PRACTICE

A Hitchhiker's Guide to the Blockchain Universe

By Jim Waldo

Communications of the ACM, March 2019, Vol. 62 No. 3, Pages 38-42
10.1145/3303868

Comments (1)

PRINT

VIEW AS: SHARE:

Credit: Andrij Borys Associates / Shutterstock

It is difficult these days to avoid hearing about blockchain. Blockchain is going to be the foundation of a new business world based on smart contracts. It is going to allow everyone to trace the provenance of their food, the parts in the items they buy, or the ideas they hear. It will change the way we work, the way the economy runs, and the way we live in general.

Despite the significant potential of blockchain, it is also difficult to find a consistent description of what it really is. A recent Google search for "blockchain technical papers" returned nothing but white papers for the first three screens; not a single paper is peer-reviewed. One of the best discussions of the technology itself is from the National Institute of Standards and Technology, but at 50-plus pages, it is a bit much for a quick read.[9]

The purpose of this article is to look at the basics of blockchain: the individual components, how those components fit together, and what changes might be made to solve some of the problems with blockchain technology. This technology is far from monolithic; some of the techniques can be used (at surprising savings of resources and effort) if other parts are cut away.

Because there is no single set of technical specifications, some systems that claim to be blockchain instances will differ from the system described here. Much of this description is taken from the original blockchain paper.[6] While details may differ, the main ideas stay the same.

Back to Top

Goals of Blockchain

The original objective of the block-chain system was to support "an electronic payment system based on cryptographic proof instead of trust ..."[6] While the scope of use has grown considerably, the basic goals and requirements have remained consistent.

The first of these goals is to ensure the anonymity of blockchain's users. This is accomplished by use of a public/private key pair, in a fashion that is reasonably well known and not reinvented by the blockchain technology. Each participant is identified by the public key, and authentication is accomplished through signing with the private key. Since this is not specific to blockchain, it is not considered further here.

The second goal is to provide a public record or *ledger* of a set of transactions that cannot be altered once verified and agreed to. This was originally designed to keep users of electronic currency from double-spending and to allow public audit of all transactions. The ledger is a record of what transactions have taken place, and

MORE NEWS & OPINIONS
How the Artificial-Intelligence Program AlphaZero Mastered Its Games
The New Yorker
When Chinese Hackers Declared War on the Rest of Us
Technology Review
Google Translate Does Not Understand the Content of the Texts
Herbert Bruderer

ACM RESOURCES
Motivating Your Employees (Includes Simulation)
Courses

the order of those transactions. The use of this ledger for verification of transactions other than the exchange of electronic cash has been the main extension of the blockchain technology.

The final core goal is for the system to be independent of any central or trusted authority. This is meant to be a peer- or participant-driven system in which no entity has more or less authority or trust than any other. The design seeks to ensure the other goals as long as more than half of the members of the participating community are honest.

Back to Top

Components of Blockchain

While there are lots of different ways to implement a blockchain, all have three major components. The first of these is the ledger, which is the series of blocks that are the public record of the transactions and the order of those transactions. Second is the consensus protocol, which allows all of the members of the community to agree on the values stored in the ledger. Finally, there is the digital currency, which acts as a reward for those willing to do the work of advancing the ledger. These components work together to provide a system that has the properties of stability, irrefutability, and distribution of trust that are the goals of the system.

The ledger is a sequence of blocks, where each block is an ordered sequence of transactions of an agreed-upon size (although the actual size varies from system to system). The first entry into a block is a cryptographic hash (such as those produced by the Secure Hash Algorithm SHA-256) of the previous block. This prevents the contents of the previous block from being changed, as any such change will alter the cryptographic hash of that block and thus can be detected by the community. These hash functions are easy to compute but (at least to our current knowledge) impossible to reverse. So once the hash of the contents of a block is published, anyone in the community can easily check that the hash is correct.

So far, this is nothing new; it is simply a Merkle chain, which has been in use for years. The wrinkle in block-chain is that the calculation of the hash needs to add a nonce (some random set of bits) to the block being hashed until the resulting hash has a certain number (generally six or eight) of leading zeros. Since there is no way to predict the value that will give that number of leading zeros to the hash, this is a brute-force calculation, which is exponentially difficult on the number of zeros required. This makes the calculation of the hash for the block computationally difficult and means any member of the community has the chance of coming up with an acceptable hash with a probability that is proportional to the amount of computing resources the member throws at the problem. Coming up with the hash and the right nonce is a proof of work (and, perhaps, luck) that can be easily verified by anyone in the community. Those attempting to calculate the right hash value for a block are the *miners* of the block-chain world; they are exchanging computation for pay.

Once a miner comes up with the right nonce that produces the right hash, they broadcast the result to the rest of the community, and all miners start work on the next block. The first entry in the new block will be the hash of the last block, and the second entry in the block will be the creation of some amount of currency assigned to the miner who found the hash for the previous block.

This works only if you have a block to start the chain. This is done in the same way all systems get started: by cheating and declaring a block to be the Genesis block.

It is possible that two different miners could both find, at the same time (or close enough), a nonce that gives a candidate hash value with the right number of leading zeros, or that someone seeing a nonce that works could claim the discovery as their own. There could even be two different blocks being proposed as the next entry in the chain. Dealing with such issues requires the next component of the system: the consensus protocol.

Consensus protocols are among the most-studied aspects of distributed systems. While it was proved some time ago that no algorithm will guarantee consensus if there is a possibility of any kind of failure,[3] a number of well-known protocols such as Paxos[4] have been used in systems for some time to give highly reliable mechanisms for distributed agreement. In consensus protocols such as Paxos, however, it is assumed the systems that must reach agreement are known.

Depending on the failure model used, the number of systems that must agree to reach consensus changes. When a majority of systems agree in such a protocol (for some definition of majority), consensus has been reached in systems that want to protect from non-byzantine failure. If the system is subject to byzantine failure, then two-thirds of the systems (plus one) need to agree. While the voting can be done in peer-to-peer systems, most efficient versions of the algorithms depend on a leader to initiate the voting and tally the results.

In the blockchain universe, however, there is a trust-free system, which means there can be no leader. Further, in the blockchain universe the number of systems participating in validating the transactions (that is, finding a hash for the block with the right number of zeros in the prefix) is not known. This makes claims that a block is accepted when 51% of the miners agree on the block nonsense, since there is no known value for the number of entities trying to agree.

Instead, the majority is determined by the calculation of the hash for the next block. Since that block begins with the hash of the previous block, and since the likelihood of the next block's hash being calculated is proportional to the amount of computing resources trying to calculate the appropriate hash for the next block, if a majority of the computing power available to the miners starts to work on a block that is seeded with the previous hash, then that block is more likely to be offered as the next block. This is the reason for consensus being tied to the longest chain, as that chain will be produced by the largest number of computing resources.

This mechanism relies on the generation of a hash with the right set of leading zeros being genuinely random. Being random also means that on occasion someone will get lucky and a chain that is being worked on by a minority of the miners will be hashed appropriately before a chain that is being worked on by a larger amount of computing resources.

In an important sense, however, this does not matter. The blockchain universe defines a majority as the production of an appropriate nonce and hash. Sometimes this means more than half of the computing power has worked on the problem, but other times it might mean only one (exceptionally lucky) miner got the answer. This might mean a set of transactions in a block that is not verified first need to be rolled back, but that is the nature of in-flight transactions.

It does mean all of the miners in the blockchain universe need to move to a newly hashed block as the basis for the calculation of the next block in the chain. This requires an incentive mechanism, which is where the third component of the blockchain universe enters the picture: digital currency.

Digital currency. The reason for a miner to do all the computational work to calculate the nonce and hash of a block is that the first to do so gets an allocation of digital currency as the first transaction in the next block. This also encourages other miners to accept a block as quickly as possible, so they can start doing the work to hash the next block (which has likely been filled with transactions during the time it took to hash the previous block). Bitcoin was the original blockchain currency and incentive; in September 2017 the reward for hashing a block was 12 bitcoins[8] when the exchange rate was 1 bitcoin = ~$4,500 U.S. (prices fluctuate rather wildly). This reward halves (for bitcoin) every 210,000 blocks. The next halving is expected around May 25, 2020.[1]

Other digital currencies work in a similar fashion. To spend the currency, entries are made in the then-current block, which acts as a ledger of all the currency exchanges for a particular ledger/digital coin combination.

Back to Top

Problems with Blockchain

While blockchain was originally proposed as a mechanism for trustless digital currency, its uses have expanded well beyond that particular use case. Indeed, the emphasis seems to have bifurcated into companies that emphasize the original use for currency (thus the explosion of initial coin offerings, which create new currencies) and the use of the ledger as a general mechanism for recording and ordering transactions. For the first use, the claim is that blockchain can replace outdated notions of currency and allow a new, private, friction-free economy. For the latter use, the claim is that blockchain can be used to track supply chains, create self-enforcing contracts, and generally eliminate layers of mediation in any transaction.

Both of these kinds of uses present some serious problems. Many are problems any new technology encounters in replacing entrenched interests, but a number of them are technical in nature; those are the ones discussed here.

A number of criticisms of blockchain center on the mechanism used to create an accepted hash for a block. To ensure this can be discovered by anyone, the mechanism needs to be one that takes significant computation but can be easily verified. To ensure the blocks that are verified cannot be changed, the computation needs to be impractical to reverse. Hashing the block using a function such as SHA-256 and requiring that a nonce value is added until some number of leading zeros appears in the hash fits these characteristics nicely. This very set of requirements, however, means the consensus mechanism has intrinsic limitations.

Scaling. An obvious worry about the consensus-by-hashing mechanism used in blockchain is whether the technology can scale to the levels needed for more general use. According to blockchain.com, the number of confirmed transactions averages around 275,000 per day, with a peak over the last year of about 380,000.[2] This is an impressive number but hardly the 400,000 transactions per minute that major credit-card systems perform on peak days. Blocks can currently be verified at a rate of four to six per second, and this is the limiting factor on the number of transactions.

While there are a number of proposals to deal with scaling blockchain, it is unclear how these fit with the base design of the system. Making the verification of a block difficult and random is an important aspect of the basic design of blockchain; this is the proof of work that is at the core of the trustless consensus algorithm. If the verification of a block is made easier, then the probabilistic guarantees of any miner being able to discover the appropriate hash decreases, and the possibility of some miner with a large amount of computing taking over the chain increases. Verifying a block is meant to be hard; that's how the system avoids having to trust any particular member or set of members.

One mechanism suggested for scaling is to shard the blockchain into a number of different chains, so that transactions can be done in parallel in different chains. This is happening in the different coin exchanges; each coin system can be thought of as a separate shard. This introduces its own complexity in order to have a transaction that crosses these shards, since the notion of ensured consistency requires that all ledgers are self-contained to allow consistency checking within each ledger. A new blockchain could be created to be used for cross-blockchain transactions, but the incentive mechanism for that blockchain would be a new electronic currency that would need to stay within the ecosystem of this new blockchain. Getting the interacting blockchains to trust the mediating blockchain is an unsolved problem.

While blockchain was originally proposed as a mechanism for trustless digital currency, its uses have expanded well beyond that particular use case.

There have also been attempts to use some mechanism other than proof of work to drive the consensus protocol. Perhaps the best known of these is the proof-of-stake approach, in which a block can be calculated in much simpler ways, and consensus is reached when those with a majority of the currency agree on the hashing of the block. Since the amount of currency and its owners are known, this is not subject to the problem of not knowing the members of the community to vote. But this does reintroduce the notion of trust to the system; those who have more money have more of a stake, and therefore are trusted more than those who have less of a stake. This is the electronic equivalent of an oligarchy, which has not worked particularly well in the past but might prove more stable in this context.

Power consumption. A second criticism of blockchain technology that is an outgrowth of the consensus mechanism is the amount of energy consumed in the discovery of an appropriate hash for a block. Calculating a hash with the appropriate number of leading zeros requires many hashing calculations, which in turn burn a lot of electricity; some have claimed that bitcoin and related cryptocurrencies are mechanisms to transform electricity into currency. The estimates of how much electricity is consumed range from the low side stating that it is about as much as is used by the city of San Jose, CA, to the high side that it is equivalent to Denmark's power consumption. No matter which model is used for the calculation, the answer is large.

The hope is that this energy drain will diminish, perhaps by changing the hardware used for the hashing to something far more efficient (such as specialized ASICs). Making the hashing process more efficient, however, is at odds with blockchain's fundamental mechanism of trusting no one; the point is that the verification of a block must be difficult and random so that any miner is equally likely to find the hash.

The energy consumption might be less worrisome if the calculations eating all of this power were generally useful. SETI@home, for example, uses a considerable amount of energy by offloading analysis of background radio-wave transmissions to Internet-connected computers. This initiative, based at UC Berkeley's SETI (Search for Extraterrestrial Intelligence) Research Center, is trying to find signs of other intelligent life in the universe, which is seen by the participants as worth doing (and paying for the extra electricity).

Perhaps the calculation used to verify the blockchain could be changed to something that offered more than just verification of the blockchain. Such a calculation would need to have the properties of being equally possible for all miners to find (given equality of computing resource), difficult to find, and easy to verify. It is not clear what this calculation might be.

Trust. Perhaps the most problematic aspect of blockchain is its core notion of being trustless. Much of the complexity of the technology is caused by this requirement. It is unclear, however, that this is even necessary for the kinds of uses people talk about as core to blockchain, or that the system is actually free of trust.

It is because of the lack of trust that the system requires verification of the block to be computationally difficult, one-way, and easy to verify. If this requirement of trustlessness were dropped, then production of a public ledger that was unchangeable and easily verified could be done easily. Suppose such a ledger is to be used for inter-bank transfer (which has been suggested as a use for blockchain). Instead of a trustless system, however, the users decide to trust a consortium of major banks, the Federal Reserve Board, and some selection of consumer watchdog agencies or organizations. This consortium could choose a member (perhaps on a rotating basis) who is responsible for keeping the ledger (a leader). Transactions are written to the ledger, and when the ledger block reaches an appropriate size, the leader hashes the ledger, uses the hash to start a new block, and continues (just as in the current blockchain).

The difference is that there is no need for the leader to randomly try values added to the block until the right number of leading zeros is produced in the hash. Without that requirement, the hash can be done very quickly with little energy expense. The block still can't be changed (since the hash is still a one-way function), and any member of the consortium (or anyone else who has access to the ledger) can quickly check the hash. A public, verifiable, and unchangeable ledger can be produced in this way but at much lower cost in both time and energy.

This does require trust in the various members of the consortium, but verifying that the consortium is not cheating on the hashing of a block would be easy. This is not a fully centralized trust in a single entity but, rather, trusting a group. The larger and more varied the group, the less likely the group would collude. Note also that such a system does not need an incentive mechanism such as a digital currency to operate.

Back to Top

Who Do You Trust?

Maybe you really do not want to trust anyone. Calibrating paranoia is difficult, and perhaps you really do want to have an economic system in which no specifiable set of entities has the ability to collude and control the system. That is the real reason for blockchain.

As Ken Thompson pointed out in 1984, trust has to happen somewhere.[7] Even if you do not trust any group to calculate the blocks, you need to trust the developers of the software being used to manage the blocks, the ledgers, and the rest. Everything from bugs to design changes[5] in the software have led to forks in the bitcoin ecosystem that have caused considerable churn in those systems. If your trust is in the security and solidity of the code, that is a choice you make. But it is not a trustless system.

A public, nonrefutable, unalterable ledger for transactions could be a useful tool for a number of applications. Building such a system on top of known cryptographic protocols could be done in a number of ways. Doing it on top of a system such as blockchain is needed if the requirement that the system be trustless (except for trusting the software) is added. Such a trustless system comes with a cost.

Whether the cost is worth it is a decision that requires an understanding of the various parts of the system and how they interact. A public, unforgeable, unchangeable ledger is possible without cryptocurrency or a consensus algorithm based on a difficult-to-compute one-way function that is easily verified. Cryptocurrencies can be created without the use of either a public ledger or a trustless consensus algorithm. And consensus algorithms can be created that do not require a financial incentive system or a public ledger.

Related articles
on queue.acm.org

Bitcoin's Academic Pedigree
Arvind Narayanan and Jeremy Clark
https://queue.acm.org/detail.cfm?id=3136559

Research for Practice: Cryptocurrencies, Blockchains, and Smart Contracts; Hardware for Deep Learning
https://queue.acm.org/detail.cfm?id=3043967

Certificate Transparency
Ben Laurie, Google
https://queue.acm.org/detail.cfm?id=2668154

Back to Top

References

1. Bitcoinblockhalf.com. Bitcoin block reward halving countdown.

2. Blockchain.com. Confirmed transactions per day, 2018; https://www.blockchain.com/charts/n-transactions?daysAverageString=7.

3. Fischer, M., Lynch, N.A., Paterson, M. Impossibility of distributed consensus with one faulty process. *JACM 32*, 2 (1985), 374–382.

4. Lamport, L. The part-time parliament. *ACM Trans. Computer Systems 16*, 2 (1998), 133–169.

5. Morris, D.Z. Bitcoin is in wild upheaval after the cancellation of the Segwit2x fork. *Fortune* (Nov. 12, 2017); http://fortune.com/2017/11/12/bitcoin-upheavel-segwit2x-fork/.

6. Nakamoto, S. Bitcoin, a peer-to-peer electronic cash system, 2008; https://bitcoin.org/bitcoin.pdf.

7. Thompson, K. Reflections on trusting trust. *Commun. ACM 27*, 8 (Aug. 1984), 761–763; https://dl.acm.org/citation.cfm?id=358210.

8. Trubetskoy, G. Electricity cost of 1 bitcoin (Sept. 2017); https://grisha.org/blog/2017/09/28/electricity-cost-of-1-bitcoin/.

9. Yaga, D., Mell, P., Roby, N., Scarfone, K. Blockchain technology overview. NISTIR 8202 (Oct. 2018). National Institute of Standards and Technology; https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf.

Back to Top

Author

Jim Waldo is a professor of the practice of computer science at Harvard University, where he is also the chief technology officer for the School of Engineering, a position he assumed after leaving Sun Microsystems Laboratories.

Comments

John Schlesinger

February 25, 2019 08:35

It is not true that distributed consensus cannot be achieved in the presence of one faulty participant. The proof of this, cited in the article, is only for asynchronous protocols. Synchronous protocols can achieve consensus when some participants are faulty. See Gray and Lamport Consensus on Transaction commit 2004 for a discussion of this https://www.microsoft.com/en-us/research/publication/consensus-on-transaction-commit/.

Displaying **1** comment

Comment on this article

Signed comments submitted to this site are moderated and will appear if they are relevant to the topic and not abusive. Your comment will appear with your username if published. View our policy on comments

□ Notify me via email when subsequent user comments are published with this article.

For Authors | For Advertisers | Privacy Policy | Help | Contact Us | Mobile Site