Software Engineering Institute
Carnegie Mellon University

# OBSIDIAN: SECURE CODING IN BLOCKCHAIN

October 2017


### EXECUTIVE SUMMARY

Blockchain technology, while only a few years old, has captured the imagination of businesses and governments around the world. It provides an authenticated, highly tamper resistant messaging system that is robust to attack and maintains a history of every single transaction that has taken place. In the government sector, the Department of Defense is examining the use of blockchain technology in managing electronic medical records, supply chain logistics, financial transactions, and resilient communications. Yet, as with all new technologies, there is room for improvement. Current tools used to create blockchain-based software are both very difficult to use and very easy to use incorrectly, a bad combination. The multi-million dollar thefts mentioned earlier are a testament to the gravity of this problem.

Our team at the Software Engineering Institute is working with the Carnegie Mellon University School of Computer Science to create a novel blockchain programming language we've named Obsidian specifically tailored to be both easy to use and hard to use incorrectly. By creating a secure-by-design language that renders certain types of bugs impossible to create, we aim to significantly reduce the risk inherent in the adoption of blockchain technology.


## Blockchain overview

Blockchain technology, at its heart, is a simple distributed ledger which tracks transactions between parties. This simple description belies the enormous interest in the technology; governments and industries across the globe are rushing to understand how to apply this new technology. While blockchain has gained significant popularity due to its role in cryptocurrency, industries as disparate as supply chain management, identification and authentication management, health care records management, and records storage of all types stand to be disrupted by blockchain.

Intrinsic to blockchain applications are four properties that are the root of all interest in the technology. Blockchain data is *shared*, making the system both robust to attack and resilient to disruption. Blockchain data is *authenticated*, which when combined with an electronic ID system links all transactions on the system to a real individual. The system is easily *auditable*, with all of history able to be recalled and reviewed at any time. Lastly, blockchain data is extremely *tamper-resistant*, in almost all cases to the point of impossibility. These highly desirable properties have led to the defense sector has identifying a number of potential use cases for blockchain technology. DHS recently distributed $400,000 to four blockchain companies to investigate the use of blockchain in identity management and privacy protection [1,2]. DARPA recently a program researching the applicability of blockchain technology to secure, resilient messaging [3]. The Office of the Assistant Secretary of Defense for Readiness recently put out a BAA which included research into the applicability of blockchain technology in training and readiness programs [4].

While there are many blockchain platforms being developed for general use, virtually all existing blockchain applications exist on the Ethereum blockchain. Programmers create "smart contracts"—a term used to describe blockchain-based applications (BBAs)—using a special-purpose language called Solidity. These BBAs are then deployed to the Ethereum blockchain where users can take advantage of their functionality.

## Obsidian: motivation and design

Unfortunately, these early applications have served to demonstrate the difficulty of BBA development. These difficulties have been highlighted in a number of high-profile hacking incidents where tens of millions of dollars were stolen by hackers who found coding errors in deployed Solidity programs (e.g., [5]). Research has highlighted these challenges [6] but as of yet tooling has not been created to address these shortcomings. The majority of the bugs relate to nuances of blockchain development; not properly coding the system's current state, not properly tracking money as it flows through the system, or not checking that a particular transaction is valid.

Our team at the Software Engineering Institute is working with the Carnegie Mellon University School of Computer Science to create a novel blockchain programming language we've named Obsidian specifically tailored to be both easy to use and hard to use incorrectly. We have followed a human-centric design philosophy to inform language design choices. This has allowed us to identify what types of features most programmers expect from a language, as well as which secure design patterns feel most natural and intuitive. Our language has introduced "state" as a first-class object, which removes an entire class of bugs by ensuring that certain functions only occur at certain times. For example, if we develop a voting application, it may have the states "Unregistered", "RegisteredNotVoted", and "RegisteredVoted". Forcing the developer to consider all application states at design time reduces the risk that, for example, an unregistered user can vote, or a user can vote twice. We have also introduced a much more robust mechanism by which currency is handled, enabling the software itself to notify the developer if money is being lost or double-spent.

Obsidian is currently under active development. Future work includes a broad set of user testing, including testing with specific subsets of users that are likely to be future blockchain developers, such as business analysts. We will modify the language based on the findings from these user tests. We are also looking to develop BBAs with government partners to ensure the language is strong enough for practical development. Our goal is to creating a secure-by-design language that renders certain types of bugs impossible to create, through which we can significantly reduce the risk inherent in the adoption of blockchain technology.

## References

[1]: News Release: DHS S&T Awards $1.3 Million to Small Businesses for Cyber Security Research and Development (link)
[2]: Applicability of Blockchain Technology to Privacy Respecting Identity Management (link)
[3]: DARPA Seeks Blockchain Messaging System for Battlefield Use (link)

[4]: adlnet.gov, BAA, section titled “ADL Focus Area: Learning analytics and performance modeling” (link)
[5]: Quartz., “A coding error led to $30 million in ethereum being stolen” (link)
[6]: “Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab” (link)

## Contact Information

Eliezer Kanal
Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

**Phone**: 412-268-5204
**Email**: ekanal@sei.cmu.edu
**Web**: www.sei.cmu.edu | www.cert.org