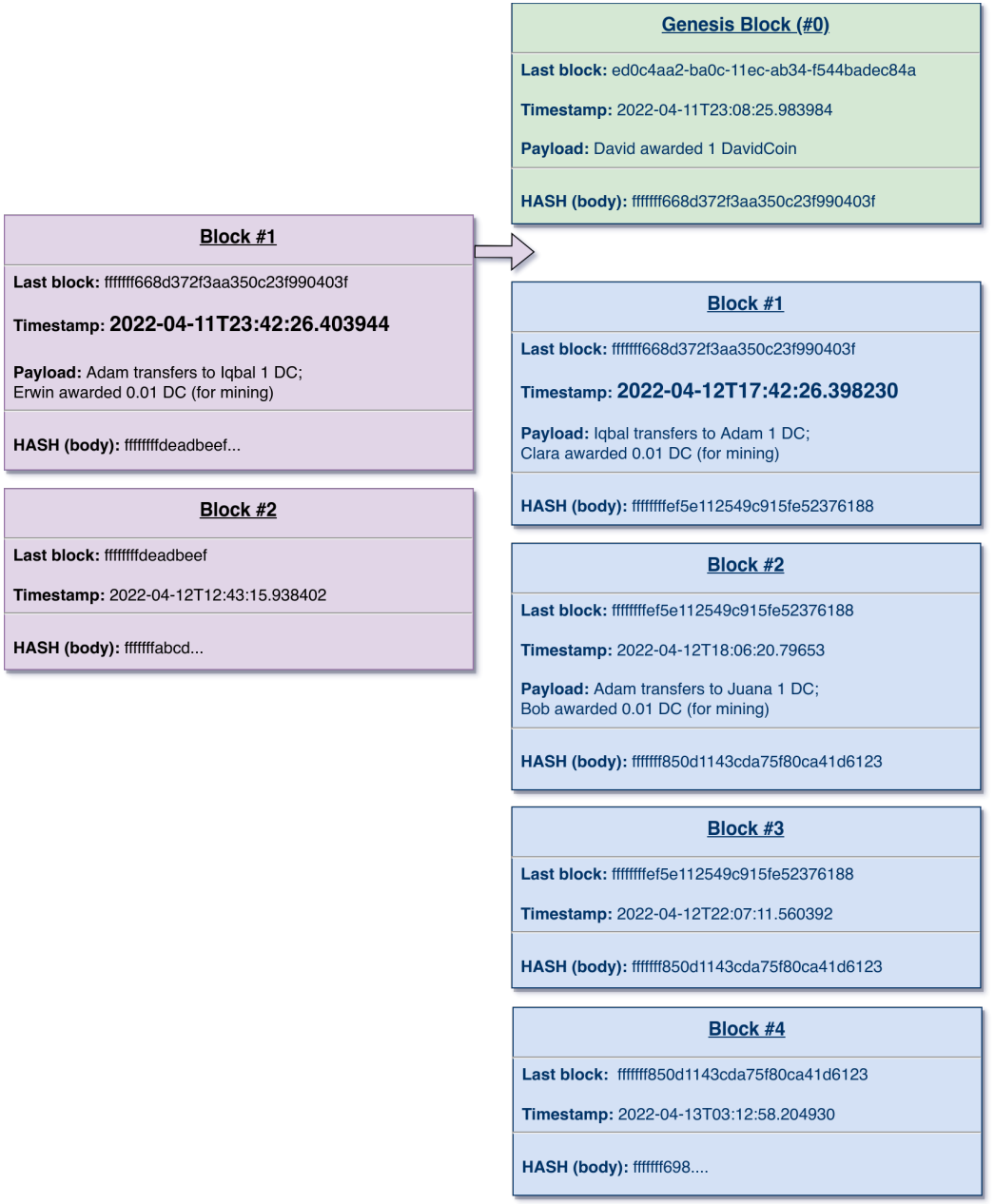
Encrypting Tulips in the Modern Prestige Society

Competing Branches

Communication is imperfect. Clocks are not always synchronized.

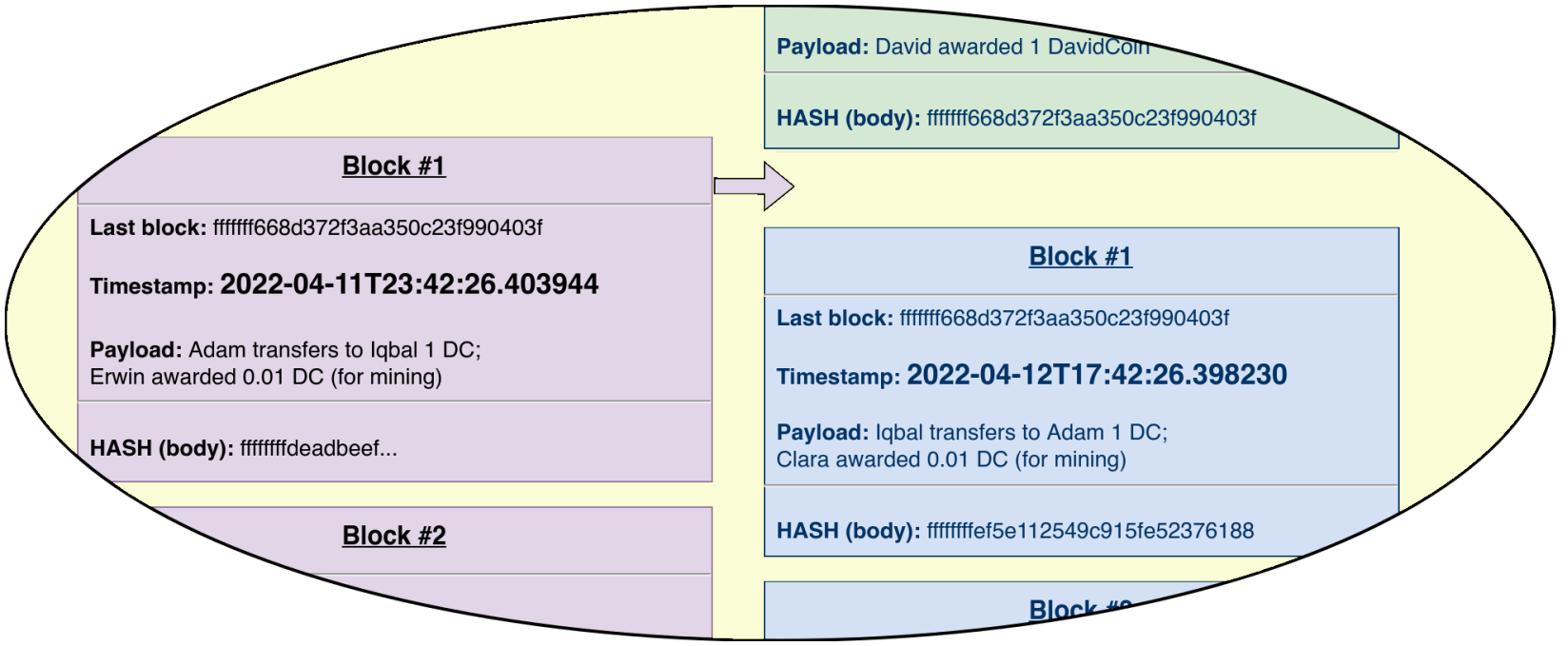
And even more significantly, both the transfer verb and miner rewards provide motivation not to "play fair" for participants.

For example, now that ₿ has become popular, forgers might wish to create branches that favor themselves.



Encrypting Tulips in the Modern Prestige Society

Competing Branches



The block with hash *ffffff...deadbeef* has an earlier timestamp than the one with *ffffffef5e...*. Let's stipulate also that it is a valid block, and references the genesis block.

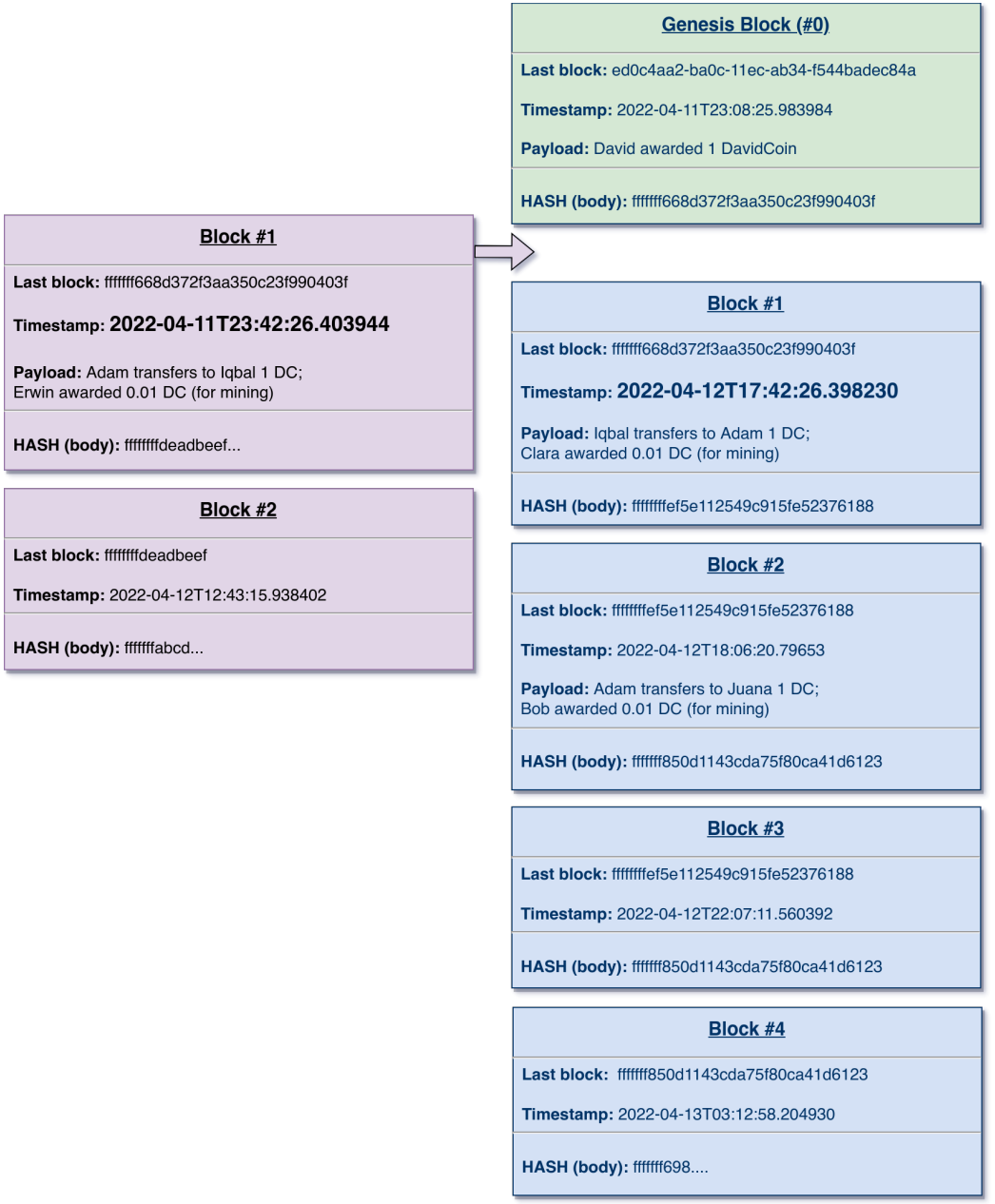
Dates can be wrong, whether by falsification or simply clock drift. Instead of timestamp itself, the rule is "longest chain wins."

Encrypting Tulips in the Modern Prestige Society

Longest Chains

The blockchain for ₿ includes **all** of the blocks shown. The violet blocks are currently *orphans* but the blue blocks could become orphas as blocks are added.

Different actors benefit from different subchains "winning." With many "players" no small group of bad actors can (hopefully) produce a longer chain than that the collective of unaligned actors produces.



Encrypting Tulips in the Modern Prestige Society

Digital Identities

> *Capitalism is the astounding belief that the most wickedest of men will do the most wickedest of things for the greatest good of everyone.*
>
> *– "John Maynard Keynes"*

One thing we can say with certainty of this most famous quote attributed to our friend, the author of *The General Theory of Employment, Interest and Money*, is that it was first spoken by someone else, at some point considerably later than 1935.

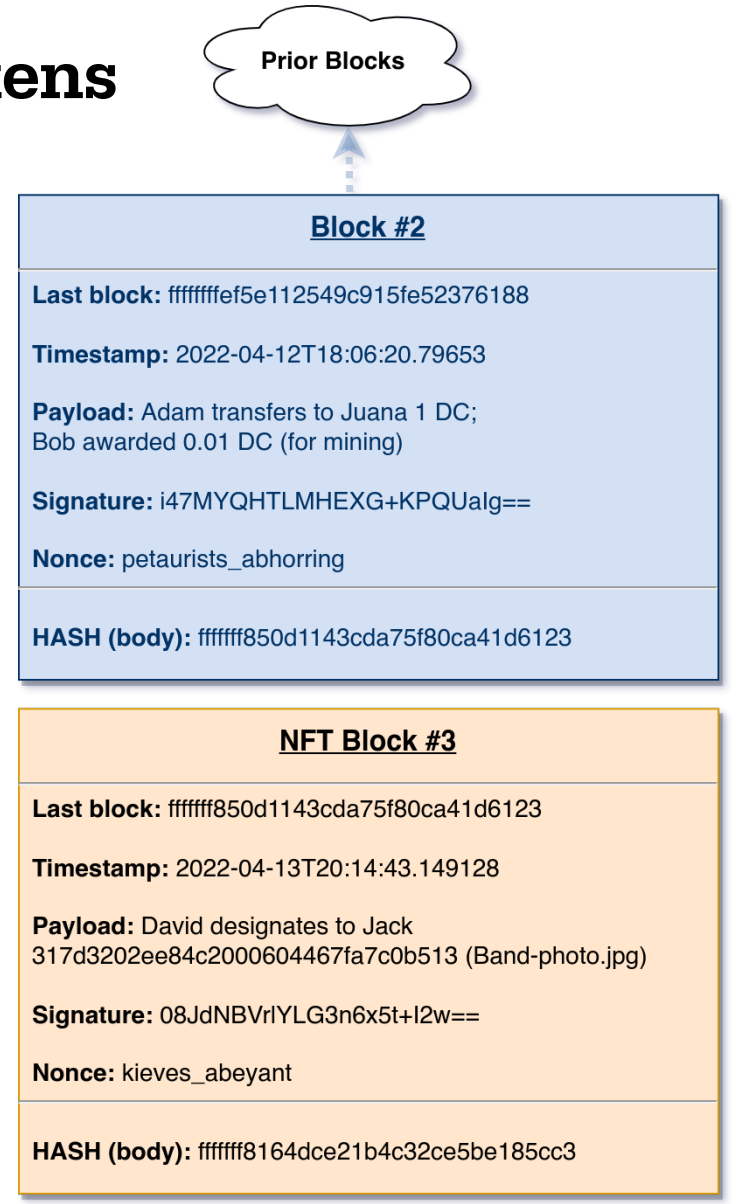
Satoshi Nakamoto, likewise, may or may not belong to that school that fetishizes Keynes' "barbarous relic" over "fiat currency." Iconographic suggestions are not definitive.

Encrypting Tulips in the Modern Prestige Society

New Verbs and Non-Fungible Tokens

In the blocks shown so far, all the "sentences" in payloads had to do with crediting or debiting ₿ among actors—either as transfers or mining awards.

We can stipulate that our grammar actually has an additional verb: "designates to" which pertains to *something* other than ₿.



NFTs and "What the Heck is *designate?!* "

The block in the last slide was valid!

The signature matches "David's." The nonce genuinely took computational work to find, and thereby to created a hash following the agreed leading 'fffffff' characters.

But what is the payload?

> *David designates to Jack*
> *317d3202ee84c2000604467fa7c0b513 (Band-photo.jpg)*

NFTs and "What the Heck is *designate?!* "

> *A commodity appears, at first sight, a very trivial thing, and easily understood. Its analysis shows that it is, in reality, a very queer thing, abounding in metaphysical subtleties and theological niceties. – Karl Marx (Capital, volume 1)*

"David designates to Jack 317d3202ee84c2000604467fa7c0b513 (Band-photo.jpg)."

The image of several farm animals, posed as if on a prog-rock album cover, has the filename 'Band-photo.jpg' on my computer.

Those bytes have the hash listed independently of the filename or where it is copied. Moreover, the hash of the block containing that sentence is globally unique, and **unforgeable** in its position in the overall chain (once enough additional blocks build from it).

NFTs and "What the Heck is *designate?!* "

"David designates to Jack 317d3202ee84c2000604467fa7c0b513 (Band-photo.jpg)."

What has Jack *gotten* by means of this block embedding in the chain?

I do not own the copyright on that image. That is ©International Color Consortium, 2009. As a reference image in a spec, I believe I have fair use rights for these slides.

Still, if the ICC were to sue me for this use, I might be liable and Jack definitely would not be. Such a suit can have no affect on the validity or immutability of the block in question, nor to the blockchain to which it belongs.

NFTs and "What the Heck is *designate?!* "

"David designates to Jack 317d3202ee84c2000604467fa7c0b513 (Band-photo.jpg)."

I am not being sneaky by designating an image I do not hold copyright on. There *are* photographs and other works that I have created myself, and hold full copyright in.

If I had instead "designated to" Jack some item I hold the copyright on, that block would *also* not in itself transfer any copyrights to him.

Of course Jack and I could execute a copyright transfer or license, but that would involve lawyers, contracts, and courts, **not** a block on the DavidCoin chain.