Comparing PEDDaL® with Bitcoin

By PEDDaL.com, 07 April 2016

Blockchaining, the technology that is so critical to the operation of Bitcoin and was publicized in a seminal 31 October 2008 academic paper by Satoshi Nakamoto ("the Nakamoto paper"), had been proposed in the application for US Patent 7,904,450 ("the '450 patent") more than six months earlier [1,2,3]. That patent application was filed on 25 April 2008 and publicly disclosed as US Patent Application Publication 2009/0100041 on 16 April 2009.

The '450 patent teaches a system named Public Electronic Document Dating List ("PEDDaL®") that was in operation, using blockchaining by March of 2009. The PEDDaL® system permits proving an asserted date-of-existence for documents held in secrecy, as well as document integrity (no alteration) since that asserted date. PEDDaL® had been mentioned earlier, in the application for US Patent 7,676,501 ("the '501 patent"), filed on 22 March 2008 and publicly disclosed as US Patent Application Publication 2008/0177799 on 24 July 2008 – more than three months prior to the Nakamoto paper's publication date. So PEDDaL® beats Bitcoin as the earlier invention of blockchaining.

Blockchaining establishes a provable sequential order for blocks of information, for example a set of digital files, without requiring reliance upon a trusted third party. Bitcoin uses blockchaining to render attempts to double-spend Bitcoin currency easily detectable by anyone, including people who know nothing about any Bitcoin transaction, apart from publicly disclosed digital fingerprints of transactions. The Nakamoto paper describes the Bitcoin implementation of blockchaining in section "3. Timestamp Server". PEDDaL® uses blockchaining to render alteration of registered documents easily detectable by anyone, including people who know nothing about any registered document, apart from publicly disclosed digital fingerprints of documents. The ’450 patent describes the PEDDaL® implementation of a blockchain in Figures 3 and 9, column 10, lines 32-51, and column 21, lines 28-41. The phrase “edition chain” is in Figure 21.

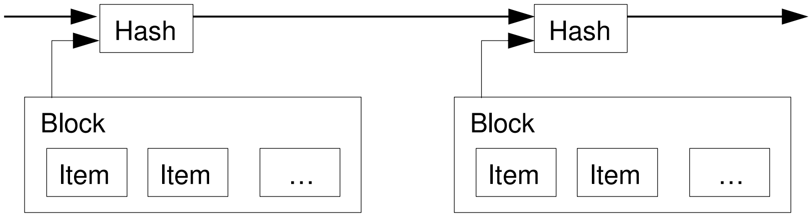
The blocks that are chained in the PEDDaL® system are labeled “DDL editions” in the ’450 patent. The ’450 patent uses the term “Integrity Verification Code” (“IVC”) to describe a digital fingerprint; PEDDaL® uses a combination of the SHA-512 and SHA-1 message digests (a.k.a. “hash values”) as a digital fingerprint for a file. The ’450 patent states:

> By iterating this process, each subsequent DDL edition builds upon prior submissions, becoming a cumulative record. A series of DDL editions can thus be chained, so that anyone possessing a copy of a particular DDL edition can then infer the existence and integrity of all DDL editions earlier in the chain, up through the initial DDL edition, …
> The now-open DDL edition is appended with the DDL IVC generated for the recently closed DDL edition ...
> Iterative chaining allows for a cumulative record of IVCs, continuously protecting all prior submissions indefinitely, …

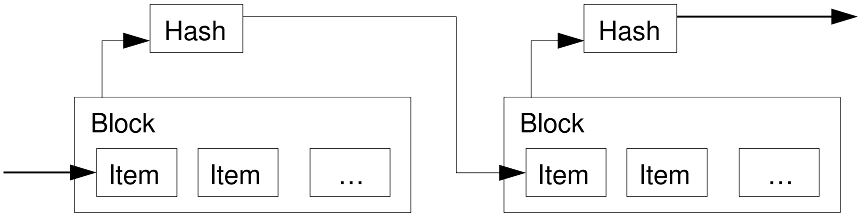
Excerpted from column 10, lines 44-50; column 21, lines 28-30; and column 21, lines 38-40.

Although the underlying enabling concept may be remarkably similar for Bitcoin and the ‘450 patent, the PEDDaL® system patents did not describe providing a financial ledger, which is what Bitcoin does. Instead, the PEDDaL® system focuses on establishing the ages of documents, and proving that they haven’t changed since the asserted date of existence.

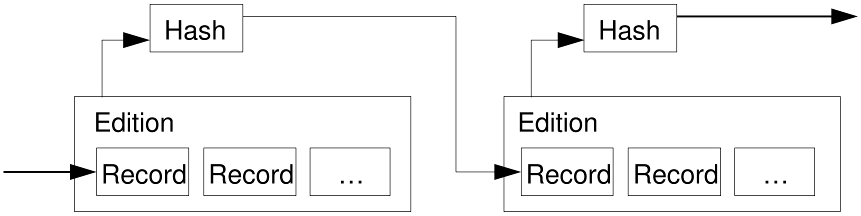
Bitcoin blockchaining. Figure copied from section 3 of Satoshi Nakamoto's 31 October 2008 paper.



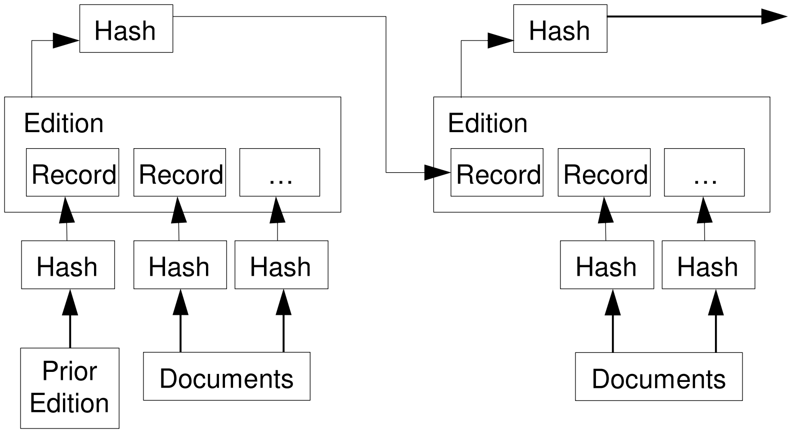
PEDDaL blockchaining, using Bitcoin terminology – no material difference. Hashing a subsequent block that is appended to the prior block's hash, is equivalent to hashing a subsequent block that includes the prior block's hash.



PEDDaL blockchaining, using terminology from the PEDDaL patents – functions the same as Bitcoin blockchaining.



PEDDaL blockchaining with additional items shown for clarity.



There are several applications of document age verification that can be covered with the patents and their continuations, including establishing the ages of website material. In some situations, it may be valuable for someone to find a website for which the substantive content meets some criteria for minimum age. Naturally, obviously real-time information, such as advertising, that may also appear on the website can be excluded from the date verification process by separating dated and undated content using appropriate html tags. The PEDDaL® system can be adapted for operation with internet browsers to alert users of date verification successes and failures for visited websites; the system can also be adapted for internet search engines that include age in website scoring or permit users to specify ages or dates of existence as search criteria.

PEDDaL® naturally helps protect intellectual property (IP) by establishing a provable date shortly after an invention idea was recorded in a document, even if there are no witnesses to that document's drafting. This can assist with insulating defendants from charges of back-dating documents that could be used to refute allegations of trade secret theft allegations or prove prior use rights in some patent-related lawsuits. The proper documents must exist, but if they do, PEDDaL® can establish their authenticity and age.

PEDDaL® can also resolve situations of forgery and document tampering. Consider, for example, a situation in which there are multiple parties to a contract, and all but one of the parties collude to disadvantage that one party, by identically altering their copies of the contract. The single party is outnumbered, and if there is a lawsuit, there is a risk that the court may incorrectly determine which version of the contract is authentic. Had the original copy of the contract document been registered with PEDDaL® shortly after signing, and the PEDDaL® record for that document distributed among the signatories, the true version of the contract could later be readily identified with little uncertainty or risk of mistake.

Using a related invention in the '501 patent, forgery detection can be extended to paper-only documents – without the need for any special paper, special ink, special printers, a trusted third party, or archiving any copies. This forgery detection is mathematical and is transferred through photocopying, faxing, and even scanning and reprinting an arbitrary number of times. So PEDDaL® proposes a wider variety of practical applications for blockchaining than does Bitcoin.

REFERENCES

[1] Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System," available at https://bitcoin.org/bitcoin.pdf

[2] See http://article.gmane.org/gmane.comp.encryption.general/12588/ for a dated announcement of the publication of the Nakamoto paper.

[3] Copies of US Patents and US Patent Application Publications are available at http://patft.uspto.gov/netahtml/PTO/srchnum.htm and http://pat2pdf.org/.