Hedera Hashgraph - A Survey Review as of Early 2021

Justin Ty

April 2021

Abstract

Hedera Hashgraph provides a fast and efficient alternative to blockchains used by current distributed ledger technologies. Consensus can be achieved with the use of gossip and virtual voting. This survey review paper investigates the project's technical innovation, history, governance and current status as of early 2021.

1 Background

To understand Hashgraph, one has to understand an overview of current distributed ledger technologies (DLT). Bitcoin[24] is a decentralised digital cryptocurrency that enabled transactions without a central intermediary. It uses a technology called the blockchain for participants to agree on their balances on the ledger. As a proof-of-work, blocks are added to the blockchain by the process of mining. Participants try to come to an agreement on a longer chain with the reasoning that more "work" has been put on it. Ethereum[30], dubbed as a second generation DLT, further improved the concept by enabling smart contracts to operate on the blockchain.

While these early generation DLTs rose in popularity, wide-spread mass adoption has been limited due to blockchain's ability to scale. At the time of writing, Bitcoin and Ethereum can only currently do around 3+ transactions-per-second (TPS)[8] and 12+ TPS respectively[11]. This is significantly below what incumbent systems such as Visa can provide[27] that powers transactions in a modern economy.

Additionally, most blockchains using proof-of-work can only offer probablistic eventual finality[2]. Finality is a guarantee that past transactions cannot be changed. With Bitcoin, confirmation generally takes about 10 mins. For larger amounts of money, it is typically recommended to wait for up to 6 blocks or about 60 mins to minimise risk of double spending or transaction reversal[19]. This type of finality is only probablistic where a shorter chain may catch up with a longer chain given enough hashing power.

Gossip protocols are known to efficiently broadcast information with high reliability and throughput[28]. Achieving consensus was historically done by

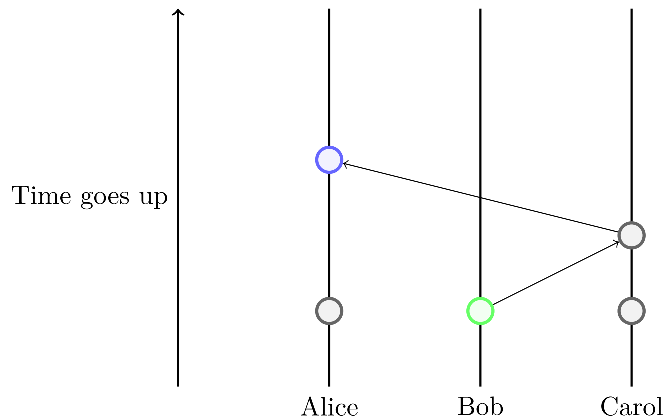

Figure 1: A simple example of how hashgraph spreads information via gossip. Bob randomly gossips to Carol, then Carol randomly gossips to Alice. Alice would have known what Bob and Carol spoke about without talking to Bob directly. This is the process of gossipping about gossip. Bob's green event is defined to be "strongly seen" by Alice's blue event as it was seen by at least 2/3 members along the way.

sending votes across the network[6]. Sending votes across is an expensive operation that has not been reliably implemented in real-world conditions.

Hedera Hashgraph[4] combined a gossip protocol with the concept of virtual voting to achieve consensus in a radically different way than a blockchain. The network can reach consensus in a more efficient manner than the current proof-of-work process of mining. As a result, it provides a fast, high-throughput, fair-ordering, finality, and asynchronous Byzantine Fault Tolerant (aBFT) alternative to blockchain solutions.

2 Overview of the Hashgraph algorithm

Hashgraph uses standard cryptographic hashes and digital signatures to securely spread events across a network by gossipping about gossip as illustrated in Figure 1. It was mathematically proven that each member will eventually have a consistent local copy of a Hashgraph for each member to run virtual voting without the need to send votes across the network[4]. Because each member knows how other members would have voted, finality and consensus can be achieved.

The Byzantine Generals Problem[26] provides the motivation to solve the consensus problem. The theorem illustrated in Figure 2 states that consensus cannot be reliably reached if 1/3 or more are malicious. That is the bound provided by the mathematical theorem in any distributed system. Distributed systems cannot do better than the bound provided by this theorem. To be

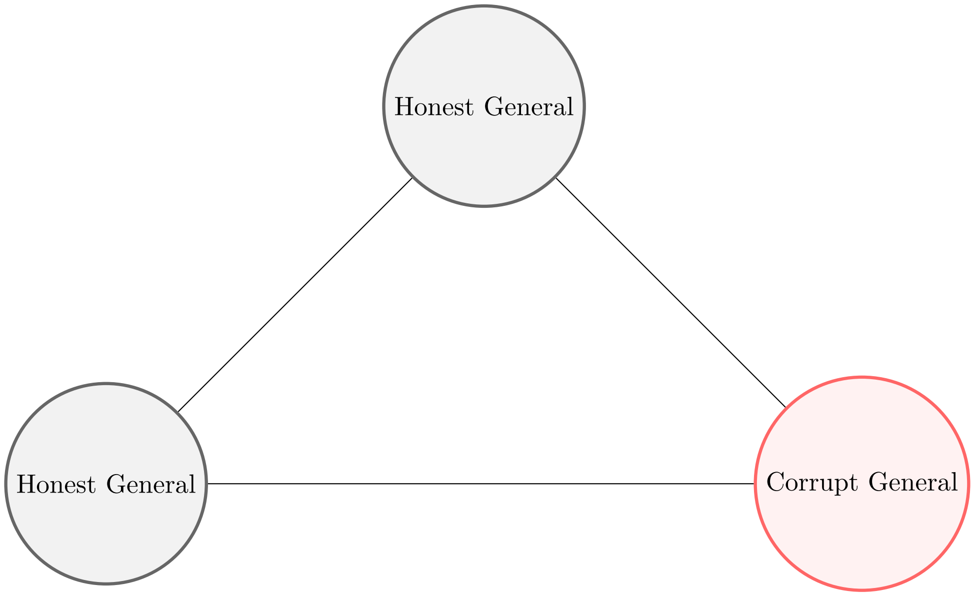

Figure 2: An illustration of the Byzantine Generals Problem. The Theorem states that consensus cannot be reached if 1/3 or more are malicious.

Byzantine Fault Tolerant means that a distributed system can withstand failure with some unreliable actors. Asynchronous adds another layer of complexity where messages may get delayed or altered, similar to the real internet with firewalls and denial-of-service attacks. Asynchronous Byzantine Fault Tolerant (aBFT) is the highest level of security a distributed system can achieve[12].

Hashgraph was proven to be aBFT[4]. While a full mathematical proof is beyond the scope of this paper, Figure 3 illustrates it's key pillar of the Strongly Seeing Lemma.

In terms of how this translates to its implementation, it is currently on a permissioned system which relies on no 1/3 or more nodes are malicious. Once it has completed it's path towards decentralisation, it's proof-of-stake system will rely on 1/3 or more of the coins are not owned by malicious actors.

3 Critical analysis

3.1 Governance

Originally under Swirlds, Hashgraph's ownership was transferred to the Hedera Governing Council. It is a decentralised council of term-limited multinational companies [5].

It's decentralised governance is based on Visa's model[14] which ensures that the council does what is best for the network. No single company has complete

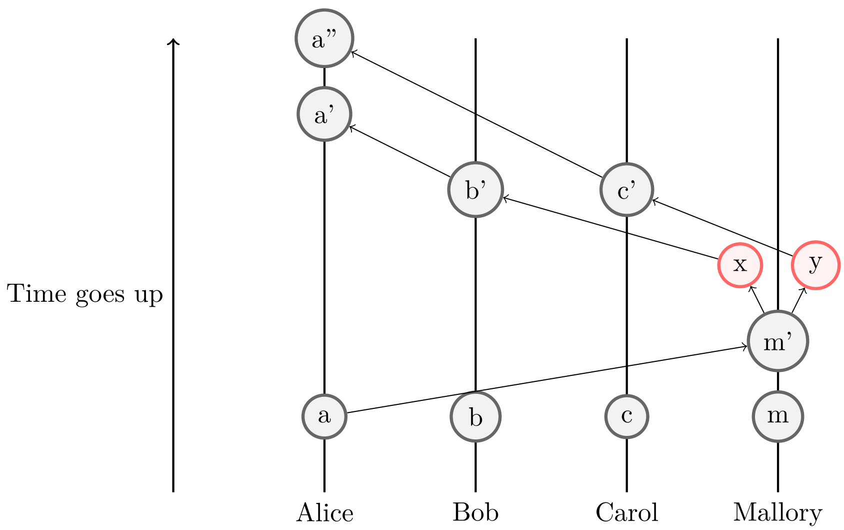

Figure 3: Suppose Mallory cheats by forking an event, eg: she could double spend her coins by gossiping two different events (x & y) to different members. The Strongly Seeing Lemma says that a forked event will not be strongly seen by honest members. A proof by contradiction shows that if 2/3 strongly sees x and 2/3 also strongly sees y, then this is impossible to be strongly seen if only less than 1/3 members are malicious. This violates the assumption that only less than 1/3 are malicious, as no honest member will strongly see both events. If Alice, Bob, and Carol are honest and communicate further, they will agree not to strongly see Mallory’s events as valid.

control and any malicious acts will certainly damage a member's reputation. Well-known companies are in the council which includes Google, Boeing, LG, and Eftpos Australia. It has seats for 39 council members with only 20 seats filled at the time of writing.

A criticism of Hedera Hashgraph is that the network must agree on N, the total number of participants [20]. As of early 2021, it is currently on a permissioned system which makes N known. Council members currently operate these nodes.

3.2 Open review, not open source

The source code will only be available as open review, not open source. However, anyone can raise a proposal to improve the network by raising a Hedera Improvement Proposal (HIP)[16]. This governance model will prevent forks similar to what happened to Bitcoin Cash and Ethereum Classic because Hedera is the only authorised body that can use the proprietary Hashgraph technology.

This model can be controversial in the cryptocurrency community which has factions that favour a fully decentralised model. However, one has to look into where mining power has been concentrated in a proof-of-work system, and coin concentration in a proof-of-stake system to fully assess a network's true decentralisation of power.

3.3 Security, staking and tokenomics

Currently on a path towards decentralisation, Hashgraph's proof-of-stake system will rely on no 1/3 or more of the coins are owned by malicious actors. Hedera has outlined a release schedule without compromising the network's security. All coins have already been minted and saved in a treasury which will be released over 15 years[13]. It will be extremely difficult for a single actor to accumulate enough coins to compromise the network. The law of supply and demand states that surges in demand with a fixed supply will result in price increases, holding other things constant.

There are plans to enable users to proxy stake their coins. This will allow users to stake their coins to well-known nodes which will help secure the network[22]. There is no slashing involved with this staking mechanism. In return, users will be rewarded with additional coins for participating. This is very different compared to a mining pool, a system purely based on luck. With staking, users are rewarded in proportion to their stake.

Gossip relies on assumptions to be fully robust [1]. The concept of gossip in a distributed system is well known, but combining it with the concept of virtual voting is novel. As it is a new concept, the algorithm was checked by a Coq system (a formal verification system) which proves that it is aBFT - the highest security possible in a distributed system [12].

3.4 Performance and efficiency

Depending on the region setup, real world experiments using AWS instances have shown throughputs of 50-000-500,000+ transactions-per-second[5]. It still remains to be battle tested in a permissionless setup, but its current transaction volumes[15] already surpass what Bitcoin and Ethereum can do. It is currently operating on a single shard, but it is possible to scale this even more with the addition of more shards.

Hashgraph has recently surpassed 1 billion transactions with the mainnet being only online for only about one and a half years[21]. For comparison as of 2021, Bitcoin[7] is still below 700 million transactions while Ethereum[10] just surpassed 1 billion this year.

Compared with the proof-of-work system used by Bitcoin, proof-of-stake is more environmentally friendly as no mining is involved. Hashgraph can also be argued that it is more fair than mining because it does not favour entities with economies of scale or access to cheap electricity.

It was estimated that Hashgraph uses 600,000 times less energy per transaction than Ethereum and a 5 million times less than Bitcoin[25]. A per transaction analysis has also shown that Hashgraph is almost on par with Visa at 0.000170 kwh and 0.001486 kwh respectively.

3.5 Current services and integrations

Hedera currently offers the following services[18] which enables the development of distributed applications:

- Hedera Token Service - enables minting, management and configuration of fungible and non-fungible tokens.
- Hedera Consensus Service - can provide fair ordering, verification, and transparency on streaming data.
- Hedera File Service - distributes files on each node which may help with storing files that need active storage on the ledger.
- Hedera Smart Contract Service - can run existing Solidity contracts. It is however recommended to use the Hedera Token and Consensus service for most use cases for higher performance at a lower cost.

Hedera also offers integrations[17] for Corda, Hyperledger, and Logstash.

3.6 Use cases

Blockchain 3.0[23] discussed use cases for a third generation DLT such as elections, micro-payments, supply chain management.

In the UK, Everyware is currently using Hashgraph to track the supply chain of the COVID-19 vaccine[9]. Temperature sensitive vaccines need a tamper-proof system to ensure the vaccine's proper delivery.

Eftpos Australia is currently developing the next-generation micropayments technology which may potentially open new ways for Australian businesses and consumers to interact. Use cases are are currently being developed as proof-of-concepts which includes sub-cent payments to unblock online paywalls[3].

Central bank digital currencies[29] (CBDC) is another potential use-case. Only a few countries have rolled out their own CBDCs. Although it is speculative which technologies central banks are evaluating, more central banks may follow given the interest and investment in the area. Hashgraph's technical innovation offers scalability while it's governance model offers stability, features central banks may consider critical.

4 Conclusion and final remarks

In a saturated market of cryptocurrencies with calls to "hodl to the moon", there is a lot of noise and hype in this rapidly changing environment. Hedera Hashgraph stands out in a number of ways. Its technical innovation provides a new level of efficiency that can enable DLTs to scale. The governance structure can enable mainstream enterprise adoption with a path towards decentralisation. It is rare to find a cryptocurrency with these features that breaks away from the blockchain, let alone a formal verification by a Coq system that proves it is aBFT - the strongest level of security in a distributed system.

It is not so often that a technology can be disruptive and make a generational leap. Bitcoin and Ethereum may have paved the way for first and second generation DLTs, Hedera Hashgraph has the potential to take the lead of the third generation DLTs. Hedera has a lot of potential on paper and on real world use cases. While there are tangible use cases happening today, there are still more items to be developed in the roadmap and there is still room for more council members to join. Similar to the early days of the internet, Hashgraph's technical capabilities and governance model may become a potential enabler for more use cases in the future.

References

[1] Alvisi et al. "How robust are gossip-based communication protocols?" In: *CS Cornell* (). DOI: `https://www.cs.cornell.edu/lorenzo/papers/p14-alvisi.pdf`.

[2] Emmanuelle Anceaume et al. "On Finality in Blockchains". In: *arXiv preprint arXiv:2012.10172* (2020).

[3] *Australia's eftpos joins Hedera Governing Council and will run Aussie Hedera network node.* 2021. URL: `https://www.eftposaustralia.com.au/news/eftpos-joins-Hedera-Governing-Council-and-will-run-Aussie-Hedera-network-node`.

[4] Leemon Baird. “The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance”. In: *Swirlds Tech Reports SWIRLDS-TR-2016-01, Tech. Rep* (2016).

[5] Leemon Baird, Mance Harmon, and Paul Madsen. “Hedera: A governing council & public hashgraph network”. In: *The trust layer of the internet, whitepaper* 1 (2018), pp. 1–97. URL: https://hedera.com/hh_whitepaper_v2.1-20200815.pdf.

[6] Piotr Berman, Juan A Garay, Kenneth J Perry, et al. “Towards optimal distributed consensus”. In: *FOCS*. Vol. 89. Citeseer. 1989, pp. 410–415.

[7] *Bitcoin Total Transaction Count*. 2021. URL: https://blockchair.com/bitcoin/charts/total-transaction-count.

[8] *Bitcoin TPS*. 2021. URL: https://blockchair.com/bitcoin/charts/transactions-per-second.

[9] Ryan Browne. *UK hospitals are using blockchain to track the temperature of coronavirus vaccines*. 2021. URL: https://www.cnbc.com/2021/01/19/uk-hospitals-use-blockchain-to-track-coronavirus-vaccine-temperature.html.

[10] *Ethereum Total Transaction Count*. 2021. URL: https://blockchair.com/ethereum/charts/total-transaction-count.

[11] *Ethereum TPS*. 2021. URL: https://blockchair.com/ethereum/charts/transactions-per-second.

[12] Hedera Hashgraph. *Coq Proof Completed By Carnegie Mellon Professor Confirms Hashgraph Consensus Algorithm Is Asynchronous Byzantine Fault Tolerant*. 2018. URL: https://hedera.com/blog/coq-proof-completed-by-carnegie-mellon-professor-confirms-hashgraph-consensus-algorithm-is-asynchronous-byzantine-fault-tolerant.

[13] Hedera. *Hbar Economics*. 2020. URL: https://hedera.com/hh-hbar-coin-economics-paper-060320-v6.pdf.

[14] *Hedera Council*. URL: https://hedera.com/council.

[15] *Hedera Dashboard*. URL: https://hedera.com/dashboard.

[16] *Hedera Improvement Proposal*. URL: https://github.com/hashgraph/hedera-improvement-proposal.

[17] *Hedera Integrations*. URL: https://hedera.com/integrations.

[18] *Hedera Services*. URL: https://hedera.com/services.

[19] *How Long Does a Bitcoin Transaction Take?* 2020. URL: https://coinmarketcap.com/alexandria/article/how-long-does-a-bitcoin-transaction-take.

[20] Josh Kauflin. *Hedera Hashgraph Thinks It Can One-Up Bitcoin And Ethereum With Faster Transactions*. 2018. URL: https://www.forbes.com/sites/jeffkauflin/2018/03/13/hedera-hashgraph-thinks-it-can-one-up-bitcoin-and-ethereum-with-faster-transactions/?sh=22d5f2abcb2a.

[21] Gehrig Kunz. *One Billion Hedera Mainnet Transactions*. 2021. URL: https://hedera.com/blog/one-billion-mainnet-transactions.

[22] Paul Madsen. *Hedera Technical Insights: Proxy Staking on Hedera*. 2019. URL: https://hedera.com/blog/proxy-staking-on-hedera.

[23] Damiano Di Francesco Maesa and Paolo Mori. "Blockchain 3.0 applications survey". In: *Journal of Parallel and Distributed Computing* 138 (2020), pp. 99–114. DOI: https://www.sciencedirect.com/science/article/pii/S0743731519308664?casa_token=2haaftsC5fwAAAAA:7n41Q9ZFYMRC5IS5Xc14k7hRDx8CTnpBn8wCiztujRjzRvSo2AVWdwL63C60SMpJa-681AI.

[24] Satoshi Nakamoto and A Bitcoin. "A peer-to-peer electronic cash system". In: *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf* 4 (2008).

[25] Jiro Olcott. "Can a Blockchain be green?" In: *PVOLTS* (2021). URL: https://ptvolts.com/sites/default/files/documents/sustainable-blockchain-power-transition.pdf.

[26] Robert Shostak, Marshall Pease, and L Lamport. "The byzantine generals problem". In: *ACM Transactions on Programming Languages and Systems* 4.3 (1982), pp. 382–401.

[27] *Visa Fact Sheet*. 2021. URL: https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf.

[28] Werner Vogels, Robbert Van Renesse, and Ken Birman. "The Power of Epidemics: Robust Communication for Large-Scale". In: *Computer Communication Review* 33 (Jan. 2003), pp. 131–135.

[29] *What is a central bank digital currency (CDBC)*. URL: https://hedera.com/learning/what-is-a-central-bank-digital-currency-cbdc.

[30] Gavin Wood et al. "Ethereum: A secure decentralised generalised transaction ledger". In: *Ethereum project yellow paper* 151.2014 (2014), pp. 1–32.