Can Blockchain Untie Itself from Bitcoin
Blockchain Industry Outlook Through 2024

Author: Ethan Harden

KEY TAKEAWAYS

- *Blockchain is being used by companies today but will see more rapid adoption across all consumers when standard processes are in place. Enterprise blockchains will open the door to understanding and building these initial solutions.*

- *Cryptocurrency is the least scalable version of a blockchain token, although it has pushed blockchain into the public conversation.*
.
- *Supply-chain transparency, healthcare, and financial services are the three major industries set for disruption in the short term due to high transaction volume and administrative costs.*

BACKGROUND

Blockchain technology has been introduced to the masses in a sub-optimal way through the hype, and subsequent correction, of Bitcoin, Ethereum and other cryptocurrency platforms. However, its true value lies in synchronizing the flow of goods, information and money between partners. In essence, business is the exchanging of value or ownership, and with blockchain's potential to simplify, secure, and facilitate trade, it offers major benefits to a wide spectrum of businesses and consumers. Santander Innoventures expects blockchain technology to lead to $15-$20B in annual savings in banking infrastructure costs by 2022.[1] Combined with smart contracts, the basis for supply-chain visibility exists creating less friction and a faster flow of assets to supercharge business markets.

Businesses are feeling pressure from both consumers and other partners within their vertical to develop better supply-chain transparency, record management and efficiency therefore increasing the speed of transactions. Blockchain has the capability to move all these essential business functions into the 21st century with its ability to securely facilitate the exchange of value and ownership. The blockchain arena is heating up quickly as more startups are bringing worthy enterprises and ideas into the investment space. According to a recent Diar report, venture capital investment in blockchain related companies has nearly tripled in the first 3 quarters of 2018 compared to all of 2017.[2] Bolstering this number is the fact that nearly 2,000 investors have invested in at least one blockchain company including Andreessen Horowitz, Danahua Capital and other notable angel investors Tim Draper and Roger Ver.[1] Illustrating the demand for this market is both the number of deals and median deal size doubling with deal size moving from about $1M to over $2.5M from 2017 to 2018. Interestingly, the ten largest deals of 2018 totaled $1.3B with nine of the ten representing traditional equity investments, rather than purchases of cryptocurrency.[3]

MARKET SIZE

Pitchbook indicates that through three quarters of 2018, blockchain and crypto-related firms have raised almost $3.9B in venture capital, representing a 280% increase as compared to 2017.[2] With the increased pace in which use cases are arising and a multitude of companies trying to solve blockchain related problems, Global Market Insights projects the blockchain market size will cross $16B by 2024,

[1] https://www2.deloitte.com/tr/en/pages/finance/articles/cfo-insights-getting-smart-contracts.html#

[2] https://cryptoslate.com/venture-capital-investment-in-blockchain-up-nearly-300-percent-in-2018/

[3] https://cointelegraph.com/news/venture-capital-investment-in-blockchain-and-crypto-up-280-in-2018-report-shows

representing around a 40% CAGR.[4] In geographic terms, the United States holds the largest portion of VC-backed blockchain startups with 79% of the activity with China coming in second at 12%.[2]

BLOCKCHAIN

Blockchain is a distributed ledger system used to record and validate data. A fundamental principle of the technology, and why it was formed, was to bring a decentralized system to the way users interact with the digital world. A centralized entity could be a bank, clearing house, or other entity which separate parties put trust in to facilitate a transaction. Therefore, blockchain allows users to execute transactions themselves and create an unchangeable secure record of those transactions leaving centralized entities behind. The decentralized aspect of the platform is facilitated by the technology running across a network of users, or nodes, who validate transactions through consensus. Once validated, the transaction is recorded in the blockchain and is impossible to modify as a single party or small group, eliminating the need for intermediaries to authenticate and settle the transaction. The one way the blockchain could be modified is if over 50% of those validating a current or previous transaction modify it to an agreed upon difference (remember, they must come to majority consensus on the transaction). The Ethereum network has over 25,000 nodes, while Bitcoin has about 7,000 making modifications very difficult, but not impossible.[5]

There's a matrix of 4 types of blockchain structures: public vs. private, and permissioned vs. permission less each with their distinct advantages for its intended use. An example of a public non-permissioned blockchain is Bitcoin or Ethereum where anyone can use their cryptographic keys, be a network node, join the network, or become a miner to the service. A private permissioned blockchain on the other hand could be extremely useful for medical records. It would involve a limited number of participants who can read the information on the blockchain and a limited number of users who can transact within it, all verified by the company/owner of that blockchain. It will be important for an investor to understand what type of blockchain is being used for a given application as all 4 have distinct advantages and disadvantages.

One of the most interesting theoretical discussions surrounding blockchain is whether a blockchain must use a cryptocurrency. A cryptocurrency token is a specific amount of digital resource which a user controls and can reassign control of to someone else. A token can take many forms but there are four possible objectives or outcomes for its use. First is to compensate someone or something for the effort to validate a transaction. Next, it can be assigned to a specific asset therefore allowing easy tracking. Alternatively, it can be used as a form of equity shares within a company and lastly, the use most people are familiar with, a currency. A currency can be used as a payment method but currently offers enormous exchange-rate risk and is the least scalable application of the four.[6]

When an investor is evaluating a blockchain venture looking to implement a token or coin dynamic within its operation, it's important to understand the limits of the role of the coin. First, a coin can be a way of monetization for founders which is often understood as monetizing the hype surrounding the inception of a company. Many recent Initial Coin Offerings (ICOs) have used this strategy as they can essentially cash out at the time of inception with no liability surrounding the company or founders. Further, a coin can be used for equity within a company, but with that, it is fundamentally no longer a coin but rather a share of equity of the company with all the legal implications surrounding a security. Other enterprises have used coins as a reward method for miners who validate the transactions, a preventative method that stops double spending through the transaction validation process. Finally, it can be used as a payment method between participants or a membership fee.[7] Employing a cryptocurrency suggests a founder is striving to

[4] https://globenewswire.com/news-release/2018/07/17/1538102/0/en/Blockchain-Market-to-surpass-16bn-by-2024-Global- Market-Insights-Inc.html

[5] https://www.trustnodes.com/2017/05/31/ethereum-now-three-times-nodes-bitcoin

[6] https://medium.com/swlh/does-a-blockchain-need-a-token-66c894d566fb

[7] https://medium.com/@pavelkravchenko/does-a-blockchain-really-need-a-native-coin-f6a5ff2a13a3

create an economy, which needs control, like all fiat currencies. Many potential startups introduce a currency without devising rules that will make that coin successful. An investor will want to determine whether that new economy will be sustainable and if a project should have a coin in the first place. Overall, private blockchains do not need a coin, and if the system doesn't manage a scarce asset, it doesn't need blockchain at all.[8]

Other large enterprises have recognized blockchain's value and potential for disruption and have begun building the infrastructure for these solutions. IBM, Intel and others are collaborating on Hyperledger, which has the highest potential to succeed as a business-wide platform. Hyperledger is a blockchain which serves as the base for the development of other blockchain solutions with modular architecture.[9] Fabric is the arguably the most interesting Hyperledger module for enterprises today as it takes different components of blockchains like consensus, membership, etc. and allows an entity to build their own individual blockchain network within its framework. It is constructed different than public blockchains, like Bitcoin, as it allows participants to build a separate channel for their assets and isolate transactions within private ledgers.[9] Fabric employs fewer nodes and computes data in parallel which allows for better scalability and confidentiality - key for business.[9] As most blockchains focus on a token, these projects demonstrate a strong potential to build the backbone of non-monetary, highly scalable industrial applications of blockchain technology like carbon-quota issuing, similar to government mandated carbon credits, in China.[10]

SMART CONTRACTS

Smart contracts are a growing tool of blockchain technology that lets organizations, governments, legal bodies and individuals exchange monetary value, properties, shares, bonds or any other asset involving value. A smart contract is formed when two parties agree on terms of the exchange of value and the contract is digitized. Payment is made through cryptocurrency or other digital means, like wire transfers. In the simplest terms, a smart contract is a piece of computer code that has an executing qualifier for each party. Once each qualification of the code has been met, the automatic exchange of value or assets occur. For example, a business receives a receipt for an inventory shipment which is kept in digital form within the contract. The business pays a supplier for the shipment which is kept as a digital asset within the smart contract on the blockchain. Once the inventory has been delivered and validated both sides of the smart contract are met, and it self-executes, sending the digital asset to the supplier. Smart contracts are seeing more applications as the blockchain ecosystem develops and as of March 2018, there were over a million smart contracts operating on the Ethereum network.[11]

Blockchain-based smart contracts offer many benefits including increasing the speed of transactions, lower execution risk, fewer intermediaries, and lower costs. While still in early stages of development, these exhibit a variety of use-cases within the finance, supply chain, real estate and insurance industries - anything that has a vast number of transactions and high administrative costs. At least seven global banking institutions, including Bank of America, Standard Chartered and the Development Bank of Singapore, are currently building proof-of-concept systems with a trade finance and supply chain platform using smart contracts.[1] Barclays Corporate Bank has recently partnered with Wave, a platform that stores bill-of-lading documents in a blockchain and uses smart contracts to execute the exchange of ownership and automatic payments.[1] An investor interested in smart contracts should key in on startup ventures who are challenging an industry typically burdened with heavy administrative fees.

INDUSTRIES SET FOR DISRUPTIONf

[8] https://medium.com/@pavelkravchenko/investor-guide-does-this-cool-project-truly-need-blockchain-bdde70a26bfb

[9] https://blockgeeks.com/guides/hyperledger/

[10] https://www-03.ibm.com/press/us/en/pressrelease/51839.wss

[11] https://arxiv.org/pdf/1802.06038.pdf

Due to blockchain's potential applications, it has the ability for disruption across a multitude of industries. Facilitating safer and quicker transactions helps both business and customers creating opportunities across a wide spectrum of issues.

Financial Services deal closely with everyday banking procedures such as payment processing, investments, and buy/sell orders. A global FinTech report mentions that 77% of financial companies expect to adopt blockchain technology in the future for lower administrative costs and higher customer convenience.[12]

The **Insurance** industry could begin leveraging smart contracts to lock in to agreements with customers without the use of notaries, lawyers or other intermediaries. A disruptive company would pass the cost savings down to consumers, curbing the trend of rising insurance costs.

Data and **Data Privacy** has been a sensitive topic since internet companies have begun collecting it. However, empowering customers through their ability to own and control their own digital identity and data would revolutionize how advertisers and third-parties can access it. Allowing a smart contract blockchain application to guide when and for what price these entities could access personal data could be revolutionary for how data is obtained and used in the future. Although this idea is seen as unlikely, the power it brings to individual consumers cannot be understated.

Healthcare is one of the most important blockchain applications today. There is currently a growing demand for integrated healthcare services along with better technology-based data-management systems. The ability of blockchain to share data in real time with doctors as well as integrating wearable data would increase the ability for correct diagnoses, cut down on forgery, and assist in the difficulty of protecting sensitive data. This market is one of the most mature mentioned herein and has already been segmented into clinical data exchange and interoperability, supply-chain management, and claims and billing.

Additionally, nearly all industries would benefit from **Supply Chain** management and transparency. This refers to the logistics and payment networks that deal with the flow and information tracking of products around the world. Blockchain technology integrated into a supply chain would provide a chain-of-custody for critical products such as food and pharmaceuticals.[13] It would also reduce human error, avoid product delays and eliminate risk of fraud or scams.[11] In my opinion, this area of blockchain application holds the most promise in the short term. For example, there were 540 food product recalls in 2016, in the US alone, up 24% from the previous year.[14] Each recall costs on average of $10M in direct costs with 5% of those recalls costing more than $100M according to the Food Marketing Institute and Grocery Manufacturers Association.[13] The ability to pinpoint exactly where in the supply chain and what products were affected would greatly reduce the cost, time, and food waste of each recall.

POTENTIAL FOR ACCELERATION

The areas in which blockchain accelerates will have more to do with the tailored construction of business applications of blockchain as opposed to technological breakthroughs. As companies find more use-cases, the potential cost-savings should lend to quicker adoption and more widespread consumer acceptance. In addition, the fourth industrial revolution is based around artificial intelligence (AI) and that is the technology that will be able to unlock blockchain's full potential.[15]

AI will allow blockchains to operate more cheaply, safely and easily than they currently do today. All blockchain data is held in an encrypted state meaning that private keys are needed to unlock the

---

[12] https://applicature.com/blog/how-to-invest-in-blockchain

[13] https://supplychainbeyond.com/blockchain-smart-contracts-in-supply-chain/

[14] https://www.rentokil.com/blog/the-cost-of-product-recalls-to-food-businesses/#.W-hYMJNKiuU

[15] https://hackernoon.com/artificial-intelligence-blockchain-passive-income-forever-edad8c27844e

encrypted data.[16] Today, there is an emerging field to bring more security to the blockchain by building algorithms capable of working with data while still in an encrypted state.[15] Any process that involves exposing unencrypted data represents security risks and reducing these instances makes the whole system safer.

Validating and processing transactions on the blockchain is essentially one very large math problem that must be solved, taking a lot of processing power and energy. Currently through 'brute force', computers try every combination of characters to solve the problem until they find the one that fits, ultimately verifying the transaction while using huge amounts of energy. To allow blockchain the ability to scale more efficiently, employing AI-based computers to attempt to solve the math problem, and become better and more efficient at solving them, would save both time and energy meaning more transactions per second (tps) could occur. These holds the largest promise to highly scalable blockchains.

BARRIERS

The three main barriers to larger blockchain adoption are scalability, confidentiality and functionality. Scalability barriers exist since every node in a blockchain network must process every transaction. Because of this, blockchain has a very low transaction per second at around 10, where PayPal handles 115 tps and Visa processes about 2,000 tps.[13] However, as mentioned above, the AI and Hyperledger innovation spheres are currently working to increase tps to greater than 1,000. Although blockchain is built around anonymity, there are confidentiality concerns with both public and private blockchains. All data is encrypted on the blockchain, but with enough tries someone can see beyond the encryption, usually resulting in a hard fork. A hard fork is a permanent divergence from the previous version of the blockchain leaving all previous blocks/transactions behind.[17] It usually occurs to correct important security risks, add new functionality or reverse transactions as in the case with Bitcoin Cash, Ethereum Lite and Ethereum Classic due to hackers.[17] The transparency blockchain provides is a double-edged sword enabling visibility while, on occasion, compromising confidentiality. Last, blockchain does not yet offer powerful enough or sophisticated solutions for supply chain management, limiting its functionality. Immediate applications like vertically integrated solutions only exist as companies continue to build sophisticated, integrated, and optimized networks.

Smart contracts are new to many and still trying to be understood by all therefore there are many negative implications to consider. Developers are just now figuring out how to build these contracts, so they can be relied on not to lose stakeholder's assets because of vulnerabilities in underlying code. The technology is advancing at such a pace that government bodies cannot keep up with development coming from every corner of the internet. All of this points to the overarching barrier to smart contracts, which is the need to create standard processes. Standard processes will help more developers understand where coding shortfalls lie. Creating standardized frameworks to write or develop a smart contract will reduce the instances where these contracts could be hacked. Siloed, or independent, development of smart contracts without a standard by which to operate is creating areas where all users are unable to experience the full benefits of blockchain solutions. It is difficult to get all developers on the same page for the need for standardized processes, as most innovators within the space "still do not have a full picture of what a security hole [within a smart contract] looks like" says Ilya Sergey at the University of London.[18]

Continuing to build smart contracts in this way, without regard for standards, will inevitably move more of these contracts to be void or not recognized under regular law. For example, marrying complex regulations of maritime law with commercial codes governing the rights to ownership and possession along shipping routes would prove difficult to master on its own, but with no regulations, almost every

---

[16] https://www.forbes.com/sites/bernardmarr/2018/03/02/artificial-intelligence-and-blockchain-3-major-benefits-of-combining- these-two-mega-trends/#5093ead34b44

[17] https://www.investopedia.com/terms/h/hard-fork.asp

[18] https://www.technologyreview.com/s/610392/ethereums-smart-contracts-are-full-of-holes/

developer is bound to create them slightly differently, or get it wrong altogether.[19] Writing smart-contract code the same as other colleagues allows legal frameworks to be established and industry norms to be developed. Some blockchain enthusiasts ascertain that smart contracts sidestep the law; however, that is not the case. Therefore, if a smart contract executes a transaction as intended and the outcome is not accepted by a party, it can be resolved through legal means.

Payments within a blockchain have two possibilities, use a cryptocurrency coin associated with the blockchain or if none exists, connect to a separate financial institution. Using a cryptocurrency coin creates enormous amounts of exchange rate risks for any party to hold funds within the blockchain, not to mention a deficit in working capital from holding assets in what is essentially escrow. On the other hand, using a separate financial institution then defeats the purpose of a decentralized technology. Determining which method makes the most sense for each application will be crucial for implementation as well as the risk of developing an economy if indeed a token is needed.

OUTLOOK/IMPLICATIONS

Blockchain's capabilities are applicable to so many different facets of data management that its influence will continue to grow in 2019 and into the future. These facets cover finance, transactional data, legality, AI and others. Matt Turck, a venture capitalist at First Mark, mentions that the beginning of the 21st century was defined by social, mobile and cloud-based services. He goes on to say that "there's a rationale for making the argument that AI, blockchain and the Internet of Things is the new social, mobile and cloud."[14] As these three industries spawned many unicorns, a surplus of these new companies will begin succeeding in the next 10-15 years.

As blockchain becomes more prevalent, established laws and financial reporting requirements will need to be revised and amended for their specific use cases. Algebraix Data CEO Charlie Silver states that with all new technologies there are always standard process debates going on, but that these standardizations will directly correlate to blockchain and its adoption rate.[20] He predicts areas where current infrastructure is lacking is the perfect use case for initial blockchain adoption, like third world countries. Western civilizations have detailed record keeping of deeds, liens and other important documents whereas these other countries do not. Specifically, Silver points to the differences between the western world's real estate ownership infrastructure and the opportunity that exists in less developed countries to begin storing this information on a blockchain.

Smart contracts within the commercial realm have yet to be proven, but in the near-term, it is expected that permissioned blockchains privately maintained by small groups will see the largest adoption. Companies that are targeting processes that include complex and manual work flows, multi-party agreements, lack of trust between parties, and interdependent transactions will see early smart contract returns in the context of cost savings.[3] A signal that indicates this technology is positioned for wider adoption is recognition of smart contracts by legal authorities. An investor will want to watch for major trials or deployments that achieve milestones in scalability, or technology that successfully addresses privacy within smart contracts.[3]

New business models and capabilities will continually be coming to the forefront as more people understand how to integrate blockchain technologies into their business. One such example will be when business models leverage smart contracts to extend beyond the digital realm to things such as IoT devices.[3] This has already occurred where access to electric vehicle charging stations are driven by smart locks connected to a smart contract enabled on the blockchain. Additionally, companies like Encrypgen leverage smart contracts to transfer patient data securely without allowing access to third

---

[19] https://hbr.org/2017/03/global-supply-chains-are-about-to-get-better-thanks-to-blockchain

[20] https://analyticsweek.com/content/2018-trends-blockchain/

parties.[21] Lastly, Follow My Vote uses smart contracts to protect voters and their votes from fraud.[19] When each vote is cast, it cannot be changed due to blockchain consensus validation and when voting ends it sends a token (value) to a digital address that represents the winner of the vote.

As an investor, it's important to analyze whether a startup is offering a new answer to a real need. It must have a use-case with incentives to its customers, otherwise it will fall victim to the hype of new technology, like many ICO-driven failures before it. As with all startup investments, a blockchain company must have a go-to market strategy to succeed, otherwise it's stuck as an impressive technology with no adopters. Finally, it needs to attract customers, and that won't happen if someone else is providing the same service at an equal level, creating an unneeded substitute. Looking at only new areas of application should prove nearsighted for an investor. Silver postulates that when "thinking about enterprise, it's got 20, 30 years of systems that need to interoperate. Old systems don't just die; they find a new way to integrate into a new architecture."[18] In any new space, understanding a startup's claims to address a problem must be verified, but it is key in blockchain where both a company's claims and motives may not be true.

Full business networks will likely prove lucrative due to blockchain's ability to span both vertical and horizontal integrations. The best solutions will be able to function across different companies; therefore, finding holistic and inclusive solutions will likely see the best returns. When assessing this technology, it can be seen similar to other internet-based entities where a network effect is both real and an effective deterrent to competitors. Alan Dickman, a blockchain solutions architect at IBM, mentioned that once one company begins to take on blockchain technology and it proves successful for its customers, all other companies will quickly follow.[22] Therefore an early product or service with a subsequent successful customer acquisition strategy could bear greater anticipated returns than other industries.

At this point, the potential for blockchain likely exceeds it practical utility for information assets. Nonetheless, with its capabilities applicable to such a broad range of areas, its influence will continue to grow in the coming years. AI technology will dramatically increase the rate of growth/adoption with the key issues at stake being the resolution of standards, semantics, and governance needed to institutionalize this technology.

Ethan Harden, MBA
www.linkedin.com/in/ethanharden

---

[21] https://www.bitdegree.org/tutorials/what-is-a-smart-contract/#What_is_a_Smart_Contract_What_Youre_Going_to_Find_In_This_Guide

[22] Dickman, A. (2018, November 18). Personal Interview