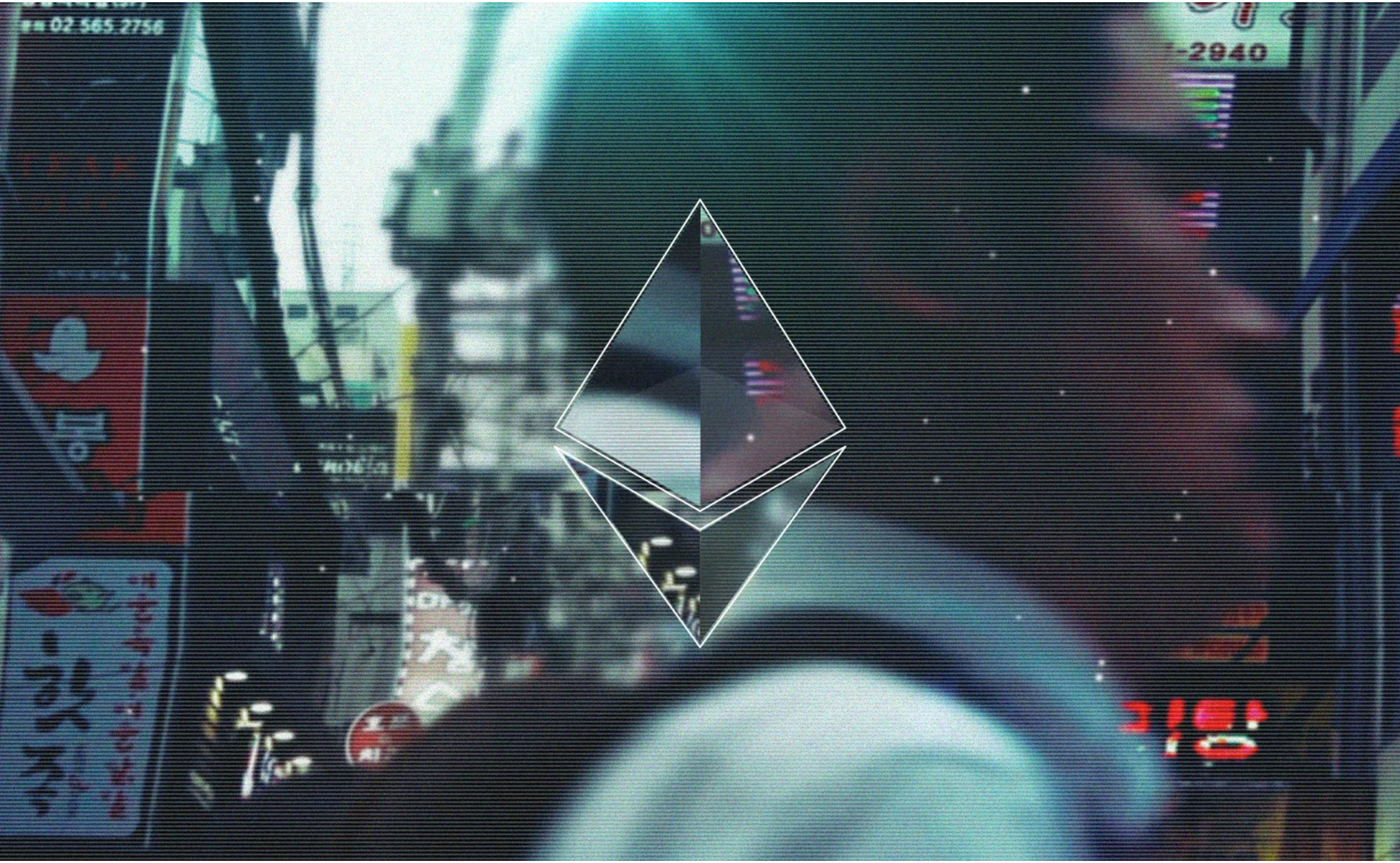

# Building a next-generation global economy

Joseph Lubin, COO, Ethereum

FRB CHI Payments Symposium — Emerging Payments Models

# Overview

- Prevailing dominant decision making mechanisms define the nature of society.
- P2P technologies —> Bitcoin —> Ethereum
  - Might usher in a new kind of economy
- Some implications of these new organizing principles for economies and payment systems.

# Decision Making in Early Societies

- Economic and social systems may be categorized by how decisions are made.
- Long ago in tribes and small villages populations and distances were small, and communication was fast and easy.
- Everyone knew who owned what and what was community property.
- Group decisions could be reached transparently with rapid consensus (or majority) formation.  No need for anything more than a shallow social hierarchy.

# Decision Making Under Emergent Complexity

- Society grew, became more geographically distributed and complex.
- Top-down, compartmentalized, hierarchical control systems became the most effective organizing principle.
  - Governmental, military and corporate systems took this form.
- Decisions flowed down the hierarchy. Compartmentalization and reduced information sharing  served as a technique to maintain and consolidate power.

# The Advent of Peer-to-peer Technologies

- Old-style: Client-Server
  - Individual clients request services and resources from centralized servers.
- The new new thing: P2P Network-based Systems
  - Peer nodes on the P2P network both provide and request services without a central authoritative server.
- Seeds of change from way back:
  - ARPANET/Internet: Decentralized and peer-to-peer network of computers (more so in the early days, but profit-motive and drive for efficiency has centralized the Internet architecture significantly).
  - World Wide Web: Initially a peer-to-peer hypertext network for content.

# Decentralized Design Evolved…

- …and continues to wring the various the centralized components from systems.

- File sharing networks: Napster (1999), Gnutella, KaZaA, eDonkey, …, BitTorrent

- Multimedia: Skype, Spotify, PeerCast

- Networking: Netsukuku (mesh routing), Open Garden

- Value Storage and Transmission: Bitcoin — fully decentralized protocol

# Historical Precursor Components of the Bitcoin Protocol

- Peer-to-peer network systems
- Proof of Work Systems
  - Adam Back's Hashcash (1997) - designed to limit email spam and denial-of-service attacks
- Digital cryptographic cash/token systems, e.g. Chaumian cash
  - Solved security and privacy (anonymity/pseudonymity)
  - But required a centralized processor or trusted platform to solve the double-spend problem.

# The Revolutionary Breakthrough of the Bitcoin Protocol

- The **double-spend problem was solved** by constructing a decentralized mechanism for arriving at a canonical, system-wide understanding of the order of transaction processing.

- The blockchain — a chain of cryptographically linked blocks — serves as a **decentralized transaction time-stamping mechanism**.

- A network of interacting actors cooperate to form a consensus regarding **what happened** and **when** with respect to storage and transmission of value even if nearly 50% of the network nodes are malicious and cooperating.

- The Bitcoin system serves as a **shared public ledger** and everyone who uses the system reconciles and maintains an up-to-date copy.

# In Summary, Bitcoin is a ..

- …decentralized system… (no centralized authoritative servers)
- …for secure storage… (addresses, wallets, accounts)
- …and transmission… (transactions)
- …of value… (the bitcoin token)
- …with user-configurable privacy… .
  (pseudonymous or fully transparent)
- …employing a decentralized, fixed quantity, token issuance model. .
  (Miners get paid in new issuance to process transactions and secure the network — no central bank; by 2140 all 21M BTC will be issued)

# Bitcoin and the Byzantine Generals Problem

- “Before the Bitcoin protocol was invented, most computer scientists thought a system like Bitcoin was impossible because of a famous problem in computer science called the Byzantine Generals Problem.

- “The problem, in a nutshell, is how to coordinate among distributed nodes to come up with a consensus that is resistant to attackers who are trying to undermine that consensus.

- “A significant component of the solution is the proof-of-work algorithm, which is the main purpose of so-called Bitcoin miners.The blockchain — a chain of cryptographically linked blocks — serves as a decentralized transaction time-stamping mechanism.”

    - Chris Dixon, (Andreesen Horowitz)

# Bitcoin Miner/Processors and Proof-of-Work

- Miners/processors on the Bitcoin Network work to form a consensus regarding what happened and when with respect to transmission (transactions) and storage of value.

- Miners earn the right to vote in the consensus formation mechanism by owning and powering very fast computers that can do a very large amount of computation.

- Various economic alignments and incentives keep the miners interested and the network secure.

# The Revolutionary Implications of Bitcoin

- Fully decentralized — nobody controls it, there is no there there.

- Compared to centralized payment and value storage systems (like PayPal or traditional banks), when the **pure Bitcoin protocol** is used with no intermediaries, it will be virtually impossible to:

  - censor payments — stop transactions from being sent or received

  - refuse access to users (e.g. the 5B global unbanked)

  - corrupt the system (break it, steal from others;  n-factor multisig)

  - co-opt the system (subvert operations top-down (buy it) or bottom-up (surreptitious back doors, coercion of developers, standards process capture))

  - manipulate the system logic (though trading manipulations will likely always be possible)

# Bitcoin is a …

- … product **of the people**, … (developers)
- …run **by the people**, … (miners)
- … **for the people**'s use. (C2C, C2B, B2B, B2C)
    - universal access through uniform interfaces

# Bitcoin is Only the First Application

- The Bitcoin system is a value storage and payments system.

- BTC (bitcoin) is a currency.

- The Bitcoin Protocol is a decentralized consensus formation mechanism under uncertainty.

- The monetary aspect is **just one narrow use case** for this technology.

# Upon all of the Bitcoin Breakthroughs, Ethereum adds…

- Faster, more secure, more efficient block/blockchain protocol.
- A computationally complete **virtual machine** for running arbitrary decentralized programs.
  - Our own programming languages and compilers.
- A centralization-hard mining algorithm (hopefully).
- An integrated EtherBrowser/App Store for finding and running decentralized applications (DApps).

# Ethereum

- Miners/processors on the Ethereum system work to form a consensus regarding what happened and when with respect to state transitions in decentralized computer programs. Essentially everyone can verify what happened in a computer program running on the network.

- Currently under development — just released version 6 in the proof of concept series.

- A decentralized app development and deployment environment.  Secure decentralized cloud for running SaaS.

- Hundreds of developers around the globe are already building DApps.

- Similar blockchain mechanisms to Bitcoin, but protocol will be a faster and more secure since it has benefitted from 5+ years of academic research since the release of Bitcoin.

- Bitcoin has 10-minute block times.  Our will probably be on the order of 12 seconds.

# History Rhymes — Decision Making in a Global Connected Economy

- We now live in a society that benefits from nearly **instantaneous communication systems**, and easy access to in-depth information on a very wide range of topics and issues.

- With the advent of telecommunications and the continued development and global spread of the Internet, we now have an infrastructure from which we can create a global village — or **many overlapping decentralized villages** — each with rapid, intimate communications systems and **each able to form consensus (or majority) quickly when necessary to make decisions**.

# The Internet was Designed in a More Naive/Trusting Era

- The Internet is a patchwork of technologies.
- Though revolutionary and transformative, it is badly broken with respect to privacy and security.
- And it doesn’t have a built-in private and secure payments system.
- Sending identity and financial info (credit card #s) to vendors and hoping they store that info securely is archaic and dangerous.
- No baked in privacy; no built-in strong cryptographic security; no intrinsic payment system.

# Web3: The Private and Secure Decentralized Internet

- The Ethereum architecture enables a decentralized Internet and web, (Web 3.0).
- Web 2 is largely a client-server architecture.
- On Ethereum, or Web 3, there are no webservers, just peer nodes that can serve and request services without hierarchy.
- This removes many intermediaries that increase cost by taking their cut and decrease privacy and security, by providing (hidden) access points for hackers or other interested parties.
- The client-server architecture facilitates types of attacks (e.g. DDoS, kill switch, focussed terrorist attack, foreign espionage) to which a P2P architecture is nearly impervious.
- On Web 3 privacy and security will be baked in at all levels: payments, messaging, application services.

# Web3: The Efficient, Market-based Decentralized Internet

- The raw materials that constitute the Internet are computation, bandwidth and storage.  And there is enormous excess/waste of each.

- Ethereum will enable personal or corporate resources (computation, bandwidth and storage) to be easily metered and sharable (for a micropayment fee).

- Efficient markets offering nearly instant, automatic access will develop for these resources.  We will build the early tools.

- A singleton global computer can emerge from efficient combination of all of these shared resources.

- Since almost everything on this system will have at least micro-costs, spam will become a thing of the past.

# Ethereum Use Cases

- ID and reputation systems
  - A fundamental component of AML/KYC
- Smart self-enforcing contracts: employment contracts, wills, betting, financial instruments
- Issue DTCC-free securities on the blockchain (sooner than you think?)
- self-insurance pools
- fund raising systems (equity and rights (governance and dividends), or pure kickstarter)

# Ethereum Use Cases

- Smart property: hotel or car locks
  - IBM and Samsung's vision for the Internet of Things
- Consensus formation: voting (in any sort of organization of social system)
  - what features to prioritize when developing software
  - what policies to institute in an organization
  - what people to elect in a government
  - OR … government by popular vote in a liquid democracy system

# Ethereum Use Cases

- Transparent accounting systems
  - Triple entry accounting.
  - Automated, real time blockchain-crawling audit bots.
    - CFOs and CEOs will not be able to manipulate numbers in a hidden, server-based accounting system.
- Provably fair online gambling systems.
- Proved reserves banking systems.

# Web2: You are the Product

- Web2/Legacy Banking System: banks control/custody your money and charge you fees to use it.

- Web3: Next generation banks offer add-on services (account insurance, lending, investment opps, financial planning, …) while the user controls access to and dispensation of own funds, fee free.

- Web2: Facebook, Google, LinkedIn, Twitter, etc., own your identity and communications.  As “trusted” intermediaries they monetize your life.

- Web3: Just like your money, you retain control of your ID, rep and comms. If you want to sell your attention or various emissions (comms, biosignals, purchase patterns, …), you should get the bulk of the payment from advertisers or other data collectors.

# Might Ethereum be Abused?

- Yes, like all great technologies it can be used by all elements of society: it can be used to facilitate crime.
    - But Bitcoin and Ether are far more easily tracked than USD cash.  Tools have been developed to trace transactions back to senders and receivers.
- Just like the Internet, dark areas will form that deem themselves not part of any country's jurisdiction.
- This fringe aspect is the price we pay for freedom and innovation.
- Just like the legacy economy or the Internet economy, most uses will be lawful.
- If you are building a business on Ethereum and it has a physical presence somewhere, it will have to comply with local law and regulatory oversight, where appropriate.

# How do we stop this?

- You can’t.

# Ok, how do we regulate this?

- Don’t.  At least for the most part.
- As with the Internet, these technologies should largely be left alone to develop.
- Where companies are responsible for people’s money or facilitating monetary exchange or transmission, existing regulation should suffice.
    - But leave all the non-money-service businesses to develop and innovate.

# An Emergent Self-regulating System

- Extreme transparency and comprehensive transaction trails will enable regulation to take shape as an emergent property of this new economy.
- Triple entry accounting systems will drastically reduce opportunity for fraud and tax avoidance.
- Companies/services will form that handle people's data with granular privacy and complete security.
- Other companies will form to police financial or other institutions.
- Financial institutions will be forced to police themselves transparently: cryptographic proof of reserves.

# If wildly successful…

- And since this is the Payments Symposium, let me emphasize this last point:
  - If wildly successful, Ethereum (or something like it) could emerge as the substrate on which next generation global economic and socials systems are built: cryptographically secure, spam-free, with user-configurable privacy and …
- …with a built-in, deeply intrinsic payment system.