

FinTech Blockchain's **5w1h**: From Journey 1755-2009 to my journey this year



Chained blocks
(Austrian roots in Switzerland)



Refreshing perspectives on
Chained blocks

This 5w1h lecture will refresh you
with insight over 250+ years. Note:
**Knowledge is NOT power, but
clarity is.** – Yuval Harari, 2018

Prof. Liao (廖世偉), liao@csie.ntu.edu.tw

#1 NEW YORK TIMES BESTSELLING
AUTHOR OF *SAPIENS*

Yuval Noah Harari



21 Lessons for the 21st Century

BigTech companies wield too much knowledge & power.

**To preserve humanity, remember:
Knowledge is NOT power.
Clarity is.**

**Now, go back to the first principles:
Blockchain Concepts & Methodologies**

Refreshing Perspectives: Blockchain's 5w1h:

Blockchain's essentials:

- WHY blockchain?
 - Decentralization
- WHAT is it?
 - Ledger formed by value-yielding consensus.
- HOW to do it?
 - Proof of work
- WHO owns this value?
 - Proof of knowledge
- WHEN to do it?
 - Blockchain literally means block chained after block, which is after another block etc. Block time = ?
- WHERE is it?
 - To the users, it's where the Lightning network is.
 - Internet companies: User-centric and growth-hacking. vs. some crypto companies' 90-10 rule.

Foundation (正本清源): 1 slide on
why Prof. Liao always prioritizes blockchain/btc over those sh*tcoins

Money-printing is arguably the most addictive behavior:

When IPFS folks decided they also want to buy Lamborghini, namely, they issued Filecoin (FIL) in 2017. At the time of ICO, I correctly predicted that there *won't* be any new technology coming out of the team for a while.

Reasons for my prediction:

1. **Money-printing** is the most addictive behavior. Once you are on this drug, you can't break the habit easily.
 - a. Ever since the ICO, IPFS team has become under **perverse incentive** system.
2. You **can't be productive** towards any meaningful goal under such perverse incentive system.
 - a. Each morning IPFS engineers stared at this screen:

Filecoin price since 2017:



Key: Prioritizes blockchain/btc/eth over those sh*tcoins. Let's 正本清源:

E.g., Prof. Liao launched Gcoin blockchain in 2014 without ICO. →

We always start with blockchain's 5w1h: Why, What, How, Who, When, Where.

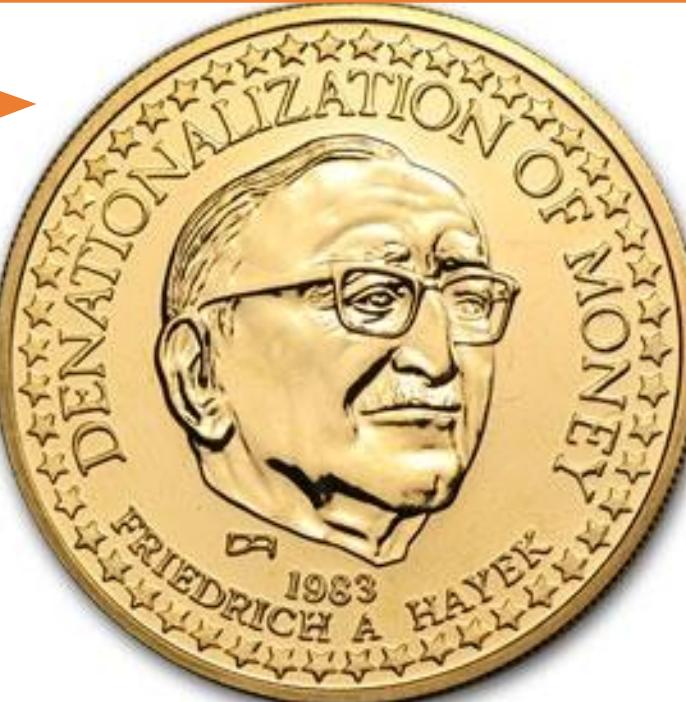
Note: What's blockchain=Blockchain basics. To appreciate What, we'll quickly tour Blockchain apps then.

Why? Decentralization

Decentralization

1. Austrian roots: “珍稀絕?”

- Scarcity
- Inflation
- Future uncertainty: Market



Hayek: Nobel Prize Winner, 1974.
“Decentralization of money”.
Great economist of the 20th century.

2. Cypherpunk Roots

- Privacy
- Surveillance
- Force asymmetry: David vs. Goliath



Hal Finney: Contemporary of S. Jobs.
PGP (Pretty Good Privacy).
Recipient of 1st BTC from Satoshi.

3. Governance failures: → Fat cat, facebook/OpenAI/... censorship, cyber gulag censorship → Occupy Wall street, protests in Russia...

- Bad incentives
- Political censorship

Journey to Decentralization:

- ~250-year journey: Journey from 1755 to 2009:
 - 1755: “Essay on the Nature of Trade in General”, Richard Cantillon
 - The birth of political economy.
 - 2009: Genesis block of BTC blockchain broadcasted, Satoshi Nakamoto
- If we have to pick 1 year out of this 250-year journey, it has to be 1976.
 - “Denationalization of Money” (貨幣的非國家化), published in 1976, is widely discussed and debated, till this day! (See the next 3 slides; **See my journey this year.**)
 - The author of “Money Mischief”, Milton Friedman, got Nobel Prize in 1976.

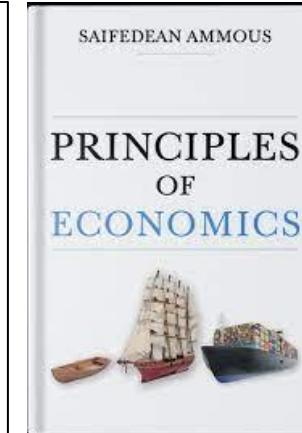
Decentralization: Austrian Roots

My study journey this year (Austria, Switzerland, Germany, 富饒的土地):

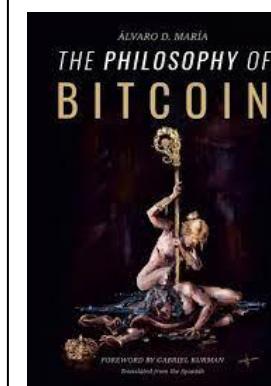
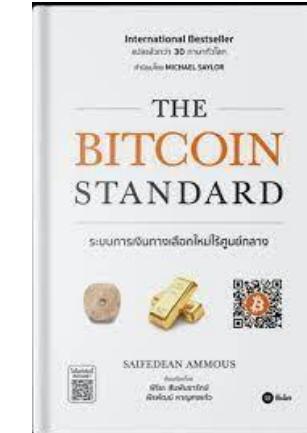


Don't decontextualize (去脈絡化): "Decentralize"'s Austrian roots:

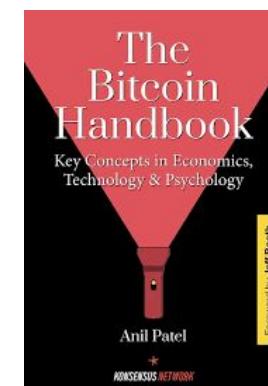
1. It's mountainous & **private**.
E.g., "\$10 of **anything**", but what if you want to become a citizen there?
 - Remember Habermas.
 - Blockchain can help Frankfurt School's vision
2. Everything is **scarce** → Go Finance. Neutrality (Austria, Switzerland): Key: **Leverage** first. "Decentralize"'s Arbitrage:
 - Now you can understand why Taiwan's A-bian's \$700-million saga happened in Lugano.



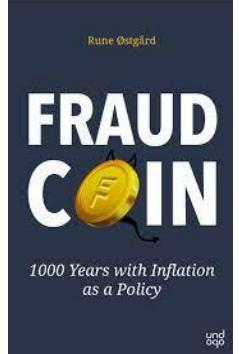
Austrian Root: by Ammous, 2023, 2018,



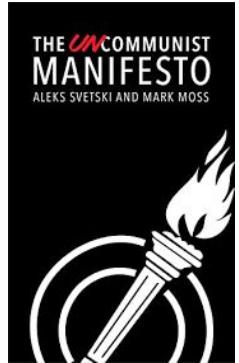
by Alvaro Mario, 2022.
Denationalization 11
crisis, cycles, BTC rights.



by Amit Patel, 2023.
Internet of value.



by Rune Ostgaard,
2022. 1000-year
fraud = Inflation.



by Moss & Svetski,
2022. Sanctity of
the individual must
counter collective's
coercion.

Not just books, but lively discussions:



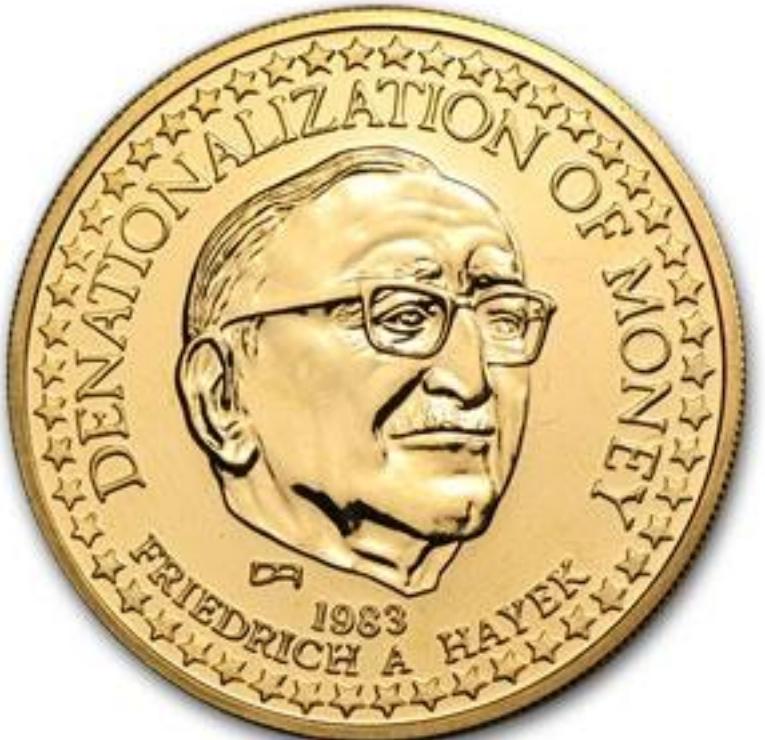
Fruitful exchanges with Amit, Adam, Tether (J.L., Paolo), Lugano, Bitcoineta, Cointelegraph, et al. during my journey this year:



Our students Kevin/Andy/Jennifer vs. Lugano, Tether et al.:

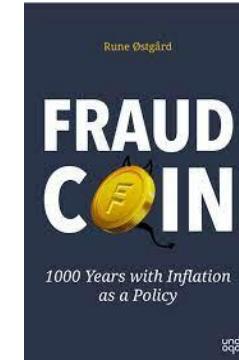


Decentralization: Austrian Roots



Nobel Prize Winner, 1974. Great economist of the 20th century

- The master of classical economics F. A. Hayek place emphasis on the power of free market:
 - The competition in the free market yields the best currency.
 - The government could no longer rig the creation of currency:
 - Hayek's revolutionary suggestion: "Abolish the central bank, and allow the individual to issue the currency. After the competition, we can discover the best currency."
 - Goods and products follow this rule, and so does the currency.
- “Denationalization of Money” (貨幣的非國家化), published in 1976, is widely discussed and debated, till this day!



An even bigger question than “Why blockchain”:

- Why “decentralization”?
 - Namely, why is “decentralization” so important?
 - This is the main reason for my study journey this year to its Austrian roots.
- My journey this year:
 - I believe in the Big 3 (See the next slide) which include “decentralization”.
 - Talking to Tether, Adam Back, ... helps me go back to Austrian roots.

3 key things in the world today, according to J.L. (CEO of Tether)

1. **Free & fair market** instead of Fraud coin.
2. **Open source**: Look at what Linux and Android have done to the world.
3. **Blockchain**: New production/consumption/governance relationships: Decentralized.

This year in Europe I attended 2 conferences: AI-for-good summit and Plan-B (7/1-7/17).

I.e., I do Plan-A and Plan-B. However, J.L. doesn't think my Plan-A above will be fruitful:



- The 3 most important things in the world all focus on **new production relationships (生產關係的改變)**. In contrast, J.L. doesn't think AI is about that anytime soon. (See next slide e.g.) Namely, AI is an accelerator (加速器). Today we got the ESG problem (地球不永續) and AI is accelerating that downward spiral! The production relationship got to change first. Hence the 3 key things above.
- Deep-learning based AI is a black box. Even its inventor doesn't know how it works.
- AI today is based on training. Computer science 101 says "**Sh*t in, Sh*t out**". Look at human nature and how we've fuuked up so far (mismanagement, ESG issues etc). A bunch of sh*t will just train AI to become a bunch of sh*t. Of course, we sh*t likes sh*t (AI) a lot. AI is hot. But it's not what sh*t likes that's the most important. It's what this earth (including her residents such as people) wants that matters.

What people think of AI (at least until ChatGPT's launch):



- Before AI TRiSM problem is solved, human being don't trust AI in terms of governance.
 - AI can function as accelerator. But not as a new governance relationship anytime soon.

Don't get me wrong. I'm working on Plan A and B day and night.

- But it's important to understand Plan B's founder's view and the tradeoffs.
- As a technical guy, I love Plan A too, especially AI is self-referencing, while B is not!
 - AI is fascinating to me since college days, not to mention Google days.
 - Anyway, self-referencing also made AI's governance issue even bigger.
- I believe technology has its own imperative – R. Oppenheimer. Let's work on Plan A and B both.

Plan A & B just got different roles: To me, it's all about technology (NOT those 重分配者):

- Technology (人類進步向來不是靠分配, 而是靠 technology): E.g., 2011: “Software is eating the world.”
 - During Google's early days, I usually interview CS folks, not even MIS folks (“資管生”).
- vs. Sh*t (社會人士去拿分蛋糕的刀, 往往是災難):
 - Previous bunch of sh*t (搶蛋糕刀的社會設計者): Robespierre, Lenin, Hitler, Franklin D. Roosevelt, Mao.
 - Why the New Deal worked, but all others (e.g., Hitler) failed?
 - Before WWII, they are under the name of communalism (“社群主義者”).
 - DAO as a technology is OK, but beware of those people hiding behind the name of DAO.
- Finally mankind has technology for consensus management called blockchain.
 - Before, we only got Robert's Rule of Order at our disposal (1876).

In short, human-only centralized-only “new deal” seldom works.

- Franklin Roosevelt is extremely lucky.

Let’s add technology (blockchain) and let’s add “decentralized”.

- The 250-year journey shows catastrophic failures caused by “new deals” all over the world, repeatedly.
- Can we escape the endless boom-bust cycles?

Can blockchain come to rescue? Thinking and thinking:

Deeply concerned: My “CPU” clock rate is very high. I have to go into the water.

- I keep apologizing to the young people: My generation really fuuked up:
 - How Switzerland achieved green power. vs. How Taiwan messed around before my trip.
 - According to Austrian roots, it's wrong to “大撒幣”:
 - 左派請客, 右派洗碗。左派翻桌, 右派拖地。
- Slogan for my journey this year: “**Before it's too late**, go do something”



Before it's too late!

Journey from 1755 to 2009

Hot debate: Keynes vs. Hayek (江山代有才人出, 各領風騷數百年)

- The fear of Keynes:
 - Supply and Demand curves no longer intersect!
 - Predict that it will happen in 100 years. But it happened in 80 years. Next 80 years?
 - The development of Ethics is not ready for Keynes' fear
 - Proof-of-work.
 - Love/belonging, in Maslow's hierarchy of needs.
- John Maynard Keynes' Planned economy

"Capitalism is the astounding belief that the most wickedest of men will do the most wickedest of things for the greatest good of everyone."
- Hayek's Market economy: The concept of neutral monetary policy in Money & banking
 - Say NO to the regulation and intervention of the government
- 1980's vs. post-2008: after the financial crisis the government adopt quantitative easing monetary policy: "In the long run"
- Reflection today: printing excessive money will lead to inflation (?).



1883~1946年, 英國經濟學家
John Maynard Keynes

Untracked digital currency: eCash

1982: Dr. David Chaum proposed privacy-oriented internet payment system

- It's a foundation of technology of bitcoin and blockchain payment; however, eCash sacrifice its traceability.
- eCash is not decentralized
- 1982: "Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups"
- 1988: "Untraceable Electronic Cash" Crypto'88.
- Panama papers

David Chaum proposed **untracked** digital currency based on the cryptocurrency: eCash, so it has the advantage of circulation like general currency - 1982.



Byzantine Generals' Problem, 1982: Consensus

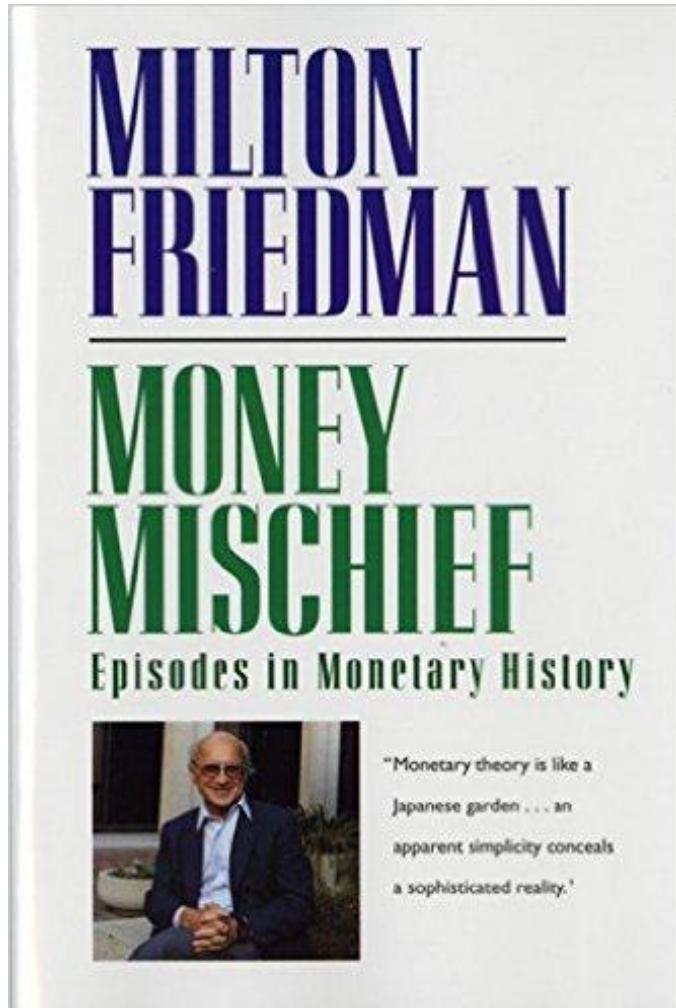
1982: Leslie Lamport formulated Byzantine Generals' Problem

- Leslie Lamport received Turing Award in 2013.
- 1999: Barbara Liskov published an algorithm that addresses Byzantine Generals' problem
 - PBFT algorithm: Practical Byzantine Fault Tolerance
 - Assumes less than $\frac{1}{3}$ failure nodes
 - vs. 51% attack
 - Barbara Liskov received Turing award in 2008.
 - PBFT is targeting about dozen(s) of nodes.
- In comparison, bitcoin blockchain: Targeting 10k nodes! But TPS is 7 only.

Barbara Liskov & Leslie Lamport 2008 & 2013's Turing Award Programming & Consensus Protocol



貨幣的禍害 (Money Mischief), published in 1992



The founder of Monetarism, Milton Friedman claimed the importance of market economy and emphasized the effect of currency.

- Money-in, money-out. Volatility.
- Value comes from consensus. Consensus may come from trust, but not necessarily.
- In addition, he challenged the argument of Keynes' opinion about government intervention by stating that every country shouldn't print the money in an unlimited way.
 - How to utilize science to evaluate the wealth and trade in an efficient way has become the biggest challenge for thousands of years.
 - An automatic device can follow the procedure to issue the currency.

Nobel Prize Winner, 1976. Great economist of the century. 26

Adama Back: Hashcash

Adam Back proposed Hashcash system in 1997.

- A kind of proof of work algorithm relying on an irreversible cost function, which is easy to verify but hard to decipher.
- In the early stage, it has been used to prevent the spam.



The screenshot shows a forum post from the Bitcointalk.org forum. The poster is identified as **adam3us**, a Sr. Member with 390 activities. The post is titled "who is this annoying Adam Back guy?" and was made on June 04, 2013, at 07:22:30 PM. The post content reads:
Taking a leaf from Meni Rosenfeld <https://bitcointalk.org/index.php?topic=121314> I figured I'd create a thread for people to dis me in. Go for it 😊
People seem to think I am trying to claim bitcoin is mostly hashcash with a small change (or it seems that that is what they assume I am saying, its hard to tell other than they find me annoying for some reason). I'm not saying that.

Adam Back
@adam3us
cryptographer, privacy enhancing tech, ecash, inventor of hashcash (bitcoin is hashcash extended with inflation control)

A blue arrow points from the text "He's not saying Bitcoin is Hashcash with a small change." to the line "I'm not saying that." Another blue arrow points from the text "Clearly, he's saying Bitcoin is Hashcash with inflation control." to the line "bitcoin is hashcash extended with inflation control".

Wei Dai: B-money

Wei Dai proposed an *anonymous*, *distributed* electronic cash system: B-money.

- B-money appeared in an email exchange at a Cryptography Symposium 1998
- Use proof of work algorithm to solve the tough problem
- Combine the *decentralized consensus* and then figure out the idea of currency

According to the slides above, we can see the importance of combining Fin and Tech

- Hayek vs. Chaum
- Friedman vs. Back and Dai

After 1998: *Some hoped B-money will be implemented.*

- But Wei Dai is still just a concept
- And Wei Dai does not combine Adam Back's hash cash system
- The large scale Trust Machine didn't appear until Satoshi (中本聰) invented Bitcoin's *Proof-of-Work* algorithm in 2008.

Hal Finney to Satoshi's Bitcoin

- Hal Finney proposed in 2005: reusable proof of work (rPoW) mechanism. This mechanism combines and optimizes Adam Back's hashcash (1997) and Wei Dai's B-money (1998).
 - Unfortunately, Finney died in 2014. No rPoW today.
- My nine-word motto: Inter-disciplinary, be real, **learn-by-doing**.
(跨領域, 玩真的, 做中學)
 - Not only 中本聰 believes this motto but Google and IETF follows these concept.
 - Bitcoin changes the world.





Bitcoin: Digital Gold?

Advantage of bitcoin :

- Compliant to classical economics: 珍稀絕?:
 - Scarcity (Proof of work)
 - Deflationary
 - Future uncertainty (不確定競爭): Mining (挖礦). Vital to market.
- Low cost
- Decentralized Trust Machine instead of Trust Company
- Immutable ledger (願賭服輸不賴皮的平台 for 年輕人)

Disadvantage :

- No Issuer support (unless you go to higher layers)
- Volatility
- Scalability
- Energy?

**Digital currency (Satoshi Nakamoto)
vs. Digital assets (Hal Finney)**

3 Lessons from Journey 1755-2009:

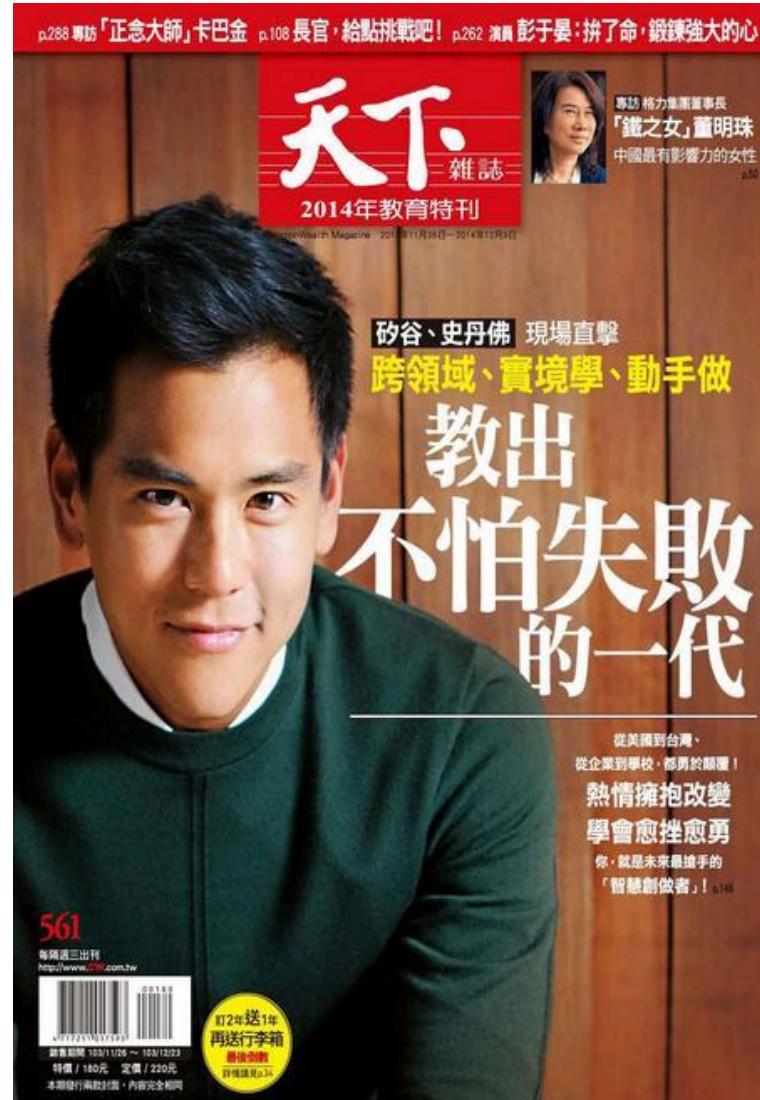
Lesson 1 from this journey to decentralization

1. Pegging to Gold until 1971 (50多年前還是金本位)
2. Then, the collapse of Bretton Woods system. Excessive QE today.
3.
 - a. Bitcoin: Similar to gold mining: non-Excessive, but its market Value is volatile. (比特幣經過百年醞釀, 不是橫空出世: 比特幣的價值來自共識.)
 - b. It does not peg to existing property nor has real-world utility. (比特幣價值 is volatile, 沒有Backing by real-world asset.)
4. Digital currency -- existing law and policy: KYC, AML: 1-2% among all currency values.

法規不應掐死 : a. If we do not take the action, then Google, Wall Street or American government will.
What's our digital currency infrastructure in the future.

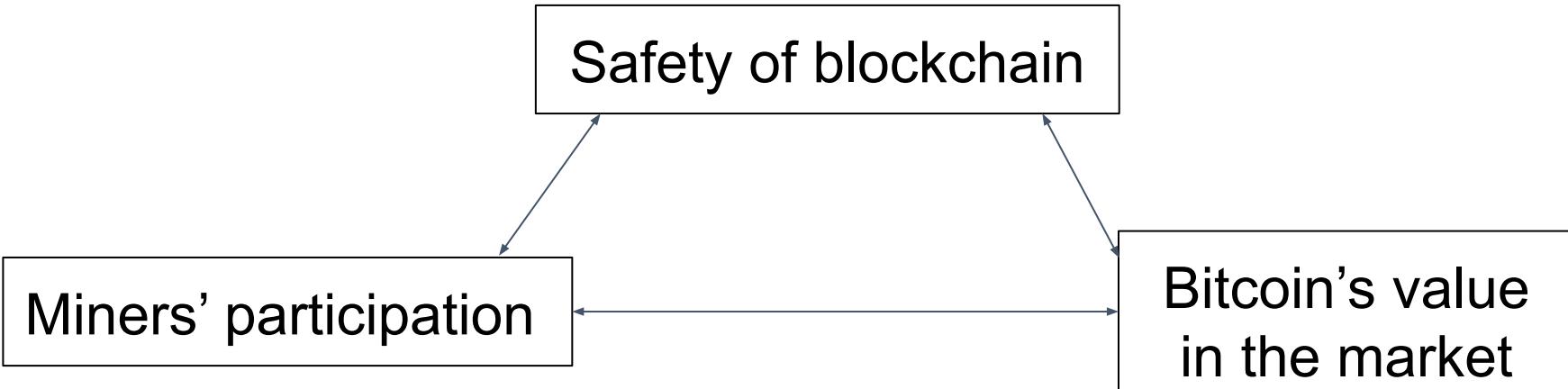
- b. 1-2% is small anyway. Note it's smaller than underground finance.

Lesson 2 from this journey to decentralization



In addition to cross-disciplinary (Fin+Tech), the only way to achieve the milestone of FinTech is coding (open-source, internet-style).

- 中本聰 clearly understands the finance and technology (cryptography, privacy, algorithm) and design a Virtuous Cycle!



Lesson 3 from this journey to decentralization

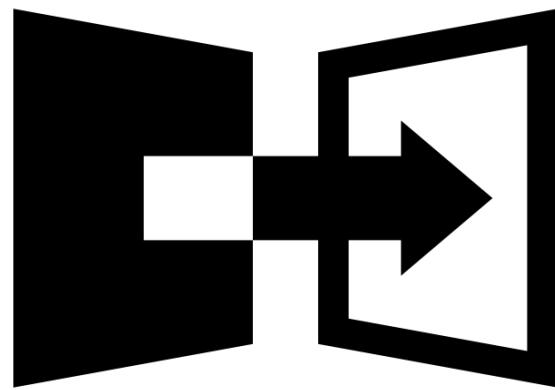


- Digital Finance era: Core technology: Big data and Blockchain.
- Digital Finance digitizes everything: Gives you E, F, G:
 - Efficiency
 - Finality (Security)
 - Gongping, Gongzheng, Gongkai (Inspectability)

**Today's issue: digital finance: digital assets,
digital currency**

Essential: Infrastructure (4D and Blockchain)

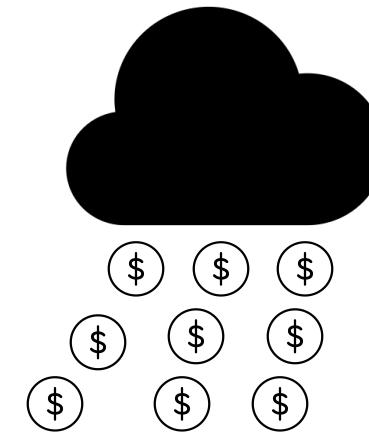
Technology-wise: Illustrate Digital Finance's problem



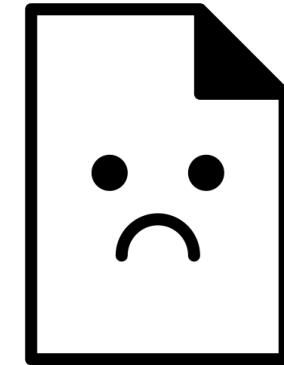
Duplication



Double
Spending



Dilution



Data Lost

The reason for Digital Finance's bad development in the past:
4D → Blockchain (如何一次解決):

Blockchain → 4D (如何解決 4D 問題)

- Duplication:
 - Protected by the Proof-of-work mechanism
 - Every client has a copy of the list of transactions
- Double Spending:
 - The transaction needs to be confirmed by the nodes in the Blockchain network.
 - For example, Bitcoin protects against double spending by verifying each transaction added to the Blockchain to ensure that the inputs for the transaction had not previously been spent
- Dilution:
 - The amount of coin can be limited by proper design via protocol and algorithm.
 - Decentralized system: no central authority controls the right to issuing currency
- Data lost:
 - All transactions are trackable and are recorded in the Blockchain

HOW DO BITCOINS WORK?



Miners' create Bitcoins by using computers to solve mathematical functions. The same process also verifies previous transactions



Users download a Bitcoin 'wallet' that works a little like an email address, providing a way to store and receive currency. Bitcoins can be transferred from one wallet to another using a web browser or a phone app



Bitcoin exchanges will trade between conventional currencies and Bitcoin, offering a way into the market for non-miners, as well as a way to cash out



Businesses create a wallet in the same way as an individual user, typically using a website button to enable a Bitcoin payment. For in-the-flesh enterprises, QR codes can be used to let customers pay quickly and easily

Since the 1st w in 5w1h is key, let's for-once-only use 3 mandarin slides to repeat the key points for “Why decentralize”:

(to wake up napping students)

數學 → 哲學: Technology → Dao (Governance)

- Crypto-Economics: 比市場經濟更大的改變
 - 是資本主義更高境界
 - 中本聰: 去中心化
 - 改變世界 → 先改變自己
 - 改變世界不是: 聲音大, 有槍有砲有Tech而已
 - 創世紀區塊後, 中本聰的權力跟人一樣
 - 比的只是誰相信的早

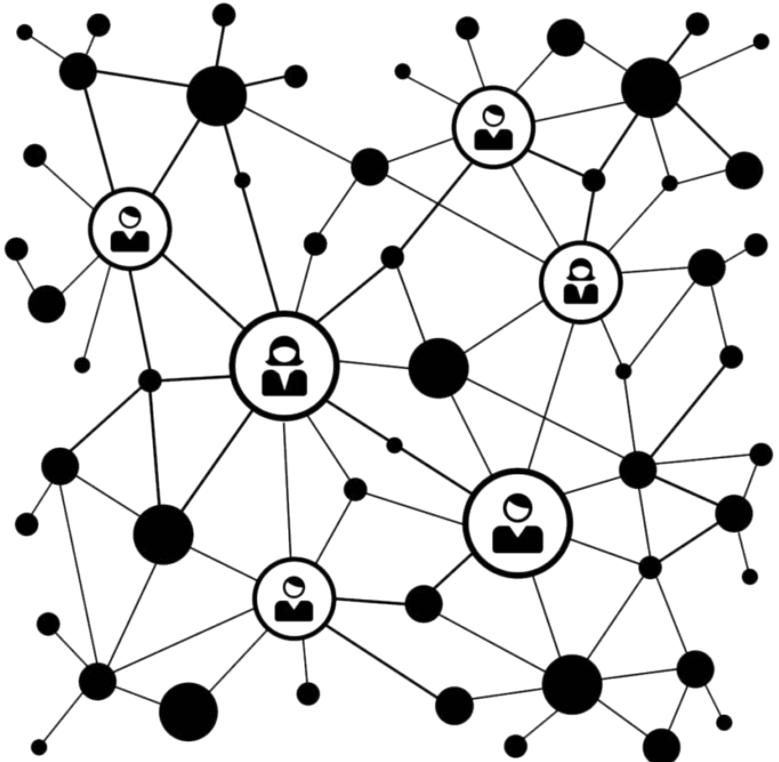
相信者的權力一樣

- 不把權力留給自己 → 大家都來挖礦
- 密碼學的本質 != 加密，而是 Transparency
 - 權力公開，算法公開
 - Most transparent Political-Technology
 - 密碼學：看似複雜，其實簡單
 - 其他的Political-Technology：看似簡單，其實複雜

道 vs. 術

- To determine Token Economy: 是否大師級
- Centralized: 作惡
 - “錢不夠，你就發”
 - 你登台，他唱戲，一段一段。
- Mining (挖礦):
 - Energy is hard to cheat
 - Don't use voting.
 - 也有不確定性競爭: vital for market. (不確定性競爭 allows market, quant, gamification... research)

Decentralization



Difference between:

- Centralized
- Decentralized
- Distributed

Decentralized ecosystem implies:

- User-centric
- Zero-trust

So, Web3 usually comes with 3 words: Decentralized, user-centric, zero-trust

Before rushing to this lecture, I was with a Google colleague at 101's 4th floor:

101: Cathedral of money: (Its center = Il Mercato)



- We're at Il Mercato cafe for 2 hours:
 - An ex-Google colleague has high IQ but low FQ (Financial Quotient).
 - High-income but low RoI (Return on Investment). His case isn't uncommon: According to "Adaptive Markets" Chapter 2 & 3:
 - “你這麼聰明，為何這麼窮？”
 - “你這麼有錢，為何這麼笨？”
- Googlers want to hedge the war risk (對沖台海戰爭風險). 該如何理財? How to invest?
 - 明顯需要跨境 (cross-boundary). Which is NOT necessarily 國外 (abroad).

FinTech = ABCD

- AI
- Blockchain
- Cloud
- Data

How to allocate your time across ABCD?

- Key (正本清源): Which one allows you to contribute? (i.e., to see 粽子頭)
- Key (正本清源): Finance & Insurance.

Example: Key concept in Finance & Insurance:

- Risk diversification
- Risk sharing

You'll learn it in this course, from foundation to practice! Details will be aided by ChatGPT:

ChatGPT: Risk Diversification:



如果我想用馬可維茲模型獲得資產最佳配置比例，需要哪些資料？



馬可維茲模型是一種投資組合優化模型，它的目標是找到一個最佳的投資組合，以在給定風險水平下實現最大化的預期收益。為了使用馬可維茲模型獲得最佳的資產配置比例，你需要以下資料：

1. 資產收益率數據：你需要獲取每個潛在投資資產的收益率數據，通常是過去幾年的歷史數據。這些數據可以用來計算每個資產的平均收益率和波動率，以及不同資產之間的相關性。
2. 預期收益率：你需要預測每個潛在投資資產未來的收益率。預期收益率可以從各種來源獲得，例如經濟學家的預測、分析師的報告、公司業績預測等。
3. 預期波動率：你需要預測每個潛在投資資產未來的波動率。這可以通過使用歷史數據來計算資產的平均波動率以及預測未來的市場環境來實現。
4. 投資組合目標：你需要確定你的投資組合的目標，例如期望風險水平、預期收益率等。這將幫助你確定最佳的投資組合。
5. 投資資金：你需要確定可用於投資的資金總額，以便通過馬可維茲模型計算每個資產在最佳投資組合中的權重。

ChatGPT: Risk Diversification:



請計算2016~2018年間，VTI、BND和TSLA的年化收益率和年化波動率



謝謝您的提問。要計算2016年至2018年間VTI、BND和TSLA的年化收益率和年化波動率，您需要先獲取每個資產在該期間的歷史收益率數據。以下是這三個資產的歷史數據：

- Vanguard Total Stock Market ETF (VTI)：2016年1月1日至2018年12月31日的年化收益率為10.88%，年化波動率為13.74%。
- Vanguard Total Bond Market ETF (BND)：2016年1月1日至2018年12月31日的年化收益率為2.97%，年化波動率為2.39%。
- Tesla Inc. (TSLA)：2016年1月1日至2018年12月31日的年化收益率為20.22%，年化波動率為51.03%。

請注意，這些數字基於過去的歷史數據，未來的收益率和波動率可能會有所不同。另外，投資者應當將投資組合中的各個資產進行適當分散，以控制風險。

ChatGPT: Risk Diversification:



請為我生成以上資產的相關性矩陣



好的，以下是VTI、BND和TSLA的相關性矩陣，基於2016年1月1日至2018年12月31日的日收益率數據：

markdown

Copy code

	VTI	BND	TSLA
VTI	1.000000	0.042479	0.228848
BND	0.042479	1.000000	-0.128520
TSLA	0.228848	-0.128520	1.000000

這個相關性矩陣顯示了每個資產之間的相關性。例如，VTI和BND之間的相關性係數為0.042479，這意味著它們之間的關聯性較低，而TSLA和VTI之間的相關性係數為0.228848，這意味著它們之間的關聯性較高。請注意，這些數字也基於過去的歷史數據，未來可能會有所不同。

ChatGPT: Risk Diversification:



你可以為我生成基於基於馬可維茲模型和50000次的蒙地卡羅模擬，有最大夏普比率的各資產最佳配置比例嗎



當然可以，以下是基於您提供的資料，使用馬可維茲模型和50000次蒙地卡羅模擬後，得到的最大夏普比率的各資產最佳配置比例：

- VTI: 30.83%
- BND: 62.68%
- TSLA: 6.49%

這個投資組合的年化收益率為 7.36%，年化波動率為 10.22%，夏普比率為 0.72。

需要注意的是，這些結果只是基於過去的數據和模型得出的，不能保證未來表現一定如此。投資者應該在選擇投資組合時綜合考慮多種因素，包括風險承受能力、長期投資目標、市場環境等。

ChatGPT: Risk Diversification:



請計算以上資產配置比例在2019年間的表現，並且回答此問題：馬可維茲模型是否能幫助投資人在嘗試最大化報酬時，同時降低風險？



根據您提供的資料，在2019年，基於上述的最佳配置比例，這個投資組合的年化收益率為19.19%，年化波動率為19.04%。因此，這個投資組合在2019年獲得了不錯的回報，但風險也相對較高。

至於您的問題，馬可維茲模型是一種常見的資產配置方法，通過考慮不同資產的收益率、波動率和相關性等因素，來最大化投資組合的夏普比率。夏普比率是一個重要的風險調整回報的指標，可以幫助投資者在最大化報酬的同時降低風險。

然而，馬可維茲模型只是一種理論上的工具，不能保證一定能夠幫助投資者在實際投資中獲得最大報酬和最小風險。投資者還需要考慮多種因素，包括市場環境、投資目標、風險承受能力等，來進行合理的資產配置和風險管理。

Web3=You own your data/users/asset. Web3's security is key:
Always think through your asset right angle (a.k.a. 資產動用權)

Because Web3 is user-centric, zero-trust, decentralized, the security problem is different. First: user-centric, zero-trust, decentralized:

↓
Wallet: Metamask



METAMASK

↓
Token: Ether



↓
Ecosystem (Top 30: >\$2B)



\: Top 30-50. Top 30 should add Shiba Inu, Avax, Leo, Ton, Atom, okb instead.
Top 50: >\$1B.
X: Below Top-50: Neo, Klaytn.

老高 & 小茉: 終將改變一切的 Web3 (2023/3/23)

介紹

[01:51](#) Web1 Web2

[04:20](#) Web3, 包括元宇宙、虛擬貨幣、DAO、DeFi、ChatGPT

[05:00](#) 區塊鏈,去中心化技術, 及現有金融體系

[09:40](#) DAO,去中心化公司, 基於智能協議 智能系統管理 不基於法律, 人力管理, 速度快 半永續

[17:20](#) Defi,去中心化金融系統 虛擬貨幣借錢融資 不經銀行

[17:43](#) NFT, 去中心化所有權認證系統

說明

[18:00](#) 視頻平台實例說明, Web2 Web3分別

[20:00](#) Web1 Web2 Web3服務商大表

[20:05](#) 新技術 與 現有衝突

[20:49](#) 元宇宙的闡述

[21:30](#) 新設備

[22:38](#) 新問題

[24:00](#) 新技術 與 現有衝突

[25:20](#) 總結, Web 2服務現實, Web3替代現實

[26:45](#) 新機會



BTW, always remember: 盡信書不如無書.

Vision: People shall view Web1,2,3 just as one Web

- People used to think “mobile” and “internet” as 2 separate things.
 - Now, it’s called “mobile internet”. (移動互聯網)
- People used to think “apps”, “webpage”, “www” as 3 different things.
 - Now it’s viewed as one.
- People don’t separate Web1 and Web2 today:
 - Historically Web1 switched to Web2 because of one simple switch:
 - Technically it’s AJAX
 - Javascript.

ChatGPT vs. other things in Web3



VS.



Web3's prioritized infrastructure: Security infrastructure.

Web3's prioritized infrastructure: Identity infrastructure. ZKP.

What? Consensus ledger

While teaching WHAT in 5w1h, our experience says: We need to also tour Blockchain Apps to help students appreciate the “WHAT”

- WHAT: Tour of Blockchain basics:
 - Installation
 - Blockchain basics
- Tour of Blockchain Apps.

Note: After 5w1h, we'll cover the following:

- Blockchain Smart Contract
- Case Study on a Blockchain Smart Contract
 - The DAO
 - Over a billion Taiwan dollars hacked
- Real-World Blockchains
- 3 Main Blockchain Smart Contracts
 - ERC20, ERC721, ERC1155

Blockchain Installation

Operating a Full Node

- Main Ethereum network
geth console
- Ethereum test network
geth --testnet console

```
→ geth console
INFO [08-10|01:21:55.275] Maximum peer count
  total=25
INFO [08-10|01:21:55.275] Starting peer-to-peer node
  h/v1.8.12-stable-37685930/linux-amd64/go1.10.3
INFO [08-10|01:21:55.275] Allocated cache and file handles
  me/pwliao/.ethereum/geth/chaindata  cache=768 handles=512
INFO [08-10|01:21:55.520] Initialised chain configuration
  config="{ChainID: 1 Homestead: 1150000 DAO: 1920000 DAOSupport: true EIP150: 2463000 EIP155
  : 2675000 EIP158: 2675000 Byzantium: 4370000 Constantinople: <nil> Engine: ethash}"
INFO [08-10|01:21:55.520] Disk storage enabled for ethash caches  dir=/home/pwliao/.ethereum/geth/ethash
  count=3
INFO [08-10|01:21:55.521] Disk storage enabled for ethash DAGs  dir=/home/pwliao/.ethash
  count=2
INFO [08-10|01:21:55.521] Initialising Ethereum protocol
  versions="[63 62]" network=1
ETH=25 LES=0
instance=Get
database=/ho
config={Ch
ainID: 1 Homestead: 1150000 DAO: 1920000 DAOSupport: true EIP150: 2463000 EIP155
: 2675000 EIP158: 2675000 Byzantium: 4370000 Constantinople: <nil> Engine: ethash}
dir=/home/pwliao/.ethereum/geth/ethash
dir=/home/pwliao/.ethash
versions="[63 62]" network=1
```

Full nodes connected as a blockchain network

A **ledger** spreads over millions of machines

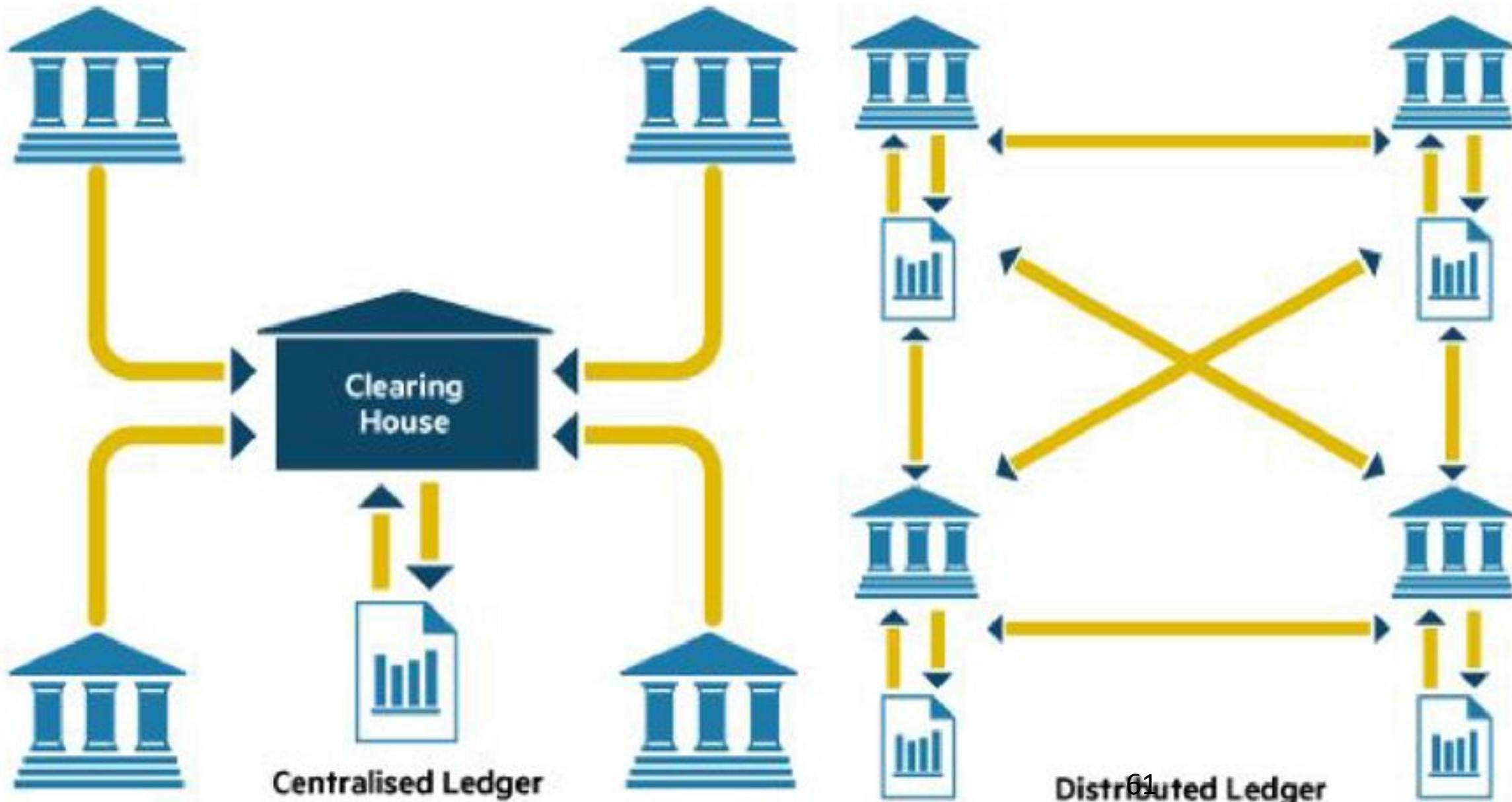
Which uses **proof of work** and **byzantine consensus**

To provide a set of **chained hashes** and **digital signatures**

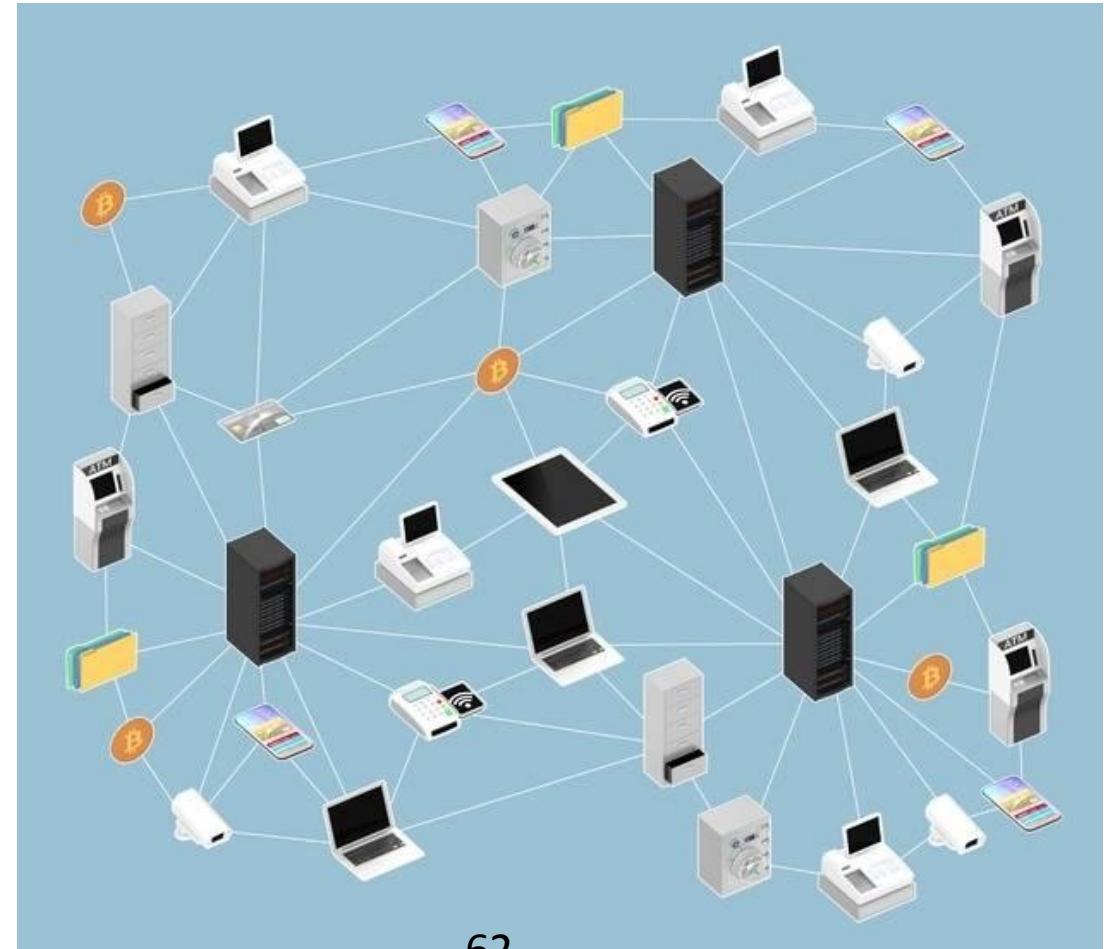
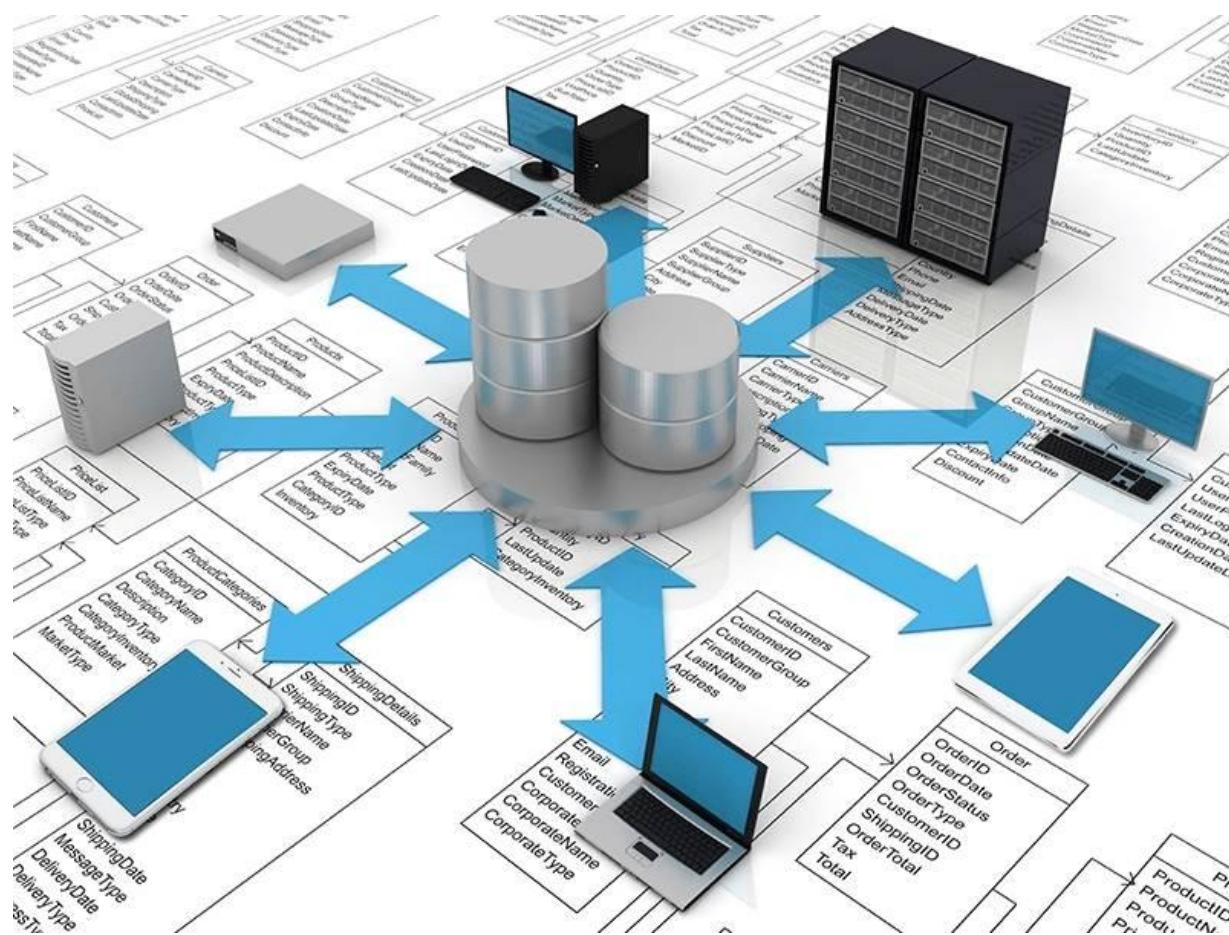
To create an **unforgeable record** of ... E.g., who owns how much bitcoin

Embedding distributed ledger technology

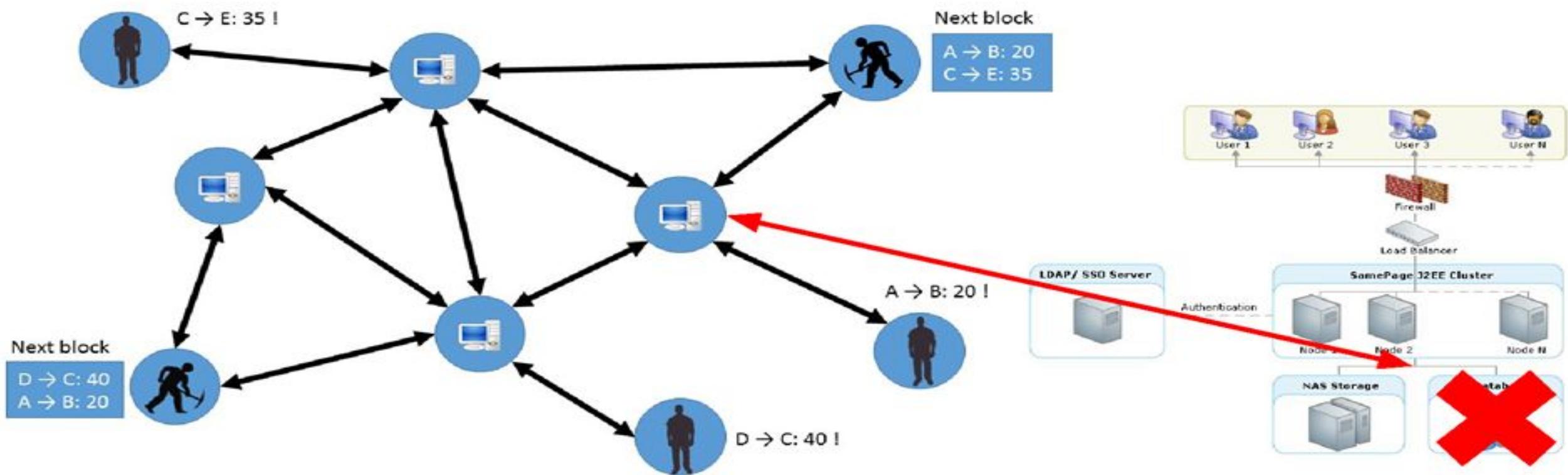
A distributed ledger is a network that records ownership through a shared registry



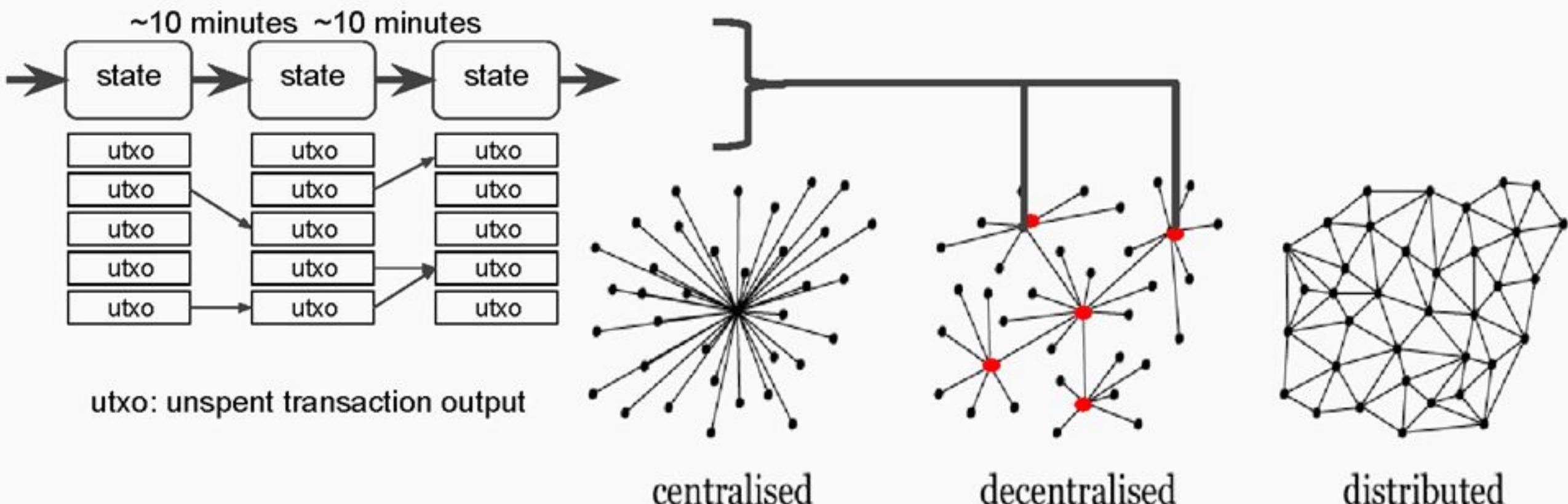
- Security through obfuscation (external cost) vs. Security through internet
- Censorship-resistant



How about Blockchain?



State machine-based immutable 多中心 Trust Machine

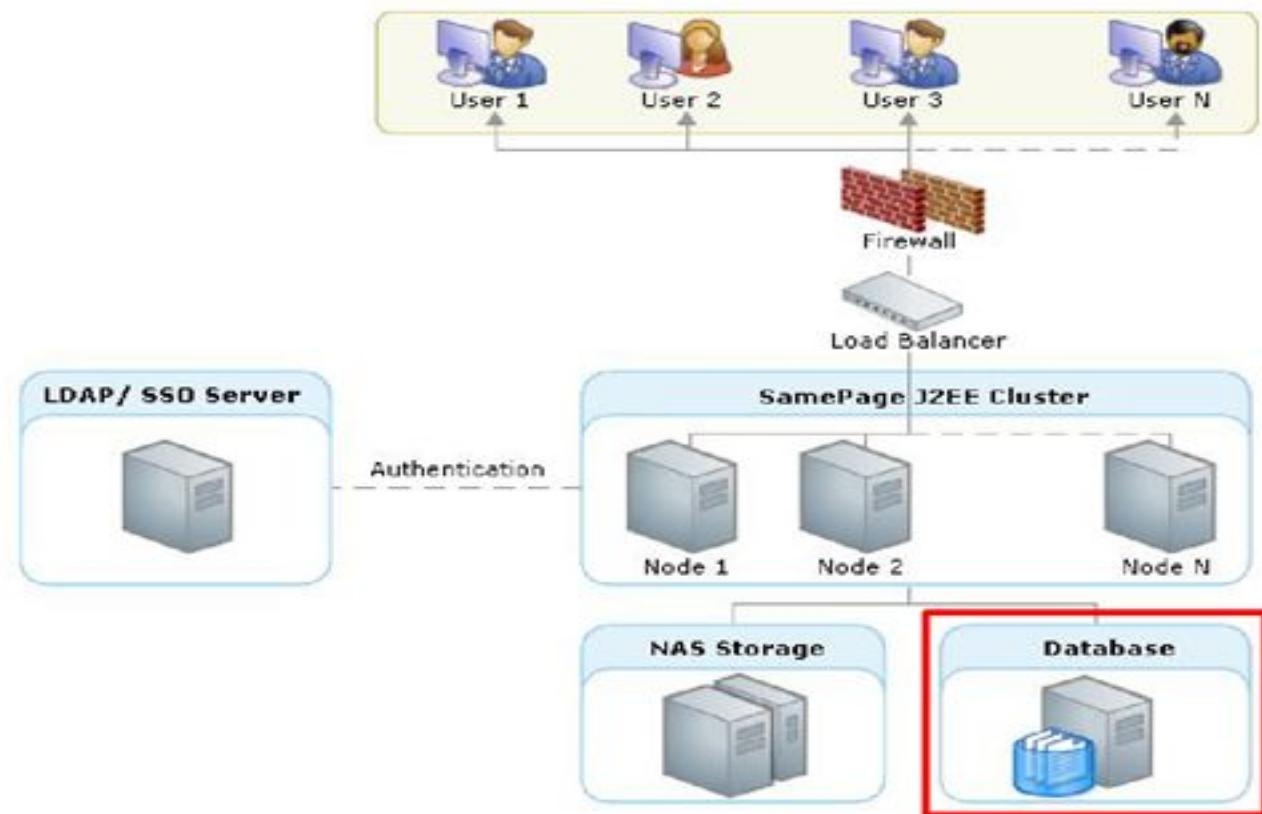


How the Internet and blockchain both work. Ledger is synchronized by “full” (red) nodes.

vs. Current Application Systems

Database!!

***How to be safety and
security smart To
protect your data?***



Blockchain - Another definition

“A blockchain is a magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publicly visible, and which carries a very strong crypto-economically secured guarantee that programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies.” — Vitalik

First Principle: Installing go-ethereum

- On a Ubuntu Operating System, to install:
`sudo apt-get install software-properties-common`
`sudo add-apt-repository -y ppa:ethereum/ethereum`
`sudo apt-get update`
`sudo apt-get install ethereum`

Operating an Ethereum Full Node

- Main Ethereum network
geth console
- Ethereum test network
geth --testnet console

```
→ geth console
INFO [08-10|01:21:55.275] Maximum peer count
  total=25
INFO [08-10|01:21:55.275] Starting peer-to-peer node
  h/v1.8.12-stable-37685930/linux-amd64/go1.10.3
INFO [08-10|01:21:55.275] Allocated cache and file handles
  me/pwliao/.ethereum/geth/chaindata  cache=768 handles=512
INFO [08-10|01:21:55.520] Initialised chain configuration
  config="{ChainID: 1 Homestead: 1150000 DAO: 1920000 DAOSupport: true EIP150: 2463000 EIP155
  : 2675000 EIP158: 2675000 Byzantium: 4370000 Constantinople: <nil> Engine: ethash}"
INFO [08-10|01:21:55.520] Disk storage enabled for ethash caches  dir=/home/pwliao/.ethereum/geth/ethash
  count=3
INFO [08-10|01:21:55.521] Disk storage enabled for ethash DAGs  dir=/home/pwliao/.ethash
  count=2
INFO [08-10|01:21:55.521] Initialising Ethereum protocol
  versions="[63 62]" network=1
ETH=25 LES=0
instance=Get
database=/ho
config={Ch
ainID: 1 Homestead: 1150000 DAO: 1920000 DAOSupport: true EIP150: 2463000 EIP155
: 2675000 EIP158: 2675000 Byzantium: 4370000 Constantinople: <nil> Engine: ethash}
dir=/home/pwliao/.ethereum/geth/ethash
dir=/home/pwliao/.ethash
versions="[63 62]" network=1
ETH=25 LES=0
instance=Get
database=/ho
config={Ch
ainID: 1 Homestead: 1150000 DAO: 1920000 DAOSupport: true EIP150: 2463000 EIP155
: 2675000 EIP158: 2675000 Byzantium: 4370000 Constantinople: <nil> Engine: ethash}
dir=/home/pwliao/.ethereum/geth/ethash
dir=/home/pwliao/.ethash
versions="[63 62]" network=1
```

Tour of Blockchain Apps:

My free sharing comes with the disclaimer (“免責聲明”):

- “投資總有風險，本人過去績效不做未來獲利之保證。最近詐騙猖獗，本人不收會員、不用追蹤、不騙流量、不需粉絲、更不必按讚分享開啟小鈴鐺”。
- 投影片僅供Google好友交流之用，如果你與我看法不同，你肯定是對的。
 - 千萬不要被我影響。
 - Below is for illustration purpose, not for any 理財建議。

Next: Risk diversification in the FinTech Era:

Note: Google Founders' motto: Do interesting things that matter. (我們在道上，所以學起來快，做的過程也有趣，能大師級的深入淺出，以改變世界：)

Ukraine war: 牛市對沖異地戰爭風險: A user-centric approach

- Key: XAUT, odos.xyz
- During Ukraine war: I have 1000 ETH. 2022/11/29 00:30am: \$1,156,700/\$1743.27=663.529 XAUT.
- On 2023/4/2: XAUT = \$1972.30 (1 oz of Gold), which is 13% higher than \$1743.27 4 months ago.

The screenshot shows the Odos mobile application. On the left, there's a summary of a swap transaction: "100 MATIC", "100 am3CRV", "100 DAI", and "120 USDC" were swapped for "0.2573 WETH". A green checkmark indicates the transaction is included in block 3220157. Below this is a button to "Return to Swap". On the right, a large, colorful diagram illustrates the complex multi-path token flow between various tokens like Wmatic, USDT, SX, WMATIC, FRAX, DYST, WMATIC, SAND, SOL, AVAX, and WETH.

ODOOS

About Arbitrage Blog Contact

Atomic Multi-Token Input Swaps

Odos is the first Dex Aggregator to allow users to swap from multiple tokens into one asset in a single atomic transaction. Effortlessly swap a basket of input tokens into the desired output all at once, saving on gas costs and limiting market volatility. Clean up the dust in your wallet and save!

Gold Pricing

Pricing comes from “實質利率預期” (Similar to 與零息債券的定價)

- Nominal interest (anticipated): 名目利率預期
- Inflation (anticipated): 通貨膨脹預期

Non-arbitrage pricing principle.

Interest rate (anticipated)	Up	Down	Up	Down
Inflation (anticipated)	Down	Up	Up	Down
Gold price	Going down	Going up	Sideways	Sideways

My Google colleague and myself: 我們都是長線, 每天還要 **build** (BDS, GenieGPT, 量化機器人, 區塊鏈基礎建設), 不是那種短線, 尋找機會者. So we do **risk diversification**, NOT day-trading ourselves.

- We're not driven by animal spirit alone, so we survived the Web3 crooks above.
- Anyway, we believe in the **user-centric, zero-trust, decentralized** spirit of Web3.
 - Below is user-centric investment:

User-centric: Taiwan Strait Risk (台海戰爭風險) → 熊市對沖

- What's the risk: 原始風險:
 - 房產 (house asset reset)
 - 銀行存款 (asset reset)
 - 上班公司倒閉 (company reset)
- Solution: Revitalize asset (活化資產)
 - 台灣有太多資產需要活化了.
 - Purpose of “大眾創新, 萬眾創業” in 2015
 - Otherwise, listless market (內需市場起不來).
 - 竹東老家 → 資產需要活化
 - Inspired by recent students' “生前遺囑見證”
 - House loans (抵押竹東房屋貸款): NT\$15m
- 20-year loan (貸款20年), 每月 NT\$72,520
 - Rent (出租): 每月 NT\$25k
 - Monthly (每月): -47,520
 - Annual (每年): -570,240
- Buy ETH @ NT\$51,000/ETH (2023/3/28)
 - 294.117647059 ETH
- Transaction: ETH → stETH
 - $1:1.0144 = \text{ETH:stETH}$
 - 298.352941177 stETH
- Or buy ETH @ NT\$37,070.6/ETH (2023/1/6)
 - 404.63332128 ETH
- Transaction: ETH → stETH
 - $1:1.0144 = \text{ETH:stETH}$
 - 410.46004 stETH

User-centric: Hedge the risk (熊市對沖台海戰爭風險)

2023/3/28:

- stETH APR 4.2%~8.5%
 - 5%
 - 14.917647 ETH per year
 - NT\$760,800 per year
 - Keep: 扣除償還貸款後, NT\$190,560 per year.
- 20 years later:
 - 298.4 stETH
 - NT\$3,811,200
 - Home intact (老屋無貸款一間)
- New risk (新增風險):
 - ETH 跌爛: However, we're hedging 台海戰爭!
 - Insolvency (無法償貸): Very unlikely for responsible 台大人: We are not going to buy drugs half-way.

2023/1/6:

- stETH APR 4.2%~8.5%
 - 5%
 - 20.523002 ETH per year
 - NT\$760,800 per year
 - Keep: 扣除償還貸款後, NT\$190,560 per year.
- 20 years later:
 - 410.5 stETH
 - NT\$3,811,200
 - Home intact (老屋無貸款一間)
- New risk (新增風險):
 - ETH 跌爛: However, we're hedging 台海戰爭!
 - Insolvency (無法償貸): Very unlikely for responsible 台大人: We are not going to buy drugs half-way.

Key data in BDS: “人用機器去賺錢”

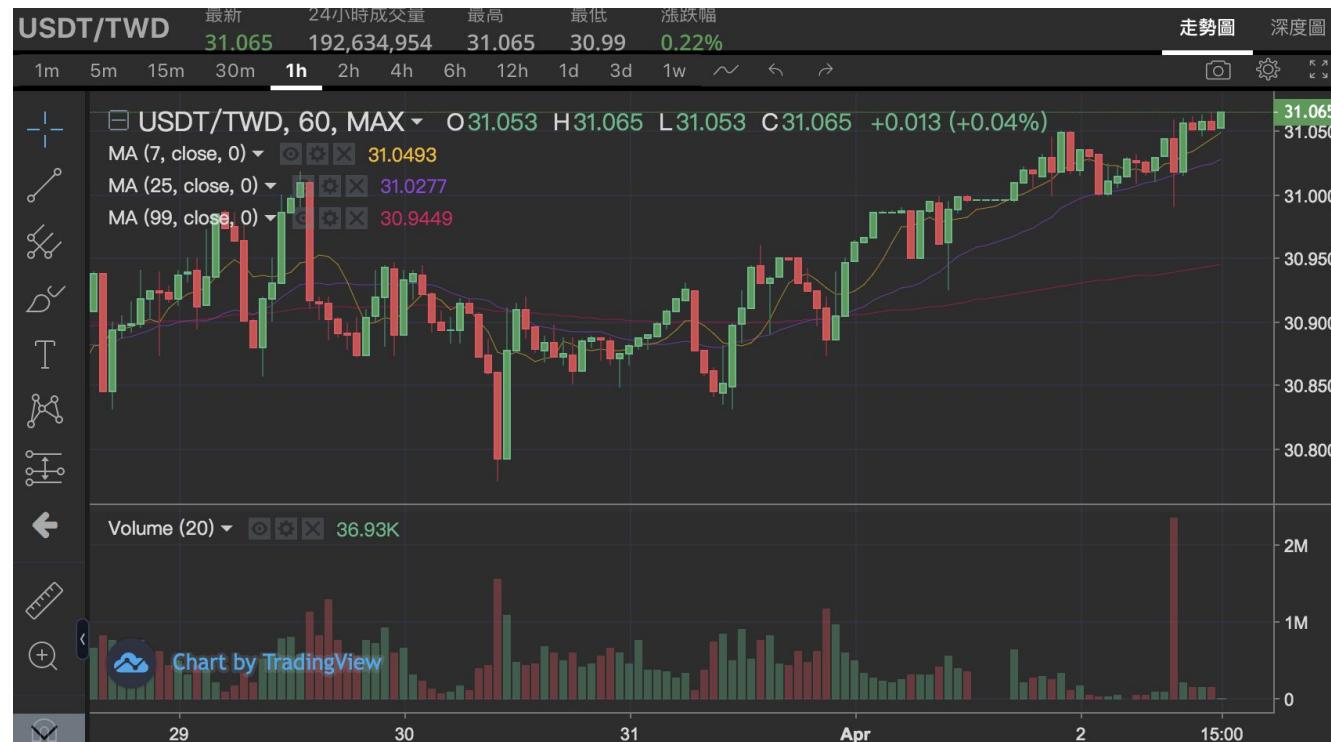
You can't do BDS in vacuum:

- 3 大哉問: **Where are your data from?** How do you process data? How do you monetize data?
- 3 most important datasets in the coming decade:
 - **人**: Healthcare BDS: 人: 是那很多0之前的1. 沒有健康, 再多的0都沒有用. E.g., 台大智慧醫療&健康資訊學程.
 - **用機器**: From Machine doctor to higher-level machine-generated data: **AIGC: GenieGPT**.
 - **去賺錢**: FinTech BDS: 光是記者認證過的, 就有100億的學生 & 20億的學生:
 - 我們專心啟發學生, 關室傳授研發; 不抽乾股. And 我們不做小奸小惡的:
 - In 2022 many asked us to launch NFT 平台 for them; some asked us to help endorse NFT/元宇宙/Web3 平台. Note: We never endorse any 平台, for \$ or for free.
 - Some requests are because they're unhappy about 20萬手續費 by Mxx NFT 平台: 1萬上架費 & 10% for each NFT sold are too expensive for them. Now: 有1萬就不錯了.
 - We offer 2 courses on this: 2H each year: 金融課 & bda課 搭配服用.
 - 金融課: **FinTech下的金融課為資工系獨有**: 正本清源 不去炫經濟理論(沒有屬於財金系的二階微分方程). **Fin&Tech**: 理論最紮實: 什麼是錢, risk management, FinTech下的期貨理論(See last slide)... **卻又最動手**.
 - bda課: a BDS: 研究量化機器人, crypto-tracing各種BDS. 還需搭配上述金融課, 效果最好. (Or you already knew **FinTech下的金融**.)

Risk Diversification: My ex-Google colleagues & I were at Il Mercato for 2 hours:

After the 1st hour going thru Risk Diversification in the past ~20 slides (深入), I went through basics in the 2nd hour: 10 slides (淺出).

- Set up wallet (錢包)
- Set up accounts
- On 2022/4/2, Rybit: 30.913. Max: 31.065. 可套利~2毛? KGI - Rybit - Max - FarEastern.
- Tether: omni vs. ERC20 vs. TRC20.



2 examples of my *Fin*-course (金融課) & *bda* course going together:

- bda: You can use bot (量化機器人) to hedge against Taiwan Strait Crisis (台海戰爭風險):
 - But you still need 金融課 to learn about the futures (期貨), hedging:
 - “你做大豆沙拉油的，要買黃豆期貨，要賣黃豆油期貨。”
- bda: You can use bot (量化機器人) to arbitrage (套利):
 - But you still need 金融課 to learn about arbitrage basics (套利的三大主軸)

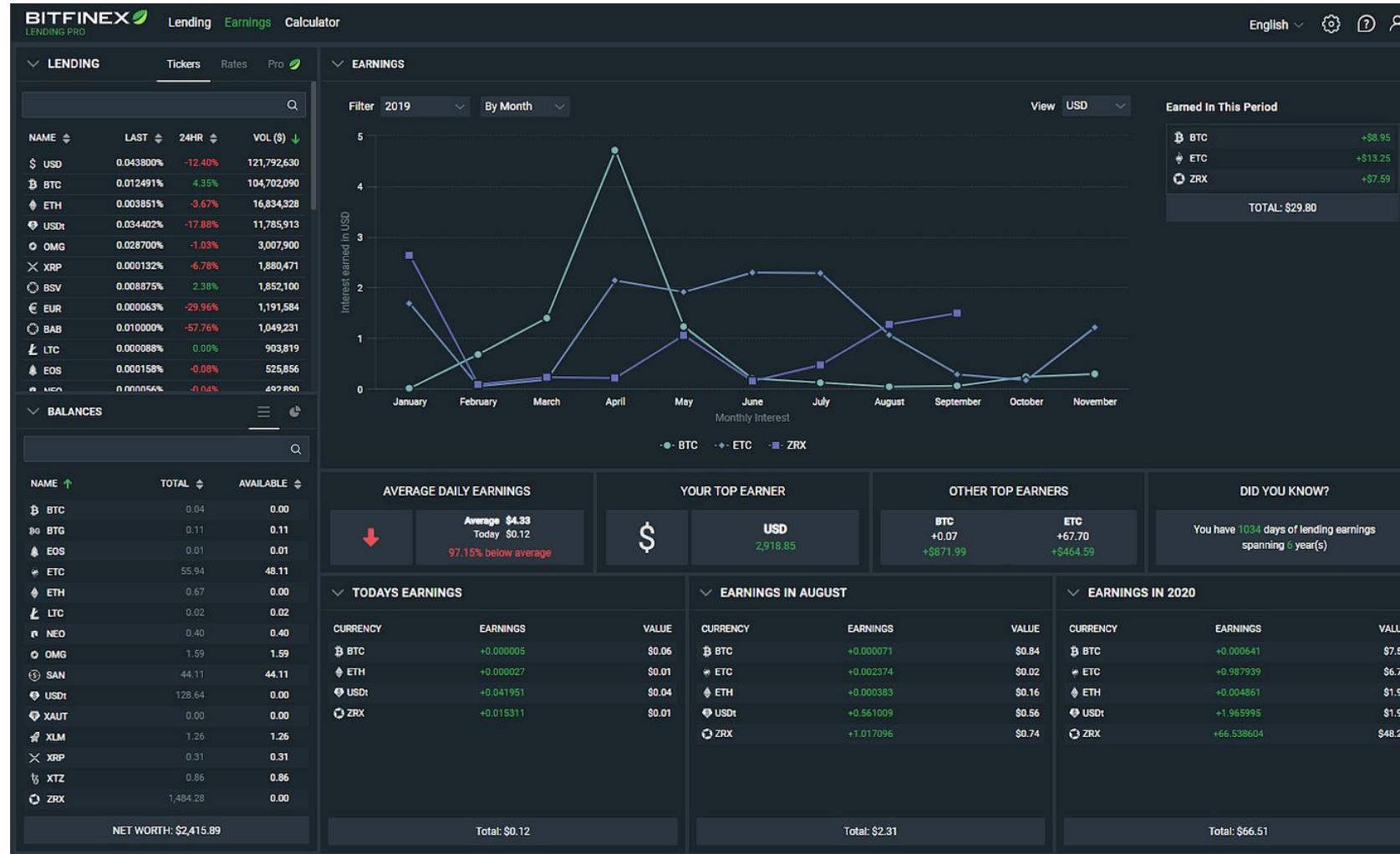
If you go to cbc (央行), you pay NT\$30.72 to buy a USD.

On 2023/4/2:

幣別	即期匯率		現金匯率	
	銀行買入	銀行賣出	銀行買入	銀行賣出
美元 USD	30.3900	30.4900	30.0500	30.7200

- But it's not a digital dollar. You need to pay 30.913 to get USDT (digital dollar).
 - 透明的美金 vs. USD.
- Rybit: 作莊: Can offer \$30.913. Max exchange: Peer-2-Peer: 兩邊賺.

With USDT, you can try Bitfinex lending pro & Pionex & many other tools:



I used to use fuly.ai, which get me good rates. Now I can do it myself.

Risk diversification: Stablecoin such as TWDT (台幣穩定幣)

- TWDT requires the coordination of government, banks and users. (公私協力)
- Why? Not for my own selfish gain, but for Taiwan's public good.
 - Rigorous: Each step we should provide hedging vehicles:
 - TWD → TWDT → USDT → crypto_1 → crypto_2
 - What's missing now is TWDT.
 - As a result, we're exposed to the risk of FOREX difference (匯差).
 - Best: We should provide many pairs with TWDT participating:

幣別	即期匯率		現金匯率	
	銀行買入	銀行賣出	銀行買入	銀行賣出
美元 USD	30.3900	30.4900	30.0500	30.7200

Recap: So far we talked about 5 personal finance: Diversify:

- Bull market: Hedging Ukraine war with XAUT
- Hedging Taiwan Strait Crisis: House loan in order to stake ETH
- Arbitrage: Rybit vs. Max exchange
- Futures: We need to teach Perpetual Contract in the Web3 world, in the future.
- Lending Pro: “老師, 我想被高利吸金”, “我想被低利放貸”.
 - From Fully AI to your own RoboAdvisor.

DAO亦有道: Above I stick to the Web3 spirit: **User-centric, zero-trust, decentralized.**

Seize the day, but say NO to brain-dead day-trading. Do FinTech, please.

Finally, TWDT (台幣穩定幣, if any) requires the coordination of government, banks and users. (公私協力)

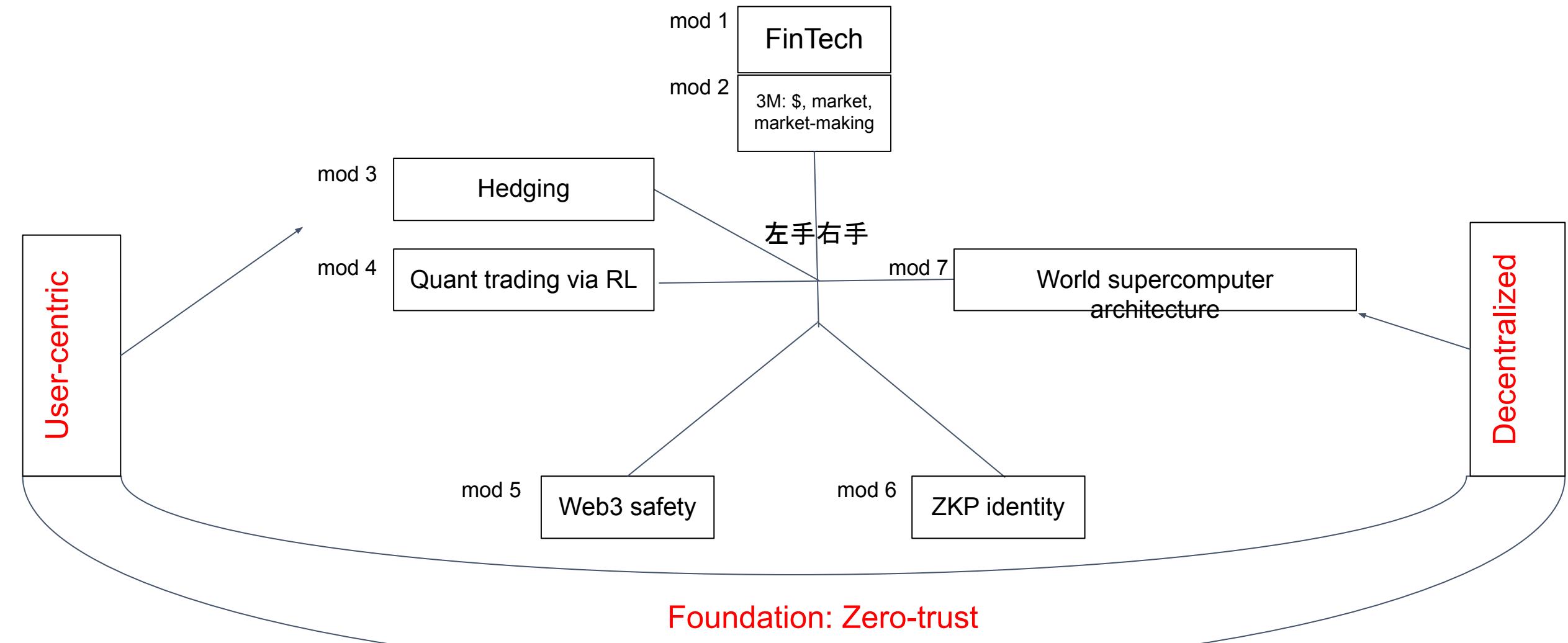
Remember: Web3 is **user-centric**, **zero-trust**, and **decentralized**:

Now that we have covered the user-centric part, let's wrap-up Part 3 of the talk by visiting zero-trust and decentralization.

What's difference between ZKP and Zero-Trust?

- Zero-Trust is required by US government starting on 2025/1/1.
- Zero-Trust is NOT just a technology question:
 - A lot of it is education and management.
 - You have the best ZKP technology, but there is some internal traitor.
 - So, on need-to-know basis.

Risk Diversification Technology (Note: Module 5: Web3 safety) as a human:



Jim Rickards' 3 narratives and what about Crypto narrative?
We need to rebuild the trust.



Web3: We need to rebuild the trust, including more rigorous definition of Web3.



https://taiwanplus.com/taiwan%20news/business/221216003?utm_source=copyurl&utm_medium=share

How? Proof-of-Work

Proof-of-Work: Starting with Hashcash 1997

Hashcash:

- Checksum
- Digital challenge
- Adjusted difficulty

Motivation for Hashcash: Anti-spam

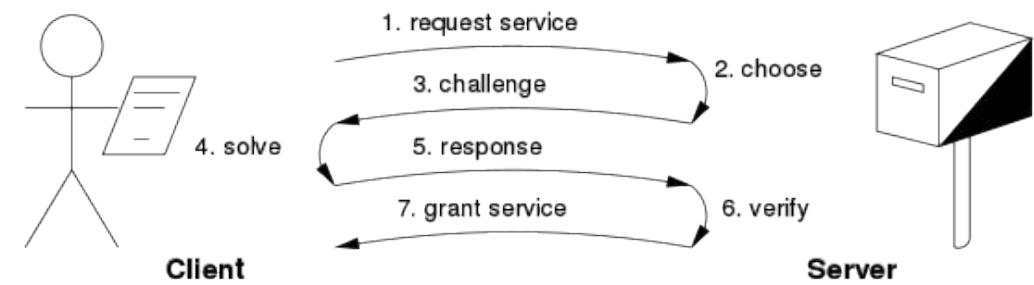
- Scarcity

Anti-spam also involves:

- Trusted lists
- Centralization in Hashcash world

Problems with Hashcash:

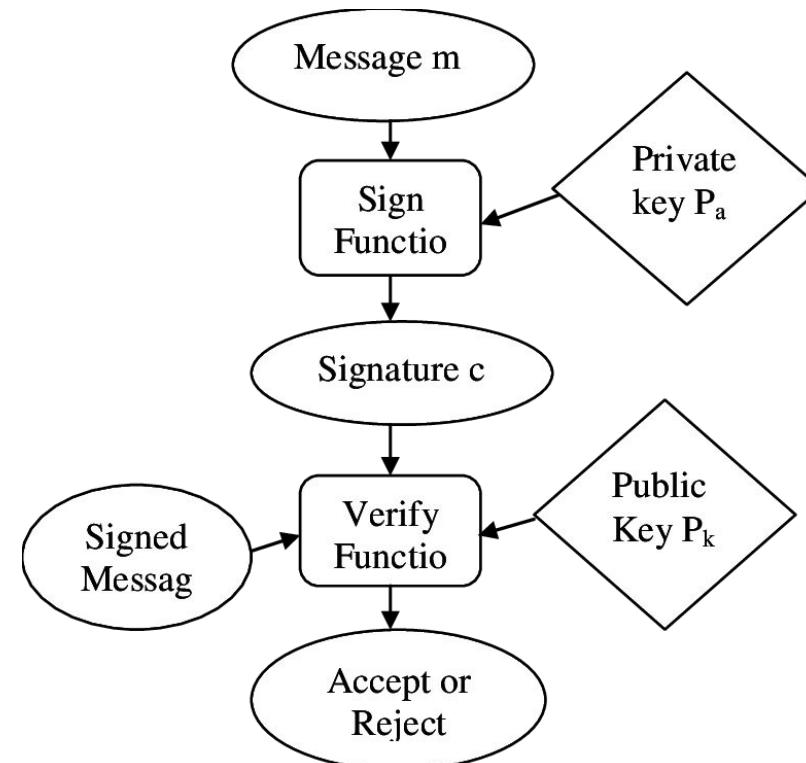
- Missing incentives
- Waste



Who? Proof-of-knowledge

Proof-of-Knowledge

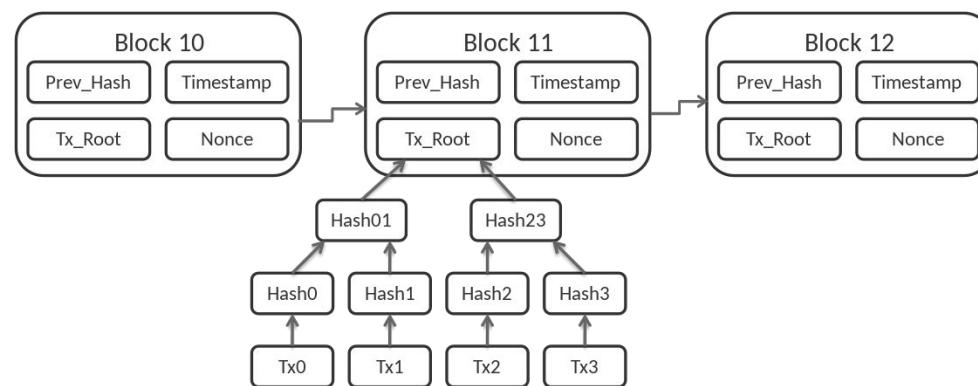
1. Leak
 - Privacy
 - Trusted Channels
 - Centralization
2. Ecash
 - Encryption
 - Digital Signature
 - Smart Contracts
3. Problems
 - Double Spending
 - Fungibility



When? Block chain

Block chain

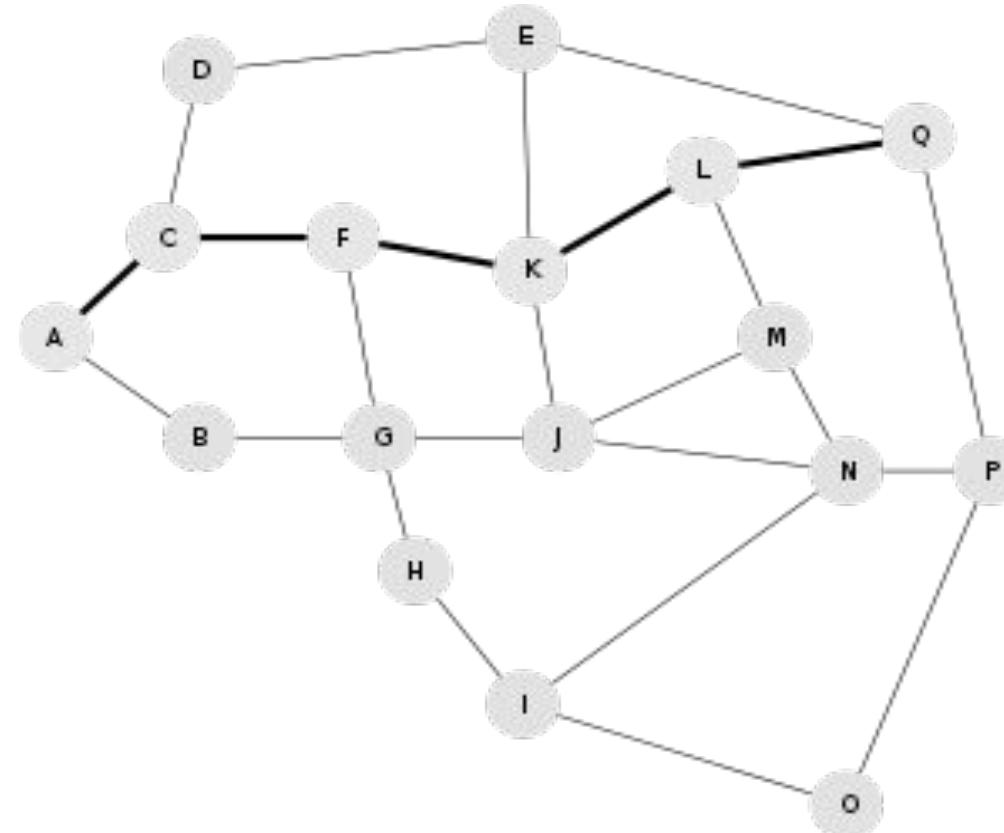
1. Dilemma
 - Voting
 - Closed vs Open
 - Staking
2. Time Chain
 - Previous Block
 - Heaviest Chain
 - Inflation Control
3. Block Space
 - Space Fees
 - Blocksize



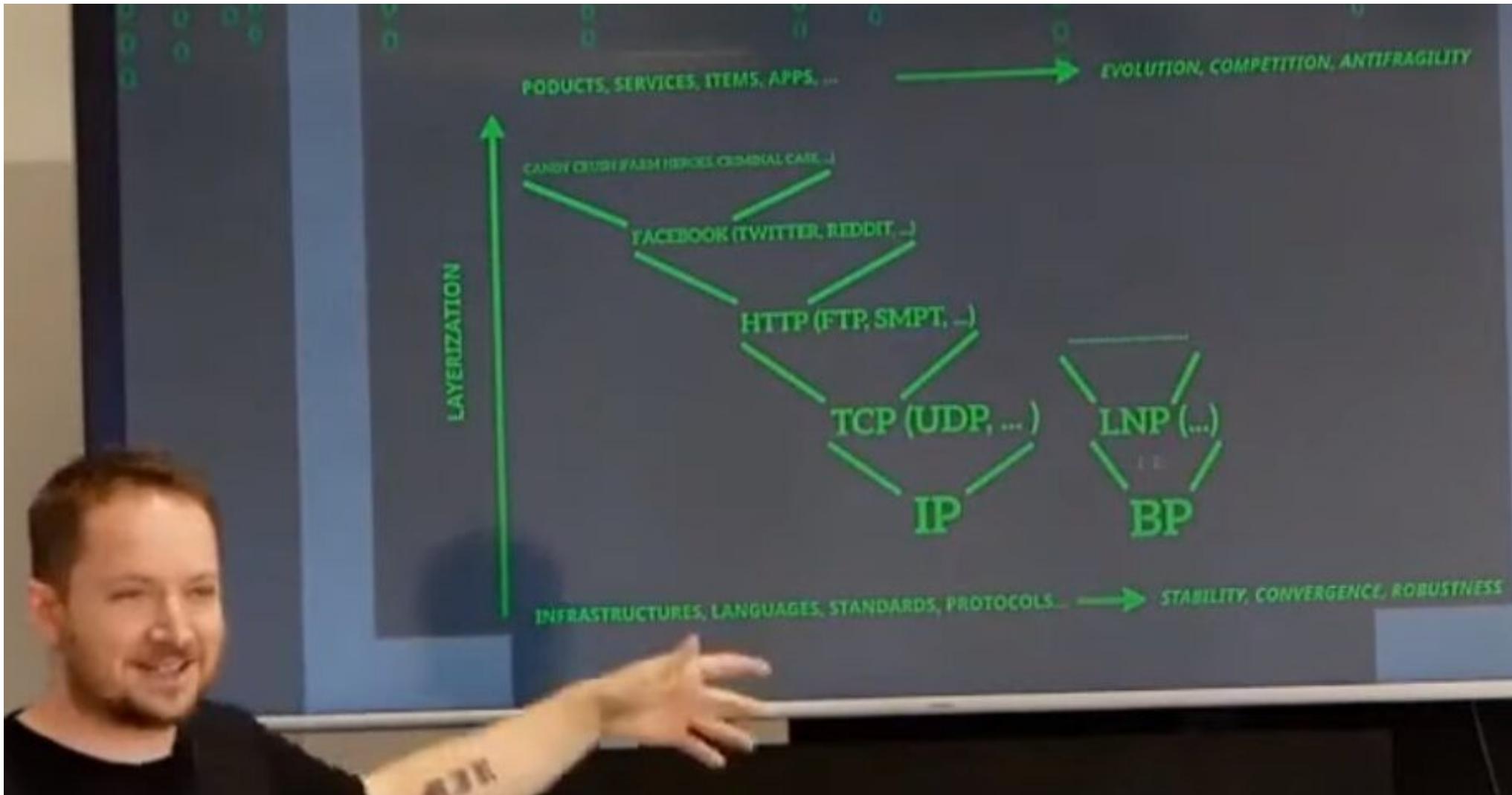
Where? Lightning network

Lightning network

1. Dilemma
 - Scaling
 - Small vs Big
 - Sharding
2. Payment channel
 - Coin sharing
 - Cooperative closing
 - Justice transaction
3. Lightning routing
 - Routing fees
 - Atomicity



LNP/BP vs. TCP/IP: Thanking to G. Zucco for below



The Layers of Bitcoin

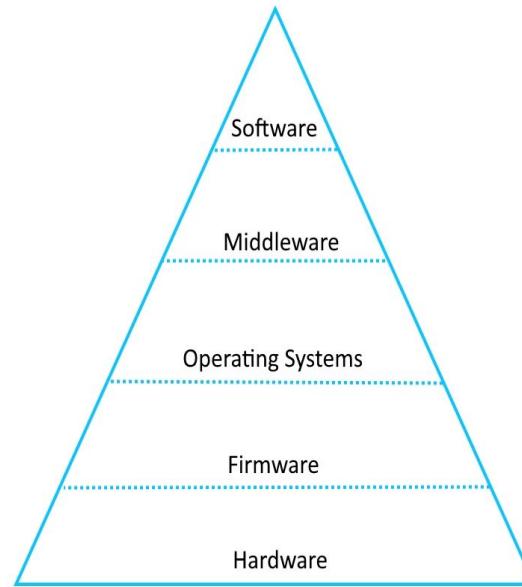
Bitcoin's layerization and the LNP/BP stack

LNP = Lightning network protocol

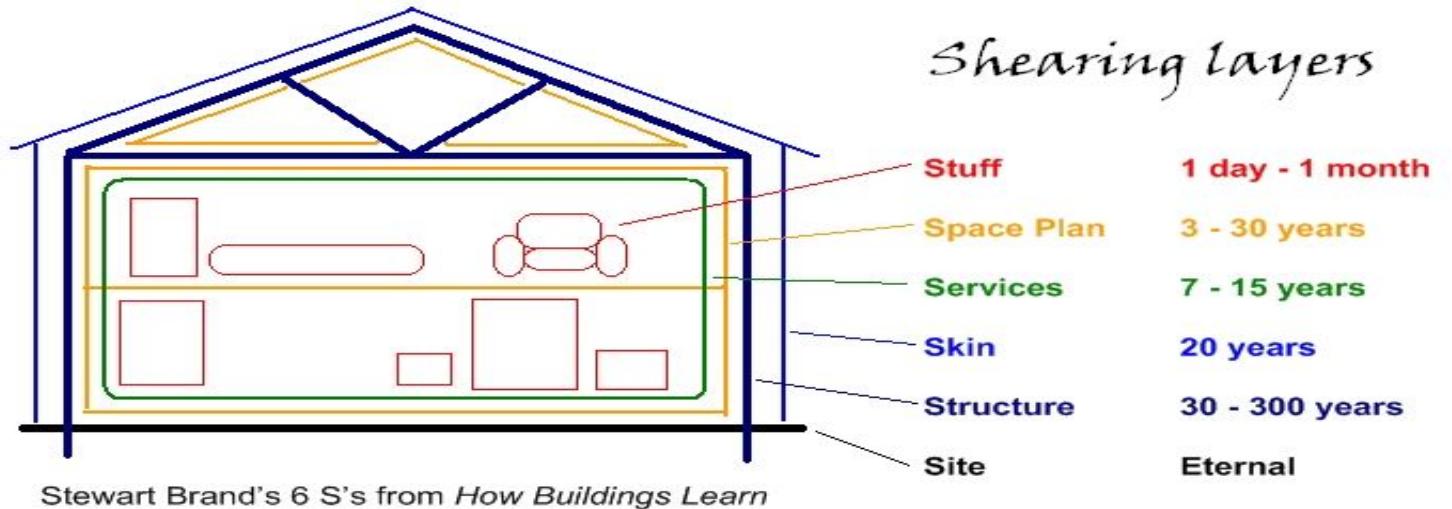
BP = Bitcoin protocol

Layers before Bitcoin:

- Shearing Layers
- Computer Science



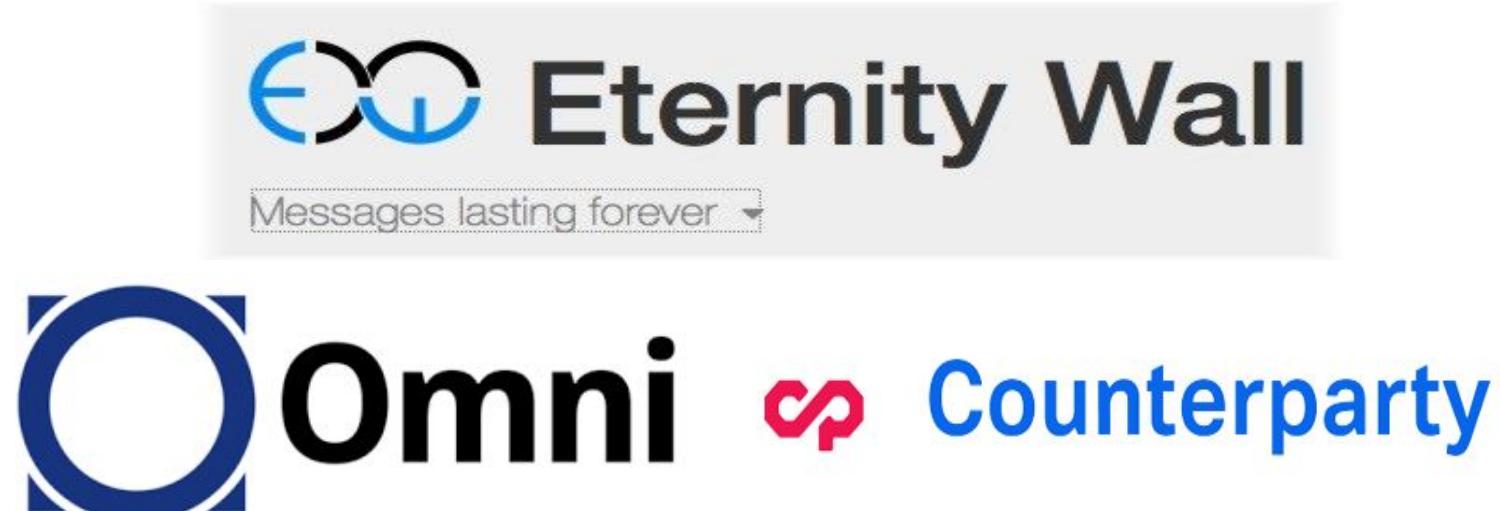
- OSI Model:



OSI Model	TCP/IP Model
Application Layer	Application layer
Presentation Layer	
Session Layer	
Transport Layer	Transport Layer
Network Layer	Internet Layer
Data link layer	
Physical layer	Link Layer

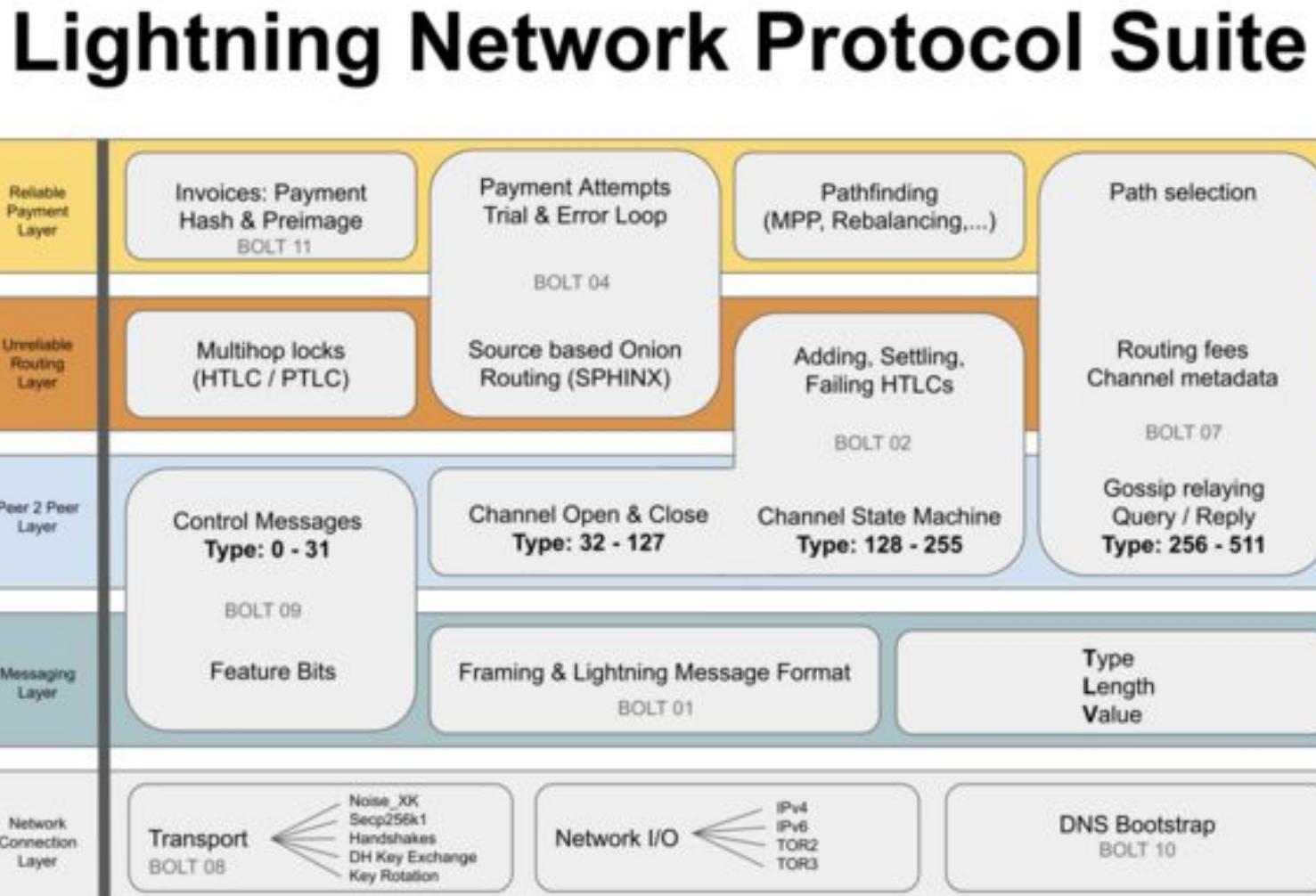
“Reinterpretation Layers” on top of Bitcoin:

- Colored Coins
 - “Color” = asset class
 - USD
 - TWD
 - ...
- Eternity Wall
- Meta-protocols



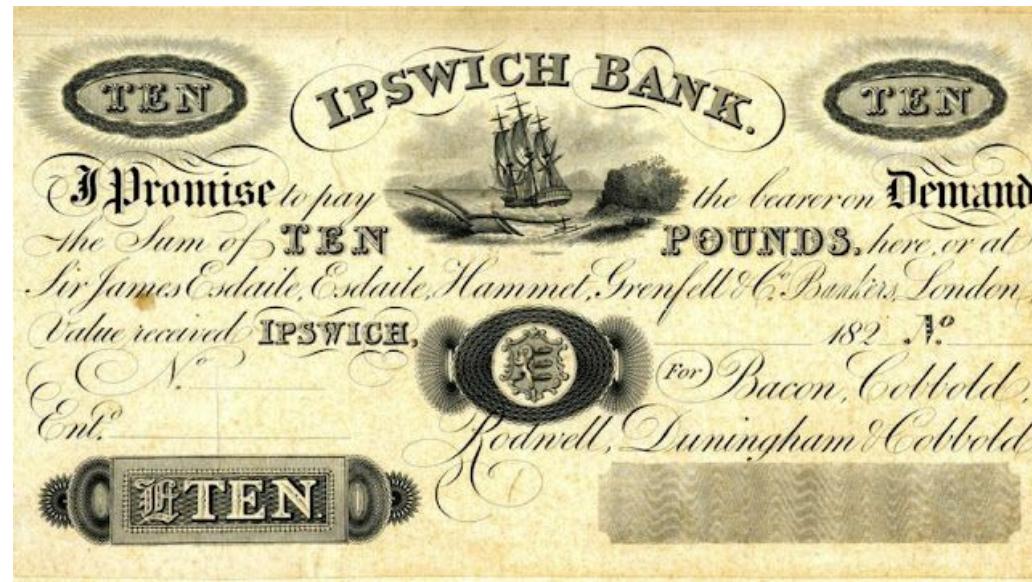
“Omission Layers” on top of Bitcoin:

- Payment channels
- Lightning routing
- Alternative designs
 - Eltoo
 - Ark
 - Hierarchical channels
 - etc.



Differences with Credit:

- Valid transactions
- Delayed publication
- Trustless security*



Hal
VIP
Sr. Member

Activity: 314
Merit: 1003

Re: Bitcoin Bank
December 30, 2010, 01:38:40 AM
Merited by mindrust (10), TheNewAnon135246 (5), LoyceV (3), ETFbitcoin (1), wh1rlw1nd (1), DireWolfM14 (1), stortz (1), BitcoinCoreBTCC (1) #10

Actually there is a very good reason for Bitcoin-backed banks to exist, issuing their own digital cash currency, redeemable for bitcoins. Bitcoin itself cannot scale to have every single financial transaction in the world be broadcast to everyone and included in the block chain. There needs to be a secondary level of payment systems which is lighter weight and more efficient. Likewise, the time needed for Bitcoin transactions to finalize will be impractical for medium to large value purchases.

Bitcoin backed banks will solve these problems. They can work like banks did before nationalization of currency. Different banks can have different policies, some more aggressive, some more conservative. Some would be fractional reserve while others may be 100% Bitcoin backed. Interest rates may vary. Cash from some banks may trade at a discount to that from others.

George Selgin has worked out the theory of competitive free banking in detail, and he argues that such a system would be stable, inflation resistant and self-regulating.

I believe this will be the ultimate fate of Bitcoin, to be the "high-powered money" that serves as a reserve currency for banks that issue their own digital cash. Most Bitcoin transactions will occur between banks, to settle net transfers. Bitcoin transactions by private individuals will be as rare as... well, as Bitcoin based purchases are today.

Hybrid ideas:

- Opendime (HSM)
- Cashu (Chaum)
- Fedimint (Chaum, Federation)
- Liquid (Federation, HSM, Confidential Assets)
- RGB (“RGBTC”???, Issuance)

- This lecture starts with Blockchain & its root in classical economics (scarcity, inflation fraud, future uncertainty) and cyberpunks (privacy, “肉食者鄙 未能遠謀”).
- Blockchain is internet of value and the value comes from consensus. (Friedman)
- (正本清源) After 5w1h, this lecture must end with consensus:

Consensus Mechanisms

PoW vs PoS (and PoA, PoP, PouW, PoT, etc.)

Consensus mechanisms:

WHAT?

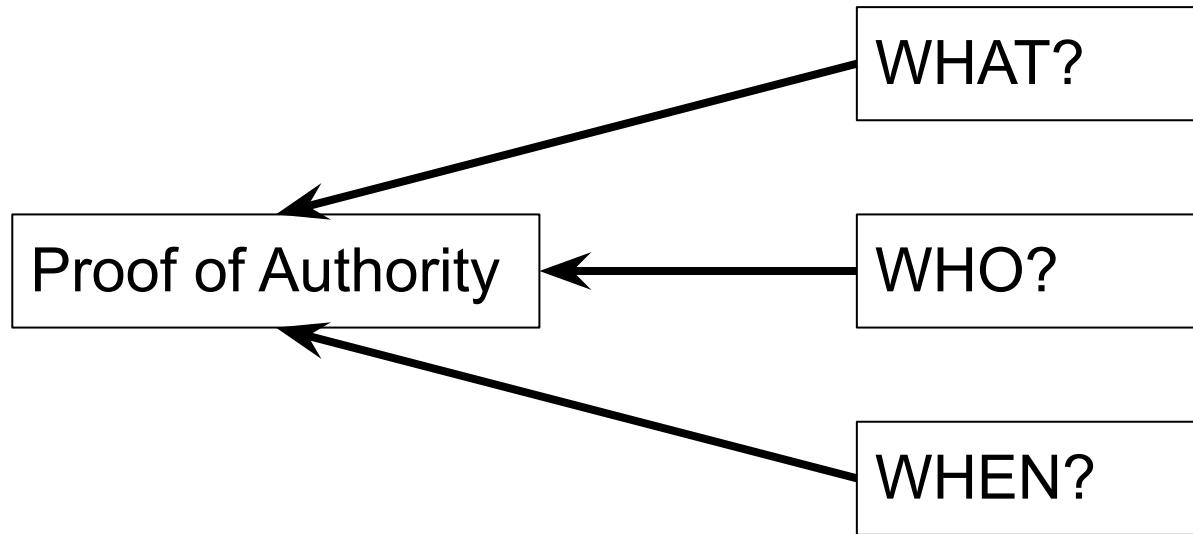
WHO?

WHEN?

CENTRALIZATION

DECENTRALIZATION

Consensus mechanisms:

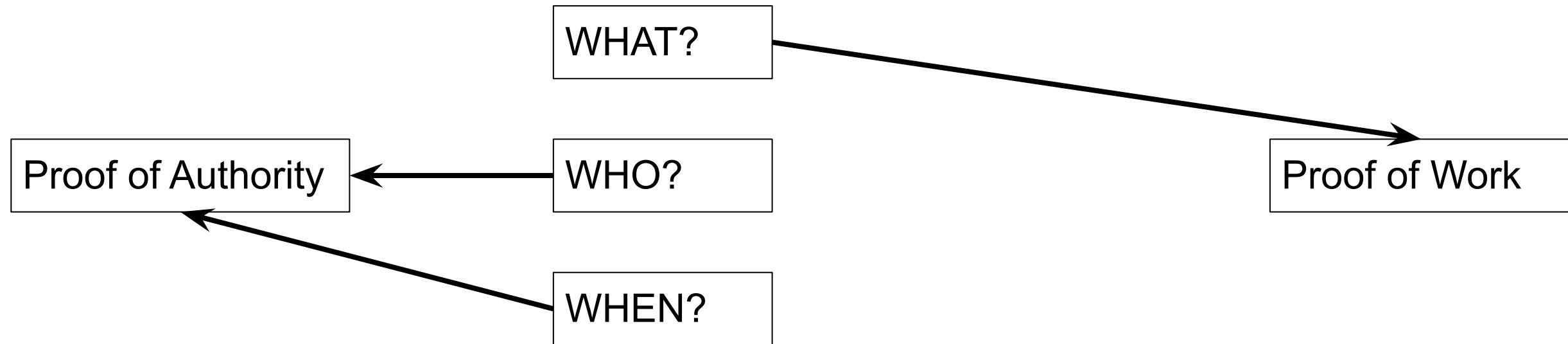


CENTRALIZATION

Es: e-gold, 1996

DECENTRALIZATION

Consensus mechanisms:

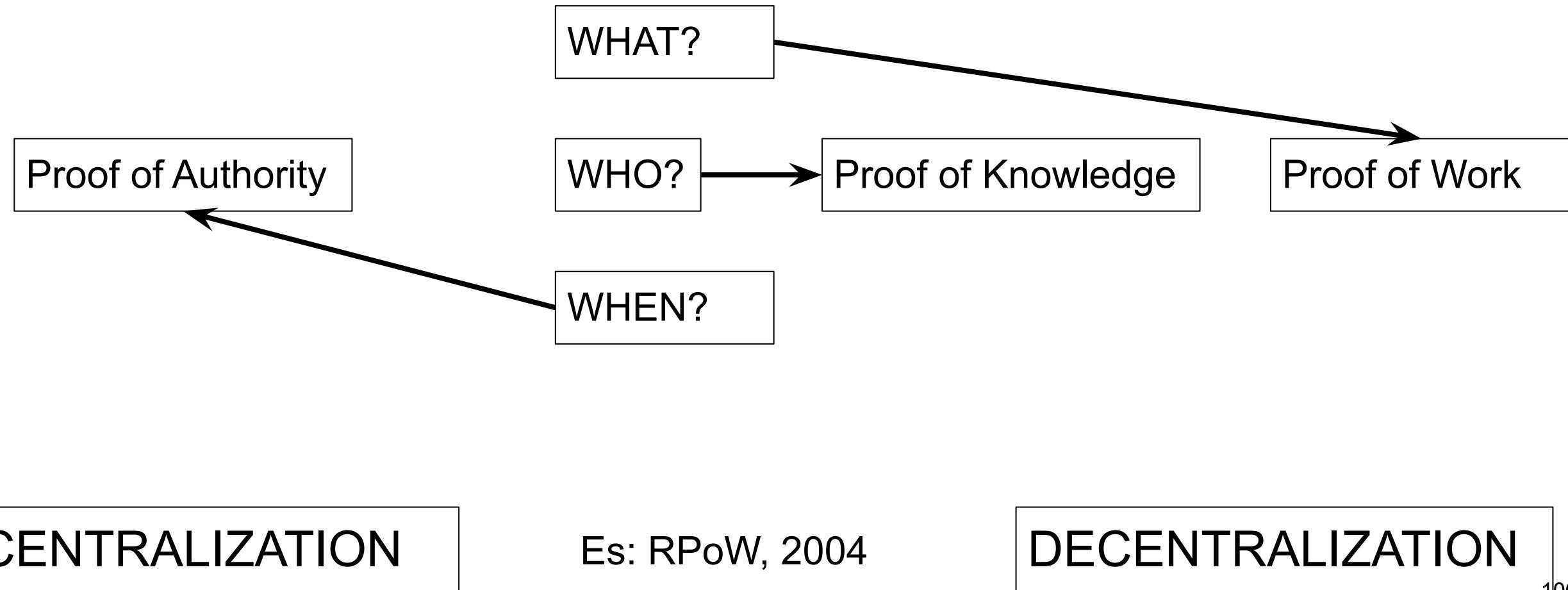


CENTRALIZATION

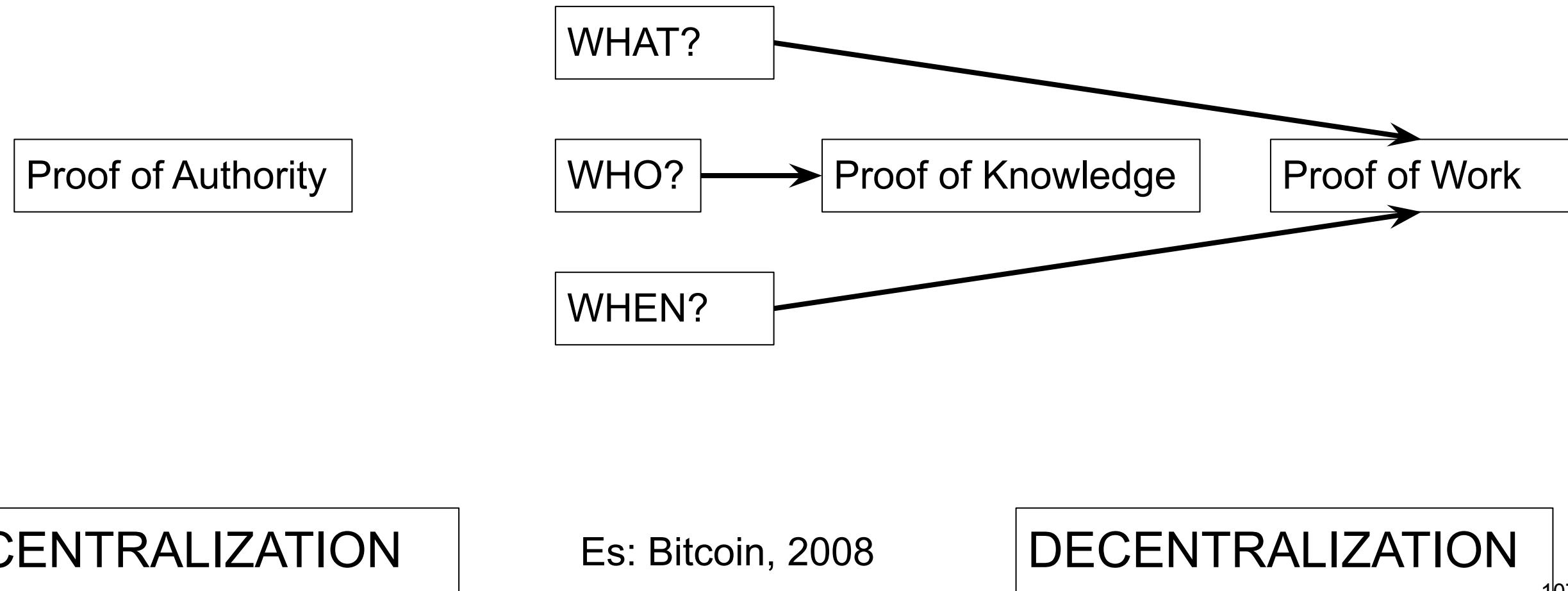
Es: hashcash, 1997

DECENTRALIZATION

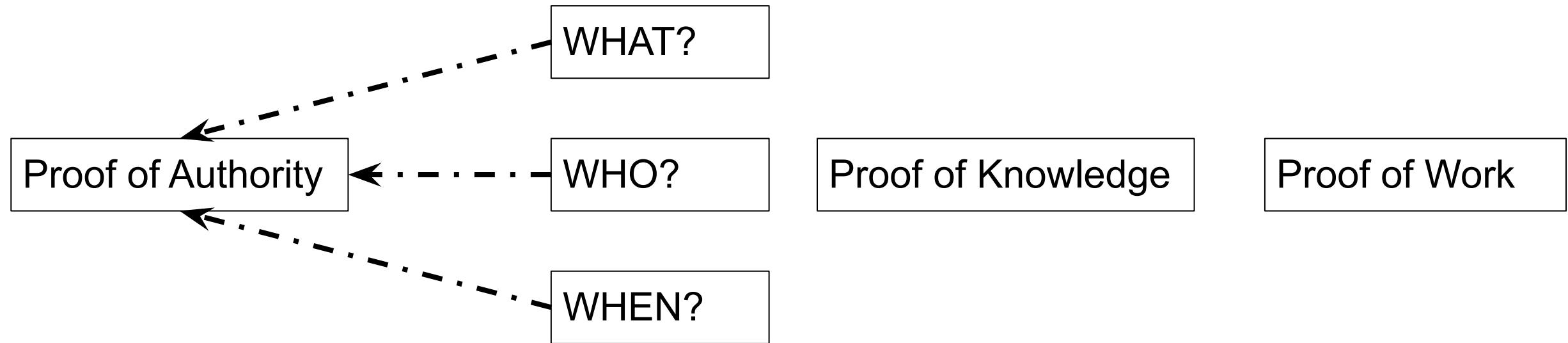
Consensus mechanisms:



Consensus mechanisms:



Consensus mechanisms:



CENTRALIZATION

Es: “crypto”, >2013

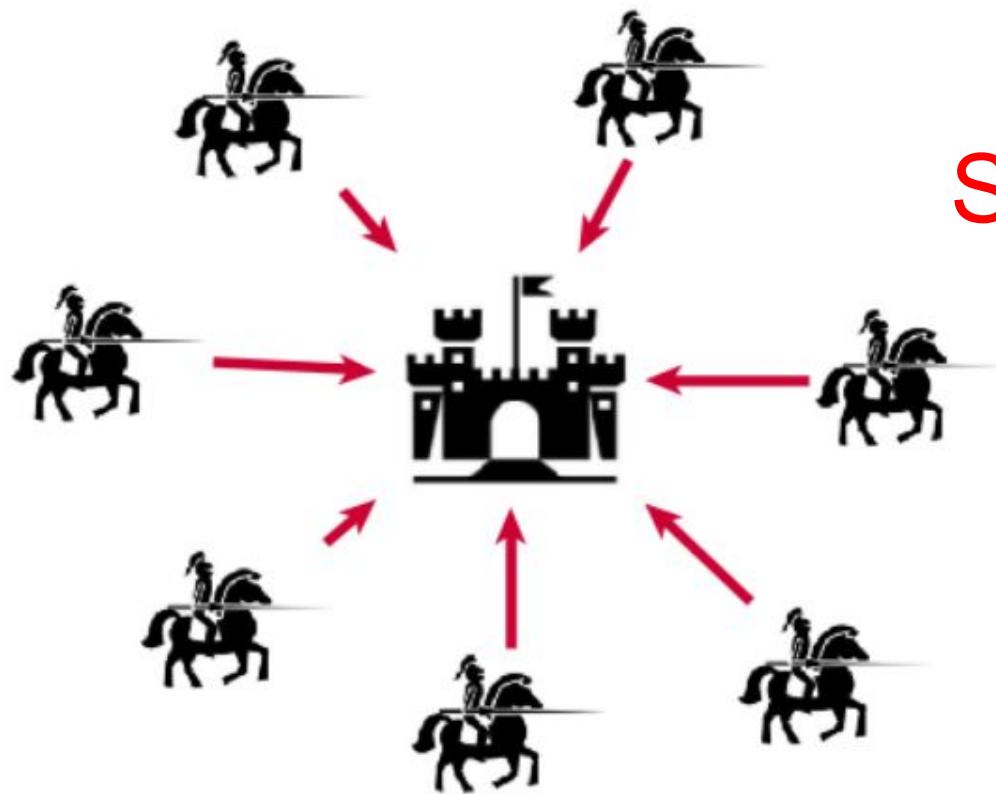
DECENTRALIZATION

Proof of Work criticisms

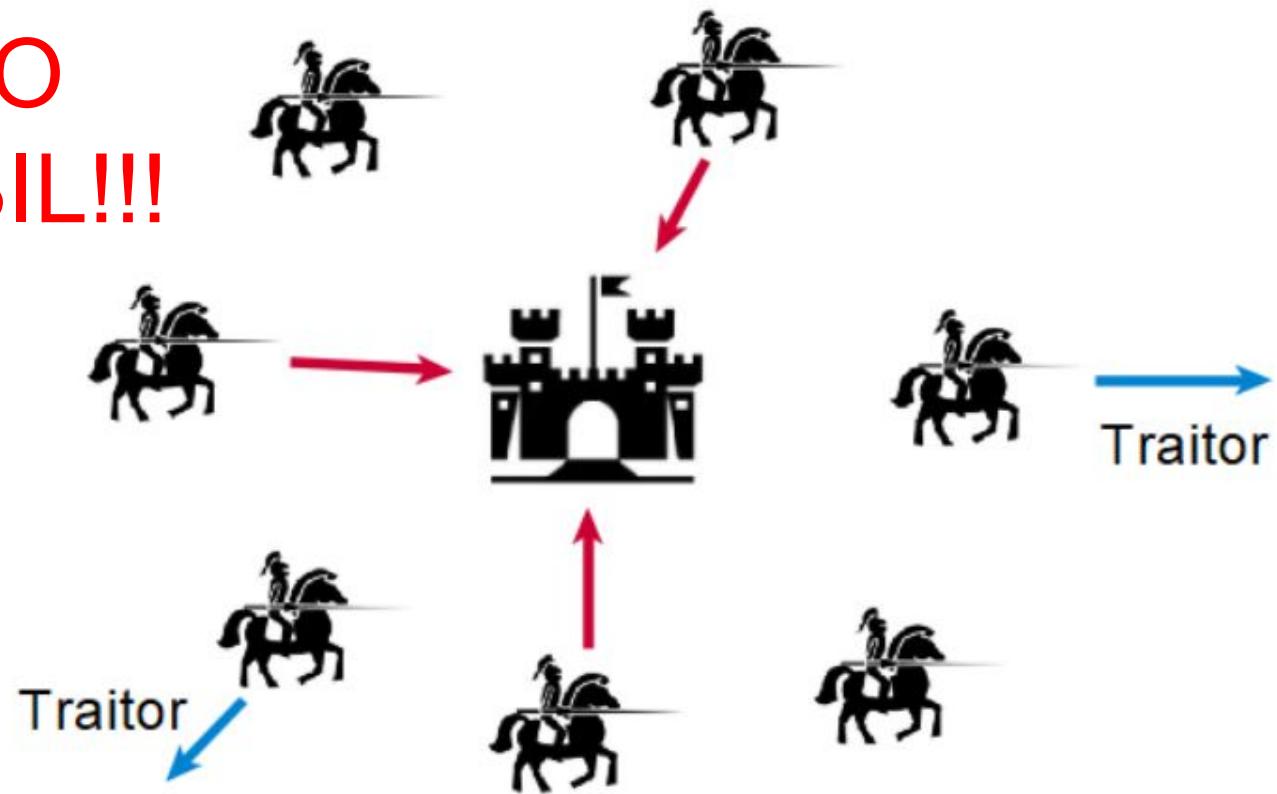
- Hashrate majority control = centralization? (WHEN)
 - Miners don't decide validity, only chronology
 - Fee mechanism to counteract censorship
 - Vested interest in coins and chips (but shorting?)
 - Diseconomies of scale in mining (but chip production?)
- Energy consumption = waste? (WHAT/WHEN)
 - Production vs consumption
 - Cost is the goal, not an accident
 - Consumption of alternatives
 - Efficiency effects of Bitcoin

Source	Synchrony	Authentication	Threshold	Rounds	Notes
Pease-Shostak-Lamport [10]	Synchronous	Oral	$n > 3f$	$f + 1$	total communication $O(n^f)$
Pease-Shostak-Lamport [10]	Synchronous	Written	$n > f + 1$	$f + 1$	total communication $O(n^f)$
Ben-Or [20]	Asynchronous	Oral	$n > 5f$	$O(2^n)$ (expected)	expected $O(1)$ rounds when $f < \sqrt{n}$
Dolev et al. [21]	Synchronous	Oral	$n > 3f$	$2f + 3$	total communication $O(f^3 \log f)$
Dolev-Strong [2]	Synchronous	Written	$n > f + 1$	$f + 1$	total communication $O(n^2)$
Dolev-Strong [2]	Synchronous	Written	$n > f + 1$	$f + 2$	total communication $O(nf)$
Feldman-Micali [22]	Synchronous	Oral	$n > 3f$	$O(1)$ (expected)	
Katz-Koo [23]	Synchronous	Written	$n > 2f$	$O(1)$ (expected)	Requires Public Key Infrastructure (PKI)
PBFT [24]	Asynchronous (safety) Synchronous (liveness)	Oral	$n > 3f$		
HoneyBadger [25]	Asynchronous	Oral	$n > 3f$	$O(\log n)$ (expected)	per tx communication $O(n)$ - requires public-key encryption
Abraham et al. [26]	Synchronous	Written	$n > 2f$	8	
Byzantine Agreement Made Trivial [27][28]	Synchronous	Signatures	$n > 3f$	9 (expected)	Requires digital signatures

**NO
SYBIL!!!**



**Coordinated attack
leading to victory**



**Uncoordinated attack
leading to defeat**

- Old alternatives (with new names)
 - Proof of Stake (WHEN)
 - direct, delegated/leased/liquid/BFT
 - First proposal: Dai 1998

In the second protocol, the accounts of who has how much money are kept by a subset of the participants (called servers from now on) instead of everyone. These servers are linked by a Usenet-style broadcast channel. The format of transaction messages broadcasted on this channel remain the same as in the first protocol, but the affected participants of each transaction should verify that the message has been received and successfully processed by a randomly selected subset of the servers.

Since the servers must be trusted to a degree, some mechanism is needed to keep them honest. Each server is required to deposit a certain amount of money in a special account to be used as potential fines or rewards for proof of misconduct. Also, each server must periodically publish and commit to its current money creation and money ownership databases. Each participant should verify that his own account balances are correct and that the sum of the account balances is not greater than the total amount of money created. This prevents the servers, even in total collusion, from permanently and costlessly expanding the money supply. New servers can also use the published databases to synchronize with existing servers.

The protocol proposed in this article allows untraceable pseudonymous entities to cooperate with each other more efficiently, by providing them with a medium of exchange and a method of enforcing contracts. The protocol can probably be made more efficient and secure, but I hope this is a step toward making crypto-anarchy a practical as well as theoretical possibility.

- Old alternatives (with new names)
 - Proof of Stake (WHEN)
 - direct, delegated/leased/liquid/BFT
 - First proposal: Dai 1998
 - Problem: circular
 - “Crypto” reboot: Peercoin, Ethereum (PoW/PoA)

- Old alternatives (with new names)
 - Proof of Stake (WHEN)
 - direct, delegated/leased/liquid/BFT
 - First proposal: Dai 1998
 - Problem: circular
 - “Crypto” reboot: Peercoin, Ethereum (PoW/PoA)
 - Proof of Personhood (WHAT, WHEN)
 - Variants: off-line, WoT
 - First proposal: Ford 2008

Home > Conferences > EUROSYS > Proceedings > SocialNets '08 > An offline foundation for online accountable pseudonyms

RESEARCH-ARTICLE



An offline foundation for online accountable pseudonyms

Authors:  Bryan Ford,  Jacob Strauss [Authors Info & Claims](#)

SocialNets '08: Proceedings of the 1st Workshop on Social Network Systems • April 2008 • Pages 31–36

- <https://doi.org/10.1145/1435497.1435503>

Published: 01 April 2008 [Publication History](#)



- Old alternatives (with new names)
 - Proof of Stake (WHEN)
 - Variants: direct, delegated/leased/liquid/BFT
 - First proposal: Dai 1998
 - Problem: circular
 - “Crypto” reboot: peercoin, ethereum (PoW/PoA)
 - Proof of Personhood (WHAT, WHEN)
 - Variants: off-line, WoT
 - First proposal: Ford 2008
 - Problem: impractical
 - “Crypto” reboot: Encointer, Worldcoin (PoA)

- New alternatives in “Crypto”
 - Proof of Useful Work (WHAT/WHEN)
 - Primecoin, 2013
 - ICP, 2021
 - Proof of Time and Space (WHAT/WHEN)
 - Burstcoin/Signum, 2013 (PoSp)
 - Hyperledger, 2016 (PoET)
 - Chia, 2021 (PoST)
 - Proof of Storage (WHAT)
 - Storj, 2014
 - Siacoin, 2015
 - Filecoin, 2017

- Possibly useful alternatives for Bitcoin
 - WHAT: Proof of Burn
 - Spacechains (Somsen 2020)
 - WHEN: “Proof of Collapse”?
 - Quantum Money (Wiesner 1970)
 - PoA/PoS/PoP/PoSt/PoT/PoSp for other purposes
 - Liquid (PoA)
 - JM fidelity bond, LN channel announcement (PoS)
 - bitcoin-otc WoT, Vexl WoT (PoP)
 - STORM (PoSt)

Q&A

Questions:

- 所謂“金融科技ABCD”不包含以下何者?
AI (人工智慧)
Blockchain (區塊鏈)
Cloud computing (雲計算或雲端計算)
Dark pool (暗池交易)
- 區塊是一串使用密碼學方法相關連產生的資料塊. 新增的資料塊可以連結到前一個區塊 形成一條類似鏈狀的資料串的尾部
這整條資料串被稱作?
礦池
比特幣
挖礦
區塊鏈
- 智能合約(Smart Contracts)是:
區塊鏈中的虛擬貨幣
應用於區塊鏈的智能手機應用程式
自動執行的合約條款
區塊鏈的密碼學算法

Questions

- 共識機制(Consensus Mechanism)用於：
確定區塊鏈中的交易順序
加密區塊鏈中的數據
維護區塊鏈網絡的安全性
壓縮區塊鏈中的數據大小
- 跨域或跨界可適合使用區塊鏈的場景 不包含以下何者?
碳權
國際匯兌
國際證照認證
鄰居理髮店的折價券
- 以金融科技可分析的各種資料, 何者正確? 選最適合選項.
保險:精算保費
證券:投資組合
銀行貸款:客戶信用評分
以上皆是

Questions

- 區塊鏈是一種: 以下選最適合選項
加密算法
分散式帳本技術
雲端儲存服務
社交媒体平台
- 區塊鏈技術的核心特點是
高度隱私保護
高速交易處理
多中心化
中央控制權
- FTX事件加深很多對區塊鏈的誤解 下列何種不屬於那些誤解?
區塊鏈是一個中心化帳本如FTX
區塊鏈一種交易所如FTX
區塊鏈是一種虛擬幣如FTT
區塊鏈是一種在點對點網路上運行的分散式帳本

Questions

- 在所謂“Web3黑暗森林”中，你可能會遭遇到甚麼危險? 選最適合選項.

智能合約風險

釣魚攻擊

Rug Pulls (軟地毯詐騙)

以上皆是

- Web3特點不包含以下何者?

Users can read

Users can write

Users can own

Users can arbitrage

- 區塊鏈是第二代互聯網 有第一代連結, 但其不包含以下何者?

Internet of information

Internet of value

Trust machine

Gambling machine

Questions

- 很多人搞混區塊鏈與資料庫 下列何者最真?

區塊鏈是一種不可儲存隱私證明的資料庫

區塊鏈是帳本 所以區塊鏈是又貴又慢的資料庫

資料庫是集中式 而區塊鏈是分散式

區塊鏈比資料庫更重視彼此信任問題

- 區塊鏈應用不包含以下何者?

供應鏈區塊鏈

台灣司法聯盟鏈

食品溯源

人臉辨識

- imB借貸平台詐騙25億. 對比imB, 區塊鏈上之借貸平台強調的好處為何? 選最適合選項.

除去中間人

透明度與安全性

能找到較低利率借你錢的人

以上皆是

Questions

- 將區塊鏈技術純粹運用到產業界中，而非單純發幣，此類的應用屬於哪一種領域？

礦圈

幣圈

鏈圈

以上皆是

- 區塊鏈技術又稱為DLT，DLT是指？

Digital Ledger Technology

Digital Layer Technology

Distributed Ledger Technology

Distributed Layer Technology

- 比特幣區塊鏈中所謂的「挖礦」是指？

與其他節點競爭交易權

與其他節點競爭軟體的下載權

與其他節點競爭轉帳權

與其他節點競爭記帳權

Questions

- 比特幣的全套帳本 置放在何處?
任何一個全節點
礦池
只放在參與挖礦的礦工節點
交易池
- 基於區塊鏈技術上的P2P貸款，以下哪個是最主要的風險? 選最適合選項.
技術風險 (technical)
拖欠行為的風險 (default)
利率風險 (interest rate)
以上皆是
- 由於沒有做好風險控管, 假設你有朋友在FTX事件中損失慘重。請問誰最該為此負責?
培訓中心
FTX交易所的對手CZ
FTX交易所的創辦人SBF
該朋友自己

Questions

- 眾多區塊鏈交易平台皆提供號稱自動化智慧化機器人下列何者敘述為非?
可以免除人的情緒影響
通過數據分析，利用演算法發現人類難以發現的機會
是絕對獲利的保證
以上皆非
- 區塊鏈技術對於金融業務應用的重大影響與效益有交易過程扁平化，降低複雜度及成本共同執行可信賴的流程
是實現共享金融的有力工具驅動新型商業模式的誕生；以及下列何者？
取代現有的資料庫結構
降低信任風險
集中式的層級處理架構
系統的不可追溯性
- 下列哪一個不是使用智能合約技術?
The DAO
Nexus Mutual insurance
Ubuntu 作業系統
以太坊合約

Questions

- 下列哪一個在台灣的保險方案最早使用區塊鏈並獲得保險卓越獎?

防疫險

旅遊險

投資型保單

年金保險

- 下列哪一項特點 不是區塊鏈所擁有的?

不可否認性

不可篡改性

以集體共識維護帳本的安全

以上皆非

- 有關區塊鏈技術敘述何者正確?

每筆交易紀錄都會隨機抽樣對照過去交易進行查核

是一種公開分散、依照時序(ordering)順序的可被驗證資料結構

不斷驗證並鏈結區塊的過程使個人可以重複使用同一錢幣，但數位偽造會被排除

有集中式驗證中心

Questions

- 下列哪個選項「不是」區塊鏈技術的創新革命的特點
資料(數據)儲存的結構格式與一般不同
信任的一種革命創新
非對稱金鑰演算法的創新
以上皆是
- 下列何者為 Nexus Mutual Insurance (保險) 背後主要所使用之技術?
IP (網際網路協定)
區塊鏈智能合約
機器學習
類神經網路
- 去中心化保險等項目往往以穩定幣出入金 下列哪種穩定幣不是以實體世界資產支撐?
以法幣支撐之穩定幣
以黃金支撐之穩定幣
以商品支撐之穩定幣
算法穩定幣