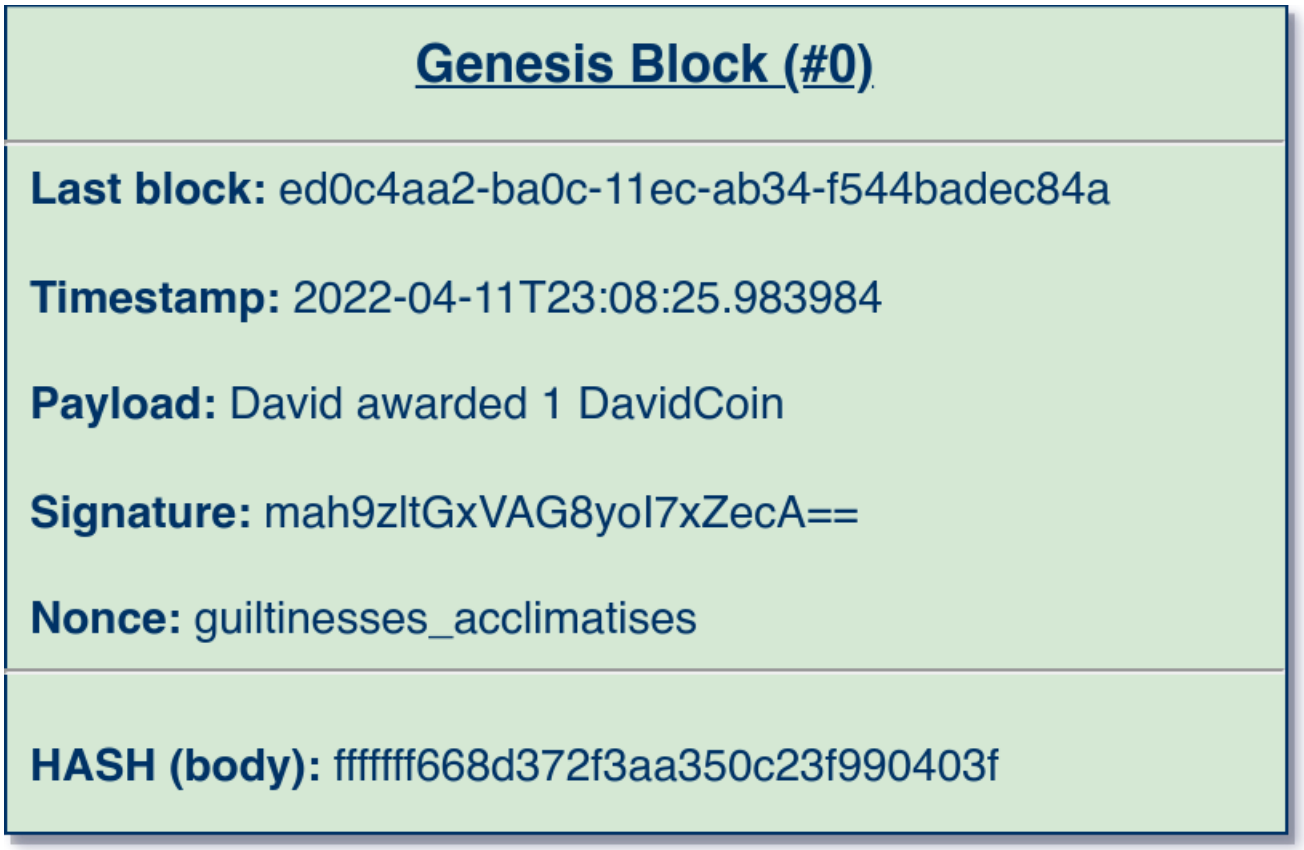
# Blockchain, cryptocurrency, NFTs, and dystopianism.

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 field 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

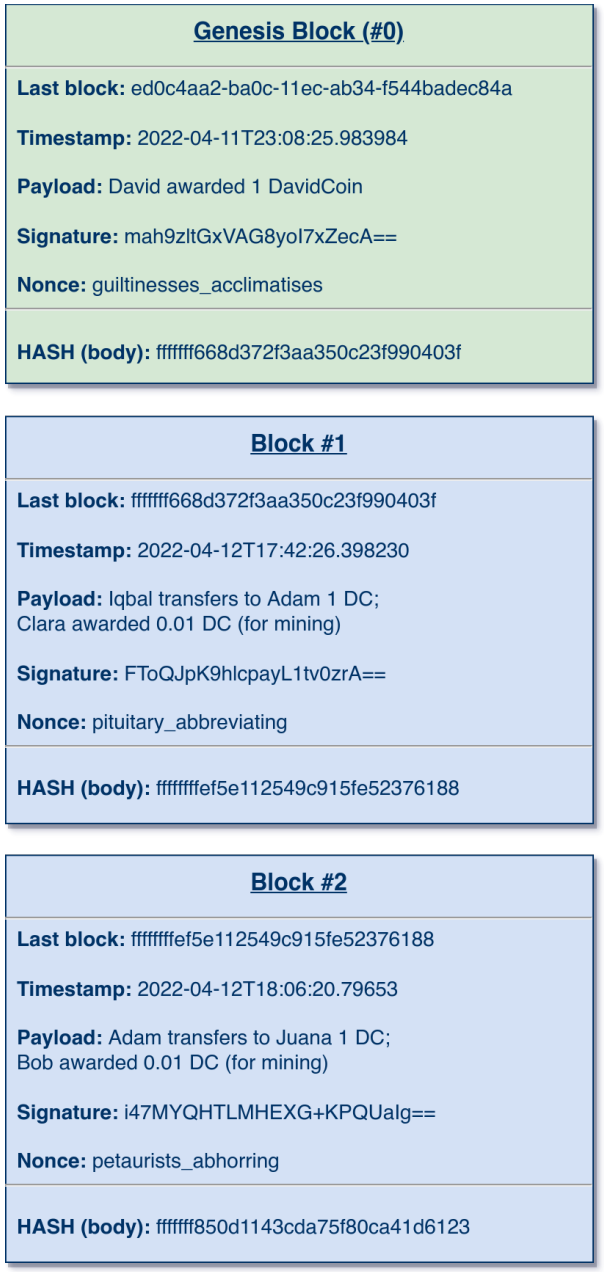
**Signature:** mah9zltGxVAG8yoI7xZecA==

**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')
```




## Adding Entries to the Ledger

Each block can be validated as before.

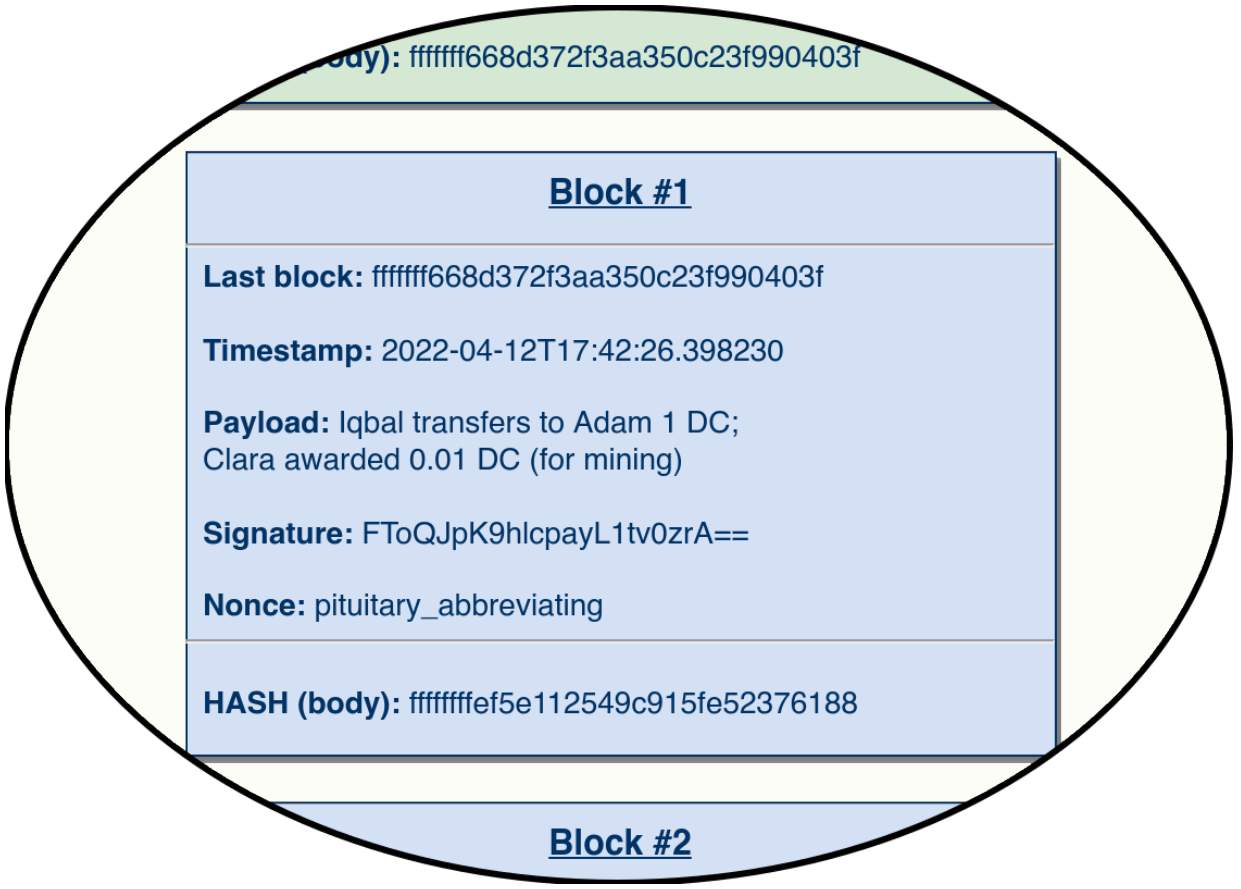
Blocks form a singly-linked list, with each subsequent block referencing its prior block via a hash of a body.

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.

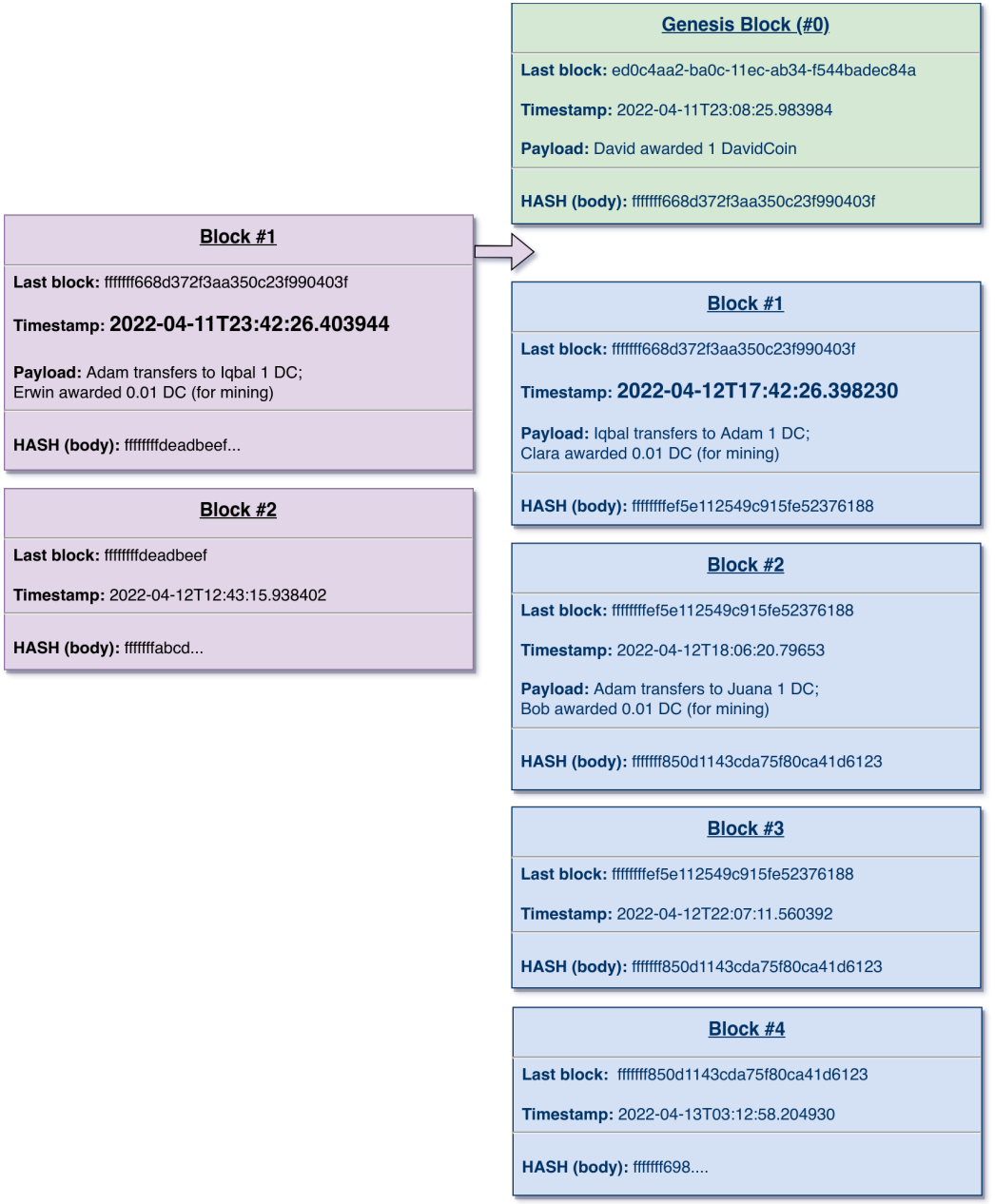
# Encrypting Tulips in the Modern Prestige Society

## Competing Branches

Communication is imperfect. Clocks are not always synchronized.

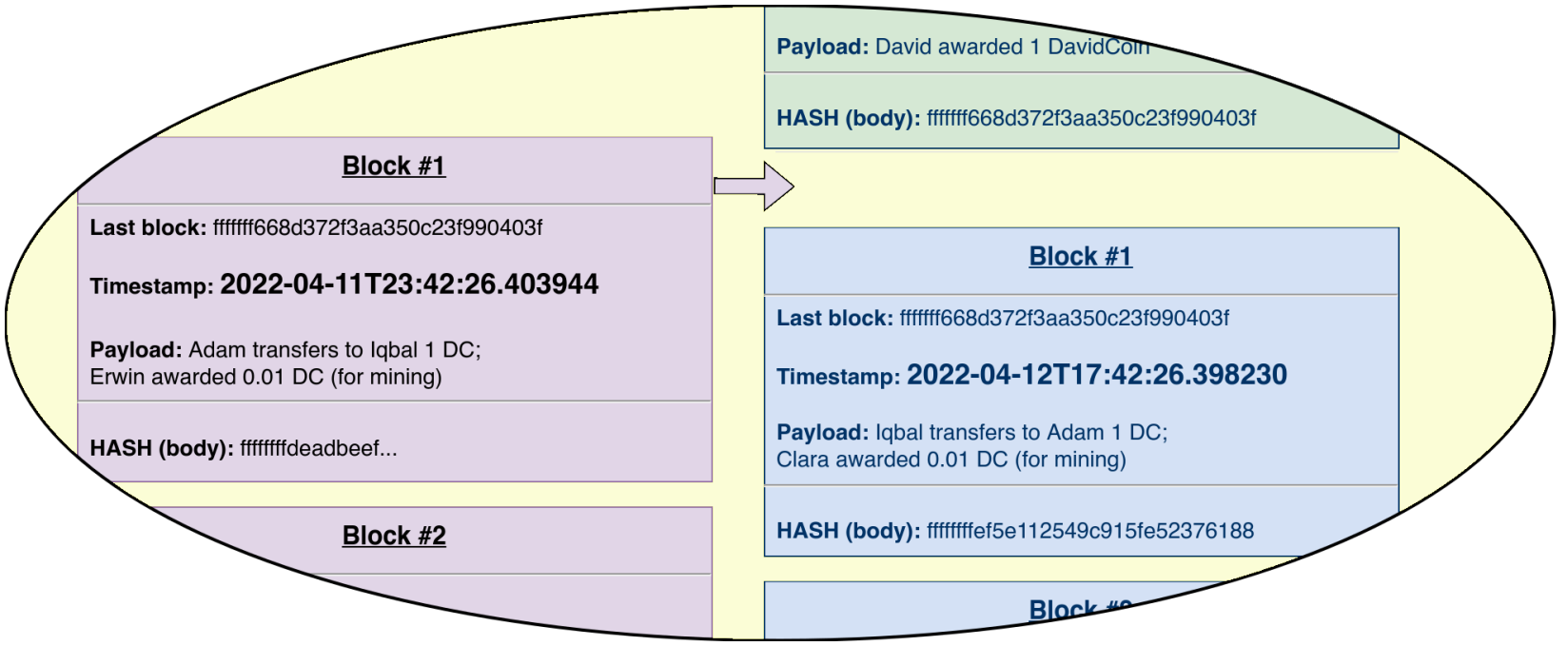
And even more significantly, both the transfer verb and miner rewards provide motivation not to "play fair" for participants.

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.

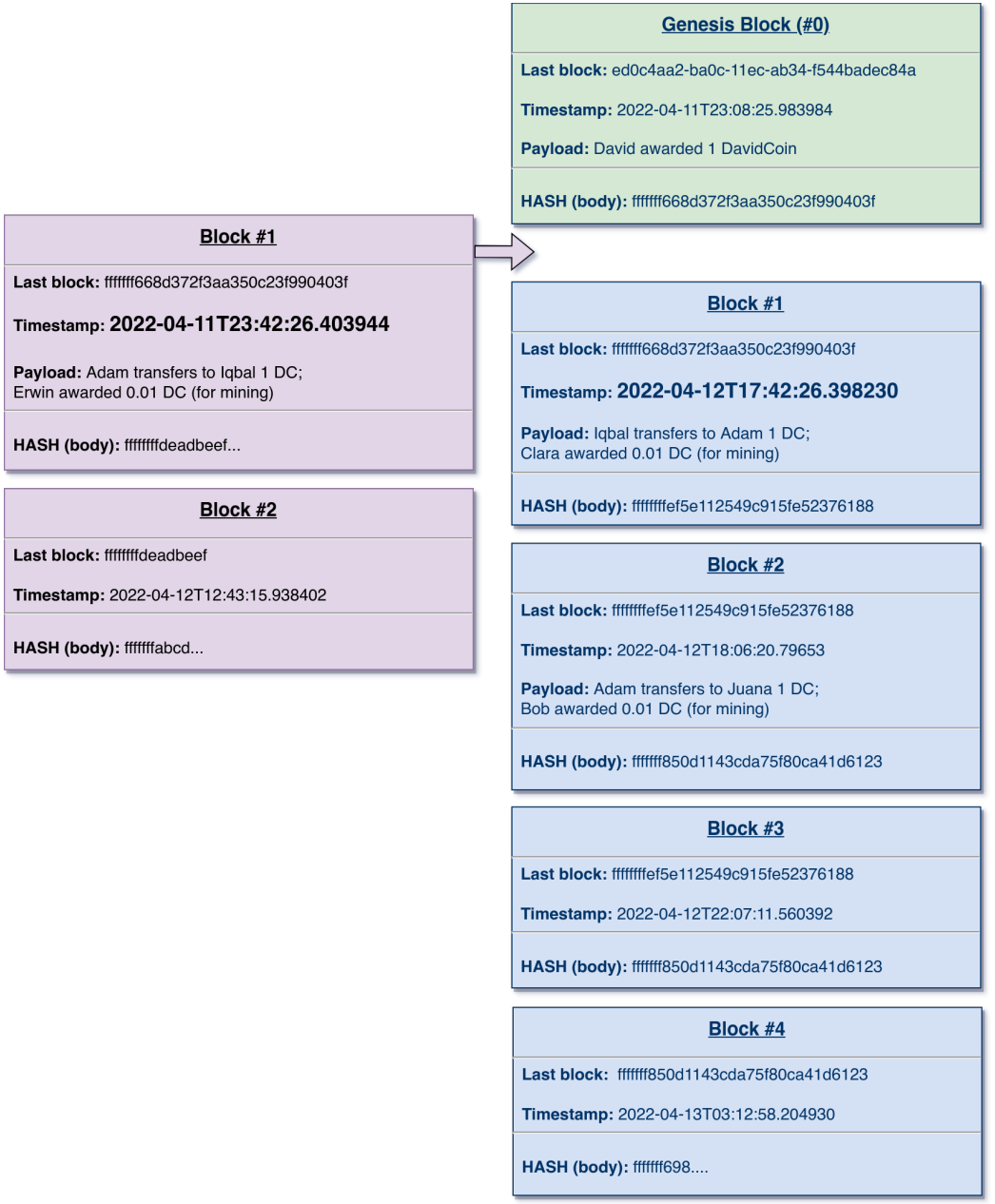
Dates can be wrong, whether by falsification or simply clock drift. Instead of timestamp itself, the rule is "longest chain wins."

# 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.

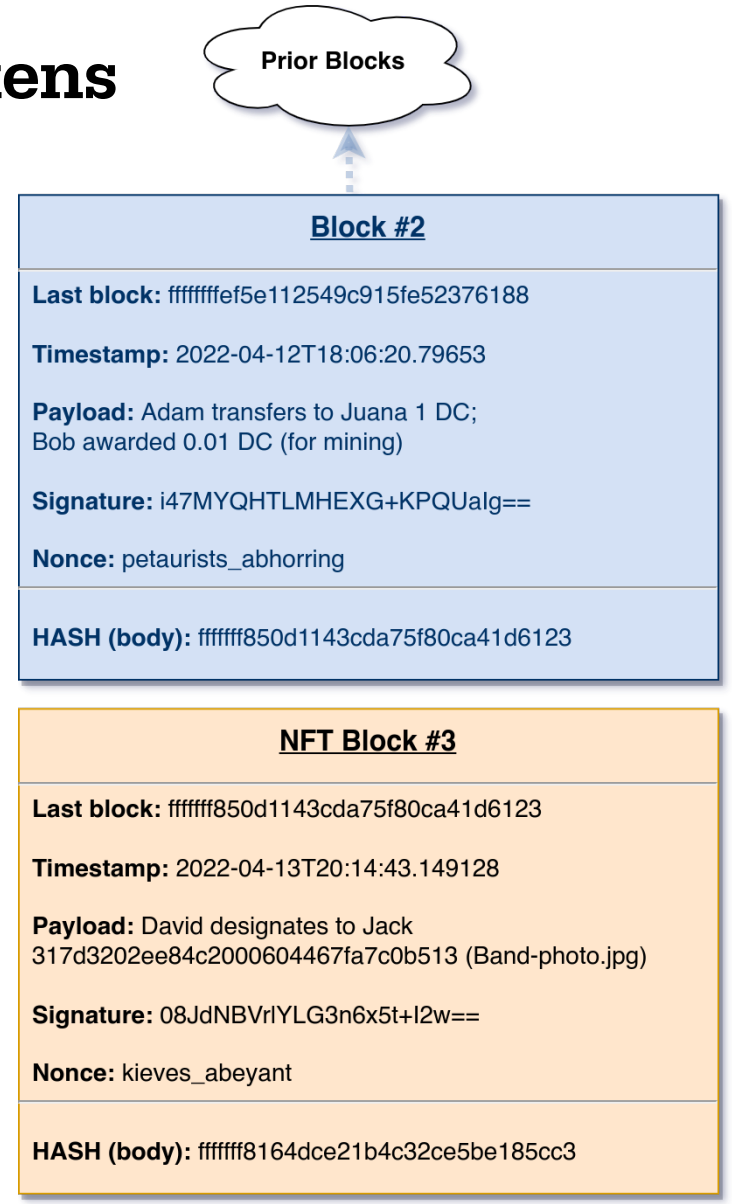
Satoshi Nakamoto, likewise, may or may not belong to that school that fetishizes Keynes' "barbarous relic" over "fiat currency." Iconographic suggestions are not definitive.

# 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?!* "

> *An NFT 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. It is held as ©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 lawsuit can not affect the validity or immutability of the block in question, nor of 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.

# Encrypting Tulips in the Modern Prestige Society

## The Map and the Territory (Smart Contracts)

The grammar of ₿ sentences could be expanded just slightly to allow for so-called "smart contracts."

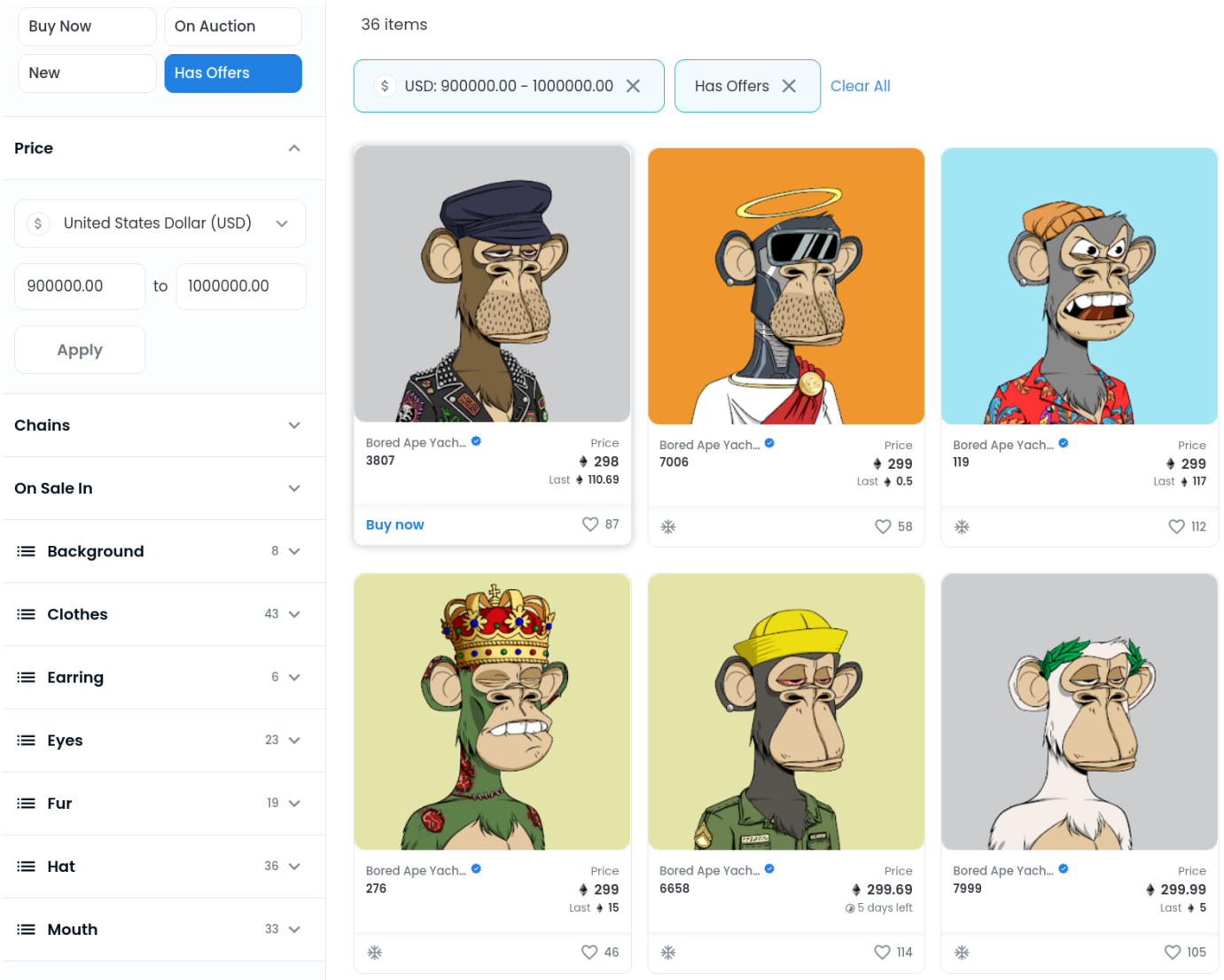
> *David designates to Jack 317d3202ee84c2000604467fa7c0b513* **contingent upon** *a subsequent block transferring 10 DC from Jack to David*

Anyone following the DavidCoin protocol will decide whether to transfer *Band-photo.jpg* from the David column to the Jack column in their balance table, based on scanning forward for blocks fulfilling the stated predicate.

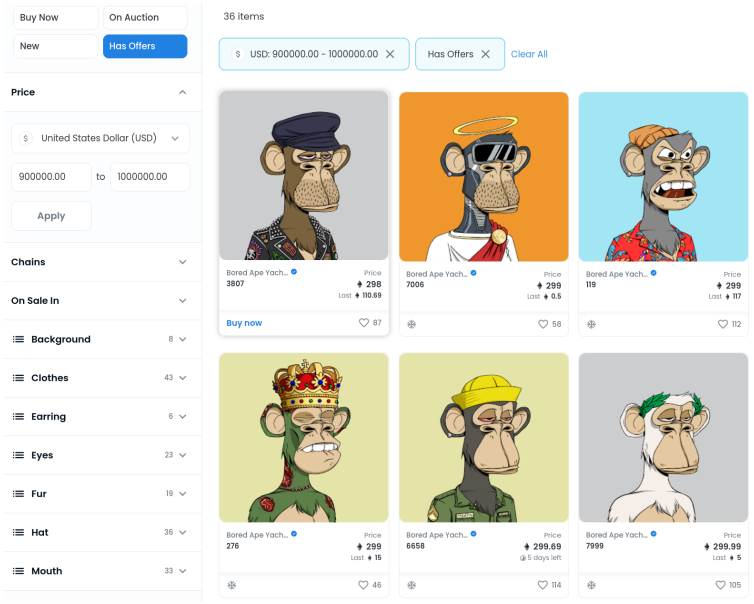
Ethereum, for example contains a little programming language for expressing predicates like that illustrated in this slide.

# Encrypting Tulips in the Modern Prestige Society

## The Map and the Territory (A Looking Glass Darkly)



## The Map and the Territory (A Looking Glass Darkly)




I do not hold copyright in any of the Bored Ape Yacht Club cartoons. However, my reproductions here are clearly Fair Use.

These cartoons consist of exactly 100k distinct images generated algorithmically.

Tens of thousands of entities have each transferred 100s of ETH (amounts currently exchangeable for up to USD 1,000,000) to have blocks placed on the Ethereum blockchain stating:

*BAYC designates <ape_###> to <buyer>*

## The Map and the Territory (A Looking Glass Darkly)

What?!

## The Map and the Territory (A Looking Glass Darkly)

What?!

# Huh?! You are joking, right?!

**The Map and the Territory (A Looking Glass Darkly)**

What?!

# Huh?! You are joking, right?!

*No, **Seriously**! Why would someone pay all that money for a few bytes in a small record?!*

## Commodity Fetishism / Abstraction as Commodity

There are a great many ways in which human societies and human beliefs are fundamentally irrational. Arguably, sport or casino gambling are such irrationalities. Arguably, many religious beliefs are so.

Extreme pricing of "prestige" goods, like collectible artwork or luxury brands, contain a similar irrationality.

Most certainly, Ponzi schemes and directly fraudulent pitches play off of irrationality, greed and wish fulfillment.

## Commodity Fetishism / Abstraction as Commodity

While cryptocurrencies and NFTs have family resemblances to these referenced human irrationalities, there simultaneously seems to be something novel in fervent enthusiasm for blockchain.

Some proponents are simply motivated by greed. Others believe that these specific technologies offer utopian possibilities for better societies.

In some ways these beliefs are akin to 1980s-90s beliefs in the inherent liberation of the internet as a technology; in other respects they continue a libertarian fetishism about gold and silver as "inherently valuable" in contrast to "fiat currency."

## Commodity Fetishism / Abstraction as Commodity

To look rigorously at the development of blockchain, we have moved through these historical stages of capital exchange:

- Commodity fetishism in which value is reified as the concrete form of sold objects rather than in human relationships of exchange.
- The financialization of almost everything, in which exchange of derivatives (or derivatives of derivatives) largely supersede exchange of commodities as stores of value.
- The pure form of exchange as simulacrum, represented in cryptocurrencies.
- A paranoic nostalgia for concrete things within the simulacra of blockchains, represented as NFTs.

## Dead Presidents and Dead Money

Like capital itself, crypto-capital is highly concentrated in the hands of very few people. The Gini coefficient of crypto assets is likely even higher than of overall wealth inequality.

I want to look briefly at several "factions" of crypto-enthusiasts, from least to most significant.

- Libertarian and conspiracy-adjacent advocates
- Leftish techno-enthusiasts with utopian aspirations
- The ultra-rich seeking new mechanisms of conspicuous display
- Big capital represented by large banks, central governments, hedge funds, and private equity.

## Dead Presidents and Dead Money

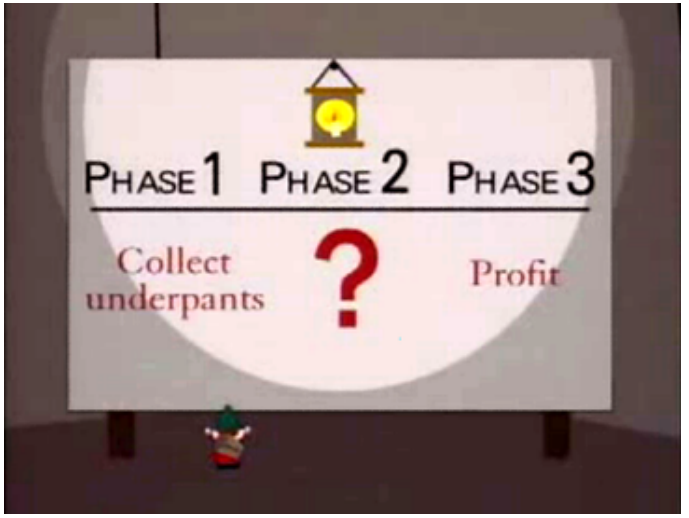
There are a fair number of working- to lower-middle-class people or technical operators of the computerized mechanisms of capital flow who, for whatever reasons, psychological or sociological, gravitate towards a bundle of libertarian, Randian, Chicago-school, or Austrian-school economics.

I think that one finds a fair convergence here with conspiracy theorist that fixate on the end of the Bretton Woods System, and obsession with "fiat currency" and the evils of government regulation, and sometimes reach into darker corners of "globalist" and anti-semitic conspiracy theories.

At heart though, cryptocurrency simply represents a "new thing" that represents, to their belief, independence from government oversight.

# Encrypting Tulips in the Modern Prestige Society

## Dead Presidents and Dead Money




Closest to my own heart are the techno-utopians who share with me admirable goals of human liberation, democratization of finance, enabling new forms of social collaboration, or even fairly banal goals like enforcing agreements among parties.

Many of these same folks are perhaps a bit too young to remember when Freenet, PGP/GPG, BitTorrent, and Tor, each represented other projects that combined many of the same cryptographic primitives with authentically lofty social goals.

All of those still exist, as do many other cryptographic projects targeted at social goods. What the others lack is mostly just ending with the final clause "on the blockchain" in their descriptions.

## Dead Presidents and Dead Money

Conspicuous consumption remains a motivation in NFT transactions, in particular.

Paris Hilton and Jimmy Fallon are rich celebrities who could afford a garrulously ugly jewel-encrusted US$1M+ Cartier watch. For less than half that price they can make a banal Bored Ape their Twitter avatars.

Or rather, I could do the same thing for free by copying a Bored Ape image, but it would not come with a “certificate of authenticity” block, similar to the one that probably comes with the overpriced watch.

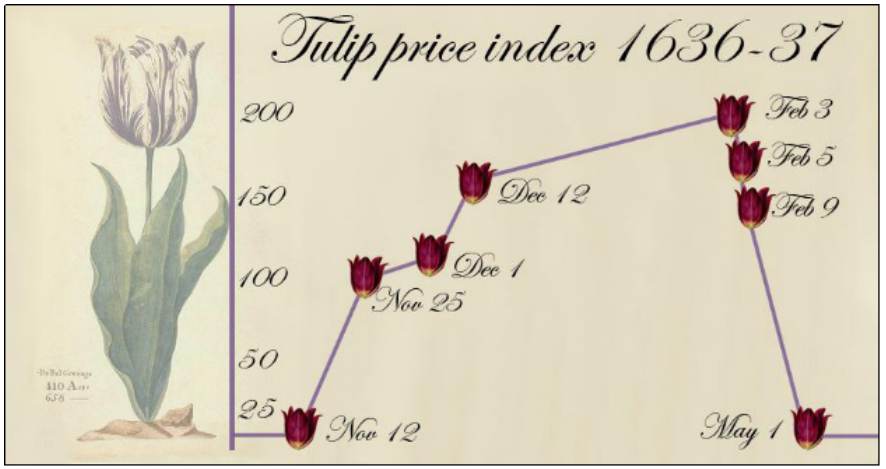
## Dead Presidents and Dead Money

"Dead Money" is a colorful term for *global savings glut.* As J.A. Hobson noted in the early 20th century (similarly analyzed by both Karl Marx and J.M. Keynes), Say's Law that "Supply creates its own demand" is both widely held and fundamentally wrong.

In times of extremes of wealth inequality and of capital reserves greatly exceeding obvious productive capital expenditures, capital relentlessly seeks new outlets. On notable recent time of such an extreme imbalance was the securitization crisis of 2008 (and its "Great Recession").

Satoshi Nakamoto's paper, *Bitcoin: A Peer-to-Peer Electronic Cash System*, introducing the blockchain concept was published in January 2009.

## Dead Presidents and Dead Money




Your struggling musician friend who believes—with a crudely fleshed-out worldview—that selling NFTs of their songs can make them more money than than sleazy record companies will part with is quite plausibly not wrong.

Your college roommate who at some point bought a Bitcoin at $1000 and sold it at $30,000 genuinely made a tidy profit that feels like it should have a rational explanation.

I have profited by a month salary making random trades of crypto-currencies. But then, my first trade ever was spending a few hundred dollars on put options on October 15, 1987. Gambling creates an endorphin rush, and wins stand out over losses in subjective recollection.

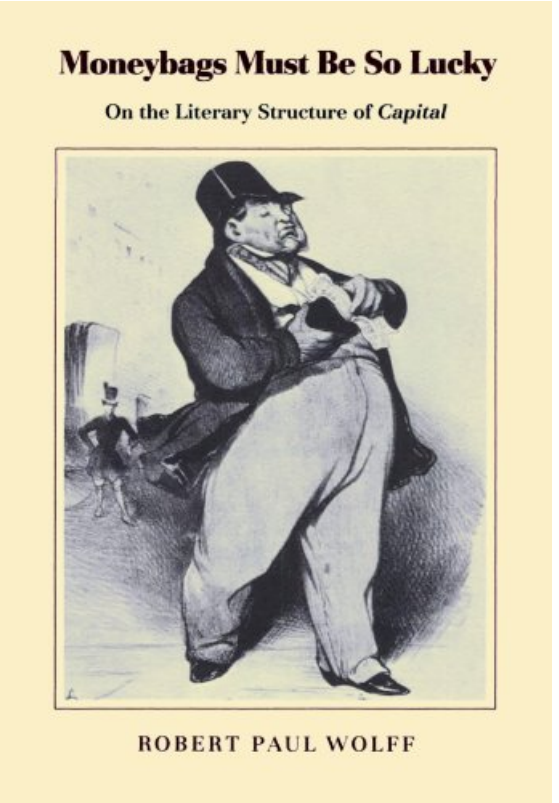
# Encrypting Tulips in the Modern Prestige Society

## Dead Presidents and Dead Money

Your friends do not run international banks that hold trillions of dollars in reserve assets.

Your friends do not chair the reserve banks of large national governments.

... or if they do, this probably isn't the room you were trying to be in.




My old doctoral advisor wrote a a clever book. My outside member, unrelated but sharing a last name, wrote quite a lot of more clever books though.

## The Misfortunes of Static Virtue

.