How Transactions Are Validated On A Distributed Ledger
George Samuel Samman

People say China's in trouble. I just got back from a trip there, and sorry, but I disagree.
David Sable

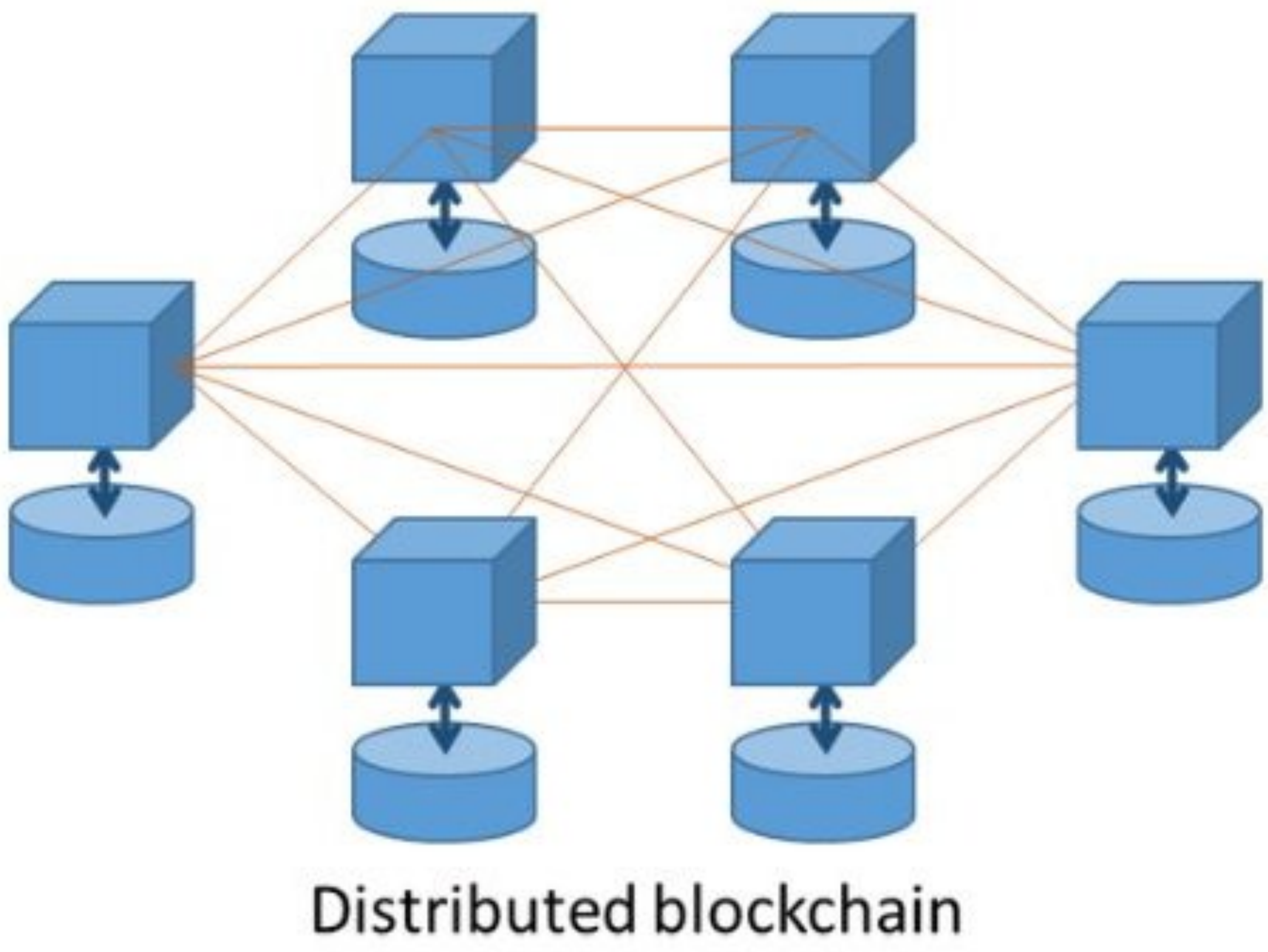
Education reform is tough. Antwan Wilson may have the answer.
Maya Pope-Chappell

How Asking 5 (Lean Manufacturing) Questions Helped Me Eat Dinner With …
Charles Duhigg

Does the Rise of Slack Signal the Slow Demise of Email?
Daniel Burrus

Zika-carrying mosquitoes developing resistance to top insecticide
www.statnews.com

The rise of the YouTube video essay



George Samuel Samman
Blockchain Advisor

Follow

How Transactions Are Validated On A Distributed Ledger

Mar 9, 2016 | 199 views | 48 Likes | 2 Comments

Originally posted on my blog: sammantics.com

(A special thanks to Simon Taylor who was instrumental in much of my thinking through conversations we had around this topic. His input was invaluable)

This post will explore how transactions will be validated using distributed ledger technology. It will also provide some use cases around who those transaction validators may be and what that would look like. First off, transaction validation will be different from the bitcoin blockchain because Proof of Work will not be used. The features of a private blockchain network are:

1. Peer to peer: transfer assets directly between parties who control the assets.

2. No bitcoin currency: networks are built for specific markets and can issue & transfer any asset.

3. No mining: transactions are ordered by trusted parties that form a "federation" or the nodes on a distributed ledger.

4. Fast: confirmation in seconds.

5. Scalable: 1000s of transactions per second.

Financial Institutions Don't Want Public Blockchains

This is not a debate anymore. Tim Swanson, Director of Market Research from R3CEV, wrote a paper titled:***"Watermarked tokens and pseudonymity on public blockchains"*** citing the reasons why this is so. Tim puts it succinctly here:

"There are at least three identifiable reasons that financial organizations looking to use some kind of public blockchain should be wary of a watermarked approach:

1) the built-in security system inherited from Bitcoin and other proof-of-work-based blockchains is not exportable in a regulated financial settlement setting (through a distortion of incentives);

2) the lack of legal settlement finality; and

3) the regulatory risks that a watermarked approach introduces

This paper prefers to use the term watermarked token to encompass two types of systems: 1) Colored coins and 2) Embedded consensus systems which use their own proprietary metacoin"

Note: A metacoin is a coin that is launched on top of another blockchain, as a "meta" layer.

I highly recommend reading this paper for deep insights into this issue. The world of public blockchains was invented so parties who don't know each other and don't trust each other could transact. The financial world operates in a very different manner. The parties must know and trust each other and be identified. When parties can trust each other there is no need for the inefficiencies associated with public blockchains in the form of mining and solving the "double spend" problem. (This occurs if two transactions attempt to spend the the same output, only one of those transactions will be accepted.) Without mining one can just validate the transactions and add to the chain by creating hash functions regardless and forming blocks. A private blockchain for the most part behaves in the same manner as a public blockchain.

One of the main differences comes from the ***transaction validators***, who need to be onboarded and accredited/trusted to join the ledger. Their identity is known to everyone. This actually adds an extra layer of security because if a node performs a malicious act, they can be persecuted and ejected from the network. As opposed to a public blockchain network, the transaction validators in a private blockchain are not incentivized in the form of tokens (money) but in having the benefit of being a part of the ledger and being able to read data they consider valuable. This post will explore this issue further as perhaps there is a role for disinterested/neutral parties to be involved as the transaction validators so there is no conflict of interest. For their services, perhaps some form of payment will be necessary. That payment would not be in the form of cryptocurrency token, since with a private blockchain the assets that are being exchanged don't live on the chain (like bitcoin). It is more of a promise of exchange.

Getting rid of mining allows for significant performance enhancements for distributed ledgers as they still have unique properties over a replicated database pattern:

1. Any node is able to write to the chain at anytime without a centralized node coordinating "write" operations.
2. The network could be a coalition of business entities with no one entity owning the network. This creates greater incentives to want to share and use the infrastructure.
3. A synchronization technology that allows some nodes on the ledger to have non-identical copies of the database. (reason for this explained below)

Transaction Validators Provide A Service

Transaction validators provide a service for the entire ledger. They determine if transactions meet protocol requirements for the ledger and make a determination that it is "valid".   In distributed ledgers, the transaction validators group these transactions into ordered units (blocks) by agreeing on the validity of the transaction and ordering them specifically so as to prevent a "double spend."

I spoke to Simon Taylor VP of Entrepreneurial Partnerships at Barclays, around this issue and he gave some good first principles to think about when trying to understand why and how transaction validators should be selected and what purpose they are serving:

"Think about why you need validation. What are you trying to prove with validation? Am I proving that records match? That business logic executed? Who needs to see this happen? Everyone in the network? Some people in the network? What's my threat model for why I might want "consensus" or validation?

So the first goal is to step back and say: Who needs to see the data? To do what in a financial transaction? This might be the counterparties. A Central Counterparty (CCP). A smart oracle. A regulator and perhaps two law firms and a custodian. Why then would I want other network participants to validate the transactions?"

These transaction validators play a critical role in the success of the blockchain as they have the ability to "write" to the ledger and send out confirmations of the transactions. They provide a unique record of truth from which all the parties act.

Security Concerns Without Proof of Work

Since malicious actors on a distributed ledger are known and can be prosecuted, the main security concerns are the stealing of private keys.

1. The actor creating the transaction can store their keys in a secure offline place. This is known as cold storage. This is not very practical though.
2. The actor can store her private key on the local hard drive of their PC. This is a problem because it could get hacked.
3. The actor could let a third party provider manage their private keys in a wallet. This is probably the most convenient for non-technical people in

financial institutions and corporations who have limited knowledge about blockchains.

This is no different than public blockchains except there is one major security upgrade: trust. Knowing the counterparties and transaction validators keeps incentives aligned for forming a distributed ledger to begin with.

Examples Of How Private Blockchains Are Validating Transactions

Different companies are using different methods for validating transactions. Most of this information is not public knowledge yet. However, a few companies have shared how they are doing it and I will list a few examples of such.

Antony Lewis, in his fantastic blog, describes how Multichain (a private blockchain company headed by Gideon Greenspan) validates via a round-robin process:

"Bitcoin's computation-intensive Proof-of-Work solves for a Sybil attack in an anonymous network i.e. a small group of entities pretending to be a large group of entities who agree on something in order to spoof the system. With a permissioned blockchain where block creators are known and have to sign blocks that they create, you don't have this problem so you don't need a 'difficult' or slow mining puzzle.

MultiChain uses a randomised round-robin system for block-adders and a concept of mining diversity which is a configurable strictness on how long a block-adder has to sit out for after he has added a block, before the other nodes will accept another block from him.

- *At one extreme of the scale (strictness of zero), any block-adder can add any block meaning it's very tolerant but also increases the risk that a single block-adder or small group of block-adders can spoof the system.*

- *At the other extreme of the scale, (strictness of 1) once you have added a block, you have to let every other block-adder add a block before you can add again. This stops single or groups of block-adders from creating forks, but if a node goes offline then at some point no further blocks will be able to be added while the network waits for the offline node to add the next block.*

- *Strictness lets you adjust the balance between security and technical* *malfunction risk."*

The block adders are transaction validators in this model and the asset owners are the parties which are performing the transaction.

Tim Swanson in his latest blog post talks about how Hyperledger, which was acquired by DAH and how they validated transactions:

"The simplest way to describe Hyperledger, the technology platform from Hyper, during its formative year in 2014 was: Ripple without the XRP. Consensus was achieved via PBFT. There were no blocks, transactions were individually validated one by one.

Hyperledger, the technology platform from Hyper, was one of the first platforms that was pitched as, what is now termed a permissioned distributed ledger: validators could be white listed and black listed. It was designed to be first and foremost a scalable ledger and looked to integrate projects like Codiusote, as a means of enabling contract execution."

Note: Practical Byzantine Fault Tolerance (PBFT)

Ripple achieves consensus via the nodes on the network sharing information about transactions. Once a supermajority of the nodes agree, consensus is achieved. This can be an iterative process before the transaction becomes validated.

Other private blockchain companies are doing exactly what public blockchains are doing without using proof of work. (as mentioned above). They are grouping transactions into blocks, creating one way cryptographic hash functions and using multi party consensus algorithms to name a few things.

The methods companies are employing to validate transactions is one I want to learn more about going forward as this is a critical piece to the success of the distributed ledger/private blockchain space. For a lot of companies they are probably still trying to sort through the best way to do this. The health of the whole ledger depends on the ability of the parts to adapt and withstand stress. In this case that would be points of failure on how transactions get validated and who those validators are.

Another major assumption which is now being challenged is around a replicated shared database in which all of the data is synchronized that all of the nodes on the ledger have identical copies. This is where the 3rd assumption above comes to play: A synchronization technology that allows some nodes on the ledger to have non-identical copies of the database. This opens the doors for an entirely new option as to how transactions will be validated on a ledger.

Let's suppose we have a distributed ledger which has 20 banks as nodes. Other nodes would include regulators, lawyers, a custodian, a smart oracle (smart contracts) and perhaps disinterested parties to be transaction validators. How is a decision made as to who the transaction validators are within that ecosystem? Are all of the banks going to be alright with only a few of them being the transaction validators? This could present a massive conflict of interest based on what data those validators are privy to. Not to mention the fact that most financial institutions, enjoy anonymity in how they are transacting and trading in today's world and consider it a distinct advantage. Are they going to have to give this up in order to be a part of the ledger or will attempts be made to be able to keep this confidential? How can the transactions be distributed as such to ensure the anonymity?

Some radical thinking has been done to avoid such issues. Only the nodes involved in a trade will validate the transaction amongst themselves. Hence, every node on the ledger will have write functionality. This works by not sharing the data and the transactions with any nodes that aren't directly involved in the trade. What is shared is the business logic (the instructions around the structure of the transaction) and the workflows (what goes where) via smart contracts. In other words, the business logic is known to all parties but the transaction itself remains anonymous except between the counterparties. This allows everyone on the ledger to see that something happened the way it was supposed to happen without sacrificing confidentiality. The data stays in each banks node, while the ledger itself contains an itemized list of where everything is held.

What comes to one mind instantly is well if the two parties are transacting amongst themselves what stops them from collusion on trades. Certainly a transaction validator would need to be someone else aside from the two parties to make sure bad acting doesn't take place. Regulators or other market infrastructure players could be nodes to oversee the transactions and trades. What is really compelling about this idea aside from ensuring anonymity of amounts and types of transactions is banks having their own data stored in their nodes. This allows each counterparty to control their own data and not the ledger as a whole which would not be acceptable to anyone involved. If the whole network were compromised, that would be perilous to that data. Storing the data in this way affords extra protections for the individual finanicial institutions.

Transaction Validation in Clearing & Settlement

Perhaps this opens the door for the incumbents to be a part of the ledger. Parties like DTCC and the exchanges who are more disinterested observers than the other participants and are experts in this could be nodes on the network. The role of both changes in this new world. No longer do they host the data, as that will remain in the banks nodes, but they could be involved in setting contract templates (smart contracts) and managing upgrade cycles. They could also have a record of all the transactions that are linked to every transaction that has occurred between participants (each and every financial institution) on the ledger. This would be extremely valuable for establishing a chain of custody of each and every transaction as it changes hands (provenance).

There is also a need for a private key administrator as well. This role will need to be filled. Maybe this falls to some of the rising stars in the cybersecurity world. Regardless of whether this a real possibility or not it will be interesting to see how these incumbents position themselves going forward. It will also be interesting to see how other types of companies begin to think about transaction validation for their own use cases. In coming blog posts, this topic will be explored further.

Distributed Systems, Financial Services, Banking   Report this

Written by
George Samuel Samman

Follow

Like   Comment   48 likes   2 comments

Add your comment

Popular

Christopher Franko 2nd
Blockchain Scientist at Ribbit.me

:)

Like Reply 1 hour ago

Show More

David Sable
Global CEO at Y&R

Follow

As the Chinese Proverb Says: The timber has become a boat. The rice is cooked.

Mar 8, 2016 | 4,151 views 336 Likes 22 Comments

木已成舟(mù yǐ chéng zhōu) 生米煮成熟饭(shēng mǐ zhǔ chéng shú fàn):

The timber has become a boat. The rice is cooked.

A Chinese proverb meaning that what is done cannot be undone.

This thought was very much on my mind this week, as I spent time with my various offices in China – mainland and Hong Kong – and reviewed business, prospects and work.

And, I think, I was particularly sensitized because of my recent trip to Cuba and my observations about the people. It is impossible not to begin to benchmark and compare – despite the fact that according to a few of my readers I am a "cretinous stooge for the totalitarian Communists of Cuba" and now I imagine China…what can I say.

Still, in this country, with pockets of incredible wealth and prosperity; of amazing innovation and creation; of ingenuity and just plain smarts…stories like this one are a jolt…

Read here from the BBC.

It tells the tale of five Hong Kong booksellers who vanished in 2015 and last week showed up on Chinese TV "confessing" to promoting and selling "unauthorized" books critical of communist leaders on the mainland.

This is a story we might have seen 50 years ago and read with horror, yet today it barely registered in the West and, let's not forget, it was a fairly hard line, conservative United States President – Richard Nixon – who so long ago helped to "chop the wood and get the rice boiling" by opening China to the US and the West.

I can never be in China without marveling at all the changes that have occurred here since I first visited, back in the 80s, when I entered through Shekou and had to pass through a "Museum of Chinese History" before I could get to the street – a museum that did nothing but highlight Chinese advancement through the years while the decadent West languished. I was assigned a dedicated secret policeman calling himself Michael Jackson (Michael Jordan was the other popular name), who was at my side 24/7. I have written about this before…the only car on the road for miles and miles, the Friendship Stores where only the elite could buy Western goods, the impossibility of actually speaking with anyone, no access to local currency – you get the picture.

Today you enter freely through modern air terminals; the cars are new and numerous…as are the traffic jams…with Maseratis and BMWs and you name it; the Friendship Stores are decaying hulks surrounded by Cartier and Vuitton; get on WeChat and you can speak to anyone and do just about anything you can think of, and currency is open to all.

Yet, surrounded by the latest fashions (global and Chinese), a sea of expensive designer bags, and a never-ending clicking of fingers on smartphones, I could not help closing my eyes, as I queued up to leave the plane on an internal China flight, and picturing a sea of people dressed alike in the same drab outfits, shuffling along…a scene that was the norm until almost 1980.

It was only some 35 years ago that the Fashion Revolution began on the street and in 1979 Pierre Cardin, the famous French fashion designer, staged the very first fashion show in China in modern times.

Today, Chinese journalists, tourists and the just plain curious travel to border cities near North Korea to ponder what it was like in China only some 50 years ago. Read further here: TIME.

And now, the society that transitioned from a narrow government-imposed Brand Slave identity to a self-imposed global Brand Slave position craves individualism and personalization, with manyChinese niche fashion brands exploding all over the world.

And yet, connecting to Facebook or Twitter is spotty if you even can connect at all – and many of your favorite shows are streamed without key scenes, as government censorship protects you from anything antigovernment or anticommunist.

On the other hand – who needs Facebook or Twitter when you have WeChat…and can do so much more with it…

I will let you read about the comparisons yourself, and I also recommend that you carefully compare the valuations of WeChat vs Facebook and Alibaba vs Amazon – and make your own conclusions…

The real question is what can we learn from China? And will the timber stay in the boat and the rice on their plates?

Here is my view.

There is a huge absence of the Digibabble fever that so pervades Western digital development, usage and valuation.

As Connie Chan of venture capital firm Andreessen Horowitz put it, “While Facebook and WhatsApp measure growth by the number of daily users on their networks, WeChat cares more about how relevant and central it is in addressing the daily, even hourly, needs of its users.”

Jack Ma talks about learning from American retail. He unabashedly buys tons of local TV time to drive digital sales. He intrinsically gets, in true Sam Walton tradition; that you follow the consumer to where the money is. In a day, Alibaba ships 4x the number of packages that Amazon does (lower average orders to be fair) yet makes a profit…HMMMMMMM – maybe that’s real disruption (a topic for another time).

WeChat is about lifestyle. And life is social. The Chinese get that and have from the start. Yet Mark Zuckerberg who seems to follow that thought, “Humans are fundamentally social…So…if a technology doesn’t actually help us socially understand each other better, it isn’t going to catch on,” uses it to argue that virtual reality will make people feel more connected to the real world…kind of like Amazon’s drones. Listen:

> *What’s happening in Asia is an inspiration – and not only WeChat…but that’s more about proof of what’s possible. It’s proof that everything starts from a conversation. There were 2,000 years when everything happened through a conversation, then a blip when the web came out when behavior was very structured – you’d go to websites, look for things to buy, and it was straight-up merchandising when you’d assume there were no human beings behind it. In Asia, the conversation was never removed. That’s why people are discovering the world through those apps.” – Stan Chudnovsky, head of product management for messaging products at Facebook*

More to ponder:

More Chinese students study outside of China than any other country’s students study outside of theirs.

There are more billionaires in Beijing than in New York.

The Chinese are buying up real estate all over the world – as an investment and to protect their money from the government – but they are not just buying in big cities and in huge blocks. They are buying residential and across the US, Australia and Europe.

Although many Chinese cannot afford to travel both due to time allotment and money, more and more do, spending $230 billion in the countries they visit.

And of course foreign investment in China continues to grow.

All of which leads me to this thought:

青出于蓝而胜于蓝 (qīng chū yú lán ér shèng yú lán)

Indigo blue is obtained from the indigo plant, but such color is bluer than the plant itself.

Bottom line? The disciple has surpassed the master.

According to the Best Countries Report, published by the *U.S. News & World Report*, in collaboration with WPP's BAV and the Wharton School of the University of Pennsylvania:

China is perceived as the number one country in the world in which to start a career.

Ai Weiwei, the legendary Chinese artist and dissident, put it all in perspective:

> *To survive, China had to open up to the West. It could not survive otherwise. This was after many millions have died of hunger in a country that was like North Korea is today. Once we became part of global competition, we had to agree to some rules. It's painful, but we had to. Otherwise there was no way to survival.*

Let me end with a personal story, from my recent visit, that spoke volumes.

I went to see the Jewish Refugees Museum, a history of the Shanghai Community of European Jews who were saved from the Nazis and their allies by the Chinese during World War II. It is a most moving exhibition, made even more so to me by the family names I recognized, as a number of my friends' parents and grandparents were saved in Shanghai. And our young guide, a local volunteer, spoke with pride about the communities – both Chinese and Jewish.

As we were leaving, a few buses pulled up and out came the students from a local school…it seems that schools visit every day – it is a part of local history and culture. What distinguished this school, an international school, was that the instructors and all the children, despite being local, all spoke English as that is the language in which they are taught. One of my friends, an "old China Hand" remarked that they would all go to school in the US or England…

Chinese students learning, in English, about China's role in saving Jews from the Holocaust…

The indigo is bluer than the plant…

So you can argue, as they did in Davos, about growth in China being 6% or 4% and bemoan the double-digit slowdown.

Or you can view (as I did) with cynicism the tears of Xi Jinping – but do pay attention to his use of social media…

Or listen to Mao…yes Mao (save the knee-jerk cretin remarks…). Listen:

> ***The world is yours, as well as ours, but in the last analysis, it is yours. You young people, full of vigor and vitality, are in the bloom of life, like the sun at eight or nine in the morning. Our hope is placed on you. The world belongs to you. China's future belongs to you.***

The timber will never leave the boat and the indigo is the most amazing blue –

time to learn from ourselves...back to basics....

What do you think?

Asian Business, Marketing And Advertising, China Business Development

Report this

Featured In Business Travel, Editor's Picks, Economy, Asia Pacific

Written by
David Sable

Follow