Power consummation of validating new blocks – negligible with Proof-of-Stake instead of Proof-of-Work - Byazian

Motivation for validating nodes, when no reward?

What to include in ledger?

Private or public blockchain?

Virtual currency?

Anonymity? – yes, to avoid someone monitoring energy usages to e.g. see when no one is home

Pricing? Factors influencing pricing?

Bidding for power? – Producer set wanted price and consumers bid at certain price. Highest bidder gets first dibs and so on.

Cryptography?

Byzantine Fault Tolerance? Consensus algorithm – required when more than one node in network, to ensure decentralization

Why resolve conflicts with longest chain?

Nodes communicating via web interface?

Voting? Settling new blocks?

Draw parallel to internet/intranet for public/private?

Blockchain vs database cluster?

Merkel trees?

Micropayments – expensive because of transaction fee – how to avoid?

Any way of knowing that power is transferred physically even though the transaction is documented digitally?

**Distributed ledger** – security?

Possible to do analytics of e.g. equipment in blockchain?

Another low-risk approach is to use blockchain internally as a database for applications like managing physical and digital assets, recording internal transactions, and verifying identities. This may be an especially useful solution for companies struggling to reconcile multiple internal databases – HBR

Possible due to TCP/IP – HBR - The analogy used by Marc Andreessen 2,5 years ago, comparing Bitcoin/Blockchain to TCP/IP as we knew it in the 1990's

Speed of transfer – bitcoin takes up to 10 minutes today – Bitcoin needs 10 minutes for global consensus based on Proof of Work.

The security of proof-of-work (also known as mining) indeed relies on spending computing power. This is used by Bitcoin and most cryptocurrencies. However, it is a not a requirement for blockchain applications and if we look at private blockchain applications, none of those use proof-of-work – HBR comments – Proof of Stake instead of Proof of Work

Blockchain is a technology for keeping records of transactions using cryptography and distributed peer-to-peer systems. Transaction equivalent to TCP/IP for communication. Transparent, irreversible and programmable (trigger events). Infrastructure and applications – slideshare

Blockchain – trust – right after Lehman Brothers fell – housing bubble burst

Kodak blockchain example of use, settling land ownership

Also known as distributed ledger technology

no single point of failure.

*Blockchain might not be necessary in this proposed application, ~~list reasons (table)~~, however, it will be implemented and the resulting pros and cons found through testing and examination of results will be evaluated*

<https://link.springer.com/content/pdf/10.1007%2Fs12599-017-0467-3.pdf> **:**

Trace exact ownership of every asset

The distributed ledger system described above offers many benefits. In contrast to centralized systems, the functionalities of the network persist even if particular nodes break down. This increases trust since people do not have to assess the trustworthiness of the intermediary or other participants in the network. It is sufficient if people solely build trust in the system as a whole.

the current practice of third parties collecting personal data implies the risk of security breaches. By utilizing the blockchain third parties can become obsolete, ultimately increasing user’s security.

<https://hackernoon.com/the-product-managers-guide-to-the-blockchain-part-1-fb95dfb7af31> :

Cryptographic proof of identity in simply means *proving* one’s identity without *revealing*it

Blockchains can be used as an exchange network to move value, assets, transactions amongst peers on the network without the need for any 3rd party intermediary to validate or maintain these movements.

smart home appliances that can bid with one another for priority so your laundry machine, dishwasher, thermostat and Roomba all run at an appropriate time while minimizing the cost of electricity against current grid prices

when it comes to cryptocurrency transactions, it’s fair to say that the future is here — but it doesn’t scale very well at this time

Public Blockchain, which ensures anonymity in identity but transparency in transactions. However, maintaining both anonymity and transactional transparency comes at a cost — it lowers the bandwidth between nodes and the entire blockchain must be duplicated by all nodes locally to be aware of the current state of the chain.

Private blockchains if they don’t need or want anonymity of nodes. Private blockchains can be secured by the familiar model of user rights and secrets that we’ve are so comfortable with while still maintaining many kinds of partial guarantees of authenticity and decentralization that blockchains provide. This can work great if the org doesn’t plan on sharing transactions or blockchain writes outside of a closed group, but there is always the chance of that hacker lurking in the wild looking for the weakest link in the chain.

Ethereum blockchain

<https://link.springer.com/chapter/10.1007%2F978-3-319-67816-0_17> :

Proof-of-Stake (PoS) protocols have been actively researched for the past five years. PoS finds direct applicability in open blockchain platforms and has been seen as a strong candidate to replace the largely inefficient Proof of Work mechanism that is currently plugged in most existing open blockchains. Although a number of PoS variants have been proposed, these protocols suffer from a number of security shortcomings; for instance, most existing PoS variants suffer from the nothing at stake and the long range attacks which considerably degrade security in the blockchain

To reach distributed agreement, the blockchain relies on consensus protocols which ensure that all nodes in the network share a consistent view on a common distributed ledger. Most existing blockchain systems rely on Bitcoin’s Proof-of-Work (PoW) to reach network consensus in permission-less systems that do not require the knowledge of nodes’ identities. However, PoW has been often criticized for its huge waste of energy

Unlike PoW, PoS leverages virtual resources such as the stake of a node in order to perform leader election and maintain consensus in the network. Since the mining resources are virtual, PoS-based consensus process is instant and results in negligible costs.

most existing PoS protocols are vulnerable to a number of security threats, such as the nothing at stake and the long-range attacks. The former attack allows the nodes to mine conflicting blocks without risking their stake which increases the number of forks in the system as well as the time to reach consensus in the network. The latter attack (commonly referred to as history attack) consists of an adversary that aims to alter the entire history of the blockchain starting from early blocks (even from the genesis block). This can be achieved when e.g., the attacker acquires the private keys of older accounts which no longer have any stake at the moment, but that have acquired majority stake at previous block height h; the attacker can construct a fork starting from block h leveraging these accounts

Proof-of-Stake (PoS) is a consensus protocol dedicated for open blockchains— which feature open membership allowing any node to join the network. PoS defines a group of validators whose task is to propose the next transaction(s) to be included in the ledger. These proposals are broadcast in the network in the form of blocks. Blocks typically build on each other, thereby forming a chain of blocks—hence the blockchain.

Each validator who finds a PoS solution then includes the solution along with the proposed block as a proof that he is “eligible” to generate the block. Blocks are deemed correct if their proof is correct with respect to all correct transactions that they confirm. If multiple validators find a solution simultaneously, a fork occurs in the block chain.

<http://proquestcombo.safaribooksonline.com/book/networking/security/9781787125445> : slett?

Distributed systems are a computing paradigm whereby two or more nodes work with each other in a coordinated fashion in order to achieve a common outcome and it's modeled in such a way that end users see it as a single logical platform. The main challenge in distributed system design is coordination between nodes and fault tolerance. Even if some of the nodes become faulty or network links break, the distributed system should tolerate this and should continue to work flawlessly in order to achieve the desired result.

Blockchain at its core is a peer-to-peer distributed ledger that is cryptographically secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers.

<https://www.engerati.com/article/blockchain-transactive-grid-set-disrupt-energy-trading-market> :

For owners of solar PV there are few options for trading their excess energy. They may be able to sell it back to their utility and aggregators are emerging who can pull together sufficient load to trade on the wholesale market. Now a new option is emerging, which may enable individuals to trade with their neighbors. And if it takes off in sufficient volume it could present both a new challenge and new opportunity for utilities.

<http://dspace.nbuv.gov.ua/bitstream/handle/123456789/101347/07-Konashevych.pdf?sequence=1> :

As the length of power lines is the main source of energy loss, microgrids technology is focused on local use of renewable sources, as a result there is no need to transport energy over long distances that reduces losses

It is hypothesized that the blockchain technology is the most effective solution for the task of automated (smart) management of interaction within such microgrids, because the blockchain itself was designed to the distributed cooperation of the large quantity of users in a decentralized manner. As a result, there is no need to maintain centralized authorities/corporations or any other relevant intermediaries to manage such grids

The blockchain is the technology which provides chronological records of transactions performed by users of a public network in the database which is cryptographically secured. The copy of such database, which is also called a “ledger” or “cryptoledger”, is stored on each node. Nodes can be freely connected to a public network by any user. The right to make each new record of a portion of done transactions (called “block”) is gained by one of the connected nodes each time when a node solves the mathematical issue. By this algorithm the unpredictability of the node choice is provided. Therefore, it prevents the network from centralization and usurpation of a right to make records. The irreversibility of made records in the ledger is achieved by cryptographic means when each block of data is cryptographically signed by node which gained the right to make a record. Each new block includes the hash sum of the previous block, so any attempt to change a certain data meets the necessity to perform computations on breaking cryptographic code the complexity of which increases in the progression with each new block of data, and that is why is called “blockchain”

The blockchain technology can be used to create an application for managing relations within the microgrid and will perform the following tasks: authentication of smart controllers which register data of produced and consumed electricity and transfer it to the blockchain; each smart controller has its own “wallet”/“address” in the blockchain, which is the open key of a certificate; the private key is the key to access to the wallet; wallet stores information of produced and consumed energy and shows the current stock of energy; wallet allows a participant to make peer-to-peer transaction with other participant of the microgrid; virtual currency provides equivalents of volumes and allows free market prices; free market in the form of stock exchange allows users to make deals on buying-selling electricity directly with each other; deals on market are done in the form of self-executed contracts, also known as “smart contracts”, which provides automatization on accounting and payments; those consumers who consume planned volumes of energy reduce their cost on electricity; and vice versa, those who overconsume the electricity, pay extra money; connection to central grid and reserve stock allows to cover the loss during an emergency and compensate the variability of renewable energy sources.

The original blockchain protocols and other blockchains have no mechanisms for identification and authentication of individuals (but still it has reliable mechanism of anonymous authorization)

https://www.governmentblockchain.org/wp-content/sabai/File/files/ff6fe78d6a47e138f7bc41c2bb824c2b.pdf

In New York state, neighbors are testing their ability to sell solar energy to one another using blockchain technology. In Austria, the country’s largest utility conglomerate, Wien Energie, is taking part in a blockchain trial focused on energy trading with two other utilities. Meanwhile in Germany, the power company Innogy is running a pilot to see if blockchain technology can authenticate and manage the billing process for autonomous electric-vehicle charging stations.

<https://www.sciencedirect.com/science/article/pii/S030626191730805X> :

Microgrids can aid in ensuring this reliable supply. They operate in both grid-connected or island-mode

Local transactions keep profits within the community and encourage reinvestments in additional renewable generation

An information technology that uses vast amounts of energy contradicts the sustainability principles of microgrid energy markets

*A distinctive difference exists between a physical microgrid, which consists of an actual power distribution microgrid, and a virtual microgrid, which simply links the microgrid participants over an information system. Contrary to a physical microgrid, virtual microgrids cannot physically decouple from the superordinate grid*

*A high-performing information system is needed to connect all market participants, provide the market platform, provide market access, and monitor the market operations. every market participant has equal access to avoid discrimination. A blockchain protocol based on smart contracts can meet these requirement*

While data consistency and security are inherent traits of blockchain technology, a secure connection from the market participants’ smart meters, which measure and monitor energy generation and demand, to the blockchain is necessary

If only trusted community members participate in the market, an identity-based consensus mechanism can be sufficiently secure. Identity-based consensus mechanisms are hash-based user authentication mechanisms that rely on every agent having a single identity that is confirmed. It is assumed that no agent can register additional identities. Thus, instead of using computational costly consensus mechanisms relying on complex cryptographic problems to prevent the dissemination of corrupted information, identity mechanisms use the simple, although hashbased, verification of the agent’s identity to prevent corrupted agents from entering the system. In a microgrid market, identities could be verified and assigned by a centralized entity (e.g. government) before providing agents with the required market access. Re-verification by the consensus mechanism then relies on the assigned identities.

<https://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable> :

Let us say that Alice wants to pay Bob for services rendered. Both have bitcoin “wallets”—software which accesses the blockchain rather as a browser accesses the web, but does not identify the user to the system. The transaction starts with Alice’s wallet proposing that the blockchain be changed so as to show Alice’s wallet a little emptier and Bob’s a little fuller.

The network goes through a number of steps to confirm this change. As the proposal propagates over the network the various nodes check, by inspecting the ledger, whether Alice actually has the bitcoin she now wants to spend. If everything looks kosher, specialized nodes called miners will bundle Alice’s proposal with other similarly reputable transactions to create a new block for the blockchain.

That hash is put, along with some other data, into the header of the proposed block. This header then becomes the basis for an exacting mathematical puzzle which involves using the hash function yet again. This puzzle can only be solved by trial and error. Across the network, miners grind through trillions and trillions of possibilities looking for the answer. When a miner finally comes up with a solution other nodes quickly check it (that’s the one-way street again: solving is hard but checking is easy), and each node that confirms the solution updates the blockchain accordingly. The hash of the header becomes the new block’s identifying string, and that block is now part of the ledger.

cap the size of a block at one megabyte, or about 1,400 transactions, it can handle only around seven transactions per second, compared to the 1,736 a second Visa handles in America. Blocks could be made bigger; but bigger blocks would take longer to propagate through the network, worsening the risks of forking.

private chains open only to vetted users. If all the users start off trusted the need for mining and proof-of-work is reduced or eliminated, and a currency attached to the ledger becomes an optional extra.

Ethereum’s distributed ledger can deal with more data than bitcoin’s can. And it comes with a programming language that allows users to write more sophisticated smart contracts, thus creating invoices that pay themselves when a shipment arrives or share certificates which automatically send their owners dividends if profits reach a certain level

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7589035> :

to generate a block, a node collects pending transactions, hash them into a hash of a merkle tree root, then along with other data iteratively hash this data set until it results in a hash that is less than or equal to a predefined target value. Target is a hash value that serves as a threshold, below which a block header must be hashed to generate a block. Target is a 256 bit number with special k numbers of zero significant digits, which constructs PoW difficulty, requires on average 2k attempts before the puzzle is solved. Finding proof for a given target is a linear function, therefore the lower the target value is, more hashing attempts are required

Proof-of-work is a probabilistic iterative procedure, hence to a certain extent decreases a chance to generate blocks at the same time.

A probability of finding nonce of proof H for a given target T is: P(H ≤ T) = T /(2256)

Signed transaction allows other peers to verify that the sender is a person he claims to be and possesses tokens he is willing to transfer

In distributed contracts, the system protects against theft by requiring multiple independent parties to sign a transaction before it can be considered as valid. This is achieved through multi-signature transaction where minimum m of n keys must sign a transaction before tokens can be spend

Energy transaction examples

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6861213&tag=1> :

Current trading of renewable energy without blockchain – pay ahead

NRGcoins directly correlating to energy transferred to grid – pay for use

Calculations for buying and selling energy

First to propose this kind of system?

<https://poseidon01.ssrn.com/delivery.php?ID=999110013020003103085114083065117065028075037051019060102005087028114081006112113101124013053029106045002086125085069024095119007001075005054065117088019016004121065049087103112123091123120121078092006019000066109125016020090087075124071016031085078&EXT=pdf>

Flaws in proof-of-stake

<https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/> :

Public blockchains: a public blockchain is a blockchain that anyone in the world can read, anyone in the world can send transactions to and expect to see them included if they are valid, and anyone in the world can participate in the consensus process – the process for determining what blocks get added to the chain and what the current state is. Public blockchains are secured by cryptoeconomics – the combination of economic incentives and cryptographic verification using mechanisms such as proof of work or proof of stake, following a general principle that the degree to which someone can have an influence in the consensus process is proportional to the quantity of economic resources that they can bring to bear. These blockchains are generally considered to be “fully decentralized”.

Consortium blockchains: a consortium blockchain is a blockchain where the consensus process is controlled by a pre-selected set of nodes; for example, one might imagine a consortium of 15 financial institutions, each of which operates a node and of which 10 must sign every block in order for the block to be valid. The right to read the blockchain may be public, or restricted to the participants, and there are also hybrid routes such as the root hashes of the blocks being public together with an API that allows members of the public to make a limited number of queries and get back cryptographic proofs of some parts of the blockchain state. These blockchains may be considered “partially decentralized”.

Fully private blockchains: a fully private blockchain is a blockchain where write permissions are kept centralized to one organization. Read permissions may be public or restricted to an arbitrary extent. Likely applications include database management, auditing, etc. internal to a single company, and so public readability may not be necessary in many cases at all, though in other cases public auditability is desired.

little emphasis on the distinction between consortium blockchains and fully private blockchains, although it is important: the former provides a hybrid between the “low-trust” provided by public blockchains and the “single highly-trusted entity” model of private blockchains, whereas the latter can be more accurately described as a traditional centralized system with a degree of cryptographic auditability attached.

the fundamental value of blockchains in a fully private context, aside from the replicated state machine functionality, is cryptographic authentication, and there is no reason to believe that the optimal format of such authentication provision should consist of a series of hash-linked data packets containing Merkle tree roots; generalized zero knowledge proof technology provides a much broader array of exciting possibilities about the kinds of cryptographic assurances that applications can provide their users. In general, I would even argue that generalized zero-knowledge-proofs are, in the corporate financial world, greatly underhyped compared to private blockchains.

Private advantages: possible to change rules and revert transactions, known validators – no risk of 51% attack, cheaper transactions, easier consensus algorithms leading to shorter block times, restricted read permissions lead to greater privacy

Public advantages: protect users from developers, reduces the problem of who transmits first

<https://perfectial.com/blog/leveraging-private-blockchains-improve-efficiency-streamline-business-processes/> :

Public: everyone, pow and pos, transparency and anonymity

Consortium and private: do not expose transaction records to whole world, managed more efficiently by a limited number of nodes

Private advantages: no single point of failure, members only, no native cryptocurrencies, secure with no anonymity, cheaper without or limited transaction fees since only a few nodes validating blocks, abide regulations to avoid criminal purposes

<https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2662660> :

Transactions initiated by future owner sending public key to current owner, then transferring coins etc. by digital signature of hash – identity free

Jeremy Allaire (2015; cited by Byrne, 2015, emphasis added), [It is often heard that] the blockchain’s interesting but the “currency” or the store of value’s not very interesting. That’s just a fallacy. They’re not possible separately. There has to be an underlying value to the token that’s used to move value, and there has to be an incentive system for the creation of that token and the exchange of that token. That is the only way these systems work… that’s a thing I think a lot of people fail to understand.

value containers (or tokens) and currencies are thus not synonymous

<https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/> :

blockchains are not necessary; **they are convenient**. They are simply marginally better than the next available tool for the job. And yet, because these applications are much more mainstream, and can benefit hundreds of millions of users, the total gain to society (which can be seen from the area on the above chart) is much larger.

Now, why are blockchains useful? To summarize:

* You can store data on them and that data is guaranteed to have a very high degree of availability
* You can run applications on them and be guaranteed an extremely high uptime
* You can run applications on them, and be guaranteed an extremely high uptime **going very far into the future**
* You can run applications on them, and convince your users that the application’s logic is honest and is doing what you are advertising that it does
* You can run applications on them, and convince your users that your application will remain working *even if* you lose interest in maintaining it, you are bribed or threatened to manipulate the application state in some way, or you acquire a profit motive to manipulate the application state in some way
* You can run applications on them, and give yourself the backdoor key if it is absolutely necessary, BUT put “constitutional” limitations on your use of the key – for example, requiring a software update to pass through a public one-month waiting period before it can be introduced, or at the very least immediately notifying users of application updates
* You can run applications on them, and give a backdoor key to a particular governance algorithm (eg. voting, [futarchy](https://blog.ethereum.org/2014/08/21/introduction-futarchy/), some complicated multicameral parliament architecture), and convince your users that the particular governance algorithm in question is actually in control of the application
* You can run applications on them, and those applications can **talk to each other with 100% reliability** – even if the underlying platform has only 99.999% reliability
* Multiple users or companies can run applications on them, and those applications can interact with each other at extremely high speed without requiring any network messages, while at the same time ensuring that each company has total control over its own application
* You can build applications that very easily and efficiently take advantage of the data produced by other applications (eg. combining payments and reputation systems is perhaps the largest gain here)

Importance/problems with public/private key identity

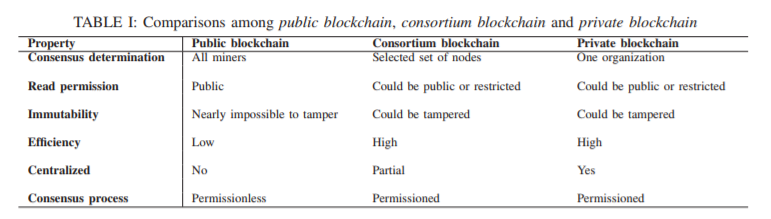
in practice most people are not well-equipped to securely store multiple keys, and there are always going to be mishaps, and often centralized services play an important role: helping people get their accounts back in the event of a mistake. In this case, the blockchain-based solution is simple: social M-of-N backup.

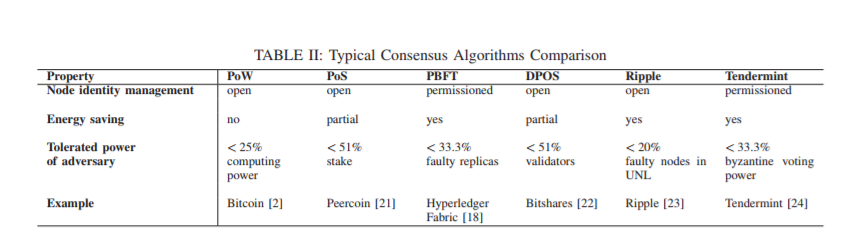
You pick eight entities; they may be your friends, your employer, some corporation, nonprofit or even in the future a government, and if anything goes wrong a combination of five of them can recover your key. This concept of social multi-signature backup is perhaps one of the most powerful mechanisms to use in any kind of decentralized system design, and provides a very high amount of security very cheaply and without relying on centralized trust

many things function very well in a centralized manner and could be upgrade just adding a cryptography layer, blockchains in many cases become meaningless because at the very end 1) what is the incentive to maintain the blockchain 2) If there are no truly distributed network of peers then again is a centralized thing at expenses of a government, enterprise or charity foundation.  (comments)

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8029379> - Bra

Architect overview, consensus algorithms and applications





PBFT and Tendermint are permissioned protocols. Node identities are expected to be known to the whole network, so they might be used in commercial mode rather than public

Each node has to store all transactions to validate them on the blockchain because they have to check if the source of the current transaction is unspent or not. Besides, due to the original restriction of block size and the time interval used to generate a new block, the Bitcoin blockchain can only process nearly 7 transactions per second, which cannot fulfill the requirement of processing millions of transactions in real-time fashion. Meanwhile, as the capacity of blocks is very small, many small transactions might be delayed since miners prefer those transactions with high transaction fee

blockchain cannot guarantee the transactional privacy since the values of all transactions and balances for each public key are publicly visible. Besides, the recent study [41] has shown that a user’s Bitcoin transactions can be linked to reveal user’s information. Moreover, Biryukov et al. [11] presented a method to link user pseudonyms to IP addresses even when users are behind Network Address Translation (NAT) or firewall

In Zerocoin [46], zero-knowledge proof is used. Miners do not have to validate a transaction with digital signature but to validate coins belong to a list of valid coins. Payment’s origin are unlinked from transactions to prevent transaction graph analyses. But it still reveals payments’ destination and amounts. Zerocash [47] was proposed to address this problem. In Zerocash, zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKs) is leveraged. Transaction amounts and the values of coins held by users are hidden

Selfish mining and stubborn mining