In Thank You for Being Late, Thomas Friedman states that we are moving into an “age of accelerations” that will transform “almost every aspect of modern life.”

Examples of this transformation are everywhere. Consider a basic one: computing power’s exponential increase has led to dizzying improvements in performance that, in turn, have enabled faster transaction speeds. Tasks that previously took milliseconds now take microseconds.

The Internet of Things (IoT) fosters acceleration—in the form of large-scale sensing, big data generation, and unprecedented parallel computing—by interconnecting a seemingly limitless number of devices, sensors, and other objects. However, trusted timing mechanisms must coordinate events in networks of things (NoTs) to make NoTs practical. For example, a global timing mechanism is necessary to synchronize data-flows and workflows in most NoTs because of the things’ potential geographic distribution. In addition, malicious owners of specific objects could deliberately modify NoT efficiency by tampering with the times data is allowed to flow to and from NoT computations. This clearly violates a central goal of net neutrality: to prohibit certain ISPs from deliberately slowing down or speeding up data uploads.

**NEED FOR TRUSTED TIMESTAMPs**

Businesses and governments have long sought the ability to link provably secure, publicly verifiable trusted timestamps to activities and transactions as evidence. Numerous use cases rely on such evidence, ranging from validating the time of creation and modification of a document to creating patents to financial accounting. “Establishing the time when a digital signature was generated is often a critical consideration,” notes Elaine Barker in NIST Special Publication 800-102. “With the
appropriate use of digital signature-based timestamps from a Trusted Timestamp Authority (TTA) and/or verifier-supplied data that is included in the signed message, the signatory can provide some level of assurance about the time that the message was signed. Beyond legal and financial accounting considerations, research by the EU Agency for Network and Information Security (ENISA) shows that trusted timestamps make services significantly more efficient and cost-effective.

For geographically distributed systems lacking global governance such as the IoT and blockchain databases, trusted guarantees of the times events occur are especially important because markets operate on a first-come, first-serve basis, and trusted timestamps can serve as a fair basis for precisely determining where and when transactions originated.

**TIMESTAMPING SECURITY RISKS**

Unfortunately, current protocols rely on a central TTA or timestamping authority (TSA) to issue timestamps, as Figure 1 shows. This provides security for individual transactions but raises reliability concerns because the integrity of the timestamping process is inevitably bound to that of the TSA. If the TSA is compromised, all of the issued timestamps can become invalid, compromising the trustworthiness of the signed data. A December 2013 survey by ENISA of 51 TSAs across 20 EU member states revealed five major security risks to timestamping services. Table 1 lists the risk, impact, probability, and deviation values (on a scale of 0 to 100) of each risk, and Figure 2 graphically depicts the impact and probability values. TSAs rank loss or compromise of a service’s signature creation date as the scenario having the biggest impact, compromise of the main time source as having the highest risk, and unavailability of the main time source as the most probable. Moreover, dependency on a single TSA raises concerns in the research and business communities about potential abuse of that service by its administrative authority, which could be either a government or private entity.

**BLOCKCHAIN TECHNOLOGY**

Can we do better? Is there a secure mechanism available that can prevent timestamping services from being secretly subverted while also allowing multiple TSAs to offer services without any geographic or other boundaries? We believe the answer is yes, and that the solution lies in recent advances in digital cryptocurrency systems.

The past few years have seen widespread adoption of bitcoin, a
digital cryptocurrency and payment system that relies upon a decentralized peer-to-peer network with thousands of distributed nodes. Any computing device connected to the network with the appropriate software can participate in the system. As Figure 3 shows, bitcoin transactions occur directly between users, without a central administrator, and are recorded in a blockchain—a ledger of publicly verifiable digital signatures shared among all nodes. Many believe that blockchain technology is what makes bitcoin and other bitcoin-inspired virtual currencies so successful.

Researchers have suggested harnessing the bitcoin blockchain to make timestamping services more secure. One application of such a service for timestamping, Proof of Existence (proofofexistence.com), was introduced in 2012.

Using blockchain protocols has the advantage of empowering multiple parties to validate timestamps but is computationally expensive and requires numerous network interactions. Moreover, there’s no direct incentive for mutually trusted independent parties to cooperate, which has limited adoption of decentralized timestamping approaches.

Furthermore, relying solely on bitcoin or any other public blockchain scheme to maintain timestamps has clear security risks: any such system can be subverted when the majority of the participating nodes (CPUs in the case of bitcoin) are subverted. Thus, a blockchain ledger won’t be provably secure, rendering the timestamps unreliable for many use cases.

Any blockchain protocol can verify a digital signature but not necessarily the timestamp used by the signature or reported by the generating entity. A public ledger can offer proof of existence based on when the timestamp was received by the rest of the network nodes and the timestamps of the previous and next transactions, but all of that information depends on the public ledger shared among the nodes and their corresponding uncertified and potentially conflicting timestamps.

**AN INTEGRATED APPROACH**

We believe that a provably secure timestamping system could be achieved by combining the trustworthiness and accuracy that come from having a set of trusted centralized timestamping authorities with the open, decentralized nature of blockchain protocols. Specifically, one or more public or private TSAs that offer trusted timestamping services would embed their timestamping data inside a publicly maintained blockchain ledger such as bitcoin.

These TSAs would issue digital signatures for timestamps as they receive them and publish them in the next block using the previous blockchain hash as part of their certificate-issuing process for the data. Thus, instead of signing a hash value of the data, they’ll sign a concatenation of the hash of the data and the previous blockchain hash. Both the hash of the blockchain block used and the certificate are returned to the customer for proof of timestamping.

Because the produced TSA timestamping becomes “part” of the public ledger, there would be publicly available

---

**TABLE 1. Timestamping security risks.**

<table>
<thead>
<tr>
<th>Risk type</th>
<th>Risk value</th>
<th>Impact value</th>
<th>Probability value</th>
<th>Deviation value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss or compromise of service’s signature creation data</td>
<td>38</td>
<td>100</td>
<td>22</td>
<td>59</td>
</tr>
<tr>
<td>Loss or alteration of evidence in chain of trust</td>
<td>37</td>
<td>51</td>
<td>39</td>
<td>68</td>
</tr>
<tr>
<td>Compromise of the main time source</td>
<td>58</td>
<td>51</td>
<td>47</td>
<td>98</td>
</tr>
<tr>
<td>Loss of accuracy of the main time source</td>
<td>47</td>
<td>37</td>
<td>60</td>
<td>94</td>
</tr>
<tr>
<td>Unavailability of the main time source</td>
<td>52</td>
<td>37</td>
<td>63</td>
<td>100</td>
</tr>
</tbody>
</table>

*All values are on a scale of 0 (minimum) to 100 (maximum).*
proof of knowledge of timestamped transactions if any TSAs were compromised. Having their transactions as part of a public ledger would also let TSAs detect a certificate compromise or leak by looking for nonauthorized transactions in the public ledger.

A side benefit of having TSAs validate timestamps in a blockchain protocol is that historical transactions stored in the blockchain are also protected: even if the majority of the blockchain nodes get subverted, they can’t modify past transactions because they’ll be “chained” with timestamping data that can be independently verified. TSAs that detect an invalid block created by attackers who refuse to provide a trusted timestamp for that block can alert the rest of the network to the inconsistency, thereby acting as sentinels for blockchain integrity.

Existing TSAs can still issue trusted timestamps for transactions, but all the data hashes are concatenated and their corresponding signatures will become part of the blockchain ledger and merged with other timestamped transactions coming from other TSAs. Binding timestamps to other transactions and their timestamps provides security in case of certificate loss or misuse. Should this occur, the time of the last valid transaction is made public, all future transactions become invalid for that certificate inside the blockchain, and a new certificate is issued.

An alternative implementation is to have TSAs form their own trusted blockchain without tethering their data to bitcoin or some other widely used digital currency system. To comply with industry best practices as well as regulatory requirements, the TSAs would become accountable for their timestamping signatures through an auditable public ledger. However, this implementation comes with a tradeoff: although it retains more control of pertinent timestamping data, there’s also higher probability of subversion given that TSAs and regulatory auditors might be the only blockchain participants due to the lack of incentive for other parties to participate.

Tethering TSA transactions to existing blockchain protocols has two important side benefits. First, it will make applications that rely on trusted, real-world time more reliable and secure by preventing attackers who might overpower the network from altering historical blocks. Second, the use of trusted timestamps by multiple TSAs can give rise to blockchain designs that use proof of knowledge instead of traditional proof of work or of storage. This can be used to slow down aggressive nodes that try to overwhelm computational or network capacity.

Currently, trusted timestamping processes are specified in Internet Engineering Task Force (IETF) RFC 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol, and the American National Standards Institute (ANSI) X9.95 standard for trusted timestamps, which expands on RFC 3161 by adding data-level security requirements to ensure data integrity. The newer ANSI X9.95 standard is used by financial institutions and regulatory bodies to create trustworthy timestamps that can’t be altered without detection. However, both specifications describe processes that require a central TSA to issue timestamps and ensure their validity.

The ultimate aim will be to extend NIST Special Publication 800-102 to cover those use cases where a TSA can participate in blockchain architectures by providing on-demand or periodic verifiable information or by including hashes inside blocks that can be further signed and disseminated by the blockchain participants. From a practical standpoint, this could be implemented using a network service leveraging the ANSI X9.95 standard for trusted timestamps but still remain compatible with the widely used RFC 3161 for older servers.

As more things become interconnected in the IoT, there’s a growing need for provably secure timestamps to establish transaction precedence whenever race
conditions or tampering with past events are possible. Integrating time-stamping services with blockchain technology provides a novel means to accomplish this by combining the reliability of recognized TSAs with the openness and flexibility of a decentralized public ledger. Verifying time at increasingly smaller time scales is a challenge that might require distributed synchronization of multiple TSAs.

REFERENCES

ANGELOS STAVROU is an associate professor in the Department of Computer Science and director of the Center for Assurance Research and Engineering (CARE) at the Volgenau School of Engineering, George Mason University. Contact him at astavrou@gmu.edu.

JEFFREY VOAS, Cybertrust column editor, is an IEEE Fellow. Contact him at jvoas@ieee.org.