Abhishek Chakravarty Follow
Product Guy, Builder and Story Teller. I’m on Twitter @chakrvyuh.
Dec 23, 2016 · 12 min read

The Product Manager’s guide to the Blockchain — Part 1

My experiments with Blockchain, Ethereum & Smart Contracts

If you are reading this post, you perhaps already know what a blockchain is. If not, here is an interesting video by the World Economic Forum on what the blockchain is today and could be in the very very near future.

What is blockchain?

Over this past year I took a keen interest in understanding cryptocurrencies such as bitcoins and quickly realized that while digital currencies were powerful, the technology that powers them—blockchains, could change the face of how business is done. This post is the first in a 3-part series (read part 2 here)where I will present an overview of cryptocurrencies & blockchains, how blockchains are born and the broad concepts that make them possible. I will also share my notes on the business use cases for blockchains and implications for our "Internet of Things" future.

In subsequent posts I will share my experiments with the ethereum blockchain (an implementation of blockchain that enables micro-transactions), create a private blockchain network, implement a smart contract—and finally build a distributed app powered by blockchain & IoT.

Since the tech is still evolving, blockchain documentation on the web can be really confusing. This post also aims to minimize the noise and serve as a "Getting Started" guide for folks that want to play around with blockchains and start building on it. This is not meant to be a

programming guide for engineers—there are tons of those on the internet, instead this is the Product Manager's guide to the blockchain tech—so the posts will go broad & deep, but not "too" deep. Ok Enough said, here we go.

. . .

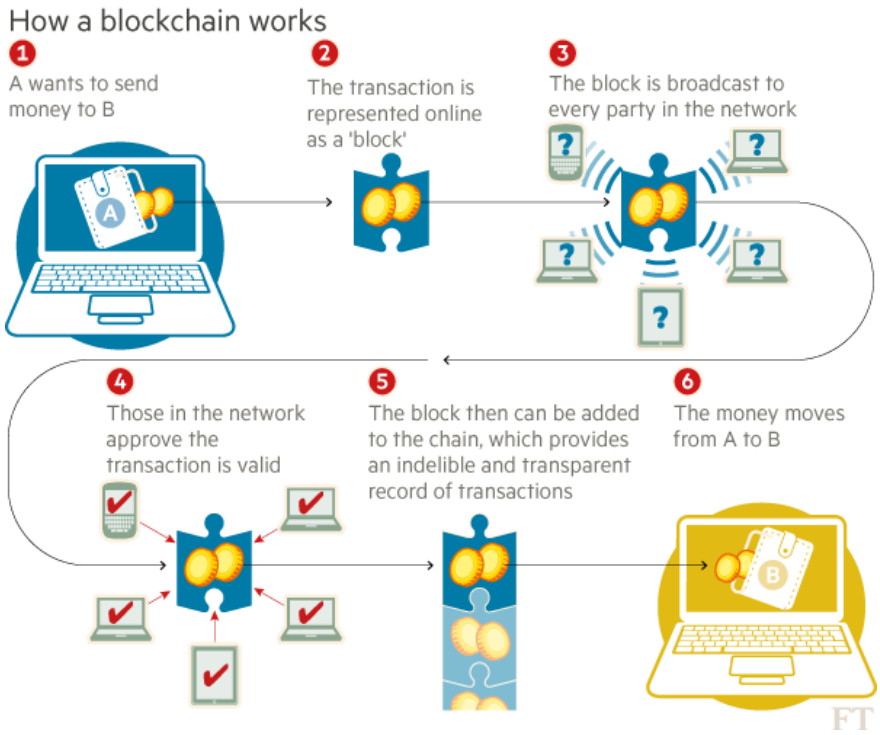
WHAT IS THE BLOCKCHAIN?

Every discussion of blockchain starts with cryptocurrencies, because the best way to understand blockchains is to understand how cryptocurrencies such as bitcoin work. If you noticed, the video starts with an overview of the current state of financial transactions—parties A and B have to *trust* a third party (a bank) to ensure transactions are valid, non-fraudulent and successful. The video then predicts the future powered by blockchains, a world where we will have to trust no-one for valid, non-fraudulent and successful financial transactions. Digital currencies backed by cryptography (a.k.a cryptocurrencies) make such trust-less systems possible.

How Bitcoin transactions work

Let's say Alice wants to transfer 1 bitcoin to Bob. (Pay special attention to the parts in ***bold.*** We will define these terms later)

Here's what a bitcoin transaction happy path looks like.



1. *Alice initiates a bitcoin transfer to Bob via a peer-to-peer network—called the bitcoin network. They must provide* ***cryptographic proof of identity*** *to the network that they are indeed who they say they are.*

2. *The transaction details are recorded in a "****block****" and the block is announced to the peer-to-peer network for transaction verification & validation.*

3. *The nodes on the network move to validate the transaction block—which basically involves solving a computationally intensive random math problem. The incentive for nodes to validate transactions are new bitcoins and associated transaction fees as reward for 'finding' the new block . The process of validating transactions in a block is called* ***bitcoin mining.***

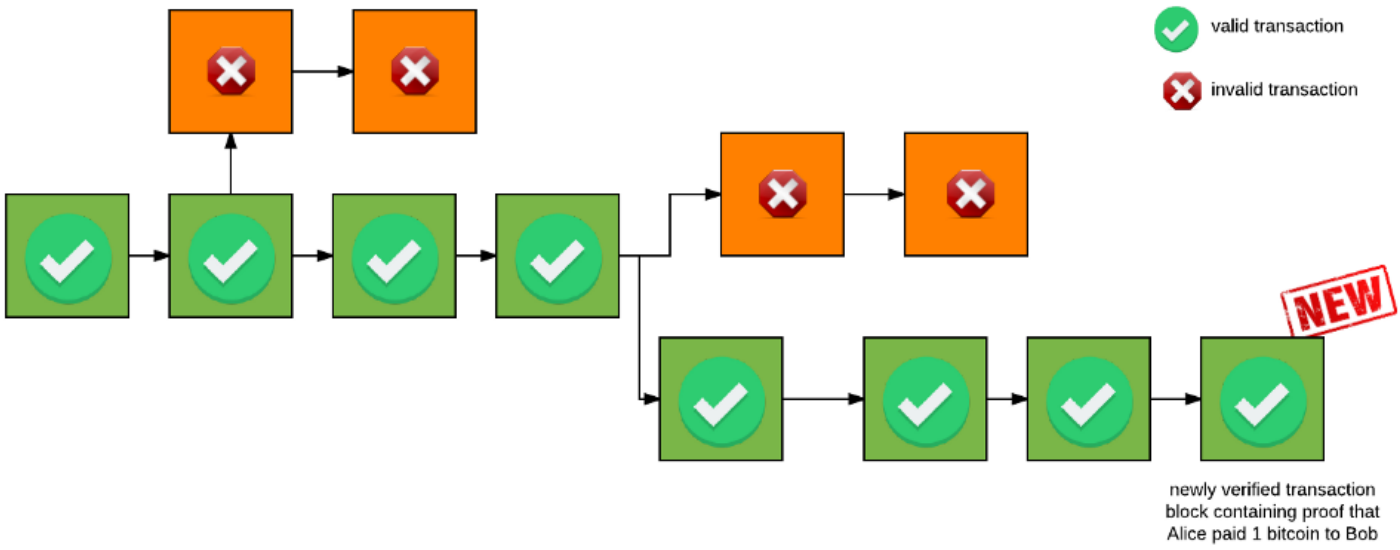
4. *Each peer/node in the network keeps a copy of all such blocks of transactions that were previously verified—sort of a chain of blocks , a running ledger. This chain is called the* ***BLOCKCHAIN****.*

5. *Once a node successfully solves the math problem, the transfer is verified and the newly verified transaction block is added to this chain by the winning node.The winning node then broadcasts to the network that a block has been found.*

6. *Next, all other nodes in the network check the winning node's claims and arrive at a* ***distributed consensus*** *that the transaction has indeed been validated , and the transfer is successful. Once consensus is achieved, each node updates their respective copy of the blockchain ledger. (More about this in a minute)*

7. *The manner in which this chain is built as transactions flow in , bestows interesting and important properties to the blockchain. It becomes an immutable, indelible and transparent record of reality to everyone on the bitcoin network . Any attempt to submit bogus transaction blocks, such as double spend bitcoins, is recorded in the blockchain and is broadcast to everyone.*

8. *When all of the above steps are complete, Alice's account balance is reduced by 1 bitcoin . Bob's balance increases by 1 bitcoin.*



Lets dive a little deeper into the key concepts that helps create this distributed ledger chain.

1. Cryptographic Proof of identity

Cryptographic proof of identity in simply means *proving* one's identity without *revealing* it. Here's a scenario that will help explain this concept.

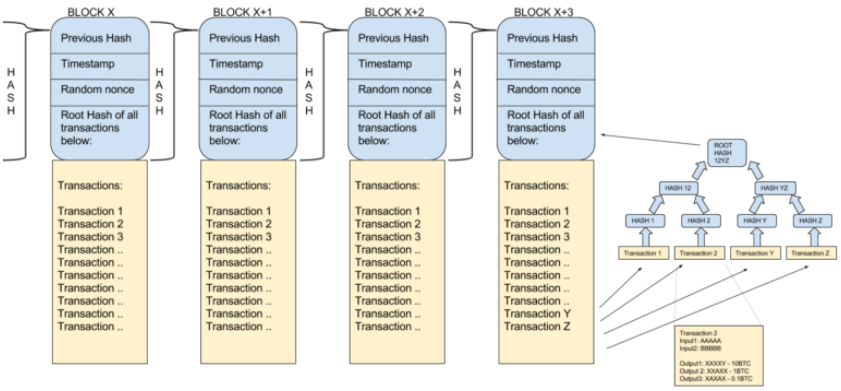
Say you publish a book under the pseudonym John. The book becomes wildly popular and now this new guy Mike—the impostor, comes along and claims to be John, to reap all the success. How do you prove that you are the real author of the book and not Mike, *without revealing who you are*?

Here's what you can do. You generate something called a public key-private key pair and include the public key in the book. Anyone can now use that public key to encrypt a chapter in the book. You then encrypt a chapter in your book and challenge Mike to decrypt it and read it. Because ONLY you have the corresponding private key to the public key used for encryption, Mike will fail to decrypt the chapter. This way, you just proved that you are the author of the book without ever revealing your personal identity.

At a high level this is how nodes/peers in the bitcoin network prove their transactional identity to other nodes in the network. Nodes don't have long term identity, meaning each node can generate as many public key - private key pairs as they want—all they need to ensure is that they use the right keys to sign transactions. No real identities are ever revealed, which is in line with the network's anonymity principles.

What is a block ?

The blockchain is just that—a chain of multiple blocks. Each block that is added to the blockchain has transaction data that is permanently recorded.



http://esotera.eu/clients-explorers/

Each block contains, among other things,

1. *a record of some or all recent transactions and their timestamps*
2. *a reference to the block that came immediately before it, ensuring any tampering with a block is propagated throughout the entire blockchain.*
3. *a "nonce"-the answer to that difficult-to-solve math problem we talked about earlier, and that can only be solved randomly via trial and error —the answer to this math problem is unique to each block.*

Obviously, new blocks cannot be submitted to the network without the correct answer. As mentioned earlier, the process of "mining" is essentially the process of competing to be the next to find the answer that "solves" the most recent unverified block. Currently a new block of unverified transactions is generated every 10 minutes or so.

Mining & Distributed Consensus

At a high level, each participating node or "miner" on a bitcoin network is running special software and hardware to solve for the nonce to verify that a block of transactions is valid. This takes a lot of computing resources, and so whoever cracks the problem is rewarded with new bitcoins from the network as well as any transaction fees that Alice included with the 1 bitcoin transfer. The successful miner announces the new blockchain (=old blockchain + the new block) to the rest of the network , the network checks the validity of this claim, arrives at a consensus and accepts the proposed blockchain as the new source of truth. The distributed consensus is largely a behavioral outcome based on game theory principles, such that it is in the best interest of the rest of the bitcoin network to validate a correct blockchain proposed by a winning node if the node shows that they indeed invested substantial resources to solve the math problem and got it correct. Such smart incentives are at the heart of bitcoin's distributed consensus which is the bedrock of what makes the blockchain so promising.

All transactions on the blockchain are traceable, back to the very first 'genesis' block. The transactions are tamper proof—any attempt to tamper with them is immediately broadcast to the entire network and detected. That also means that once transactions are committed to the blockchain, there is no going back to edit or delete it.

Thats pretty much all you need to know to get started with Blockchains. But if you are really nerding out right now and want to dig deeper, here

is Satoshi's paper on bitcoin mechanics and how all of this works in greater detail.

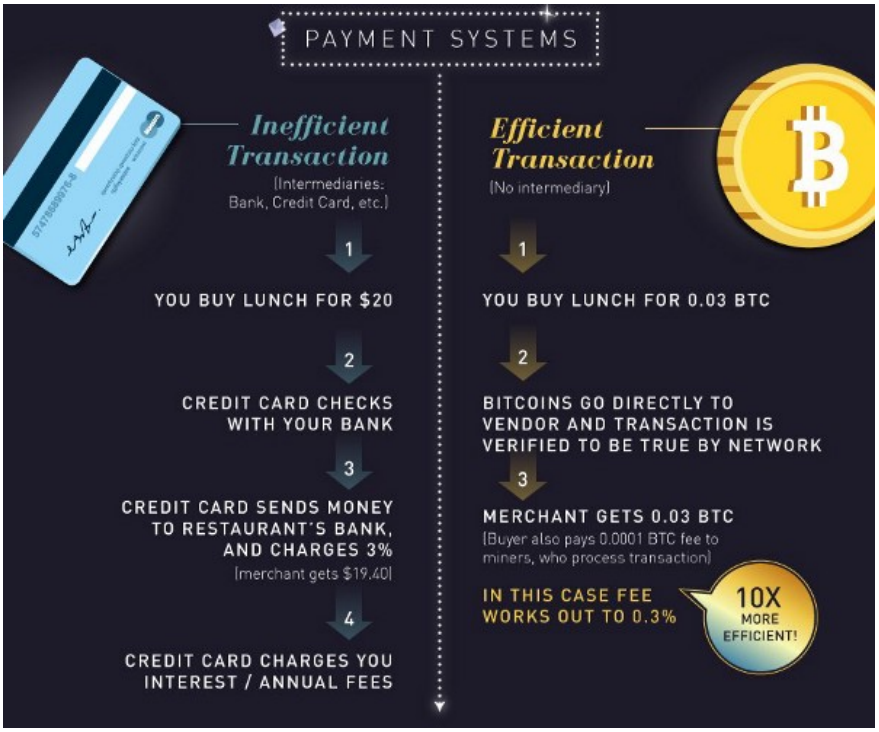
Again, this post is about blockchains and not cryptocurrencies but I talk about the latter to make two specific points —first, that cryptocurrencies such as bitcoin are just value exchange applications built on top of blockchain technology—and that cryptocurrencies were instrumental in demonstrating the power of blockchains and the many applications that blockchains will one day support and power.

. . .

What's Possible with Blockchains?

As Product Managers, what we really need to know is what's possible with Blockchains, and how is it going to shape the future of various products industries and markets.

From a Business perspective, Blockchains can be used as an *exchange network* to move value, assets , transactions amongst peers on the network without the need for any 3rd party intermediary to validate or maintain these movements. At first this might seem trivial, but let me tell you that moving assets, value and transactions without 3rd party intermediaries is huge. One of the direct benefits is drastically reduced transaction costs.



http://tabletsandtech.com/116/bitcoin-vs-visa-transaction-fees/

Add to that the upsides of a fully secure, distributed, never-down network. After ignoring it for a while, the banking industry has now started to take note of how disruptive blockchain powered exchange networks can be to their core business. Most big banks have some sort of blockchain experiment going on as they see blockchain tech as a key part of their competitive advantage going forward.

Internet of Things (IoT) & Blockchain

Another big implication of this technology (and one that I am personally excited about) is that it could really give the much needed boost to the "Internet of Things" future. The future where machines are connected to each other and are communicating seamlessly to get jobs done, with minimum or no human intervention. But how can blockchain help us realize this future ?

dilbert explains it well

The prerequisites for true IoT functionality is not only that machines be connected to the internet as well as to other devices, but also communicate with each other *securely* and on an *as needed basis* (due to hardware / battery life constraints). These machines should also be autonomous and smart, in making decisions based on a set of rules that cannot be tampered with. Current manifestations of IoT architectures suffer from poor cybersecurity implementation in applications, networks, data and equipment have made IoT projects very challenging. Blockchains can change all that as they enable connected devices to be smart independent agents, that can not only identify themselves to other machines securely, but also carry out micro-transactions based on a set of rules or smart contracts that cannot be tampered with.

Here is a classic example that can be realized with IoT + blockchains: Imagine a vending machine that can monitor and report its own stock, and accept bids from distributors AND make payments automatically via micro transactions for delivery of new items. Other scenarios such as smart home appliances that can bid with one another for priority so your the laundry machine, dishwasher, thermostat and Roomba all run at an appropriate time while minimizing the cost of electricity against current grid prices.

Several blockchain startups such as Ethereum have realized this opportunity and are already extending blockchain functionality beyond cryptocurrency. Ethereum's blockchain has its own cryptocurrency called "ether", but it also provides the capability to write secure and tamper proof *smart contracts* into the blockchain enabling micro-transactions when specific conditions are met. This has the potential to unlock entirely new business and economic models for various industries in the future. I will explore the Ethereum Blockchain in Part -2 of this series.

Paying for Coffee with Cryptocurrency?

At the time of writing this post, there are over 700 cryptocurrencies being traded on various online exchanges globally, Bitcoin being the most popular amongst these. But, most people don't use cryptocurrencies to move value around. That is because the infrastructure necessary for such *trustless* transactions don't scale well in their current form. Bitcoin transaction processing is restricted (for reasons outside of the scope of this post) to 7 transactions per second (tps), compare this with Visa processing speeds which has a peak capacity of around 56,000 transactions per second. Bitcoin loses by a lot.

From a cryptocurrency user standpoint here is the UX you can expect today. Say you wanted to pay for your Starbucks using bitcoins. Once you made the payment you will have to wait until your transaction is validated by bitcoin's blockchain network @ ~7 tps. Your wait times are positively correlated with how many others are paying with bitcoins at that very moment as well as the number of active public nodes validating the transactions, but you could be waiting anywhere from 20 minutes to 2 hours. Your coffee will go cold before your payment is confirmed.

At this time, this is clearly a big limitation for blockchain transaction processing, but a lot of smart people are working to fix these issues, from increasing the transaction block size, to incentivizing nodes to validate blocks quickly. In short, when it comes to cryptocurrency transactions, its fair to say that the future is here—but it doesn't scale very well at this time.

Public & Private Blockchains

Bitcoin is a cryptocurrency **powered by its Public Blockchain**, which ensures anonymity in identity but transparency in transactions. However, maintaining both anonymity and transactional transparency comes at a cost—it lowers the bandwidth between nodes and the entire blockchain must be duplicated by all nodes locally to be aware of the current state of the chain. Its replicates into the slow transaction processing that you faced paying for that coffee with bitcoins.

On the other hand an organization or a **group of organizations can create Private blockchains** if they don't need or want anonymity of nodes. Private blockchains can be secured by the familiar model of user rights and secrets that we've are so comfortable with while still maintaining many kinds of partial guarantees of authenticity and

decentralization that blockchains provide. This can work great if the org doesn't plan on sharing transactions or blockchain writes outside of a closed group, but there is always the chance of that hacker lurking in the wild looking for the weakest link in the chain. One can certainly create private blockchains for testing and experiment purposes as well, we will create one in one of my subsequent posts.

Examples of private blockchains may be "Consortium blockchains" setup by an industry consortium or group where the consensus process of a transaction is controlled by a pre-selected set of nodes. E.g. , one might imagine a consortium of 15 companies in an industry, each of which operates a node in the consortium blockchain and of which 12 must sign every block in order for the transactions in that block to be valid. The consortium or company running a private blockchain can easily, if desired, change the rules of a blockchain, revert transactions etc. Transactions are cheaper and faster as well, since they only need to be verified by a few nodes that can be trusted to have very high processing power, and do not need to be verified by the entire network. So in sum, while private blockchains may not be the right way to create a global cryptocurrency that is anonymous & trust less, they can be used for a lot of other practical applications, including industry specific IoT applications.

Vitalik Buterin, ethereum's founder puts it in perspective.

> *The solution that is optimal for a particular industry depends very heavily on what your exact industry is. In some cases, public is clearly better; in others, some degree of private control is simply necessary. As is often the case in the real world, it depends.*

. . .

This has been a long first post, but understanding this technology is key to demystifying the use cases of blockchains and think about product possibilities. In the next post I will discuss my experiments with the ethereum blockchain, and how I created a simple private blockchain with two nodes to test things out. Follow me if you'd like to be notified when the post is up!

If you found the post helpful, please recommend it to others by clicking the green heart below! If you have insights or comments, I would love to hear from you . You can also reach out to me directly on twitter.