Tow Center for
Digital Journalism
A Tow/Knight Report

BLOCKCHAIN IN JOURNALISM

BERNAT IVANCSICS

Columbia Journalism School

Funded by the John S. and James L. Knight Foundation.

Table of Contents

Executive Summary

Blockchain, like the internet, or democracy, or money, is many overlapping things. It is a decentralized record of cryptocurrency transactions. It is a peer-to-peer network of computers. It is an immutable, add-on-only database. What gets confusing is the way in which these overlapping functions override one definition or explanation of blockchain, only to replace it with an altogether different one. The conceptual overlaps are like glass lenses dropped on top of one another, scratching each other's surface and confusing each other's focal dimensions.

This guide takes apart the stack of these conceptual lenses and addresses them one by one through the reconstruction of the basic elements of blockchain technology. The first section of this report gives a short history of blockchain, then describes its main functionality, distinguishing between private and public blockchains. Next, the guide breaks down the components and inner workings of a block and the blockchain. The following section focuses on blockchain's journalistic applications, specifically by differentiating between targeted solutions that use blockchain to store important metadata journalists and media companies use on a daily basis, and hybrid solutions that include targeted solutions but introduce cryptocurrency, therein changing the journalistic business model altogether. Finally, the report speculates on the proliferation of what are known as Proof-of-Stake blockchain models, the spread of "smart contracts," and the potential of enterprise-level and government-deployed blockchains, all in relation to what these mean to newsrooms and the work of reporters.

Key findings

For media organizations, the use cases of blockchain can be grouped into three key areas:

1. Auditable (and officially verifiable) database solutions for editorial and advertising
2. Cryptocurrency-based business models
3. Access to public data secured in blockchain-based file systems

As an aid to editorial work, blockchains can serve as secure registries for important metadata, such as a story's time of publication, bylines, tags, and so forth. As a tool for sales teams, blockchain-based registries can rank and filter trusted advertisers and ad content, and become an alternative to the often inscrutable auction-mechanism of digital ad exchanges. These database solutions may become essential in the journalism industry for building trust among media organizations, and between the media and the public. Storing and auditing data on the origin of stories, or filtering harmful advertising spam, are just two immediate and actionable examples supported by the properties of blockchains.

Additionally, cryptocurrencies can be used to reward reporters, contributors, or even readers for completing specific tasks. For reporters, freelancers, and contributors, tokens can be used as a flexible component of their compensation package, similar to stock options in many sectors. For readers specifically, subscriber accounts can be credited tokens for approving ads that readers wish to see—thus signaling to publishers what ad vendors they should favor—or even for tipping journalists.

The security of token transactions are granted by decentralized and immutable blockchains. With cryptoeconomics, however, the success of blockchains depends on the overall usability of a business model where the valuation of tokens—as well as their means of distribution—is determined by a collective of stakeholders; in this case, those stakeholders could include reporters, editors, freelancers, or audience members. In other words, cryptoeconomics requires the radical restructuring of traditional news business models.

Finally, with the rise of government-deployed blockchains that secure citizens' public data, distributed file systems and smart contracts that rely on rules codified in computer code to automate processes like closing contracts, settling claims, notarizing documents, and recording deeds will reconfigure data access for investigative journalists. Instead of public records request, journalists might be confronted with blockchain-based smart contracts that provide and restrict access to government files. While such an infrastructure might be more efficient, it may also be more expensive. Also notable for journalists is that metadata for any submitted request for information would be logged immutably on the blockchain and publicly accessible to anyone looking. This is a scenario still very much in the future, but one journalists will have to reckon with as it changes the infrastructure of public records.

Introduction: The Difficulty of a Definition

What is it that's so elusive about blockchain? Why do people's eyes glaze over as soon as the increasingly familiar jargon is thrown around in densely phrased, for-dummies guides and tech talks? "Decentralized," "trustless network,"[1] "distributed ledger," "proof of work," "cryptographic hash" . . . the list goes on. Why are elevator pitches on blockchain so vague, and detailed explanations so confusing?[2]

Part of the answer is that blockchain is a mixture of technologies,[3] and it also can be used for different purposes. As a result, when it comes to explaining what blockchain is, it sounds a lot like the parable of the blind men and the elephant: with each man describing an important part of the whole, yet missing the bigger, more coherent picture.

To put it plainly, blockchain is a technology to store data securely. Bits of data is packed into small "blocks" and strung up into a "chain" so that the strict order of blocks allows users to see how the data was recorded and whether someone attempted to rearrange or substitute blocks in the chain. In abstract, blockchain technology is a sophisticated way to reimpose irreversibility and stability in our digital lives where data is produced, exchanged, and analyzed continuously.

---

[1] Gili Vidan and Vili Lehdonvirta, "Mine the Gap: Bitcoin and the Maintenance of Trustlessness," *New Media & Society* 21, no. 1 (July 2019): 42–59, https://doi.org/10.1177/1461444818786220.
[2] Adrianne Jeffries, "'Blockchain' Is Meaningless," The Verge, March 7, 2018, https://www.theverge.com/2018/3/7/17091766/blockchain-bitcoin-ethereum-cryptocurrency-meaning.
[3] Arvind Narayanan and Jeremy Clark, "Bitcoin's Academic Pedigree: The Concept of Cryptocurrencies Is Built from Forgotten Ideas in Research Literature." *ACM Queue* 15, no 4. (2017): 1–30, https://queue.acm.org/detail.cfm?id=3136559.

People can't tolerate a world without the rule of law for too long, so public and private organizations, including governments, municipalities, banks, retail and media companies, build closed systems in which they can offer their services. The price paid for security and stability among these services is often that a single entity administers them—in many cases failing to do so efficiently or fairly, or exploiting its customers or citizens in the process.[4]

In contrast, blockchain can act as a new "social contract,"[5] wherein citizens do not defer authority to a single governing entity, but instead to each other. With shared or "distributed" agency, participants in a blockchain network can perform various computational tasks, such as storing records or running applications that send money or retrieve those digital records.

What follows in this guide addresses most of blockchain's functionalities, and describes the technology's nuts and bolts in detail. It then analyzes blockchain's application in newsrooms by editors, reporters, sales teams, and product developers. While the applicability and efficiency of blockchain in journalism is still in its experimental phase,[6] notable trends and use-case scenarios are being developed. At present, the case for blockchain applications in journalism has distinctive advantages and drawbacks.[7] This overview aims to begin a productive conversation around blockchain while acknowledging the premise that, like every newly deployed "solution," applications are still very much in flux.

[4] "The Promise of the Blockchain Technology," *The Economist*, September 1, 2018, https://www.economist.com/technology-quarterly/2018/09/01/the-promise-of-the-blockchain-technology?.
[5] Wessel Reijers, Fiachra O'Brolchain, and Paul Haynes, "Governance in Blockchain Technologies & Social Contract Theories," *Ledger* 1, no. 1 (2016).
[6] Paul Ford, "Bitcoin Is Ridiculous. Blockchain Is Dangerous," *Bloomberg Businessweek*, March 9, 2018, https://www.bloomberg.com/news/features/2018-03-09/bitcoin-is-ridiculous-blockchain-is-dangerous-paul-ford.
[7] Lloyd Armbrust, "Bitpress: An Open Protocol for Tracking the Credibility of News," Medium, May 16, 2018, https://medium.com/bitpress/bitpress-an-open-protocol-for-tracking-the-credibility-of-news-2f8c961cd67c.

What Is Blockchain?

Background

To most of the public, blockchain is associated with cryptocurrencies such as Bitcoin, Ether, or many other virtual "coins." The reason for the strong connection between digital money and blockchain is that computer-based currencies are where the design principle of blockchain is still most commonly found today. It's what made blockchains famous in the first place.

When Bitcoin popularized blockchain in 2009, following the publication of a white paper authored by the pseudonymous Satoshi Nakamoto,[8] computer scientists and cryptographers had already thought about much of blockchain's underlying technology, mostly in academic circles.[9] For instance, in an effort to develop tools to combat email spam and securely send payments online, computer scientists had looked into cryptography and secure transmission protocols. The use of cryptography to generate public and private keys, or the specific algorithms that create long numerical codes (hashes), emerged during this phase of research. In blockchain technologies today, these same design principles have now gained a wider field of application.

Nakamoto's explosive paper on the proposal for Bitcoin can be seen as the repurposing of many different solutions and technologies published at the right time. The idea of a peer-reviewed and mathematically robust payment system hit a nerve for many, arguably because of the global fallout from the Great Recession. As major financial institutions went bankrupt and caused a global bank run, the silver bullet of a mysterious technology solving at least some of the world's financial problems sounded curious and inviting.

---

[8] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," bitcoin.org, 2008, https://bitcoin.org/en/bitcoin-paper.

[9] Narayanan and Clark, "Bitcoin's Academic Pedigree."

Blockchain was first popularized as a bank-less, cheap, and secure way to pay for things, creating value for digital currencies by recording transactions as secure and immutable. The core underlying value of cryptocurrencies is the trust of its users that it will be accepted as a form of payment—just like in the case of national currencies around the world—and that, due to blockchain's technological properties, it cannot be faked or hacked.

More recently, however, other industries have begun experimenting with blockchain's design principle for applications beyond digital money. The broader media industry, which includes journalism, digital advertising, audience analysis, music, et ak., is just one of many.

The purpose of blockchain

Generally speaking, blockchains are meant to do three things:

- **store** (small amounts of) data (in containers called "blocks");
- **keep track** of all modifications made to the data (by threading them into a "chain" that cannot be altered); and
- **secure** the data and its many edited versions in a way that multiple users can agree on, including how data is stored, protected, and remains unchanged. This is where cryptography, proof-of-work, and community consensus come in.

In most blockchain examples, a fourth component is also included: the **incentive** to participate in the network of people who store, keep track of, and secure data. Incentives motivate miners to create and validate blocks in the blockchain, or nudge stakeholders to police and regulate a blockchain. (More on miners and stakeholders later.)

The most popular terms used by blockchain explanations are decentralized, immutable, transparent, distributed (ledger), and trustless networks. Most of these descriptions refer to the same basic idea: let there be a record of stuff (data) that people can agree on

and not change in the future, and secure that stuff so that all its history is constantly visible to everyone. In the world of blockchain, trust and memory are built block by block.

Things stored by a blockchain

For the most famous examples (think Bitcoin), the record of stuff is a list of transactions (the so-called "ledger" used in banks). But stuff (data) can be a lot of things. It can be:

- a **timestamp** for documents published or released into the public;
- a **list** or rank of things put together by people who have a stake in how those things are listed and ranked;
- an algorithmically automated **contract** between a lawyer and a client, or an editor and a freelancer;
- or even the **source code** for an app with instructions from the original developer on how to use and further develop that code. And so forth.

A special type of record

Blockchain becomes useful when the data is used or recorded by a lot of people simultaneously, who also want to keep track of and secure all the edits made to the data without having a central database or authority (like a bank in finance, a publisher in the book or journalism industries, or a single tech company in the advertising industry) do the storing, securing, and tracking all by itself.

A recurring pattern in the examples given above is the presence of people who produce and use the data in blockchains simultaneously and collaboratively.

Thus blockchain has two main ingredients: **computers** and **people**.

Computers store and secure stuff, and people make decisions about the way that stuff is stored and secured. More specifically, people make the decision when to create a new block, and how to link it to the previous block. The cooperation of computers and the

people who work on the blockchain to create blocks of data and secure them is crucial because avoiding a central authority comes with the tradeoff of constant cooperation and negotiation. If a lot of data has to be recorded and modified within a split second, and if—for obvious reasons—nobody wants someone to modify part of the record without being approved by everyone else, the most important thing is the validity of the record: that it remains immutable forever.

Forks in time

So far the way of storing data, as described above, can still resemble a special kind of Wikipedia: many people edit a single database, and all edits are tracked. What sets blockchains apart from a Wiki page or a Google Doc is, first, that once a new chunk of data (block) is added to the database, it cannot be edited, and second, that everyone in the blockchain network keeps a copy of the entire blockchain for themselves. There is no centralized, shared database, and edits can't be tracked by clicking on an "Edit history" button. Instead of rewriting the same page or database, blockchain is cumulative, or in other words, append-only. It's not a palimpsest; it's more like a lot of pages stacked on top of each other in a fixed order. Only a single—final—version of it exists (with a copy on everyone's computer that's very frequently updated).

To illuminate this idiosyncratic characteristic of blockchain, we must understand why blocks are important. Beyond computers and people, another thing to take into account is **time**. Time is essential to blockchain because in order for people to agree on which kind of data they want to store in what way, all of the participants need to have access to the same data at the same time. If the same copy of the data is floating around on the computers of hundreds and thousands of people, it can get difficult to decide which version of the data will be recorded, especially if that data is growing in real time.

What's more, in most blockchain applications such as Bitcoin not all computers in the network are required to have every piece of data simultaneously at any given time. Instead, if a certain number of computers ("nodes" in the network) have enough data to create a new block, they can propose what the next block should be by creating that

block, encrypting it (more on this later), and adding it to the chain. The "proposal," in fact, is more like a competition.[10]

Occasionally multiple blocks are added to the chain simultaneously, and forks appear in the chain. When a fork happens, new branches of the chain sprout from the main trunk. Eventually, however, the community of computers (once again, the nodes in the network) decide which proposed new block or set of blocks they wish to validate, and the chain continues to be built without digressions.

The decision to choose one path over the other is based on how securely the blocks are encrypted. This is why usually the longest chain wins, since each new block makes it more difficult to alter something earlier in the chain. If a block back in the chain is altered, every block after it needs to be rewritten and revalidated. The sequence of blocks is more organic than what the term "chain" might suggest. Blockchain is more like a tree than a chain: a slice of the trunk or the branch cannot be cut out and replaced by a new slice. Instead, the whole new trunk or branch needs to be grown.

If the data is money, participants will want to make sure that transactions are not recorded twice (double spending the same money!). If the data is a timestamp of when a digital ad appeared on a website for customers, it shouldn't be overwritten by another timestamp of the same ad appearing on a different website. If the data is a list of items gathered by users for ranking or categorization, there should be a consensus around which is the final version of the list.

In short, data is never static in databases—it grows and is modified constantly. Blockchain is a solution in which anyone can create little snapshots of the data, store these snapshots as blocks, and agree with other people in the community that there is only one single collection of snapshots (the chain of blocks) that will tell the true story. To solve these problems in practice, blockchain uses cryptography and community consensus to establish a single stable public record of data.

---

[10] Taylor Pearson, "How Does Blockchain Technology Work?" Medium, July 18, 2018, https://hackernoon.com/how-does-blockchain-technology-work-ceeeee47eaba.

Private and public blockchains

So far we have described blockchains as a special kind of public database, potentially used by anyone who has a computer in the network. This is true of **public blockchains**, which are the most notable ones today and include Bitcoin, Ethereum, and a lot of other mostly currency-producing blockchains. By extension, **private blockchains** restrict who can join the network of computers and who can participate in the consensus-driven act of validating a new block. This guide tackles this distinction below, under the description of the Proof-of-Work and Proof-of-Stake models.

For now, what may be worth remembering is that a fully public network will diminish trust—since any kind of computer, even a hacker's, can participate in the network and potentially commit fraud. More computing power and more effort to maintain cryptographic security are required to secure public blockchains. In a private network, the community can check on one another by requiring participants to hold a stake in the network—to store the entire publicly accessible ledger on their computer and keep it updated—and can establish rules. For the violation of those rules, bad actors can be kicked out of the network. Participants can even write and ratify a constitution of rules to set the guidelines.

To put it differently, in private blockchains the level of trust is increased but the network is more closed. By contrast, public blockchains accommodate all kinds of actors but the price for participation is the computing power (in the form of high-end computer CPUs, time, and electricity) of each node that it needs to perform.

As we will see, journalistic applications of blockchain tend to favor constitution-driven, private networks with agreed-on community guidelines. They do so to minimize required computing power for validating blocks and increase trust in a community where stakeholders know each other and have the power to police the actions of others.

Blockchain Basics

The blocks that contain data have a uniform structure across almost all blockchain applications.

The block

Each block consists of a:

- **version number** (to mark the position it occupies in the chain)
- **header hash** (a number code that links it to the previous block's output hash)
- **timestamp** (the time when the block was created)
- **Merkle root** (the block's content encoded into a hash, which is a number code, as mentioned above)
- **nonce** (a random number used to randomize and create the output hash of the block, which will then link it to the next block and thus lock the block into its place within the chain)
- **output hash** (the version number, the header hash, the time stamp, the Merkle root, and the nonce ALL encoded into yet another single code number).

There are also some other universal characteristics of blocks.[11] Blocks are usually a couple of megabytes in size since they merely consist of strings of numbers (hash outputs). In most blockchains, each block is accessible to anyone with a computer and an internet connection. Entire blockchains can be downloaded to a personal computer (e.g., the entire history of Bitcoin transactions is now reaching 200 gigabytes, although it used to be only a few gigabytes just a few years ago).

[11] Michael Noferl, Peter Gomber, Oliver Hinz, and Dirk Schiereck, "Blockchain," *Business & Information Systems Engineering* 59, no. 3 (June 2017): 183–187, https://doi.org/10.1007/s12599-017-0467-3.

Blocks are transparent, although meaningless to the human eye with their long lines of numbers and letters. Once opened, all hashes (the large, mostly 32- to 64-digit numbers and letters) can be seen. The point of blockchain is that even if somebody wants to change something in a block by rewriting a couple of characters in the content of any block, the entire chain following that block will be modified. This is practically a domino effect, because the following blocks are encoded based on the data found in the previous blocks.

Since the community-approved chain of blocks is always stored on many computers in the network, it can be restored easily. The earlier the block is in a chain, the more difficult it is to alter because more and more blocks after it would need to be adjusted. In practice, changing a single block only one position removed from the "freshest" block cannot be done without being detected by a lot of nodes in the network.

Hashing

Perhaps the most widespread tool in digital cryptography today is the hashing algorithm. It is based on the principle of creating long numeric codes of fixed length from any kind of input data: a word, a number, a sentence, or an entire text. For the human eye, the process of hashing looks as if a perfectly normal sentence or number entered the hashing algorithm, and a split second later, long and scrambled sequences of numbers and letters emerged. These "hashes" are very difficult to guess, but very easy to verify by a computer if the input data from which the numeric code was created is known.

In computer science, the difficulty of guessing a specific hash for given input data is called collision resistance. To avoid a collision—getting the same hash for distinct input data—the hashing algorithm has to be designed in a way as to produce extremely random hash outputs. The cryptographic hashing algorithms used in blockchains are like that: random, easily generated by hashing algorithms, and reversible if the original data is known, but difficult to decode without it.

Hashing is the computer's way to understand data. There are many ways data that is intelligible for humans can be turned into a computer-readable code, but the design principle is simple: input data is paired with a numerical code, like a personal name is paired with a telephone number. The way a computer connects the two is through hashing, so that it understands this data pair and can retrieve it easily if a user wants to access it.

In blockchains, the data contained in each block is hashed, which means that sentences, words, dates, or numbers that make sense to humans are run through the hashing algorithm. Hashing algorithms do a series of predetermined mathematical calculations to create a code for any kind of data. Once again, hashing still looks as if numbers or texts were scrambled to produce an unintelligible code.

But computers can quickly reverse their calculations and produce the input data, which humans can read or understand again, if the computer is told what the input data was. In practice, these algorithms accept any kind of information, and produce a number of fixed length, such as 32 or 64 digits. Hash outputs often look like a long line of both numbers and letters since most popular hashing algorithms encode hexadecimally, meaning that each "digit" can contain 16 characters: the numbers 0 to 9 and the letters A to F—10 numbers and six letters altogether.

For cryptographic purposes, specific hashing algorithms are useful because the way they scramble any kind of input into a finite set of numbers is very random. So random that if the input data is unknown, someone would need to try all possible hash combinations to come up with the input string. Even on the fastest computers, testing all combinations would require tens of thousands of years.

The output (or, in the jargon of cryptography, the digest or the hash) is independent of the input's length. A single exclamation mark will produce a hash of the same length as the hash produced from an entire novel. More interestingly, if a single exclamation mark is deleted from the text of said novel, the hashing algorithm will create a totally different number for its digest.

But randomization only works one way: while the digest that's being produced is random, the same input will always produce the same digest. Computer scientists call this one-way nature of hashing deterministic. There is no way to piece together hash outputs, like finding what the recurring hash output for the number 9 is and trying to locate it in the long numerical hash that's produced for the number 19: the two outputs will be totally different, and the output code of 19 may actually resemble the hash output of our novel in the previous example.

In blockchains, blocks don't actually contain humanly legible numbers or texts, but instead carry pairs of hash outputs. Every item in a list, every transaction, or every chunk of data in the block is made into a hash, and the resulting hashes are paired randomly to become the input data for a single new hash. Once every piece of data in the block is hashed, and all the hashes are hashed with each other again and again, a single final hash is created. This final hash is called the Merkle root, named after the mathematician Ralph Merkle who patented this way of multi-layered and secure way of storing data.

The "root" comes from the tree-structure of the way hashes are attached to each other: hashes are like leaves that are joined together in pairs on a branch (which is the next hash), and branches are joined together in the root of the tree (the final hash). Storing data in such a hierarchical way within each block is useful because every bit of data becomes deterministic. Each brick in the one-brick-per-level Jenga is itself made up of a smaller bricks supporting each other. When one brick is removed or changed, everything above it—within the block and following the block—collapses.

Adding a new block to the chain

So far we have discussed what is stored in a single block, and how things are stored in it. The final computational ingredient of the blockchain is the link that threads blocks into a chain. As mentioned previously, the main component of that thread is the block hash, which is the hash output of the version number, the Merkle root, the timestamp, the

header hash (the previous block's output hash), and the nonce. All of these numbers are scrambled together by the hashing algorithm to produce the block hash, which the next block will contain as its header hash.

But which block hash will be agreed on? Nodes in the network are still competing to have their new bundle of data (the block) added to the chain. So who decides which block gets added? This is where the mysterious number, the **"**nonce,**"** comes into play. The "n(umber only used)once" is a random number, and is generally shorter than the hash number. Since it is mixed in with the Merkle root, the version number, and all the other numbers contained in the block, it determines the final block hash.

If the nonce changes, so does the block hash. When miners in the blockchain network try to find the final hash for a block and get it approved by their peers in the network, they try millions of variations of the nonce to find that final hash. Since the nonce is random, it cannot be derived from any other data encoded in the block, and that is the point. Mixing this random element into blocks requires the competing computers to always recalculate the output hash when creating a new block.

There is a final twist to producing a new block, however. In order to avoid calculating trillions of versions of the output hash (which would take thousands of years) to find a specific one, the blockchain protocol is designed to make miners find any random hash that is smaller than a target number. This seemingly simple technical solution was Bitcoin's innovative idea, so as to make block validation less time-consuming, more competitive, and financially rewarding.[12]

Smaller hashes can be identified with the human eye if the hash begins with lots of zeroes. The more zeroes there are, the smaller the hash, like 0010 is smaller than 1000, except hashes are fixed-length and even their zero digits are required to be spelled out. Miners have to find a random hash that is smaller than the target number. That is, the hash they find must contain more zeros than the target number. To find this sufficiently small number, which will then become the block hash, miners iterate

[12] Michele D'Aliessi, "How Does the Blockchain Work?" Medium, June 1, 2016, https://medium.com/s/story/how-does-the-blockchain-work-98c8cd01d2ae.

through millions of nonces. They try as many nonces as required to catch the first hash that's lower than the target number. In practice, they don't look for a specific hash, only a good-enough hash.

The target number is arbitrarily determined by the blockchain network's protocol. "Protocol" here simply means the software that each computer in the blockchain network has to run in order to get access to the network. The protocol, like *http* for web browsers, determines how computers connect to each other and how they can validate blocks. Http for the internet determines how personal computers can communicate over the web with servers and gain access to websites. Protocols for blockchains are usually open source but proprietary; Bitcoin and Ethereum have separate protocols written in different programming languages.

In Bitcoin the target number is adjusted depending on how many computers there are in the network. If there are more computers, they will likely find an acceptably low random hash faster, so the target is lower and thus the difficulty level is increased. We see here how the protocols of the community are working behind the scenes: all the computation and technical competition would be meaningless without agreed-on rules and guidelines, such as what the target number (and hence: the difficulty) are.

Also, if two computers come up with good-enough hashes at almost the same time, and try to add their block to the chain, the blockchain community will still double-check who has the lowest hash number (which is a proxy for how many nonces the computer tried to plug in to find the good-enough hash, and how much work it has invested in making the new block), and will accept that block at the expense of the other—competing—block.

Note, however, that by lowering the value of the target number, the blockchain network doesn't reduce the number of possible solutions a computer must try. It merely reduces the number of acceptable solutions from trillions and trillions (this is why the difficulty rises by lowering the target number). Since nodes are not required to find a specific hash (they don't have to decode a hash to find the input string), they

merely have to find a hash that's within the limits of the target number by inserting a new nonce every single time they try to find the new block hash.

This is still time and energy consuming, but manageable for powerful computers that are able to try many variations very fast. Blockchain protocols usually adjust the target level based on the level of competition among nodes to evenly pace out hash-solutions in the network. In the Bitcoin network today, a new block is created every 10 minutes on average.

Proof-of-Work, Proof-of-Stake

Blocks require a lot of computational trials and errors to achieve an appropriately complex block hash. The time and energy consumption of computers to mine each new block is the proof that participants in the network invested work into maintaining the system. The original Bitcoin manifesto by Satoshi Nakamoto called this the "one-CPU-one-vote" model.[13] In cryptocurrency applications, the work of miners, which is purely based on computers' CPU output, is rewarded by gaining money in the form of digital tokens, such as Bitcoin or Ether. Even if two nodes find a good nonce for the block hash at about the same time, the winning block will be the one that required even a little bit more CPU output.

This model is the **Proof-of-Work** scenario.[14] The security and integrity of the blockchain is undergirded by a vast army of computers that encrypt huge amounts of data, and keep track of every new piece of data added to the chain. Constant and automatic surveillance of the network is required since hackers may want to alter parts of the blockchain in order to record fake transactions that would add digital money to their digital wallets. As we have seen, however, even modifying a single character in a single block's single hash will trigger the Merkle root to change, and along with it the

[13] Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System."
[14] Blockgeeks, "Proof of Work vs. Proof of Stake: Basic Mining Guide," Blockgeeks Guide, 2016, https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/.

entire block's output hash, and consequently the next block's header hash, as well as the next one's, and so forth.

To revalidate each subsequent block in order to hide someone's tampering would require the recalculation of each block's nonce to find new output hashes to relink them to subsequent blocks. This would take hours of work during which most of the network would realize what is happening, and prompt them to intervene. These nodes have the correct and approved blockchain locally on their computers, and can restore it and double-check it with other nodes.

The value of the tokens awarded to miners is, of course, dependant on the exchange rate between tokens and "real" currencies. The economy of blockchain-based tokens depends on a variety of human factors, such as trust in the network, media attention, the threat of regulation, market panic, and so on. Like stocks and currencies, the monetary value of tokens fluctuate based on token holders' trust.

Moreover, the infrastructural environment of mining new tokens have changed dramatically. Today miners often coalesce into pools to perform computational tasks together and then share token rewards among themselves. Computer processing units specifically designed to efficiently run hashing algorithms are also available on the market. These are called ASICs, or application-specific integrated circuits. All this is to say that while mining cryptocurrencies might have been tenable as a hobby a decade ago, with fewer computers in the network and a lower difficulty rate, today the ecosystem of mining pools means that only a handful of pool managers control all miners.[15]

These managers often enter into artificial agreements with each other to avoid pool centralization where one pool amasses over 50 percent of the CPU power of the entire network, thereby compromising the integrity of the blockchain. If more than half of the network nodes are utilized to validate the same block, they become capable of what is known as the "51-percent attack," when there are more computers to retroactively

[15] G. Andresen, "Centralized Mining," The Bitcoin Foundation, 2014, https://bitcoinfoundation.org/centralized-mining/.

amend the blockchain and validate the revision than there are peers to reverse those edits. In short, while centralization is exactly what blockchain networks intended to avoid, the current physical infrastructure of popular blockchains, like Bitcoin, is centralizing at an alarming rate.

Partly to counter the design flaws of Proof-of-Work blockchains, an alternative to PW has emerged in the form of the **Proof-of-Stake** model.[16] Peercoin was the first popular cryptocurrency to use PS as its main regulating principle, and Ethereum is following suit. Instead of requiring computers to race against each other and guess the nonce to create a block hash, a single computer within the network is selected to validate a new block. The node is selected based on its stake in the network, which can be the amount of cryptocurrency it holds. It is assumed that if someone holds more money in a given cryptocurrency, the more stake they will possess—and wager—to responsibly validate a new block. The validator essentially bets their own money to validate a new block, and receives all the transaction fees from the block they were able to validate.

Other nodes in the network trust the validator node based on how much stake this node has in invested cryptocurrency. In PS, no new coins are mined, and instead validators receive monetary reward in the form of transaction fees (this is the incentive to become a validator). Validators are selected from a pool of applicants after they are vetted and inducted into the applicant pool.

In contrast to the PS system, the benefits of PW is the network effect of peer-to-peer trustlessness, which keeps everyone on their toes to monitor if someone wants to hack the blockchain. Its drawbacks are: wasteful energy consumption and the anonymity of participants. Distrust is ingrained in the design principle of blockchain so that participant nodes stay alert and keep each other in check.

Conversely, the benefit of PS is the trust and transparency of the vetted community of peers, but the drawback is that arbitrariness is introduced into the system. Someone has

---

[16] Robert Greenfield IV, "Explaining How Proof of Stake, Proof of Work, Hashing and Blockchain Work Together," Medium, July 20, 2017, https://medium.com/@robertgreenfieldiv/explaining-proof-of-stake-f1eae6feb26f.

to create a protocol by which validator applicants are selected, and more human governance is required to rein in fraudulent actors. To gain stake in the network, a potential new actor must invest capital through the purchase of coins, which in turn may create inequality in the system right from the beginning.

Even if the amount of coins that can be acquired is capped, and even if token transactions are heavily governed to avoid liquidity, resolving disputes by displaying the amount of bargaining chips a node holds may perpetuate unequal power dynamics. Alliances and majorities may be formed, and reining in powerful actors in the community who might become easily disgruntled can put pressure on the network.

Blockchain in Journalism

If blockchain can store almost any kind of data that needs to be secured, and can be accessed and modified by many different people, then it is a potential solution to a lot of scenarios involving both data that needs to be kept track of and people working collaboratively. The journalism industry is one such case study, since the way tens of thousands of stories generate value every day is based on the intricate system of news production, distribution, and consumption—meaning how stories are created, shared, marketed, listened and reacted to.

Journalists need to be paid, news stories must be trusted by audiences, and uncorroborated information or rumors must be countered by maintaining a level of transparency around how information is gathered and how news stories are being told.

Legacy news organizations with ample financial resources design and build intricate systems that employ reporters and sales professionals to produce and deliver stories, as well as developers and systems managers to build and maintain data servers, firewalls, recommendation algorithms, user tracking systems, and so forth. What has been called "post industrial journalism"[17] has its own specific set of traps and opportunities: news organizations have been forced into constantly monitor platform companies and the consumer electronics industry at large with an eye toward forming partnerships or otherwise pivoting strategies in a rapidly changing digital information ecosystem.

Like virtual reality, augmented reality, live videos, or gamified news, blockchain technology is viewed as a potential solution to emergent problems.[18] Some young, startup news organizations have looked to create blockchain-based solutions to specific

[17] C.W. Anderson, Emily J. Bell, and Clay Shirky, "Post Industrial Journalism: Adapting to the Present," Tow Center for Digital Journalism, 2014, https://academiccommons.columbia.edu/doi/10.7916/D8N01JS7.
[18] Matthew Ingram, "Does 'Universal Attention Token' Sound Good? Then You're Going to Love the Blockchain," CJR, September 4, 2018, https://www.cjr.org/the_new_gatekeepers/universal-attention-token-blockchain.php.

problems, or to combine multiple blockchain technologies with blockchain-based cryptocurrencies to create sustainable business models.

Targeted solutions use blockchain as an add-on to a news organization's infrastructure, for instance by subscribing to a blockchain-based service. These services include creating blockchains to securely store the timestamps of the publication date and provenance of news stories. For the advertising business, on which journalism heavily relies, blockchains can store and keep track of ad impressions so that media organizations do not overpay for the inflated statistics of a particular ad. News organizations can become stakeholders in what are called "token-curated registries" (TCRs), where a list of business partners or other entities are ranked for specific purposes, and the registry is "edited" through a blockchain.

Alternatively, hybrid solutions may use blockchains to store different kinds of data (like the examples given above), but also construct a network of stakeholder-driven organizations around a private blockchain so that participating nodes can curate the data stored under the blockchain, such as a token-curated registry, and also participate in the governance of the entire network.

Hybrid solutions may use blockchains to store different kinds of data (like the examples given above), but also construct a network of stakeholder organizations around a private blockchain so that participating nodes can curate the data stored in the blockchain and also participate in the governance of the entire network.

Here's a breakdown of the type of blockchain applications that are currently being tested in the media industry:

- **Targeted solutions:** using blockchain to store important metadata that journalists and media companies use on a daily basis, and which they want to securely store and edit through a blockchain.
- **Hybrid solutions:** targeted solutions + cryptocurrency = a transparent and accountable business model based on self-governance.

A third area explored in this section is the journalist's access to public data in an age where blockchains become government-adopted gatekeepers of digitized records. The world of fully digitized public records and automated access, in which Freedom of Information requests, whistleblowers, and leaks fade into distant memory, is still years away, but trends seen in some recent applications will illuminate some of the traps and opportunities of blockchain-mediated government records.

Targeted solutions for newsrooms and advertisers: Po.et, AdChain, SocialFlow

Targeted solutions include Po.et,[19] a company designing blockchain solutions to securely track content metadata, such as timestamps, copyright, authorship, and distribution of digital assets. Media companies are natural customers. Reporters want to see their bylines and claims for intellectual property secured, and freelancers want to avoid their content being illegally appropriated by others. Syndicated news content works only if royalties are paid to content providers according to agreed-on forms of distribution, and news archiving prompts a level of security through immutable logs of the time and venue of publication.[20]

Po.et doesn't handle plagiarism just yet. Instead, the company wants to filter scammers by protecting the "reputations" of legitimate content providers. Essentially, Po.et is focused on making the discovery of original content, which it protects, easier—and less about intervening when duplicate content occurs on the internet. On a technical level, to do this the service provides special, immutable links for bibliographies and archives, and immutable timestamps to accompany published content. On a network level, Po.et functions as a secure marketplace for content providers to help content discovery, long-term licensing, and copyright-protected usage.

---

[19] The Po.et Foundation's whitepaper, https://uploads-ssl.webflow.com/5a0c978e0d22aa0001464356/5a7796662b07370001ace7a1_whitepaper.pdf.

[20] Matthew Ingram, "Jarrod Dicker on What the Blockchain Can Do for News," CJR, March 2, 2018, https://www.cjr.org/innovations/blockchain-poet.php.

In practice, Po.et records a number of "claims" on the Bitcoin blockchain. Claims contain the metadata of a news story, or a piece of content, such as the timestamp, author bylines, copyright information, and so on. Po.et's open-source protocol batches these claims into larger groups and then anchors (i.e., validates) the batches on the blockchain network.[21] The data batched and anchored in blocks is very small in terms of file size. Most often they merely contain a directory address to the IPFS network where the actual data of the claims are stored. (More on IPFS later—for now, the InterPlanetary File Systems is a network of servers that store data, and—similarly to blockchain—the files stored in its system are tamper-proof because they are identified through a unique hash.)

Po.et streamlines claim submissions by providing access to its blockchain through an API (application programming interface), which it calls Frost. Frost can be integrated into WordPress-based content management systems. In practice this means that once a news organization publishes a story on its website, or if a blogger creates new content, the CMS-integrated channel of Frost immediately sends a snapshot of the metadata to Po.et, where it gets batched and stored on an IPFS-participant computer, whose address then gets anchored on Po.et's blockchain.

In order to not lose sight of a claim's address in a Bitcoin block, Po.et's own system of nodes oversees this long line of transactions: the claim submitted, the IPFS location, and the header hash as well as block hash of the block in the Bitcoin network. News organizations may subscribe to Po.et's service and secure their content and publication data securely and immutably.

On the sales side, digital advertising is infamously difficult to keep in check, especially if social media platforms monopolize most of the digital ad market, or if automated ad exchanges fail to report correctly and accurately what kind of ads they display on which website to which audience. AdChain,[22] a company funded by the blockchain company

[21] David Turner, "Breaking Down Po.et: The Architecture," Medium, November 26, 2018, https://blog.po.et/breaking-down-po-et-the-architecture-f468216a7ae7.
[22] Mike Goldin, "Token-Curated Registries 1.0," Medium, September 14, 2017, https://medium.com/@ilovebagels/token-curated-registries-1-0-61a232f8dac7.

accelerator ConsenSys, licenses a token-curated registry to keep track of advertisers with whom news organizations want to partner. The registry itself is stored on a blockchain, and the organizations participating in the blockchain network can contest or approve the registry ranking by suggesting a new block with a newly ordered ranking, which then the rest of network participants are expected to approve (i.e., validate) or reject.

The history of the registry is immutable because it is on a blockchain, of which every participant keeps a copy. Instead of paying fees to ad brokers, who unilaterally mediate between publishers and advertisers, a token-curated registry is a transparent way of monitoring the list of advertisers and their services.

The registry is token-curated because in order to propose a new block with a modified ranking, nodes use tokens to initiate the block validation process. The incentive for doing so is based on game theory. Stakeholders are motivated to propose an accepted, high-value list because such a list draws more interest, thereby increasing the value of the list.[23] Ranking colleges, football teams, restaurants, or any other service is a competitive and potentially rewarding game for both the entities on the list, as well as the entities benefiting from the agency to curate that list.

When a participating node proposes a modification to the registry, other nodes may vote in favor or against that proposal by also staking some of their tokens in the form of a bid. Winning voters then share some portion of the bid, while the winning proposal (or challenger against the original proposal) takes most of the bid and the losing voters and challengers receive nothing.

A transparent list that is curated in a decentralized fashion ideally invokes trust and prompts accountability. Keeping a well-maintained registry is crucial if it is an automated list, where the ranking determines the rates for ads or the frequency of ad placements. For advertisers and publishers, being part of a list means constantly tweaking the contracts among themselves. As the ranking mutates, so does the payout or the type of ad allocated to websites or mobile apps. Consequently, it is in the interest

[23] Mike Goldin, Ameen Soleimani, and James Young, "The AdChain Registry," MetaXchain, Inc., https://adtoken.com/uploads/white-paper.pdf

of both curators and registry participants to play the transparent game of challenging or approving each new version of the registry.

Finally, an attempt to cut through the digital advertising model is exemplified by SocialFlow's Universal Attention Token (UAT), which intends to directly tokenize user attention and reward publishers by their users' real engagement.[24] SocialFlow plans to leverage its relationship with major news organizations to track user engagement within its ecosystem and reward publishers for the engagement that they prompt from users. Blockchain enters the picture when SocialFlow selects users and rewards them with digital tokens as they interact with branded content published on SocialFlow's partner sites.

Advertisers pay for ad placements, and SocialFlow curates that content in a broader landscape of editorial content supplied by its partners, rewarding both users (by giving them tokens) and publishers (by giving them hard cash based on users' unique IDs that SocialFlow tracts throughout its system, from branded content to publishers' content). User movement and token transactions are hashed and wrapped into blocks to be validated by, once again, Bitcoin's blockchain network.

Incentivizing user and publisher behavior through token transactions segues into the following section on hybrid solutions. It's one thing to use blockchain networks to store hashed metadata and monetize the benefits of security and accountability. It adds another layer of service when tokens (also blockchain-based) are mixed into decentralized networks, cryptographic transactions, and distributed databases. Tokens' ability to shape organizational behavior by practically establishing an autonomous currency system within the broader world of national currencies and other financial instruments such as stocks, bonds, or options is one of the trends that fascinate—and puzzle—investors, technologists, and scholars.

[24] Frank Speiser et al., "Universal Attention Token," SocialFlow, August 2018, https://more.socialflow.com/acton/attachment/24868/f-0106/1/-/-/-/-/UAT%20White%20Paper.pdf.

Hybrid solutions for media organizations and freelancers: Civil

One current (and developing) example of the hybrid system is Civil,[25] a network of news organizations, journalists, and investors. Civil is an organization also funded by ConsenSys, and is an amalgam of blockchain technologies and traditional news organizations organized around a cryptocurrency-driven business model.[26] Following a failed initial coin offering (ICO) in October 2018, where the company released its digital token to lure investor funds and recruit stakeholders for its blockchain network, today Civil continues to rely on funding provided by ConsenSys to maintain and expand its registry of newsrooms. Reporters are still getting paid and newsrooms in the collective remain afloat because Civil has independent backing. .

The organization, however, continues to look for other opportunities to expand its blockchain-based technology offerings to small and midsize media companies as evidenced by its most recent partnership with WordPress.org's parent company Automattic to insert a feature into its new publishing platform, Newspack, where journalists, bloggers, and other content creators can archive their material on an IPFS domain and log metadata on Civil's Ethereum-based blockchain.[27]

Underscoring Civil's hybrid approach to blockchain, news organizations participating in the Civil network hold tokens to "govern"[28] their network by voting on the makeup of the network and proposing or challenging the organizational rules governing Civil. On the infrastructural level, Civil is using Ethereum's application platform to create a customized content management system (CMS) for participating news organizations.

---

[25] Matthew Iles, "The Civil Constitution (beta)," Medium, May 4, 2018, https://blog.joincivil.com/the-civil-constitution-beta-64460a181e08.
[26] Matthew Ingram, " A Civil Primer: The Benefits, and Pitfalls, of a New Media Ecosystem," CJR, August 13, 2018, https://www.cjr.org/business_of_news/civil.php.
[27] Guillermo Jimenez, "Make Journalism Sustainable Again," Decrypt, January 18, 2019, https://decryptmedia.com/4586/newspack-wordpress-civil-make-journalism-sustainable-again.
[28] John Keefe, "How to Buy into Journalism's Blockchain Future (in Only 44 Steps)," Nieman Lab, September 19, 2018, http://www.niemanlab.org/2018/09/how-to-buy-into-journalisms-blockchain-future-in-only-44-steps/.

This CMS resembles a WordPress-style editing platform, but integrates a micropayment system where journalists can accept donations from readers in the form of Civil tokens. Participating journalists are incentivized by the Civil token valuation, since a substantial part of their salary is paid in Civil tokens. The logical consequence of such an employment contract is that reporters become shareholders of Civil, except wage-based token payments are not considered to be actual shares or securities by the US federal government. Of course, the token itself, with all its transactions, is based on the blockchain.

In short, Civil's blockchain serves multiple purposes: it is the underlying infrastructure for its tokens, which participating news organizations use for governance purposes (like a combination of stocks and voting rights for shareholders) and which also facilitate payments and royalties to journalists.[29]

Since "value" and "stakes" are different in journalism (as compared to a digital currency system), the role of blockchain will also be different. Instead of constant "trustlessness"—required for cryptocurrencies to keep every node in the network in check and exploit (as well as reward) the work that these nodes invest to maintain their network and, by extension, the value of their currency—the world of journalism requires trust, transparency, and constant negotiation. Journalists and editors may also want to dispense with the central authority of a parent company or a disinterested publisher, and wish to work in a more peer-to-peer networked environment. For journalists, then, blockchain-based applications are a useful solution because these applications are open-source and can be modified to power journalistic products (like a content management system, a timestamping tool, an ad tracking device, etc.).

In tandem, blockchain-based cryptocurrencies can make investors and new news organizations "buy into" the network and use their "stake" to govern (initiate, challenge, support, etc.) the actions of their peers in the network. Finally, the same cryptocurrency can be used to support journalists through micropayments (the transactions of which are stored in the blockchain), thus avoiding expensive credit card

[29] Vivian Schiller, "A Non Blockchain-y Person Explains Civil," Medium, July 27, 2018, https://blog.joincivil.com/a-non-blockchain-y-person-explains-civil-d9f59d5d2c96.

transaction fees that would normally render small payments (sometimes only a few cents) worthless.

Blockchains and public data

Some governments today experiment with implementing blockchain to provide secure access to public records for their citizens. Estonia is a frequently mentioned as the first nation state to implement public blockchain services on a national level.[30] "E-Estonia" allows its citizens, as well as entities doing business in the country, to access public records through a blockchain. All requests and modifications to the country's public record system are stored and validated by a blockchain network. Digitized public records are still stored on secure databases, but any action to the data is logged immutably in blocks.

The country is expanding this basic blockchain implementation to bridge the accountability gap between private companies and government contracts by deploying smart contracts on a cloud computing network. While storing digital public and private records on cloud services has become relatively mainstream in the last decade (think of Amazon's AWS hosting computing capabilities and data by State Department agencies, such as the CIA[31]), having a blockchain layer on top of the cloud allows each task and transaction performed in the cloud to be logged and rendered traceable. However, such enterprise-level implementations of blockchains will have to figure out the scalability of blockchain applications so as to be able to record and validate petabytes of transactions in any given minute.

For journalists in the future who use public record requests for their stories, the proliferation of blockchain-secured pubic databases will potentially pose new challenges and opportunities to access the same records. Instead of submitting Freedom of

---

[30] E-Estonia, "FAQ: KSI Blockchain in Estonia," https://e-estonia.com/wp-content/uploads/faq-ksi-blockchain-1.pdf.
[31] AWS Government, Education, and Nonprofits Blog, "Announcing the New AWS Secret Region," November 20, 2017, https://aws.amazon.com/blogs/publicsector/announcing-the-new-aws-secret-region/.

Information requests, government blockchain overlays will need to be configured to provide differential access to citizens and the public at large, including reporters. Anyone requesting public records will leave a record of their data request, and the data released will be logged in the blockchain. This could become highly problematic for journalists on the trail of a story wishing to act covertly before it breaks.

Future(s) of Blockchain

The in-flux state of blockchain makes even the most-informed projections sound unpersuasive for the long run. However, three emergent trends seem to pop up in the academic and trade literatures more often than others. These are: the transition to Proof-of-Stake blockchain models, the spread and adoption of smart contracts, and finally the emergence of enterprise-level blockchain protocols. All of these trends have at least one characteristic in common: the streamlined centralization of blockchain applications.

The Wild-West approach to sustaining universally deployable blockchain networks, in which anyone can participate through Proof-of-Work, is giving way to proprietary blockchain protocols, private networks, and targeted applications. While the benefits of peer-to-peer validation, cryptographic hashing, and the immutability of data within the robustly layered structure of blockchains are seen as useful and actionable in many industries, the universalistic, free-for-all, and crudely competitive idealism of the first generation of blockchain tools are increasingly considered to be an impediment to widespread applications. As an alternative to Bitcoin-style blockchain networks, we see IBM, Google, or even national governments experimenting with tailored blockchain applications, accompanied by Proof-of-Stake networks, and the deployment of blockchains for not only storing metadata but also for automating contractual relationships between stakeholders.

The proliferation of Proof-of-Stake

According to critics and blockchain entrepreneurs, a potentially new phase for blockchain applications will come from the increased adoption of Proof-of-Stake models. The traditionally PW-based Ethereum, for instance, is planning a “hard fork” for its blockchain to transition to the PS model by raising the difficulty to a level where

it becomes financially wasteful for miners and mining pools to continue their CPU-heavy efforts of validating new blocks.[32] As mentioned previously, the PS model does not generate new coins, and so no mined money can be awarded to the nodes in the network that validate each new block. Instead, validators who have enough stake in the system will validate each new block and benefit from transaction fees, which are still less than what banks and credit reporting agencies charge for their services, but which in bulk can become substantial.

Exchanging cutthroat competition for a rule-governed system is seen as an economically sound tradeoff between full and good-enough levels of decentralization. By the same token, the faultlines of "trustless networks" undergirding PW blockchains increasingly become clear: the competition of nodes is wasteful; the consolidation of the computer infrastructure by itself creates the walled gardens that early blockchain visionaries intended to circumvent; and the valuation of the cryptocurrencies (which incentivize participation in the blockchain network) fluctuate according to external conditions, such as the ebbs and flows of the hype surrounding a particular cryptocurrency, or the looming threat of state regulation of digital tokens.[33]

For media organizations, PS blockchains are probably the most preferential solution for organizing publishers into communities, curating registries, or incentivizing and rewarding independent freelancers to circulate their content. The blockchains that validate tokens or registries will still rely on PW-based hashing, but instead of paying miners with new tokens, PS systems would reward reliable network participants and reward them for their stewardship over the network.

[32] Marie Hulliet, "Ethereum Devs Reach Consensus to Delay Constantinople Hard Fork until January 2019," Cointelegraph, October 20, 2018, https://cointelegraph.com/news/ethereum-devs-reach-consensus-to-delay-constantinople-hard-fork-until-january-2019.
[33] Max Raskin and David Yermack, "Digital Currencies, Decentralized Ledgers, and the Future of Central Banking," National Bureau of Economic Research, May 2016, https://www.nber.org/papers/w22238.

Smart contracts: Law firms, governments, journalists

Smart contracts are simple blockchain-based applications that are self-executed once a node triggers them. To some degree, the challenge-and-approval mechanisms of TCRs, as well as the governance model of Civil, are examples of smart contracts. In action this means that a node in the network may propose an amendment to the blockchain. To perform this amendment, the node pays or wagers some of its tokens, and the rest of the network (or at least select computers on the network) run the same request on their own computers to validate the first node's proposal.

The sequence of triggering and validating a request is automatic, like running an application on one computer and expecting every other participating computer to sync up with the first node by performing the same task. The first node's proposal can be challenged, for instance when other nodes wish to reject the amendment. Otherwise, the request can be an actual request to access a data center to edit or retrieve data from it, such as adding copyright data or logging a financial transaction. Beyond syncing, the immutability of the blockchain network is needed to record and securely store a single node's request based on the node's credentials. If the node holds sufficient credentials, access to the database—guarded by the blockchain overlay—is given, otherwise it is rejected.

Smart contracts are like the simplified, automated versions of legal contracts, or laws and rules codified into computer code. For law firms, blockchain-based smart contracts can potentially replace paralegal work, such as closing contracts, settling claims, notarizing documents, recording deeds, and so on. Transactions are immediate with little to no cost. Note, however, that public and private records, such as titles and deeds, are still stored in databases, not on the blockchain (since blockchain cannot store that much data to begin with). Those databases might still be centralized or

decentralized—an example for the latter is the IPFS, or the InterPlanetary File System,[34] a network service and file-exchange protocol that allows data storage on many different servers around the world and provides secure access to its libraries. IPFS resembles blockchains in its explicit mission to decentralize the web by building a distributed network of nodes to store and share data (anything from metadata to cat videos) efficiently and safely.

Each file in the IPFS network receives a unique hash with which it can be identified. Instead of asking a giant commercial server, like YouTube, to locate a specific video within its database, the IPFS protocol asks for the file hash to locate the file. To close the loop between blockchain and a distributed file-sharing system, IPFS issues its own Filecoin to tokenize and reward nodes for storing files without removing them.

Blockchains and smart contracts can be combined with the IPFS service to provide multiple layers of data security and specialized access to digital records. Here, one layer is the blockchain network running smart contracts and logging the metadata of transactions, a second layer is the access to IPFS servers, and the final—physical—layer is the suburbs-worth of data warehouses where the data is located. The difficulty of implementing law into code is an obvious problem,[35] one that leaves legal scholars, blockchain designers, and government regulators still scratching their heads.

For one, if smart contracts are irreversible and self-executing, means have to be developed to give proper access to those who wish to modify their contracts or amend details in a settlement. The often indeterminate and open-ended legal language has to be married to deterministic computer code. For all intents and purposes, simple smart contracts will need to form the foundation of the more complex automated legal agreements that have yet to be developed.

Finally, as mentioned in the previous section, government databases increasingly migrating to clouds and blockchains might become "overlays" on top of the cloud

[34] Kaspar Triebstok, "How IPFS Is Challenging the Web as We Know It," Rubiks Digital on Medium, May 3, 2018, https://blog.rubiksdigital.com/how-ipfs-is-disrupting-the-web-e10857397822.
[35] Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Cambridge: Harvard University Press, 2018).

infrastructure. This setup not only signals new opportunities for data security and convenient data access, but potentially forecasts a series of limitations, such as if public access to a file is mediated by a smart contract, or when an entire blockchain network will witness each individual "smart FOIA" request from a journalist.

The same question of access becomes problematic when insurance companies will want to access national healthcare records, or when banks want to see government loans to private individuals. Investigative and data journalists will have to reckon with a dramatically altered world of data, in which the ownership and control of, as well as access to, important records will require new technological skills and increased awareness from reporters.

Enterprise-level blockchains and global public/private adoption

Since blockchain networks require lots of computers and computing power, it is perhaps unsurprising to see profitable technology companies mobilizing their readily existent computer infrastructure to provide blockchain services to business partners and customers.[36] Storing some sort of data securely (in an immutable, tamper-proof, and decentralized fashion), and providing access to databases through a blockchain overlay are just some of the examples blockchains are leveraged to monetize new digital surfaces. Enterprise level services will generally bundle developer tools, cloud computing capabilities, access to a proprietary blockchain protocol, and even a monitoring agency to help with disputes if something goes wrong.[37]

Blockchain will likely not be able to fully strip its cryptocurrency heritage, and so analysts expect a wider adoption by mostly financial institutions. While it is ironic in

[36] Hyperledger Performance and Scale Working Group, "IBM Hyperledger Performance Metrics," October 2018, https://www.hyperledger.org/wp-content/uploads/2018/10/HL_Whitepaper_Metrics_PDF_V1.01.pdf.
[37] C. Mohan, "Blockchains and Databases: A New Era in Distributed Computing," Conference paper, 17th International Workshop on High Performance Transaction Systems, Asilomar, October 10, 2017, http://www.hpts.ws/papers/2017/mohan.pdf.

hindsight to see the same banks instrumentalizing the very technology that sought to circumvent their role in sending money around the world, it's not hard to see the natural affinity of banks to a solution that provides immediate transactions, low costs, and robust security.

Conclusion

While seemingly arcane and complicated, blockchains are fairly simple ways to coordinate between a peer-to-peer network of computers. Blockchains freeze time by securely signposting the history of edits to a shared database. As blockchains and cryptocurrencies are increasingly decoupled in future applications, the underlying core functionality of blockchains will become ever more transparent.

For journalists and news organizations, blockchains are both a potentially monetizable, shiny new thing and a moment of reckoning at the same time. Blockchains can be deployed as solutions for micropayments, digital advertisement tracking, or copyright validation, all of which secure and boost a media company's bottomline.

Conversely, blockchains prompt a serious rethinking of organizational hierarchies and distributed responsibilities. At this pivotal moment, when blockchain technology detaches itself from its past of being a vehicle of extra-legal monetary transactions and shifts to broader targeted applications, it remains to be seen whether the communality, forced transparency, and data-freezing affordances of this technology garners mainstream support in the journalistic community.

Citations

1. Gili Vidan and Vili Lehdonvirta, "Mine the Gap: Bitcoin and the Maintenance of Trustlessness," *New Media & Society* 21, no. 1 (July 2019): 42–59, https://doi.org/10.1177/1461444818786220
2. Adrianne Jeffries, "'Blockchain' Is Meaningless," The Verge, March 7, 2018, https://www.theverge.com/2018/3/7/17091766/blockchain-bitcoin-ethereum-cryptocurrency-meaning
3. Arvind Narayanan and Jeremy Clark, "Bitcoin's Academic Pedigree: The Concept of Cryptocurrencies Is Built from Forgotten Ideas in Research Literature," *ACM Queue* 15, no. 4 (2017): 1–30, https://queue.acm.org/detail.cfm?id=3136559
4. "The Promise of the Blockchain Technology," *The Economist*, September 1, 2018, https://www.economist.com/technology-quarterly/2018/09/01/the-promise-of-the-blockchain-technology
5. Wessel Reijers, Fiachra O'Brolchain, and Paul Haynes, "Governance in Blockchain Technologies & Social Contract Theories," *Ledger* 1, no. 1 (2016).
6. Paul Ford, "Bitcoin Is Ridiculous. Blockchain Is Dangerous," *Bloomberg Businessweek*, March 9, 2018, https://www.bloomberg.com/news/features/2018-03-09/bitcoin-is-ridiculous-blockchain-is-dangerous-paul-ford.
7. Lloyd Armbrust, "Bitpress: An Open Protocol for Tracking the Credibility of News," Medium, May 16, 2018, https://medium.com/bitpress/bitpress-an-open-protocol-for-tracking-the-credibility-of-news-2f8c961cd67c.
8. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," bitcoin.org, 2008, https://bitcoin.org/en/bitcoin-paper.
9. Narayanan and Clark, "Bitcoin's Academic Pedigree."
10. Taylor Pearson, "How Does Blockchain Technology Work?" Medium, July 18, 2018, https://hackernoon.com/how-does-blockchain-technology-work-ceeeee47eaba.
11. Michael Noferl, Peter Gomber, Oliver Hinz, and Dirk Schiereck, "Blockchain," *Business & Information Systems Engineering* 59, no. 3 (June 2017): 183–187, https://doi.org/10.1007/s12599-017-0467-3.
12. Michele D'Aliessi, "How Does the Blockchain Work?" Medium, June 1, 2016, https://medium.com/s/story/how-does-the-blockchain-work-98c8cd01d2ae.
13. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System."

14. Blockgeeks, "Proof of Work vs. Proof of Stake: Basic Mining Guide," Blockgeeks Guide, 2016, https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/.
15. G. Andresen, "Centralized Mining," The Bitcoin Foundation, 2014, https://bitcoinfoundation.org/centralized-mining/.
16. Robert Greenfield IV, "Explaining How Proof of Stake, Proof of Work, Hashing and Blockchain Work Together," Medium, July 20, 2017, https://medium.com/@robertgreenfieldiv/explaining-proof-of-stake-f1eae6feb26f.
17. C.W. Anderson, Emily J. Bell, and Clay Shirky, "Post Industrial Journalism: Adapting to the Present," Tow Center for Digital Journalism, 2014, https://academiccommons.columbia.edu/doi/10.7916/D8N01JS7.
18. Matthew Ingram, "Does 'Universal Attention Token' Sound Good? Then You're Going to Love the Blockchain," CJR, September 4, 2018, https://www.cjr.org/the_new_gatekeepers/universal-attention-token-blockchain.php.
19. The Po.et Foundation, whitepaper, https://uploads-ssl.webflow.com/5a0c978e0d22aa0001464356/5a7796662b07370001ace7a1_whitepaper.pdf.
20. Matthew Ingram, "Jarrod Dicker on What the Blockchain Can Do for News," CJR, March 2, 2018, https://www.cjr.org/innovations/blockchain-poet.php.
21. David Turner, "Breaking Down Po.et: The Architecture," Medium, November 26, 2018, https://blog.po.et/breaking-down-po-et-the-architecture-f468216a7ae7.
22. Mike Goldin, "Token-Curated Registries 1.0," Medium, September 14, 2017, https://medium.com/@ilovebagels/token-curated-registries-1-0-61a232f8dac7.
23. Mike Goldin, Ameen Soleimani, and James Young, "The AdChain Registry," MetaXchain, Inc, https://adtoken.com/uploads/white-paper.pdf.
24. Frank Speiser et al., "Universal Attention Token," SocialFlow, August 2018, https://more.socialflow.com/acton/attachment/24868/f-0106/1/-/-/-/-/UAT%20White%20Paper.pdf.
25. Matthew Iles, "The Civil Constitution (beta)," Medium, May 4, 2018, https://blog.joincivil.com/the-civil-constitution-beta-64460a181e08
26. Matthew Ingram, " A Civil Primer: The Benefits, and Pitfalls, of a New Media Ecosystem," CJR, August 13, 2018, https://www.cjr.org/business_of_news/civil.php.
27. List of newsrooms participating in the Civil network: https://civil.co/newsrooms/

28. Guillermo Jimenez, "Make Journalism Sustainable Again," Decrypt, January 18, 2019, https://decryptmedia.com/4586/newspack-wordpress-civil-make-journalism-sustainable-again
29. John Keefe, "How to Buy into Journalism's Blockchain Future (in Only 44 Steps)," Nieman Lab, September 19, 2018, http://www.niemanlab.org/2018/09/how-to-buy-into-journalisms-blockchain-future-in-only-44-steps/.
30. Vivian Schiller, "A Non Blockchain-y Person Explains Civil," Medium, July 27, 2018, https://blog.joincivil.com/a-non-blockchain-y-person-explains-civil-d9f59d5d2c96.
31. E-Estonia, "FAQ: KSI Blockchain in Estonia," https://e-estonia.com/wp-content/uploads/faq-ksi-blockchain-1.pdf.
32. AWS Government, Education, and Nonprofits Blog, "Announcing the New AWS Secret Region," November 20, 2017, https://aws.amazon.com/blogs/publicsector/announcing-the-new-aws-secret-region/.
33. Marie Hulliet, "Ethereum Devs Reach Consensus to Delay Constantinople Hard Fork until January 2019," Cointelegraph, October 20, 2018, https://cointelegraph.com/news/ethereum-devs-reach-consensus-to-delay-constantinople-hard-fork-until-january-2019.
34. Max Raskin and David Yermack, "Digital Currencies, Decentralized Ledgers, and the Future of Central Banking," National Bureau of Economic Research, May 2016, https://www.nber.org/papers/w22238.
35. Kaspar Triebstok, "How IPFS Is Challenging the Web as We Know It," Rubiks Digital on Medium, May 3, 2018, https://blog.rubiksdigital.com/how-ipfs-is-disrupting-the-web-e10857397822.
36. Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Cambridge: Harvard University Press, 2018).
37. Hyperledger Performance and Scale Working Group, "IBM Hyperledger Performance Metrics," October 2018, https://www.hyperledger.org/wp-content/uploads/2018/10/HL_Whitepaper_Metrics_PDF_V1.01.pdf.

38. C. Mohan, “Blockchains and Databases: A New Era in Distributed Computing,” Conference paper, 17th International Workshop on High Performance Transaction Systems, Asilomar, October 10, 2017, http://www.hpts.ws/papers/2017/mohan.pdf.