Blockchain in Vermont: A Primer

Jeremy A. Hansen, PhD
Certified Information Systems Security Professional
Assistant Professor of Computer Science

Norwich University, Northfield, VT 05663 USA
jeremyhansen@acm.org

Abstract. In this report, I describe the software protocol popularly referred to as "blockchain," which has attracted much attention for its ability to facilitate electronic contracts and other transactions in a decentralized environment. Section 1 begins with the history of blockchain and related technologies, and is followed by Section 2, which offers a brief overview of the specific components that make up the technology and what it is capable of. I describe some well-known risks inherent in the technology and its implementation in Section 3, then conclude with a high-level description of the cryptologic components involved. While I do not feel that blockchain itself is inherently interesting, the applications that it (as a foundational technology) enables are interesting. Today, Vermont has an opportunity to build the legal scaffolding upon which technologists and entrepreneurs can develop these applications.

1 Introduction and History

Physical signatures have provided verification of the authenticity of various legal transactions for thousands of years. More recently, computers have enabled several additional forms of transaction verification, including digital signatures. Digital signatures have been accepted for legal contracts for some time already, but the term has two distinct meanings. The first meaning is when users explicitly agree to legal terms or conditions by clicking a checkbox, a button, or otherwise makes known their acceptance of the terms of a transaction. These agreements do not require physical signatures, proof of identity, or any robust mechanisms for ensuring their authenticity. The second meaning covers a mathematical technique to provide for the *authenticity* of a document or other data. These digital signatures prove that a certain party signed the document and ensures that the signing party cannot later claim to not have done so. That is, the digital signatures provide *non-repudiation*. For the remainder of this document, I will only use the term digital signature with this second meaning. I discuss digital signatures in more technical detail in Section 4.1.

A *blockchain* is a distributed record of transactions whereby parties involved in an exchange certify and share their transaction with other participating parties, which in turn share the transaction more and more widely until the transaction is accepted as valid by the entire community of participating parties. Users

of a blockchain certify the authenticity of their transactions with digital signatures (as above), and other users of the blockchain verify and re-endorse past transactions by "chaining" their own transactions onto those of earlier users. This solution contrasts with "traditional" ledger systems that record transfers of property[1] in two important ways. First, no centralized repository maintains records. Second, rather than being a separate entity, currency transacted over the blockchain can exist *within* the blockchain ledger.

This distributed record was first introduced as an inseparable component of the digital currency Bitcoin to facilitate anonymous currency transactions, but has since been used for other digital currencies and in more general purpose applications.[2] Exactly what form the transactions take and how the participants interact with the blockchain is determined by a software protocol. Practically speaking, users may not change this protocol once it is set.[3]

2 Components and Capabilities

A blockchain is made up of four primary components: participants, transactions, blocks, and a protocol. The *protocol* describes how participants interact with one another, how blocks are created, and how transactions are incorporated into the blockchain. *Participants* are entities interested in either using the blockchain to record a transaction or to profit from some incentive mechanism designed into many blockchain protocols. Provided that a participant uses the protocol correctly and has a means of communicating with other participants, joining a blockchain is trivial.

Transactions are data stored within the distributed ledger, and in the case of the Bitcoin protocol, these transactions are transfers of currency ownership that are signed by the sender. Participants append new transactions to the chain of prior transactions. These updates are passed to other participants, which are forwarded and re-forwarded around the network of participants, until participants come to consensus on the entire chain of transactions. The protocol defines valid transactions, such as those that are digitally signed and do not involve *double spending*, or spending the same unit of digital currency twice. Participants using a blockchain can easily determine whether or not some transaction has been added. That determination is quite reliable, since changing the record of transactions is difficult[4] and becomes more difficult as time goes on. The protocol resolves any conflicts between mutually exclusive transactions that are appended to the block chain at roughly the same time.

Blocks assist with sequencing of transactions and measuring when they were added to prior transactions. They are produced in a manner prescribed by the protocol, such as through a *proof of work*, which may require a huge amount of computing power. For example, Bitcoin uses a proof of work system based

[1] Including currency, real estate, stock certificates, or goods.
[2] A general purpose example is Ethereum, found at `https://ethereum.org/`
[3] Not without a great deal of difficulty and coordination, anyway.
[4] See Section 3 for more details.

on the difficulty of computing cryptographic hash algorithms.[5] Participants who lend their computing power to producing blocks are called *miners*.

3 Risks

Users of blockchain protocols should be aware of two different types of risks: those within the protocol and those on participant computers. Attackers may compromise blockchain transactions after compromising participants' personal computers in the same way they do consumer bank accounts. Compromises of PCs are common and likely to remain this way, so developers building applications using a blockchain to record transactions must engineer security into these applications. We should not take this as any more an indication that blockchain itself is insecure than any other medium is insecure.[6]

Risks and drawbacks inherent to the blockchain exist, however:

1. Malicious participants with a large amount of processing power[7] are risks primarily to new blockchain instances or those instances with only a handful of participants. These participants can use their massive processing power to double spend currency without other participants detecting the behavior. They may also be able to block transactions and otherwise deny service to legitimate participants.
2. The blockchain is a file which must be transmitted from participant to participant and grows larger with every new transaction. With frequent use, the blockchain file may become very large and increasingly difficult to manage.[8]
3. Participants may be able to store illegal material in the blockchain as part of their transactions.
4. Mining of blocks can be incredibly energy-intensive. In 2014, high-efficiency miners consume about 240 kilowatt hours to produce one Bitcoin.[9]

4 The Cryptology, Briefly

4.1 Digital Signatures

A digital signature is a common operation that relies on an asymmetric pair of keys and a cryptographic hash algorithm to work properly. One key in the pair is the *public key* and the other is the *private key*. Data encrypted using one key may only be decrypted with the other. That is, if I encrypt a message with my private key, only the public key will decrypt the *ciphertext* and return the original message. The reverse holds true as well. This arrangement of keys

[5] See Section 4.2 for more about cryptographic hashing.
[6] True, badly-written applications themselves may contribute to insecurity, but a blockchain itself does not compromise security.
[7] Compared to the other participants on the blockchain.
[8] As of September 29, 2015, the Bitcoin blockchain is over 43 Gigabytes.
[9] `http://www.coindesk.com/carbon-footprint-bitcoin/`

is a cornerstone of the operation of *asymmetric encryption*. The mathematical properties that allow the keys to operate in this manner are found in *modular arithmetic* and *elliptic curves*. Cryptographic schemes using modular arithmetic include the RSA[10] algorithm, while those using elliptic curves include ECDSA.[11]

4.2 Cryptographic Hash Algorithms

Cryptographic hash algorithms produce "fingerprints" of messages called *hashes* in such a way that it is practically impossible[12] to determine the original message given a particular hash, and several other properties. These algorithms must satisfy three basic criteria to be considered useful: *collision resistance*, *preimage resistance*, and *second preimage resistance*. Finding the original message given a particular hash would be a violation of preimage resistance. Collision resistance ensures that it is practically impossible to find *any* two messages that produce the same hash. Second preimage resistance ensures that, given a message and its hash, it is practically impossible to find a second message that produces the same hash. When these properties are satisfied, the cryptographic algorithm can be used in a digital signature scheme to ensure that a message to be signed cannot be maliciously modified after the signature is in place.

5 Conclusion

The State of Vermont will not build the technical means to support blockchain applications, nor should it. At the same time, Vermont is in a position to drive the narrative for development and adoption of such applications. However, we should reject outright any proposals or solutions that require closed-source or proprietary products. The architects of the Internet decided early on that the technology must be open and available for use by all, and creativity flourished. The stage has not yet been set for blockchain, but a free and open stage in the same vein as the Internet will ensure that it remains a platform for all. I encourage you to help Vermont take the initiative with blockchain, including a clear mission of providing for the common good.

About the Author

Prof. Hansen's 2009 doctoral dissertation *A Four-Component Cryptographic Hash Framework* was an analysis of cryptographic hash algorithms, which underpin the digital signatures that blockchain uses. Later related research of his explored practical applications of (non-blockchain) digital currencies and peer-to-peer resource sharing between computers. In 2012, while running for Vermont's state Senate, he became one of the first candidates in the United States to accept Bitcoin for campaign contributions. He is an Assistant Professor of Computer Science at Norwich University and a member of the Selectboard of the Town of Berlin.

[10] The algorithm was named for the inventors Rivest, Shamir, and Adleman.

[11] Elliptic Curve Digital Signature Algorithm

[12] In cryptology, we often say "computationally infeasible" here, as it is *not* impossible to find violations of any of these properties. Doing so must remain measurably very difficult, though.