TRAUB BLOCKCHAIN PRIMER
PT.1: AN INTRODUCTION TO BLOCKCHAIN'S KEY TERMS

Date: December 20th, 2017

By: Michael Boord of Marvin Traub Associates

It's December 20th, 2017 and the price of 1 Bitcoin (1 "BTC") is hovering around $17,000 per coin[1]. With a global supply of 16.7 million Bitcoins, the cryptocurrency's current market capitalization is ~$280 billion. This market capitalization for Bitcoin would be equivalent to the 13th largest company in the S&P 500 by market capitalization. While Bitcoin was only created 8 years ago, its current market valuation is greater than some of the world's most established companies including Visa, Procter & Gamble, Chevron, and AT&T.

Bitcoin's price has now appreciated by ~1,700% in 2017 and most market participants can only speculate as to where its price will settle. What can be said with certainty is that Bitcoin adoption is growing. Coinbase, the largest U.S.-based Bitcoin exchange, now has more users than brokerage firm Charles Schwab with 13.3 million[2]. Data from Coinbase, compiled by Alistair Milne of the Altana Digital Currency Fund[3], shows that in November alone, the exchange added 100,000+ users over a 24-hour period three separate times. Along with the meteoric rise of Bitcoin's price, mainstream media's coverage of Bitcoin has surged this year as well. While

[1] CoinMarketCap.com.
[2] Bitcoin exchange Coinbase has more users than stock brokerage Schwab. CNBC.com
[3] Bitcoin gets in on the post-Thanksgiving shopping spree, surges to new record above $9,000. CNBC.com

we at TRAUB have also been amazed by the unrivaled[4] price appreciation that Bitcoin has experienced; we are more fascinated by the technology upon which Bitcoin is built – blockchain technology.

Bitcoin's long-term potential, value and use cases are extremely hard to predict. The teams of Bitcoin bears and bulls[5], while being firmly divided, each are comprised of all-stars from the global financial markets. Among the bulls you have Christine Lagarde, James Gorman, Mike Novogratz, Lloyd Blankenfein and Peter Thiel. The bears include Warren Buffet, Jamie Dimon, Brian Moynihan, Ben Bernanke, Ray Dalio and Howard Marks. Although these industry titans are firmly split on Bitcoin's potential, they are much more aligned on the potential that blockchain technology has. TRAUB shares this view and believes blockchain will be a highly disruptive force in our industry, the global consumer and retail sector. We have compiled this two part report to explain some of the basic terminology (Pt. 1), in plain English, and highlight specific applications that this revolutionary technology can have on the broader retail sector (Pt.2). This first part of the report will serve as a basic primer on the technology for those in our industry who are unfamiliar with blockchain.

Let's set the table, **what is a ledger?**

A ledger is essentially a record of transactions. If you've ever balanced a checkbook, you've worked on a ledger. If you've ever entered transactions into a spreadsheet, you've prepared a ledger of sorts.

Ledgers are most commonly associated with accounting functions; they have historically been used primarily by accountants to record financial transactions. While ledgers originally had a physical medium, clay, stone, paper etc. they have since evolved into digital mediums and are now kept on computers, spreadsheets and cloud-based applications.

How is that related to blockchain?

While it sounds like a technology more suited for Wade Watts in the fiction novel Ready Player One, at its core, a blockchain is just a distributed digital ledger. The distributed element of blockchain is critical to understanding its revolutionary nature. The information kept on traditional digital ledgers is centralized somewhere, either locally on a computer or on a cloud-based system. Information on a blockchain however is not stored centrally; it is distributed across all participating computers (known as "nodes") of the blockchain. Since the information is distributed across all of these nodes, and can therefore be audited at any point in time by any network participant, the records are easily verifiable. Additionally, no centralized version of the information exists for a hacker to corrupt. Hosted by all nodes simultaneously, a blockchain's data is accessible to any participating node with an internet connection[6].

One of the core functions that blockchain optimizes is the establishment of trust between counterparties. The current model for completing transactions does this in a fragmented way: requiring that each party keep their own set of records, which they each independently verify prior to executing a transaction, and/or also through the use of a 3rd party intermediary. One of blockchain's technological innovations is its ability to establish trust without the need for local information storage or the use of an intermediary.

How does blockchain establish trust?

- Security: Blockchain is designed to store information in a way that makes it virtually impossible to add, remove or change its data without being detected by other users. Once new information is recorded

[4] Bitcoin's 'bubble' is unlike anything we've seen recently. Business Insider
[5] Bitcoin Bulls and Bears: Who's hot, who's not on Crypto. Bloomberg.com
[6] Blockgeeks: What is Blockchain Technology? Blockgeeks.com

onto a blockchain, it is nearly impossible to change. This is why information on a blockchain is said to be immutable (unchangeable).

  - In simplest terms, transaction blocks are strung together in a way that new blocks have traces of the previous blocks encrypted in them, forming a chronological "chain" of blocks of information (transactions). If any one block in the chain is altered, the links in the chain are broken and the fraudulent transaction(s) can be easily identified by network participants. Additionally, changing the information on a blockchain requires the approval of a consensus of the blockchain's users, making it extremely hard to add fraudulent or invalid information.

- Decentralization: Today, counterparties often rely on a central authority such as a government, bank or a credit card clearinghouse to establish trust. Blockchain applications instead replace these centralized systems with decentralized ones, where verification comes from the consensus of multiple users. As it pertains to the Bitcoin Blockchain, the process of adding new blocks is as follows:
  - New bitcoin transaction are broadcast to the blockchains network of nodes. Some of these nodes, known as miners, actually process these pending transactions on behalf of the bitcoin blockchain network. Providing this mining service is quite costly[7] and therefore these miners are compensated with transaction fees[8]. When a miner has prepared a new block and submits it to be recorded on the Bitcoin blockchain, approval by at least 51% of nodes is required before the new block can be added to the chain.
    - This effectively means that a hacker attacking Bitcoin would have to control a majority of the blockchain's nodes in order to conduct such an attack. Given the scale of the current Bitcoin network, an attack of this kind is considered almost impossible as it would cost billions of dollars to execute.
  - The distributed nature of blockchain's transaction processing and verification process therefore creates additional security by requiring multiple network participants to execute new transactions.

These 2 key features of blockchain – security and decentralization – establish trust between counterparties and reduces the need for intermediaries. Reducing the number of intermediaries across supply chains reduces costs. Examples of these intermediaries include banks, layers, regulatory compliance officers, notaries, etc…[9]. Blockchain therefore can significantly reduce operating expenses for companies and industries by streamlining supply chains. A report by Accenture estimates that Blockchain technology could help the world's largest investment banks cut their infrastructure costs by $8-$12 billion a year by 2025.[10] While the first applications of blockchain have been implemented in the financial sector, blockchain has applications across nearly every industry.

How is blockchain related to Bitcoin?

Bitcoin first appeared in a 2008 white paper authored by a person, or persons using the pseudonym Satoshi Nakamoto[11]. The white paper detailed a peer-to-peer digital cash technology called Bitcoin that allowed for online payments to be transferred directly, without an intermediary[12].

Bitcoin is a cryptocurrency that is based on blockchain technology. All bitcoin transactions are verified and recorded on the bitcoin blockchain protocol. Being the first and largest blockchain application by market value and active users; Bitcoin has become synonymous with blockchain. However, Bitcoin is just one application of

---

[7] Is Bitcoin Mining Profitable in 2018? 99bitcoins.com
[8] Bitcoin miners are making a killing in transaction fees. Businessinsider.com
[9] What is a Distributed Ledger? Coindesk.com
[10] Blockchain could save investment banks up to $12 billion a year: Accenture. Accenture.com
[11] Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org
[12] How does the Blockchain Work? (Part 1), Collin Thomson for Medium.com

blockchain technology. There are actually now over 1,000 cryptocurrencies[13], all of which are based on blockchain.

A helpful analog for bitcoin's relationship to blockchain is Email's relationship to the internet. "The "killer app" for the early internet was email; it's what drove adoption and strengthened the network. Bitcoin is the killer app for blockchain right now. Bitcoin drives adoption of its underlying blockchain, and its strong technical community and robust code review process make it the most secure and reliable of the various blockchains (Harvard Business Review, 2017)"[14].

See the figure in the Appendix for a graphical representation of how a Bitcoin transaction works.

What is Ethereum and how is it different from Bitcoin?

Ethereum is the second largest cryptocurrency by market capitalization. Ethereum currently has a market capitalization of approximately $80 billion (~29% the size of Bitcoin's market capitalization). While the two cryptocurrencies are based on blockchain technology, they are quite different in terms of their purpose and capabilities. As defined earlier, Bitcoin's singular application is that of a peer to peer electronic payment system. Ethereum however allows for developers to build and deploy any number of decentralized applications using its blockchain technology. In that sense, Ethereum is much closer to a blockchain platform than a blockchain with a singular application like Bitcoin is. One of the decentralized applications that can be built using Ethereum's blockchain software platform are smart contracts.

What is a Smart Contract?

A smart contract is a set of computer code that can be written to automatically execute once certain conditions have been met. Because smart contracts run on the blockchain, they run exactly as programmed. This is both their greatest strength and weakness. Smart contracts are inherently inflexible, they are automatically programmed to perform an action once certain conditions have been met. This prevents them therefore from containing clauses which include ambiguous language. Ambiguous language is a necessary element when perfect knowledge of future events isn't possible. Unless smart contracts can evolve to include flexible language, they will be employed in specific environments where absolute rigidity isn't a problem.

Conclusion

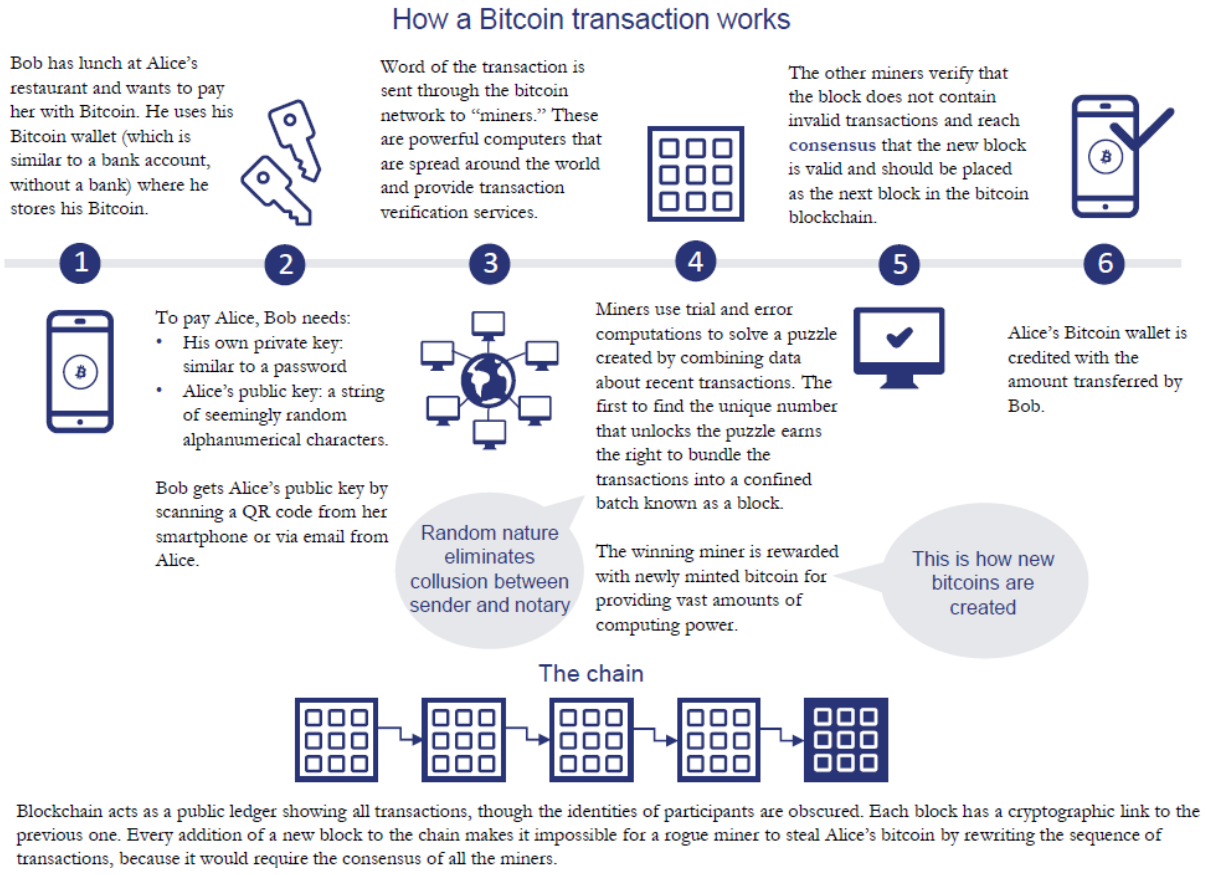
Bitcoin's incredible price appreciation has captured most of the consumer mindshare and media coverage this year. We believe however that blockchain's many other applications will ultimately have a more pronounced impact across industries. The summaries above are an intentionally overly-simplistic explanation of some of blockchain technology's key terms. This first part of our two part report, is intended to set the table by simplifying a technology that can seem daunting to many at first glance. The technology behind Blockchain is pretty complex; we believe this is part of the reason that many players within the retail industry haven't fully grasped how it will impact key pieces of the retail operating models that are in use today. We will focus on several ways blockchain can be applied within the retail industry in the forthcoming second part of our report.

---

[13] Cryptocurrency Market Capitalizations. CoinMarketCap.com
[14] The Blockchain Will Do to the Financial System What the Internet Did to Media. Hbr.org

Appendix: Graphical Representation of a Bitcoin transaction[15]

Bitcoin: a worldwide distributed network



Blockchain acts as a public ledger showing all transactions, though the identities of participants are obscured. Each block has a cryptographic link to the previous one. Every addition of a new block to the chain makes it impossible for a rogue miner to steal Alice's bitcoin by rewriting the sequence of transactions, because it would require the consensus of all the miners.

[15] Bloomberg, American Banker, The Economist and Lydians Capital