Alan Shteynberg | + Follow

Goodbye Blockchain. Hello Hashgraph.

Published on October 29, 2017

If you thought blockchain tech was immune from obsolescence, you have either been misled or are simply being naive. The overwhelming greed and malformed hype in the blockchain space as it relates to cryptocurrencies has been so grand that it's clouding our better vision and judgement and is creating a cult like atmosphere – perhaps unwittingly so.

It's time to snap back to empirical reality and accept the fact that a better technology exists. This tech retains most of the properties that blockchain introduces – that is being a distributed, cryptographically secure, fault tolerant network that achieves fair consensus, all without the scalability and security issues that plagued "legacy" blockchain networks.

The new consensus algorithm

Introducing Hashgraph – a fair and fast, byzantine fault tolerant consensus algorithm. According to the founding Hashgraph team consisting of computer science and cybersecurity pioneers Dr. Leemon Baird and Mance Harmon, the hashgraph consensus method achieves the following notable feats:

- It's fast: 250,000+ transactions per second and limited only by a users bandwidth (Pre-Sharding)
- It's fair: mathematically proven fairness (via Consensus Time Stamping)

- It's secure: bank-grade security (Asynchronous Byzantine Fault Tolerant)

Why is Hashgraph superior to Blockchain?

Unlike the presently employed blockchain networks such as that of Bitcoin and Ethereum, hashgraph eliminates the need for the massive computational and energy requirements that Proof-of-Work consensus succumbs to. Using the 'gossip about gossip' protocol enables hashgraph to be lightweight, nimble and much like gossip between friends, is able to spread exponentially and almost by definition is transparent. For example, the Bitcoin blockchain is about 60GB in size, where as hashgraph uses a fraction of that memory, about 1GB, allowing cell phones to act as nodes. Here is an image that provides a reasonable comparison by analogy.

Gossip about gossip uses votes instead of 'blocks', and as a result can achieve transaction times the likes of which blockchain can only dream of. If used to create another cryptocurrency, hashgraph will eliminate the issue of network forks caused by network congestion thanks to its ability to scale infinitely. Some blockchains are Byzantine and others are Fault Tolerant, but no blockchain is both Byzantine AND Fault Tolerant. With hashgraph, the network is guaranteed to be Byzantine Fault Tolerant, 100% of the time. Unlike a blockchain where a miner can choose the order for which transactions occur in a block, can delay orders by placing them in future blocks, and can even stop them entirely from entering the system, the hashgraph consensus method timestamps each node (event), so assumptions are no longer required, ergo Byzantine. In other words, no member can prevent the community from reaching a consensus, nor can they change the consensus once it has been reached. Blockchain merely assumes that a consensus was reached as probability approaches 1 whereas hashgraph guarantees it thanks to its generational "gossip about gossip".

Here is an updated community message from the Hashgraph team that makes further necessary distinctions and clarifications:

> *Note that we are our own consensus algorithm. While Ethereum is looking at PoS with Casper, our algorithm uses something called Virtual Voting – its a voting system – without having to do the votes. Hashgraph uses a protocol called "Gossip about Gossip" to achieve consensus. Gossip is a well known computer science term, which can be defined as calling any random node and telling that node everything you know, that it does not know. In distributed ledger technology the*

"baseline" or minimum bandwidth required is that the transactions go to every node. Gossip about Gossip refers to attaching a small additional amount of information to this Gossip, which contains the last person we talked to, hence, we are gossiping about the information we gossiped. Using this information, we can build the Hashgraph. Once we have the Hashgraph, it is extremely easy to know what a node would vote, because we know what each node knows, and when they knew it. We now can use the data from the Hashgraph as an input to 30 year old voting algorithms, and achieve consensus essentially for free. These 30 year old voting algorithms have strong math proofs- they are Asynchronous Byzantine Fault Tolerant, which means we know when we will achieve consensus, guaranteed, and our math proofs make no assumptions about the speed of the internet, due to firewalls, ddos attacks, viruses or botnets. In addition, because of gossip about gossip, Hashgraph is extremely fast, (250,000 transactions/sec), and we also get fair ordering and time stamping on every event.

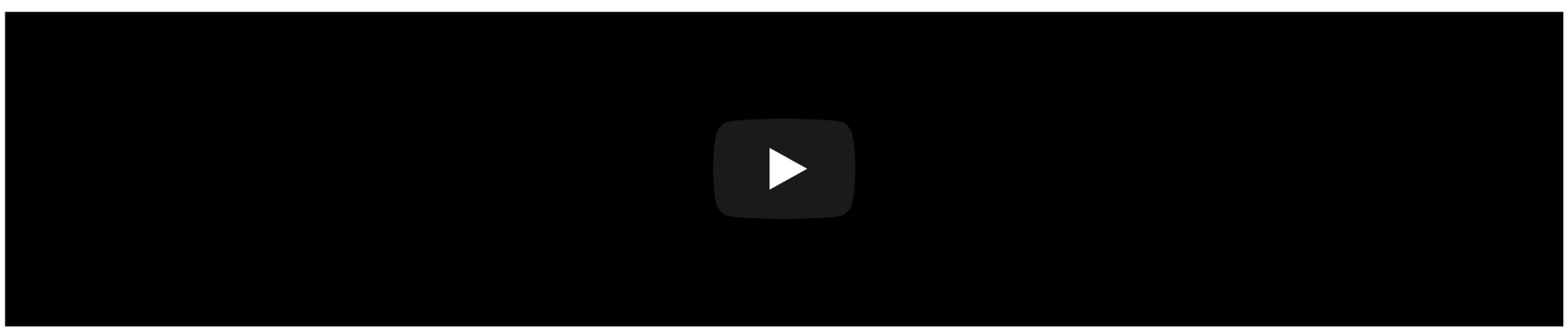
Use cases for Hashgraph

If you thought Blockchain was powerful, think again. Here are just some of the possible applications that can be built on top of hashgraph:

- Markets
- Identity
- Gaming
- Cryptocurrency
- Online Collaboration
- Public Ledger

Here are some promising, sample test-bed projects that were built on top of Hashgraph at a recent TechCrunch hosted Hackathon event.

Project Fair Auction Ledger



Project Ground Zero

All is not lost

Don’t fire sell your Bitcoin or Ether just yet. Blockchain paved the way for cryptocurrencies which still have their place in our new decentralized eco-system. For starters, unlike Satoshis original vision, Hashgraph is NOT open-source and therefore is not truly decentralized. The technology is patented by Leemon Baird and his colleagues over at Swirlds, a startup that has recently raised over $3 million to help commercialize the use of Hashgraph. Think of Swirlds as a distributed Oracle, in that their main clients would be corporations and institutions that want to leverage the decentralized properties of permissioned consensus algorithms with absolutely no possibility of downtime, rather than just cryptocurrencies used by enthusiasts and cypherpunks alike.

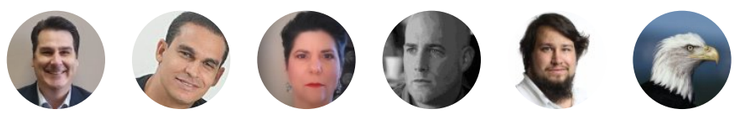
However, Swirlds also stated that making hashgraph open-source is still on the table, and if that happens, the free and open market will ultimately decide where to appropriate their value as it relates to cryptocurrencies and beyond.

If you are interested in learning more about Hashgraph, watch Leemon Baird’s layman break-down of the inner-workings of a hashgraph.

Original article can be found here.

Report this

6 Likes



1 Comment

Mark Morris now ···

All-Star -- Principal Software Architect for Smart Alerts, Lower Colorado River Authority (LCRA) IIoT & Bloc…

Patents hinder open source success, so they would need to be neutralized, if open source were a real desire. Ping is a major investor, so it would be a failure on Ping's part to let a strategic opportunity slip through their fingers--it seems they see new revenue opportunity utilizing this initially for "Global Logout", a thorn in SSO and Federation. Would they really allow it to become open source and take a chance that a couple of kids crank out a killer platform for "Global Logout", SSO, Federation, etc. thus cannibalizing their business or would they consume it and resell it? With the protection of the patent to scare away competitors. Perhaps they will more likely offer a light open source version and charge for the real thing, like so many today do. Personally, I doubt the patent(s) would withstand ALICE and rightfully so. This may only be a proprietary product suitable for specific use cases employed by entities that are able to pay perpetual fees allowing the company to jack up the fees for perceived competitors and lower them for non-competitors. The performance numbers are not unique and you will see others publish higher numbers (red belly for one) and eventually open source code will implement the ideas without infringing or a totally new idea will emerge. This space is new and just beginning, so as the body of work grows so too will the innovations and available solutions. As for size and mobility well again that is not unique either. I downloaded the SDK, analyzed it, and ripped it apart. The magic is in the underbelly hidden away from the public Java API and implemented in an open source version of LISP--funny implement closed source with your secret sauce implemented by embedded artifacts produced by open source--an open source implementation of LISP :) I studied the published paper. It is impressive and a wonderful read. The math is exquisite and beautiful. I can see why Leemon took 5 years to formulate it and human nature would demand reward measured by effort rather than utility. If you can't tell I love open source but I do understand the strategic and tactical nature of trying to combine and leverage open source with proprietary secret sauce. Not everyone want to build an open source services company--it is tough and a long hard road to profitability where as a niche is easy money and a lot beach time :) If they do get onboard and become an open source company I will be an advocate and user. But if they go dark I will not be employing it. Too many ways to skin the blockchain or hashgraph cat and achieve the end goal. That's why clients hire and love me, I can deliver the goods even if it means inventing new goods. Software is like life if you don't like it change it, if you can't change it, replace it, if you can't replace then get something new, if nothing is new, then make it.

Like Reply

Goodbye Blockchain. Hello Hashgraph.

Published on October 29, 2017

Report this

6 Likes

1 Comment

Mark Morris 8m ···
All-Star -- Principal Software Architect for Smart Alerts, Lower Colorado River Authority (LCRA) IIoT & Bloc…

Patents hinder open source success, so they would need to be neutralized, if open source were a real desire. Ping is a major investor, so it would be a failure on Ping's part to let a strategic opportunity slip through their fingers--it seems they see new revenue opportunity utilizing this initially for "Global Logout", a thorn in SSO and Federation. Would they really allow it to become open source and take a chance that a couple of kids crank out a killer platform for "Global Logout", SSO, Federation, etc. thus cannibalizing their business or would they

Like **Reply**

Add a comment…

Messaging