

Fintech Tsunami: Blockchain as the Driver of the Fourth Industrial Revolution

David LEE Kuo Chuen, Singapore University of Social Sciences

Introduction

When the Internet was first created in the 1990s, no one expected it to have such a great impact. Blockchain is in a similar position today. In the strictest sense, the term blockchain refers to appended immutable blocks of information by a pre-determined consensus algorithm. Satoshi Nakamoto (2008) circulated his white paper on it to a group of Cypherpunks.¹ The community was then excited but no one outside knew that it would be so influential. That paper described how a digital currency created by cryptography called bitcoin (using blockchain technology) can transfer value without any central authority.

Although Nakamoto (2008), creator of bitcoin, did not use the word blockchain in his seminal publication, there were a few sentences linked to blockchain).² The concept of *Cipher Block Chaining* was first mentioned by Ehrsam, Meyer, Smith and Tuchman (1976). Bitcoin features are very powerful, but their implications are neither fully understood nor revealed yet. Nonetheless, blockchain, as one of its underlying technologies, is now hailed to be the main game changer for the 4th industrial revolution.

The sections to follow in this chapter will discuss Bitcoin as the most popularly-known practical application of blockchain, the role of blockchain in the new digital economy and the characteristics of a sustainable blockchain company; and elaborate on the 4Ds, LASIC principles, Hinternet, and the deep business skills and strategies needed to excel in the blockchain industry.

Bitcoin

After the first Bitcoin block was created in early 2009, the world experienced a revolution that few understood. Indeed, without many knowing it, the invention of the resultant Bitcoin network – with a capital B to differentiate it from the small b for the digital currency bitcoin it creates – begun a global shift just like the Internet did (Lee 2015a and 2015b). Reaching a current market value of over USD40 billion in 2017, Bitcoin has lasted more than 9 years now.

The key reason no entity or person that tried to create a new currency system before was ever successful is that they operated within the system. The Bitcoin network transformed businesses by defining a class of business entities that either has no legal status, or is very difficult to enforce a closure when there is one. Without a collective legal entity status, this particular class of entities now exists in a space that is outside the jurisdiction of both fiat currencies and legal systems that we know of or operated in.

The reaction of most people when they first heard about bitcoin was almost certainly negative, or with a sense of confusion. There was a misguided perception that bitcoin was used mainly for money laundering, or as payments for drugs and pornography. But most also realized simultaneously that the mathematics, cryptography, system design, and philosophy behind the network were created by a genius or geniuses who understood the imperfections of the global economic and financial system. Naturally, it appealed to

those who were losing faith in the fiat system, and to those who believed that existing financial and economic systems were biased and functioned to generate wealth exclusively for the wealthy.

The major social-economic contribution of bitcoin was the use of a decentralized filing system and peer-to-peer network to redefine a world using only open-source software concurrently ran by many users anywhere in the world. The second contribution of bitcoin was the elimination of the need for a middleman for the verification of transactions or records. Previously, centralized activity would require an intermediary to facilitate or verify transactions of goods and services, but this is not required if there are many copies of a public register with timestamps. The third contribution was the removal of known identities. With decentralisation, all you need is a public address and a private key to facilitate any movement of values or digital assets using cryptography. There is no need for personal identity information – a major headache for financial institutions that need to comply with *Know Your Client* regulations.

Digital Economy and the 4Ds

The new digital economy introduces new thinking, particularly the 4Ds (Digitalisation, Disintermediation, Democratisation, and Decentralisation). As incumbents struggle to hang on to what they have and are comfortable with, mindset is more important than skillset. This display of inertia prompted many thought leaders to be forceful in their public speeches, to get the change going. Perhaps the following quotes will demonstrate the thoughts and attitudes towards innovation in a transforming economy:

1. “It is not the (offline) economy that is in trouble, it is your (offline) business that is in trouble.” – Jack Ma’s speech (paraphrased from Chinese) to the business community warning that business change may not be fast enough, against the rise of the Internet and Artificial Intelligence (AI). He sounded the alarm about disappearance of physical stores and businesses with the introduction of e-commerce years ago.
2. “Failure is an option here. If things are not failing, you are not innovating enough.” – Elon Musk of Tesla, in response to the many who believe in processes rather than outcome in the new economy. The fear of not being able to change has prompted him to conclude that processes are for people who are incapable of changing the mindset of incumbents.
3. “This is your last chance. After this, there is no turning back. You take the blue pill – the story ends, you wake up in your bed and believe whatever you want to believe. You take the red pill – you stay in Wonderland, and I show you how deep the rabbit hole goes. Remember: all I'm offering is the truth. Nothing more.” – Morpheus, the prophetic forerunner character in *The Matrix* movie, explaining to saviour-to-be Neo that the Matrix is an illusory world. The two pills are popular culture symbols representing the choice between embracing the sometimes-painful truth of reality (red pill) and the blissful ignorance of illusion (blue pill).

Paradigm Switch in the Production Function

The fourth industrial revolution, evolved from digital innovation, has rewritten the entire production function with emphasis on a different set of factors. In classical economics, the essential factors of

production are land, labour and capital. However, the arrival of digital devices, the Internet, and the ability to harness data changed the landscape of the economy and business. The new economy cares more about data, time, and capital-raising ability. Let's examine these factors together.

In the supply chain of e-commerce and online business, land and geographical location are less important since the computational power server they use occupies a small area and can be located far away in the digital Cloud. Labour can be replaced by data technology that helps to serve customers better than before; and if that is not enough, AI and robots can take of mundane and factory jobs.

Machinery and equipment that workers leverage to produce goods efficiently are capital in the old economy. With the convergence of data technology, computing power, 3D printing, and other software and hardware; and the long (7 or more) years before reaching profitability, the ability to raise funds displaces the acquisition of physical equipment as the new essential for businesses. Good fundraisers, using keen understanding of investment behaviour change, need to entice investments into businesses with long profit drought in return for exponentially large gains.

There is little point in making distinctions among the 'old economy' primary or secondary factors of production of land, labour, and capital; it is more important to focus on the 'new economy' essential factors of data, time, and the ability to raise funds. This means that any new economy business that is not investing enough in data technology, computing power, and ability to attract new funds will be irrelevant in the future economy.

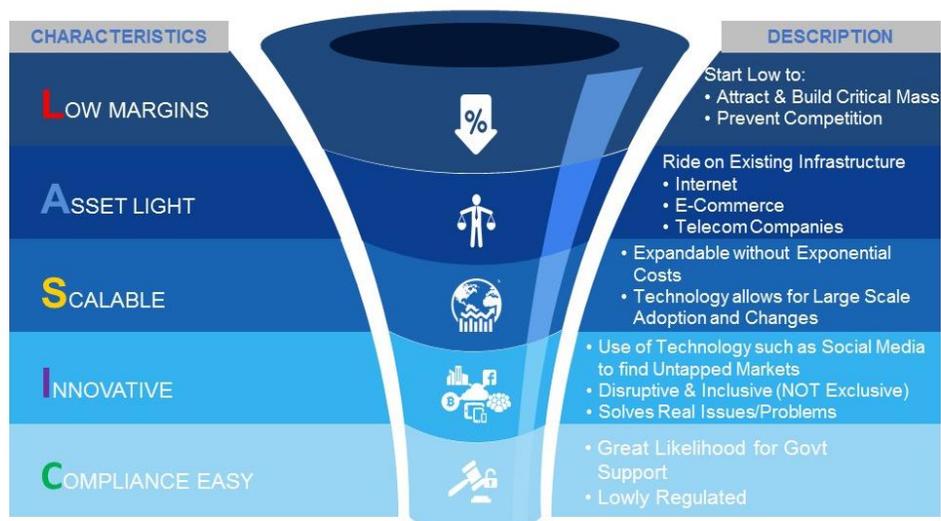
LASIC Principles

As the economy started moving towards a digital-base, with AI, Big Data, Internet of Things (IoT), 3D printing, and blockchain, research studies were conducted to search for factors that are common to successful companies. In their studies, Lee and Teo (2015) explore the characteristics of successful companies such as Ant Financial, M-PESA and Fidor Bank. Ant Financial's Alipay has close to 500 million mobile users, and both M-PESA and Fidor Bank have grown substantially in a short time period.

All three companies exhibit the LASIC (Low Margin, Asset Light, Scalable, Innovative, and Compliance Easy) characteristics (see Figure 1). Attracting critical mass with low margin and preventing competition from others are essential for these online businesses. The companies that incur substantial capital expenditure tend to have high depreciation cost. However, riding instead on existing infrastructure such as the Internet, E-commerce platforms and telecom facilities allows them to operate with a light balance sheet. As a result, these companies can scale without exponential costs and with existing technology expanded easily to meet changing demand from adopters.

At the same time, their business models are innovative in searching for underserved and untapped markets with disruptive, yet inclusive technology to address pain points of customers. Finally, most of them operate in a compliance friendly environment with government support and are almost unregulated in some areas of business.

Figure 1. LASIC Principles



Lee, David K.C. and Teo, Ernie G. S., Emergence of Fintech and the Lasic Principles (September 30, 2015). Available at SSRN: <http://ssrn.com/abstract=2668049>

In discussing these models that conform to the LASIC principles, researchers point out that to build a Hinternet, decentralisation is not a necessary condition. A Hinternet is a virtual or digital space with a large population of sticky customers such as Alibaba's e-commerce platform on the Internet. Alipay and Grab have large LASIC Hinternets that ensure they can sell a wide range of products to the sticky customers (Lee 2016; Lee & Dula 2016). Blockchain is not needed for building a Hinternet business, but for sustained growth, the last D, i.e., decentralisation, is needed and thus may involve blockchain.

Decentralisation builds a higher barrier so that monopoly and oligopoly market structures will not take shape easily. A Hinternet that has grown too large in size may create systematic risk and thus attract regulation to break it up. With decentralisation, regulation may play a smaller part but the purpose of the democratisation of information, technology, and services is achieved. Price discovery in a decentralized environment is an important issue but beyond the scope of this paper.

Satoshism

The timing of the release of the Nakamoto (2008) paper coincided with the global financial crisis. While the actual identity of Satoshi Nakamoto is not known, Satoshism that embraces decentralized sharing of immutable data, P2P consensus algorithm, and anonymous access has many followers. The main reasons stem from the imperfection of the existing financial architecture:

1. Lack of Transparency. Transaction details and fees were opaque, with high costs for cross border transactions.
2. Lack of Resilience. Fears of potential lack of business continuity by single points of attack, and the perceived lack of protection of historical record.
3. Lack of Distribution of Wealth. Lack of decentralized and super-divisible money – the smallest unit of bitcoin is 10^{-8} BTC or 1 Satoshi but theoretically, higher precision is possible – that catered to the

bottom of the pyramid. There was also a lack of suitable technology to distribute wealth and assets more evenly over time with more than 70% of the people being excluded from the financial and economic system.

4. Lack of Individual Control of Privacy. Lack of control over encrypted personal data.

The philosophy of Satoshi is however not without its weaknesses. First, a decentralized network is less efficient than a centralized one. In terms of transaction per second and latency, a centralized network can be organized more efficiently. With Proof of Work that is not only computationally expensive, it is also environmentally unfriendly. With blockchain, storage of data is an issue and each individual block size is a point of contention. Storing multiple copies is far from being space efficient.

Second, there is a lack of privacy because the public ledger records all transactions. And third, there is a lack of further guidance from Satoshi as he has faded into the background with the community testing the boundaries of his creation. The issue of first mover advantage in ownership (No Expiry Date of Ownership) is an issue for those who believe in intergeneration equity. Bitcoin technology can be hijacked to rule society rather than serve it by convincing the majority of the users to focus on profit motives and self-interest rather than the community's interests.

Blockchain Essentials

A good blockchain should possess the following qualities:

1. LASIC principles
2. Resilience
3. Transparency of transactions
4. Personal control of privacy
5. Enabler for 4Ds
6. Enabler for collaboration of untrusted parties globally
7. Enabler for asset ownership sharing globally

Despite the hype about blockchain since 2015, it is just a new form of database, the special kind that allows shared ownership across organisational boundaries. There are two types of blockchains: Private and Public. The differences between them are tabulated in the Figure 2 below. Both types are similar in design, but worlds apart in use cases (Lee & Ding 2017; Lai & Lee 2017). Whereas in contrast, the differences between Private Blockchains and Databases (see Figure 3) are similar in use cases, but worlds apart in design.

Blockchain is a form of distributed ledger with specific distinguishing features that other distributed ledgers may not have. In particular, the decision to have a blockchain is usually engendered by a certain degree of distrust among nodes users. Another critical push-factor is the requirement for transparency for the entire or part of the ledgers. Finally, blockchains are useful if there is a need to ensure that past records are almost permanent with every node, or made available to every node. Without the need for improvement of trust and transparency, it may well be more efficient to use a distributed or centralized ledger.

Figure 2. Comparing Private and Public Blockchains

Conditions	Private Blockchain	Public Blockchain
Centralization /Purpose	Semi-decentralized Business-to-business	Decentralized Peer-to-Peer
Authentication	Authenticated	Not-authenticated
Permissions	Permissioned	Permission-less
Advantages	<ul style="list-style-type: none"> • Support legal entities • Higher performance • Better scalability 	<ul style="list-style-type: none"> • Support anonymity • Higher immutability • Trustless environment

Figure 3. Comparing Private Blockchains and Databases

Conditions	Private Blockchain	Traditional Database
Ownership	Designed for shared ownership	Not designed for shared ownership
Performance	Slower	Faster
Scalability	Easier and cheaper	Harder and expensive
Immutability	Append-only	Editable

There is a class of very powerful blockchains that records and transfers tokens with value. This special feature allows blockchain to create tokens in the form of transferable “currency” or “stake”, just like national currencies and shares in the fiat currency world.

Digital Asset Ownership

The most powerful feature of blockchain is to allow for shared ownership of assets or rights. There has been a great interest in Initial Coin Offerings (ICO), sometimes known as Initial CryptoToken Offerings (see Figure 4) and basically an Initial Token Sales (ITS). ICO may sound like IPO (Initial Public Offering), but it has a totally different structure and almost no legal recourse.

Figure 4. ICO Status Statistics³

ICOs Status	Number
Past	139
Ongoing	15
Upcoming	57
Total	211

The Top 10 ITSs (see Figure 5) are successful in that they have raised a substantial amount of proceeds in the form of Cryptocurrency in exchange for the Tokens being sold. For an ITS to be successful, the founders or project must have an Online Identity, with a good Standing in the Community (, issue a technical and other Whitepapers, publish its Technology and Source Codes, conduct a Pre-Sales with clear Reward/Incentives Structure, transparent with its Use of Proceeds and Valuation, Outline the Governance Structure, and engage prominent Advisors and Governors.

Figure 5. Top 10 ITS (as at 15 April 2017)³

Name	Amount (USD)
ETHEREUM	18,439,086
COSMOS	16,800,000
WAVES	16,436,095
QTUM	15,664,829
GOLEM	8,600,000
FIRSTBLOOD	6,267,767
LISK	6,150,000
DIGIXDAO	5,500,000
AUGUR	5,133,000
Total	98,990,778

DAO	150,000,000
Total	248,990,778

Unlike shareholding in an IPO, an ITS must specify role of the tokens being sold. In general, there are three possible roles: user, commodity and debt (Brener 2016). These roles can be summarised as follows:

1. User Tokens (App Coins or Protocol Tokens): access services provided by the distributed network.
2. Commodity Tokens: finance development of the network.
3. Debt Tokens: 'short term loan' to the network, in exchange for interest payments on the amount.

The Token software can create user; commodity; debt; user and commodity combination; or user, commodity, and debt combination tokens. However, unlike shares, these tokens may 1) have no voting rights, 2) have not cash-flow distribution, 3) have no legal rights and recourse, 4) have no group decisions rights, 5) have no shares and debts, 6) have no avenues to remove the management, and 7) be building user base, investor base or both. We can summarise token rights as Payments, Access, Profit for Fees, Contribution, Block Creation, and Governance. More than half of the tokens issued have payments and access rights (discussed in Lee 2017 and Chwierut 2017).

Hybrid Legal or Crypto Structure

Under the Howey four-pronged test of US Security Regulation, an instrument is a security if it 1) involves an investment of money or other tangible or definable consideration used in, 2) a common enterprise with, 3) a reasonable expectation of profits to be, and 4) derived primarily from the entrepreneurial or managerial efforts of others. If a token falls under the definition of security, then security laws and regulation will apply. So, there are good reasons to approach ITS with care so that there is no violation of law and regulation. Another US legal question is to determine if a Blockchain is a transfer agent. If it is, a license is required under the law SEC (1946).

In countries where tokens are not securities, there are four models that have been used to launch an ITS:

1. Award of Contract. A legal entity (e.g., Pte Ltd) awarded a contract by a client (blockchain) to write the code for the blockchain, and subsequently have an ICO of the resulting blockchain with tokens.
2. Commodity Sales. A foundation (e.g., Swiss GmbH-LLC) initiates a sale of a commodity (fuel/token) required to run the blockchain on an open source platform.
3. CODE. Centralized Organized (CO) legal entity spends the tokens collected from the Decentralized Entity (DE) blockchain ICO and the CO also collects the revenue generated, for example, after the project of building an app.
4. Plain Vanilla Token Allocation. Tokens are first mined by allocators and allocated via a computer algorithm that does not specify any specific public addresses to receive funds.

Is ITS & DAO Structure all Bad?

Lior Zysman (2017) argued that ITS has perhaps brought many benefits to the community:

1. Flows of funds are recorded real-time on an open blockchain.
2. The new JOBS Act Title 3, which opens investment in startups to individuals, requires startups to publish financials once a year; in contrast, blockchain accounting guarantees their investors financial reporting all year long. The Act also requires businesses to publish a business plan once a year. In contrast, some ITSs are powered by transparent open-source codes that any machine on a distributed network can run.
3. Funds that the ITS directs are also published on the blockchain, and the by-laws themselves that determine the relationship between the ICO participants are embedded in the code.
4. The execution of those bylaws and ITSs accounting do not depend on familiar figures, like the CEO or an auditor, although the status of humans on the edges of the network or curators has never been debated in case law and might be replaced using formal verification methods.

Zysman contends that, perhaps for the first time in corporate history, investor expectations – a big concern for lawmakers and regulators – are being directly met by the ITS code. Communication is key in selling the token, transparency is essential with no over-promising of product goals or return on investment. It is best to emphasize that these are experiments and to ensure there is awareness of the fiduciary duties.

There are many ICO Scams! So, buyers beware. ICOs rank high in terms of Risk and Complexity Classification, indicating there is a high uncertainty of outcome. As such, these tokens are not suitable for widows and orphans, speculators, traditional fund managers, and sophisticated investors. Given that it is an experiment and suited for a learning portfolio that may have zero rate of return, the participants should be from the community of blockchain, mentors, and angel investors.

Concluding Remarks

Blockchain is not needed in many use cases where database will do. For sustainability and network effect, blockchain must scale to serve the underserved. It will scale faster if it is open, engages AI, Big Data, and IoT.

We need to watch and plug into China, which has mastered the skills of scaling, financial inclusion, and user experience. The business strategies of combining economies of scales and economies of scope in Fintech will spill over to blockchain in China with emphasis on financial inclusion and green finance. China will dominate the blockchain industry because of its size and capital expenditure on research and development.

Unlike company shares that give voting rights and a share of the profits, Crypto Tokens are just an entitlement to rights. These are rights to facilitate P2P payments, rights to access and use a network, rights to share the profits from a crypto cash-flow business model, rights to contribute to a network for charity or other activities, rights to create a new blockchain or a block of data, and the right to participate in governance activities. ITS/ICO is a new way to raise global funds in a crypto economy. ITS's or ICOs are for those interested in the technology and its associated experiments. An online identity with community spirit, a good understanding of fiduciary duties, transparent communication, under-promise in technology goals, no promise of ROI, and assisting communities to serve the underserved are key success factors.

It should be emphasized that the most powerful feature of blockchain is the sharing of asset ownership, which takes place in a centralized environment that lacks full trust and is in need of democratisation of information, technology, services, as well as micro ownership. Blockchain will be the driver of the fourth industrial revolution as it enhances not only the productivity of the system, but harnesses the talents of an open and inclusive community. There is no lack of capital nor a lack of good technology. But, no amount of capital or technology can do what blockchain does: enhancing collaboration and enabling distrust parties working efficiently together in a decentralized and innovative environment. Those powerful crowdsourcing and harnessing features make blockchain the main driver for the fourth industrial revolution.

Notes

1. See <https://en.wikipedia.org/wiki/Cypherpunk>.
A Cypherpunk is any activist advocating widespread use of strong cryptography and privacy-enhancing technologies as a route to social and political change.
2. See <http://ethereum.stackexchange.com/questions/4454/who-coined-the-term-block-chain/4455>.
 - a. On Page 3. "As later blocks are chained after it, the work to change the block would include redoing all the blocks after it."
 - b. On Page 7. "This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at "that moment."

3. Data extracted from:

<https://cyber.fund/radar>

<http://Icocountdown.com>

<https://www.ico-list.com>

<http://iof.hexun.com/2016-07-25/185142280.html>

https://en.wikipedia.org/wiki/List_of_highest_funded_crowdfunding_projects

<http://icorating.com>

<https://tokenmarket.net/ico-calendar>

<https://coinmarketcap.com/assets/maidsafecoin/#charts>

<http://digitalmoneytimes.com/equinoxcoin-turns-into-a-scam-after-bittrex-ico-despite-coinssource-rating/>

<https://safenetwork.wiki/en/FAQ>

References

Brener D 2016. On Tokens and Crowdsales: How Startups Are Using Blockchain to Raise Capital (<http://www.coindesk.com/tokens-crowdsales-startups/>)

Chwierut M 2017. Token Rights: Key Considerations in Crypto-economic Design. (<https://www.smithandcrown.com/token-rights/>)

Lai R & Lee DKC, 2017. From Public to Private Blockchain. In Handbook of Blockchain, Digital Finance and Inclusion. Edited by Lee DKC & Ding R. Academic Press, Elsevier.

Lee DKC 2015a. On the Edge of Disruption. *Asia Management Insights* 2(2) (http://ink.library.smu.edu.sg/lkcsb_research/4870/).

Lee DKC 2015b. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. Elsevier, Academic Press (<https://www.elsevier.com/books/handbook-of-digital-currency/lee-kuo-chuen/978-0-12-802117-0>)

Lee DKC 2016. The Fintech Promise. *The European Financial Review*. 23 June (<http://www.europeanfinancialreview.com/?p=6093>).

Lee DKC 2017. The Deep Skill of Blockchain Business (<https://www.slideshare.net/DavidLee215/the-deep-skill-of-blockchain-david-lee-27april2017-final>).

Lee DKC & Dula C 2016. How the Internet is Democratizing Global Finance. *The Straits Times*. 23 February (<http://www.straitstimes.com/opinion/how-the-internet-is-democratising-global-financeLee>).

Lee DKC & Teo E 2015. Emergence of Fintech and the LASIC Principles. *Journal of Financial Perspective* 3(3) (<https://fsinsights.ey.com/thejournal>).

Lee DKC & Ding R 2017. *Handbook of Blockchain, Digital Finance and Inclusion*, Volumes 1 and 2. Academic Press, Elsevier.

Nakamoto S 2008. Bitcoin: A Peer-to-Peer Electronic Cash System (<https://bitcoin.org/bitcoin.pdf>).

SEC 1946. Securities and Exchange Commission v. W. J. Howey Co. 328 U.S. 293.
(<http://www.casebriefs.com/blog/law/securities-regulation/securities-regulation-keyed-to-coffee/definitions-of-security-and-exempted-securities/securities-and-exchange-commission-v-w-j-howey-co/>)

William FE Meyer CHW, Smith JL & Tuchman WL 1976. Message Verification and Transmission Error Detection by Block Chaining. US Patent 4074066.

Zysman L 2017. DAOs and Securities Regulation (<https://www.smithandcrown.com/daos-securities-regulation/>).