Haseltine Lake Kempner

The Patents Behind Blockchain

July 2020

In a recent review of blockchain patenting at the EPO we noted the rapid increase in numbers of patent applications related to developments in blockchain technology in the last couple of years.

Perhaps surprisingly, the basic idea of what is now called a blockchain has been outlined in patent applications since the early 1990s. Following a hiatus, the idea did not reappear in patent applications until some time after the publication of the 2008 "Bitcoin" paper by "Satoshi Nakamoto" (which can be found at here).

Blockchain Essentials

From the 2008 Bitcoin paper:

"The solution we propose begins with a timestamp server. A timestamp server works by taking a hash[1] of a block of items to be timestamped...The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it."

This core blockchain idea is found in US Patents Nos. 5136646 and 5136647 (= EP0541727), issued to Haber and Stornetta as inventors in 1992 with priority and filing dates of 9 March 1991 and 2 August 1990, respectively. These patents are related to a 1991 paper by Haber and Stornetta ("How to Time-Stamp a Digital Document", Journal of Cryptology, Vol. 3, No. 2, pp. 99—111, 1991) which is referenced in the 2008 Bitcoin paper along with a slightly later paper by Haber, Stornetta, and Bayer ("Improving the Efficiency and Reliability of Digital Time-Stamping", March 1992).

[1] This involves a cryptographic one-way hash function which takes an input of any number of bits and yields a so-called "hash" of the input which has a fixed number of bits (e.g. 256 bits). The function is such that (i) the hash cannot feasibly be "reverse-engineered" to recreate the input, (ii) the same input always produces the same hash, (iii) a change of even one bit of the input results in a different hash, and (iv) it is computationally infeasible to find two different inputs which yield the same hash.

According to Haber and Stornetta, whenever clients have documents to be time-stamped, they transmit requests containing hashes of the documents together with client IDs to a central time-stamping service. That service issues signed, sequentially numbered, time-stamp certificates. Each certificate consists of the sequence number, the time, the client ID, the hash of the document from the request and, crucially, linking information relating to the immediately previously issued certificate. This linking information holds the time, client ID, and document hash from the immediately previously issued certificate, together with a hash of the linking information from that previously issued certificate. This establishes a chain of linked, temporally sequential, time-stamp certificates. As stated in the 1992 paper: "In the linking solution, the hash values of documents submitted to a time-stamping service are chained together in a linear list into which nothing can feasibly be inserted or substituted and from which nothing can feasibly be deleted" and as set out in the 1991 paper: "Thus the only possible spoof is to prepare a fake chain of time-stamps, long enough to exhaust the most suspicious challenger that one anticipates".

The use of cryptographic one-way hash functions is essential for the Bitcoin proposal, as it is for the Haber and Stornetta proposal. US Patent 4908861, issued to Brachtl et al as inventors in 1990 with a priority/filing date in 1987, provides an example of a cryptographic one-way hash function.

The Haber and Stornetta proposal refers to an early hash function (known as "MD4"). The Bitcoin paper refers to a later hash function ("SHA 256") which is the subject of US Patent No. 6829355, issued to Lilly as inventor in 2004.

The Blockchain in Bitcoin

The 2008 Bitcoin paper says that "a hash of a block of items" is taken (each item being a transaction involving a transfer of Bitcoin from one owner to another). For this, the paper proposes the use of a "Merkle Tree" of hash values - roughly speaking, each individual item is hashed, then the hashes themselves hashed pairwise together until there is only one: the "root hash" or "Merkle Root". The Haber and Stornetta proposal also contemplates that several documents may be hashed together in a "Merkle Tree" but notes that, in this event, only the collection as a whole is time-stamped and not each individual document, which may be what is needed in some cases. US patent 4309569, issued in 1982 to Merkle as inventor, describes the "Merkle Tree".

The aim of the 2008 Bitcoin proposal is to keep parties' transactions anonymous. To this end, each party receives a public-private key pair. Parties use their public keys in transactions, but the private keys are kept anonymous so that the parties cannot be identified. Beyond that, an owner may use a different public-private key pair for each transaction to hide the fact that the same party is involved in a number of transactions.

US patent 4218582 (GB patent 2006580), issued to Hellman and Merkle as inventors in 1980, provides one example of a public-private key pair system.

Bitcoin is of course concerned with the specific application of a blockchain to provide a so-called "cryptocurrency". Though "cryptocurrency" is not a stated concern of the Haber and Stornetta proposal – the information in its "documents" could be anything, e.g. alphanumeric, audio, video, pictorial – it is mentioned that the information may relate to financial transactions. The Haber and Stornetta proposal is also not concerned with client anonymity.

Public or Private?

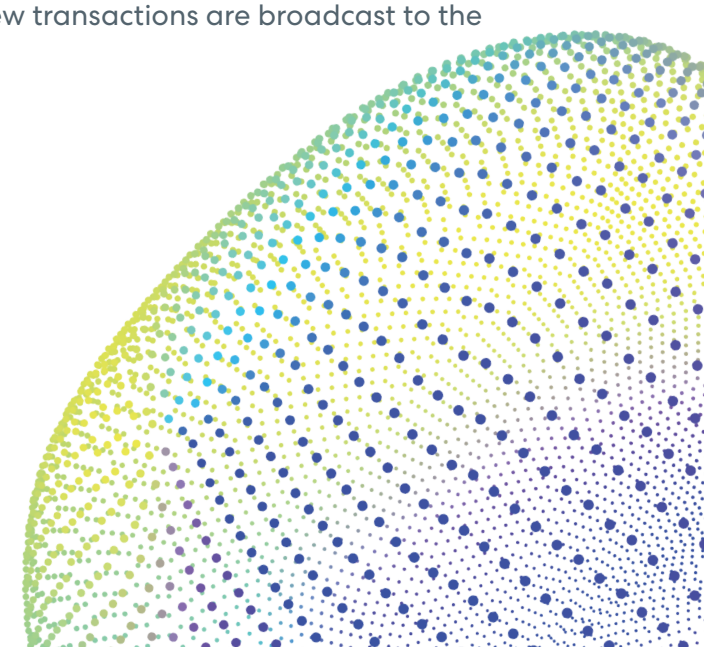
The basic Haber and Stornetta proposal, with its central time-stamping service, sets out a form of what might now be called a "private" blockchain. Haber and Stornetta do consider that there might be multiple time-stamping services, but the 2008 Bitcoin paper goes beyond that with a proposal "to implement a distributed timestamp server on a peer-to-peer basis..." or what would now be called a "public", distributed, blockchain.

Whether private or public, the core blockchain idea is as set out by Haber and Stornetta: a chain of linked, temporally sequential, time-stamped, blocks of data (whatever that data might represent). Different possibilities for managing blockchains can be built from this core idea. For example, the management of a private blockchain might be relatively easy, with some central authority determining who may produce new blocks and what blocks may be added to the chain, and who may inspect the blocks along the blockchain etc., whereas the management of a public, distributed, peer-to-peer blockchain presents a different challenge.

Managing a Public, Distributed, Peer-to-Peer Blockchain – the Bitcoin proposal

The Bitcoin proposal for maintaining a viable public, distributed, peer-to-peer blockchain is, beyond doubt, ingenious and has inspired many other alternative proposals since the Bitcoin paper was published.

In this context, "distributed" means that there are multiple copies of the blockchain distributed across a network. The sites that maintain these copies are called "nodes". New transactions are broadcast to the



network and received at these nodes. The nodes verify that the received transactions are correct and, by checking against the blockchain, which contains all earlier transactions, the nodes verify that the Bitcoin concerned has not already been spent. Some nodes function as "miners", which build and broadcast timestamped blocks of transactions for the potential addition to the blockchain (only when in a block which is added to the blockchain is a transaction finally effective).

"Public" means that anyone can inspect the blockchain. Anyone may establish a node, including a miner node.

"Peer-to-peer" means that all nodes are equal in the sense that no higher authority supervises nodes or timestamped blocks.

One critical issue recognised by the Bitcoin proposal is that if it is easy to create blocks then there might be a risk of the system being swamped by new blocks issued by miner nodes, or multiple different and competing chains of blocks could persist and subvert the system. Additionally, some nodes could be "dishonest" and provide fake blocks. This means that a mechanism is required for hindering the easy creation of blocks, including fakes, and to provide a basis for one version of the chain of blocks to be accepted as authoritative by all nodes.

Various possible mechanisms have been proposed since the Bitcoin paper was published but a proposal in the Bitcoin paper itself provides so-called "proof of work" as such a mechanism. "Proof of work" is an example of what is called a "client puzzle protocol" in accordance with which, broadly speaking, to obtain approval the "client" must solve a computationally difficult puzzle (the

"The Bitcoin proposal for maintaining a viable public, distributed, peer-to-peer blockchain is, beyond doubt, ingenious"

puzzle being such that it is easy to verify that the solution, once found, is correct). Typically, the approval might be approval to use some resource, e.g. to access a server or to send an email.

US patent 7197639 issued to Juels and Brainard as inventors in 2007, with a 1999 priority date, provides examples of "proof of work" client puzzle protocols.

In the Bitcoin proposal the approval is effectively authority for a miner to issue a new block for addition to the blockchain. The solution to the puzzle is included in the block, so that any other node can verify the solution as correct. If the solution is incorrect then the block will be rejected by the other nodes.

The need to solve the puzzle adds a (computational) cost to each block. This means that it is not easy for a miner to gain authority to issue a new block. Further, once the computational effort has been expended to make a block satisfy the proof-of-work, the block cannot be changed without redoing the work. If later blocks are chained after it, then the work to change the block would include redoing all the blocks after it. This hinders the ready creation of fake versions of the chain of blocks.

"Proof of work" is also the basis for the nodes to accept the longest chain as authoritative - because it has the greatest proof-of-work effort invested in it – and nodes will always work to extend the longest chain.

Should it happen that two miners broadcast different versions of the next block simultaneously, some nodes may receive one, or the other, first. In that case, each node works to extend the chain with the first block it received, but saves the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

The particular puzzle posed in the Bitcoin proposal is to take the hash of a block of transactions and find a number (a so-called

"nonce") which gives the block's hash a required number of (leading) zero bits. A similar proposal is called "Hashcash" and was made in 1997 and is referenced in the 2008 Bitcoin paper, but apparently never patented. The 2008 Bitcoin paper also references a related proposal, apparently made in 1998 and called "b-money", but again apparently never patented. The Bitcoin proposal provides that by varying the required number of leading zeros the difficulty of the puzzle can be increased or decreased, for instance to compensate for increasing hardware speed or varying interest in running nodes over time.

Who pays?

The infrastructure resources required to put a blockchain system into effect are not free which begs the question: "who pays?"

In the case of private blockchains, proprietors might be expected to pay for infrastructure. In the case of a public, distributed, peer-to-peer basis system, such as the Bitcoin system, the answer is not so simple. How are participants (e.g. miners and other nodes) incentivised to apply resources to the system?

The Bitcoin proposal provides that new Bitcoin are "created" as rewards for miners solving the proof-of-work puzzle and providing new blocks, apparently drawing on an idea from the "b-money" proposal. These rewards are the only source of new Bitcoin. The reward for solving the proof-of-work puzzle and providing a new block was originally 50 Bitcoin. Now, the reward is 6.25 Bitcoin[2]. A miner generally also receives a "transfer fee" for including a transaction in a block - only when a transaction is in a block which is added to the blockchain is the transaction effective, so there is an incentive to offer a fee to a miner. Otherwise, it might be a considerable time before any miner includes the transaction in a block.

It seems that, for the time being at least, nodes which are not miners receive no reward but are run effectively as a hobby. This may be a viable proposition so long as a sufficient number of people are prepared to provide nodes on this basis. However, below some number of nodes the Bitcoin network could be unacceptably vulnerable to attack.

Of course, there are many aspects of the Bitcoin proposal which have not been mentioned here and there are many other features of the rich Bitcoin ecology as it has developed (e.g. different "wallets", "exchanges" and blockchain explorers) that we consider to be beyond the scope of this article.

Conclusion

Bitcoin uses a blockchain, but many aspects of Bitcoin do not concern the core blockchain idea. The 2008 Bitcoin paper brought about renewed interest in the blockchain concept and its possible uses, not only for cryptocurrencies but in many other areas. As a result, many other proposals have been made, and increasing numbers of patent applications have been filed. We only expect the number of patent applications filed to blockchain technology to increase with time and indeed we are seeing applications being filed that utilise blockchain in areas such as network management protocols and the aerospace industry.

Contact us

Frances Wilding
Partner
fwilding@hlk-ip.com

Stuart Clarkson
Senior Associate
sclarkson@hlk-ip.com

[2] The present Bitcoin protocol provides that the reward is halved every 210,000 blocks which, if this protocol continues to be followed, means that there will only ever be 21 million Bitcoin. The reward halved from 12.5 Bitcoin per block to 6.25 Bitcoin per block on 11 May 2020 with the halving to 3.125 expected in 2024.