Blockchain: building trust one block at a time

Mamy Ratsimbazafy

Ethereum 2 / Nimbus developer @ Status.im

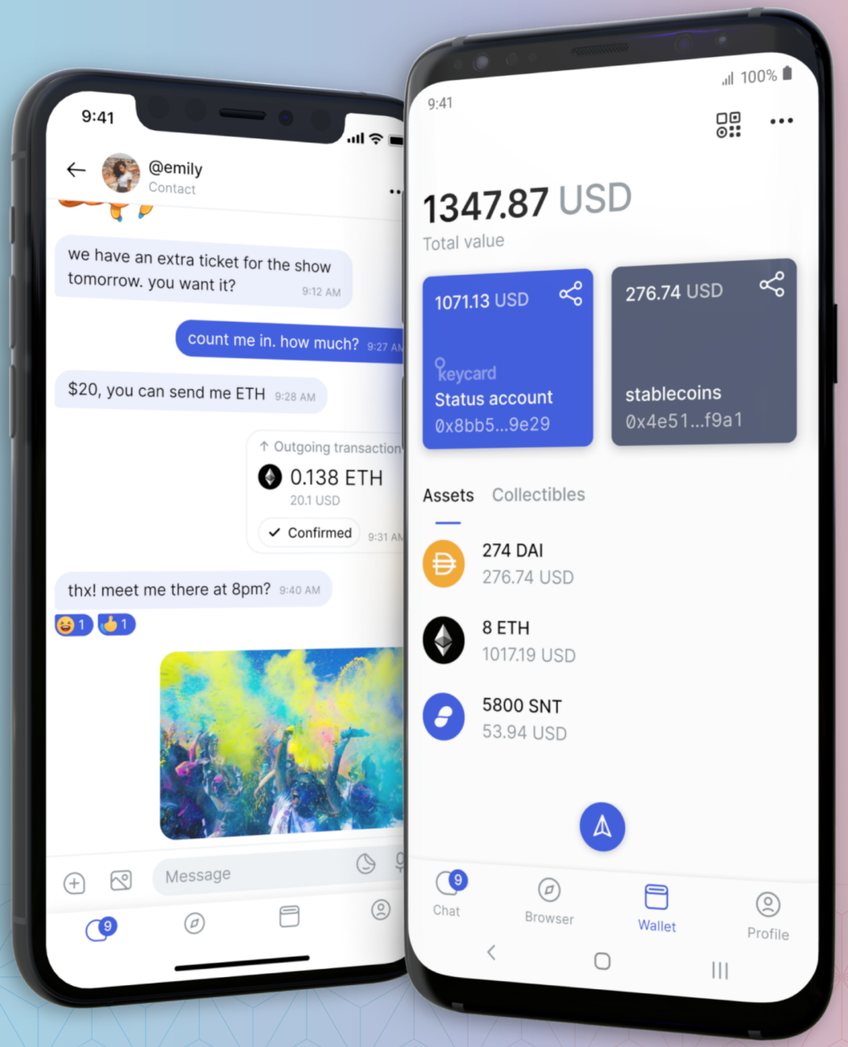
m_ratsim

mratsim

Status focuses on

https://status.im

Products



Developer tools

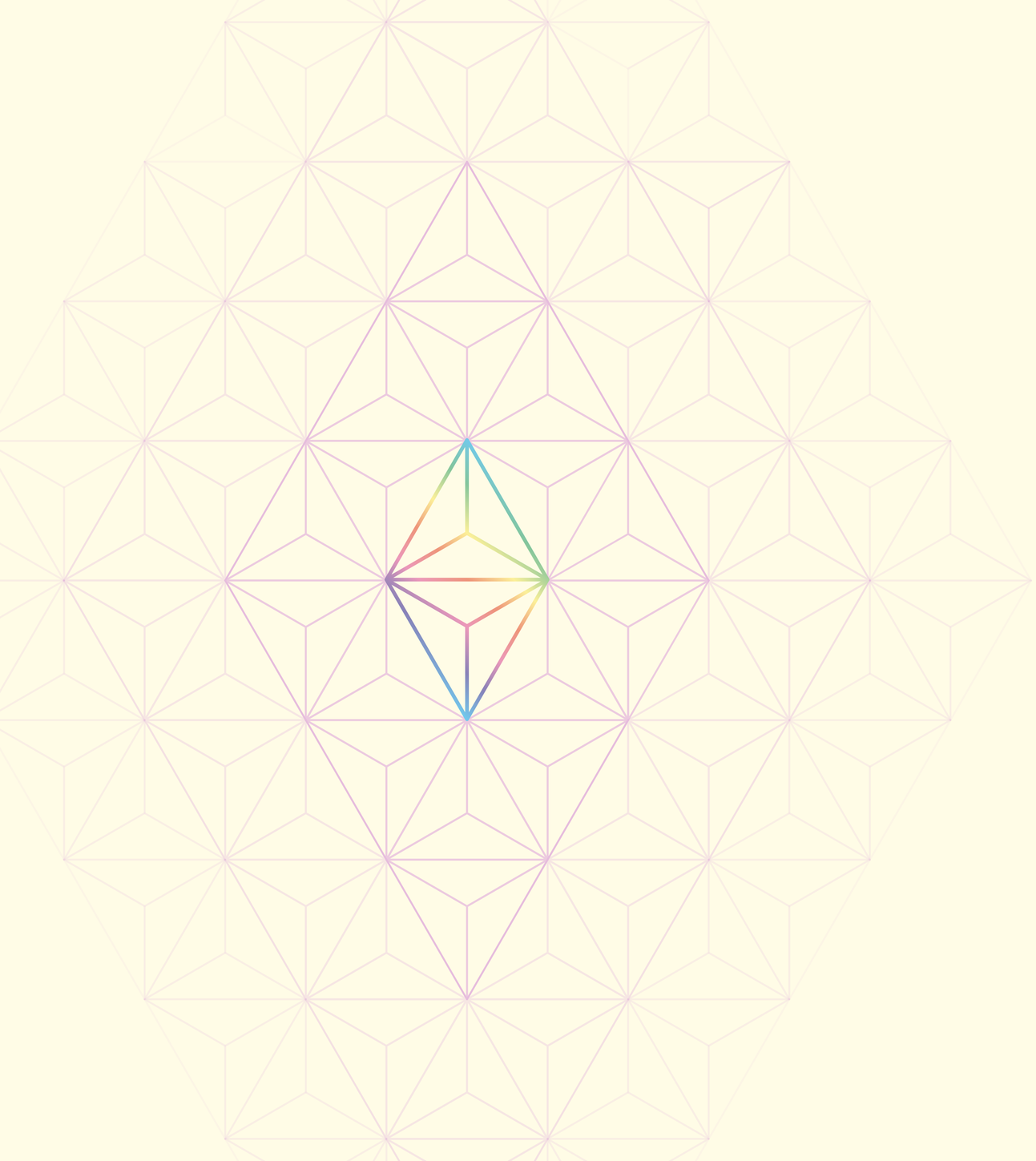
Infrastructure and protocol research

Addressing the decentralized trinity

- Decentralized messaging
- Decentralized consensus
- Decentralized storage

Providing the foundations of a global P2P economy

All open-source and transparent, including meetings and financials



Blockchain prehistory

Blockchain prehistory: digital money

Digital money isn’t a new idea, it has been brewing for over 25 years.

Blockchain prehistory: philosophy

The “philosophy” behind Bitcoin was over 15 years old.

A cryptoanarchist manifesto, 1988

Timothy C. May

“Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures.”

A cypherpunk manifesto, 1992

Eric Hughes

Privacy is the power to selectively reveal oneself to the world.

We must defend our own privacy if we expect to have any.

We cannot expect governments, corporations or other large, faceless organizations to grant us privacy out of their benificence.

We are defending our privacy with cryptography, with anonymous mail-forwarding systems, with digital signatures, and with electronic money.

Our code is free for all to use, worldwide.

We don’t much care if you don’t approve of the software we write.

We know that software can’t be destroyed and that a widely dispersed system can’t be shutdown.

Blockchain prehistory: technology

Your parents may have used the foundation of blockchain P2P technology to access music and movies before streaming was cheap & convenient enough.

Napster, 1999

Popularized P2P file sharing to mainstream.

Bittorrent, 2001

Decentralized, censorship-resistant P2P

Kademlia (eMule), 2002

Distributed hash tables. Further decentralisation, censorship-resistance, faster discovery.

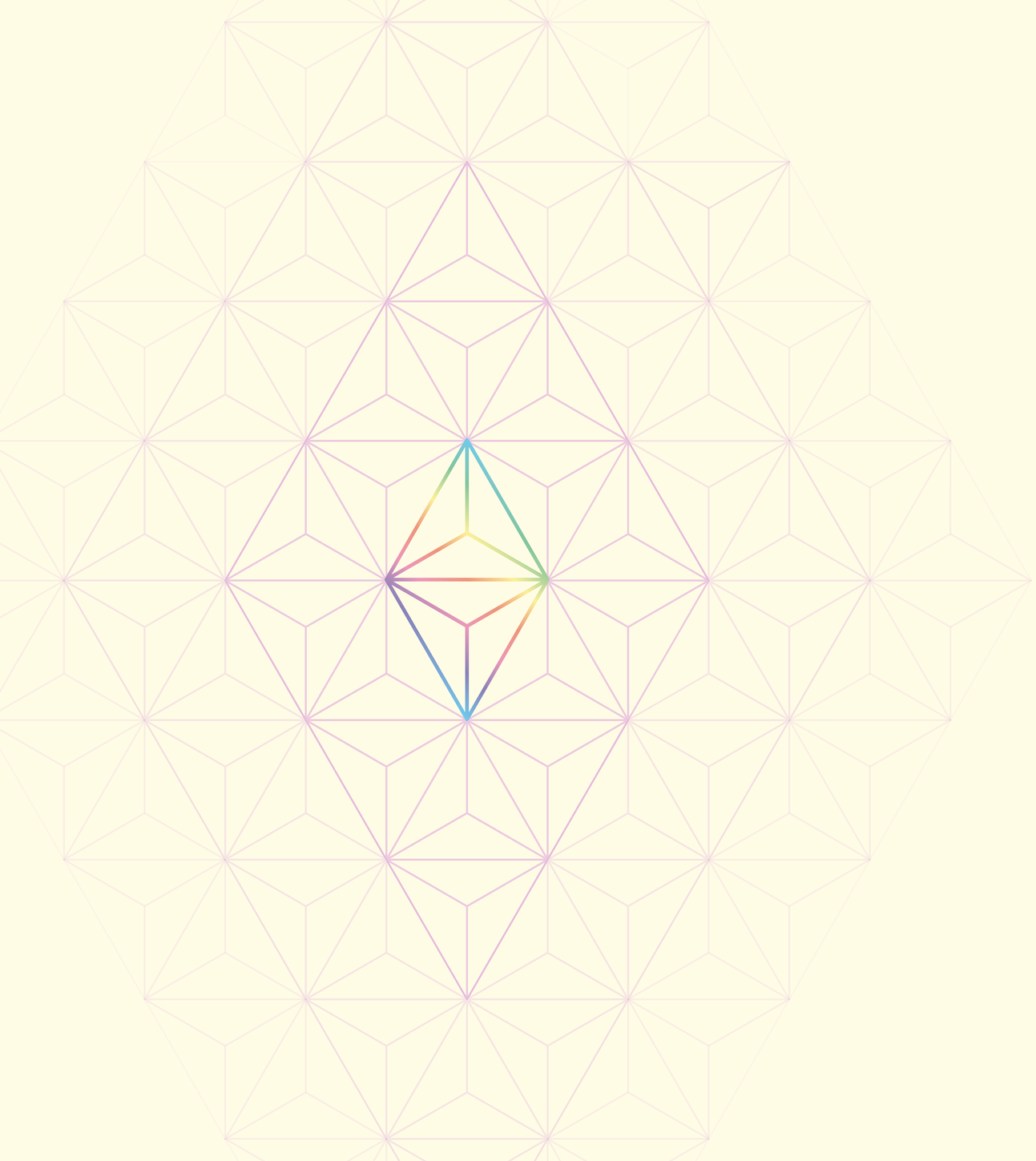
Video games currencies

Castronova in 2001 studied and showed that EverQuest (1999) generates more wealth than some real world countries.

Ultima Online (1997), RuneScape (2001), EVE Online (2003) all had extensive Real Money Trading (RMT).

China used prisoners to farm gold in World of Warcraft (2004).

Players in Korean MMORPGs spend thousands to millions to get an edge (https://www.bizhankook.com/bk/article/21594, 1 player spend 4 billions Korean wons in Lineage ~= $3.6M).



Bitcoin

Bitcoin

Cryptography + Game Theory = cryptoeconomics

Solving the double-spend problem

A blockchain is immutable. An account cannot edit an old transaction to spend the fund elsewhere. Ownership can be proven.

Solving the sybil problem

When getting involved is cheap you get fake identities that spams a protocol. Proof-of-Work makes those impractical and encourage honest behaviour.

Trustlessness & Decentralization

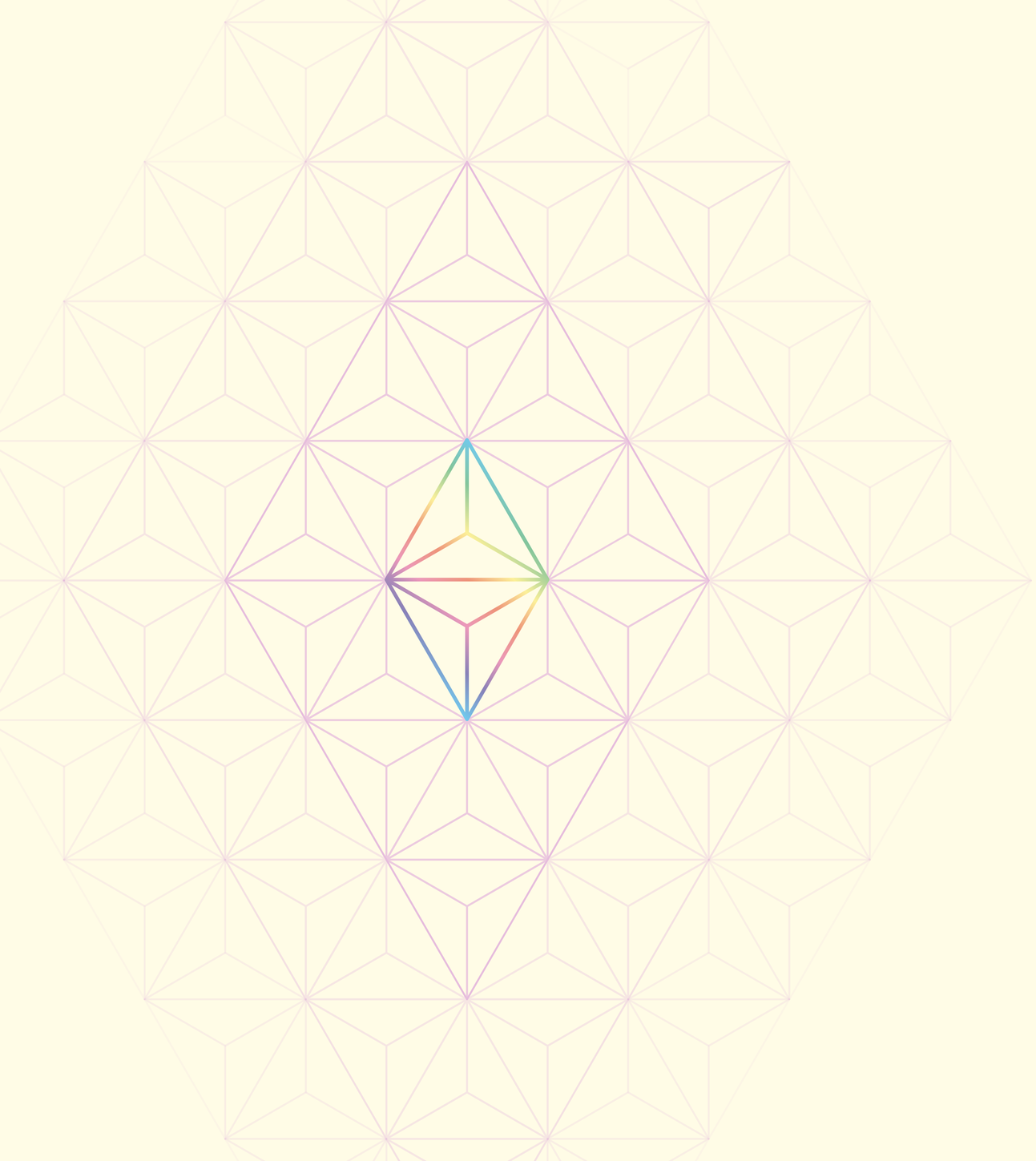
Blockchain history and current state can be computed by following the trail of transactions, proving step by step correctness without a trusted third-party that “certifies” the accounting. Consensus is reached even if there is no trust between parties.

Transparency & Censorship-resistance

The history of transactions is tamper-proof and accessible to everyone.

Permissionless

Anyone can join as long as they follow the rules of the protocol.



Ethereum

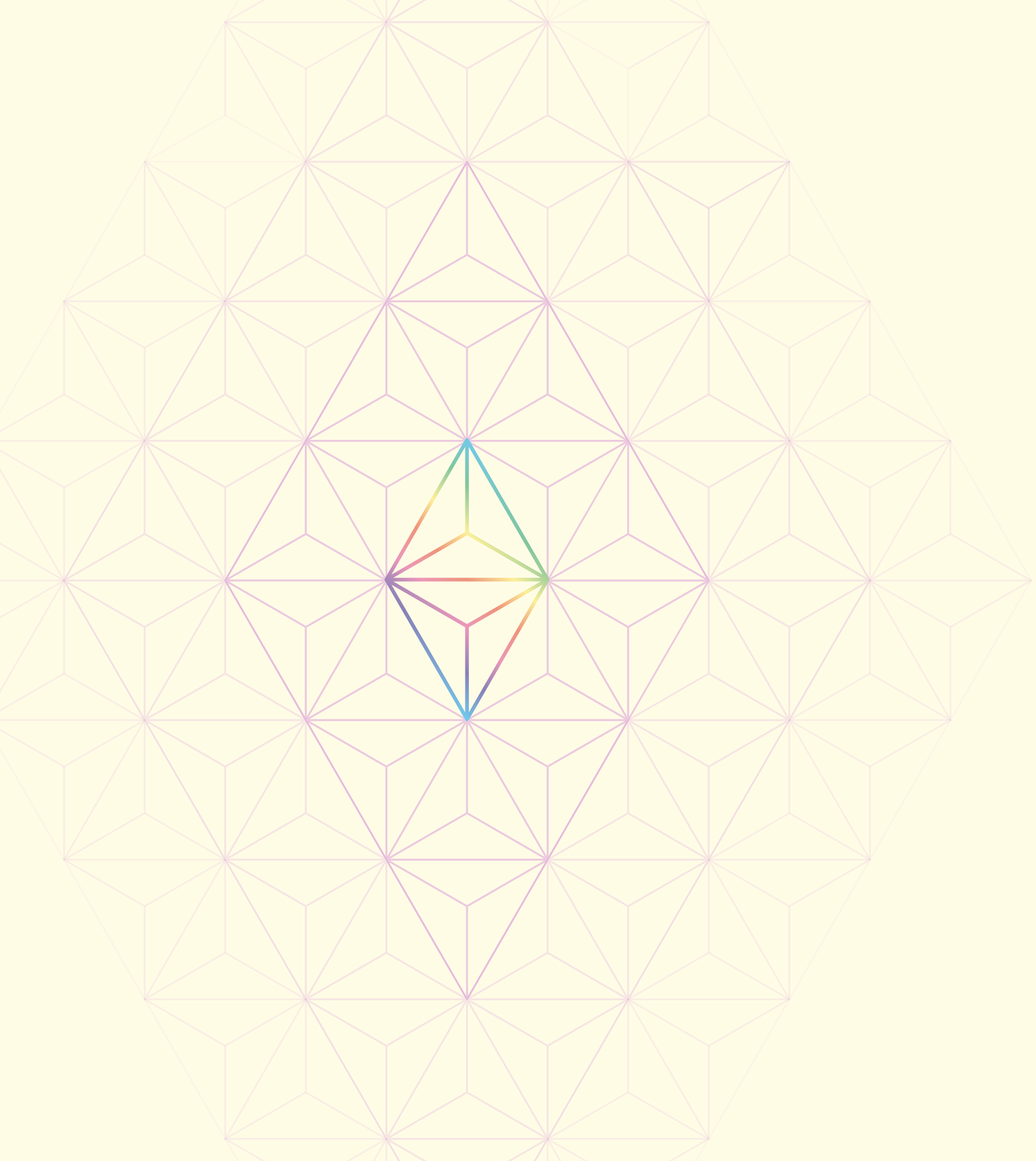
Ethereum

The blockchain is now programmable.

It’s not just about money, you can encode and enforce any rules without lawyers, police, notaries, judges, witnesses or EULA. The rules and their effects are public and not subject to interpretation. Code is law.

Introducing the “smart-contracts”.

4 slides of use-cases incoming



Web 3.0

Web evolution

Web 1.0

Static, hyperlinks, no interactions.

The web 1.0 is dominated by personal pages.

The web 1.0 allows free flow of information.

Web 2.0

Interactive, social.

The web 2.0 is dominated by platforms (and bots).

The web 2.0 allows censorable flow of interactions.

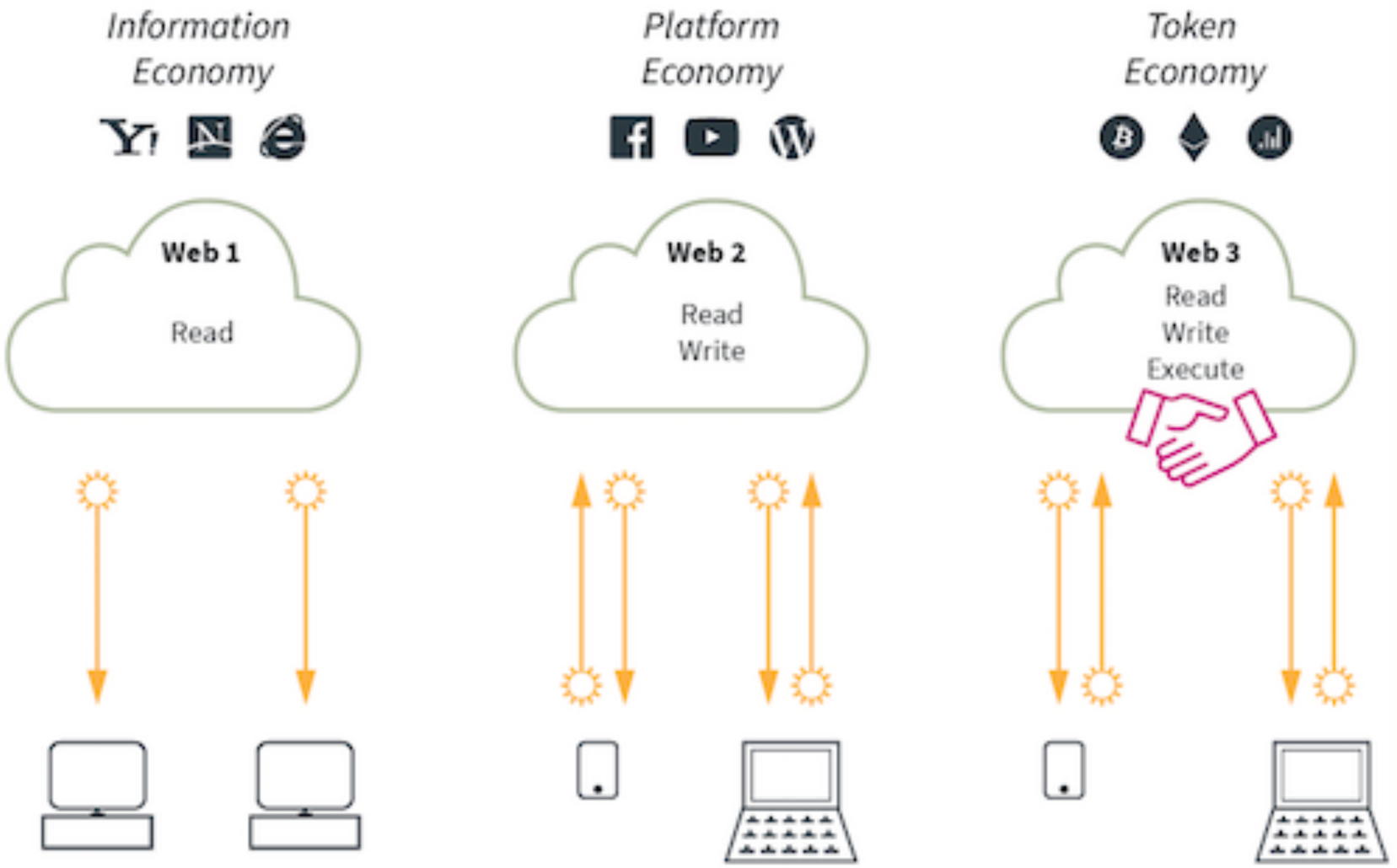
Web 3.0

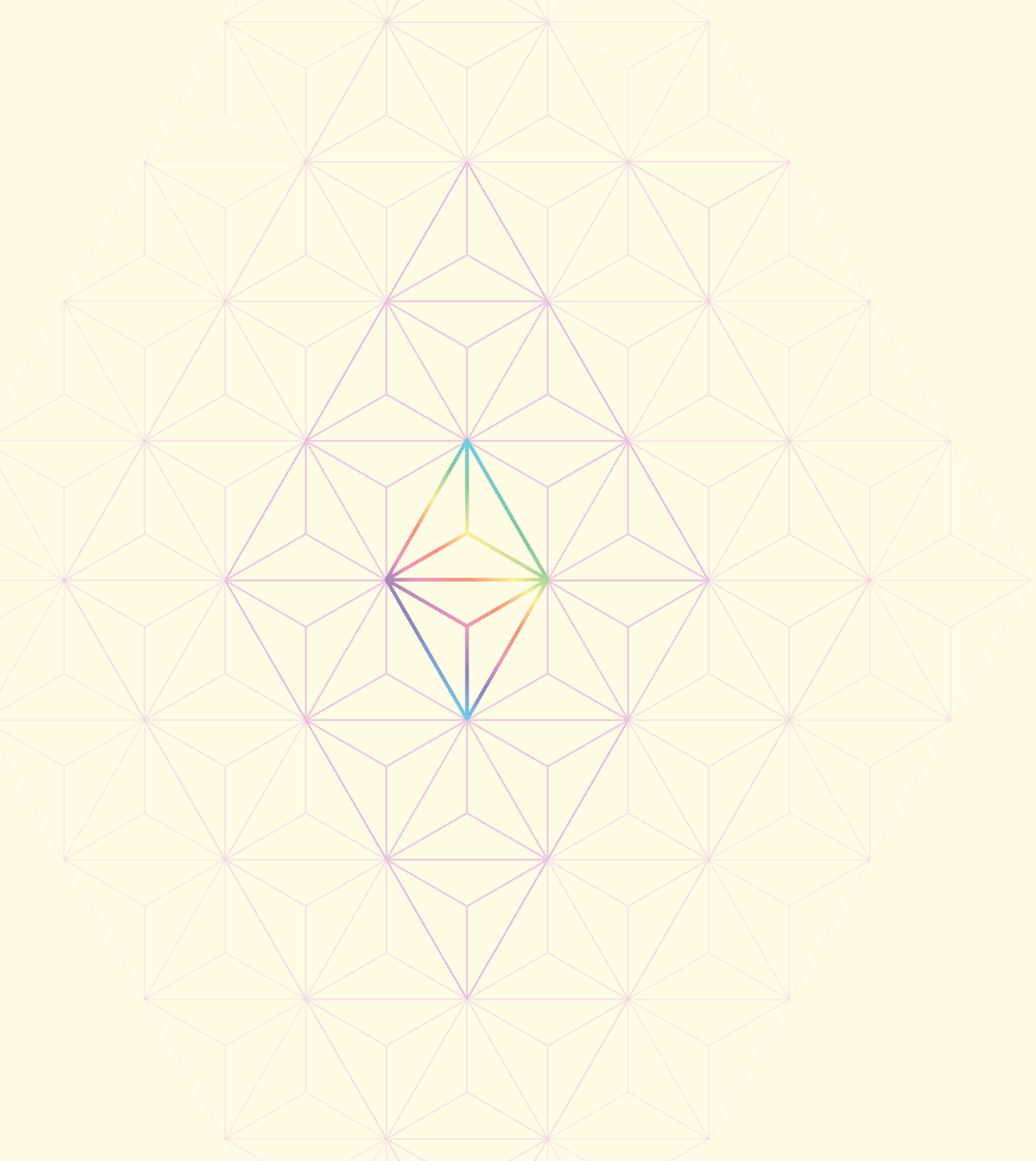
Permissionless, censorship-resistant, transparent.

The web 3.0 allows transactions without the need of a trusted third-party. Transactions are recorded and transparent, removing asymmetry of information.

History of the Web

From the Book "**Token Economy**" by Shermin Voshmgir, 2019
Excerpts available on **https://blockchainhub.net**





Use-cases

Countries in crisis

- Combating hyperinflation (Venezuela, Argentina, Zimbabwe, …)
- Fighting bank withdrawal bans or confiscation of assets.
- Avoiding outsized remittance fees (Western Union, …)

Notes:

- 4G coverage vs landlines
- Forget about desktops, mobile-first
- Paying by SMS is very popular

Transparency & accountability

in royalties-based industries, for charities, public funding or supply chains

Publishing industry

How many books or songs sold? What went to marketing, distribution, to the authors, composers, translators, to shareholders, to taxes? Is it fair?

Charities

Donors can follow the trail of transactions, ensure they are directed to the causes. Inefficiencies can be spotted and addressed. Transparency drives trust.

Public funding

How taxes are used can be consulted by citizens to ensure that their hard work is well used. Funds can be directed through votes that can be tallied publicly.

Food & Luxury

Where did your food or clothes came from? Are they counterfeit? How many hands did it pass through before reaching you?

Decentralized finance

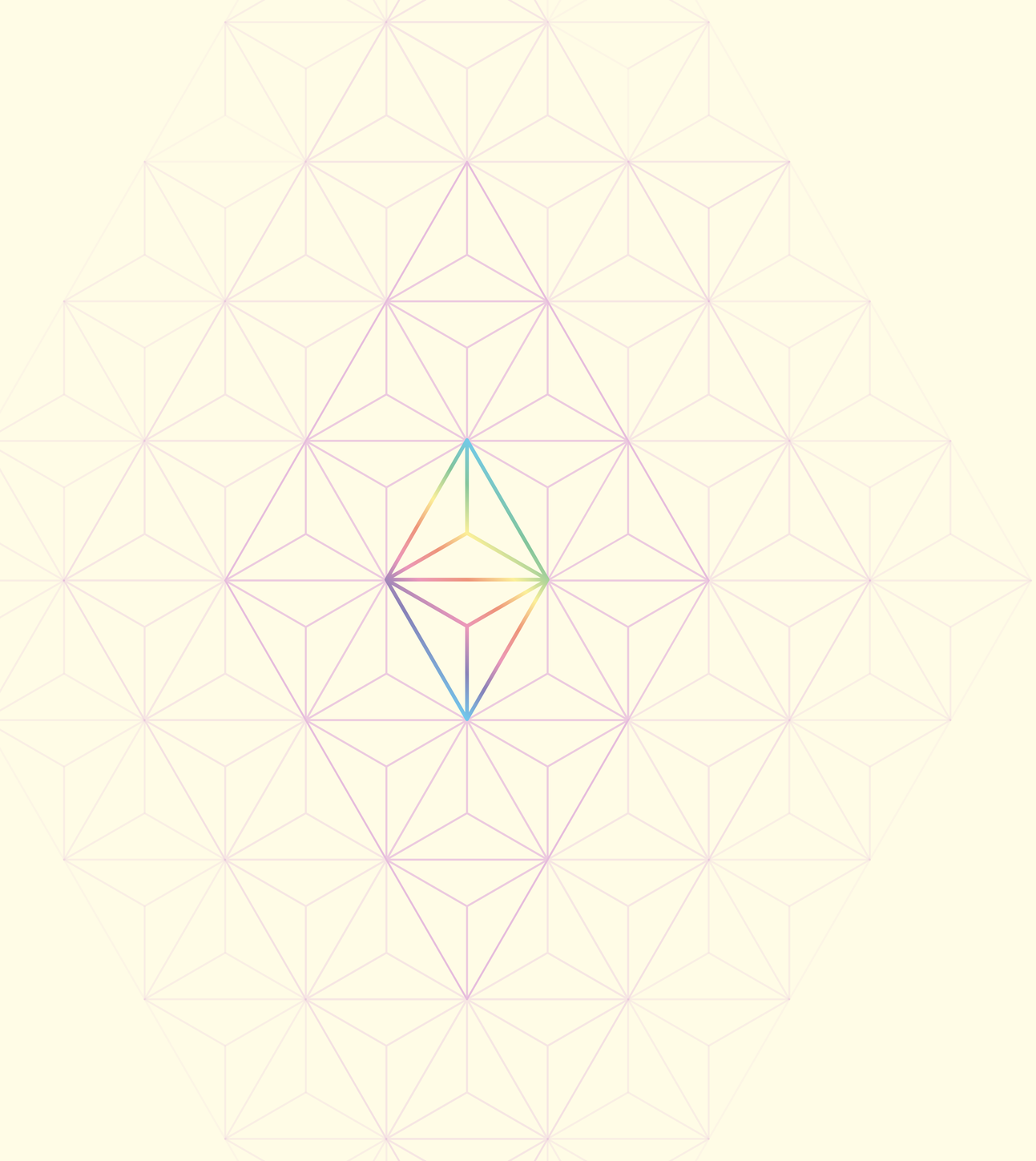
- Lending & borrowing
  - Be your own bank
  - Flashloans
- Decentralized Exchanges (DEX), Market makers, Liquidity Providers (LPs)
- Staking
- Yield farming
- Complex strategies, fund management, futures on yield
- Insurance
- Synthetic stocks

Non-Fungible Tokens (NFTs)

- Credentials, diplomas, proofs of attendance
- Game assets, trading cards, unique skins
- Arts, books, swag, limited edition memes
- Tickets, VIP privileges

The web used to only be able to transfer information in a P2P manner.
With NFTs it can also transfer assets, hence value.

You don’t need to trust your counterparts, only the blockchain.



Naysayers

Bitcoin: criticisms

are very easy to find, so just use your favorite search engine. Some are true, some are because the technology is young, some are FUD (Fear, Uncertainty, Doubt).

Influential counterpoints:

Michael Morell, 33 at the CIA came to 2 conclusions.

- The broad generalizations about the use of bitcoin in illicit finance are significantly overstated.
- Blockchain analysis is a highly effective crime fighting and intelligence gathering tool.

David Andolfatto, Vice President at the Federal Reserve Bank of St. Louis, stated that bitcoin is a threat to the establishment, which he argues is a good thing for the Federal Reserve System and other central banks, because it prompts these institutions to operate sound policies.

Standardized building blocks and programmability can quickly lead us in very unexpected directions

Credits: u/pbrody

Digital Building Blocks

- Technology building blocks that came into being independently but could be used together

Predictable Results

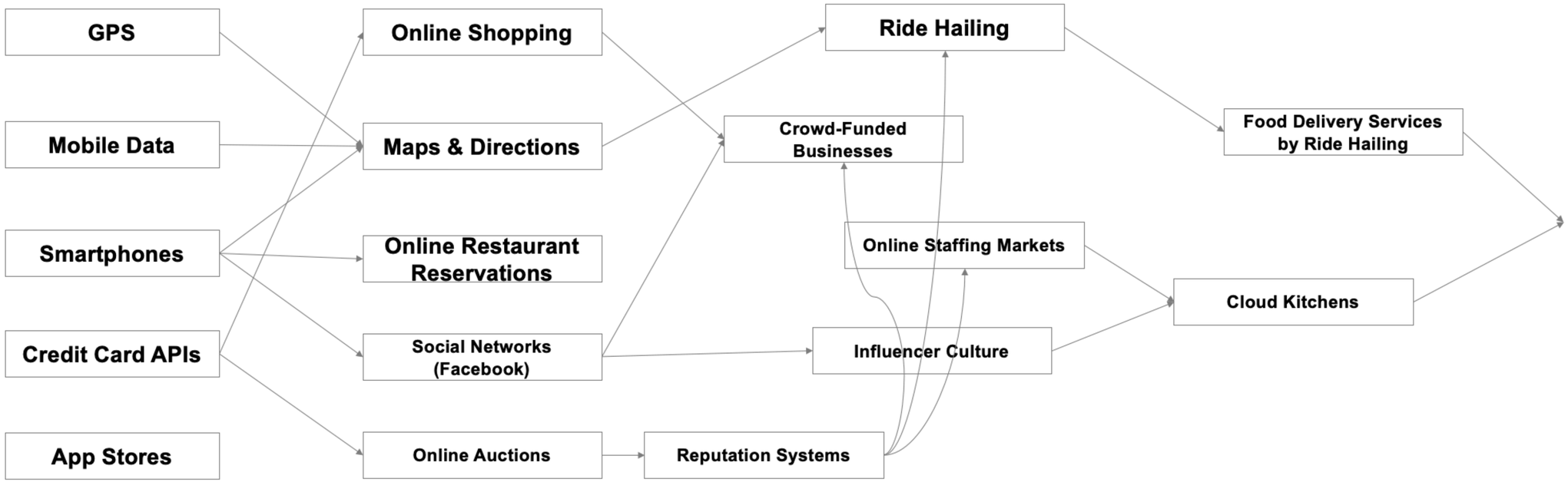
- The ability to link these together initially produced very predictable results – things done online as they were offline

Accelerating Disruptions

- API (Application Programming Interfaces) make it possible to start build "composite" models that layer one innovation atop the other

On Nobody's Bingo Card

- Eventually leading to some very unpredictable end results…



Celebrity-Chef Branded Restaurants that have no physical locations, no permanent staff, only do delivery through ride-hailing app networks and are only marketed on Instagram

Right now, it looks like DeFi is just re-building standard banking applications in a new ecosystem. This is a very predictable "stage 1" activity. What follows will start to be very very disruptive.

When we had horses, people dismissed cars.

When we had post mail, people dismissed email.

You couldn’t phone and use the Internet at the same time.

In 2017, Jamie Dimon (J.P Morgan Chase) called Bitcoin a fraud.
In 2018, he regretted it. He also created JPM coin.
In 2021, he is recruiting Ethereum developers.

Even if blockchain fails, just like P2P 20 years ago or neural networks 35 years ago, it serve as the foundation for greater things.

Even today, Silicon Valley is looking for experts in distributed computing, fault-tolerant systems, state-of-the-art cryptography.

Blockchain is recruiting Silicon Valley’s talents.

What if you’re not a developer?

Love pointing out mistakes?

Auditing is big. There is a global shortage of code auditors. There are hacking challenges with up to $2M USD (Balancer v2) in prizes if you break the code.

Love mind-reading?

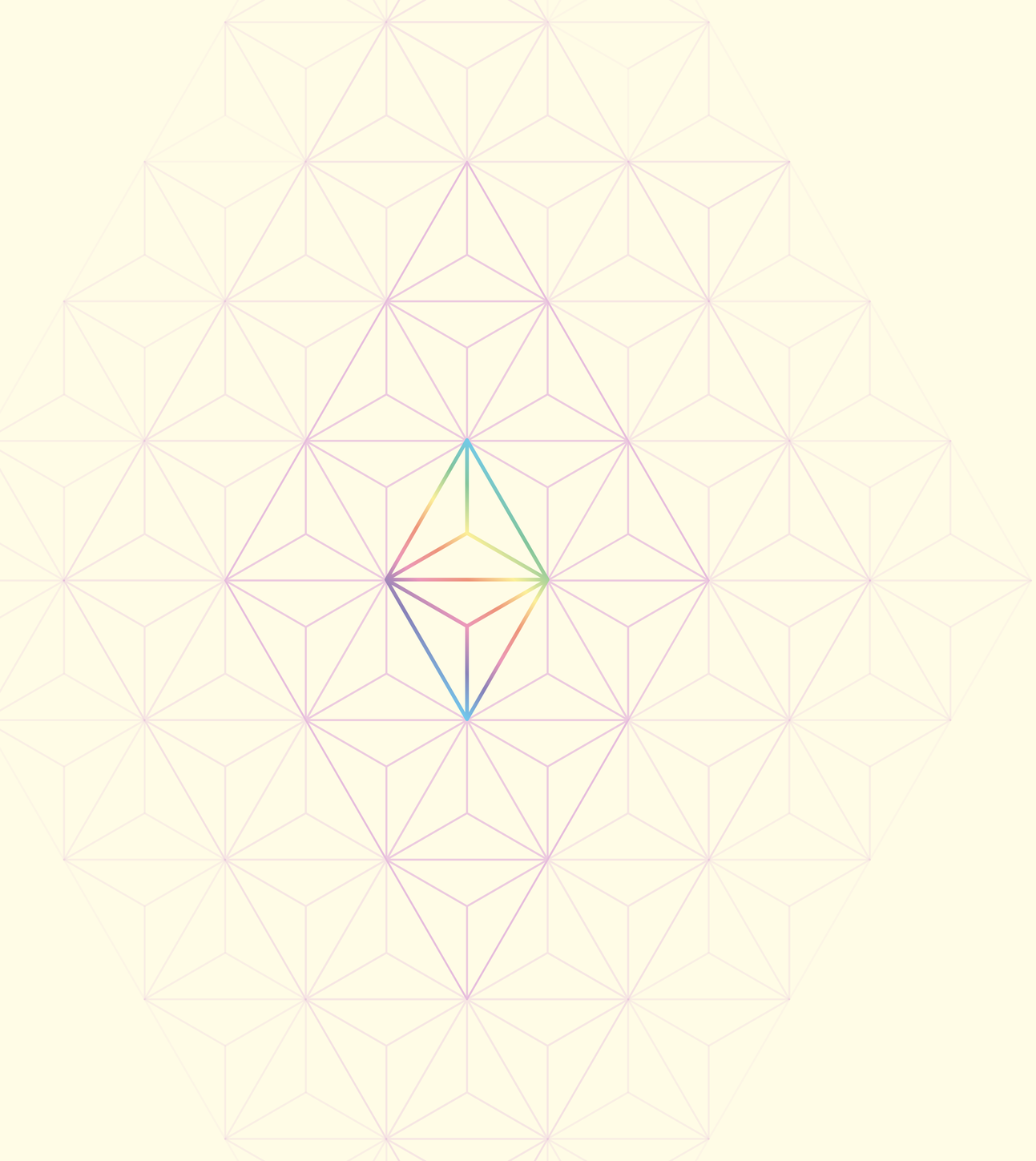
Psychology & economics are key to design proper incentives to bring both supply and demand to your product. Ever heard of the prisoner’s dilemma & game theory?

Love building a community?

In blockchain, legitimacy and community are among the scarcest resources. If you love to take care of followers on Discord, Twitter, Telegram, forums, you’re wanted.

Love design & polish?

Blockchain projects have an accessibility problem. The concepts are foreign, complex with a lot at stake. UX/UI magicians and designers are needed.



How many people does it takes to change the world?

How many people to change the world?

https://www.weforum.org/agenda/2018/06/want-to-change-society-s-views-here-s-how-many-people-you-ll-need-on-your-side/

How many people do you need to change the world?

A social study revealed that it could just take one person to change the views of the majority opinion within a group.

Image: REUTERS/Stefan Wermuth SEARCH "WERMUTH PHONES" FOR THIS STORY. SEARCH "THE WIDER IMAGE" FOR ALL STORIES.

This article is published in collaboration with
Futurism

12 Jun 2018

Kristin Houser

Read the 'Davos Manifesto'

How many social activists does it take to change the world? No, this isn't the setup for some lame joke. It's a question no one really knew the answer to. Until now.

We've seen plenty of shifts in society's views — in just the last hundred years in America, the majority's opinion on everything from gay rights to gender equality changed dramatically. However, we've never really nailed down if there was a "tipping point" for this social change — a specific number of people needed to push a belief from the fringes into the mainstream.

Estimates ranged from as low at 10 percent of a population to as high as 51 percent, but now, researchers from the University of Pennsylvania and the University of London claim an online experiment let them hone in on the most likely number: 25 percent. They published their study today in the journal Science.

How many people to change the world?

https://www.bbc.com/future/article/20190513-it-only-takes-35-of-people-to-change-the-world

BBC FUTURE

By David Robson
14th May 2019

Nonviolent protests are twice as likely to succeed as armed conflicts – and those engaging a threshold of 3.5% of the population have never failed to bring about change.

In 1986, millions of Filipinos took to the streets of Manila in peaceful protest and prayer in **the People Power movement**. The Marcos regime folded on the fourth day.

In 2003, the people of Georgia ousted Eduard Shevardnadze

Let's BUIDL!

Blockchain:
building trust one block at a time

Mamy Ratsimbazafy

Ethereum 2 / Nimbus developer @ Status.im

m_ratsim

mratsim