SOFTWARE AND VIRTUALIZATION

Blockchain – basics and beyond

In a blockchain, transactions are executed once and immutably recorded in a fault-tolerant and tamperproof manner. These properties make a blockchain ideal for a wide range of uses. However, blockchain technology is in its infancy and has shortcomings that must not be overlooked.

01

Yvonne-Anne Pignolet
Thomas Locher
ABB Corporate Research
Baden-Dättwil, Switzerland

yvonne-anne.pignolet@ch.abb.com
thomas.locher@ch.abb.com

A blockchain is a database that is replicated across multiple machines and used to maintain a continuously growing list of records. Records are compiled into so-called blocks, which contain a timestamp and a link to the previous block, thus forming a chain of blocks. The current high level of interest in blockchain technology is due to its desirable properties: Transactions are executed exactly once and an immutable record of all transactions is maintained in a fault-tolerant and tamperproof manner. Moreover, if the ledger is publicly available, anybody can verify the correctness of its records →1.

A blockchain is a database that is replicated across multiple machines and used to maintain a continuously growing list of records.

Traditionally, such features are powered through a trusted third party, which hosts multiple databases – for the sake of availability and fault tolerance – and vouches for the integrity of the stored data. The main disadvantage of relying on a third party is that trust is required in this party not to abuse its power and to provide its services faithfully. What is more, there is a risk that a malefactor could gain control over the third party and, for example, delete or modify records. In a blockchain, however, control is distributed, which makes the system much more resilient to malicious or inadvertent manipulation →2.

—
01 Blockchain transactions are executed just once and an immutable and tamperproof record of all transactions is maintained. This makes blockchain ideal for a wide range of applications in today's digital world. Probably the best-known application of blockchain technology is its use as a basis for cryptocurrencies, of which there are many.

Origin

The original blockchain is the foundation of Bitcoin, the world's first successful incarnation of a so-called virtual currency [1]. Bitcoin was proposed, in 2009, by "Satoshi Nakamoto" – a pseudonym. Satoshi's real identity is unknown and the name may even refer to several people. The blockchain that underpins Bitcoin is described in Satoshi's seminal work.

Unlike traditional currencies, virtual currencies are not controlled and regulated by banks and governments. Instead, control is decentralized and anybody in the world is free to join and dedicate (computational) resources to uphold the integrity of the system. Building a robust virtual currency is no small feat: If there is no centralized authority, such as a bank, who can prevent a malicious user from spending his or her virtual money multiple times? How can a seller be certain that a buyer has sufficient funds to purchase a chosen item? How can nonrepudiation of transactions be guaranteed? These questions hint at some of the crucial problems that any virtual currency must solve.

The Bitcoin blockchain addresses these issues by providing global consistency and serialization of transactions, ie, it defines for any two transactions which transaction occurred first. The additional key property of the Bitcoin blockchain is that the records are immutable, ie, recorded transactions cannot be altered or deleted →3.

02

Despite what some analysts claim, the blockchain concept is rather simple. In fact, the blockchain is of interest because it is simple yet offers several properties that are essential for many distributed applications. In short, the blockchain has the potential to simplify and automate processes for a wide range of use cases.

—

The current high level of interest in blockchain technology is due to its desirable properties.

Potential future use cases

The main difference between using a third party and a blockchain lies in the claim that the blockchain removes the need to trust any particular party. In other words, trust is shifted from a specific party to a distributed system and its embedded protocols. As a consequence, one needs to trust that the majority of the parties involved in maintaining the ledger follow the protocols, ensuring that the ledger operations are carried out as intended and the remaining (malicious) entities cannot corrupt the system.

An entry is submitted to the blockchain

—
02 The distributed nature of blockchain control makes it ideal for tracking and verifying all sorts of transactions – for example smart contract execution.

—
03 Blockchain principles.

Since trust is a valuable and crucial commodity in any distributed system, it comes as no surprise that numerous use cases for blockchain technology, other than virtual currencies, have been proposed and are being investigated by ABB as well as many other companies. Most proposals can be classified into three categories, of increasing complexity:

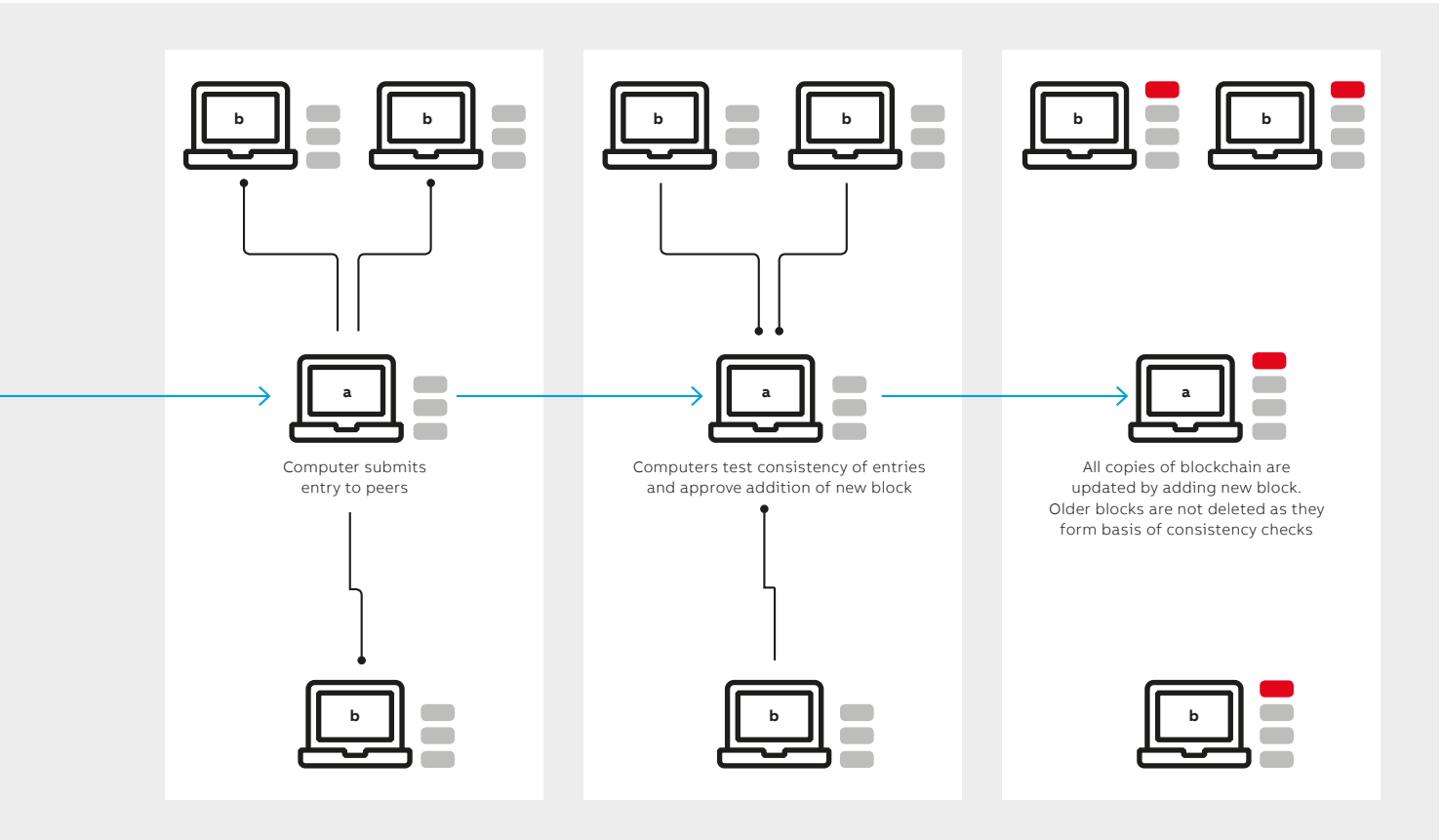
—

The Bitcoin blockchain provides global consistency and serialization of transactions, as well as record immutability.

1. Registry service:
   Storing digital records in an immutable and auditable distributed ledger.
2. Asset exchange:
   Asset creation and ownership transfer.
3. Smart contract execution:
   Automate business processes through the execution of code.

The information stored in the blockchain can represent physical or digital assets, identities, transactions, or contracts. A protocol governs how entries are created, validated, recorded, and distributed. For the applications belonging to the first category above, the blockchain is used as a ledger to record important facts and events such as births, marriages, deaths, property deeds, intellectual property, election results, legal decisions, financial investments, insurance policies or medical history →**4**. For such registry services, the main appeal is that records stored in the blockchain are immutable and that they can potentially be used across organizational boundaries (with data protection and privacy mechanisms in place). The ability to share records across boundaries is viewed as an especially important prerequisite for digitization in the financial and medical industries as well as for governmental services. This capability could be of great interest for ABB.

In the second category, banks are particularly interested in the exchange of (digital) assets, the facilitation of cross-border payments, and trade in stocks, derivatives and options. In the industrial arena, transactions that change the ownership of, or provide access to, physical goods can be carried out on a blockchain. Use cases being discussed here include tracking parties involved in a supply chain and decentralized approaches to access control.



One step beyond transactions are so-called smart contracts, a distributed protocol that executes the terms of a contract autonomously, with the aim of reducing the risk of error and manipulation. It has been proposed to add support for smart contracts on top of a blockchain: The contract would be stored in the blockchain in the form of executable code. When a smart contract is executed, the blockchain network members run the executable code according to the terms agreed upon in the contract. Since each execution starts with the same initial state, this automatic and distributed execution ensures consensus on the result among all members that execute the contract correctly. Smart contracts offer the potential for new financial instruments, parameterized insurance contracts and other services combining a shared database with the means for verifiable calculations or automated approval processes between two or more participants without trusted third parties. For example, smart contracts are envisioned to facilitate energy exchange and trading – both activities for which ABB supplies solutions →5.

04

While use cases are often described in terms of their potential compared to the state of the art – eg, by outlining potential cost savings – there is little discussion on how well the blockchain fits the given use case. In other words, the discussion as to whether or not a blockchain can be used to transfer trust from key parties to a distributed system is often missing. One needs to analyze carefully if a blockchain approach can resolve trust issues or if other, more traditional methods – eg, distributed databases – can provide the same benefits.

It has been proposed to add support for smart contracts on top of a blockchain. These could facilitate, eg, energy trading.

Challenges and limitations

Apart from the many advantages and great potential of blockchain technology, there are also some challenges that may hinder its adoption. In particular, lack of flexibility is a serious limitation as modifying the underlying protocols and implementations is almost impossible because any change must be adopted universally. If some participants update their protocols and some do not, a so-called fork of the chain is created, essentially creating two (conflicting) realities. Thus, massive coordination is required among all major participants before any change is possible. This limitation even holds for minor implementation bugs – some bugs in the Bitcoin blockchain implementation were identified a long time ago and are still not fixed. In addition to this rigidity, a further drawback is the fact that blockchain approaches suffer from limited scalability possibilities with respect to the number of users and the number of items to be appended per time unit. For example, the Bitcoin blockchain has a new block added every ten minutes, which corresponds to a growth rate of around 8 GB per year. While this number looks small enough in the light of modern computing resources, it also implies that the number of transactions is fixed to about seven per second, which is far too low for a global transaction system.

—
04 A blockchain can reliably register a whole range of important records such as personal, financial and legal data as well as intellectual property information, election results or medical history.

—
05 Smart contracts enabled by blockchain technology could revolutionize the world of energy exchange and trading.

—
Reference
[1] www.bitcoin.org

05

As mentioned above, any suggested change must find a majority of participants to support it, so there is no quick fix for this issue around the corner. Moreover, the energy consumed maintaining the Bitcoin blockchain is massive – and rising, as it relies on a proof-of-work approach that continually ramps up the computational power needed to compute a new block. The energy consumption is currently estimated to be of the order of the production capability of two nuclear power plants.

—

One needs to analyze if a blockchain approach can resolve trust issues or if more traditional methods can provide the same benefits.

While the basic idea behind blockchain immutability is sound, there are many potential modes of attack on the implementation and application sides that require attention. For example, Bitcoin wallets are vulnerable to theft, packets can be sniffed, distributed denial-of-service attacks could be mounted, etc. Furthermore, it is not possible to prevent an attacker who controls more than 50 percent of the blockchain computational power from controlling the blockchain itself. Such an attacker can even undo past transactions.

A significant amount of research is being invested to mitigate these limitations. The lack of flexibility can be addressed by putting control over the blockchain protocols into the hands of a consortium. In this case, the consortium, but no individual party, must be trusted. The expensive proof-of-work mechanism can be replaced with a much more energy-efficient approach based on distributed consensus algorithms (the Hyperledger project is a noteworthy example). It remains to be seen if a blockchain-based system can be implemented that overcomes the most crucial current limitations while preserving the features that make blockchains interesting in the first place.

Blockchain's future

On the application level, the hype around blockchain technology has led to inflated expectations. A closer look at many proposed use cases reveals that trust is a key prerequisite for their success. However, it is not always possible to resolve trust issues with a blockchain-based approach. In general, blockchain technology is no silver bullet. Each use case requires a carefully implemented solution that can benefit from concepts used in Bitcoin or blockchains. Blockchain technology is still in its infancy and has obvious shortcomings that, despite all the hype, must not be overlooked. It is worthwhile for ABB to observe the ongoing development as innovations will most likely bring the blockchain technology to a level of maturity that will unlock its business potential to automate and simplify processes in the industrial domain. ●