Innovative Learning Using Smart-Contract Blockchain Technologies

Nian-Shing Chen(陳年興)

Chair Professor

http://www.nschen.net

Which one is the most disruptive technology?

- VR/AR/MR
- IoT
- Big Data
- Machine learning (Deep learning)
- Artificial intelligence
- Robot
- …

The answer is

The Blockchain technology

Why?
The shift from

The Internet of information (Sharing)

To

The Internet of value (Exchange)

So what is Blockchain?

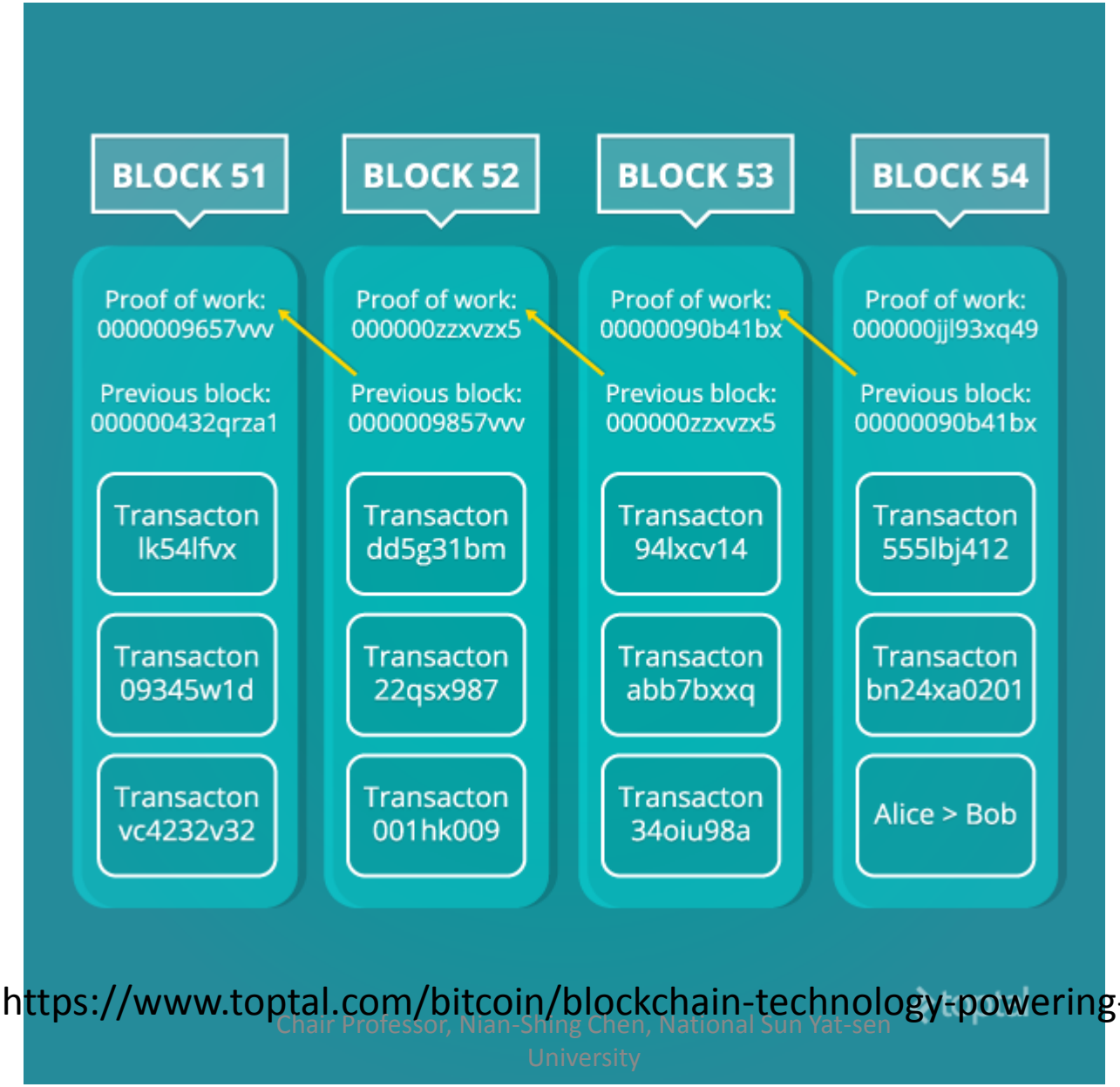
- Online poll using Zuvio (IRS: Instant Response System)

- http://irs.zuvio.com.tw

What is Blockchain?

- A decentralized public digital ledgers
- A complete record of all transactions store on thousands of computers
- Minors competing with each others to maintain the validity of all transactions
- Minors get some digital money as a rearward for their work (Proof of Work)

What is Blockchain?



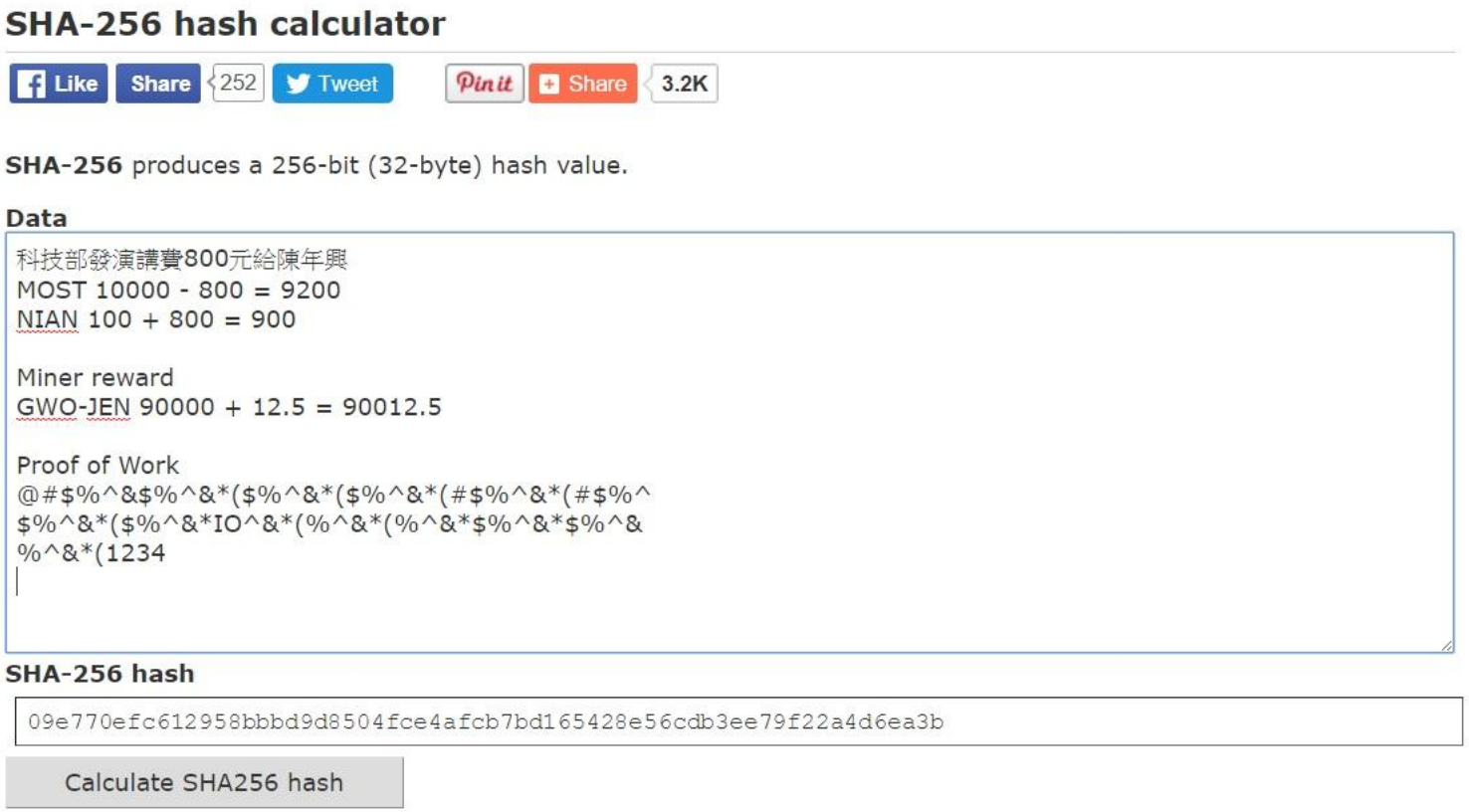
Source: https://www.toptal.com/bitcoin/blockchain-technology-powering-bitcoin

Consensus Algorithms (Mining)

- Proof of Work
- Proof of Stake
- Proof of Zero-Knowledge

How a New Block is created?

- http://www.xorbin.com/tools/sha256-hash-calculator



Facts about the Blockchain

- Blockchain is a disruptive technology which is going to change the whole world
- Blockchain is a new Internet infrastructure for Decentralized Applications (DAPPs)
- Blockchain as a service
- Blockchain is a new supply chain network
- Blockchain is a permission less network
- Ledger recorded in the Blockchain network is immutable

The very first application of Blockchain

Bitcoin
The Digital Gold

So what is Bitcoin?

- Online poll using Zuvio (IRS: Instant Response System)

- http://irs.zuvio.com.tw

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

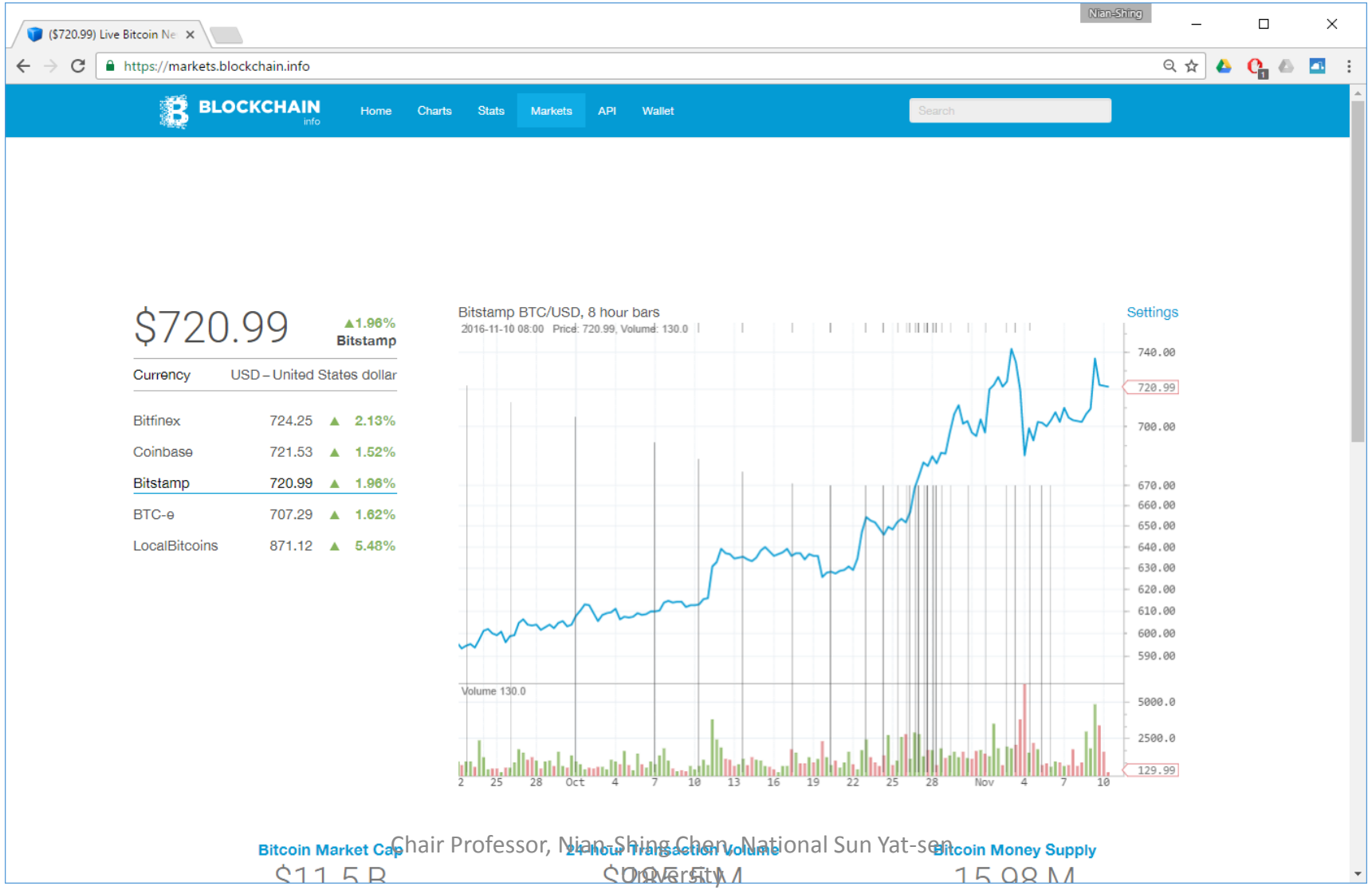
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model

What is Bitcoin?

- A digital cryptocurrency
- A peer to peer payment network without involving any third-party.
- Get rid of the Government capital control
- Store value today for tomorrow using Bitcoin (Digital Gold)

Blockchain Info
https://markets.blockchain.info/



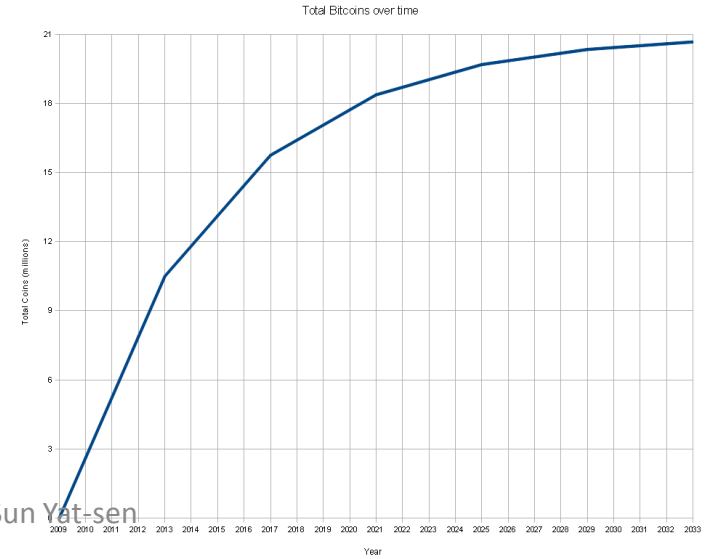
Facts about the Bitcoin?

- 1 BTC = 768 USD
- Exchange rate change based on free market
- It is caped to 21M bitcoins as maximum (Gold)
- Roughtly 10 minutes, a new Blockchain is added into Bitcoin Blockchain
- Miners are competing in the process of validating transactions in a new block, the first one achieve the goal get some bitcoins as rewards
- Initial 50 bitcoins (2009), 25 bitcoins (2012), 12.5 (2016), 6.25 (2020), …
- A total of 5417 nodes in the Bicoin network as the date of 2017/11/01
- The Size of the Bitcoin Blockchain Data Files Has Reached 60GB

How many bitcoins will there eventually be?

- A pre-defined schedule limits the total number of bitcoins so that they gradually approach a total of 21 million (ignoring those that have been lost through deleted or misplaced wallet files). **The limit of 21 million bitcoins is "hard-wired" in to the protocol**, and there will never be more bitcoins than this.

$$\sum_{n=0}^{\infty} \frac{210000 \times 50}{2^n} = 210000 \times 50 \times \frac{1}{1-\frac{1}{2}} = 21000000$$



What is Ethereum?
https://www.ethereum.org/

- **Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference.**
- **These apps run on a custom built blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property. This enables developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet, all without a middle man or counterparty risk.**

What is Smart Contracts?
https://en.wikipedia.org/wiki/Smart_contract

- **Smart contracts** are computer protocols that facilitate, verify, or enforce the negotiation or performance of a contract, or that make a contractual clause unnecessary. Smart contracts usually also have a user interface and often emulate the logic of contractual clauses. Proponents of smart contracts claim that many kinds of contractual clauses may thus be made partially or fully self-executing, self-enforcing, or both. Smart contracts aim to provide security superior to traditional contract law and to reduce other transaction costs associated with contracting.

What is Zcash?

- Zcash (ZEC), the new digital currency lauded for its privacy features, is launching Oct. 30, 2016 midst some massive hype. But until enough tokens become available on exchanges, Zcash enthusiasts are poised to acquire their ZEC first-hand by mining for it, either by setting up a home rig or by signing up for a cloud mining contract.
- Created from a fork of Bitcoin's codebase, Zcash promises all the best features and stability of Bitcoin with the added bonus of total payment confidentiality. Zcash transactions can be shielded to hide the sender, recipient and value of all transactions on the blockchain. Only those with the correct view key can see the contents.
- Another interesting aspect of Zcash is it uses a memory-hard proof-of-work known as Equihash. This means the best hardware for mining Zcash tokens is standard GPUs and RAM. The hope is this will lead to a more decentralized set of miners.

The needs for different kinds of cryptocurrencies

- The existence of Bitcoin is the first cryptocurrency using open blockchain technology (proof-of-work)
- The existence of Ethereum is the first programmable smart contract using open blockchain technology (proof-of-stake)
- The existence of Zcash is the first privacy guaranteed open blockchain technology (Zero-knowledge proof)

Educational Applications Using Blockchain

- A handful of schools have also started to experiment with the blockchain, primarily in creating cryptographically-signed, verifiable certificates.
- These include MIT (the Media Lab, specifically), the University of Nicosia in Cyprus, and the (unaccredited) Holberton School, an alternative, teacher-less software engineering school in San Francisco.
- The King's College in New York, and Simon Fraser University in British Columbia, also announced that they would accept the cryptocurrency for tuition payments.

Learning is Earning
http://www.learningisearning2026.org/

- Until recently, we thought of learning, earning, and living as separate experiences. We went to school when were young. We spent our adult years working, and we squeezed our personal lives into whatever brief windows of time were left.
- But imagine a world where all of this has changed.
- Imagine a world, ten years in the future, where learning has become a kind of currency that ties together every aspect of our lives.
- In this future, the currency of learning is tracked and traded on a digital platform called the Ledger. It's a complete record of everything you've ever learned, everyone you've learned from, and everyone who's learned from you. The Ledger not only tracks what you know - it also tracks all of the projects, jobs, gigs, and challenges you've used that knowledge to complete.

Sony Develops Blockchain Tech for the Education System

- Sony is looking to leverage blockchain and its secure properties by developing a blockchain-based technology that establishes secure open sharing of academic proficiency and progress records through encrypted transmission.
- After taking an examination to demonstrate his or her academic proficiency level, an individual could direct the testing organization to share the test results with one or more third-party evaluating organizations
- With this infrastructure in place, each evaluating organization sent an individual's testing records could assess those results and calculate a score in a way that fits its own methods.
- A platform for sharing your qualification and educational history.

Two Key factors

- The very low cost and easy implemented micro-level transactions with value (money)
- The transparent global trust-worthy blockchain networks

My ideas

- Learning is a smart contract between related stakeholders
  - Write and execute within Smart Contracts on public blockchain networks
- For students: Earn portion of your paid tuition back by demonstrating the degree of your efforts and the level of learning outcomes
- For teachers: Improve the quality of course delivery by the percentage of fulfillment according to the original course designs
- For everyone: Trade your future success and profit today for investors

My Visions

- There are four essential values of our humanity in the 21st century: SECURITY, PRIVACY, TRUST and EQUALITY.
- The way to offer these four values to every single person on this planet is to provide trust-worthy peer-to-peer transactions executed by decentralized applications without middle man based on the new upper-level Internet infrastructure using the Blockchain technologies.
- In this new state/society, all transactions/operations can be audited by anyone and all the governance are fully transparent to everyone.

My Suggestions

- The most important national development project/initiative for many countries is to build:
- An advanced Internet Infrastructure using the "Blockchain" technology on top of the existing Internet.
- This new Internet infrastructure will enable decentralized Smart-Contract applications to flourish [Dapps].

Blockchain Infrastructure

- The 20th century's national infrastructure is more "Hardware-oriented" like High Speed Rails, Internet Backbone Routers & Fiber-optics Cables, etc.
- The 21st century's national infrastructure should be more "Software-oriented" like Smart Contracts Platforms, Blockchain-Ready Internet Infrastructure, etc.
- There are four pillars needed to build such kind of software-oriented infrastructure, NATIONAL POLICY, TALENT EDUCATION, CORE TECHNOLOGY, PLATFORM & TOOL, LAW & REGULATION.

Conclusion

- In conclusion, the most important core technology today is “The Blockchain Technologies”. This technology is going to change everything we know today about how the state govern, the institution function, the business operate, the education provide and the living of people’s daily life.
- So, my dear friends, please join the next generation of the Internet where “BLOCKCHAIN As A Service” is a new norm”.

Some useful tutorial videos

- Understand the Blockchain in Two Minutes by Institute for the Future (IFTF)
  - https://www.youtube.com/watch?v=r43LhSUUGTQ
- What is Blockchain (13.58min) by Prof. Shai Rubin
  - https://www.youtube.com/watch?v=93E_GzvpMA0

Useful Youtube Videos

- 'Understanding The Blockchain' Andreas Antonopoulos
  - https://www.youtube.com/watch?v=OxFI02XFwio
- "Blockchain. The Era of Disruption" – Alex Tapscott
  - https://www.youtube.com/watch?v=gA7Fsa9Tr94
- What the #?!* is Bitcoin? | Jeremy Rubin
  - https://www.youtube.com/watch?v=Vzjtvt77mgc

Useful Websites

- Bitnodes is currently being developed to estimate the size of the Bitcoin network by finding all the reachable nodes in the network.
  - https://bitnodes.21.co/
- Blockchain network live updates
  - https://blockchain.info/
- Network Where Active Traders Exchange Ideas
  - https://www.tradingview.com/chart/
  - http://www.plus500.com/
- CRYPTO MINING BLOG
  - http://cryptomining-blog.com/
- Ethereum Community Forum
  - https://forum.ethereum.org/

新一代Internet基礎建設已經啟動了

The Internet of Information Sharing

To

The Internet of Value Exchange

第一波Internet: 是一個以資訊分享為主的網路

to

第二波Internet: 是一個以價值交換為主的網路

Q&A

Thanks for your attention, you may send some bitcoins to my wallet.

Tap to copy this address. Share it with the sender via email or text.

15bRuUkZhdC1XWr6qYLSgPiZbcvew5yFiL

Chair Professor, Nian-Shing Chen, National Sun Yat-sen University