Who Invented Blockchaining - the Platform Technology for Bitcoin, PEDDaL® and Potentially Many Other Applications?

By Brian Johnson*

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. Copies of all related blockchain patents are available at www.patentmarketingllc.com.

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

* Chief Operating Officer, PEDDaL Operations; brian1337johnson@gmail.com

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.

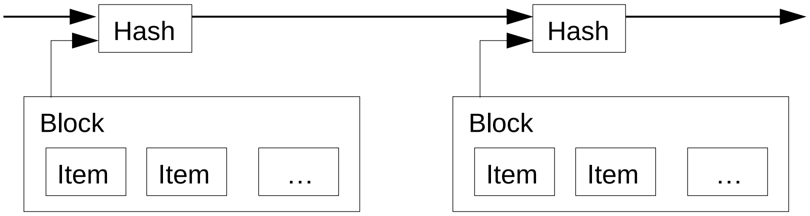

FIGURE 1: Bitcoin Blockchaining from 31 October 2008 Paper

Figure 1 shows how Satoshi Nakamoto describes blockchaining. As you can see, as each block is completed, it is "chained" to all earlier blocks using a one-way hash function operating on the combination of the prior block and the newly-completed block. This process then iterates with the stream of subsequent blocks.

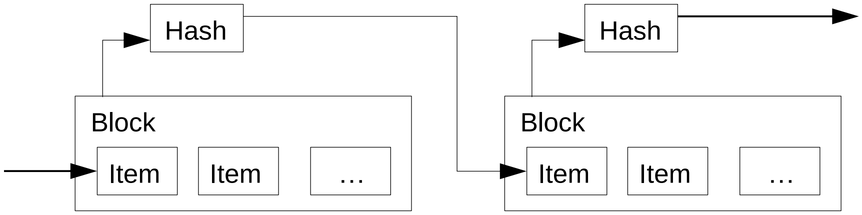

FIGURE 2: PEDDaL® Blockchaining with Bitcoin Terminology

Figure 2 shows how the PEDDaL® patents describe blockchaining, but using the Nakamoto terminology for a ready comparison with Figure 1. In the PEDDaL® system, the hash of the prior block is inserted into the current block. This is functionally equivalent to the Nakamoto blockchaining method, because the hash function operates on a data stream. Whether the data stream being hashed is two digital files appended together and sent to the hash function, or one digital file is inserted into another and the combination file is sent to the hash function, the same data is sent - and the same result is achieved. The two blocks are "chained" together the same, with either convention.

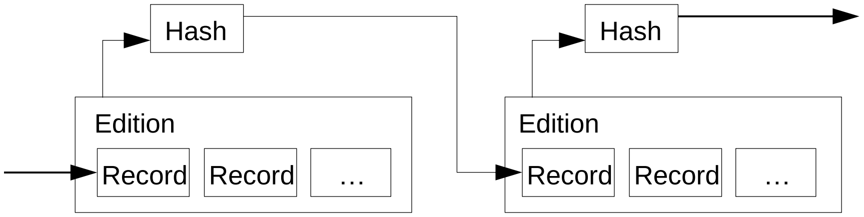

FIGURE 3: PEDDaL® Blockchaining with PEDDaL® Patent Terminology

Figure 3 is a repeat of Figure 2, but using the terminology from the PEDDaL® patents. PEDDaL® refers to the blocks as editions, and the items as PEDDaL® records.

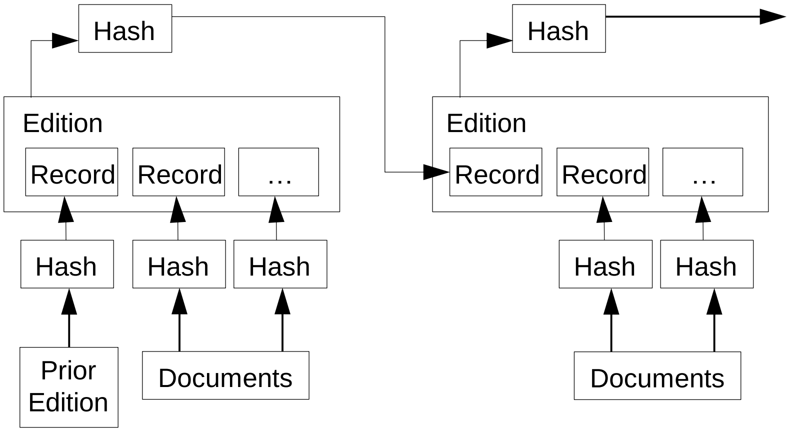

FIGURE 4: PEDDaL® Blockchaining with Enhanced Detail

Figure 4 adds more detail, to illustrate how documents are added to each edition in the blockchain. This process has been on-going since March of 2009.

PEDDaL® Applications Using Blockchaining

We have an on-going blockchain system that can prove both a "no-later-than" date of existence and also lack of any alterations since that date. This can be used to detect and deter forgery. For example, specific applications include:

-verifying the non-tampered age of any legally-significant documents, such as wills, contracts, and property listings

- verifying the non-tampered age of any documents stored in secrecy, such as engineering drawings and specifications describing inventions and trade secrets

-determining the ages of website material

--protect internet property as in establishing a verifiable discovery date and trade secret issues

-detect forgery on paper copies if the paper copy is registered in PEDDaL®.

The above examples only represent a small number of potential applications of the platform known as blockchaining. PEDDaL® is only one commercial application of the technology. As the inventor of blockchaining, as shown in the '450 patent, we believe that technology will find many uses, not the least of which is in banking and finance, smart contracts, stock transfers, real property transactions, validating ownership, digital currencies and the internet of things.

REFERENCES

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

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

[3] Copies of PEDDaL®/Bitcoin US Patents and US Patent Application Publications are available at http://www/patentmarketingllc.com