ITL BULLETIN FOR October 2018

One Block at a Time – Helping to Build Blockchain Knowledge

Dylan Yaga
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

One of the biggest questions today is: "What is blockchain?"

Depending on who you ask, the answer is wildly different. Some might answer that blockchain technology is completely useless compared to existing technologies while other might say it can solve every problem imaginable. The true answer lies somewhere in the middle.

Blockchain technology is new, hyped and is made up of a combination of complicated technologies. These facets combined lead to confusion, bad decisions, or missed opportunities.

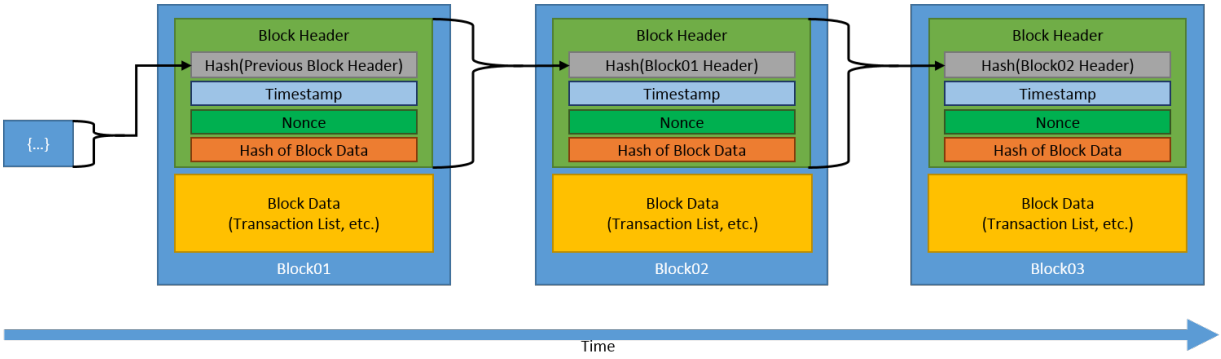
The problem was that there was no good, high level document presenting the topic neutrally. Most publications skew to one extreme or the other, never quite reaching the middle ground. Government agencies and organizations were dealing with many conflicting publications and asked NIST for help. NIST researchers began writing a draft report, which was released for public comment in January 2018. A substantial number of comments was received, including additional questions about blockchain or offering technical advice. After a long comment resolution period, NISTIR 8202 – Blockchain Technology Overview was published in October 2018.

Building a Foundation

NIST computer scientists investigated blockchain technologies and obtained firsthand experience with multiple blockchain platforms, their source code, and setting up development environments; additionally, NIST researchers collaborated with industry experts, as well as enthusiasts to leverage their expertise. The goal of this research and collaboration was to obtain the knowledge necessary to write a fundamental baseline document on blockchain technology. NISTIR 8202 attempts to present the topic of blockchain technology as simply and straightforward as possible. Each section builds on concepts introduced in previous sections. The introduction section sets the stage, presenting the scope of the document as well as the nomenclature for some terms up front. It was noted early on that the term "blockchain" itself was overloaded. It meant the ledger, the technology, an entire field of research, a network, as well as a specific instance of a technology. The authors attempt to be explicit in the document, by specifically using which aspect of the term "blockchain" meant.

Section 2 discusses the high-level categorization of blockchain technology: permissionless and permissioned. Since there are many different blockchain platforms, with many differing aspects, some distinction had to be made when discussing how they differ. These top two high level categories were chosen to help facilitate discussion throughout the remainder of the document. Although there are many more specific categories that could be utilized, those were not appropriate for a high-level document. Since one of the first choices is about who will be using the blockchain system, deciding if anyone (permissionless) can use it, or only select people (permissioned) is critical to the design and the choices made after.

Section 3 defines the high-level components of a blockchain network architecture, including cryptographic hash functions, transactions, asymmetric key cryptography, ledgers, blocks, and chaining blocks together. These are the fundamental building blocks of blockchain technologies. Understanding these concepts are key to understanding how the technology works. These sections make use of diagrams, tables and examples to help illustrate the concepts.



Section 4 discusses several consensus models employed by blockchain technology. Because blockchain technology is about users of a system collaboratively maintaining records instead of a central record keeper, a formalized method for adding records is critical. There are many ways to achieve this, and the document delves into several of the popular methods.

Section 5 introduces the concept of forking. Forking is the term used for updating blockchain software. There are two types of forking identified in the document, hard fork and soft fork. A hard fork of blockchain software is an update that is not backwards compatible; if a user wishes to continue operating with the other blockchain users they will need to adopt the update. A soft fork of blockchain software is an update that is backwards compatible, so updated and non-updated users can continue to operate together.

Section 6 discusses smart contracts. Blockchain-based smart contracts are executable code, which is stored on the blockchain ledger itself, and executed collaboratively by the blockchain users. Smart

contracts allow for business processes to be codified, and the results of execution to be recorded on the blockchain for the involved parties to see simultaneously, thereby reducing costs of data reconciliation.

Section 7 discusses several limitations as well as misconceptions surrounding blockchain technology. This section only scratches the surface of some questions, comments, and misconceptions that have been heard around this technology. It discusses the notions that use of a blockchain means cyber security practices are unnecessary; that blockchain use by itself can be a solution for identity management; and looks at the concept of trust in relation to governance, as well as in the technology itself.

Section 8 discusses various application considerations, as well as provides additional considerations from government, academia, and technology enthusiasts. This section is more of a resource to find additional papers to read. Some are very critical and ask the reader to critically think about whether blockchain technology is appropriate, others are a more interactive questionnaire set up to help evaluate whether there is a need for blockchain technology. The section also includes some considerations and situations where use of a blockchain may be appropriate.

Conclusion

The NIST blockchain technology program is growing. Researchers are investigating many aspects of the technology, such as decentralized security models, blockchain platforms and their compliance to Federal Information Processing Standards, potential areas of cybersecurity concern, smart contracts and their uses, and use of blockchain technologies for identity attribute management. The stage has been set, and NISTIR 8202 serves as the foundational document for additional research to build upon.

Additional Resource

NISITR 8202: Blockchain Technology Overview,
https://csrc.nist.gov/publications/detail/nistir/8202/final

ITL Bulletin Publisher: Elham Tabassi
Information Technology Laboratory
National Institute of Standards and Technology
Elham.tabassi@nist.gov