The Blockchain is the New Database, Get Ready to Rewrite Everything

27 Dec 2014 By : William Mougayar 22 Comments Tag: bitcoin, blockchain, software development

via shutterstock

If you understand the core innovations around the blockchain idea, you'll realize that the technology concept behind it is similar to that of a database, except that the way you interact with that database is very different.

The blockchain concept represents a paradigm shift in how software engineers will write software applications in the future, and it is one of the key concepts behind the Bitcoin revolution that needs to be well understood. In this post, I'd like to explain 5 of these concepts, and how they interrelate to one another in the context of this new computing paradigm that is unravelling in front of us. They are: **the blockchain, decentralized consensus, trusted computing, smart contracts and proof of work / stake**. This computing paradigm is important, because it is a catalyst for the creation of decentralized applications, a next-step evolution from distributed computing architectural constructs.

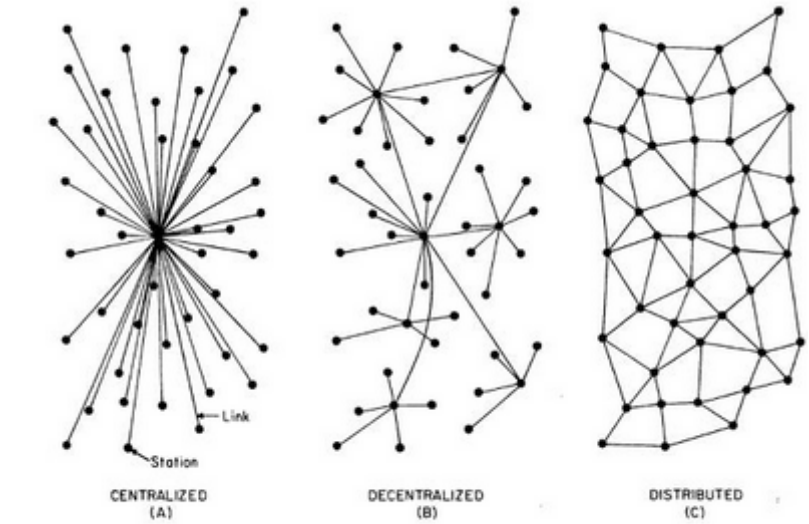

Figure 1 Centralized, Decentralized and Distributed Systems (Paul Baran, 1964)

These concepts are computer engineering related. They are technical in nature, but they will have business implications, because they are capturing the imagination of developers and business visionaries who are rushing to create a new generation of applications.

But this is not just a computing phenomena. Decentralized applications are going to enable a decentralization trend at the societal, legal, governance and business levels. As I wrote earlier, There is a Race to Decentralize Everything and Give Power to the Edge of the Networks, so, let's get ready to understand these concepts.

Decentralized Consensus (on or off Bitcoin's Blockchain)

To fully understand the blockchain concept and the benefits of cryptography in computer science, we need to first understand the concept of "decentralized consensus", a key tenet of the crypto-based computing revolution.

Decentralized consensus breaks the old paradigm of centralized consensus, i.e. when one central database used to rule transaction validity. A decentralized scheme (which the Bitcoin protocol is based on, transfers authority and trust to a decentralized virtual network, and enables its nodes to continuously and sequentially record transactions on a public "block", creating a unique "chain", the blockchain. Each successive block contains a "hash" (a unique fingerprint) of the previous code, therefore cryptography (via hash codes) is used to secure the authentication of the transaction source and removes the need for a central intermediary. The combination of cryptography and blockchain technology together ensures there is never a duplicate recording of the same transaction.

What's important here is that with this degree of unbundling, the consensus logic is separate from the application itself, therefore applications can be written to be organically decentralized, and that is the spark for a variety of system-changing innovations in the software architecture of applications, whether they are money or non-money related.

You could think of Consensus as the first layer of a decentralized architecture. It is the basis for the underlying protocol that governs a blockchain's operation.

The Blockchain (and Blockchain Services)

A blockchain is like a place where you store any data semi-publicly in a linear container space (the block). Anyone can verify that you've placed that information, because the container has your signature on it, but only you (or a program) can unlock what's inside the container, because only you hold the private keys to that data, securely.

So the blockchain behaves almost like a database, except that part of the information stored, its “header” is public.

The data stored can be a token of value, or a crypto money balance. So, the blockchain acts as an alternative value transfer system that no central authority or potentially malicious third party can tamper with (because of the encryption process). It’s based on the public/private hegemony, which is the yin-yang of the blockchain: public visibility, but private inspection. It’s a bit like your home address. You can publish your home address publicly, but that doesn’t give any information about what your home looks like on the inside. You’ll need your private key to enter your private home, and since you have claimed that address as yours, no one else can claim a similar address as theirs.

The blockchain can also be seen as a software design approach that binds a number of peer computers together that commonly obey the same “consensus” process for releasing or recording what information they hold, and where all related interactions are verified by cryptography.

Smart Contracts (and Smart Property)

Smart contracts are the building blocks for decentralized applications. A smart contract is equivalent to a little program that you can entrust with a unit of value (as a token or money), and rules around that value. The basic idea behind smart contracts is that a transaction’s contractual governance between two or more parties can be verified programmatically via the blockchain, instead of via a central arbitrator, rule maker or gatekeeper. Why depend on a central authority when 2 (or more) parties can agree between themselves, and when they can bake the terms and implications of their agreement programmatically and conditionally, with automatic money releases when fulfilling services in a sequential manner, or incur penalties if not fulfilled?

Here’s a simple example of a smart contract to “sell 100 beanie babies” using a form of natural contract programming language, based on Ethereum.

```
# Initialization
init:
    # *** An Ethereum smart contract to sell 100 beanie babies for "5000 by January"
    # First, store buyer's ethereum address:
    contract.storage["BUYER"] =
    # Then, store seller's ethereum address:
    contract.storage["SELLER"] =
    # December 31, 2014 is 1419984000 in "computer time"
    contract.storage["DEADLINE"] = 1419984000
# Code
code:
    # If the agreed amount is received on time...
    if (contract.balance >= 5000*10^18 and block.timestamp <= contract.storage["DEADLINE"]):
        # ... then designate the buyer as the new owner and pay the seller
        contract.storage["OWNER"] = contract.storage["BUYER"]
        send(contract.storage["SELLER"], contract.balance, (tx.gas - 100))
```

The starting point that you assume when applying smart contracts is that third party intermediaries are not needed in order to conduct transactions between two (or several) parties. Instead, the parties define and agree on simple (or complex) rules, and they embed them inside the transactions, enabling an end-to-end resolution to be self-managed between computers that represent the interests of the users. Smart properties are digital assets (or things) that know who their owners are. Their ownership is typically linked to the blockchain.

Trusted Computing (or Trustless Transactions)

When you put the concepts behind the blockchain, decentralized consensus and smart contracts together, you start to realize that they are enabling the spread of resources and transactions laterally in a flat, peer to peer

manner, and in doing that they are enabling computers to trust one another at a deep level.

Whereas institutions and central organizations were necessary as trusted authorities, a certain number of their central functions can be codified via smart contracts that are rather governed by decentralized consensus on a blockchain.

Namely, due to the blockchain's role as the unequivocal validator of transactions, each peer can proceed and trust one another, because the rules of trust, compliance, authority, governance, contracts, law, and agreements live on top of the technology.

If you fast forward to a not-too-distant future, smart contracts and smart property will be created, dispensed or executed routinely between consenting parties, without either of them even knowing that blockchain technology was the trusted intermediary.

Arguably, "trusted computing" on the Web is a key tenet of the new crypto-driven paradigm.

Proof of Work (and Proof of Stake)

At the heart of a blockchain's operations is the key concept of "proof-of-work", an integral part of Satoshi Nakamoto's original vision for the blockchain's role as the unequivocal authenticator of transactions. The "proof of work" is a "right" to participate in the blockchain system. It is manifested as a "big enough hurdle" that prevents users from changing records on the blockchain without re-doing the proof of work.

So, proof of work is a key building block because it cannot be "undone", and it is secured via the strengths of cryptographic hashes that ensure it authenticity.

But proof of work is expensive to maintain (estimated cost of $600M per year for Bitcoin), and may run into future scalability and security issues, because it depends solely on the miners' incentives which will be declining over time. An upgraded solution is "proof-of-stake" which is cheaper to enforce, but more expensive/difficult to compromise. Proof of stake not only determines who gets to update the consensus, but it also prevents unwanted forking of the underlying blockchain.

Edging Towards a Decentralized World

There will be a rush to develop new decentralized apps as a way to enable the decentralized world that we are edging towards.

To that end, business leaders and visionaries will need to learn a new vocabulary around crypto-related frameworks. Developers need to learn how to write decentralized apps that are enabled by blockchain technology. And end-users need to learn how to create or use smart contracts, e.g. as depicted via the Mist browser vision (Ethereum), which is a mix of marketplace discovery, management dashboard, and creation platform, all-in-one.

I recently outlined a comprehensive list of Bitcoin White Papers, and there were lots of protocols and proposals, but a protocol alone doesn't make a robust development environment. We will need to see comprehensive development environments that support a full stack of capabilities and value-add components on top of the blockchain services and consensus engines.

The original Bitcoin blockchain technology had limitations as we started to push its limits outside of money related services and into the software applications realm, so we shouldn't be surprised that the way forward is a

world of multiple blockchains. Some of them will be working together, some competing with one another, and others just being benevolent to each other.

Despite all the excitement and high expectations surrounding blockchain technology, there will be important issues that need to be addressed pertaining to deployment, scalability, security, and robustness, and many of these challenges are being worked on today.

Decentralized Apps will come in different flavors, sizes and complexity levels, so we must be prepared for that variety, and we must see beyond the Bitcoin promise to be the Internet of money, and into the Blockchain's promise to become a new development environment, just as Web development was the new paradigm back in 1996.

Update: Also read Part II and Part III
Blockchain Apps: Moving from the Jungle to the Zoo
It's Too Early to Judge Network Effects in Bitcoin and the Blockchain.

« *Previous Story*
The Ultimate List of Bitcoin and Blockchain White Papers

Next Story
Blockchain Apps: Moving from the Jungle to the Zoo »

Actually, check my 2nd post on blockchain apps, specifically- http://startupmanagement.org/2...

1 · Reply · Share ›

fredwilson · 2 years ago

i'm not sure we are going to see multiple blockchains because of the massive amount of liquidity and mining that is already happening on the bitcoin blockchain. i prefer the model Joel outlines here http://joel.mn/post/1035462152..., in which overlay networks are built on the bitcoin blockchain to provide the functionality that alternative blockchains are trying to provide

5 · Reply · Share ›

Vitalik Buterin ➚ fredwilson · 2 years ago

So, a few problems with that:

1. The Bitcoin blockchain simply is not designed to be scalable enough to support every transaction for every possible use case. The fundamental limitation that every node must process every transaction will ensure that (i) transaction costs stay in the $0.01-$0.05 range, which is fine for now for financial applications but people are not willing to accept anything even 10% as high for non-financial apps, and this will get even worse once scalable blockchain architectures start to come online in ~1-2 years that have 10-100x lower fees, and (ii) you just can't have more than a few hundred transactions per second without centralizing the blockchain to the point where there are fewer "full nodes" than in SWIFT.

2. Protocols "built on top" of Bitcoin are not light-client friendly. Now, you could argue side chains fixes that, but that's beyond the scope of this discussion; you really need to consider the question "will app X be using the Bitcoin _blockchain_" entirely separately from "will app X be using the Bitcoin _currency"; all that sidechains do is let you use the Bitcoin currency on other blockchains.

3. Different use cases are probably going to need different security models. For

see more

21 · Reply · Share ›

Josh Fuchs ➚ Vitalik Buterin · 2 years ago

You're the man Vit!

3 · Reply · Share ›

Sonu ➚ Vitalik Buterin · a year ago

Very good. I was looking for a similar architecture view. many thanks.

Reply · Share ›

William Mougayar Mod ➚ fredwilson · 2 years ago

But in terms of using the blockchain as a software development building block, the Bitcoin liquidity itself may not be as important as the blockchain's technical capabilities. Plus, there's a possibility that the miners' powers and influences will be decreasing over time for several reasons, some outlined here: http://mobile.breakingviews.co...

Not all blockchain-related apps will be money-related. What I'm thinking about is the other side of the blockchain's use which is - the "value store/transfer" aspect, and I'd hope that multiple blockchains will be uniquely geared for these apps, especially as they scale.

The future of blockchain technology is certainly a fascinating topic that's still developing and maturing as we speak. I think the best of that technology is still ahead of us.

7 ^ v • Reply • Share ›

Dave W Baldwin • 2 years ago

Have only had a chance to scan, but this looks well done!

1 ^ v • Reply • Share ›

William Mougayar Mod ➚ Dave W Baldwin • 2 years ago

Thanks Dave. Read the following 2 posts as well :)

^ v • Reply • Share ›

greg_not_so • 2 years ago

if we equate blockchain with a public GL or a register of all bitcoin ownership changes then it does require some kind of a database. RDBMS market is quite crowded though and more details are needed on what specific implementations blockchain is actually deployed on like hardware, operating systems, data center, energy use, funding, etc.
in the interest of the new payment system public, the more public disclosure the better.
mining reminds me a bit of auditing or financial control, so again some kind of verification by the public is required.

1 ^ v • Reply • Share ›

Adrian Reason ➚ greg_not_so • a year ago

Sun & Son is working on a IBM Bluemix enabled platform for BlockChain apps - see www.sunandson.com Lightning Blockchain Enterprise - The Virtual NSF is a scalable RDBMS/NoSQL designed to support BlockChain Objects....

^ v • Reply • Share ›

Lisa Cheng • 10 months ago

Hello William - are you aware that you are using my Beanie Babies Smart Contract in your article? Would appreciate a credit please, thanks

^ v • Reply • Share ›

William Mougayar Mod ➚ Lisa Cheng • 10 months ago

No, I wasn't aware it was yours, but I had already linked to its original page where it says lisa on it.

^ v • Reply • Share ›

gail_c67 • a year ago

Hi, it seems that you have lots of knowledge about blockchains. Can you help me choose at least 5 companies where I can invest in blockchain startups?

^ v • Reply • Share ›

William Mougayar Mod ↗ gail_c67 • a year ago

Email me wmougayar@gmail.com

^ v • Reply • Share ›

Daniel • 2 years ago

To someone who does not come from a tech background, the block chain technology seems to represents a way forward in developing solutions to problems that we dont even know they exist in todays systems. Network inefficiencies and resource constraints such as human interjection in confirming 'security' check in a system or as in this example would be interpreted as proof of work is of tremendous value. With a transportation background I can think of an array of applications where this could become useful. As a way of promoting decentralization in current systems - What would be the recommended approach in starting to use block chain as a way to promote alternative thinking in managing existing networks? And, to what extent can the the existing block chain be customized to fit into the various industries where it could be deployed outside of crypto-currencies?

^ v • Reply • Share ›

jamie247 • 2 years ago

Nice breakdown for newbies. Note decentral.tv announced a recent breakthrough (can't find exact link) that someone has just done the inevitable; got Nodes to communicate on two separate blockchains.

^ v • Reply • Share ›

William Mougayar Mod ↗ jamie247 • 2 years ago

I must have missed it....is there a link?

^ v • Reply • Share ›

Mark Ranford ↗ William Mougayar • 2 years ago

Jamie may have meant the Blocknet which recently released an API for cross chain communication and their test between two chains

CALENDAR

December 2014

M	T	W	T	F	S	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

Follow

Subscribe by Email

POPULAR TAGS

29 30 31

M« NovW T F Jan » S

About | Contact

bitcoin blockchain boards branding

business model Canada ceo

content marketing crowdfunding

customer development Enterprise

entrepreneurship Europe growth

growth hacking growth metrics hiring

human resources innovation leadership

lean startup management marketing

marketing communications metrics

organizational structure pitching planning

product/market fit product management

raising money SaaS Sales

sales management scaling seo

software engineering ui/ux

unicorn analysis user conversion

user conversions user experience

VC-CEO relationship VC role

Venture Capital