ocs, You Can Understand Blockchain

William Mougayar (@wmougayar) | Published on September 8, 2016 at 14:51 BST

OPINION

William Mougayar is the author of "The Business Blockchain" and a board advisor to, and investor in, various blockchain projects and startups (See: Disclosures).

Here, Mougayar explains how blockchains can be more easily understood if users compare their functionality to popular document creation and collaboration tools.

The more people understand the blockchain, the more we will see a proliferation of useful cases for it.

Just like any technology, those who invent it have not necessarily thought of all of its applications, which is why I believe that the best use cases are yet to come from a growing number of entrepreneurs and subject-matter experts that have deep expertise in a particular field or domain.

But, the first step is to have a fundamental understanding of how blockchain technology is different from what we are currently doing today.

Almost everything in life is about taking evolutionary steps.

Even the brightest startups need to understand the behavioral switching psychology of their users (eg Facebook understood the concept of sharing), while large enterprises need to prepare for the ambitious management challenges they'll need to navigate to get blockchain projects moving.

The 'new database'

The idea that the blockchain is another kind of database is a popular analogy that has been used a lot (I wrote about this subject almost two years ago). In reality, the blockchain doesn't disrupt databases, but it disrupts how databases get synchronized between each other.

Imagine two entities (eg banks) that need to update their own user account balances when there is a request to transfer money from one customer to another. They need to spend a tremendous (and costly) amount of time and effort for coordination, synchronization, messaging and checking to ensure that each transaction happens exactly as it should.

Typically, the money being transferred is held by the originator until it can be confirmed that it was received by the recipient.

With the blockchain, a single ledger of transaction entries that both parties have access to can simplify the coordination and validation efforts because there is always a single version of records, not two disparate databases.

Let's take that analogy further into the shared documents domain, and think about what happens when we share a document where two or more users need to make changes to it.

Google Docs

The traditional way of sharing documents with collaboration is to send a Microsoft Word document to another recipient, and ask them to make revisions to it.

The problem with that scenario is that you need to wait until receiving a return copy before you can see or make other changes, *because you are locked out of editing it until the other person is done with it.*

That's how databases work today. Two owners can't update the same record at once. That's how banks maintain money balances and transfers; they briefly lock access (or decrease the balance) while they make a transfer, then update the other side, then re-open access (or update again).

With Google Docs (or Google Sheets), both parties have access to the same document at the same time, and the single version of that document is always visible to both of them. It is like a shared ledger, but it is a shared document. The distributed part comes into play when sharing involves a number of people.

Imagine the number of legal documents that should be used that way.

Instead of passing them to each other and losing track of versions, why can't *all* business documents become shared instead of transferred back and forth? So many types of legal contracts would be ideal for that kind of workflow.

You don't need a blockchain to share documents, but the shared documents analogy is a powerful one.

This article previously appeared on Startup Management and has been reproduced with the author's permission.

Old way of sharing image via Shutterstock

Disclaimer: *The views expressed in this article are those of the author and do not necessarily represent the views of, and should not be attributed to, CoinDesk.*

Banking distributed ledgers

PREVIOUS ARTICLE

Italy Wants to Tax Speculative Bitcoin Use

NEXT ARTICLE

Santander: Bitcoin Threatens Credit Card Issuers

RELATED STORIES

OPINION

Sep 9, 2016 at 14:10 | Frances Coppola

Blockchain Requires Radical Change, Not Compromise

A retro-fitted version of same-old system? That's what blockchain may become if financial firms aren't ready to be radical.

NEWS

Sep 8, 2016 at 18:33 | Pete Rizzo

Quick Blockchain Adoption a 'Myth', Says Russian Central Banker

Blockchain technology isn't ready to replace banks today, according to a high-ranking official at Russia's central bank.

Sep 7, 2016 at 17:38 | Michael del Castillo

INDUSTRY PRESS RELEASES

Sep 8 | 15:34 **Deloitte brings Bitcoin ATM to Toronto's Financial District**

Sep 8 | 15:01 **Nav Coin Updates Anonymous Network**

Sep 8 | 14:49 **Diginomics Announces Affiliate Marketing Program**

Sep 1 | 14:32 **Using BlockchainTechnology to Promote Regional Development: Announcement of the Start of Collaborative Research in Smart Local Currencies**

VIEW MORE SUBMIT RELEASE

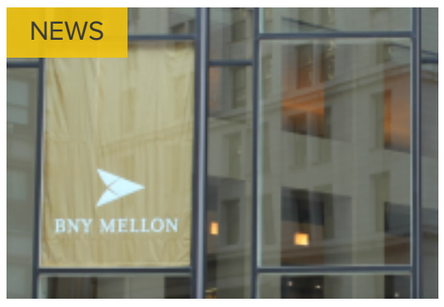
Got a news tip or guest feature?

NEWS

BNP Paribas Opens Lab to Boost Productivity With Blockchain

BNP Paribas has unveiled a new Innovation Lab with a blockchain focus.

NEWS



Sep 7, 2016 at 14:56 | Stan Higgins

BNY Mellon is Backing Up Bank Transactions With Blockchain Tech

BNY Mellon has developed a trial system which leverages the blockchain in order to create a backup record for transactions.

4 Comments CoinDesk 1 Login

Recommend Share Sort by Best

Join the discussion…

Tracer289 • a day ago

"The distributed part comes into play when sharing involves a number of people."

I think this is where the analogy departs from the reality of blockchains.

Bitcoin isnt "distributed" so that we can share and give everyone unlimited access to the blockchain.
Bitcoin is available to all, but compartmentalized so that any given user can only alter their portion of the blockchain, according to strict rules.

The blockchains "killer app" is still it's use as sound money.
Go Honeybadger!

2 • Reply • Share ›

Dinofelis • a day ago

The "shared document" analogy illustrates perfectly the problem. Suppose that we have a document where the title is "go go block chain". Now, *I* want to change that in "go go database", and my colleague wants to change that into "giga blockchain", and we are editing simultaneously.
What happens ? In the "traditional" back and forth way: the last one to change the document gets his thing done. I send the document to Jack, who modifies the title into "giga blockchain". I get it back, the lock is now with Jack, and I get what I want: "go go database"

What happens with Google docs ? We fight: he changes it, I change it, and we end up with something like "gigao datachain" when the link breaks down. But there is still a single document.

What happens with a block chain ? It forks. We have now two chains, one with the last block "title = giga block chain"< and another one with the last block "title = go go database".

see more

1 • Reply • Share ›

bruno cecchini Dinofelis • 11 hours ago

Your analogy only apply for public blockchain, is the referee paradox that create the gridlock.

• Reply • Share ›

Dinofelis bruno cecchini • 6 hours ago

The essence of a block chain is the "struggle for the single chain" which is supposed to be won each time by the "immutable and honest" chain. It is the fact that all possible forks can and may occur, but that, by lack of collusion over anything else but the original protocol, only the "immutable, original protocol one" will survive. If you have any other way of arbitrage, through a centralized authority, then it is not a block chain (even if it contains blocks that make up a linked list of hashes).

In other words, if there is an agreed-upon referee who has "power to decide", then your thing is not a block chain, but a signed database, because your referee has a signature that nobody else has.

In the bitcoin block chain, the arbiter is simply PoW: the chain which has the highest amount of PoW muscle will win. A pure PoS chain is or self-defeating, or the final arbiter is the creator of the genesis block (the only guy who can construct a totally new chain with the same genesis block, and assign himself all PoS at every instant).

The immutability, and the coherence amongst the distributed versions of the

see more

• Reply • Share ›