Blockchain Enabled Cyber-Physical Systems

Subjects: Computer Science, Theory & Methods

Contributor: Heena Rathore , , Mohsen Guizani

Cyber-physical systems (CPS) is a setup that controls and monitors the physical world around us. The advancement of these systems needs to incorporate an unequivocal spotlight on making these systems efficient. Blockchains and their inherent combination of consensus algorithms, distributed data storage, and secure protocols can be utilized to build robustness and reliability in these systems. Blockchain is the underlying technology behind bitcoins and it provides a decentralized framework to validate transactions and ensure that they cannot be modified.

healthcare smart grids cyber-physical systems bitcoin blockchain

1. Blockchain Technology

The hacking of over a billion Yahoo accounts [1], the Equifax data breach [2], and increased ransomware attacks [3] are just a few of many reported cyber attack incidents in recent years. As a matter of fact, over one million cyber threats are released every day and by 2020, over 200 million IoT devices [4] will need security. Some industry experts anticipate this number to reach 29 billion in the next couple of years. Blockchain, a distributed system to manage transactions, which uses consensus among network participants to build trust, is being considered as a viable alternative to protect against cyber-attacks. Such distributed systems have many advantages as compared to centralized systems, which fail to scale as the number of connected devices increases. In [5], authors outlined how a chain of cryptographically secured blocks can be used to preserve and protect the integrity of past information [5]. The idea of proof-of-work was established in 1993 as a countermeasure to the proliferation of spam and other system abuses. Later in 2008, a white-paper [6] was released which established the foundation of bitcoin, a cryptocurrency based on the concept of blockchain. This triggered new research in this emerging topic that achieved significant milestones, such as the adoption of smart contracts based ethereum [7], application in the financial industry, and mention in the Harvard Business Review as a basic and fundamental innovation for financial industries. Today, there is a robust and fast-growing ecosystem encompassing blockchain, and an increased number of applications are migrating towards a decentralized approach for securing transactions. While blockchain was originally developed for cyber-only applications, over time, applications that combine both cyber and physical aspects are also benefiting from this concept.

1.1. Blockchain Explanation

A blockchain is an immutable distributed database to which new time-stamped transactions can be appended and grouped into a hash-chain of blocks [8]. The underlying blockchain protocol defines how multiple copies of such

blocks can be constructed and maintained in a distributed fashion. A key aspect of this protocol is deciding how a network of participants, known as miners, can establish consensus on the current state of the blockchain. This algorithm assumes that, in any given time epoch, only a fraction of the miners could turn malicious or faulty. There are different types of blockchain architectures (i.e., public, private, permissioned, and permission-less). A public blockchain is one that allows anyone to join. They are usually permission-less where all the users have equal rights. A private blockchain is a closed blockchain where privacy is important. Here, every participating node is pre-selected and vetted. They are permissioned and the users do not have equal rights in the network. One of the first, and still popular, permission-less blockchain protocol is bitcoin [6]. Every 10 minutes, on average, it selects a new miner in an unbiased fashion who then gets the right to commit or append a new block to the blockchain. The key question to be determined is who adds the next chain of transactions and how is it added. There are two prevailing strategies for the same, namely Proof of Work (PoW) and Proof of Stake (PoS). In simple terms, consider a situation where P1 wants to pay P2. P1 first announces its intent and then provides authenticity by signing the transaction using a cryptographic key. The Network operators, or miners, validate the authenticity of the digital signatures and availability of assets. Once these tasks are complete, the new transactions are added to the blockchain. Each block contains a unique code called a hash, which also contains the hash of the previous blocks in the chain, and is used to connect the blocks together in a specific order. Any miner has to perform a set of computations to establish their credibility as a leader. These computations solve a puzzle to map arbitrary size data to a fixed size. In any network, a leader can be chosen in one of these two ways. In Proof of Work (PoW), many miners try to solve the puzzle and the one that finishes first, broadcasts to the group proof that the work is done. Other miners then validate that the work done is correct. Once everyone confirms this, they select that particular miner as the leader. This approach is computationally expensive because many miners are trying to solve the puzzle simultaneously, until one of them succeeds.

The typical top level view of blockchain is shown in **Figure 1**. Here, once the transaction is requested, a data structure for keeping the set of transactions is distributed to all nodes in the network. All the nodes perform the block verification process before adding anything to the blockchain structure. Once the nodes do the block verification, they receive reward for the proof of work. Likewise, each new node joining the distributed system of blockchain gets a full copy of the blockchain. When another block is made, it is sent to every node inside the blockchain framework. At that point, every node confirms the block and checks whether the data expressed there is right. If everything is correct, the block is added to the local blockchain in every node.

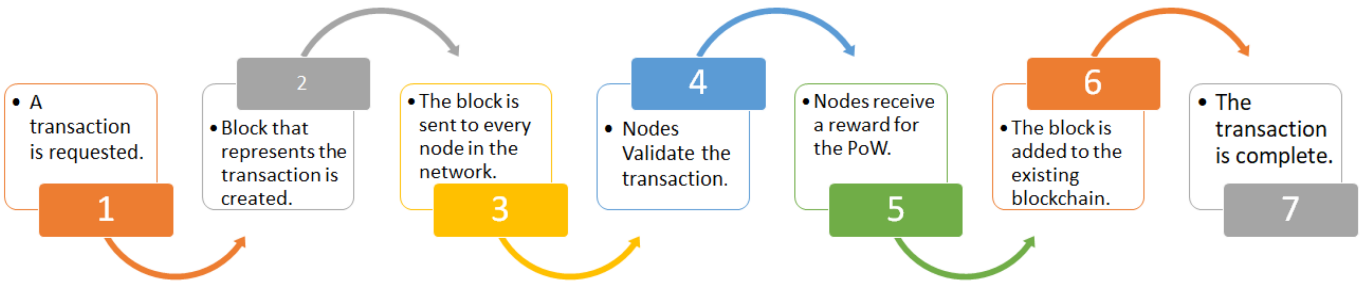

Figure 1. Blockchain process.

The second method of doing this is called PoS. In this method, a leader, who has the highest amount of stake in the network, is selected. The amount of stake in the network is determined by the number of coins that the miner owns. This is based on the theory that the miner with a lot of stake in the network is most likely, to be honest. The rest of the network then implicitly accepts this leader by attaching its block to the leaders' block. This maintains the longevity of consensus in bitcoin. The protocol also defines a reward mechanism as PoW involves significant computation, which also leads to one of the significant shortcomings related to scalability and transaction throughput. **Figure 2** shows the illustration of transaction records of blockchain.

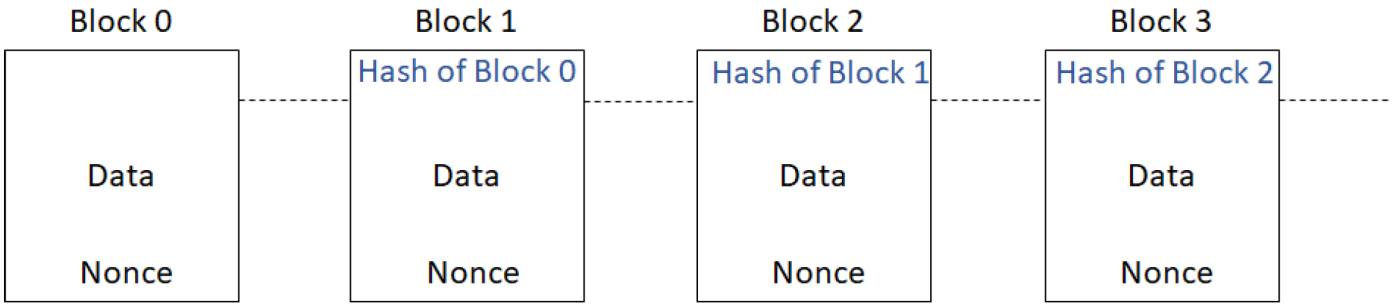

Figure 2. Blockchain: A chain of blocks where each node references the previous block. POW = Proof of Work.

The primary purpose of the block is to maintain a list of verified transactions using a cryptographic hash function. The hash function is efficient because of the following properties:

- It generates an output of fixed length irrespective of the length of the input.
- It is deterministic which means that it generates the same output for a given input.
- It is irreversible which means that getting the same input from the output is not possible.
- Any slight perturbations to the original input generate new output.
- The hash computations are fast with minimal overhead.

The blocks in the blockchain are linked to the very first genesis block and are verified by the hashes. All the blocks are connected through the relationships of all their hashes, which means each block contains the previous hash, and these get further hashed in the next block. Any changes to the hash cause the chain to be broken because the original hash is still attached to the next block in the chain. Recalculating the original hash to restore the chain requires an enormous amount of computing power. In addition, nonce is added so that the miners can play with the data to produce a hash which outputs three leading zeroes, as shown in **Figure 3**. Once the miners have found a nonce that results in their block's hash being below the difficulty threshold, the block is finally considered valid, and it can be broadcast to the network with that miner taking a reward for their effort.

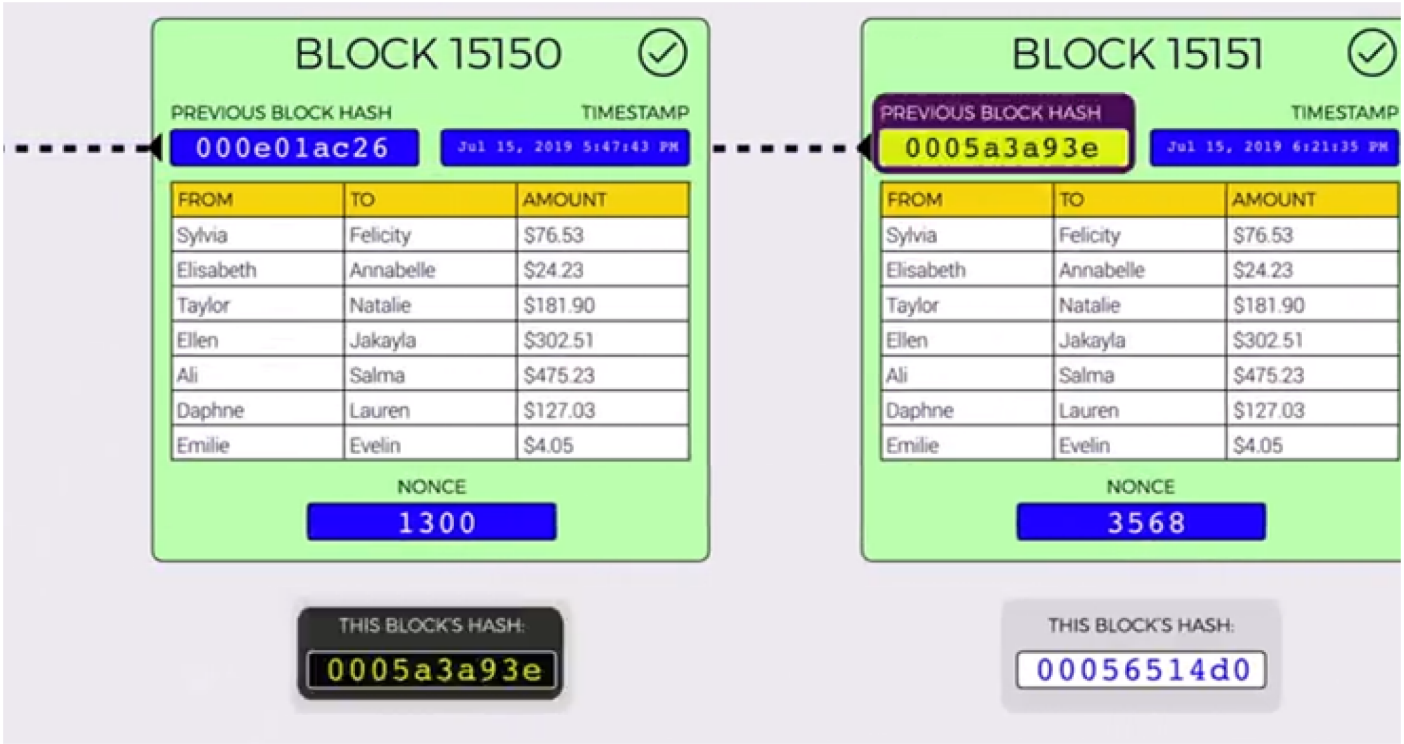

Figure 3. Chain of blocks.

A possible attack scenario in such a chain is that an attacker can alter the contents of the database and creates another chain of records by producing another set of transaction records. However, the action of changing anything in the chain has a domino effect, thereby invalidating all the blocks that follow. If a transaction on the chain is altered by a hacker, it invalidates the entire block, thereby requiring the network miners to repeat the task of finding a nonce that yields a hash value below the target difficulty. This makes the blockchain as the most revolutionary technology that is not only efficient but also the most secure among all the other state of art technologies.

Public blockchain architectures, such as bitcoin and ethereum, are open source and are permission-less. These types of blockchain architectures allow anyone to download the code, demonstrate proof of work, and earn the right to validate the transactions in the network. This type of architecture is open and transparent. Private blockchain architecture on the other hand, examples of which are R3 [9] and EWF [10], operate under the leadership. It is a type of semi-distributed architecture with permissioned read and/or write authority. This type of architecture is faster and has pre-approved participants with known identities.

1.2. Understanding Blockchain Using Financial Transaction as An Example

Normally, whenever two people want to transfer money among each other, they require a centralized authority, such as a bank, to manage the transactions entered in the bank logs, managed as a database. In other words, to establish trust between two people who typically know each other, the researchers depend on an external third party, such as a bank. In order to avoid this, the concept of blockchain came into the picture. Consider, a situation, wherein there are ten individuals who do not want to use a bank to record the exchange of currency amongst

themselves. They mutually agree to have constant access to each other's accounts, without knowing the other's identity. To start with, everyone has an empty folder. As time progresses, each of these 10 individuals will add transactions to their folder and a historical record of these transactions is maintained on a ledger. Let us suppose that person number 2 wants to send $10 to person number 9. To make the transaction, everyone checks whether person number 2 has sufficient balance to transfer $10 to person number 9. If she does, everyone makes a note of the transaction on their blank page. Transactions keep happening within the network and everyone keeps writing them down until their pages get filled. When this happens, everyone puts the page away in their folders, bring out a new page and start the whole process over again. The magic of blockchain lies when the page has to be put away in the folder. The deal is that when the page goes in the folder, everyone's version of the page must look the same and it must not be modified ever in the future. To accomplish this, everyone needs to seal the contents of the page, which is accomplished by using the hash function, as described earlier. In this case, the hash function outputs a number with three leading zeros and it does so by trying various inputs. Thus, to seal a page containing a list of transactions, the researchers need to figure out a number, which when appended to the list of transactions and fed to the machine, gives a code that starts with three leading zeros, as shown in **Figure 4**.

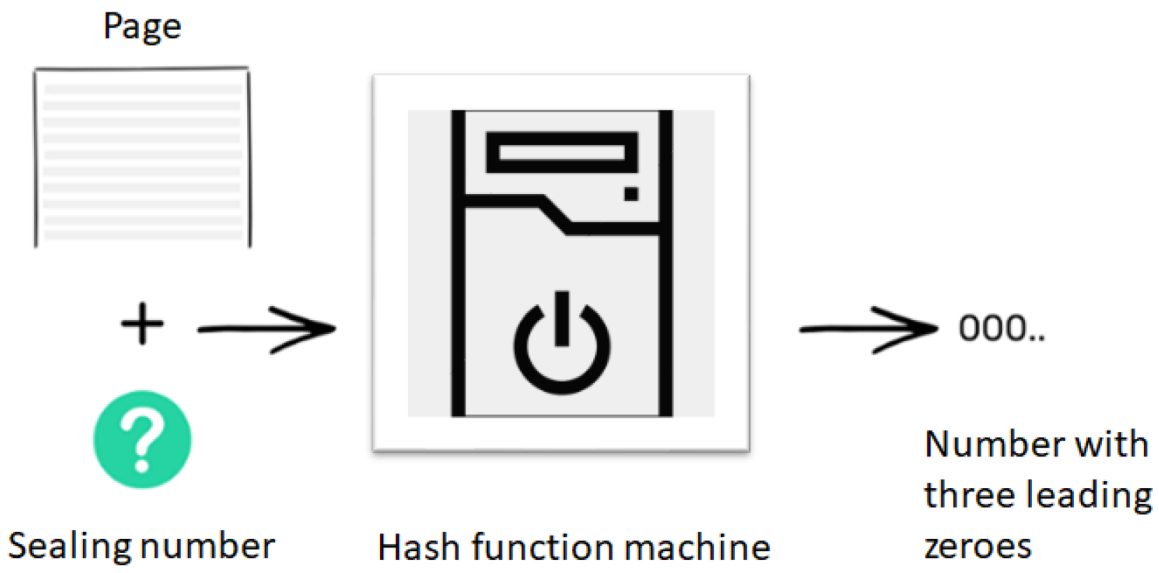

Figure 4. Hash function machine generating sealing number.

This step is done when there is no more room on the page to add new transactions. A sealing number for the page is calculated by everyone in the network. The network participant who figures this out first announces the sealing number to other members of the network. Once this event happens, all the other network participants verify that the hash number announced is valid. If it is, then the participant is chosen as a miner and everyone else seals their page with this same number and places it in their folder. In addition, every page in the blockchain depends on its previous page. If a hacker tries to modify a historical page, then the contents and sealing number of all subsequent pages would have to be modified in order to keep the chain consistent. This process of adjusting several pages and calculating new sealing numbers is time-consuming and provides a strong deterrent to doing so. **Figure 5**

shows if the hacker tries to modify the content the chain is shorter than the original chain. This is on the because from the page the untrustworthy person attempts to cheat, he would make another chain in the system, however that chain be unable to make up for becoming the legit chain—simply in light of the fact that one person's speed can't beat combined speed of other people in the network, hence guaranteeing that the longest chain in a network is the honest chain. In addition, other members of the network are quickly alerted about a potential threat from one of the members in case this happens.

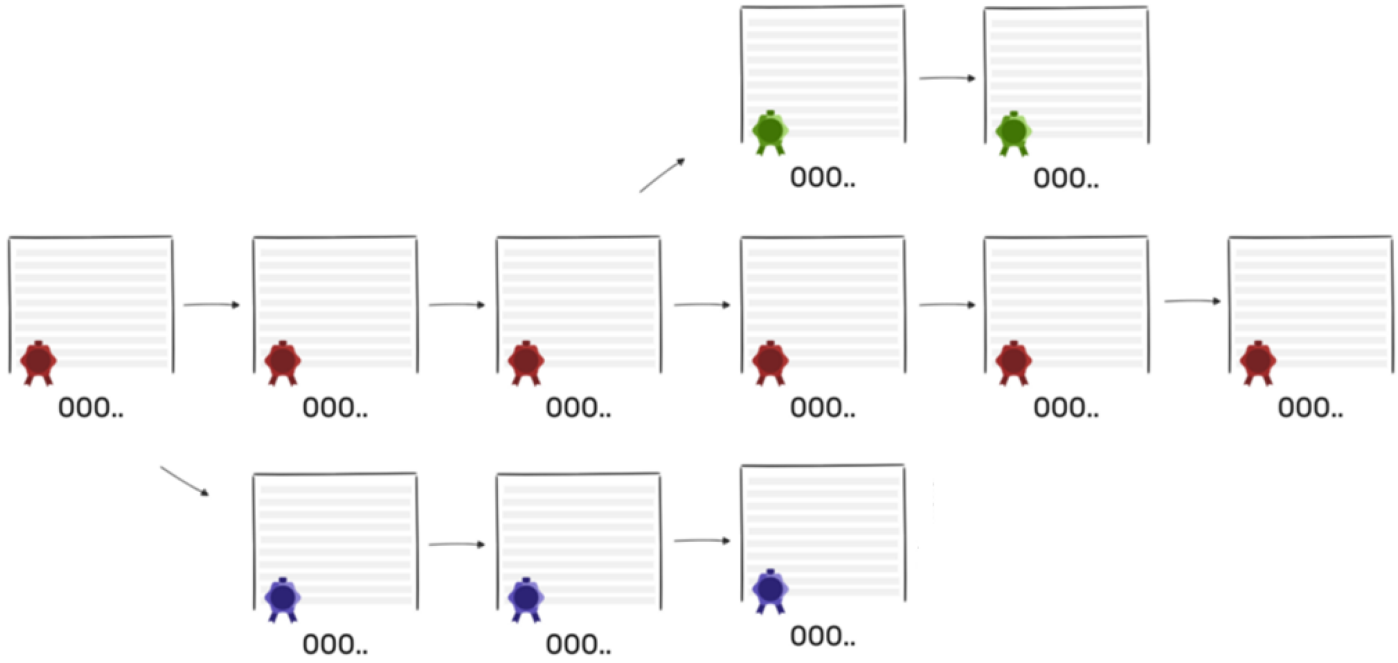

Figure 5. Longest chain in the network is the honest chain. Red is the honest chain. Green and blue are dishonest chains.

1.3. Benefits of Blockchain

Blockchain has several advantages, such as it is one of the most secure ways of recording and authorizing information stored on the network. It is also a transparent storage mechanism where anyone on the network can verify the authenticity of the information. Furthermore, the data that is stored on the network cannot be changed without incurring huge overheads, which makes it secure and efficient. Blockchain transactions typically contain a peer-based proof, either of validity or authorization, instead of relying on a centralized application as an enforcer of constraints. It is a type of replicated and shared that is synchronized across members of the network. It records the transactions, such as the exchange of assets or data, among the participants in the network. It acts as a consensus mechanism ensuring that nodes that independently verify and process transactions stay in sync. There are some differences between blockchain and traditional centralized databases which are listed below:

- Since transactions propagate between nodes in a peer-to-peer fashion, blockchain uses a public-private cryptography scheme, such as Elliptic Curve Digital Signature Algorithm (ECDSA) [11], to digitally sign each transaction. However, it is computationally expensive to generate and verify these signatures. Additionally, due

to the lack of sufficient randomness during the signature process, a hacker can recover the user's private keys, thereby making the scheme more prone to attacks, especially since it is done by all the peers [12].

- In a distributed database, arriving at consensus among network members is a computationally intensive effort. Additionally, it also involves significant back-and-forth communication, depending on the consensus mechanism used. The consensus mechanism has 51% vulnerability, which means a single miner with more than 50% of the total hashing power can unilaterally launch an attack. This is practically impossible when the network size is large. Such attacks are less likely in a centralized database, even though they also have to contend with conflicting and aborted transactions.

- Whereas there is some level of redundancy in a centralized database, it is far less as compared to a blockchain which must process every transaction by every node independently to achieve better security and transparency.

2. Blockchain Applications for Cyber-Physical Systems (CPS)

With the growth in acceptance of computers over the past few decades, records have mostly migrated from being physical paper documents to digitized versions, created and managed on a computer.

This is one of the many cyber applications, the ones enabled by computers. While such records are created and stored on computers, it still involves a human being entering the information. Financial transactions, health records, insurance records are some of the many examples in this category. So, one can say that humans were still the primary source of data collection in these applications. Over the past few years, fueled by the emergence of IoT and driven by the proliferation of sensing technology, sensors are now replacing humans as the primary source of data collection in many systems. Such systems, called CPS, combine physical processes, software, and communication to provide an integrated system with abstractions, design, and analysis capabilities. The technology spans research across multiple disciplines, having core components, such as embedded systems, real time communication, computer, networking, and physical systems dynamics. The use of blockchain for making a financial transaction has been well researched and documented. Advances in this technology have helped in sending money directly to the authorized people without including centralized authorities. Application of blockchain as smart contracts minimizes the possibility of delays, suppression, or any other outside influence. It applies comprehensive financial security, monitors the terms of the contract and is unbreakable. It also makes it easier to track and monitor digital identities using blockchain. The usage of blockchain as a cheap notary system has been described in [13], thereby avoiding different types of scams by creating unique certificates which would be easy to verify. In similar lines, a recent review of blockchain in education is given in [14]. This entry mainly focuses on an emerging application of blockchain for cyber-only systems, namely health records and four representative applications of CPS, namely implantable medical devices, industrial control systems, smart grid systems, and connected cars (**Figure 6**). **Table 1** outlines the application domains of various systems discussed in the entry, along with the societal impact in each system.

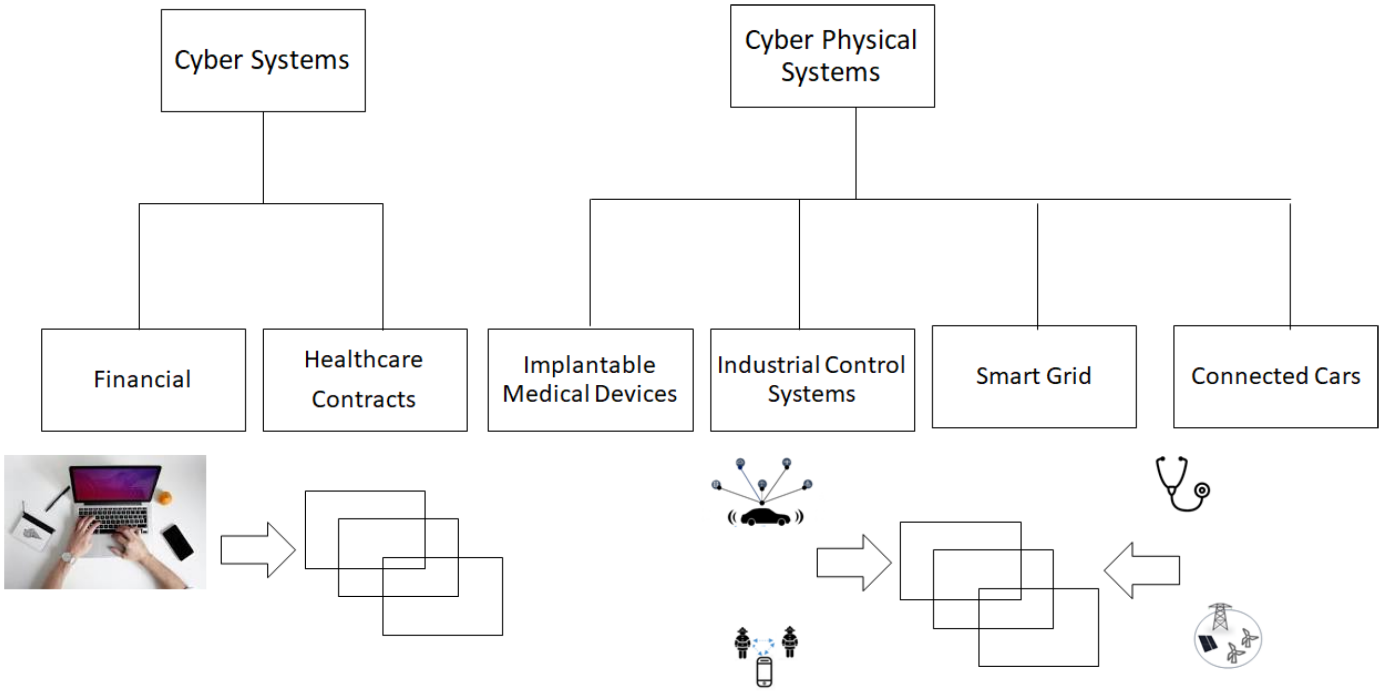

Figure 6. Four applications of CPS.

Table 1. Application domains of CPS.

Systems	Applications	Societal Impact
Healthcare	Medical devices, health management networks	World class medicine and health care systems
Transportation	Automotive electronics, railroad systems, vehicular networks, aviation and airspace management	Zero automative traffic fatalities, reduced traffic congestion and delays
Industrial Control Systems	Physical infrastructure monitoring and control	Maximum yield and performance
Smart Grids	Electricity generation and distribution, building and environmental control	Blackout free electricity and distribution, environmental benefits

References

1. Smith, K.T.; Smith, M.; Smith, J.L. Case studies of cybercrime and its impact on marketing activity and shareholder value. Acad. Mark. Stud. J. 2011, 15, 67.

2. Gressin, S. The Equifax Data Breach: What to Do; Federal Trade Commission: Washington, DC, USA, 2017.
3. Brewer, R. Ransomware attacks: Detection, prevention and cure. Netw. Secur. 2016, 2016, 5–9.
4. Evans, D. The Internet of Things How the Next Evolution of the Internet Is Changing Everything. Cisco White Paper 2011. Available online: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (accessed on 1 January 2020).
5. Haber, S.; Stornetta, W.S. How to time-stamp a digital document. In Proceedings of the Conference on the Theory and Application of Cryptography, Santa Barbara, CA, USA, 11–15 August 1990; Springer: Berlin/Heidelberg, Germany, 1990; pp. 437–455.
6. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System; ResearchGate: Berlin, Germany, 2008.
7. Wood, G. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Proj. Yellow Pap. 2014, 151, 1–32.
8. Coron, J.S.; Dodis, Y.; Malinaud, C.; Puniya, P. Merkle-Damgård revisited: How to construct a hash function. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2015; Springer: Berlin/Heidelberg, Germany, 2005; pp. 430–448.
9. Ghafarian, A.; Seno, S.A.H. Exploring Digital Forensics Tools in Backtrack 5.0 r3. In Proceedings of the International Conference on Security and Management (SAM), Las Vegas, NV, USA, 21–24 July 2014.
10. Goranović, A.; Meisel, M.; Fotiadis, L.; Wilker, S.; Treytl, A.; Sauter, T. Blockchain applications in microgrids an overview of current projects and concepts. In Proceedings of the IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society, Beijing, China, 29 October–1 November 2017; pp. 6153–6158.
11. Hankerson, D.; Menezes, A.J.; Vanstone, S. Guide to Elliptic Curve Cryptography; Springer Science and Business Media: Berlin/Heidelberg, Germany, 2006.
12. Mayer, H. Ecdsa Security in Bitcoin and Ethereum: A Research Survey. 2016. Available online: http://blog.coinfabrik.com/wp-content/uploads/2016/06/ECDSA-Security-inBitcoin-and-Ethereum-a-Research-Survey.pdf (accessed on 1 January 2020).
13. Arredondo, A. Blockchain and Certificate Authority Cryptography for an Asynchronous on-Line Public Notary System. Ph.D. Thesis, The University of Texas, Austin, TX, USA, 2018.
14. Fernández-Caramés, T.M.; Fraga-Lamas, P. Towards Next Generation Teaching, Learning, and Context-Aware Applications for Higher Education: A Review on Blockchain, IoT, Fog and Edge Computing Enabled Smart Campuses and Universities. Appl. Sci. 2019, 9, 4479.