Blockchain economics

Jiangang Wu

Advisor of Skrumble

Email: imahero@gmail.com

July 26, Toronto

Contents

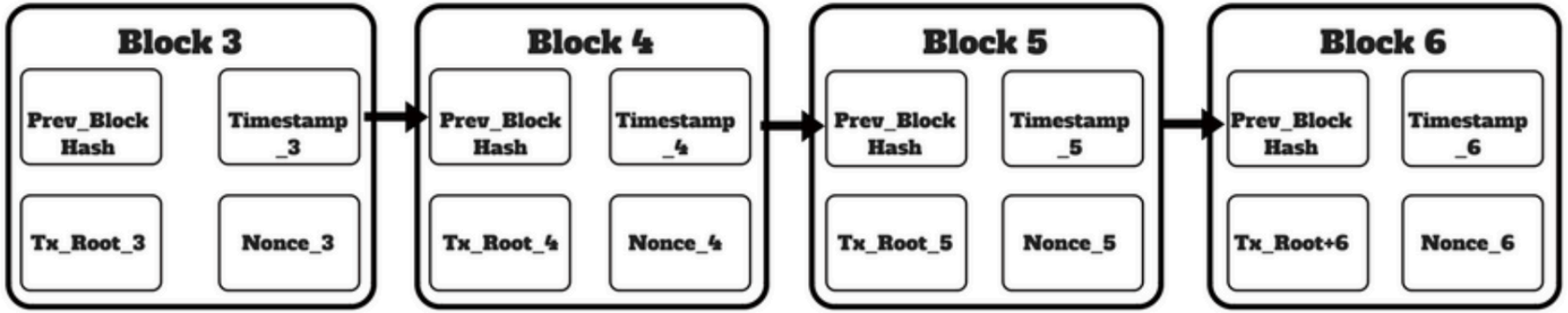
1. What is blockchain economics?
2. Civilization’s evolution perspective
3. Institutional economics’ perspective
4. Financial economics’ perspective
5. Distributed autonomous organization’s perspective
6. Cryptoeoconomics’ perspective
7. Application’s perspective
8. The calling of blockchain autonomous society

1. What is blockchain economics?

- 1.1 What is blockchain?
- 1.2 Characteristics of blockchain
- 1.3 What is blockchain economics?
- 1.4 The questions blockchain economics addresses

1.1 What is blockchain?--definition

- A blockchain is a distributed accounting technique on a peer-to-peer network.
  - It records the participants' transactions during this period of time, forming a data block.
  - It uses consensus to choose one bookkeeping node before broadcasting the block to others so that every node has the same ledger.
  - These blocks are linked together in a chain by timestamps.
  - Blockchains use tokens as the bookkeeping symbols.
  - The chosen node can run a program (smart contract) to generate the numbers that need to be recorded.



1.2 Characteristics of blockchain—cooperation through blockchain

- Characteristics bringing by Internet of Information
  - Digitalized
  - Peer to peer
  - Programmable
- Disintermediary
  - Open source
  - Transparency in data
  - Code is law: consensus
- Inclusiveness
  - Easy to enter: to buy tokens, to join development, to consume, to help propagate …
  - Easy to retreat: to sell tokens, keep indifferent to it
- The cost to solve conflicts is low:
  - Internal conflicts: to form
  - Conflicts between blockchains: they all can exist as long as they have users

Characteristics of blockchain—blockchain as a problem solver

Characteristics	Problems of human society and its solutions
Decentralization	Human beings use a large number of centralized organizations and pay a painful price for them. The development of civilizations were accompanied by conflicts, wars and the oppression of various central organizations. Through the decentralization mechanism of blockchain, it is expected that the entire human race will work together smoothly.
Consensus	Through the blockchain consensus mechanism, consensus can be reached more widely.
Transparency	The nature of highly transparency of blockchains reduces transaction costs caused by information asymmetry.
Trustless	Consensus mechanisms will code human transaction and trust mechanisms and make them automatic and algorithmically optimized. With different opinions, people need not to choose to fight with each other, they can fork and create a new blockchain.

Characteristics of blockchain—blockchain as a problem solver (continued)

Characteristics	Problems of human society and its solutions
Collectively Maintenance	Ecosystems can be enriched and stabilized through collective maintenance, economic incentives, and big data spillovers.
Reliable database	The blockchain's cryptographic mechanism, incentive mechanism and multiple backup mechanisms ensure that the data cannot be changed and the authenticity of the information is guaranteed.
Data retroactivity	Blockchain transaction chain data structure makes it easy for data traceability and cross-checking.
Open source	The feature of transparent blockchain code is the basis for achieving consensus and can help achieve autonomy on code basis.
Smart contract	Smart contracts can automate complex transactions. With the improvement of ecology, various contracts will be more and more formatted, greatly reducing transaction costs and improving transaction efficiency.

Characteristics of blockchain--shortcomings

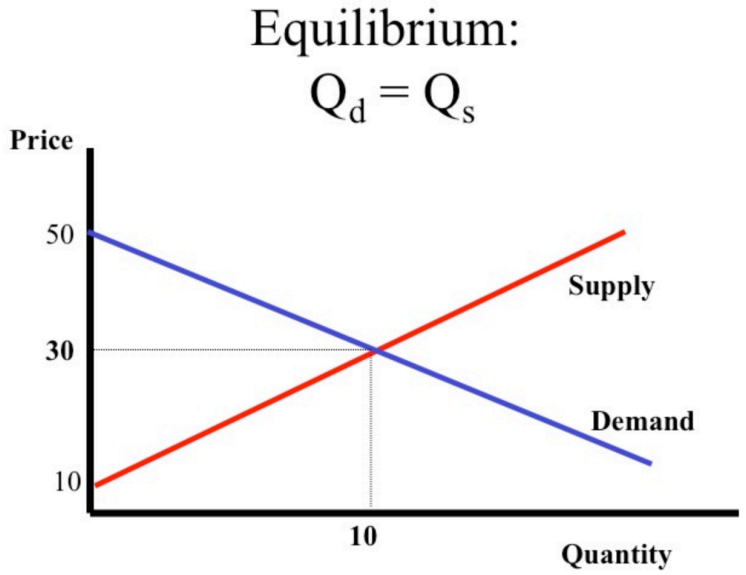
- Single point bottleneck
  - Only a few machines are confirming transactions at any time in the P2P network
- Cost of consensus mechanism
  - Proof of work
- Interoperability
  - Communication problems between blockchains
  - Communication problems between blockchain and centralized organization
  - Blockchain and data source communication problems
- Future prospects
  - These problems will gradually resolve as technology develops

Characteristics of blockchain--essence

- In essence, it is a method of using distributed nodes to help humankind to **solve problems**.
  - For computer perspective: distributed calculation and **world status** storage
  - For value transfer: **distributed ledger** technology
  - For smart contract: a protocol to **automatically execute contract**
  - For cloud service: it is a protocol of cooperation rules to help distributed nodes to work together to provide **distributed cloud services**.
  - For the development trend of society: it is the network infrastructure for a **virtual society** based on distributed cloud services

1.3 Blockchain economics

- Economics means the study of how to help people work together to reach their dreams, or help supply meet demand under limited resources.
- Blockchain economics means the study of how to use blockchain technology to help people work together to reach their dreams.



1.4 Questions blockchain economics need to address

- What is its impact to humankind civilization?—civilization perspective
- How will it affect human societies' institution?—institutional perspective
- What does it mean to the humankind's finance?—finance perspective
- How will it reform the humankind's organization?—organization perspective
- How does its economics work in blockchain networks?--cryptoeconomics
- How will it be applied to human's daily life?—application economics
- What changes will it bring to human society eventually?—blockchain autonomous society

2. Civilization evolution’s perspective

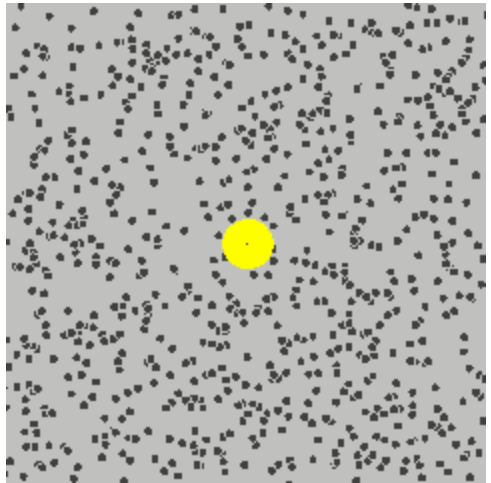
- 2.1 What is civilization
- 2.2 Evolutionary stages of the humankind
- 2.3 Impetus and bottleneck of humankind civilization
- 2.4 What blockchain can do to solve problems of civilization
- 2.5 Evolutionary stages of the universe

2.1 What is civilization?

- It means a lot, but mainly it means animals abilities:
  - The ability to survive?
  - The ability to use power?
  - The ability to use tool?

What is civilization?

- The ability to work together!
- The technologies that help people work together:
  - Communication
  - Contract
  - Institution
  - Culture
  - Blockchain
  - Smart contract
  - Code is law
  - Autonomous society
  - …



2.2 Evolutionary stages of the humankind: Kardashev scale

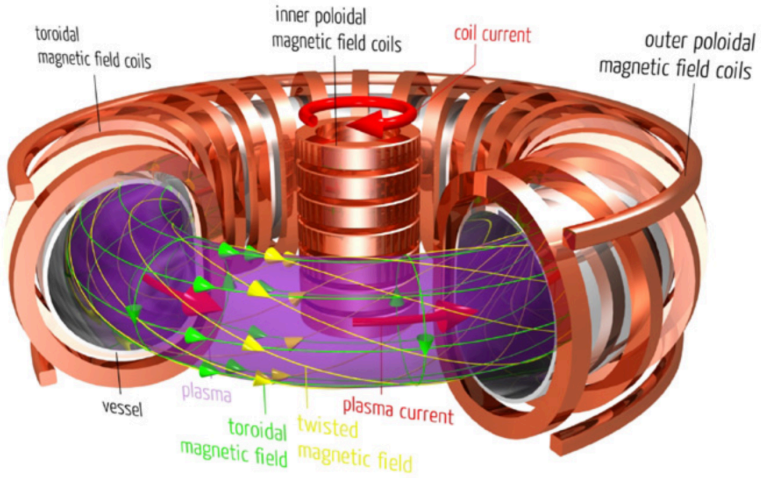
- A method of measuring a civilization's level of technological advancement
  - Based on the amount of energy a civilization
  - Based on the material of tools
  - Proposed by Russian astrophysicist Nikolai Kardashev

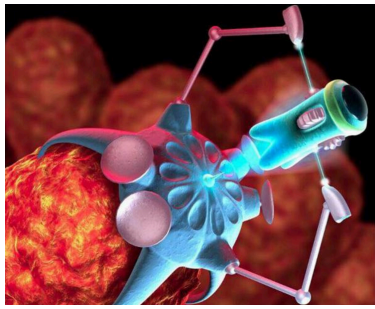
Type 0 civilization: a planetary civilization

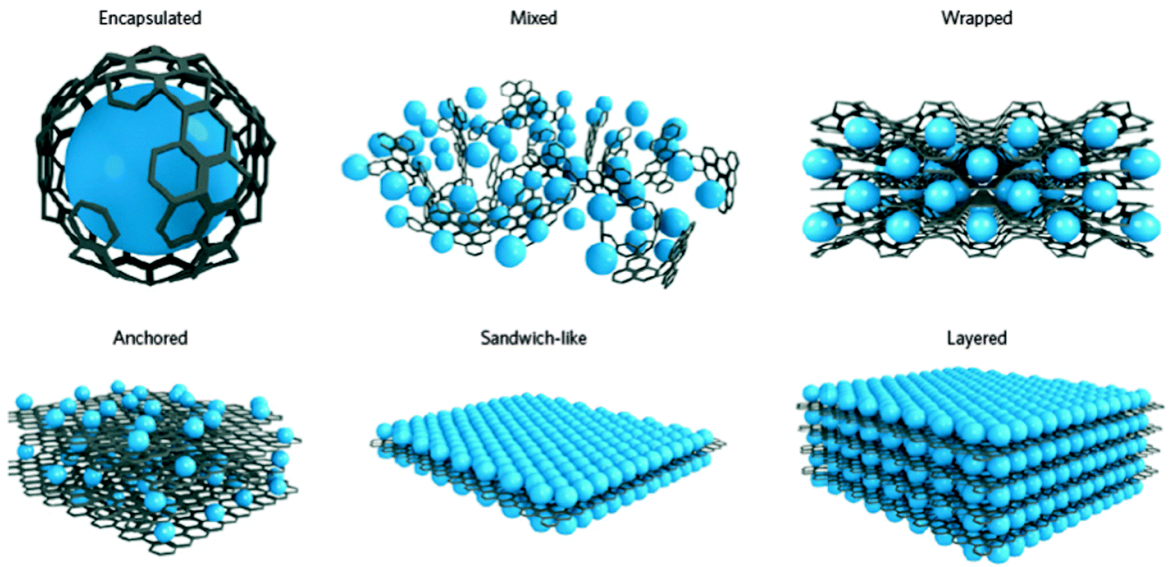
- Type 0 civilization:
  - Type 0: molecular group, stoneware, metal, paper → stone age, copper iron age, paper age
  - Type 0+: composite material, micron technology → industry era, space age, information age

Type I civilization: a planetary civilization

- Type I Civilization: Ability to use all available resources in its home planet
  - Type I: nanotechnology (10^{-9} m), molecular structure materials, carbon nanotubes, synthetic organisms, robots, earth transformation, smart materials, ultra-deep mining → planetary age
  - Type I+: picometer technology (10^{-12} m), atomic structure materials, earth-based exoplanets, geocentric exploration, printing complex physical → planetary system era

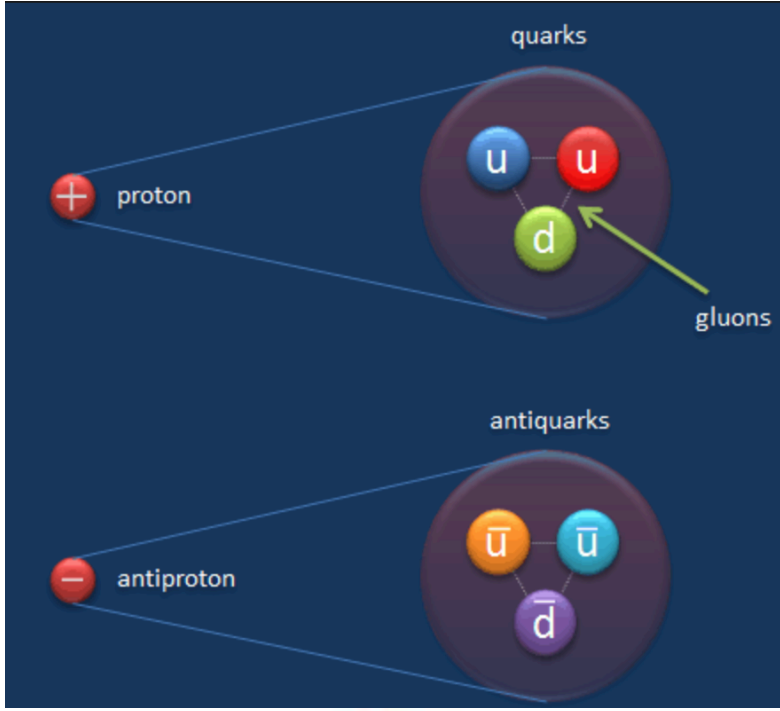


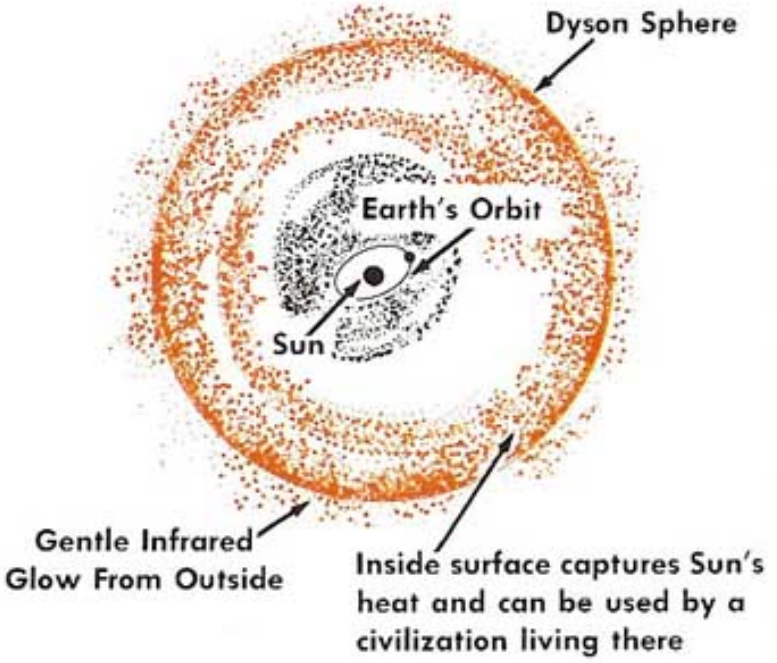




Type II civilization: a stellar civilization

- Type II civilization: able to take advantage of all the energy of its stars
  - Type II: Fermi technology (10^{-15} m), strong interaction materials, artificial singular atoms, exotic materials, long-distance transmission of matter, stellar industry, artificial star stellar age
  - Type II+: Ami technology (10^{-18} meters), basic particle materials, development of extreme stars in the universe, artificial stars, energy and mass transformation of the galaxy era

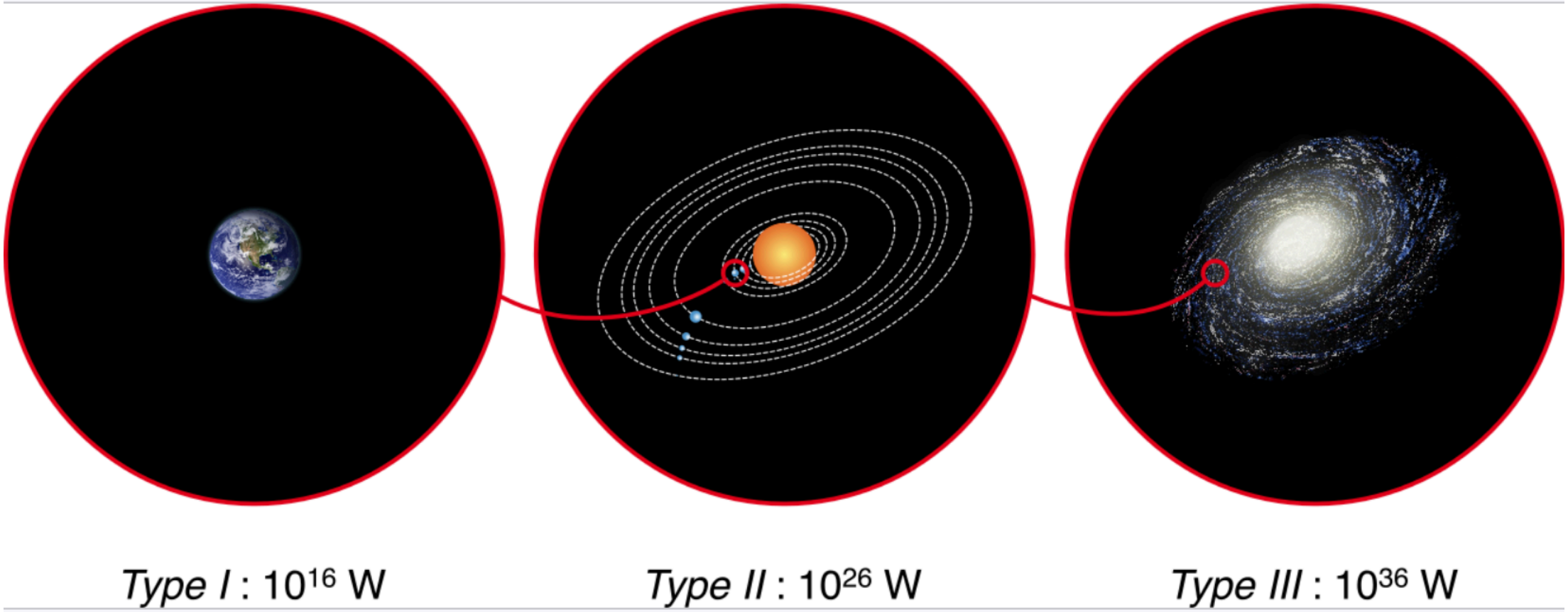




Type III civilization: a galactic civilization

- Type III civilization: all the energy that can utilize its galaxies
  - Planck technology (10^{-35} meters), photon, primer force, space-time structure, pan-universe development, artificial universe, high-dimensional space manipulation, space-time exploration, quantum ultimate → **universe era**

Evolutionary stages of the humankind



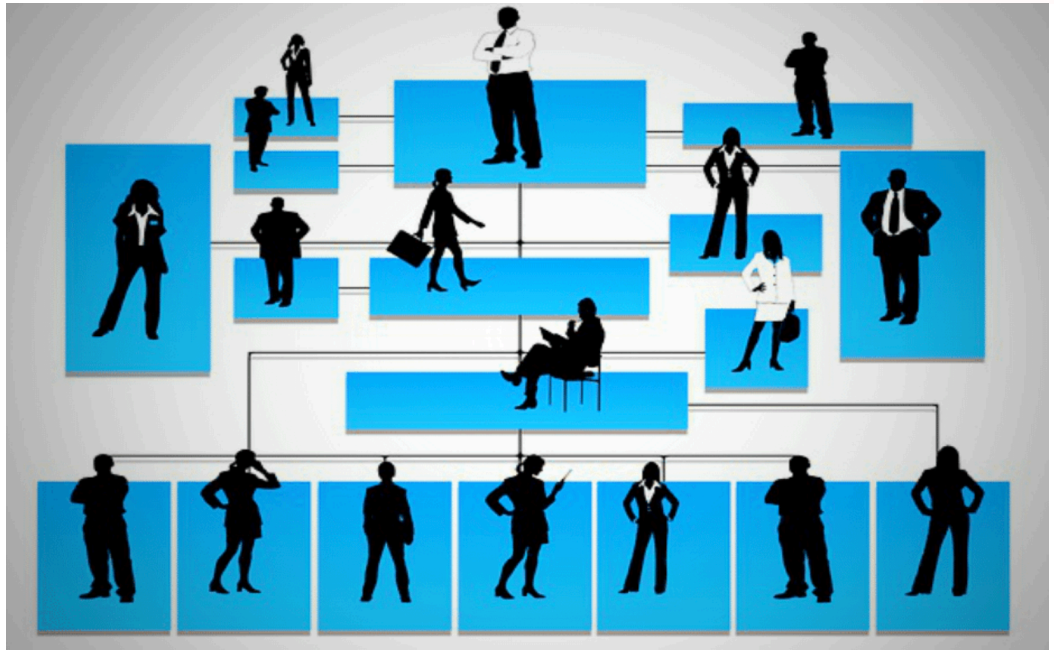
Energy consumption estimated in three types of civilizations defined by Kardashev scale

Scale of humankind civilization: 0.7

- Calculated by the total world energy consumption, Humankind's Kardashev scale is about 0.7
- Physicist and futurist Michio Kaku suggested that Humans may attain:
  - Type I status in 100–200 years,
  - Type II status in a few thousand years,
  - Type III status in 100,000 to a million years.

2.3 Impetus and bottleneck of humankind civilization

- Brain
- Machine
- Organization



Impetus and bottleneck of humankind civilization—brain

- Strength of brain
  - Curiosity
  - Endless desire
  - Endless creativity
- Weakness of brain:
  - Limited life
  - Black box: cannot trust each other
  - Unreliable: change ideas all the time
  - No direct cloud interface:
    - Brain → hand → mobile phones → servers → mobile phones → other brains
  - Slow calculation speed
  - Can't charge directly

Basic concepts to help brains to work together

- Democracy
- Freedom
- Fraternity

Basic concepts to help brains to work together-- democracy

- To deal with how brains should cooperate
  - Hypothesis: the difference between the brains is small
  - Corollary: the more brains who participate in cooperation, the more civilized humankind will be
  - Democracy is the way to let more brains participate in the progress of civilization
- Problems
  - It is difficult to balance conflicts between majority and minority
  - It is inefficient to make decisions
  - The greater the ability of one person's using technology, the greater the chance that the system will be crashed by a single person.

Basic concepts to help brains to work together-- freedom

- To deal with how to stimulate brains to meet its desires
  - To have consciousness means to have concept of freedom
    - Ability to think independently
    - Ability to have desire
    - Ability to satisfy desire
      - Pursue more knowledge
      - Pursue more technology
  - Technology brings freedom
- Problems:
  - One man’s freedom can be another’s slavery

Basic concepts to help brains to work together-- fraternity

- To solve conflicts between brains
  - A way of searching compromise
  - Fraternity is a basic mechanism for civilization to continue
- Problem:
  - One group’s fraternity can bring hatred to another group
  - The system can punish good persons while benefiting bad persons.

Impetus of humankind civilization—machine

- Strength of machine (codes):
  - Fast
  - Rechargeable
  - Reliable: transparent, predictable
- Weakness of machine (codes):
  - lack of creativity
- General artificial intelligence:
  - To replace human brain
  - Or to integrate with human brain
  - A long way to go

Impetus and bottleneck of humankind civilization—organization

- Distributed market:
  - Invisible hand
    - Lack trust mechanism
    - Incomplete contract
- Centralized organization:
  - Trust and specialized contract
    - Struggle within the organization: agency cost (internal deception and oppression)
    - Conflicts between organizations: nuclear terror, arms race, religious war, patriotism, communism...
- Human beings need to remedy the problems of organizations, otherwise, human civilization may be interrupted at any time because of nuclear war, resource exhaustion or other reasons. We all have certain responsibilities.

2.4 What blockchain can do to solve problems of civilization

- Conflicts between human brains
  - Trustless network to help them cooperate
  - Proof of reputation to help credit rating
- Incomplete contract of making a deal
  - Smart contract is transparent and will execute automatically
  - Code is law
- Conflict inside organizations: agency cost
  - Human VS Human will be replaced as: **Human VS machine VS human**
  - Distributed autonomous organizations
- Conflict between organizations:
  - Blockchain as organizations: virtual communities will replace companies and governments
  - They can use both blockchains
- Combine the strength of distributed market and the strength of organizations
  - Use distributed network to replace traditional distributed market
  - Use blockchain consensus to replace traditional layer of managers and stockholders

2.5 Evolutionary stages of the universe--Principles

- Universe comes from the Big Bang
- Stages are divided by encoding types and evolution controlling variables
- Every stage prepare materials and environments for a next stage
- Use time and environment to chose who will be survivors
- Everything is coded and varieties are introduced for natural selection
- Human beings are the survivors who can observe the evolution process and affect it.
- Humankind’s aims in a sense represent the universe’s aims.

2.5 Evolutionary stages of the universe--stages

- Stage 1: Particle coding evolution
  - Coded by quarks and other more fundamental particles
  - Controlled by strong interaction
  - Survivors: electron, neutron, proton
- Stage 2: Celestial coding evolution
  - Coded by celestial bodies
  - Controlled by strong interaction and gravity:
  - Survivors: chemical elements, fixed stars, planet, nebula
- Stage 3: Chemical coding and its evolution
  - Coded by atoms
  - Controlled by electromagnetic interaction
  - Survivors: inorganic molecules, organic molecules

2.5 Evolutionary stages of the universe--stages (continued)

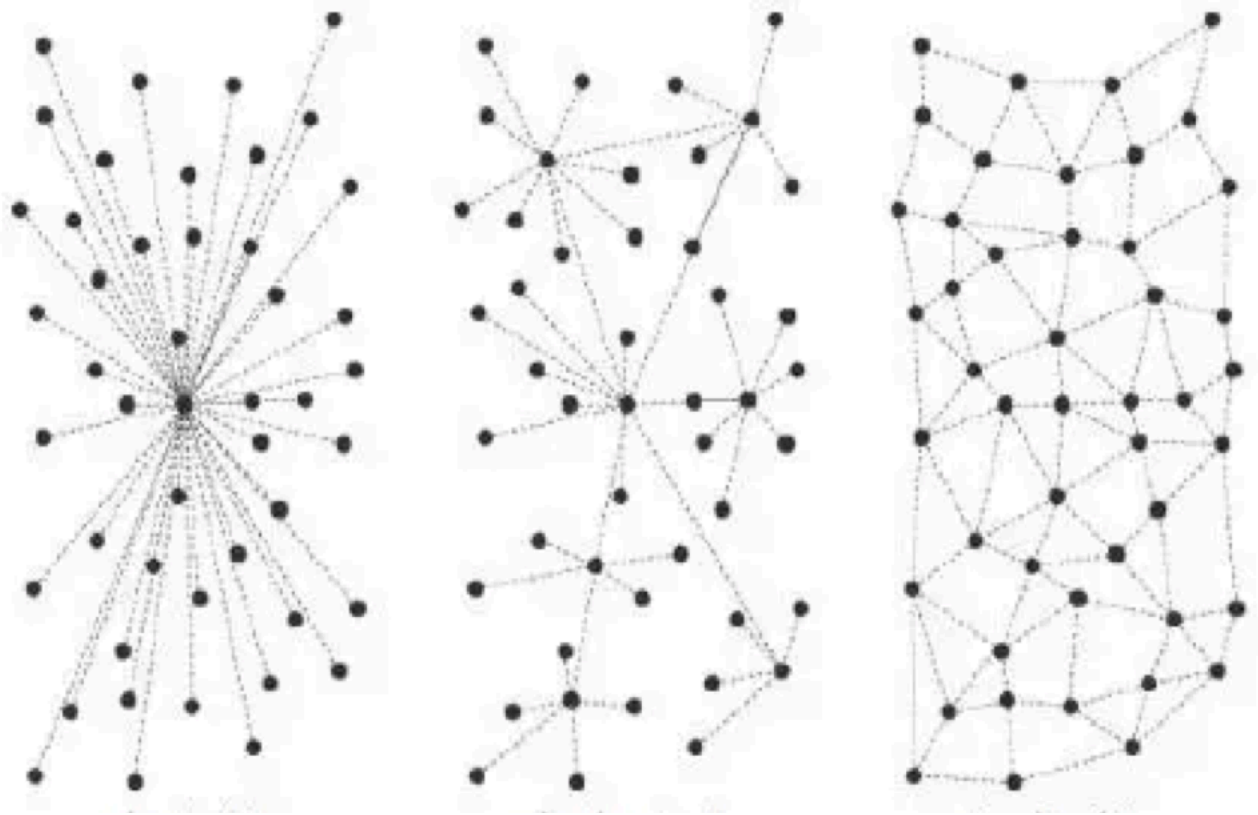
- Stage 4: Biological coding evolution
  - Coded by gene
  - Controlled by natural selection
  - Survivors: Animalia, Plantae, Fungi, Protista, Archaea/Archaebacteria, and Bacteria/Eubacteria
- Stage 5: Information coding evolution
  - Coded by bit
  - Controlled by value of information
  - Survivors: big data and its applications
- Stage 6: Value coding evolution
  - Coded by tokens
  - Controlled by efficiency of human cooperation
  - Survivors: blockchain platform, DApps, blockchain autonomous society

3. Institutional economics' perspective

- 3.1 Types of human organizations
- 3.2 Two ways of analysis of human organizations
- 3.3 Theoretic basis
- 3.4 Finding of new institutional economics (NIE)
- 3.5 NIE on concept, culture, contract, rules and law
- 3.6 Institutional competitiveness
- 3.7 Why NIE is important for blockchain industry

3.1 Types of human organizations

- Distributed organization:
  - Market
  - Public chain
- Centralized organization:
  - Family
  - Enterprise
  - Country
  - Private chain
- In the middle:
  - Association
  - Community
  - Alliance chain



3.2 Two ways of analysis of human organizations

- Two analysis approach:
  - Game Theory → Mechanism Design → New Institutional Economics → Incentive Compatibility
  - Coase Theorem → Contract Theory → Property Theory → Transaction Cost Theory
- The basic assumption: incentive & react

3.3 Theoretic basis

- Institutional economics, property right and organization theory:
  - Masahiko Aoki, Armen Alchian, Harold Demsetz, Steven N. S. Cheung, Avner Greif, Yoram Barzel, Claude Ménard, Daron Acemoglu
  - Five Nobel laureates: Ronald Coase, Douglass North, Elinor Ostrom, Oliver Williamson, and Oliver Hart
- Game theory:
  - Four Nobel laureates: John Nash, John C. Harsanyi, Reinhard Selten, Jean Tirole

Theoretic basis: Nobel laureates

- 1991, Coase, Coase's first theorem, Coase's second theorem
- 1993, Douglas North, Property theory
- 1994, John Nash, John Haysani, Rheinhard Zeerten, game theory
- 1996, James Morris, William Wickley, Information economics, incentive theory
- 2001, Michael Spencer, George Akerlof, Joseph Stiglitz, Moral hazard, adverse selection
- 2005, Robert Oman, Thomas Schelling, Non-cooperative continuous game
- 2007, Leonid Hevich, Eric Maskin, Roger Myerson, Mechanism design, incentive compatibility
- 2009, Eleanor Ostrom, Oliver Williamson, Social organization, new institutional economics
- 2012, Elvin Rose, Lloyd Shapley, Distribution theory, market design
- 2014, Jean Tirole, New industry organization theory, regulation and incentive, game theory
- 2016, Oliver Hart, Bent Holmstro, Contract theory

3.4 Findings of NIE

- Invisible hand solves everything (Adam Smith, 1776)
- Market also has transaction cost, firm can save the cost (Coase, 1937)
- Property right can fundamentally affect economic results (Coase, 1960)
  - An asset's property rights are hard to define
  - Externalities: one asset's right is another's source of harm
- Information asymmetry brings distrust which destroys markets (Akorlof, 1970)
- Firm has its agency cost (Alchin & Demsetz, 1972)
  - Before contract: adverse selection
  - After contract: moral hazard
- Contract can reduce agency cost (Williams, 1971; Hart, 1995):
  - Uncertainty
  - Incomplete information
  - Incomplete contract

3.5 NIE on concept, culture, contract, rules and law

- Concepts and cultures as unwritten institutions:
  - Concepts and cultures can help one group of people cooperate efficiently.
    - One may not want to accept the culture or concepts, but may be punished by unwillingness to believe traditions.
  - Concepts and cultures can cause conflicts between groups of people.
    - One group of concept can be another's poison.
    - NIE doesn't give solutions.
- Organization contract, rules and laws as written institutions:
  - Distributed market are great, but contract are incomplete, it is hard to trust one another
  - Centralized contract and rules are great, but internal trust and trust between organizations can be costly
  - Rules and laws can help remedy the problems of incomplete contract, but they are costly and can only fix part of it.

3.6 Institutional competitiveness

- The competitiveness of systems
  - Common features of all great civilizations:
    - The distributed market is sufficiently developed (through legal, property rights, market supervision, etc.)
    - Low cost of trust (achieved through legal, ethical, religious, etc.)
- Future trends:
  - Centralized organizations transition to distributed organizations
    - Human-to-human trusts transition to trusts between people and machines
    - Human-oriented systems transition to human-machine system

3.7 Why NIE is important for blockchain industry?

- Blockchain can remedy the problems of both markets and organizations:
  - It points out the strength and weakness of distributed markets and centralized organizations.
  - It explains in many aspects what blockchains can do to the world institutionally.
- Blockchains are a new type of distributed markets:
  - Blockchains will replace distributed market and centralized organizations
  - New institutional economics gives us tools to design and analyze economy inside blockchain and the communities around blockchain.
  - The two analysis ways of new institutional economics are helping creating an economics of blockchain which is cryptoeconomics.
- Code is law: When we use consensus to replace culture and rules, we are using smart contract to replace written institutions

4. Cryptoeoconomics’ perspective

- 4.1 Concept, task and characteristics
- 4.2 What questions do cryptoeconomics ask?
- 4.3 Cryptoeconomics of bitcoin
- 4.4 Application of cryptography
- 4.5 Economic incentive mechanism
- 4.6 Main concepts
- 4.7 Defect detection

4.1 Cryptoeconomics—concepts, tasks and characteristics

- Terminology: cryptoeconomics or cryptomics is still not widely used and the definition has not widely recognized.
- Main tasks:
  - Design a human-machine system to have the desired characteristics.
  - Ensuring past information through cryptography can prove that these characteristics existed in the past.
  - Use economics design incentives to keep the required features in the future.
- Characteristics:
  - It is not a new discipline, it’s more like “mechanism design” in economics.
  - Mainly used to design blockchain economic systems

4.2 Cryptoeconomics--what questions do cryptoeconomics ask?

- General questions:
  - How do mutual distrustful entities cooperate through peer-to-peer networks?
  - How the centralization mechanism in each field achieves decentralization?
- Specific questions:
  - What is the economic problem that a blockchain aims to solve?
  - Who are the participants?
  - What are their respective demands?
  - What are their common appeal?
  - How to establish a governance mechanism?
  - How to generate a homogeneous peer-to-peer network protocol?

4.3 Cryptoeconomics of bitcoin--cryptography

- Consensus: proof of work
- Signature: proof of the validity of the issuer of the transaction
- Hash:
  - Guaranteed block order
  - Light client can issue trading orders (Meckel tree certificate)

Cryptoeconomics of bitcoin--consensus

- Generate a blockchain
- Record transactions in each block
- Record status:
  - The state of the UTXO set
  - State change: s’ = STF(s, tx)
- Maintain one clock: used to hold state machine s' = STF(s, tx)
- New blocks can be added, but old blocks cannot be removed or replaced
- Maintenance effectiveness: only valid transactions can be recorded in the block
- Data is always available: full blockchain data can be downloaded
- The transaction can be carried out at any time if the transaction fee is reasonable

Cryptoeconomics of bitcoin--incentives

- Bookkeeping miners receive 12.5 bitcoins and they have temporary right to decide which transactions can be included
- If the miners' blocks are not included in the chain and will have nothing to gain.
- Difficulty adjustment: in the long run, the return is zero margin

4.4 Cryptoeconomics--application of cryptography

- Hash: confirm the order of the information
- Signatures: justification of the transaction
- Zero knowledge proof: prove that the information exists without delivering the information itself
- Proof of work: prove that a minimum amount of work has been achieved
- Proof of stake: prove that a minimum amount of stake has been put in
- PBFT: prove that a minimum amount of signatures has been collected
- Erasure codes: transforms a message of k symbols into a longer message with n symbols such that the original message can be recovered from a subset of the n symbols.
- Time-lock crypto: prove that a certain amount of time has elapsed between information A and B.
- Homomorphic encryption: performing a specific algebraic operation on ciphertext results in the same result as doing the same for plaintext

4.5 Cryptoeconomics--economic incentive mechanism

- Tokens: a protocol-defined command loop that has some kind of power on a peer-to-peer network that can be used for block rewards.
- Privileges: certain specialties according to the agreement, such as transaction fee income
- Rewards: if you do something “good”, increase the profit or privilege of a node on the peer-to-peer network.
- Penalties: if you do something "bad", reduce the profit or privilege of a node on the peer-to-peer network.

4.6 Cryptoeconomics—main concepts

- Security margin: X-number of token incentives, if the incentive node above this number is in compliance with the G agreement, the low number of token incentives violates the G agreement.
- Signature proof: the signed information is interpreted as: I confirm that P is correct, otherwise I will lose X tokens.
- Uncoordinated selection model: a model that assumes that the network protocol participants in the model cannot coordinate with each other, that is, have different incentives, and are less than the margin of safety X.
- Bribery attacker model: an uncoordinated selection model that assumes that the model has agents who are willing to pay a certain amount of expenditure to enable a certain strategy to be implemented. The budget and cost refer to the amount that is willing to pay for the attack and the amount actually paid.
- Destruction index: if a node uses one token to cause damage to X tokens for a node, the damage index is X.

4.7 Cryptoeconomics--defect detection

- Ignore or delay confirmation input
- Do not issue or delay the output
- Use an incorrect value:
  - Special case: Sending information too early
- Peer-to-peer network defect: delayed or missing information
- To avoid DDos and sibyl attack

5. Distributed autonomous organization’s perspective

- 5.1 Distributed autonomous organization (DAO): Definition
- 5.2 The difference between DAO and cryptoeconomics
- 5.3 System design

5.1 DAO--Definition

- Distributive Autonomous Organization (DAO) is a human-machine system that relies on computer code to create and automate, rather than using traditional enterprise organizational structures.
- DAO Theory is the study of:
  - What a distributed autonomous organization is
  - How it works
  - Why it works
  - How it is designed
  - How it will be in the future

5.2 DAO theory—the difference to cryptoeconomics

- Theory vs. technology:
  - DAO theory is used to study the economics of human organizations. It emphasize theory.
  - Cryptoeconomics is the design of a well-functioning distributed autonomous organization using DAO theory, cryptography, blockchain technology, and so on. It is more inclined to engineering and technology.
- Blockchain vs. various organizations:
  - DAO theory studies various organizations, not just blockchains
  - Cryptoeconomics mainly studies the intrinsic mechanism of blockchain system
- Node role VS various roles
  - DAO theory studies various roles in a distributed organization
  - Cryptoeconomics focuses on the role of each node in the blockchain

5.3 DAO theory--system design

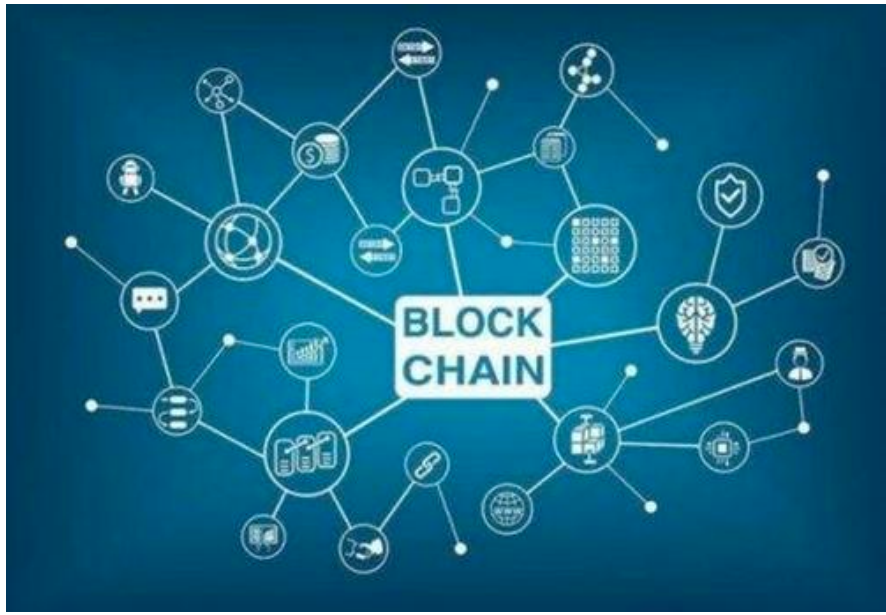
- What type of blockchain should be chosen?
  - Private chain
  - Alliance chain
  - Public chain
- What role does the different participants in the community play?
  - Miner
  - user
  - Core programmer
  - Marginal person or organization
- Whether to establish contact with other blockchains?
- Whether to contact other centralization organizations?

6. Financial economics' perspective

- 6.1 Internet of values : from B/S to P2P
- 6.2 Online information VS on-chain values
- 6.3 Problems of the Internet of Values
- 6.4 Types of assets
- 6.5 Reasons of tokenization of off-chain assets
- 6.6 Coding of various values
- 6.7 Qualification of currency
- 6.8 Token swap will become more important
- 6.9 Cryptofinance

6.1 Internet of values : from B/S to P2P

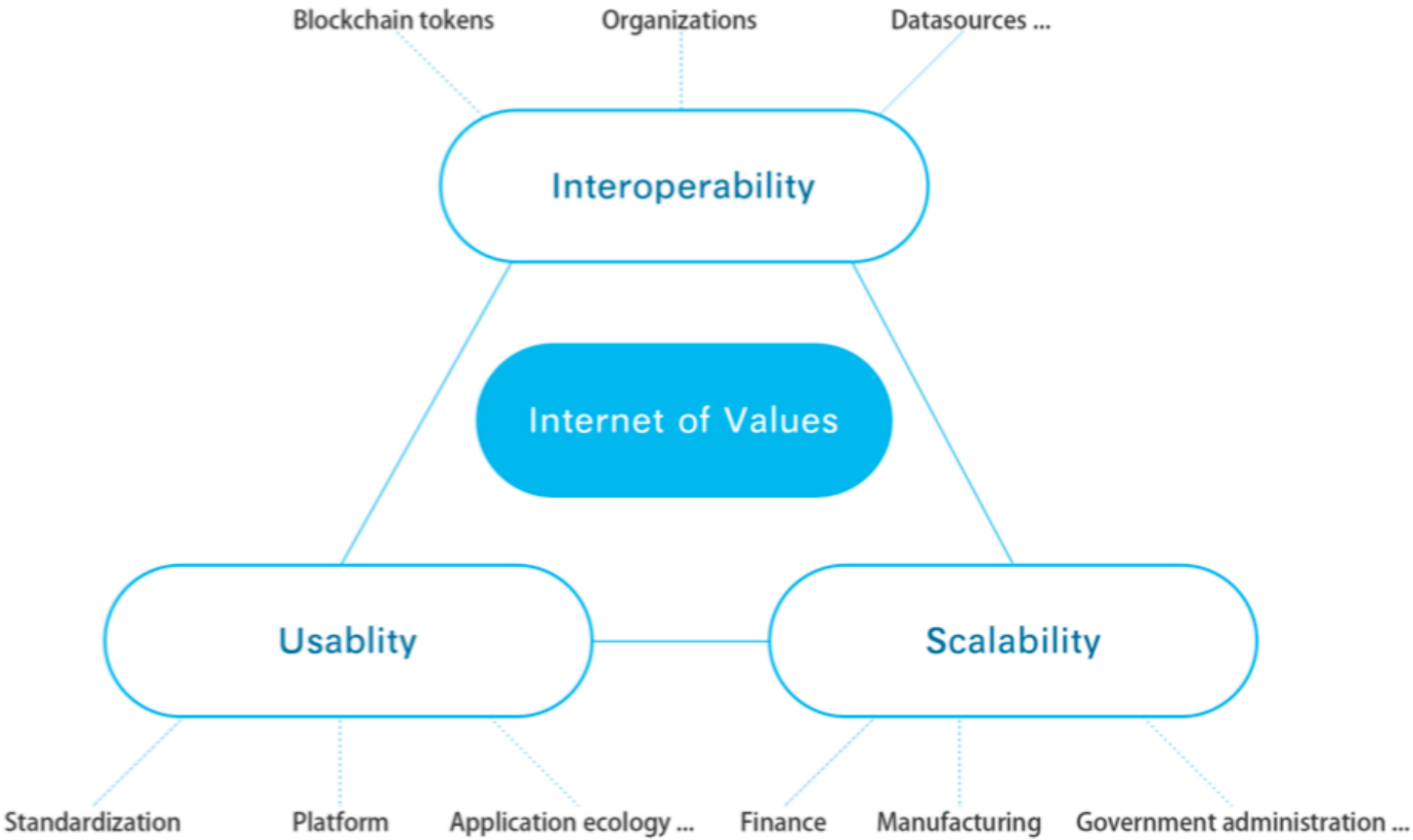
- Architecture for Internet of information
  - TCP， C/S， B/S
  - Interoperability: text, image, audio, video
    - → Various coding methods
    - → Programmable within a unified framework
  - Scalability: PC, mobiles, IoT
  - Usability: modular, web, framework, rich ecology
  - Thin protocol, thick application
- Architecture for Internet of values:
  - UDP， P2P
  - Interoperability: blockchain, organization, data feeds
  - Scalability: token, land, finance, manufacture
  - Usability: standardization, smart contract ecology, SDK
  - Thin application, thick protocol



6.2 Online information VS on-chain values

- Why is information eager to be online?
  - Digitization
  - Rapid spread
  - Programmable
- Will values rush to be on-chain?
  - Digitization
  - Rapid transfer
  - Programmable

6.3 Problems of the Internet of Values



6.4 Types of assets

- What do human need?—driven by secretions, such as:
  - Hormone: release
  - Adrenal gland: stimulation
  - Endorphin: happiness
- Human wealth
  - Unreachable: various resources in the universe
  - Accessible: the resources we are consuming
  - Tradeable: goods
  - Not tradeable: such as air

Types of assets (continued)

- There are mainly three types of assets for humankind:
  1. Physical (atomic, touchable) assets
     - They can be tokenized by bonding services
  2. Data
     - They can be tokenized by bonding services
  3. Gas
     - They are the fuel for running smart contracts

- To sum up, in a more mature society, most assets have been tokenized, so there are mainly two types of assets:
  - Token
  - Coin (gas)

6.5 Reasons of tokenization of off-chain assets

- Easy to use:
  - Easy to represent: symbol
  - Easy to split: digit
  - Easy to carry: bit
  - Easy to calculate: programmed
  - Easy to transfer: p2p transfer
  - Easy to store: wallet
- Programmability

Two ways of realizing programmability of assets

- Centralized bookkeeping
  - With intermediary
  - Difficult to cross organizations
  - Difficult to bound, arrange, trade and protect property rights
- Distributed bookkeeping
  - Disintermediary
  - Easy to cross organizations
  - Easy to bound, arrange, trade and protect property rights

6.6 Coding of various values--identity data

- Proof of reputation
  - Personal ID
  - Diploma
  - Marriage certificate
  - Work ID
- Industry:
  - Multi-party verification service

Coding of various values—behavior data

- Portraits of consumers
  - Geographic data
  - Consumption data
- Industry:
  - Privacy protection
  - Data validation
  - Data mining

Coding of various values—blockchain gas

- Public chain services:
  - Protocol token
- Application token
  - Used in DApps

Coding of various values—atomic assets and human time

- Atomic assets:
  - Land, property, and so on
    - Smart contract mapping
    - Offline delivery
- Human time:
  - Human service
    - Binding services: hosting, accounting, auditing, legal, etc.

Coding of various values—property rights

- Ownership vs. use rights: use rights will become more important
- Token property: for the first time, human can have full control of their assets
- Data property: data privacy and property will be well protected by blockchain protocol
- Offline property rights: they will be eager to be mapped on blockchains.

6.7 Qualification of currency

- Money does not have to have value other than payment
- Metalist VS symbolist
- The monetary system is the record system of human value transactions and the basis of human cooperation.
- Money is essentially a symbol of record value that depends on a certain monetary system, and the monetary system is essentially a widely recognized value bookkeeping system.

Qualification of currency (continued)

- Widely accepted
- Currency unit: have a currency unit that can be used to mark the price.
- The value of it is stable: there is no way to issue it on a large scale, that is, there is a certain scarcity. Or there will be no serious deflation.
- Value balance: ability to record the holder's value balance. That is, if a person claims to have a certain amount of money, it is easier to prove or falsify.
- Value transfer: to solve the double spending problem. That is, when the value is transferred from one party to the other, one party reduces one quantity and the other party increases the same amount.

Gold standard accounting system

- Gold is easy to use in weight units as a currency unit
- Gold is easy to gain wide recognition
  - The characteristics of precious metals are:
    - Relatively soft, easy to divide;
    - Chemically stable, easy to store;
    - Relatively scarce, small in size, easy to carry.
- Gold value is stable.
- Gold is easy to record its balance.
- The gold standard is easy to solve the double flower problem.

Three major effects of the currency world

- Network effect: the amount of resources locked
- Matthew Effect: Snowball
- Standpoint effect: easy to support something once you have it

6.8 Token swap will become more important

- Tokenization
  - Every valuable goods has its own token.
- Barter
  - In trade, barter is a system of exchange where participants in a transaction directly exchange goods or services for other goods or services without using a medium of exchange, such as money.
- Swap:
  - A swap is a derivatives in which two counterparties exchange cash flows of one party's financial instrument for those of the other party's financial instrument.

- Token swap will be more important, currency will be less important.

6.9 Cryptofinance

- Cyptofinance is the finance running on blockchains.
  - Cryptocurrencies: to replace central banks
  - Cryptoassets: to use tokenization to replace securitization services of investment banks
- Industries:
  - Interoperability: to replace exchanges
  - Data feeds: to provide data services
  - Insurance: to replace centralized insurance
  - Traditional banks: need to change themselves as interface for the fiat and atomic world—providing bonding services
  - Funds: to use DAO to replace most funds

7. Application’s perspective

- 7.1 Finance
- 7.2 Manufacture
- 7.3 Proof of reputation
- 7.4 Data management
- 7.5 Communication
- 7.6 Distributed cloud service
- 7.7 Human-machine system

7.1 Application’s perspective--finance

- Finance
  - Issue currencies
  - Exchanges
  - Tokenization
  - Complete financial functionalities:
    - Insurance
    - Securitization
    - Loan
    - Fund
- Projects
  - Bitcoin
  - Ripple
  - Bancor
  - EtherDelta
  - WanChain
  - Fusion

7.2 Application’s perspective--manufacture

- Manufacture
  - IoT
  - Supply Chain: product information traceability
  - Photovoltaic
  - Autopilot system
  - Tolls
- Projects
  - Vechain
  - Ruff
  - Aidoc

7.3 Application’s perspective—proof of reputation

- Proof of reputation
  - Personal ID
  - Storage of legal evidence
- Projects:
  - Ontology
  - Falian
  - Baoquan

7.4 Application’s perspective—data management

- Data management
  - File storage
  - Big data transaction
  - Social media
  - Audio market
  - Video market
- Projects:
  - DataX
  - Filecoin
  - GXchain

7.5 Application’s perspective—communication

- Communication
  - Data privacy: no censorship
  - Rules transparency
  - With smart contract
  - Difficult to block
- Projects:
  - Telegram
  - Skrumble
  - BeeChat
  - Status
  - Steemit

7.6 Application’s perspective—distributed cloud services

- Blockchain platform
  - Storage
  - RAM
  - CUP
  - Consensus
  - DApps
- Projects
  - Ethereum
  - Dfinity
  - GTB
  - Nervos
  - Penta
  - EOS
  - IOTA

7.7 Application’s perspective—human-machine system

- Distributed autonomous organization
- Smart city
- Blockchain autonomous society

8. The calling of blockchain autonomous society

- 8.1 Public chains as infrastructure of virtual societies
- 8.2 Smart contracts as companies
- 8.3 Wet codes and dry codes
- 8.4 Human minds as plugins
- 8.5 Address is everything
- 8.6 Three steps towards a blockchain autonomous society
- 8.7 Welcome to join the Republic of Cryptoeconomy
- 8.8 What should we do?

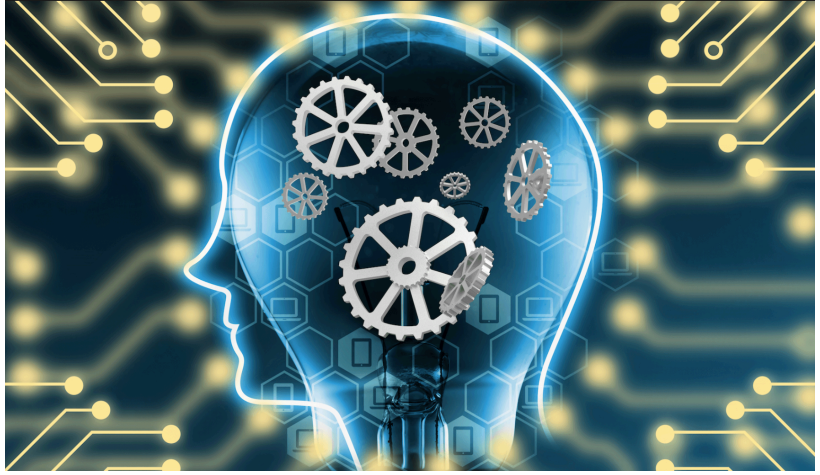
8.1 Public chains as infrastructure of virtual societies

- Distributed cloud services
- Cross-chain technologies will make public chains as an integrated net
- Organizations, individuals and smart programs will interact with each as on the chain

8.2 Smart contracts as companies

- Autonomous society controlled by programs
  - More and more automated
    - Automatic data recording by Internet of Things
    - Automatic decision-making by artificial intelligence
    - Automatic transaction by smart contract
  - The scale of cooperation is growing
    - It takes dozens of people to cooperate in the production of a needle.
    - It takes hundreds of millions of people to make a plane.
- A smart contract embedded artificial intelligence and reliable data feeds can replace the managers of a company to make a company truly unmanned.

8.3 Wet codes and dry codes



- Wet codes: rules in human brains
  - Slow: the speed of brain memory and thinking is very unacceptable
  - Fatigue: sleep 8 hours a day
  - Fraud: The same bed can be a dream
  - Abnormal: antisocial personality destructive type personality
  - Change your mind: people are changeable
  - Calculation error: as long as someone has an error
  - Unable to automate: people and machines can't connect directly
  - ……
- Dry codes: machine codes
  - Flexibility: artificial intelligence, big data is changing the problem of lack of flexibility
  - Trust: blockchain technology is changing the lack of trust

8.4 Human minds as plugins

- How to make wet codes to cooperate with dry codes?
  - To use dry codes as platform for DApps
    - Machine as tools to take care of all boring works
    - Machine as intermediaries to take care of all activities that need trust
  - To use wet codes as plugins
    - Human as consumers, what they do is to enjoy being alive
    - Human as creative activities, what they do is to enjoy being creative

8.5 Address is everything

- An address has its own asset
- An address has its own social medium
- An address can communicate with others at any time
- An address has its own app store, database
- An address has its own reputation
- An address can owned by a person, an organization or a smart program

8.6 Three steps for human-machine system

- Short-term task: to transfer human tasks to machines
  - A lot of **production** is handed over to the machine (smart production)
  - A lot of **decisions** are given to the machine (artificial intelligence)
- Mid-term task: to turn social organization into blockchain DApps
  - A large number of social **organizations** are using machines through blockchain technology to turn human organizations in communities
  - A large number of transactions are handed over to smart contracts to digitalize human **contracts**
- Long-term task: to help human brains connect machine directly
  - **Upload human beings**
  - Human-machine system becomes a pure machine system
    - Machines need to introduce a black box mechanism
    - Machines need to introduce endless desires
    - Machines need to introduce randomness mechanisms

8.7 Welcome to join the Republic of Cryptoeconomy

- Community in the cloud
  - Trading together
  - Have a system
  - Freedom of entry and exit
  - Large-scale, functional **communities**.
- Republic of Cryptoeconomy
  - Interconnected by blockchains
  - Global transfer of funds
  - Strong and large, like a **country**
- Globalization 2.0: a true global **village**
  - Global identity
  - Blockchain assets are difficult for the government to collect taxes
  - Economic entities have no geographic borders

8.8 What should we do is to embrace the future and have fun

- ‘The future is already here — it’s just not evenly distributed’. (William Gibson)
- Let’s:
  - Approach it
  - Understand it
  - Realize it

Thanks for your contribution to the human civilization by spending time on learning!

- Q&A