NYCU BDAF guest lecture

May 22, 2025

With the kind invitation of Martinet at Quantstamp/Zircuit, I gave a guest lecture at NYCU in Taiwan for the Blockchain Development and FinTech course, on May 6. I took the liberty to define the nature my talk, one that situates the advent of decentralized consensus networks in a bigger picture. I challenged myself to trace things back 100 years, back to when Hitler became the leader of the reestablished Nazi party. Why?

"*Chancellor on brink of second bailout for banks*" was engraved into the genesis block of Bitcoin. This industry was born from the invention of a global digital ledger that explicitly wishes to disassociates itself from the governments of the world. Why? On the streets, one would have no trouble finding a large number of answers - the issue with the dollar's worth, US debts and so on. Case in point, just over the last few days the industry's timeline is filled with comments about the downgrade of US credit rating and the rising of bond yields.

ECONOMY | CENTRAL BANKING

U.S. Loses Last Triple-A Credit Rating

Moody's downgrades the U.S. government, citing large fiscal deficits and rising interest costs

By Matt Wirz Follow and Sam Goldfarb Follow

Updated May 16, 2025 9:52 pm ET

Yet, this industry cares enormously about what the regulators think. News about ETF approvals stroke the nerves of market participants. A system that was created to operate fiercely

independently in spite of governments are valued by investors closely watching the sentiment of governments toward said system. That is a fascinating paradox.

All in all, I wish to dig into the history about the tanglement of money, US fiscal policy, and geopolitics. Gain my own perspective. And share my learning with the students.

History fascinates. One can depth-first-search endlessly in the literatures. History also dwarfs. There are so much interdependent factors at work that I am afraid any of my attempts to connect some dots in support of specific arguments are doomed to be premature.

But I reconsidered. A while ago I stumbled upon *Bird by Bird* by Anne Lamott, a book about how to write:

> *We were out at our family cabin in Bolinas, and he was at the kitchen table close to tears, surrounded by binder paper and pencils and unopened books on birds, immobilized by the hugeness of the task ahead. Then my father sat down beside him, put his arm around my brother's shoulder, and said "Bird by bird, buddy. Just take it bird by bird."*

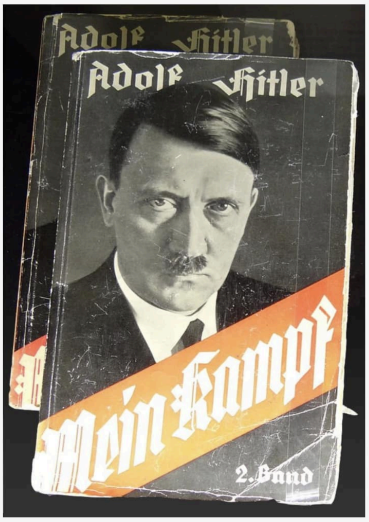
I decided that it's ok to take the convoluted history bird by bird. It's ok to share my embeddings in-flight, as I rummage through my input data.

The following captures the talk in cleaned up text form.

Thank you Martinet for the graceful introduction. Originally I wanted to give you guys some ideas about decentralized systems and consensus. But, I thought that we are in a very interesting time, and blockchain is not just a technology for the sake of technology, it actually has lots of implications in the big big picture. So I thought it would be very useful to tell you what I see at the big picture level, what does that mean to blockchains and beyond.

Debt & Currency

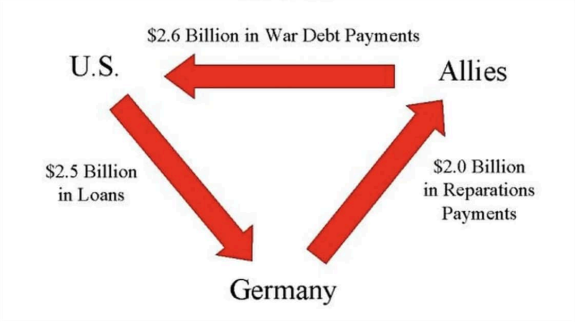
So I wanted to start with the idea of debt and currency which are extremely old ideas dating back to at least 5000 years ago.



Mein Kampf; Hitler became Nazi party leader
Feb 25, 1925

But let's just go back by 100 years. In 1925, Hitler came out of prison. He went to prison because he attempted a coup at the Weimar government and failed. He was sentenced to 5 years in prison but was very quickly bailed out. In 1925 he came the Nazi party leader. Mein Kempf is the book he wrote in the prison, where he talked about his struggle and his political ideology, which is a widely read book and banned because it obviously contributed to the massacre of Jews.

Dawes Plan
1924-1929



Wall Street crash of 1929

Going to 1929. What happened in 1929 was a bunch of things. But we have to cover the Dawes Plan. Basically Germany came out of the WWI, losing the war, owing a lot of money to allie countries. So Germany had to pay for the reparations for other European countries. That put a lot of pressure on the German economy. Therefore a plan was in place for the US to loan money to Germany to pay for the reparations. Because of this loan, the economic pressure was relieved and that actually caused a golden period, the *Goldene Zwanziger*, where the economy was booming. That was when the hyperinflation just receded around 1923. But what happened in 1929 was that the Wall Street crashed. If you're American and your economy is not doing so well, the first thing you would cut is paying the country that just lost the war. So the US cut down their loans to Germany and asked for repayments sooner, causing the German economy to deteriorate very quickly So that was the historical context where the Nazi rose.

Election year	Votes	%	+/–	Seats won	+/–	Position	Leader
1928	810,127	2.63	▲ 2.63 pp	12 / 491	▲ 12	9	
1930	6,379,672	18.25	▲ 15.62 pp	107 / 577	▲ 95	▲ 2	
July 1932	13,745,680	37.27	▲ 19.02 pp	230 / 608	▲ 123	▲ 1	
November 1932	11,737,021	33.09	▼ 4.18 pp	196 / 584	▼ 34		 Adolf Hitler
March 1933	17,277,180	43.91	▲ 10.82 pp	288 / 647	▲ 92		
November 1933	39,655,224	92.11	▲ 48.20 pp	661 / 661	▲ 373	– 1	
1936	44,462,458	98.80	▲ 6.69 pp	741 / 741	▲ 80		
1938	44,451,092	99.08	▲ 0.28 pp	813 / 813	▲ 72		

Nazi Party parliamentary elections
-- 1928: 2.63%
-- 1930: 18.25%
-- 1932: 37.27%

If you look at this election results of the Nazy party at the German parliamentary. In 1928, the Nazi party got 2.6% of the parliament. Already in 1932, just four years later, it's got 37% of the parliamentary. It was a very fast rise.

Article 48 of the Weimar Constitution;
Hitler appointed Chancelor
Jan 30, 1933

That ultimately resulted in 1993 where Hitler was appointed the chancellor of Germany by the president, Hindenburg, who was a very old man (85 years old). Before Hitler became Chancelor, there were two more Chancelors that were trying to keep Hitler out of the office, but the German economy was doing so badly, they couldn't really change it. And in a democracy, you are supposed to make decisions based on the people's will, and with Nazi party's rise in the parliamentary, that basically meant the Nazi represented the people's voice. Due to the rule of democracy, it was almost inevitable that the Nazi party leader became the Chancelor. Article 48 of the Weimar Constitution basically meant that before Hitler became the Chancelor, the parliamentary was blocking so many laws from passing, obviously Nazi being very much at odds with other parties. They couldn't reach consensus and the parliamentary broke down all the time. If you have a parliamentary breakdown, no laws can be passed, the government basically stops operating. So Article 48 was the idea that in extraordinary time, the president can sign special laws that go into effect immediately, bypassing the congress. But that means the democracy was failing, which further incited people's anger, espeically the people that were under Hitler's influence.

One thing that is tragically interesting to note is that in 1925 Hitler was ordered by the court to not give public speech for two years. Because Hitler was great at public speeches and so great at making people angry and follow what he said. His public speech was dangerous. The court ordered he could not give public speeches. In fact, he attempted the coup, and treason warrants the death sentence. But he actually gave public speeches at the court which changed the opinions and he go sentenced to 5 years and came out in mere 9 months. So that was a demonstration of his ability to influence and trigger the madness of the crowd, a central topic of the WWII.

Normandy Landing
June 6, 1944

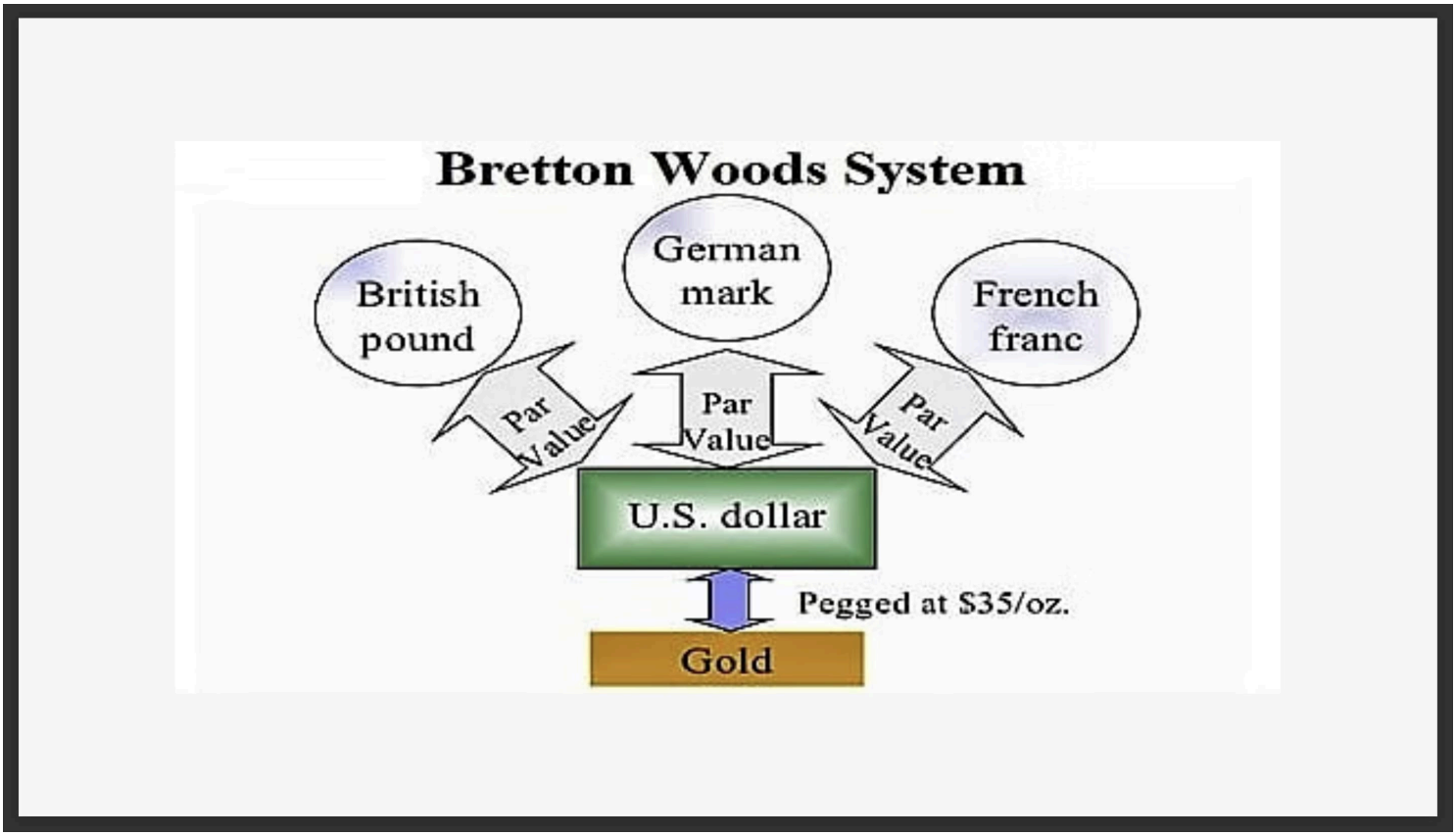
Bretton Woods Conference
June 1-22, 1944

WWII happened. Fast forward to 1944. Germany was losing. At the time of the Normandy Landing, on June 6, 1944, another very famous conference that was quietly happening but determining the world order after the war was the Bretton Woods Conference, between June 1st and 22nd, 1944. It happened in this very old and shabby hotel where the leaders of many countries came to talk about “so what are we going to do with our money after the war?” Because, in a sense, Germans started the war because there was tremendous monetary problems and the order of money. In order to prevent another war from happening - 50 million people died from WWII - let’s find a much better world order for international monetary system.

What’s interesting is in 1940, Nazi was imagining that they would win the war and they were already imagining how they would design the international monetary order. They came up with this idea of a gold backed system, which ultimately became the gold-backed system decided at the Bretton Woods Conference.

What’s also interesting is before the gold-backed system was decided, another system was considered. What’s problematic about currencies is that you have a country that is importing a lot but exporting a little, or vice versa, you have problems where the currencies are either unfair to country A or country B. So the best idea is for countries to import and export the same amounts of different goods and commodities. So the first proposal at the conference was - let’s design a system that incentivizes countries to balance their trades. If you have unbalanced trades, you would be punished by the system. But it was obviously rejected because the US had massive trade imbalance and they thought “*we won the war, so we want the system to work in*

favor for us, not against us. We don't want a international monetary order that is punishing us right out of the war."



So eventually we came to this Bretton Woods system. The idea is that gold is rare and everyone wants gold. Gold is cleraly the desire of all human beings. Let's use gold as the ultimate value denominator. Let's fixed the US dollars to one ounce of gold exchanged for 35 US dollars as a constant. And let's negotiate fixed exchange rates between the US dollar and each of the currencies of other nations. So all the rates were determined at the conference, obviously a lot of politics were involved, based on who contributed and who had stronger voices. But this was the order coming out of WWII.

Domino Theory and Vietnam War
Nov 1, 1955 – Apr 30, 1975

But what happened after WWII in ten years time was the Vietnam war. There was a dominant theory called the Domino Theory. The idea is that the US feared communism and they wanted to contain communism from spreading from the Soviet Union and China. They had to stop it from spreading across Vietnam because the Domino Theory stated that if Vietnam were to be lost to communism, it would spread through other countries eventually reaching all the other South Asian countries. So Vietnam was where the fight had to happen. But there were agreements in place that forbid Western countries from putting armies in Vietnam. So the US deployed military advisors, who didn't carry guns and were supposed to teach people how to fight their own war, sort of technically bypassing the agreement. That was in 1955.

John F. Kennedy took the oath of office
Jan 20, 1961

John F. Kennedy became the US president in 1961. The idea was that he was going to protect the liberal world order. I'm going to read a little bit from his inauguration speech when he took the office. "*Let every nation know, whether it wishes us well or ill, that we shall pay any price, bear any burden, meet any hardship, support any friend, oppose any foe, in order to assure the survival and the success of liberty.*" Which meant that the US increased spending and its involvement in Vietnam.

privilège exorbitant
Feb, 1965

Guess what, when you have to fight a war you need to spend a lot of money. But the money, which was the US dollar in this case, was pegged to the gold at a fixed rate. Substantial increase in war spending, among other spendings, led to a growing budget deficit. You have massive people that were questioning the worth of the US dollar.

In 1965, there was this idea of *privilège exorbitant*. Enormous privilege was conferred to the country whose money was the international settlement dollar, allowing them to not care about trade imbalances while all other countries had to. What happened was that French warships carrying US dollars from the French treasury were sent to New York to redeem said dollars for gold from the US government. Many countries followed suit. This caused gold to exit the US. After the WWII, the US had 70% of circulating gold worldwide. With these redemptions, the US had gone down to 40% of the global gold. And you can't have only 40% of the gold worldwide for backing the international dollar. It stopped making sense.

"All the News That's Fit to Print"

The New York Times

LATE CITY EDITIO

VOL. CXX ...No. 41,477 NEW YORK, MONDAY, AUGUST 16, 1971 15 CENT

NIXON ORDERS 90-DAY WAGE-PRICE FREEZE, ASKS TAX CUTS, NEW JOBS IN BROAD PLAN: SEVERS LINK BETWEEN DOLLAR AND GOLD

A WORLD EFFECT

Unilateral U.S. Move Means Others Face Parity Decisions

REACTION MIXED

Mansfield Pleased by Wage-Price Action—McGovern Critical

SPEAKS TO NATIO

Urges Business Aid t Bolster Economy—Budget Slashed

Iate Pursues British Troops in Ulster

Highlights of Nixon Plan

Nixon Shock
Aug 15, 1971

So with redemptions, and rampant speculative trading activities, what happened in 1971 was the Nixon Shock. *Ok, everybody cools down, and from today no one can redeem the US dollars for gold.* This severed the connection between the US dollars and the gold. Widespread controversy and panic ensued. What's the worth of the US dollar now if you can't redeem it for its underlying asset? As if it has become a game coin.

Smithsonian Agreement
Dec, 1971

Jamaica Accords
Jan, 1976

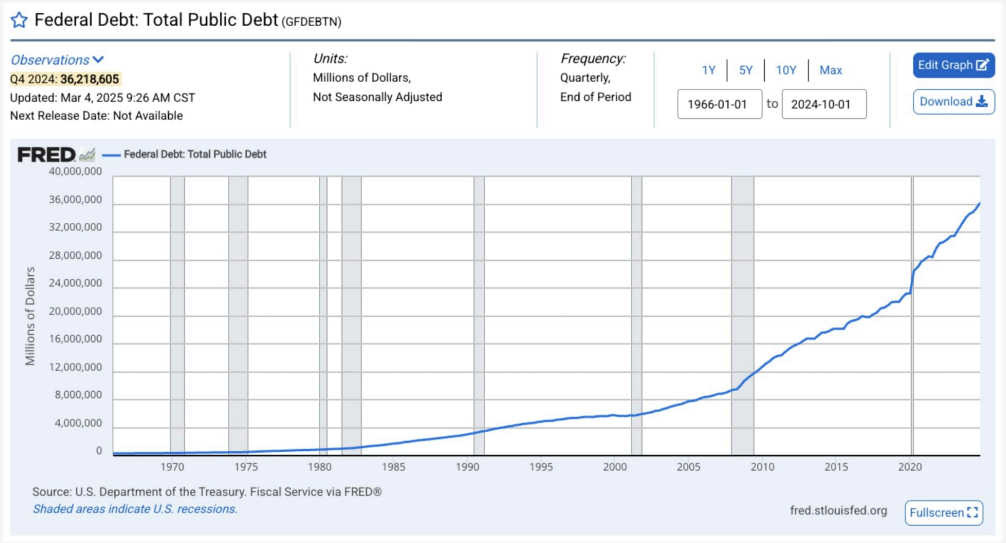
Immediately at the end of the same year was the Smithsonian Agreement. If everyone questions the worth of the US dollar, let's devalue it. It was devalued by 8.25% at the end of 1971. And other currency were renegotiated. For reasons such as the oil prices and other things, which we will cover later, in 1976 basically everyone gave up and said ok from now on, the currency rates are floating.

2011 US Debt Ceiling Crisis
April 15, 2011

2023 US Debt Ceiling Crisis
Jan 19, 2023

Fast forward to 2011. US debt ceiling. Imagine you are the US government. Congress has written into the law that says there is only so much debt you can bear at any given moment, so you want to be responsible and don't borrow too much money to stay below the ceiling. What happened in 2011, which happened many times in the past, was that the debt ceiling was reached but the government needed to borrow more money from other countries. Congress said no. So the government had to start cutting all kinds of expenses. Imagine if US cannot pay back the interests on the money they borrowed from other countries. That basically means the US government is defaulting, effectively bankrupt. And if the US government bankrupts, what does that say about the worth of the US dollar? The world is going to look very different not in a very good way. So the congress was scrambled together and lifted the debt ceiling. The ceiling then sit at $14 trillion.

In 2023 the ceiling was hit again, this time at $31 trillion. What happens when you hit the ceiling is that you stop paying your medical systems and your social programs, because you cannot afford to bankrupt, so you have to keep paying other countries to maintain your trustworthiness. But the people end up suffering, particularly the people that are underprivileged.



US national debt
1966-2024

This is a screenshot of the federal debt chart. Right now US debt stands at $36 trillion. There was an act in 2023 that froze the debt ceiling two years ago until January 2025, around the time when Trump came to office the second time. The ceiling came back. Now the ceiling has been breached already, meaning the US government is in the regime of exercising extraordinary measures - cutting down aids for poor people, cutting down social programs, including aids that go to Vietnamese families who suffered from the Vietnam war.

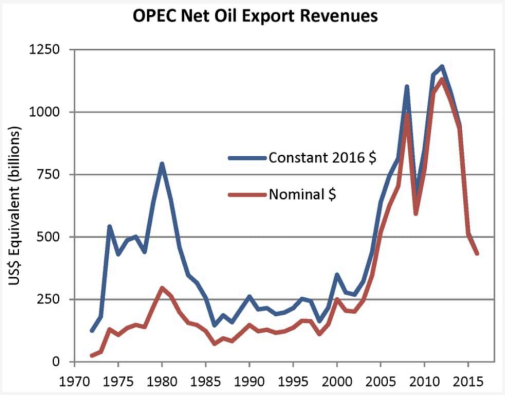
Petrodollar

We are switching to the topic of the petrodollar. No more gold backing the dollar. What then is the worth of the dollar?

“The Concept” and Yom Kippur War
Oct 6-25, 1973

The Yom Kippur War occurred in 1973 on Yom Kippur, the holiest day for the Jewish people. For context, Israel’s intelligence and military leadership had held on to “The Concept” since Israel won the Six-Day War in 1967. The idea of The Concept is that (1) Egypt would not start a war with Israel until their air force recovers (Egypt lost nearly half of its air force on the first day of the Six-Day War) (2) Syria would not start a war with Israel unless Egypt attacks as well. The Concept turned out to be incorrect. Egypt and Syria coordinated a successful surprise attack on October 6, 1973. Israel lost around 1300 soldiers in the first 3 days.

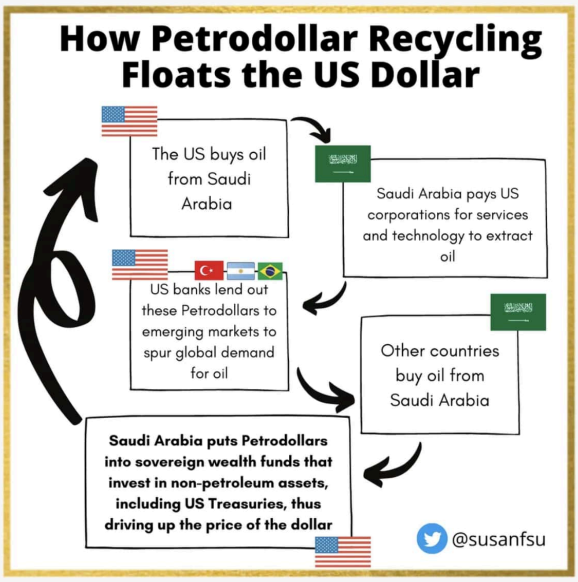
Eventually a ceasefire was mediated by the United Nation. Then president of Egypt - Anwar el-Sadat - and prime minister of Israel - Menachem Begin - received the Nobel Peace Prize in 1978 for their efforts to create peace between their countries.



Oil Crisis
1970s

The oil-producing Arab countries (OAPEC) did not recognize the sovereignty of Israel (most of them today still don't). In 1973, they protested against the countries that supported Israel during the Yom Kippur War by stopping the oil shipping to these countries, including the US, UK, Canada and Japan.

The US was importing 70% of its oil from the OAPEC. The oil embargo had a great impact. In 1974 oil price surged as much as 400%, from $3 a barrel to nearly $12. Cars sit idle at gas stations because there were no gas. Odd-even rationing were practiced.



Petrodollar recycling

Eventually the embargo ended. However oil prices did not return to their pre-crisis levels. Wealth transfer, denominated in US dollars, continued from oil-importing nations to the oil exporters. Yet agreements were formed to create, in theory, the so called “petrodollar recycling” system.

The idea of petrodollar recycling is that Saudi Arabia would price their oil in US dollars, take the US dollars it earns through oil export and reinvest them US financial assets, primarily by buying US bonds and equipments for oil excavation. In return, the US offers military support. This created a sustained global demand for the US dollars and reinforced its status as the world’s reserve currency.


Iraq War
Mar 20, 2003 - Dec 15, 2011

To reinforce the idea of the petrodollar system. In 2000, the president of Iraq, Saddam Hussein, unilaterally announced that their oil export would be denominated in euros, not US dollars.

Perhaps no one could really draw the causality between this dollar-severing act and the Iraq War that ensued in 2003. Official reasoning for the War was Iraq's alleged possession of weapons of mass destruction, which was never found. After the war, the US took over the oil producing facilities in Iraq, and Iraq's oil export returned to the US dollar for pricing and settlement.

We can see how national interests are deeply entangled in the world of currencies, which the wellbeing of many are relied upon.

Ideology vs realism

This brings us to the topic of ideology vs realism, in the context of geopolitics.

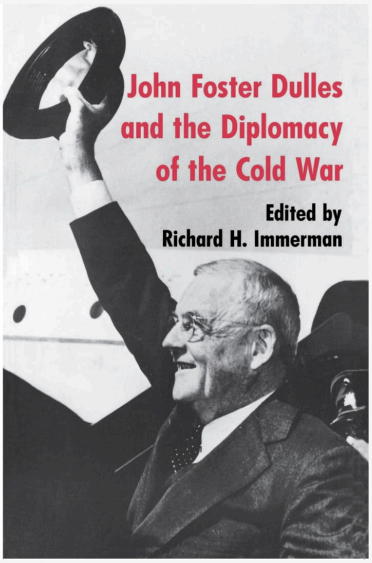
Tiananmen Square protests and massacre (天安門事件)
June 4, 1989

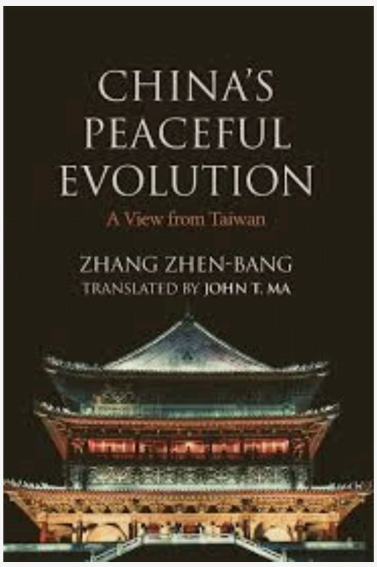
The Tiananmen Square protests and massacre transpired on June 4, 1989. Around 100,000 soldiers and 200 tanks rolled into Beijing. Estimated 3000 civilians dead.

Officially the root cause was that there were students, manipulated by the West, protesting for democracy and the rejection of the Chinese Communist Party (CCP).

double track price system(價格雙軌制)、price reform(價格闖關)
1980s

What happened was that the cultural revolution ended. There were plans to transition from the planned economy to the market eocnomy. In a planned economy, prices are dictated. In a market economy, prices are driven by the supply and demand in the markets. You can imagine in the planned economy post-revolution, productivity was destroyed, commodity prices were dictated to be artificially low while the demand for these commidities was overwhelmingly strong. The transition into the market economy, if done without control, would be pretty violent. So there was a policy in place called the double-track price system (價格雙軌制). For each commodity, there would be a quota. Below this quota the price is dictated, in the planned regime. Above the quota the price is market price. Arbitrages opportunities were exploited by people with relationships with the government officials (官倒). They would buy at low planned prices and sell back to the public at high market prices. A major company co-crreated by the eldest son of Deng Xiaoping was involved (中國康華發展總公司). People were angry and the double-track price system was cracking. In 1988, a price reform was in the planning, where in a short period of time the planned commodity prices were to be forcefully raised to market prices on a schedule (價格闖關). Tragically, the idea of the policy reform leaked before it was implemented. People expected everything would become much more expensive very soon, so they withdrew money from the banks and began panick-buying. Banks were going bankrupt from the mass withdrawals. The price reform was never implemented. Public discontent from these events all contributed to the 1989 protests.





Peaceful Evolution theory
1957

There is a long-standing ideology that all human beings ultimately desire and pursue the "Western" values: liberty, democracy, enlightenment and so on. All human beings eventually trend towards those values. After WWII, the US practiced the policy of containing China just like how the Soviet Union was contained. The strategy was based on the idea of *peaceful evolution*: due to the universal desirability of the Western values, eventually, the Chinese people would peacecfully demand democracy for China.

In 1989, the CCP condemned the US for conspiring the idea of peaceful evolution by infiltrating Chinese campuses and brainwashing the students with dangerous Western ideas.

Fukuyama's End of History essay
Summer 1989

Fall of the Berlin Wall
Nov 9, 1989

In merely two years after, a really strange essay, from today's standpoint, was published in *The National Interest*. Titled "The End of History?", author Francis Fukuyama argued that the history is ending. With the cold war concluding, the days of great ideological struggles and big wars were over forever. Romantic and ambitious people must find new pursuits. The liberal democracy has won. Moreoever there is this idea that in the world there are developed countries and developing countries. The primary goal for the developing countries is to educate their people and raise their economic standards so that they graduate to the club of developed countries, where they embrace the values of liberal democracy.

The essay came out and was not well received, but at the end of the same year the Berlin Wall fell. The essay was propelled to stratosphere.

Global Financial Crisis
Jan 3, 2009

But is it really so? Has the history really ended then? With the wisdom of the hindsight, we know that the global financial crisis (GFC) happened in 2009. What happened was that credit expanded, there were lots of money slushing around seeking returns and finding their way to real estates. The housing bubble formed and bursted. Multiple rounds of quantative easings - the minting of new US dollars into the Federal Reserve - were initiated to buy up the bad debts.

David Graeber, author of *Debt: The First 5000 Years*, argued that despite the US being a democracy, the financial elite of 1% wield disproportionate power in policy-making at the expense of the other 99%. The aftermath of GFC demonstrated a form of injustice where the large banks were relieved but the many bankrupted and unemployed people were left to their own devices. Graeber later became a significant figure in the Occupy Wall Street movement.

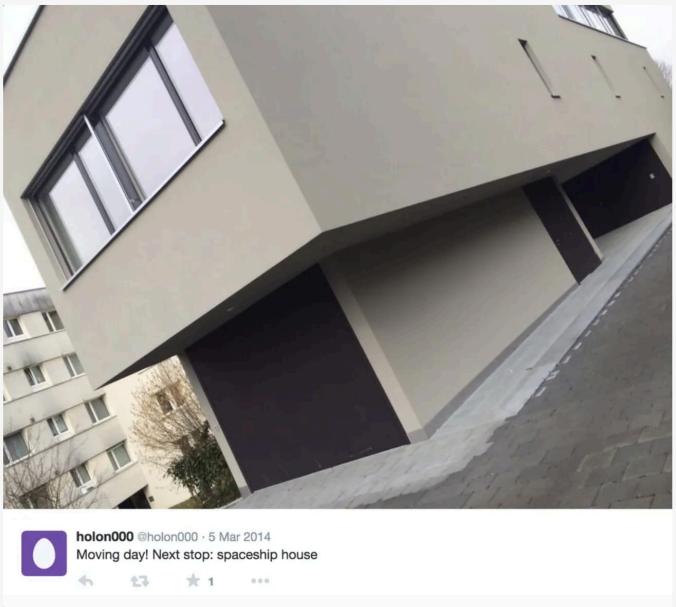
Global consensus argmin geopolitics

So we have seen many examples. When some people owe some other people money and (geo)political interests are involved, lots of people end up getting hurt badly in one way or another.

Which bears the question: can we design a global system where the influence of (geo)politics is minimized? In this system, we want no ambiguity as to what exactly has happened. It would

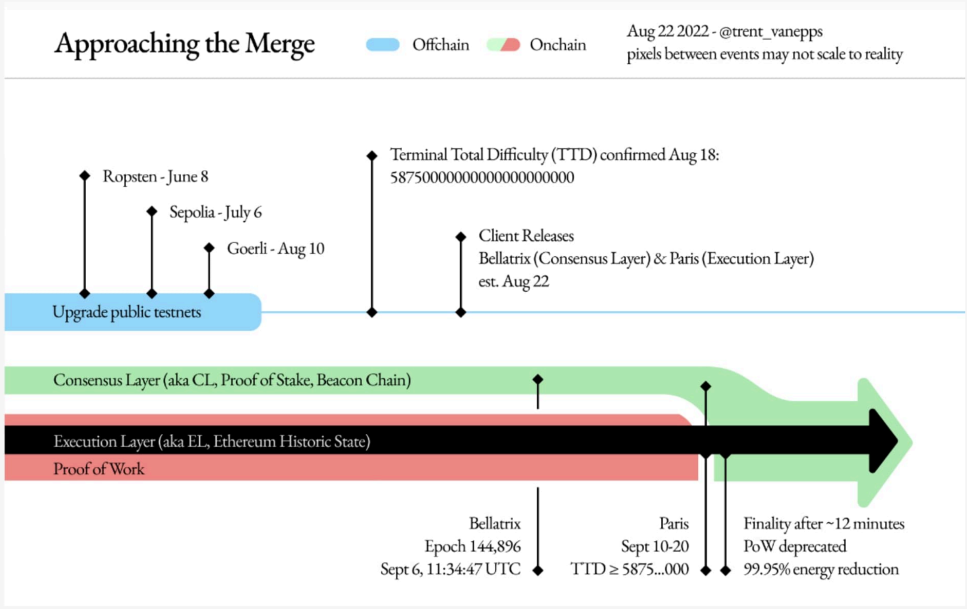
operate as the global, canonical book of truths. Its access would be open to all without discremination. Its correctness endures even when facing the strong-arming of entites as powerful as nation states.

Let’s talk about Ethereum.



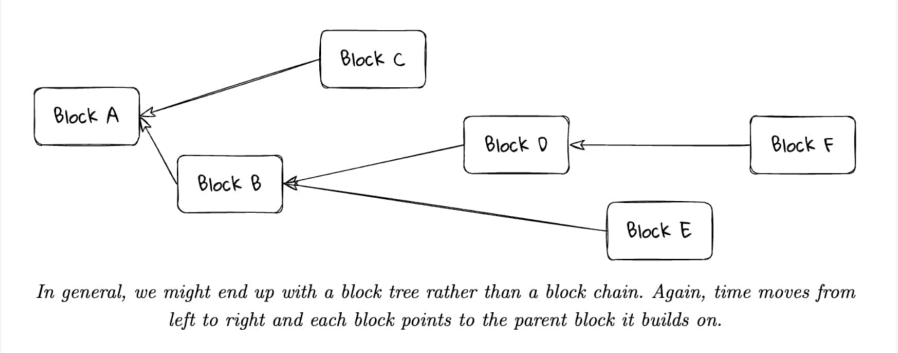
Ethereum “Spaceship” in Zug
2014

In 2014, the founders of Ethereum were living in a house in Zug, nicknamed “Spaceship”. It’s where the early codes were written and the vision was debated.



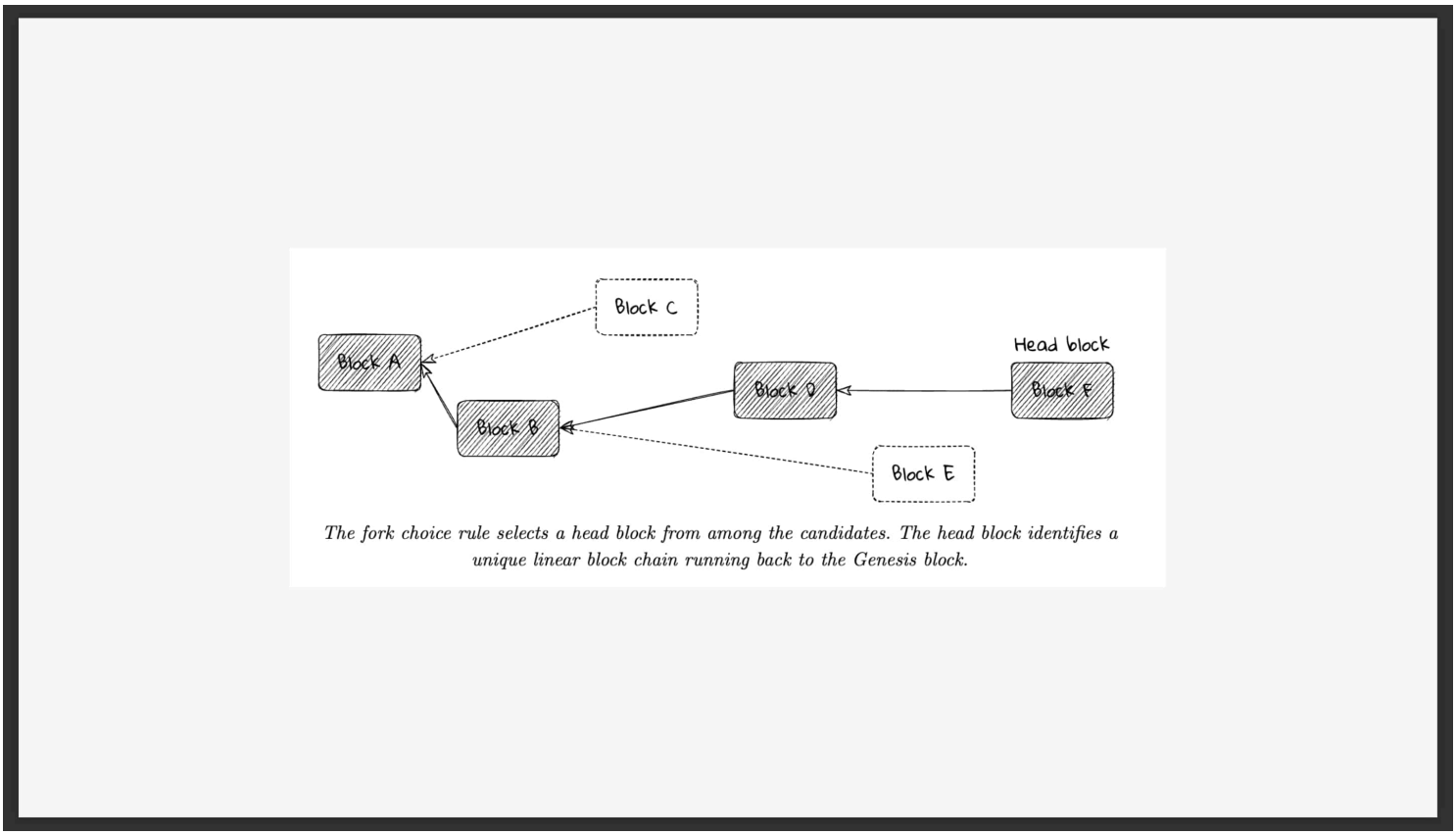
Ethereum Merge
Sep 15, 2022

In 2022, the merge happened. The Ethereum codebase was modularized into consensus and execution client. At the merge proof-of-stake consensus clients replaced their proof-of-work predecessors.



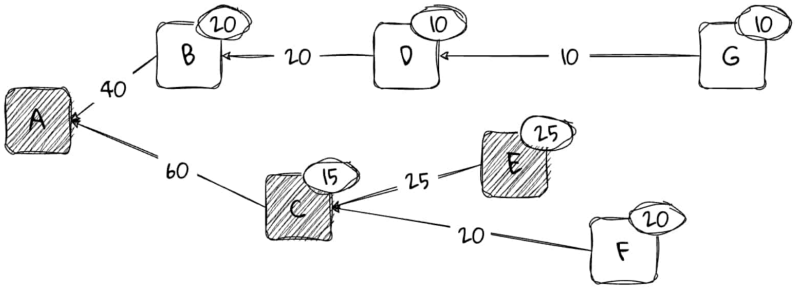
In general, we might end up with a block tree rather than a block chain. Again, time moves from left to right and each block points to the parent block it builds on.

Nowadays, how Ethereum works is that we have the users of Ethereum submitting transactions, with no single entity possessing the globally complete bird's eye view. It's a distributed system. So the transaction log naturally looks like a tree, because the different copies of the chain would be looking at different views, and they append new blocks to their frontier (head). As these copies merge, you get a tree. But we want a blockchain, not block-tree. We want a canonical sequence of events that is agreed upon globally. How do you get that?



The fork choice rule selects a head block from among the candidates. The head block identifies a unique linear block chain running back to the Genesis block.

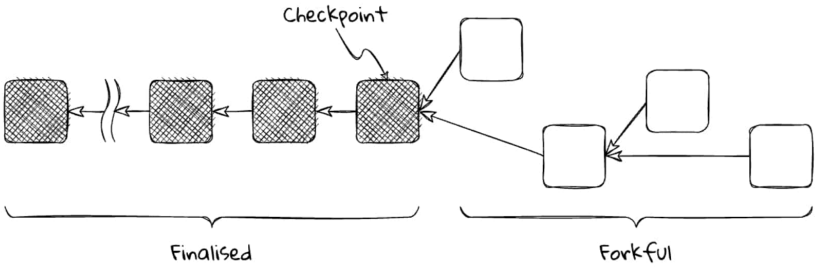
You find a linear path among the nodes of the tree, originating from its root. The algorithm to find that path given a tree is the called the fork choice rule. The outcome is you get a sequence of blocks and that's your canonical sequence. Every (full) node of your blockchain runs this algorithm.



At block A, branch C is heavier. At C, branch E is heavier. Block E is a leaf block, so it is GHOST's choice for the head of the chain. Our blockchain is $[A \leftarrow C \leftarrow E]$. A "longest chain" rule would have chosen block G, although that branch has minority support from validators.

Ethereum's fork choice rule works by the validator nodes "voting" (attesting) for blocks they saw on the network, propagated to them by their peers. The power of their vote depends on how much ETH the validator has staked into the system, so that there's something at stake. Tallying the votes give you a score per block. The linear path is found based on these scores.

Ethereum's fork choice rule is called the LMD-GHOST.



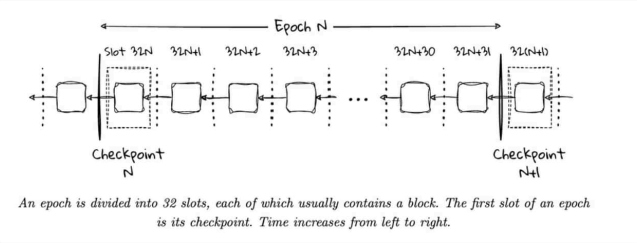
The honest nodes have agreed that the checkpoint and all its ancestor blocks are "final" and will never be reverted. There are therefore no forks before the checkpoint. The chain descending from the checkpoint remains liable to forking.

We have covered how the fork choice rule works to find a linear sequence of blocks. What Ethereum also does is it can finalize this path. Unlike Bitcoin, which strictly speaking does not really finalize things. So in Bitcoin or Bitcoin-like systems, you can have drastic shift from a linear path to another linear path because some minders were mining many blocks in secret with superior hash power. This is undesirable, because the users don't have the strict guarantee that what's onchain will stay there forever. It's a problem of probability. That's why Bitcoin recommends a 12-block waiting time.

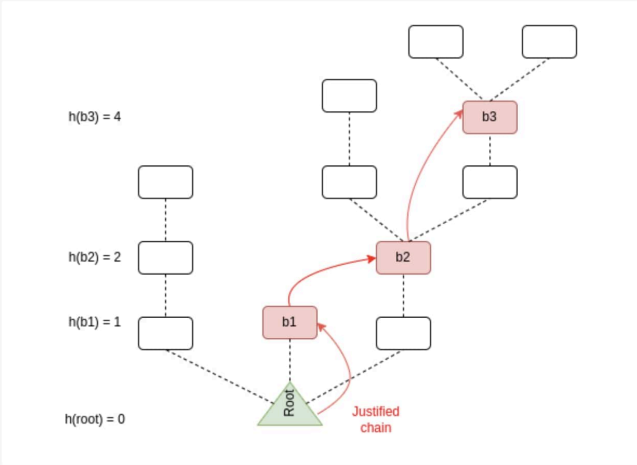
The post-merge Ethereum provides finality. What's finalized is final, they will never change, based on the underlying cryptoeconomic guarantees. Ethereum uses an approach that essentially is just a variation of the two-phase commitment.

Ethereum's finality algorithm is called the Casper FFG. So Ethereum has LMD-GHOST* looking at the tree and picking the linear path up front, like the explorative tendrils of a starfish, and Casper FFG following closely behind to produce the finalized, ossified path.

*LMD-GHOST has to be modified to work with Casper FFG, so that instead of finding a path that originates from the tree root (genesis block), it originates from the latest finalized block by Casper FFG.

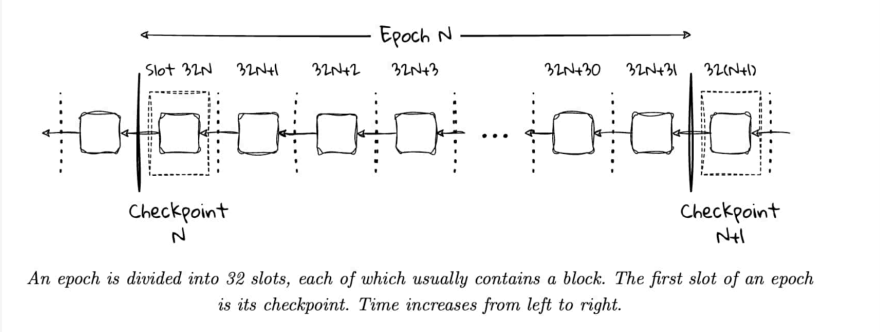


An epoch is divided into 32 slots, each of which usually contains a block. The first slot of an epoch is its checkpoint. Time increases from left to right.



The temporal structure of the Ethereum blockchain consists of slots and epochs. A slot is the basic unit of time, where a single block happens. 32 consecutive slots form a single epoch.

If a supermajority of validators attested to a block, that block becomes “justified”. If I, as a block, have a child block that is justified, I become double-justified which simply means I become finalized.



An epoch is divided into 32 slots, each of which usually contains a block. The first slot of an epoch is its checkpoint. Time increases from left to right.

- ETH total staking at September 2022 (the merge): ~14M
- Minimal staking requirement: 32 ETH
- Supermajority: 2/3
- # of BLS signatures per second verified by **consumer laptop**: ~800
- # of slots per epoch: 32

=> 14M ÷ 32 × ⅔ ÷ 800 ÷ 32 ~= 11.4 seconds

Slot time set to 12 seconds.

I want to specifically point out that the choice of these numbers is not arbitrary.

Ethereum's slot time is set to 12 seconds. Why chose 12? We can through an estimation:

- Back in September 2022, the total amount of staked ETH was about 14 million.
- A validator must stakes minimum 32 ETH to qualify. So the maximum amount of validators is 14M/32.
- Supermajority is two thirds. So a block needs to get 14M/32*2/3 (~291600) attestations to become justified.
- For home stakers, they must stay caught up to the tip of the blockchain. This means a consumer laptop needs to be able to verify the attestations of a justified block within one slot time. To verify an attestation largely means to verify a BLS signature attached to it. So a home staker needs to verify 291600 BLS signatures per slot time.
- How many BLS signatures can a consumer laptop verify in a second? About 1000, according to my benchmark in Go. Let's give it a 20% margin. So 800 per second. This means a consumer laptop can work with a 14M/32*2/3/800 (~365 seconds) slot time.
- However, a 365-second slot time is not very useable. One must wait about 6 minutes of a spinning circle for just the earliest sign of transaction confirmation. So Ethereum divides up the validators into 32 groups, and distributes the attestation job across 32 slots, one group per slot. The amount of signatures to be verified per slot becomes 14M/32*2/3/32 ~ 9110. The slot time acceptable by home stakers become 9110/800 ~ 11.4 seconds, which gets us very close to 12.

The keyword here is “consumer laptop”. Ethereum wants consumer laptops to be able to participate directly in its consensus process. I think one part of the motivation is that Ethereum wishes to minimize geopolitical influence in its system. So it wants the little guys to be able to participate directly.

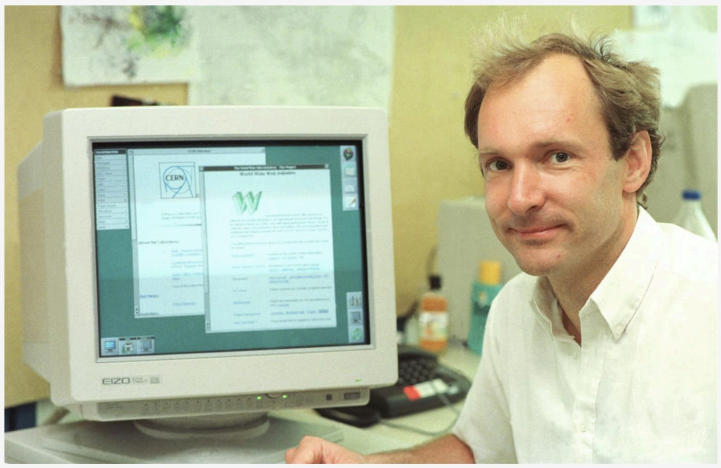
If you have a system that requires the big guys to work, you are tying your system correctness to the relatively affluent participants, whose population is very unevenly distributed in the world. In short, you would not be minimizing geopolitcal influence in your system then.

I think these design choices really illuminate what Ethereum is designed for.

Coordination avoidance

I want to move on to the topic of coordination avoidance.

At first glance it might sound very strange. After all, global consensus is all about coordination, right? We are in a network, you tell me what you’ve seen, I tell you what I’ve seen, and let’s cryptographically signed on things to find agreement. So why avoiding coordination?



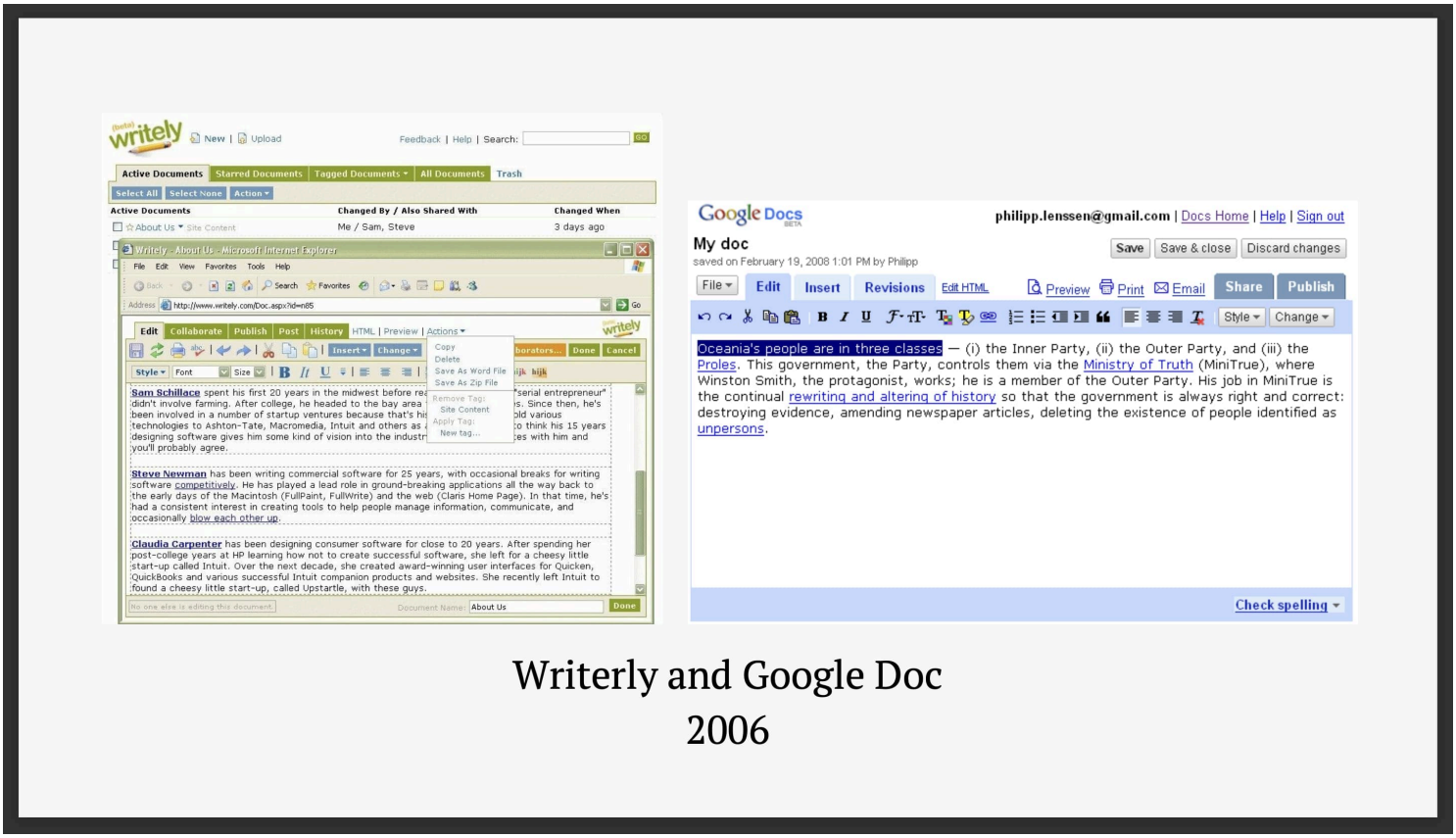
Birth of the Web
1989

I want to go back to 1989. This is Tim Berners-Lee, who invented the World Wide Web at CERN.

The idea of the Web was not just a read-only Web. In the 90s, a bunch of people were running blogs and static sites. The Web was effectively a big catalog of static information, you can publish things and people read them. Most people were reading them, few were writing.

The original browser written by Tim Berners-Lee actually wanted to have a feature where people could edit HTML documents within the the browser and publish their changes to the sites. The Web actually wanted to be read-and-write kind of system.

But it was difficult, because what happens when two people want to write to the same site at the same time? Whose changes are accepted? This was not a trivial problem.

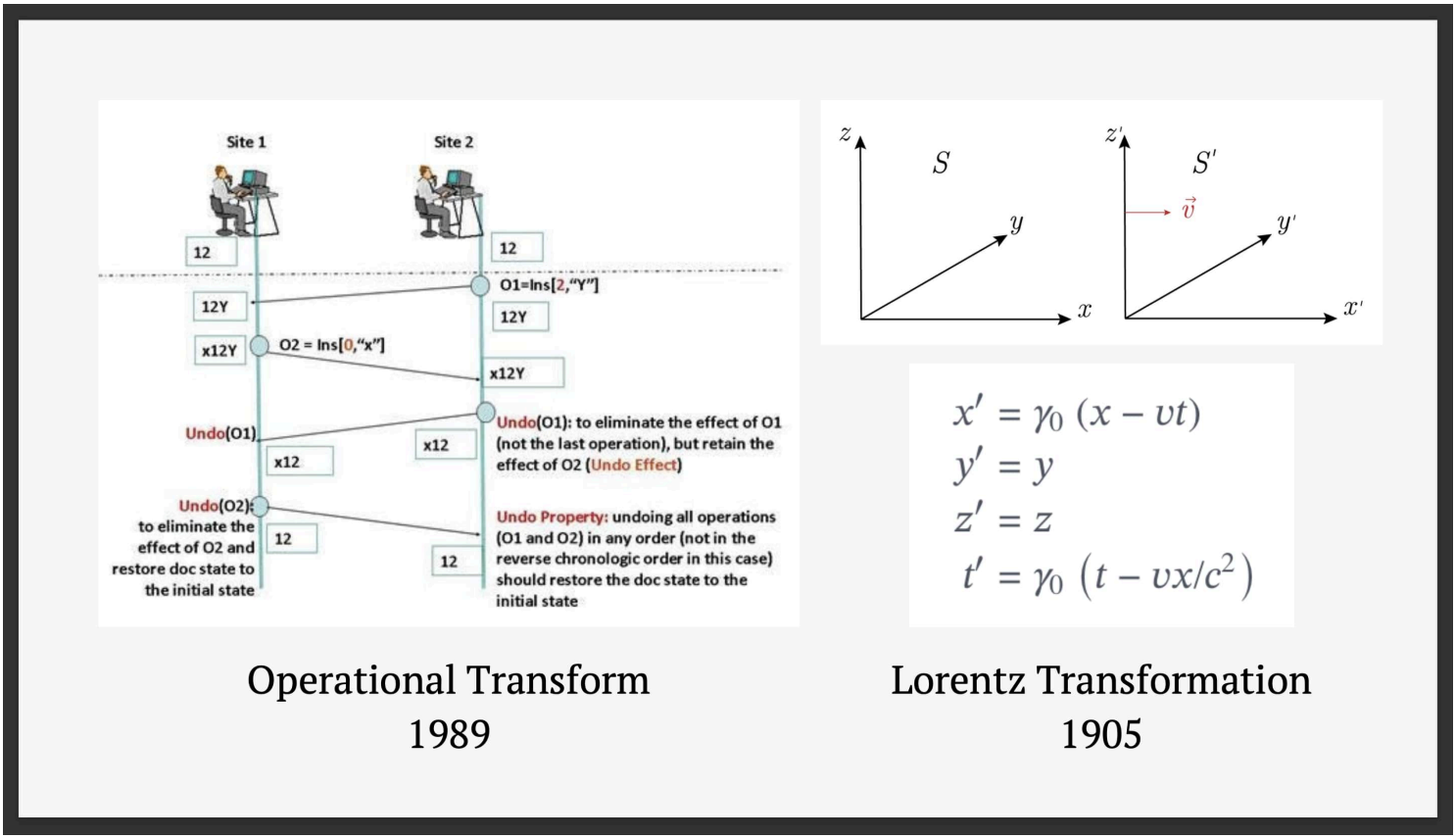


Writerly and Google Doc
2006

In 2006, a company called Writerly, which basically created a collaborative document editing application on the Web, was acquired by Google. The same year Google acquired Youtube, so the Writerly acquisition was paid much less attention.

It later culminated in the Google Doc product. What is Google Doc? It is a collaborative document right? You can see each other's cursor in the document and type at the same time, mutating the same document. The important thing here is the document must somehow guarantee that everyone is seeing the same thing. Because if two editors of the same doc are seeing different versions, Google Doc effectively stops working, and they might as well be editing different documents, or forks.

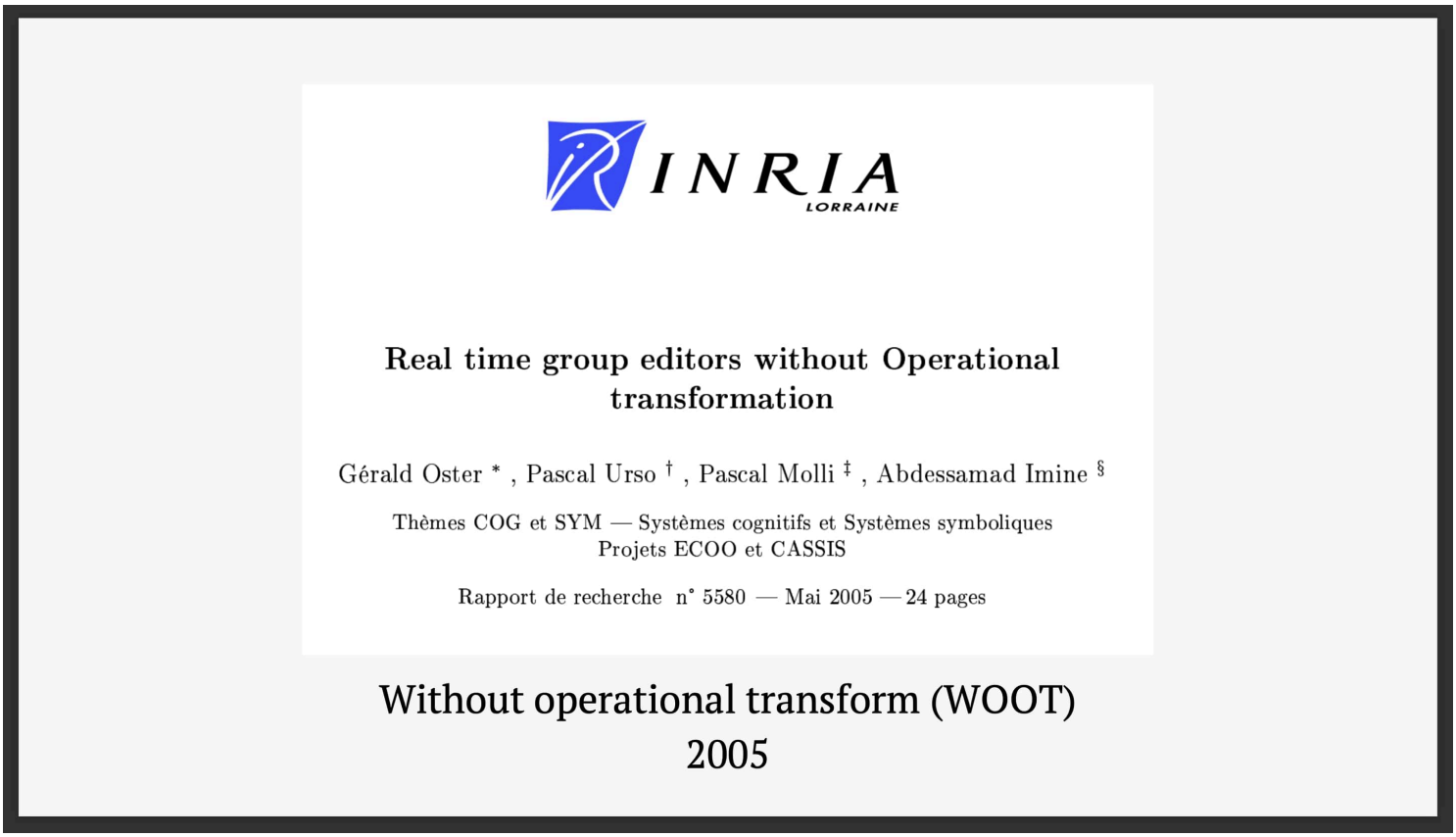
So this consistency problem is very important.



It used a technology that was rooted back in 1989 called *operational transformation* (OT).

It works like this. If I do something to this piece of data and tell you about it, you need to transform it first in a specific way before applying it to your copy of the data.

Interesing side note. There's something called the Lorentz Transform in modern physics. You have multiple frames of references observing the same physical phenomena. Physical observables have to be transformed to preserve the physical laws across these frames of references. So abstractly you can say that something similar is involved in operational transformation.



INRIA
LORRAINE

Real time group editors without Operational transformation

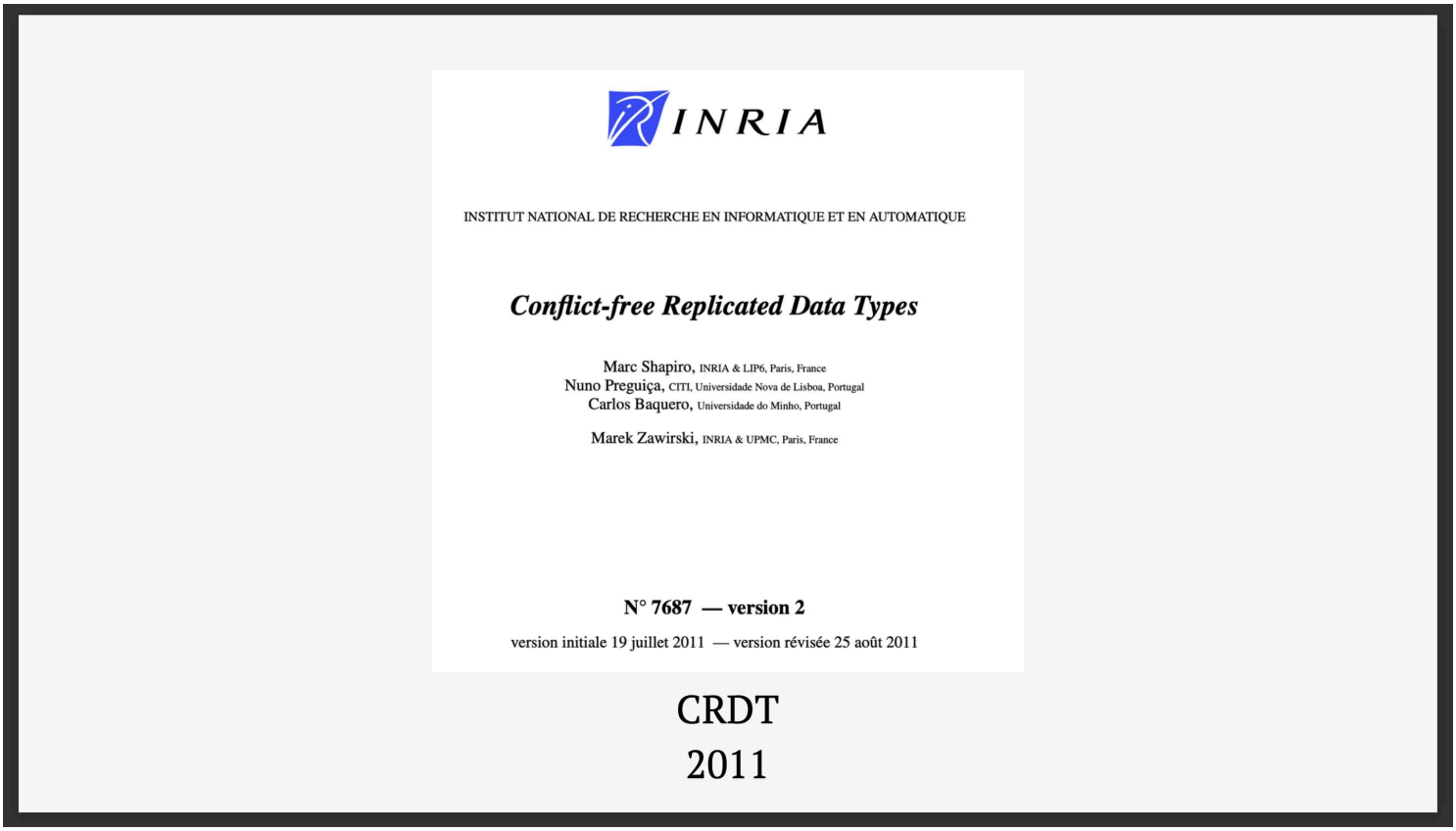
Gérald Oster * , Pascal Urso † , Pascal Molli ‡ , Abdessamad Imine §

Thèmes COG et SYM — Systèmes cognitifs et Systèmes symboliques
Projets ECOO et CASSIS

Rapport de recherche n° 5580 — Mai 2005 — 24 pages

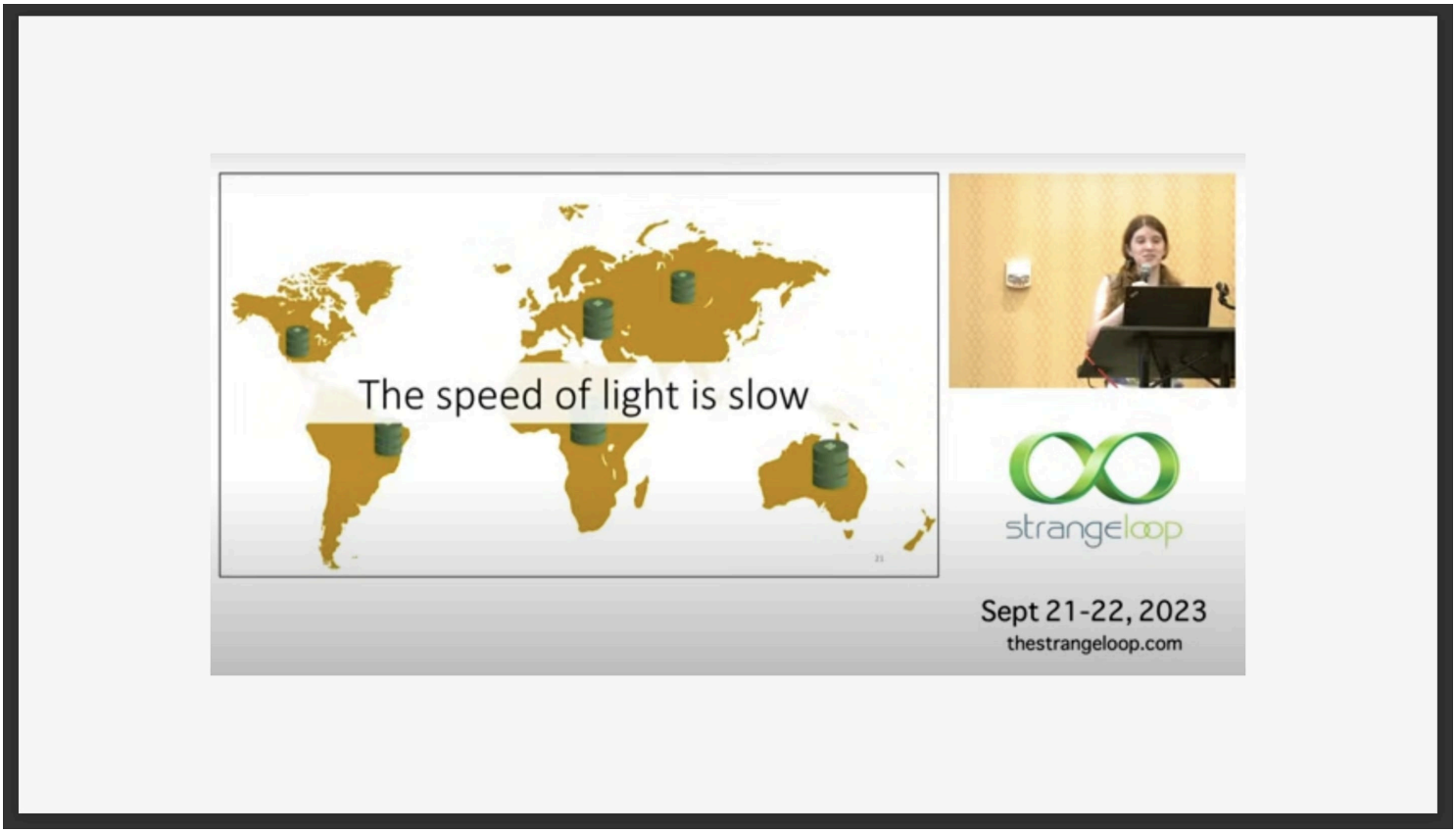
Without operational transform (WOOT)
2005

In 2005, papers started to be published that were titled “without operational transformation”. The idea is that OT has been great, but we want to do more. We want to make rich text concurrently editable, and generally perform operations that are more complex than character insertions and deletions.



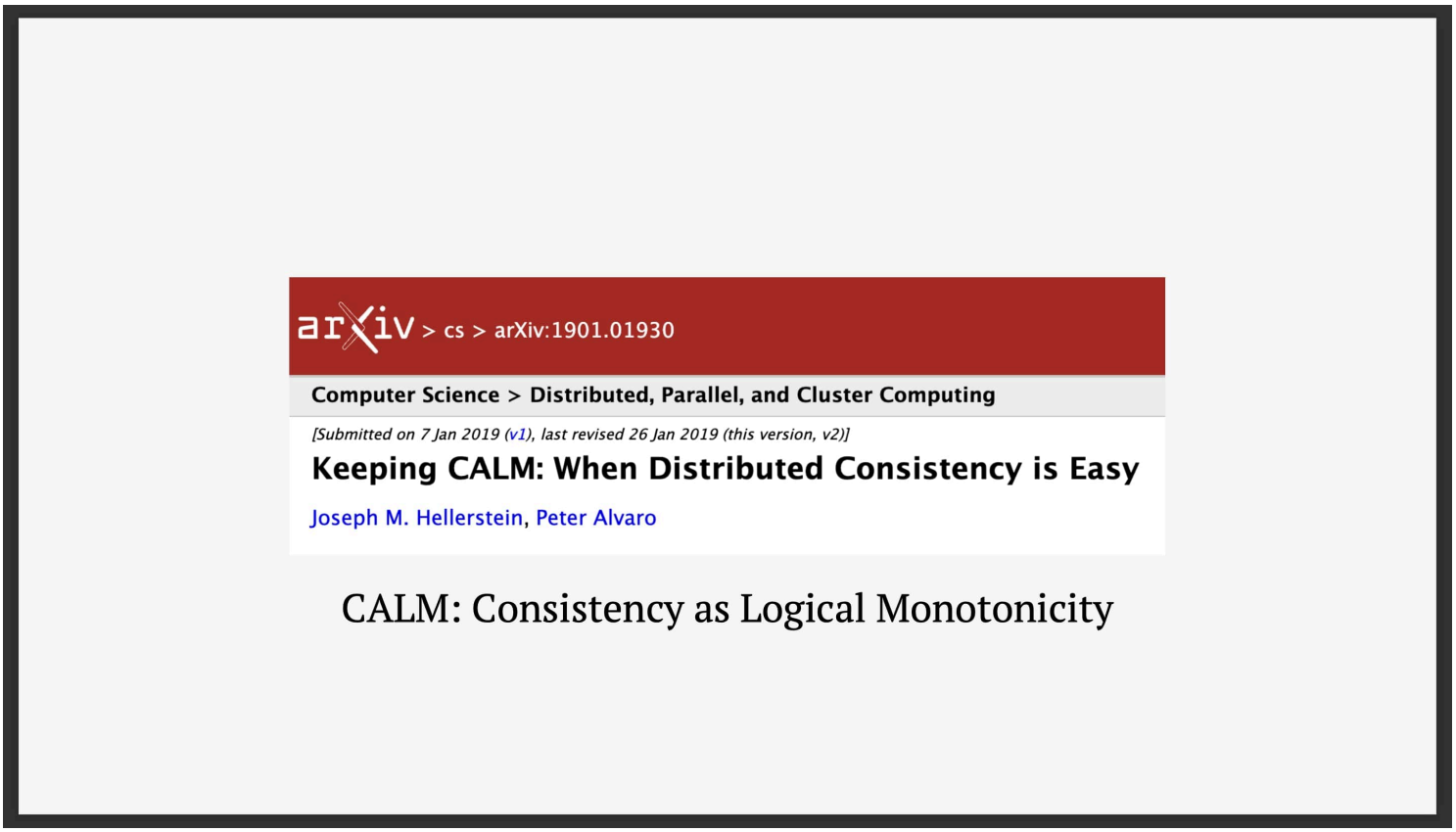
How do we do that? Eventually the research efforts converged to the technique of CRDT, which stands for Conflict-free Replicated Data Type. It's a data type that is replicated into many many copies, and all these copies are always mergeable with one another and you always get the same result regardless of the merging order. That means you don't have to coordinate.The system of copies become consistent merely by information exchanges.

There's idempotency and commutativty in this kind of system.



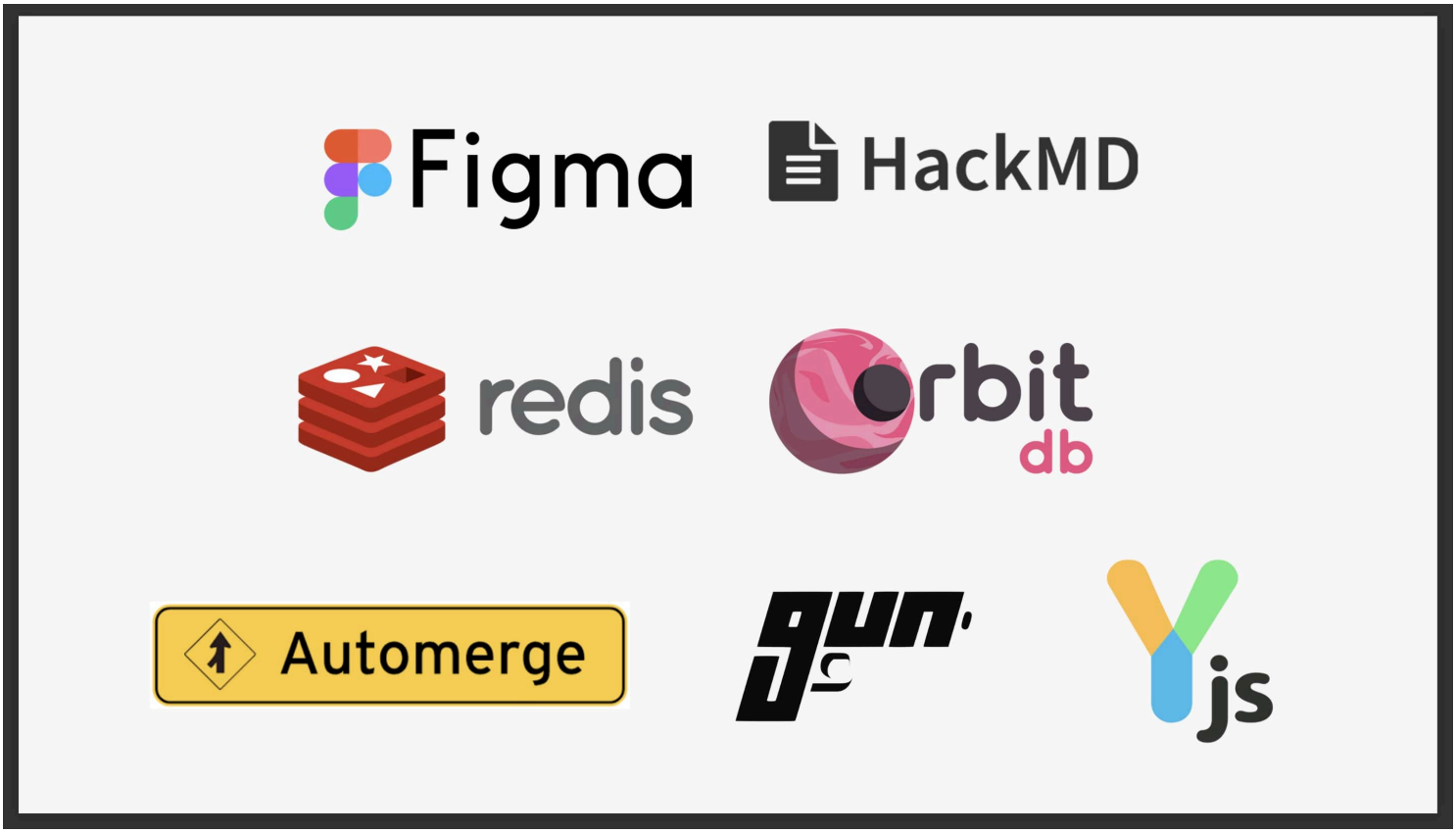
Sort of the ultimate limitation of all distributed systems (geo-distributed ones) is that the speed of light is not fast enough (with respect to how fast different actors are introducing changes in different parts of the system).

It takes about 130ms for light to travel half way around the world. So if you have different people at different places on the planet, changing their copies of the same piece of data at a period that's smaller than 130ms, they start seeing different views. You have to reconcile that. The speed of light is a physical limitation that we cannot yet surpass.



The idea of why CRDT works is sort of formalized in this paper about the CALM theorem. CALM stands for Consistency as Logical Monotonicity.

The idea is that if your application only grows in size, meaning it only adds information, never destroy information (which also mean the application runs on monotonic logic), your application is safe under concurrent operations. That's the CALM theorem.

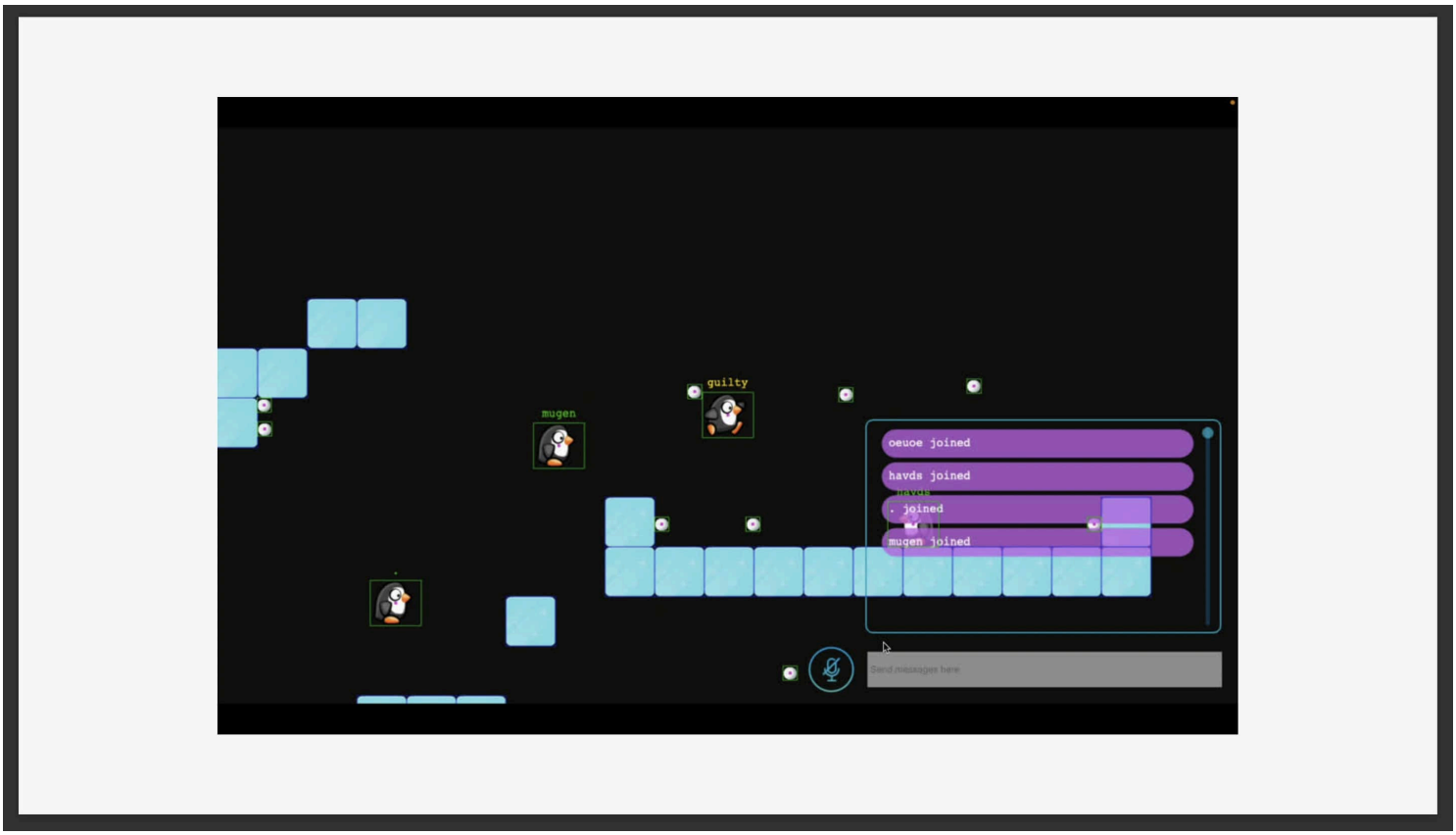


CRDT is in the wild.

Figma uses a CRDT-like approach for its multiplayer feature. HackMD originally used OT and now also uses CRDT.

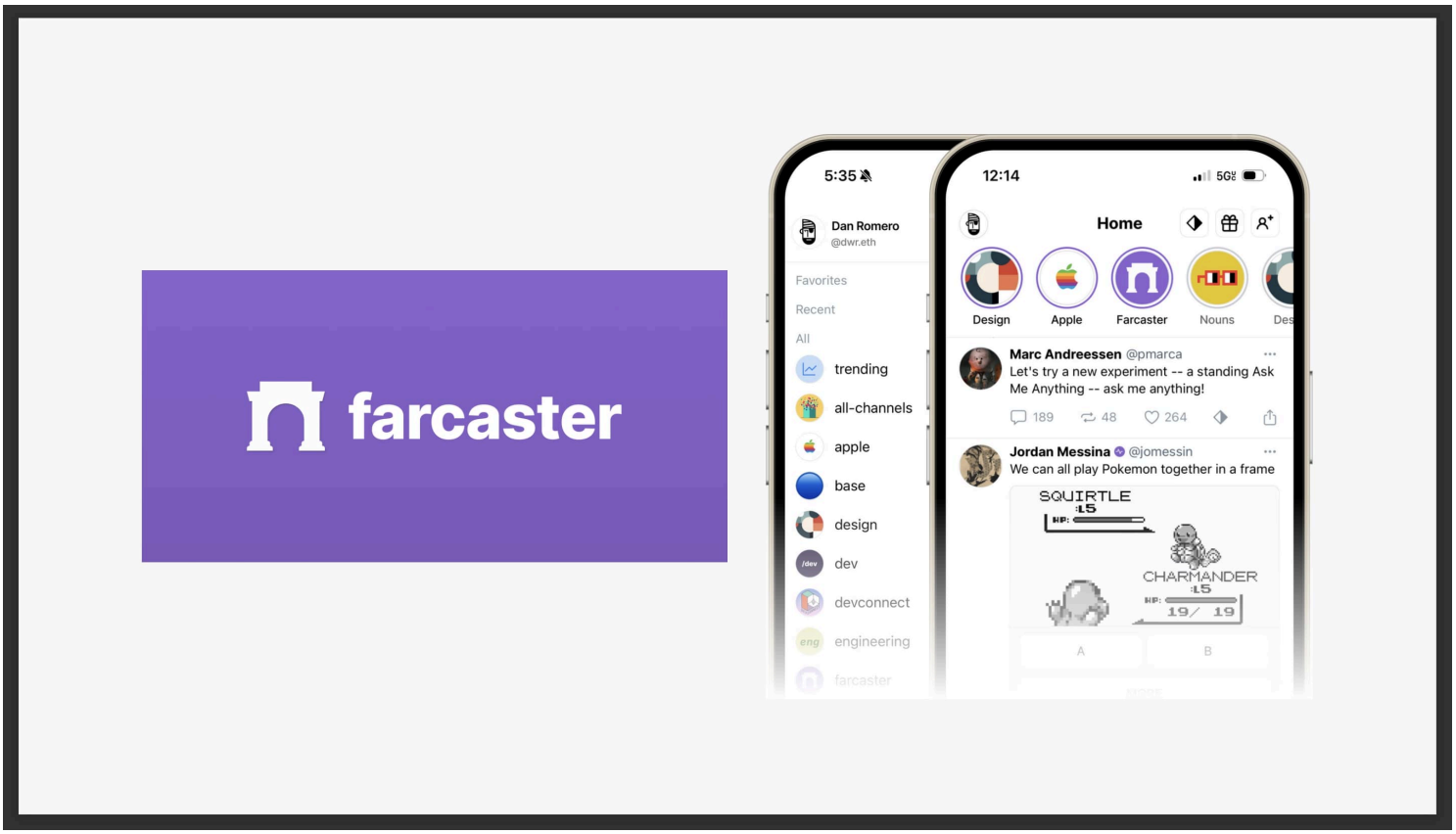
Redis offers a geo-distributed large scale database service that uses CRDT to reconcile changes. OrbitDB is an open-source CRDT database built on libp2p, a p2p networking stack from Protocol Labs, the company behind IPFS and Filecoin.

On the bottom of the slide these are open source libraries for you to build Web apps using CRDT. Automerge, Gun js, and Yjs, an approach that was also implemented in Python (Ypy) and Rust (Yrs). There are more.

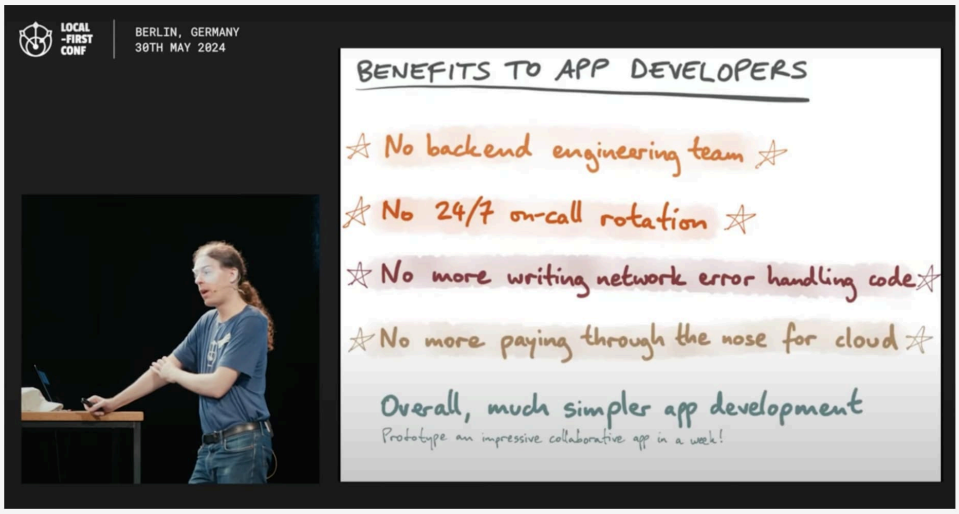


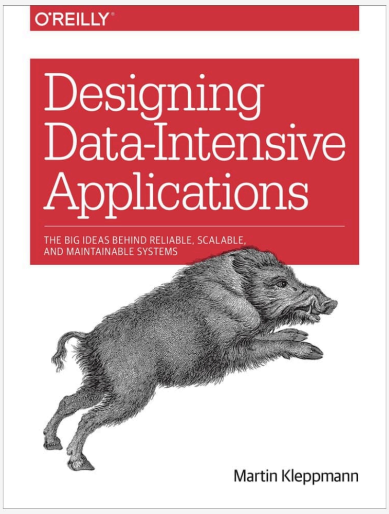
So we decided to test how well this works. This was done by Topology two years ago. We thought, ok CRDTs allow documents t be edited concurrently, but what about game states? Make a mental jump from document state to game state.

This game prototype was running at 30 frames per second, built on Yjs on top of WebRTC as network transport. Each penguin was controlled by a team member of Topology from their laptop. Laptops were connected in a p2p mesh by WebRTC.



In terms of commercialization in Web3, Farcaster famously originated as a social network built on CRDT.





Local-First Conf in Berlin 2024

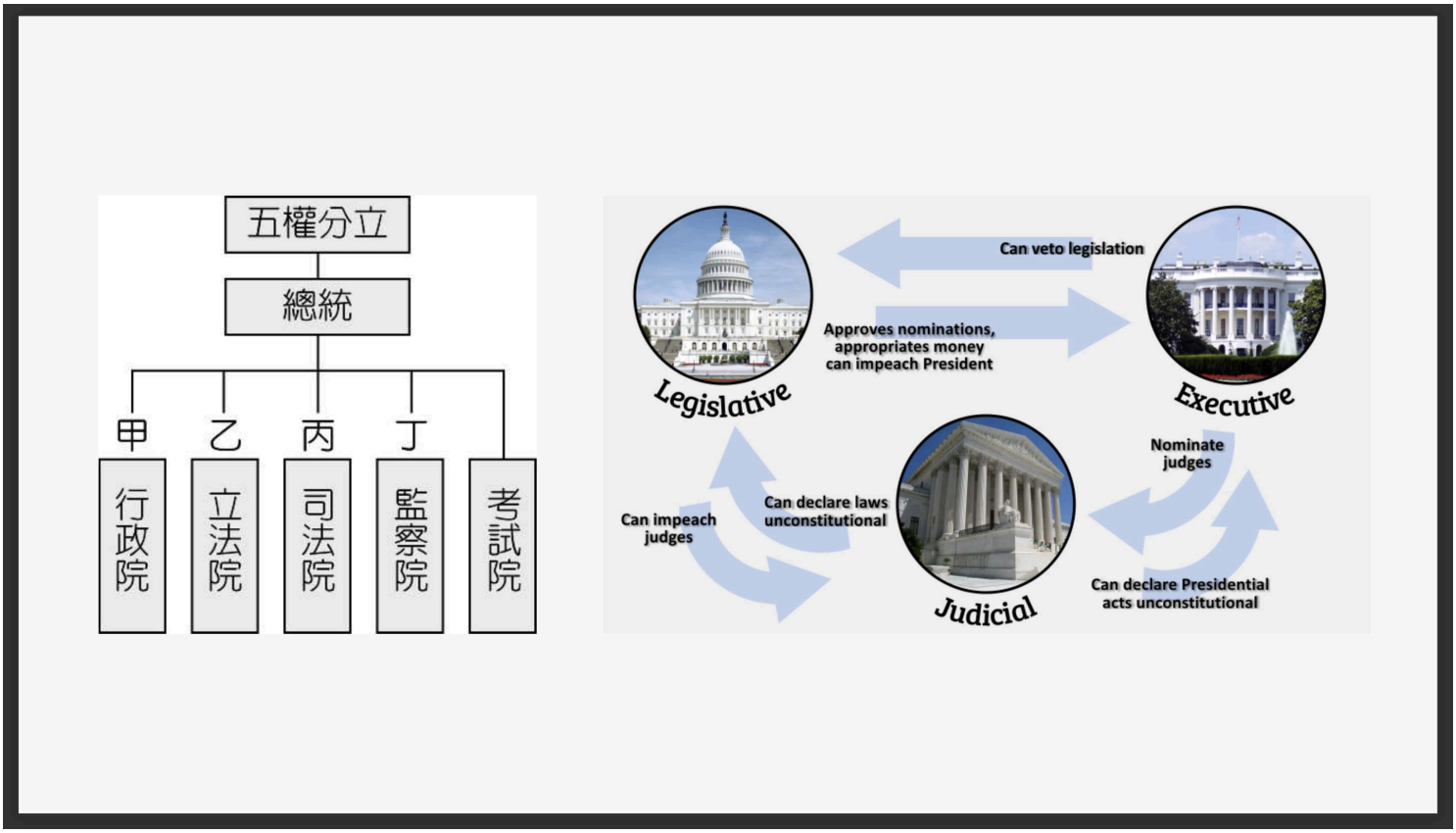
I want to bring this up to wrap up this section. Local-first conference happened last May in Berlin, also happening this year.

Local-first is the idea that we should be able to use our cloud applications despite being disconnected from the cloud. It may sound weird. But for example today if I use ChatGPT, I prompt the AI and switch off my Internet connection and switch it back on, I won't get the AI response. I have to reset the session and prompt again. In local-first paradigm, if I disconnect and reconnect to the cloud, I re-sync and find out the AI has been working without interruption.

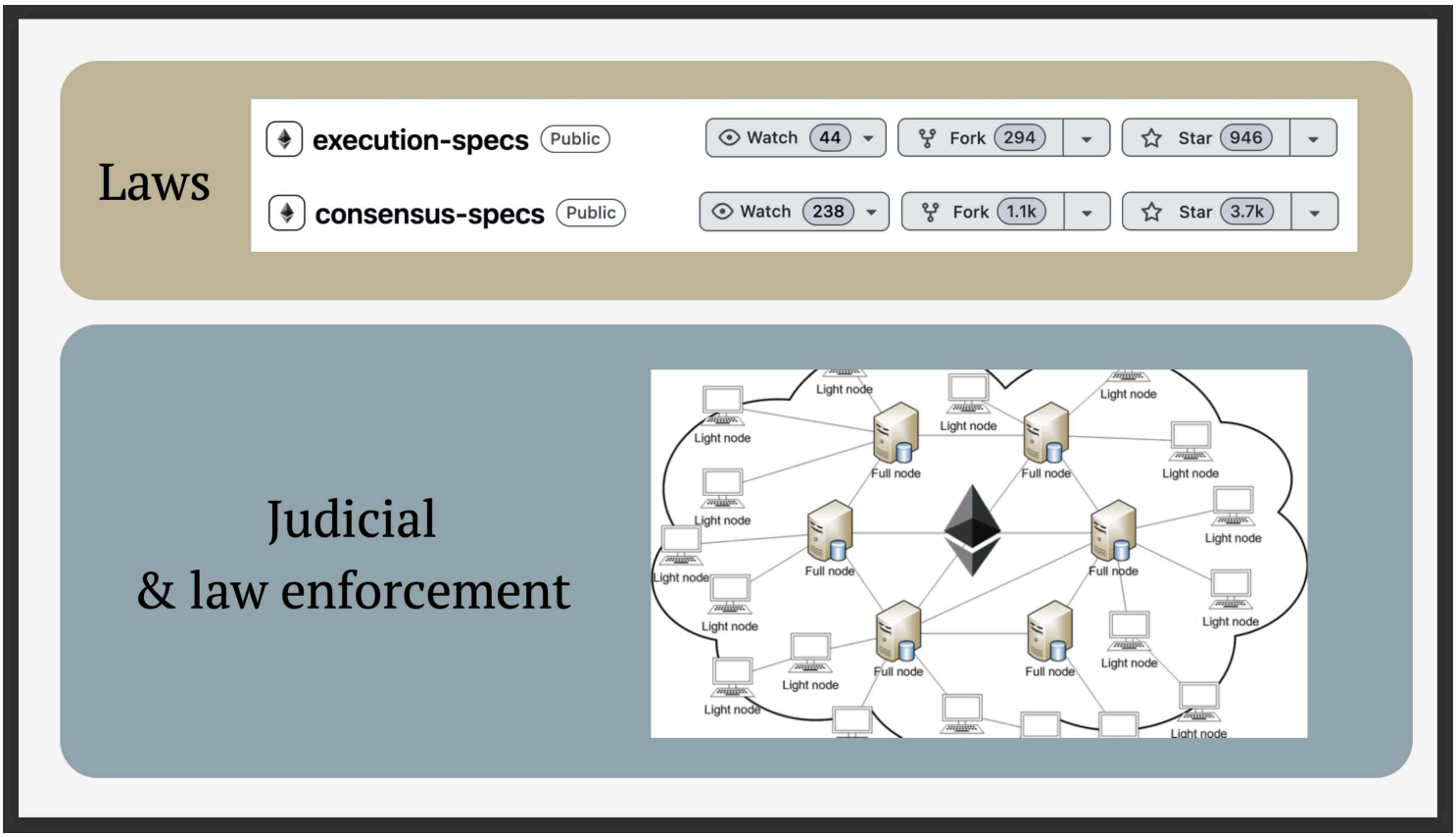
There's this drive to think about promoting and proposing the local-first paradigm to the IETF for standardization. THe basic idea is that CRDT is great for making a distributed application *multiplayer*. Let's make the Web read & write by default by formalizing CRDTs into the Internet protocol stack. Martin Kleppmann, the professor who authored the book on the right, suggested that we would need a couple years more before pursuing the standardization discussion. We haven't seen enough experiments in the wild, and still need some time to explore design trade-offs. Better understanding and broader adoption is the predecessor to standardization. So we might be only a few years away before multiplayer software blossom across the Internet.

Ethereum congress

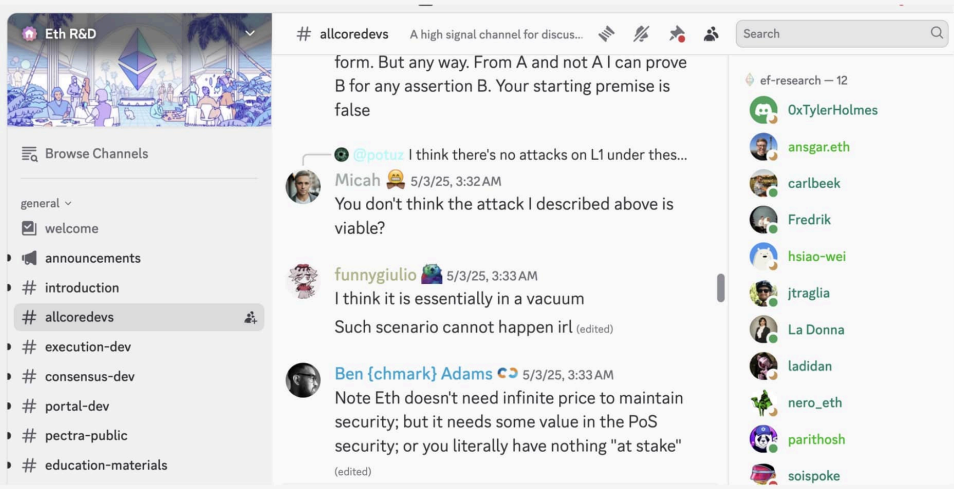
So what can this mean for Web 3? I want to propose a little radical idea. The "Ethereum congress".



It comes from the idea that we have different designs of the constitutional government in the world. In Taiwan we have the five powers, in the US they go with the three powers. But the common idea is you have the balance and porportion of powers. The legislative function can create laws. The executive function can approve new laws and reject them. The judicial system is an enforcing function making sure the laws are carried out correctly. That's the three-power system.



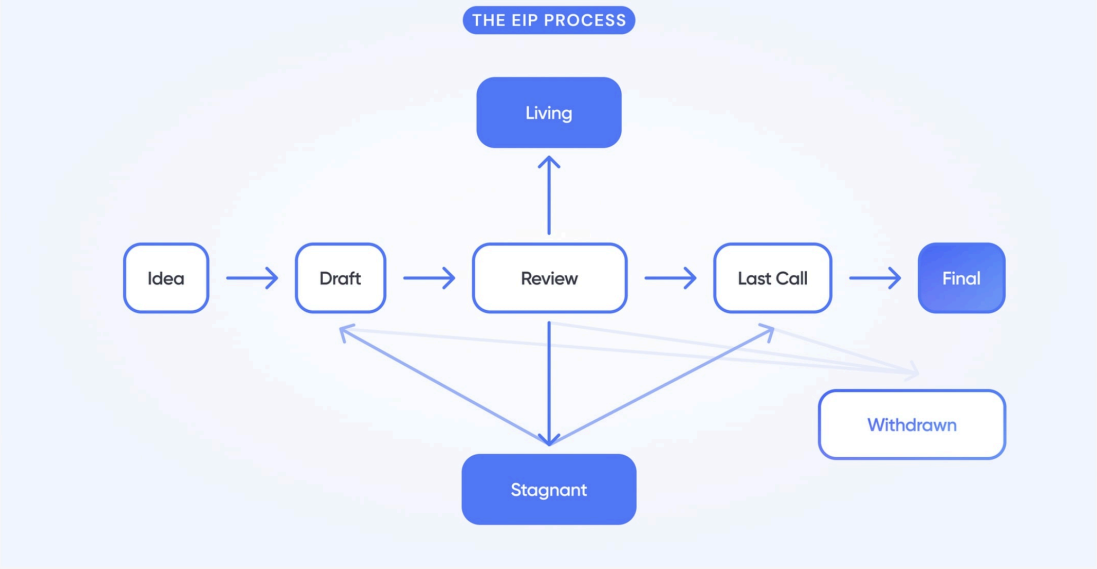
One can argue that Ethereum today has its law, which is the spec. The L1 spec, consisting of the consensus spec and the execution spec, is the law of Ethereum. Client teams implement this law, turning it into working software, at the stewardship and empowerment of the Ethereum Foundation. All the full nodes are running the client software, effectively operating the Ethereum's judicial function together. It works like a decentralized judicial system. There's not a single dominant judge. All the full nodes collectively enforce the law of Ethereum, the L1 protocol.



Running **legislative** sessions on *Eth R&D Discord server* + *ethereum-magicians.org* + *EIP Github* ~ “conducting American Revolutionary meetings on Victorian land”

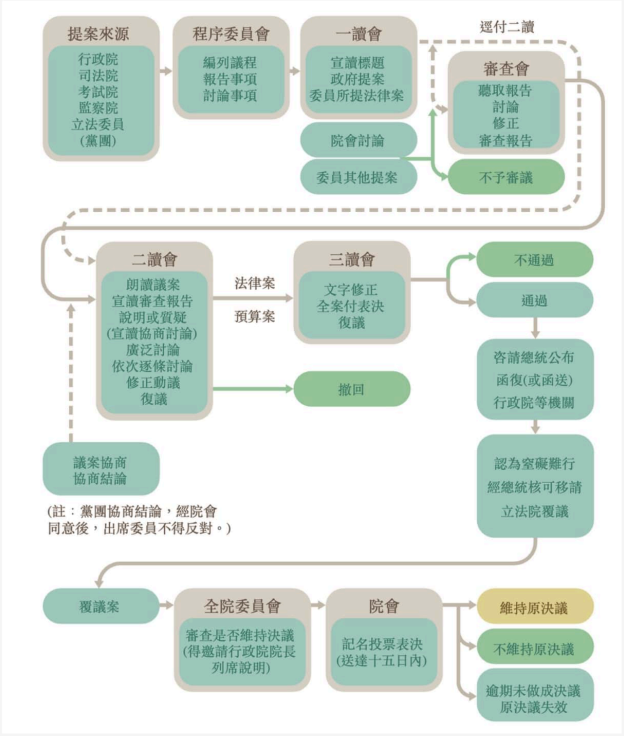
But one can ask: where’s the legistlative function? There’s an EIP process. EIPs are like bills. People discuss them on Discord (Eth R&D server), a Web forum (ethereum-magicians dot org), as well as in the pull requests of the EIP Github repo.

So we are discussing the laws of a Web3 system on the Web2 rail, in a fragmented way. Imagine the American revolutionaries conducting meetings on Victorian land.

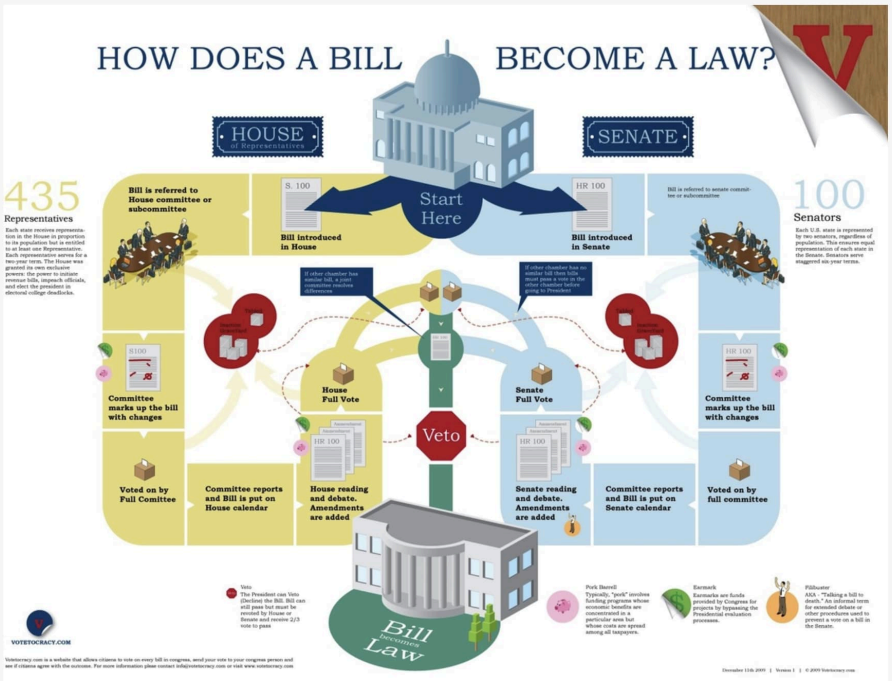


Let's look at the EIP process. Every proposal goes through this state machine. What's possibly problematic, or beneficial depending on how you see it, is the state transition function. The arrows in the diagram. Who gets to decide when a EIP transitions from draft status to review status? The process may not be super clear.

I'm not suggesting or advocating for changing this radically, nor proposing a concrete plan for doing so. One view goes that Ethereum is way too early to be formalized. Because a formalized system attracts all kinds of attack. So this founder-driven spirit, people-driven culture with great alignment, closely safeguarding the system is important. The benevolent dictator. But one can argue that given what has happened in the past few years, maybe we are at the precipice of needing to reform the Ethereum legislature.

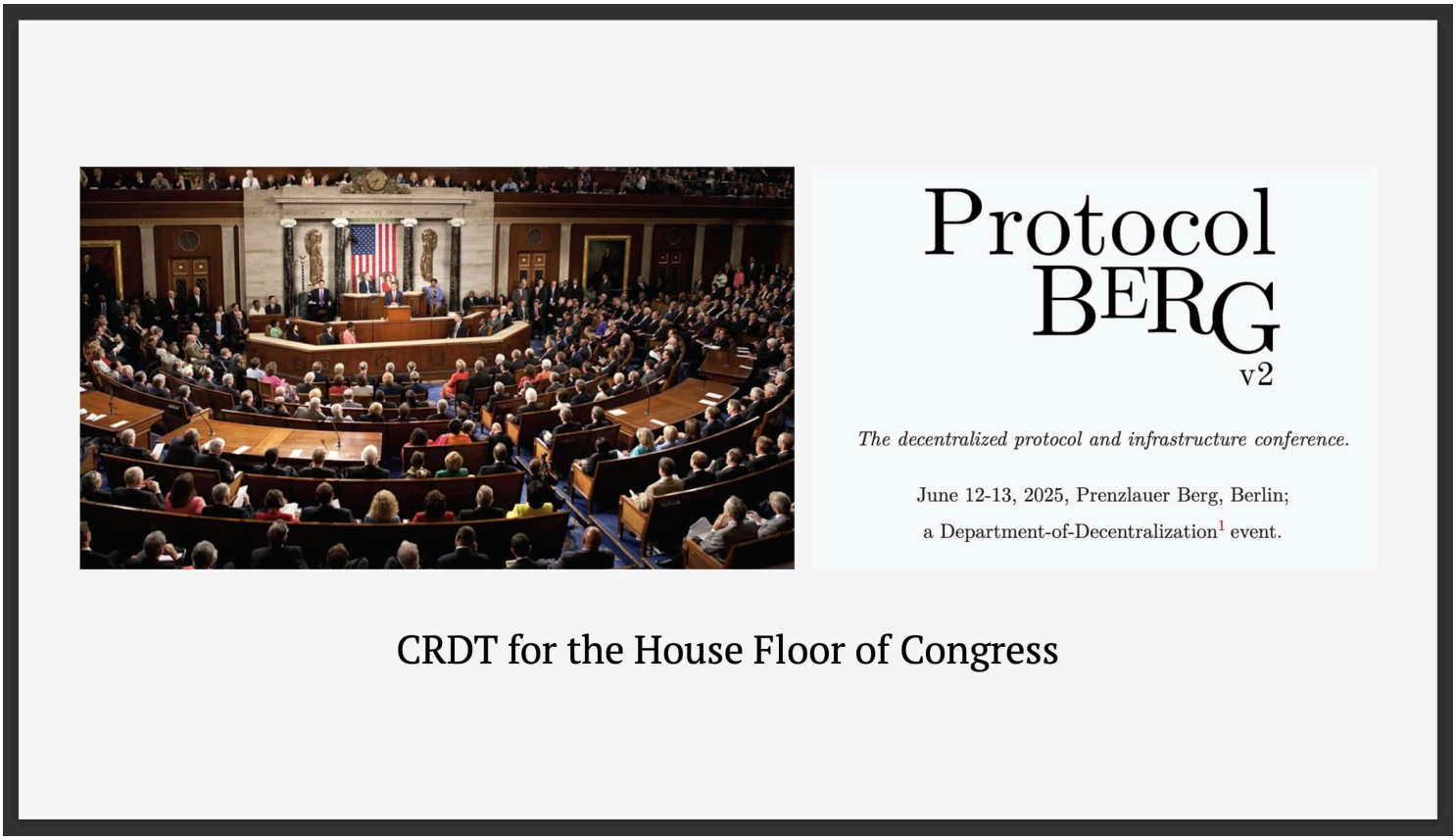


Maybe we can learn from the legislature of constitutional governments. Lots of wisdom has gone into the design of such systems despite the public image of the legislative yuan (立法院) where the legislators sometimes fight in ridiculous ways.



Maybe we can also look at how the US designed their legislative process. You have two houses, the Senate and the House, where the representatives of the people reside. There's an elaborate process for proposing, discussing, and passing the bills.

Obviously I'm not suggesting we should skeuomorphically copy these systems into Web3. Merely saying that wisdom can be gained from looking into the past.



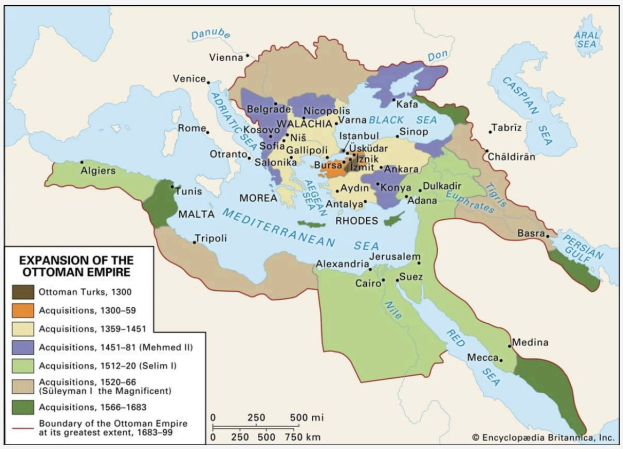
We're maybe far from ready to design such an elaborate system for Ethereum legislature, but we can start from designing the Floor first.

The Floor of the House is the location, where representatives come together, discuss the benefits and trade-offs of the bills, negotiate party interests and so on. One may argue that CRDT is great for implementing the digital House Floor, beacuse (1) it doesn't make sense to put the Floor onchain, which is too slow and expensive for frequent exchanges (possibly with rich data) required in legislative discussions (2) CRDT can be fast, responsive, and cheap, while being built as a strongly decentralized system.

So maybe CRDT can graduate from the technology behind Google Docs to the technology for discussing digital laws.

Empires

I want to end the talk about the idea of empires.



Ottoman Empire
1299-1922

Empire of the Great Qing
1636-1912

Historically, empires come and go. The Ottoman Empire last about 600 years. The Qing Empire lasted about 300 years. They don’t tend to last forever.

Galactic Empire, lasted ~12,000 years
(*Foundation* by Isaac Asimov)

This comes from the Foundation series by Isaac Asimov. There's a galactic empire that governs the entire galaxy. I thought it might be interesting to read a little bit from the book itself, what happened to this great empire, specifically to Trantor, the central governing planet:

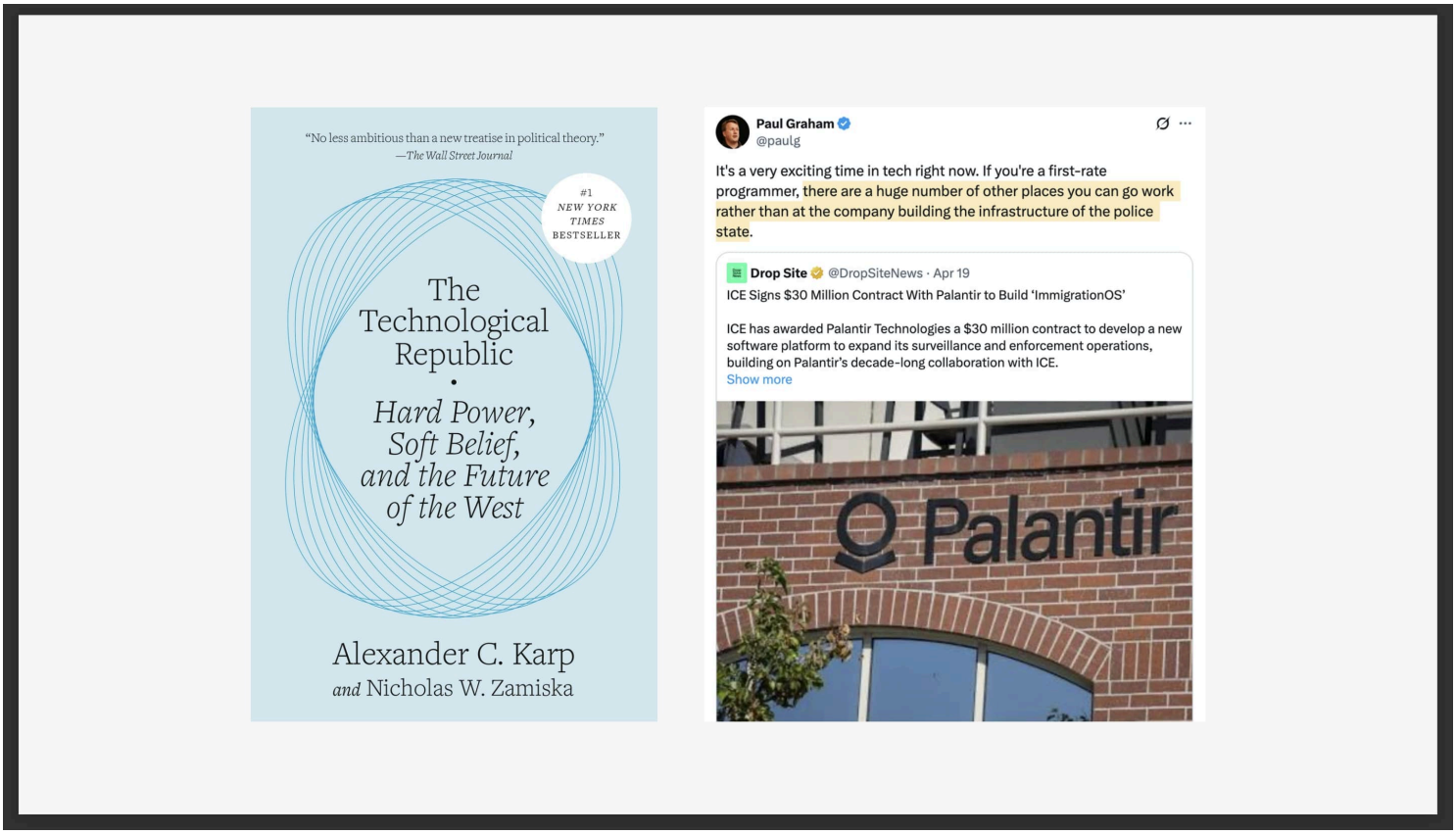
> *Time had been when the insubstantial ribbons of control had stretched out from its metal coating to the very edges of stardom. It had been a single city, housing four hundred billion administrators; the mightiest capital that had ever been.*

> *Until the decay of the Empire eventually reached it and in the Great Sack of a century ago, its drooping powers had been bent back upon themselves and broken forever. In the blasting ruin of death, the metal shell that circled the planet wrinkled and crumpled into an aching mock of its own grandeur.*

> *The survivors tore up the metal plating and sold it to other planets for seed and cattle. The soil was uncovered once more and the planet returned to its beginnings. In the spreading areas of primitive agriculture, it forgot its intricate and colosal past.*

Empires don't tend to last forever. But I'm not trying to say that we should be looking at empire-like countries of our world and consider they may be expiring. For American people maybe they should really think about the finitude of being and the problems they face collectively. Complacency is dangerous. But more importantly for Taiwanese and all these other countries that are dependent on the empire in place. We have the US dollar that denominates a lot of the

world economies. So this is about the well-being of individuals and systems that are relying on a stable world order.



I want to end the talk in this. This is a book published by Alex Karp and his colleague at Palantir. Palantir is a Silicon Valley startup founded about two decades ago. The main idea of the book is that digital technology is powerful and it should contribute to the protection of national interests, specifically the American ones. Palantir works closely with the US military to provide actionable intelligence and recommendations to the soldiers on the ground.

On the right, this is a heated discussion that happened on Twitter less than a month ago. Palantir started working with the US immigration office to apply their technology to real-time identification of those who overstay their Visas so they can be deported as soon as possible. Paul Graham of Y Combinator said that talented programmers have many avenues to invest their talents rather than working for the police state.

I'm not here to argue for one side or the other. The point here is, it has been proven that the history has not ended after all.

We are at a very interesting time in 2025. We are seeing rising nationalism and receding globalization. It's clear that the history is still going. I hope this talk has demonstrated to you that blockchain was invented with censorship resistance against actors as powerful as nation states. Clearly this is a kind of system that is participating in the evolution of our time.

So I think that as you are learning about how blockchains work and how to build applications and so on, this is actually much more than choosing a career. Whether you like it or not, blockchain is participating in the evolution of the world order in front of our eyes. And I think especially in stable times, your actions have outsized influence in the world.

But I think the most dangerous thing is that we forget about the history, and we make the same mistake. We don't have a very good brain. "*We have Paleolithic emotions, medieval institutions and godlike technology.*" If we forget about the past, we'll probably be repeating our mistakes, and the future prospect won't be very good.

Lastly, I'm not suggesting any particular views or manipulating you into particular beliefs. My intention is to present what I see, as objective as possible. I hope that every one of you would be open-minded, develop your own view of where the world has come from and where it is going, and from that view you get to choose your path with wisdom.

Twitter / Github