Big Data
Volume 5 Number 4, 2017

DOI: 10.1089/big.2017.0071

ORIGINAL ARTICLE

Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains

Steve Huckle* and Martin White

Abstract

In this article, we introduce a prototype of an innovative technology for proving the origins of captured digital media. In an era of fake news, when someone shows us a video or picture of some event, how can we trust its authenticity? It seems that the public no longer believe that traditional media is a reliable reference of fact, perhaps due, in part, to the onset of many diverse sources of conflicting information, via social media. Indeed, the issue of "fake" reached a crescendo during the 2016 U.S. Presidential Election, when the winner, Donald Trump, claimed that *The New York Times* was trying to discredit him by pushing disinformation. Current research into overcoming the problem of fake news does not focus on establishing the ownership of media resources used in such stories—the blockchain-based application introduced in this article is technology that is capable of indicating the authenticity of digital media. Put simply, using the trust mechanisms of blockchain technology, the tool can show, beyond doubt, the provenance of any source of digital media, including images used out of context in attempts to mislead. Although the application is an early prototype and its capability to find fake resources is somewhat limited, we outline future improvements that would overcome such limitations. Furthermore, we believe that our application (and its use of blockchain technology and standardized metadata) introduces a novel approach to overcoming falsities in news reporting and the provenance of media resources used therein. However, while our application has the potential to be able to verify the originality of media resources, we believe that technology is only capable of providing a partial solution to fake news. That is because it is incapable of proving the authenticity of a news story as a whole. We believe that takes human skills.

Keywords: fake news; blockchain; big data; Ethereum; hash functions; cryptography; public-key cryptography; digital signatures; Preservation Metadata

Introduction

The issue of fake news hit the headlines when Donald Trump, the winner of the 2016 U.S. Presidential Election, accused various media outlets of mounting a concerted effort to discredit him[1] by publishing hoaxes and propaganda.[2] Even before the President's accusations, one of the implicated newspapers, *The New York Times*, printed a story asserting that one of Trump's prominent supporters was spreading disinformation.[3] After, presumably, much journalistic investigation, the newspaper claimed falsehood by showing that a photograph (illustrated in Fig. 1), which was used on the *Christian Times* website to suggest that the U.S. President's opponents were rigging votes, was, in fact, a picture from the United Kingdom's *Birmingham Mail*. The picture showed ballot boxes used in a U.K. election, not fraudulent Clinton votes found in an Ohio Warehouse, as the website claimed. However, what if such detective work was unnecessary? What if it were trivial to ascertain the provenance of a picture or video? Not only could we trust that material but also we could distrust any material that was not validated that way.

The primary aim of this article is to introduce a blockchain-based distributed application that we are calling Provenator (intended as the agent noun of the verb form of provenance, which means establishing the origin of something), a tool that helps prove the

Department of Informatics, School of Engineering and Informatics, University of Sussex, Brighton, United Kingdom.

*Address correspondence to: *Steve Huckle, Department of Informatics, School of Engineering and Informatics, University of Sussex, Chichester 1, Falmer, Brighton, BN1 9QT, United Kingdom,* E-mail: s.huckle@sussex.ac.uk

FIG. 1. *Birmingham Mail* picture of the delivery of ballot boxes used in a U.K. election. The picture was misappropriated by a Trump supporter, who (falsely) claimed that the image showed that the Clinton campaign team was rigging votes.[4]

originator of media sources. Before describing Provenator, we provide some background by introducing the motivation for this work—fake news. Then we present big data's role in technological attempts to counter false reporting. Next, we describe the technologies underlying Provenator—blockchains and a data schema for recording metadata about media resources. Then we discuss Provenator in detail, including its use, current limitations, and future improvements that might address those limitations, before concluding.

Fake News

Fake News is, quite simply, invented information.[5] Unfortunately, it is often difficult to spot invented from real. For instance, in a recent survey, when the United Kingdom's Channel 4 News showed three real and three fake stories to 1684 adults, only 4% of the respondents were able to identify all the stories correctly, and nearly half thought that at least one of the fakes was real.[6]

While the Channel 4 survey may not appear, at first glance, to raise a major issue, a somewhat more nuanced interpretation of fake news is that they are stories that are distorted or decontextualized and deliberately designed to deceive. Often, such stories have an undeclared political bias.[5] Thus, fake news is a synonym for propaganda, a term which has sinister connotations. As an example, during the recent annexation of the Crimea, NATO accused Russia of using fake news to spread disinformation about their actions there.[7] Moreover, in a follow-up to their survey, Channel 4 ran a news series on fake news, in which they interviewed Janis Sartis, the Director of the NATO Strategic Communications Centre. During the interview, Sartis said: "You don't need tanks. You might actually achieve your goals if you change the perception of a given society in a way that corresponds to your interests and the society starts to act how you want them to act".[8]

Social media companies have come under political pressure for not providing tools to counter the problem of fake news. Consequently, politicians have accused those companies of having an undue influence on elections both in the United Kingdom and United States.[9] Indeed, analysis has shown that, during the final 3 months of the U.S. presidential campaign, Facebook's fake news stories about the U.S. presidential election generated much more interest than stories from traditional news outlets.[10] Indeed, Facebook admitted that: "more and more…debate is mirrored online on platforms like Facebook, leading to an increase in individual access and agency in political dialogue…as well as the diversity of influences on any given conversation".[11]

To counter this issue, Facebook placed advertisements in U.K. newspapers, giving tips to its users on how to spot fake news items.[12] The company also implemented several design features on its platform's user interface; measures included stronger automated detection of fakes, convenient user reporting of suspicious content, and third-party verification of news items.[13] The founder of Wikipedia, James Wales, also announced a new initiative for countering fake news.[14]

The criticisms of social media platforms and fake news suggest that the issue is a new phenomenon. However, propaganda has a long history.

A brief history of fake news

During a recent TED talk, Yuval Noah Harari said: "I think fake news has been with us a long time; just think of the Bible!"[15] Indeed, the earliest example of propaganda is considered to be the Behistun Inscription, authored around 515 BC, which is an inscription in three different cuneiform dialects on a cliff at Mount Behistun in Kermanshah Province, Western Iran. It details the rise to the throne of the Persian Empire of Darius I and his success in quelling multiple rebellions.[16] However, Pope Gregory XV was the first to use the term "propaganda," when in 1622, he formed the "Congregatio de Propaganda Fide," or "congregation for propagating the faith." The word itself comes from the Latin word "propagare," meaning propagation. Hence, propaganda is understood to mean the propagation of an ideology.[17]

A more modern example of propaganda, yet still 100 years old, was described by Dr. David Clarke in a recent piece for the BBC.[18] Dr. Clarke tells how, in 1917, the British Government, in an ultimately successful attempt to bring China onto the Allied side in The Great War, fabricated a gruesome story about the German military, whom they (falsely) accused of extracting glycerin from human corpses. Apparently, Conservative MP John Charteris, Head of Intelligence at the time of the story's fabrication, transposed captions from a photograph that showed a train of dead horses that were to be rendered onto another showing a train taking dead soldiers for burial. Unfortunately, the story was later used by the Nazi Party as proof of British lies during the Great War, and it may have led to doubts about news of Nazi atrocities during the Second World War; as Dr. Clarke comments: "lies have consequences."[18] The Nazi Party, realizing the importance of war propaganda, formed the Reich Ministry of Public Enlightenment and Propaganda. The Ministry's head, Joseph Goebbels, used his control of the press to help reinforce Nazi ideology through fake news: "If you tell the same lie enough times, people will believe it; and the bigger the lie, the better."[19]

Much like Nazi Germany, Stalinist Russia, in an attempt to convince its people that the Soviet Union enjoyed much higher living standards than those in the Capitalist West, used propaganda extensively.[20] During the lead-up to the Second World War, the Soviet media suppressed heretical opinion through the censorship of dissonant voices. Newspaper headlines took a standard form: "all workers greeted the policy (of the Russian Government) with satisfaction." They repeated the message often, giving credence to Goebbels' mantra that if you tell a lie often enough, people will believe it. Soviet propaganda continued after the war too, with books heavily censored and newspapers propagating idealized reality.[21] Television and radio gave that reality a degree of formality. Meanwhile, cinematography took a triumphalist tone, depicting happy lives and the fulfillment of the "Soviet dream."[21]

Despite increasing press freedom in the 1990s, following Glasnost (a Soviet policy of open discussion of political and social issues), Russian authorities appear to continue propagating fake news stories. Indeed, on February 22, 2017, the Russian Minister of Defence, Sergei Shoigu, admitted that 4 years prior, the Russian Government had established "Voyska Informatsionnykh Operatsiy," a dedicated information warfare force, because: "Our propaganda needs to be clever, smart, and efficient."[22] For instance, they may deliberately take images out of context so that they support the state narrative.[23] For example, to refute the Western narrative that the passenger aircraft MH17 was shot down by Russian-backed Ukrainian Separatists, Russian state television has reported on an aerial photograph of a jet fighter firing a missile at the downed plane. However, an organization called StopFake has gone to great lengths to debunk the picture, citing evidence such as the incorrect placement of the Malaysian Airlines logo and the lack of aircraft vapor trails.[23]

The Russian State has not been the sole purveyors of fake news in the modern world. In 1928, Cornell Graduate Edward Bernays published a book called *Propaganda*, which has become, essentially, a manual of mass manipulation.[24] The book opens with the following paragraph: "The conscious and intelligent manipulation of the organized habits and opinions of the masses is an important element in a democratic society.

Those who manipulate this unseen mechanism of society constitute an invisible government which is the true ruling power of our country." In fact, before the First World War, the term propaganda was not used negatively, but the public began to mistrust the term once they realized the extent to which the Anglo-American political machinery had deployed propaganda in an attempt to demonize "The Hun."[24] Its use by the Nazi Party in the Second World War,[25] and later by Communist Russia, appears to have sealed the term's fate; now propaganda has extremely negative connotations. However, that does not mean that its use in the West has diminished. Immediately after the war, U.S. President Truman instigated NSC/10, a policy to contain the Soviet state using wide-ranging covert operations, including propaganda.[26] During the 1960s and 1970s, the media corporations of Western nations were instrumental in promoting neo-colonialism (the practice of exerting influence or control over less developed countries using trade policies and economic or financial means) and incapacitating attempts at self-determination by third world countries.[25] There are recent examples of Western propaganda too; in 2005, the U.S. Government tried to sway public opinion as to the benefits of the Iraq War by spending US$300 million on an initiative to propagate "positive news."[27]

Democracy and the free press

Perhaps the most famous example of fake news from the literary fiction is George Orwell's *1984*.[28] The book depicts the Inner Party, a tyrannical organization who govern a Super State. One of the novel's main themes is censorship through the Inner Party's modification of records, such as photographs. The protagonist is Winston Smith, who works for the Ministry of Truth; it is his job to rewrite past newspaper articles and thereby distort records so that they correspond to the party's propaganda. By depicting a state that enforces suppression through historical revisionism, Orwell demonstrates that press freedom is core to the healthy functioning of a democratic nation. Undoubtedly, a free press plays a pivotal role in a democracy's political culture because it relies upon a "healthy and vibrant" media system, which keeps its citizens adequately informed.[25] Indeed, the media's ownership, management, and funding directly affect its capacity to serve the democratic process.[25]

The President of the United States is the "Leader of the Free World." The "Free World" includes nations who espouse certain freedoms, such as those based on a free press, and it is formed primarily by the countries who opposed both Fascism in the Second World War and Soviet Communism during the Cold War. Hence, the United States is at the zenith of all the supposed free democratic nations. The First Amendment to the U.S. Constitution guarantees individual and press freedom by prohibiting government from impinging on those freedoms: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."[29] It is, then, somewhat disconcerting when the U.S. President starts to undermine the free press by accusing them of spreading fake news. Coleen Christie, the host of Canada's CTV News, believes that the President's fake news accusation is merely a symptom of the explosion of digital media, which has changed our legacy news platforms and undermined our trust in such platforms.[30] Indeed, she warns that: "in this modern news age, information is power, yet never has our ability to leverage that power been more at risk." As we have already seen, social media outlets are coming under increasing political pressure to ensure the integrity of the items published on their platforms, so they have started to implement measures to help counter the phenomenon. Could new digital technologies help rather than hinder? Might blockchains provide methods for circumventing the issue of fake news by establishing the credentials (or not) of media resources used in such stories? Much of the rest of this article discusses such a possibility. However, first, we describe some ongoing research into big data and fake news.

Big Data and Fake News

Big data refers not just to the large quantities of digital data, but also to the quality of the data and the relationships formed.[31] In other words, big data is networked, and recognizing patterns therein creates value. Unfortunately, as we have shown above, the data may not always reflect the truth.[32] Hence, even if big data has the potential to transform our understanding of world events,[31] there are dangers presented by inaccuracies and/or (deliberate) falsities.[33] Indeed, news, in its purest sense, is meant to convey truthful, unbiased, and informative facts about issues affecting the world. Hence, gathering reliable information is an important part of a journalist's skills[34]; they must take a critical perspective on all information collected because their stories must stand up to later scrutiny.

Library and information science is adapting to the challenges of big data news streams, by attempting to use automated methods for analyzing text and verifying online information[33]: "separating the news from the noise is key to the verification of digital information."[35] We take a look at some such initiatives next.

Fake news detection technologies

City University has instigated a project, sponsored by Google, with the goal of helping journalists identify fake news by analyzing relationships in large, complex news-based datasets.[35] City is developing a web-based tool that combines machine learning and artificial intelligence technologies to visualize those relationships.[35] They are aiming to test their product with European-based news organizations, such as the United Kingdom's Telegraph media group and the Guardian, as well as Ireland's national broadcaster, RTE.

As we have already shown, nowadays, users don't get their news solely from traditional print and broadcast media; they also get it from social media sources. Hence, both Narwal et al.[36] and Jin et al.[37] focus their attention on overcoming fake news on platforms such as Twitter. Jin et al. describe a tool that analyzes messages and creates a hierarchical graph optimization of the relationship between news events. By so doing, their application propagates the credibility of those events.[37] Narwal et al. have developed a tool called UnbiasedCrowd, whose purpose is to, first, identify bias, second, identify images that are used out of context to support a particular opinion, and third, create a call to action, whereby activists are urged to expose the inherent bias.[36]

The application developed in this article, Provenator, stores provenance metadata on a blockchain, thus enabling content creators to prove, unequivocally, the origins of their media resources. Because of the properties of blockchains (which we will describe later), this also means users can trust the authenticity of the metadata about those resources. In addition, Provenator provides an interface whereby users can check the provenance of media resources used in news stories. However, this supposes that Provenator was used to document the resource in the first place; in reality, this functionality is only useful given wide-scale deployment of our application. Of course, since we are at the prototype stage, this is yet to happen. However, such wide-scale use is possible, so later in the article, when we describe such a scenario, we feel justified in doing so.

Before we detail Provenator itself, we first describe the technologies it uses to help facilitate data integrity and authenticity.

Methods for Trust and Authenticity

As we have already discussed, it is crucial that reporters trust the integrity and authenticity of the media resources contained within their news stories. For example, suppose Alice is the *Birmingham Mail* Photographer who was responsible for the picture of the U.K. ballot boxes, which we discussed in the introduction. Imagine that Bob is her Picture Editor, who must be satisfied with the image's integrity and authenticity. For instance, he has to be sure that, without Alice's knowledge, someone has not swapped the picture for another (or that any modifications have a verifiable provenance trail). We will show that, to achieve such confidence, Bob requires methods from the field of cryptography.

Cryptography

Cryptography is the mathematics of information security,[38] a field of study that investigates the confidentiality, integrity, authenticity, and nonrepudiation of data.[39] Next, we describe some tools that apply techniques from cryptography; namely, public-key cryptography (PKC), cryptographic hash functions, and digital signatures.

Public-key cryptography.

Data encryption is a process that produces ciphertext by combining some original text (to be kept secret, for whatever reason), with a much shorter key. Later, it is possible to use the key to transform the ciphertext back into the original text, a process known as decryption.[40]

PKC is a particular form of encryption that uses a pair of asymmetric keys; a private key that is known only to the owner, and a public key that is widely shared.[38] The basic idea is that encryption is achieved using the public key and decryption using the private key.[39] Figure 2 shows how Alice could use PKC to send a secure message to Bob about her picture; she uses Bob's public key to encrypt the message, and subsequently, only Bob can decrypt Alice's message since he is the only person who has the paired private key. Thus, the security of PKC systems relies upon the secrecy of the private key.

Figure 3 shows the process Bob uses to generate his private and public keys; he feeds a random number into a key generation program, from which it produces the required keys.

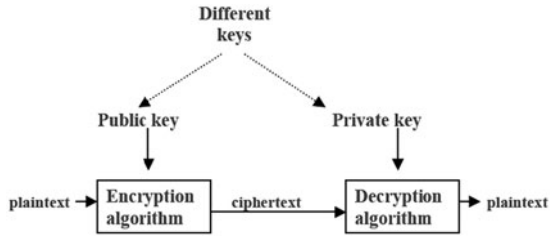


FIG. 2. Public-key cryptography.[39]

In PKC systems, it is trivial (computationally) to generate public and private keys, but once the public key is known, it is infeasible to find the private key. This is a result of a class of mathematical problems that have no efficient solution. One such problem is the discrete logarithm, which uses the modular exponentiation of large prime numbers that are easy to compute, but practically impossible to invert.[39]

Cryptographic hash functions. When Alice sends her photograph, Bob must be satisfied that, while in transit, it has remained unaltered. Cryptographic hash functions can help there. The basic idea is that Alice computes a cryptographic hash of the picture, which she then sends to Bob alongside the image itself. Bob then calculates the cryptographic hash value of the received photo and checks that the hash matches the value Alice sent.

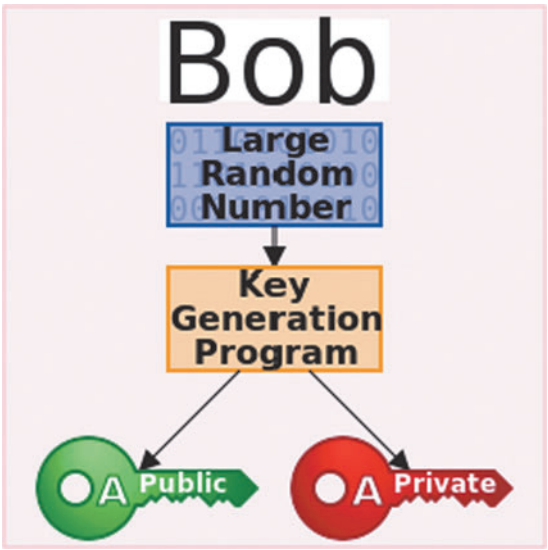


FIG. 3. Key generation.[41]

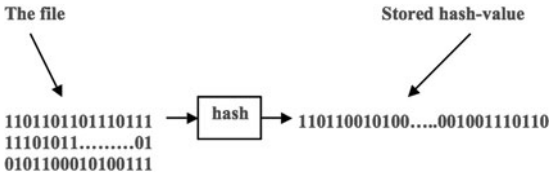


FIG. 4. A hash function.[39]

A cryptographic hash is a one-way function that maps arbitrary data to a fixed-size string. They are mathematical algorithms that are infeasible to invert (much like their PKC counterparts). The ideal cryptographic hash function has five main properties:

(1) Deterministic—the same message results in the same hash.
(2) Fast—for any message, it is quick to calculate the hash.
(3) One-way—it is practically impossible to generate the message from its hash.
(4) No correlation—a small change to a message will drastically modify the hash.
(5) Collision resistance—it is computationally infeasible to find any two distinct inputs, M and M*, which hash to the same value.[39]

Figure 4 shows a hash function that converts an arbitrary length block of data into a unique fixed-length "hash value" that serves as a compact representation of the original data.[39]

Figure 5 shows that, after receiving Alice's photograph, the hash Bob computes must be unique to a given input.[42] In other words, if the hash is the same as the original, then Alice's image must have remained unaltered.

Similarly, Figure 6 shows that if the hash generated by Bob does not match that sent by Alice, then the picture must have been modified.

An example of hash function is SHA-256, which produces many fixed-size 256-bit (32-byte) hashes. For all practical purposes, finding collisions is beyond the capabilities of present-day computing. It is an

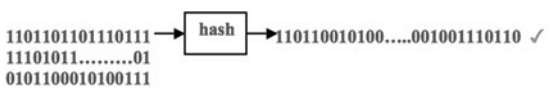


FIG. 5. The validated hash.[39]

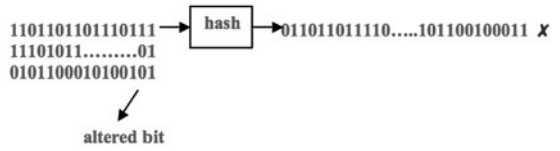


FIG. 6. An altered file.[39]

iterated hash function, a process shown in Figure 7; its design ensures the use of all message bits in the final hash value Hk. It works by splitting the input into a sequence of fixed-size blocks M1, M2, M3,…, Mk, with some padding rule for the last block Mk. Input blocks are processed in order, using a one-way compression function that gives a set of intermediate hash values H0, H1, H2,…, Hk. H0 is a predefined initializing value, and Hk is the hash value output of the SHA-256 function.

Earlier, while giving an overview of hashing functions, we showed that a computed hash must match that of the origin. However, that raises the problem of ensuring the validity of the original hash. In other words, Bob may question whether it was Alice who sent the hash of the picture in the first place. Digital signatures can help there. We discuss those next.

Digital signatures

From an early age, we learn the importance of a written signature as it serves to identify, authorize, and validate.[38] In the electronic world, it is trivial to append to a document a signature that does not belong to the originator, so cryptography has developed advanced digital signature techniques that would allow Alice to bind her identity to her photograph. The process would involve Alice executing a transform so that the final message she sends to Bob combines the original image together with some secret information held only by Alice.[38]

An overview of the digital signature process is shown in Figure 8. To allow Alice to share information with Bob (in a manner that guarantees the data's authenticity), she creates a signature that Bob can use to validate her message. Moreover, Alice would be unable to deny that it was she who shared the information, due to the nonrepudiation properties of digital signatures.

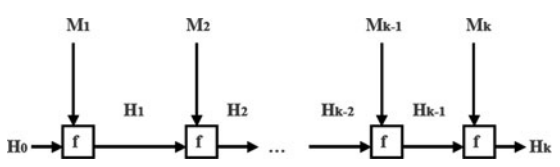


FIG. 7. An iterated hash function.[39]

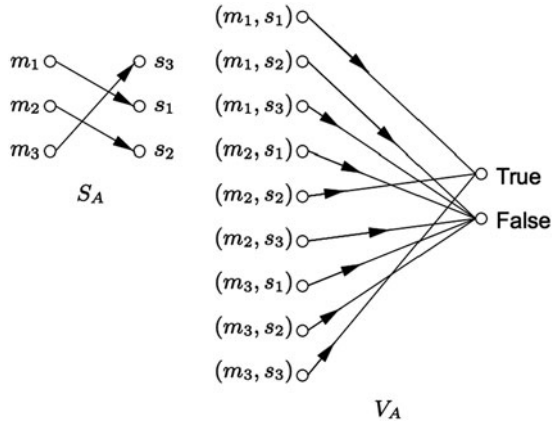


FIG. 8. The digital signature process. M—the set of messages to be signed by Alice. S—a collection of Alice's signatures. S_A—a secret signing transformation that will be used by Alice to create signatures from messages M. V_A—a verification transformation, from the set $M \times S$ to the set {true, false}, for Alice's signatures. V_A is publicly known, so Bob can use it to verify signatures created by Alice, thereby authenticating the messages they share.[38]

A typical usage of a digital signature is to sign a cryptographic hash of a message (the information that must be signed),[38] using the signees private key.[43] The signature then takes the form of a number, which proves that the signing operation took place.

Technologies Used by Provenator to Prove Authenticity

The application we are about to describe, Provenator, uses technologies that use methods from cryptography to help determine the authenticity of media resources. In addition, it uses a schema to record and retrieve metadata describing those media resources. We describe those technologies next.

Blockchains

Blockchains have capabilities resulting in their suitability for determining integrity and authenticity because they are, essentially, an immutable database technology[44] with inbuilt trust mechanisms.[45] They include cryptographic

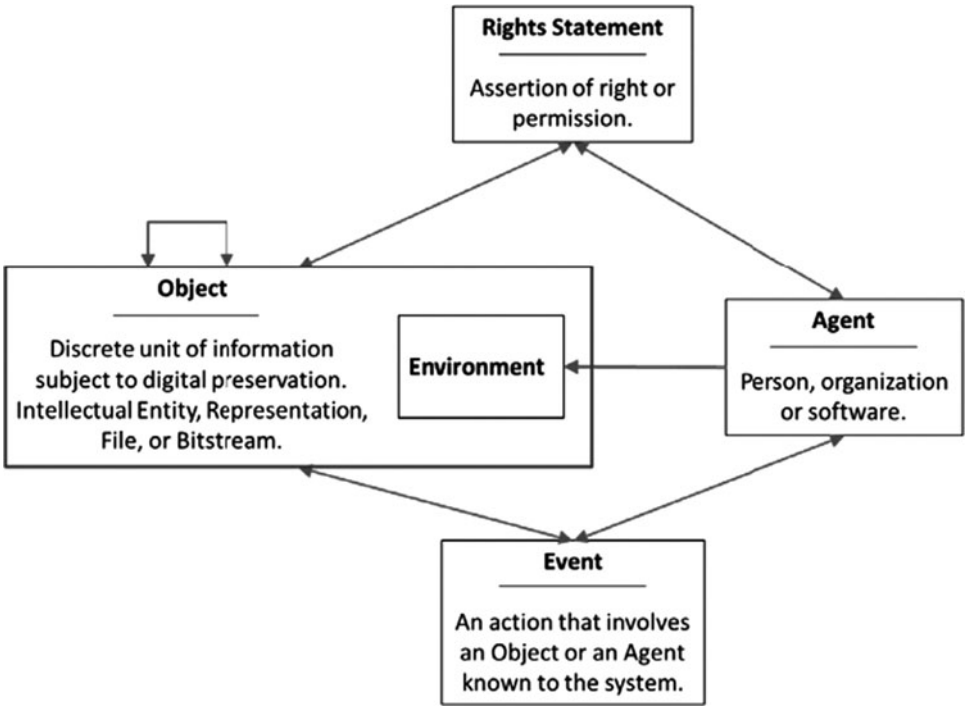


FIG. 9. The PREMIS 3.0 data model.[50]

algorithms and digital signatures that allow secure electronic collaboration, without requiring any centralized authority.[46] Blockchains also have the ability to execute smart contracts, which are verifiable scripts that automate a system's rule set.[47] In essence, then, blockchains are a trusted ledger capable of running application logic.[47] Furthermore, they cannot be controlled by any single entity.[48] Those mechanisms mean that we can use a blockchain to record data about our media resources and any entity that views those records will be satisfied that the information conveyed is authentic. However, we still require an appropriate schema for recording data on the blockchain. We discuss that next.

Provenance metadata

PREMIS stands for "Preservation Metadata: Implementation Strategies"; it outlines a provenance schema which helps identify a resource.[49] The PREMIS data model,[50] shown in Figure 9, describes four separate preservation entities: (1) Objects, (2) Events, (3) Agents, and (4) Rights.

Provenator uses PREMIS definitions to record the provenance of digital media items on the blockchain, using smart contracts. This ensures that the data conform to an open standard, which should "future-proof" the information held and help facilitate further interactions with different users.[51] It also develops some of the ideas of Mannens et al.,[52] who propose using metadata, alongside descriptions, to accompany news items because that would facilitate transparency and trust estimation.

The Provenator Application

The general principle of Provenator is that a content creator should be able to prove the provenance of the resources they create. To do so, Provenator gives creators the ability to store relevant authentication information about their creations on the blockchain so that it can be retrieved easily later and used to verify those same resources.

Requirements of the Provenator application

We are almost in a position to discuss Provenator in detail. However, we still need to consider the steps required to prove the provenance metadata of media resources. Thankfully, we need not think of those steps ourselves, because a similar "trust" process is used when distributing new releases of the Ubuntu operating system software, which we describe next.

Distributing the Ubuntu operating system software. The steps for distributing Ubuntu, shown below, involve combining digital signatures with PKC to help ensure that the software downloaded and installed can be trusted. The process is as follows:

(1) Download the operating system's disk image, together with a file of checksums and the signature used to sign the checksums file.
(2) Fetch the public key used for the signature.
(3) Use the key to verify the checksums file's signature.
(4) Run a command that generates a SHA-256 cryptographic hash on the operating system disk image.
(5) Check that the generated hash matches the hash from the downloaded checksums file.[53]

Hence, by following the process above, if the hashes match, a user can install the operating system and trust that they have an official Ubuntu release. Indeed, Alice could use a similar process to share her image with Bob.

Operations of the Provenator application

Borrowing from the Ubuntu process for verifying the Ubuntu software, Provenator should do the following:

(1) Get a cryptographic hash of the digital media resource.
(2) Create the PREMIS of the digital resource.
(3) Sign the transaction that stores the cryptographic hash of the digital resource, and its associated metadata, on the blockchain.

By following that process, subsequent users of the data will be able to trust the integrity and authenticity of the digital media metadata because of the immutability of blockchain records. Below shows how Provenator will allow such users to check a digital resource's provenance data on the blockchain:

(1) Get a cryptographic hash of the digital resource.
(2) Check whether that hash exists on the blockchain.
(3) If the hash exists, retrieve the associated metadata.

Next, we will look in more detail at Provenator's architecture.

Provenator's architecture

Provenator consists of the following architecture:

- An Ethereum blockchain,[54] which stores the provenance metadata about media resources.
- Ethereum smart contracts, written in the language Solidity,[55] which read and write PREMIS about media objects.
- A JavaScript web application, written in React,[56] used for creating and accessing the PREMIS data stored in the Ethereum smart contracts.

A working prototype of Provenator, as well as its source code, is available via the source code repository GitHub (https://github.com/glowkeeper/Provenator).

The working prototype

The working prototype of Provenator exists on the network of the InterPlanetary File System (IPFS). IPFS is a peer-to-peer content-addressed file system that forms the final component of our application's architecture; by publishing there, it means that the application is wholly distributed because, as discussed above, its underlying database, the blockchain, is also distributed. Furthermore, IPFS deploys cryptographic tools to ensure the authenticity of resources stored on its network. Thus, it is a good match for our technology. Below is a brief description of IPFS.

The InterPlanetary file system. IPFS deploys a generalization of a Merkle directed acyclic graph (DAG) to establish a decentralized network of trusted data. Applying cryptographic hashes to a graph was Ralph Merkel's solution for transferring reliable information over an untrusted network.[57] The idea was profound; many systems that rely on trust use Merkle DAGs—IPFS and Bitcoin[58] are just two examples among many. The fundamental principle behind a Merkle DAG is that if you have the hash of the root node, and the hash came from a trusted source, then, as long as the hashes match that of the root, you can trust all leaf nodes.[42] IPFS deploys a Merkle DAG to represent links between objects, which are cryptographic hashes of target blocks on the file system,[59] a concept it has borrowed from the version control system Git.[60] Figure 10 shows the representation of an image on IPFS. Hence, any file stored under IPFS is guaranteed to be unique. Moreover, as long as the file forms a Merkle DAG of objects, it can be trusted too. Furthermore, because new objects hash differently, objects on IPFS are, essentially, immutable.[59]

Nodes on the IPFS network, which connect to one another to transfer and store objects, can be considered as trusted sources since they use PKC to establish their identity; they do so using a cryptographic hash of the public half of their public and private key pair. When

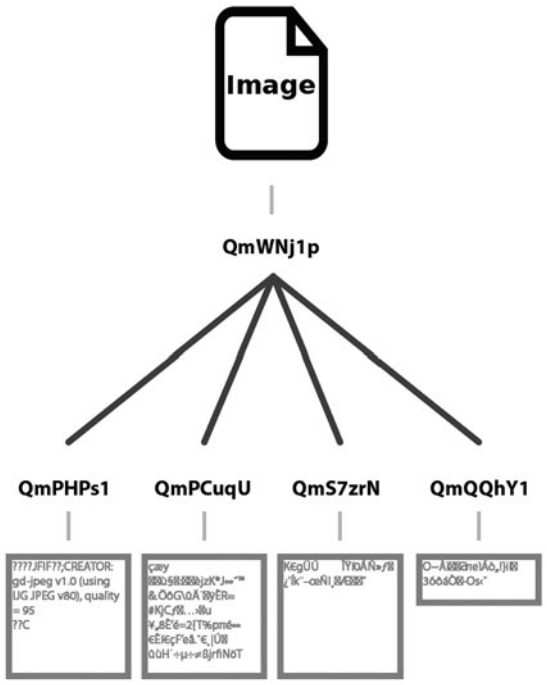


FIG. 10. A hash tree.[61]

two nodes connect, they do so by exchanging those public keys, which are then used to encrypt subsequent communication. IPFS nodes generate their key pairs using the asymmetric cryptographic algorithm Rivest–Shamir–Adleman public-key cryptosystem (RSA),[62] which uses random numbers via entropy sources of the IPFS nodes themselves. RSA's security relies on the properties of the integer factorization problem (IFP):

Given $n = pq$, find p and q, where p and q are primes.

IFP looks deceptively simple. However, provided that p and q are sufficiently large, solving it is, actually, computationally infeasible.[39]

Not so smart contracts. At the time of writing, the working prototype of Provenator uses the Ethereum Testnet, Ropsten.[63] However, we hope to produce a viable production release, so it may be that, by the time of publication, the application is running on the Ethereum blockchain itself. If that is the case, then Ethereum transactions that update the blockchain cost Ether (the unit of currency on Ethereum), so there will be a fee for storing metadata about digital resources.

Appendix G of the Ethereum yellow paper details some reasonably complex calculations for determining the fee schedule of Ethereum transactions.[64] However, the essence of those fees is less code leads to less cost. Furthermore, retrieving information from the blockchain is free. That leads to some important design decisions when building a distributed application (dApp); not least is that the JavaScript web application, which serves as the user interface, should do much of the heavy lifting and the smart contracts should only set and get, rendering them not so smart, after all. An example will serve to illustrate—when adding a media resource to Provenator, the user must also input the agent, or content creator, who owns that resource. A reasonable application design would be to send that agent information to the smart contracts and have them check whether the agent already exists in the database. However, that check, if it leads to a blockchain update, could be prohibitively expensive. A less costly design is to have the smart contracts expose a simple accessor method for retrieving agent data from an index of agents—an operation that can be carried out for free. That way, the web application can use the accessor method to perform the same check for nothing and only pay for agent data to be stored on the blockchain if the agent does not already exist.

Use of Provenator

Consider the situation we described in the introduction to this article, whereby the supporter of the then-Republican candidate for the U.S. Presidency published a photograph of a man behind some ballot boxes as an accompaniment to a claim that the Democrats were rigging votes. Figure 11 below shows a screenshot from the *Christian Times* website making that claim.

The exchangeable image file format (Exif) is a standard for specifying information about image files,[65] including data such as descriptions and copyright information. Unfortunately, such data are easily changed.[66] Presumably, the editor of the *Christian Times* did just that, and therefore, *The New York Times* had to go to great lengths to prove out of context use of the image. Now imagine that Alice was the photographer who took that photograph and that she used Provenator to record data about the picture on the blockchain. Under that circumstance, proving that the *Christian Times* had used Alice's picture falsely would be a simple matter of using Provenator. Thus, *The New York Times* could have saved itself much bother.

Next, we discuss the schema Alice uses to register herself, using Provenator, as the creator of that photograph.

Provenator's PREMIS. Figure 12 below shows Alice using Provenator's PREMIS data model[50] to create

FIG. 11. A snapshot of the *Christian Times* Website, where it was claimed that the Clintons' were rigging votes. Picture Courtesy of *The New York Times*.[3]

information about her photo, which she stores on the blockchain. She records a cryptographic hash of her picture, along with associated metadata (such as a description of the image), as a PREMIS object. She also records the date the photo was taken, as a PREMIS event. The PREMIS agent describes Alice herself. The PREMIS rights detail the image's license.

The implementation of the metadata, which we show above, describes a single object—Alice's picture of the ballot boxes used in the Sheldon election. That object has a single agent—Alice herself. It has a single event—the date when the picture was taken, and a single right—the *Birmingham Mail's* copyright. However, the implementation of the PREMIS used by Provenator is more complex. It describes a PREMIS object that can have many properties, as well as many agents, events, and rights (e.g., the licensing rights may be different in the United Kingdom to those in the United States). Similarly, although an event may only belong to a single agent, an agent may record multiple events, own many objects, and deploy many different rights. Finally, specific rights belong to a single object and a single agent.

MetaMask. MetaMask[67] is a tool able to run an Ethereum dApp in a browser. When using Provenator, Alice can use MetaMask to sign the transactions she creates for storing the PREMIS about her picture on the blockchain. By doing so, anyone accessing those data are confident that it was Alice herself who recorded the information.

Viewing the PREMIS data. Now Alice has recorded information about her photograph; Bob, her eEditor, can use the image Alice sends to generate a cryptographic hash and retrieve information about that hash from the blockchain. Figure 13 shows a screenshot of Provenator, after Bob has recovered data about the picture Alice sent to him.

Due to the deterministic and collision resistance properties of cryptographic hashes, by retrieving the data above, Bob is confident as to the authenticity of the image Alice sent. He can also apply edits and record information about those changes, thus creating a provenance chain for the picture. Hence, rather than going to great investigative lengths to prove out of context use of Alice's image, *The New York Times* would have been able to check the validity of the picture simply by uploading the *Christian Times*' copy to Provenator. Then they would have retrieved the same metadata as Bob, which would have shown the picture to be fake.

However, although that would have shown that the image itself was fake, it would not have proved that the article as a whole was fiction. Proving that might take a little more than technology. We consider that issue, next.

Validating News

The BBC has had many difficulties in providing accurate news stories from behind the frontlines of the Syrian conflict.[68] Indeed, journalists have lost their lives there, so it has become common practice to source stories from ordinary Syrian citizens. However, ensuring the validity of such "user-generated content" (UGC) has been "a skill journalists have had to learn."[68] To that end, the BBC has become proficient at developing new practices that ensure the validity of

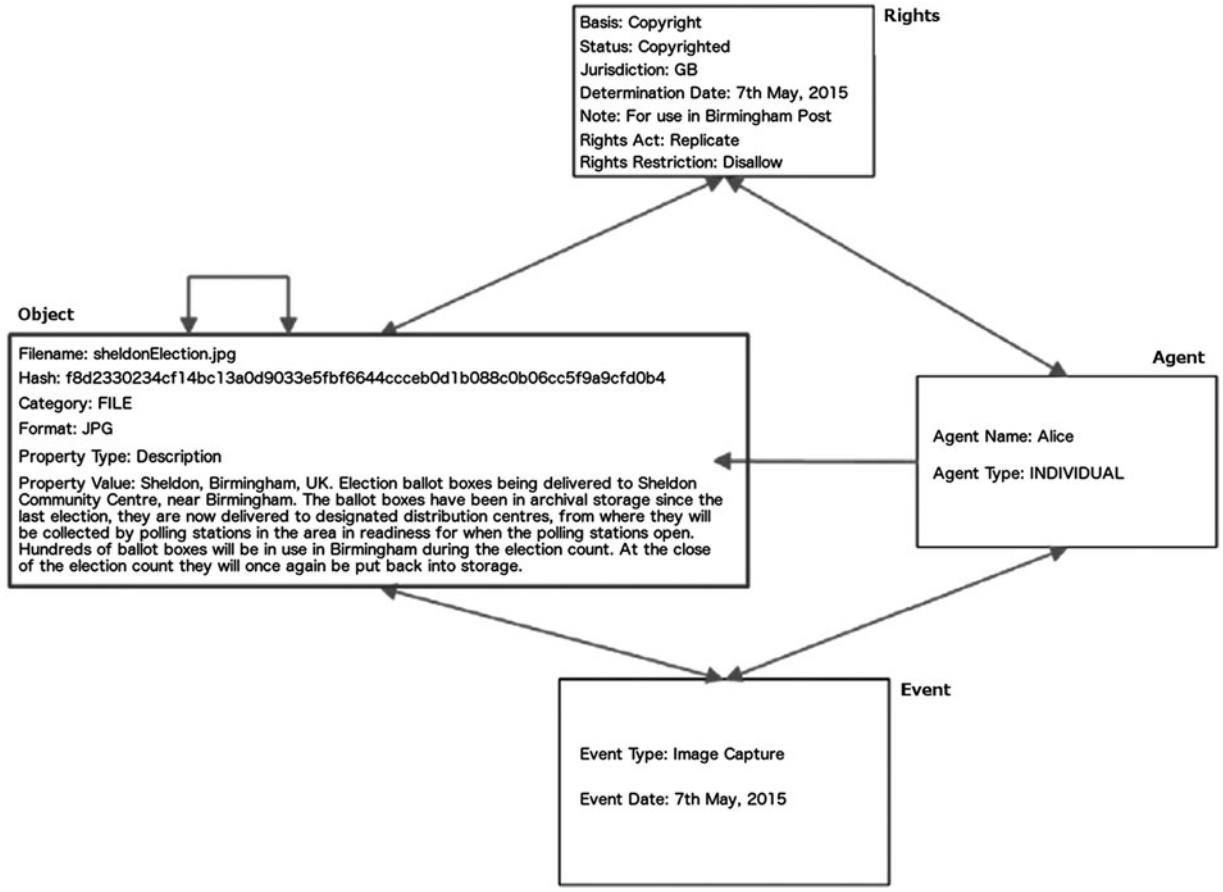
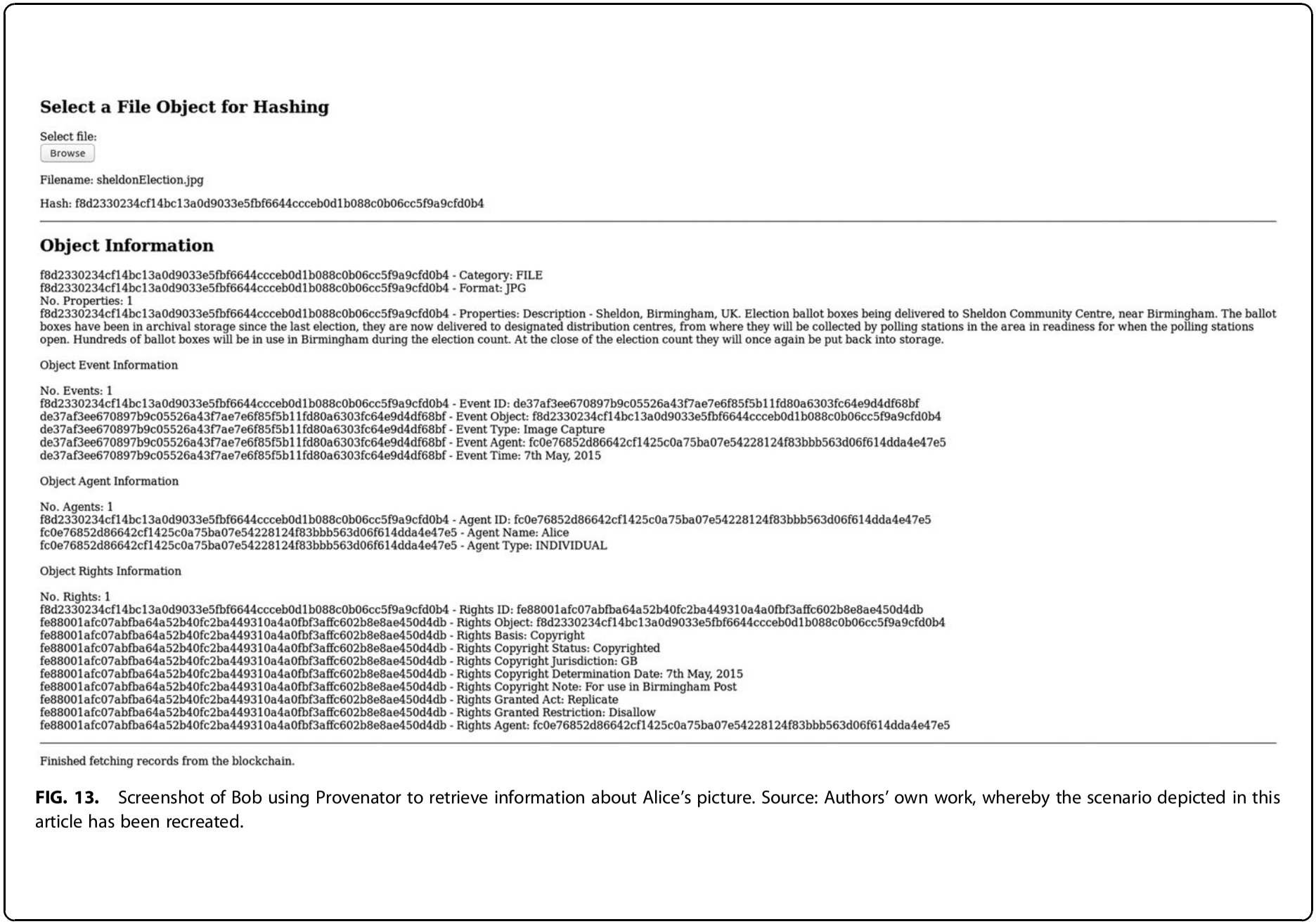


FIG. 12. The PREMIS 3.0 data model[50] applied to Alice's picture of the Sheldon Election Ballot Boxes.

UGC. Apparently, such methods involve technology, but also common sense and fostering healthy relationships with reliable Syrians.[68] Augmenting big data news stream technology with a "human touch" to verify items is a common theme.[69] For example, one project argues for the formation of a fake news corpus to aid deception detection, and to that end, when collecting the data, qualified participants will be required to spot the fakes.[33] In fact, all of the big data technologies we mentioned above require some form of human action—either through visualizing graphs or acting upon some visual data. Therein lies the crucial point; when the BBC checks the validity of stories given by users behind the Syrian front lines, technology can only go so far. A good deal of human skill is required, too. Moreover, while technology, such as Provenator, will make it possible to prove the validity of media resources used within news, proving the authenticity of fake news stories as a whole often takes good journalistic practices. Another good example is the experience of Facebook; while countering propaganda in the run-up to the 2016 U.S. Election, the company found that their algorithms were not always up to the job of spotting fake stories. Instead, to curate the news items appearing on their site, they had to fall back on human editors.[70]

Current Limitations of Provenator and Future Work

A strength of Provenator is also a weakness. The strength is that the same digital media resource will always generate the same cryptographic hash. Thus, if two hashes match, it is certain that it is the same object. Therefore, we can retrieve provenance data and trust that it accurately reflects the object's origins. To put that in another way, changing a single pixel in a digital resource will generate an entirely different cryptographic hash. Therein lies the weakness—it would not have been difficult for the *Christian Times* to alter the image of the Sheldon Election ballot boxes, thus, as it stands, defeating our tool.



Select a File Object for Hashing

Select file:
Browse

Filename: sheldonElection.jpg

Hash: f8d2330234cf14bc13a0d9033e5fbf6644ccceb0d1b088c0b06cc5f9a9cfd0b4

Object Information

f8d2330234cf14bc13a0d9033e5fbf6644ccceb0d1b088c0b06cc5f9a9cfd0b4 - Category: FILE
f8d2330234cf14bc13a0d9033e5fbf6644ccceb0d1b088c0b06cc5f9a9cfd0b4 - Format: JPG
No. Properties: 1
f8d2330234cf14bc13a0d9033e5fbf6644ccceb0d1b088c0b06cc5f9a9cfd0b4 - Properties: Description - Sheldon, Birmingham, UK. Election ballot boxes being delivered to Sheldon Community Centre, near Birmingham. The ballot boxes have been in archival storage since the last election, they are now delivered to designated distribution centres, from where they will be collected by polling stations in the area in readiness for when the polling stations open. Hundreds of ballot boxes will be in use in Birmingham during the election count. At the close of the election count they will once again be put back into storage.

Object Event Information

No. Events: 1
f8d2330234cf14bc13a0d9033e5fbf6644ccceb0d1b088c0b06cc5f9a9cfd0b4 - Event ID: de37af3ee670897b9c05526a43f7ae7e6f85f5b11fd80a6303fc64e9d4df68bf
de37af3ee670897b9c05526a43f7ae7e6f85f5b11fd80a6303fc64e9d4df68bf - Event Object: f8d2330234cf14bc13a0d9033e5fbf6644ccceb0d1b088c0b06cc5f9a9cfd0b4
de37af3ee670897b9c05526a43f7ae7e6f85f5b11fd80a6303fc64e9d4df68bf - Event Type: Image Capture
de37af3ee670897b9c05526a43f7ae7e6f85f5b11fd80a6303fc64e9d4df68bf - Event Agent: fc0e76852d86642cf1425c0a75ba07e54228124f83bbb563d06f614dda4e47e5
de37af3ee670897b9c05526a43f7ae7e6f85f5b11fd80a6303fc64e9d4df68bf - Event Time: 7th May, 2015

Object Agent Information

No. Agents: 1
f8d2330234cf14bc13a0d9033e5fbf6644ccceb0d1b088c0b06cc5f9a9cfd0b4 - Agent ID: fc0e76852d86642cf1425c0a75ba07e54228124f83bbb563d06f614dda4e47e5
fc0e76852d86642cf1425c0a75ba07e54228124f83bbb563d06f614dda4e47e5 - Agent Name: Alice
fc0e76852d86642cf1425c0a75ba07e54228124f83bbb563d06f614dda4e47e5 - Agent Type: INDIVIDUAL

Object Rights Information

No. Rights: 1
f8d2330234cf14bc13a0d9033e5fbf6644ccceb0d1b088c0b06cc5f9a9cfd0b4 - Rights ID: fe88001afc07abfba64a52b40fc2ba449310a4a0fbf3affc602b8e8ae450d4db
fe88001afc07abfba64a52b40fc2ba449310a4a0fbf3affc602b8e8ae450d4db - Rights Object: f8d2330234cf14bc13a0d9033e5fbf6644ccceb0d1b088c0b06cc5f9a9cfd0b4
fe88001afc07abfba64a52b40fc2ba449310a4a0fbf3affc602b8e8ae450d4db - Rights Basis: Copyright
fe88001afc07abfba64a52b40fc2ba449310a4a0fbf3affc602b8e8ae450d4db - Rights Copyright Status: Copyrighted
fe88001afc07abfba64a52b40fc2ba449310a4a0fbf3affc602b8e8ae450d4db - Rights Copyright Jurisdiction: GB
fe88001afc07abfba64a52b40fc2ba449310a4a0fbf3affc602b8e8ae450d4db - Rights Copyright Determination Date: 7th May, 2015
fe88001afc07abfba64a52b40fc2ba449310a4a0fbf3affc602b8e8ae450d4db - Rights Copyright Note: For use in Birmingham Post
fe88001afc07abfba64a52b40fc2ba449310a4a0fbf3affc602b8e8ae450d4db - Rights Granted Act: Replicate
fe88001afc07abfba64a52b40fc2ba449310a4a0fbf3affc602b8e8ae450d4db - Rights Granted Restriction: Disallow
fe88001afc07abfba64a52b40fc2ba449310a4a0fbf3affc602b8e8ae450d4db - Rights Agent: fc0e76852d86642cf1425c0a75ba07e54228124f83bbb563d06f614dda4e47e5

Finished fetching records from the blockchain.

FIG. 13. Screenshot of Bob using Provenator to retrieve information about Alice's picture. Source: Authors' own work, whereby the scenario depicted in this article has been recreated.

However, this weakness in our early prototype of Provenator is not insurmountable. For example, it may be possible to use some form of mathematical filter to remove or reduce the "noise" of an object, thus rendering two seemingly disparate resources identical.[71] There may be better approaches than filtering, however. Narwal et al. describe how they classify similar images using fisher vectors and k-means clustering.[36] Indeed, object classification via fisher vectors appears to be an active area of computer vision research.[72] Hence, if Provenator used such techniques, users may be able to classify images, discover similarities, and find fakes that way. Furthermore, fisher vectors are used for classifying videos, too,[73] so Provenator's scope could broaden beyond images. That could be true for another technique, too—perceptual hashes,[74] which establish object matches based on perceived content.[75] While any change in two multimedia resources will generate vastly different cryptographic hashes, perceptual hashes produce comparable results if the resources are similar. Hence, if future versions of Provenator extend its resource metadata to include a perceptual hash, this single pixel change above would render a complimentary perceptual hash that can be matched against the original by calculating their hamming distance.[76] Indeed, perceptual hashing is already used by organizations such as Shazam, Google, and also by YouTube to detect copyright infringement across a broad range of digital objects, such as audio, video, and images.[75] Indeed, although this article uses the example of a picture to help explain the application's functionality, Provenator can be used to prove the provenance of any media objects, even the news stories themselves. In fact, improvements in future versions, using methods such as fisher vectors and or perceptual hashes, would make it even more suitable as a tool for helping to prove the origins of different media resources.

Conclusion

Fake news has hit the headlines recently. Indeed, Donald Trump has continued to accuse various media outlets of distributing falsehoods that undermine him.[77] We have not examined the reasons for his doing so; such an examination would be interesting, but it is not the focus of this article. Moreover, although we have given some background history on the issue of fake news, it is beyond the scope of this article to discuss propaganda itself. In addition, although we discuss the issue of social media platforms and fake news, we do not examine the methods and processes for distributing fake news items on such platforms or the efficacy of the measures taken by those platforms to counter the problem. Instead, the purpose of this article has been to propose a technological solution to the problem of proving the validity of media resources used in fake news. Various research groups are investigating technologies capable of overcoming the problem of verifying big data news streams. However, the application we have developed, Provenator, is uniquely capable of recording metadata about digital media on blockchain technology so that it becomes trivial to prove their authenticity in a manner that can be trusted. The ultimate aim of our tool is to make content creators accountable for the resources they create.

Unfortunately, as it stands, although Provenator works well for recording the origins of a media resource, it is easy to defeat the "find fake" capabilities of this early prototype, simply by changing a single pixel of a misappropriated image. This may be addressed in future version, since there are techniques available, such as fisher vectors and perceptual hashes, which can improve future versions of the application and make it much more capable.

However, while Provenator may become more proficient at verifying the authenticity of media resources used within a story, the application will only ever be capable of providing a partial solution to the problem of fake news. Unfortunately, we do not think technology will ever be wholly capable of proving the truth of the story as a whole. We believe, currently, that takes human skills. Certainly, while it might take some sophisticated mathematics to determine the similarity between two media resources that only differ by a single pixel, the same complexity does not apply to the human eye, which would quickly decide that those resources are the same.

Although we have reservations about the possible limitations of technology in combating fake news, we believe that the trust mechanisms of blockchains make them better positioned than other technologies for proving the authenticity of media resources. Indeed, organizations are investigating using blockchains for purposes such as transparency and publicly auditable content ranking.[78] Moreover, our application is an example of a tool that can help fight "fakeness." Indeed, in our supposed scenario, where Alice was the photographer who took the image used by the *Christian Times*, *The New York Times* would have had a much easier job of proving falsehood.

Acknowledgments

The idea for this article came after a discussion over tea with colleagues at the University of Sussex; namely, Phil Watten and Patrick Holroyd. Thank you also to Ian Wakeman, Head of Informatics at the University of Sussex, who provided feedback on the first draft of the article and, in particular, provided useful references on image capture. Also thank you to Konstantin Blyuss, reader in Mathematics at the University of Sussex, who provided insight about cryptography. Finally, the authors are grateful to the anonymous reviewers, as well as the editors, who gave suggestions that improved the article immeasurably.

Author Disclosure Statement

No competing financial interests exist.

References

1. Watts AW. How Russia dominates your Twitter feed to promote lies (and, Trump, too). The Daily Beast. August 6, 2016. Available online at www.thedailybeast.com/articles/2016/08/06/how-russia-dominates-your-twitter-feed-to-promote-lies-and-trump-too.html (last accessed February 5, 2017).
2. Morin R. Trump: New York Times is 'fake news'. POLITICO. 17AD. Available online at http://politi.co/2jAdgwn (last accessed February 5, 2017).
3. Shane S. From headline to photograph, a fake news masterpiece. The New York Times. 2017. Available online at www.nytimes.com/2017/01/18/us/fake-news-hillary-clinton-cameron-harris.html (last accessed February 5, 2017).
4. Walker J. Birmingham mail photo used in a 'fake news' Trump story shared with 6 million. Birmingham Mail. 2017. Available online at www.birminghammail.co.uk/news/midlands-news/birmingham-mail-photo-used-fake-12476900 (last accessed September 27, 2017).
5. Hunt E. What is fake news? How to spot it and what you can do to stop it. The Guardian: Media. 2016. Available online at www.theguardian.com/media/2016/dec/18/what-is-fake-news-pizzagate (last accessed February 27, 2017).
6. Goodfellow J. Only 4% of people can distinguish fake news from truth, Channel 4 study finds. The Drum. 2017. Available online at www.thedrum.com/news/2017/02/06/only-4-people-can-distinguish-fake-news-truth-channel-4-study-finds (last accessed March 23, 2017).
7. Chee FY. NATO says it's seen a sharp rise in Russian fake news since the Kremlin seized Crimea. Business Insider. 2017. Available online at http://uk.businessinsider.com/r-nato-says-it-sees-sharp-rise-in-russian-disinformation-since-crimea-seizure-2017-2 (last accessed April 20, 2017).
8. Fake news series part two. Channel 4 News. 19:00 00:41:21-00:55:54: Channel 4. 2017. Available online at https://learningonscreen.ac.uk/ondemand/index.php/clip/90422
9. MacIntyre D. Facebook—the secret election weapon. BBC News: UK. May 8, 2017. Available online at www.bbc.co.uk/news/uk-39830727 (last accessed May 8, 2017).
10. Silverman C. This analysis shows how viral fake election news stories outperformed real news on Facebook. BuzzFeed. 2016. Available online at www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook (last accessed May 9, 2017).
11. Weedon J, Nuland W, Stamos A. Facebook and information operations. Facebook. 2017. Available online at https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf (last accessed May 8, 2017).
12. Cellan-Jones R. Facebook publishes fake news ads in UK papers. BBC News: Technology. Los Alamitos, CA: May 8, 2017. Available online at www.bbc.co.uk/news/technology-39840803 (last accessed May 8, 2017).
13. Zuckerberg M. What we're doing about misinformation. 2016. Available online at www.facebook.com/zuck/posts/10103269806149061?pnref=story (last accessed May 9, 2017).
14. reporter AHT. Wikipedia founder to fight fake news with new Wikitribune site. The Guardian: Technology. 2017. Available online at www.theguardian.com/technology/2017/apr/25/wikipedia-founder-jimmy-wales-to-fight-fake-news-with-new-wikitribune-site (last accessed May 8, 2017).
15. Nationalism vs. globalism: The new political divide. 2017. Available online at www.ted.com/talks/yuval_noah_harari_nationalism_vs_globalism_the_new_political_divide (last accessed March 3, 2017).
16. Nagle DB, Burstein SM (Eds.). The ancient world: Readings in social and cultural history. 4th ed. New York: Prentice Hall, 2010, p. 280.
17. Online Etymology Dictionary. Propaganda. 2017. Available online at www.etymonline.com/index.php?term=propaganda (last accessed March 27, 2017).
18. Clarke D. The corpse factory and the birth of fake news. BBC News: Entertainment & Arts. February 17, 2017. Available online at www.bbc.co.uk/news/entertainment-arts-38995205 (last accessed February 25, 2017).
19. A-Z Quotes. Joseph Goebbels Quote. A-Z Quotes. 2017. Available online at www.azquotes.com/quote/1419276 (last accessed March 4, 2017).
20. Davies S. Popular opinion in Stalin's Russia: Terror, propaganda, and dissent, 1934–1941. Cambridge; New York: Cambridge University Press, 1997, p. 236.
21. Zasurskiĭ I. Media and power in post-Soviet Russia. Armonk, NY: M.E. Sharpe, 2004, p. 269.
22. Jane's 360. Acknowledgement of Russia's information warfare capability indicates its strategic importance and impracticability of maintaining plausible. 2017. Available online at www.janes.com/article/68267/acknowledgement-of-russia-s-information-warfare-capability-indicates-its-strategic-importance-and-impracticability-of-maintaining-plausible-deniability-policy (last accessed May 4, 2017).
23. Khaldarova I, Pantti M. Fake news: The narrative battle over the Ukrainian conflict. J Pract. 2016;10:891–901.
24. Bernays EL, Miller MC. Propaganda. Brooklyn, NY: Ig Publishing, 2005, p. 168.
25. McChesney RW, Wood EM, Foster JB, editors. Capitalism and the information age: The political economy of the global communication revolution. New York, NY: Monthly Review Press, 1998, p. 254.
26. Office of the Historian. Foreign relations of the United States, 1945–1950, emergence of the intelligence establishment. 1948. Available online at https://history.state.gov/historicaldocuments/frus1945-50Intel/d292 (last accessed May 4, 2017).
27. Love R. Before Jon Stewart. Columbia J Rev. 2007. Available online at www.cjr.org/feature/before_jon_stewart.php (last accessed March 1, 2017).
28. Orwell G. 1984: A novel; revised and updated bibliography. New York: New American Library, 1985.
29. Staff LII. First amendment. LII/Legal Information Institute. 2010. Available online at www.law.cornell.edu/constitution/first_amendment (last accessed March 1, 2017).
30. Fixing the News. 2015. (TEDxVancouver). Available online at www.youtube.com/watch?v=NwmGTM5Py8Y (last accessed May 4, 2017).
31. boyd d, Crawford K. Six provocations for big data. SSRN Electron J. 2011. Available online at www.ssrn.com/abstract=1926431 (last accessed September 20, 2017).
32. Labrinidis A, Jagadish HV. Challenges and opportunities with big data. Proc VLDB Endowment. 2012;5:2032–2033.
33. Rubin VL, Chen Y, Conroy NJ. Deception detection for news: Three types of fakes: Deception detection for news: Three types of fakes. Proc Assoc Inf Sci Technol. 2015;52:1–4.
34. Vieregge Q. Journalism: Gathering information and writing your story. 2017. Available online at https://writingcommons.org/open-text/research-methods-methodologies/empirical-research/interviews/journalism-gathering-information-and-writing-your-story (last accessed April 12, 2017).
35. Grover E. City journalism academics to lead European big data and fake news project. City, University of London. 2017. Available online at www.city.ac.uk/news/2017/june/google-digital-news-initiative-dminr (last accessed September 21, 2017).

36. Narwal V, Salih MH, Lopez JA, et al. Automated assistants to identify and prompt action on visual news bias. New York: ACM Press, 2017. pp. 2796–2801.
37. Jin Z, Cao J, Jiang Y-G, Zhang Y. News credibility evaluation on microblog with a hierarchical propagation model. Los Alamitos, CA: IEEE, 2014. pp. 230–239.
38. Menezes AJ, Van Oorschot PC, Vanstone SA. Handbook of applied cryptography. In: CRC press series on discrete mathematics and its applications. Boca Raton: CRC Press, 1997, p. 780.
39. Blyuss K. Cryptography—Lecture notes. 2016. School of Mathematical and Physical Sciences, University of Sussex.
40. Ethereum. Ethereum glossary. GitHub. 2016. Available online at https://github.com/ethereum/wiki (last accessed March 22, 2017).
41. KohanX. Public key cryptography. 2010. Available online at https://commons.wikimedia.org/wiki/File:Public-key-crypto-1.svg
42. Cipriani T. Visualizing Git's Merkle DAG with D3.Js—Tyler Cipriani. 2016. Available online at https://tylercipriani.com/blog/2016/03/21/Visualizing-Git-Merkle-DAG-with-D3.js/ (last accessed March 13, 2017).
43. Bitcoin Wiki. Elliptic curve digital signature algorithm. 2015. Available online at https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm (last accessed March 27, 2017).
44. Swan M. Blockchain: Blueprint for a new economy. Surrey, UK: O'Reilly Media, Inc., 2015, p. 149.
45. Umeh J. Blockchain double bubble or double trouble? ITNOW. 2016;58:58–61.
46. Huckle S, White M. Socialism and the blockchain. Future Internet. 2016;8:49.
47. Eris Industries. Explainer | Smart Contracts. Eris Industries Documentation. 2016. Available online at https://docs.erisindustries.com/explainers/smart_contracts/ (last accessed March 19, 2016).
48. The Economist. The trust machine. The Economist. 2015. Available online at www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine (last accessed February 17, 2016).
49. Caplan P. Understanding PREMIS. The Library of Congress. 2009. Available online at www.loc.gov/standards/premis/understanding-premis.pdf (last accessed September 23, 2017).
50. PREMIS Editorial Committee. The PREMIS Data Dictionary Version 3.0. 2015. Available online at www.loc.gov/standards/premis/v3/premis-3-0-final.pdf (last accessed June 29, 2017).
51. W3C. Data on the Web—Best Practices. 2015. Available online at www.w3.org/TR/2015/WD-dwbp-20150224/ (last accessed May 11, 2017).
52. Mannens E, Coppens S, Verborgh R, Hauttekeete L, Van Deursen D, Van de Walle R. Automated trust estimation in developing open news stories: Combining memento and provenance. Los Alamitos, CA: IEEE, 2012. pp. 122–127.
53. Ubuntu. VerifyIsoHowto—Community Help Wiki. 2016. Available online at https://help.ubuntu.com/community/VerifyIsoHowto (last accessed March 11, 2017).
54. Ethereum. Ethereum Project. 2017. Available online at www.ethereum.org/ (last accessed January 10, 2017).
55. Solidity. Solidity—Solidity 0.4.8-develop documentation. 2016. Available online at https://solidity.readthedocs.io/en/develop/ (last accessed January 13, 2017).
56. React. React—A JavaScript library for building user interfaces. 2017. Available online at https://facebook.github.io/react/ (last accessed June 29, 2017).
57. Merkle RC. A digital signature based on a conventional encryption function. In: Pomerance C (Ed.): Advances in Cryptology—CRYPTO'87. Berlin, Heidelberg: Springer Berlin Heidelberg, 1988. pp. 369–378.
58. Bitcoin. Bitcoin—Open source P2P money. 2015. Available online at https://bitcoin.org/en/ (last accessed November 27, 2015).
59. Juan Benet. IPFS—Content Addressed, Versioned, P2P File System (DRAFT 3). 2017. Available online at https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf (last accessed March 13, 2017).
60. Git. Git. 2017. Available online at https://git-scm.com/ (last accessed March 13, 2017).
61. flyingzumwalt. The decentralized web primer—Lesson: Turn a file into a Merkle tree. 2016. Available online at https://flyingzumwalt.gitbooks.io/decentralized-web-primer/content/ipfs-dag/lessons/files-as-dags.html (last accessed March 13, 2017).
62. Dell EMC. RSA laboratories—PKCS #1: RSA cryptography standard. 2017. Available online at www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs-rsa-cryptography-standard.htm (last accessed May 23, 2017).
63. Ethereum. Ropsten: Ropsten public testnet PoW chain. Ethereum. 2017. Available online at https://github.com/ethereum/ropsten (last accessed July 16, 2017).
64. Wood G. Ethereum—A Secure Decentralised Generalised Transaction Ledger. EIP-150 revision. 2013. Available online at http://gavwood.com/paper.pdf (last accessed January 16, 2017).
65. EXIF.org. EXIF and related resources. 2017. Available online at www.exif.org/ (last accessed September 26, 2017).
66. Huculak M. How to edit image metadata on Windows 10. Windows Central. 2017. Available online at www.windowscentral.com/how-edit-picture-metadata-windows-10 (last accessed September 26, 2017).
67. MetaMask. MetaMask. 2017. Available online at https://metamask.io/ (last accessed March 28, 2017).
68. Johnston L. How is citizen journalism transforming the BBC's Newsroom practices? 2017. Available online at www.academia.edu/20427847/How_is_citizen_journalism_transforming_the_BBC_s_Newsroom_practices
69. Sethi RJ. Crowdsourcing the verification of fake news and alternative facts. New York: ACM Press, 2017. pp. 315–316.
70. McHugh M. Facebook can try to fix fake news, but it can never be an arbiter of truth. The Ringer. 2016. Available online at https://theringer.com/facebook-can-try-to-fix-fake-news-but-it-can-never-be-an-arbiter-of-truth-75d4d0ca0176#.9pdaniqlk (last accessed May 9, 2017).
71. Datta R, Joshi D, Li J, Wang JZ. Image retrieval: Ideas, influences, and trends of the new age. ACM Comput Surv. 2008;40:1–60.
72. Liu L, Wang P, Shen C, Wang L, van den Hengel A, Wang C, et al. Compositional model based Fisher vector coding for image classification. IEEE Trans Pattern Anal Machine Intell. 2017;1–1.
73. Sun C, Nevatia R. Large-scale web video event classification by use of Fisher vectors. IEEE, 2013. pp. 15–22.
74. Bertolami J. Perceptual hashing. 2014. Available online at http://bertolami.com/index.php?engine=blog&content=posts&detail=perceptual-hashing (last accessed September 24, 2017).
75. rfraimow. Adventures in perceptual hashing. AAPB National Digital Stewardship Residency. 2017-2017-04-20T14:27:45+00:00. Available online at https://ndsr.americanarchive.org/2017/04/20/adventures-in-perceptual-hashing/ (last accessed September 24, 2017).
76. Hamming RW. Error detecting and error correcting codes. Bell Syst Tech J. 1950;29:147–160.
77. Schwab N. Trump calls NBC and ABC 'totally biased and fake news' AGAIN. Mail Online. 2017. Available online at http://www.dailymail.co.uk/~/article-4342518/index.html (last accessed March 28, 2017).
78. Richmond J. Using blockchain technology to fight fake news. Distributed. 2017. Available online at /news/how-blockchain-can-fight-fake-news/ (last accessed July 16, 2017).

Cite this article as: Huckle S, White M (2017) Fake news: a technological approach to proving the origins of content, using blockchains. *Big Data* 5:4, 356–371, DOI: 10.1089/big.2017.0071.

Abbreviations Used

DAG = directed acyclic graph
IFP = integer factorization problem
IPFS = InterPlanetary File System
PKC = public-key cryptography
RSA = Rivest-Shamir-Adleman public-key cryptosystem
UGC = user-generated content