Summary of the Confidentiality and Privacy Report

Mike Ward

November 14, 2016

Summary of the Confidentiality and Privacy Report

R3's recent report, by Danny Yang, Jack Gavigan and Zooko Wilcox, evaluates the current state and surrounding theory of privacy and confidentiality in the various blockchain (or distributed ledger) systems.

Blockchain technology is widely believed to be capable of driving innovation across a range of industries. Before the technology can reach its potential, however, the issues of confidentiality (protecting *data* from unauthorized third parties) and privacy (protection from intrusion into the identity of parties to transactions) must be addressed. These requirements are fundamental to the financial industry and are driven by a variety of legislative, regulatory and contractual obligations.

The report provides a brief overview of the underlying technologies that enable privacy and confidentiality (P&C). It does this, however, in a largely untechnical manner that allows the reader to grasp the concepts without needing to delve into underlying proofs.

A simple framework used in the report is the CIA triad: confidentiality, integrity and availability. Security specialists maintain that each of these areas requires a trade-off to another. Public and private blockchain implementations are the simplest approach to managing the trade-offs of this triad, but each come with their own cost. The accessibility of Bitcoin and Ethereum, along with the broad adoption of public platforms, have both contributed to the significant work in the public blockchain space towards gaining further P&C qualities through applying advanced techniques in cryptography.

In the document, several different applications of blockchain-related technology are explored. The potential of these applications is explained in further detail in the report and include the following:

- The ability to commit to a specific data set publicly, while not revealing the data, but still holding proof of such commitment
- Creating transfers of assets, notably bitcoin, while attempting to ensure there is no trail of spend that can identify the asset owner
- Ensuring reminting scenarios do not occur with negative outputs in UTXO transactions while retaining no visibility into outputted amounts
- Creating a signature with a group of possible signers, without revealing which member of the group created the signature
- Supporting anonymous voting, while preventing voters from voting twice
- Allow a party to prove to another a statement is true without revealing any information underlying information about how it arrives at such a proof

A good portion of the report addresses existing attempts at implementing privacy on a blockchain. A lot of work has been done with applied cryptography in the cryptocurrency space in order to gain qualities of P&C seen in private blockchains while retaining the strengths of a public network.

In public blockchains, counterparties are only identified by their public keys (commonly referred to as Bitcoin addresses or Ethereum accounts). There is no formal mechanism for identifying the person who controls a given public key. However, if information leaks lead to specific individuals, it begins to open up patterns not only of their spend, but of those they interact with.

Several cryptocurrencies have arisen with the main objective to enforce certain characteristics of privacy and confidentiality. While none have arisen as a primary alternative, each has a set of trade-offs in either its CIA characteristics or simply in its liquidity. Monero, as an example, uses the CryptoNote protocol which combines ring signatures with other keys holding the same number of funds.

Bitcoin, as the largest of the cryptocurrencies, has seen several active projects to add further P&C. However, with a fixed protocol, these implementations often involve the use of sidechains or other technologies that run in parallel to Bitcoin.

The cost of P&C can often be found in performance. For example, the ability to leverage zero-knowledge proofs (ZKP) requires an interactive querying between parties in several queries. With each query, the confidence increases but the performance suffers, thus increasing the transaction cost.

Recently, however, we have seen a practical implementation of ZKP with Zcash. Zcash leverages zk-SNARKs, a recently-invented type of zero-knowledge proofs that requires no interactive querying. It contains a unique ledger model to support this capability, making it incompatible with the Bitcoin system. Zcash is yet unproven and exposes several new potential points of failure, such as 'trusted setup,' and does not yet possess a liquid market.

The final section of the paper deals with smart contracts, defined as computer programs that embody a self-executing and -enforcing contract to which users may become party. Smart contract P&C is a much newer field of exploration, and as such, it has only a small number of active projects applying advanced techniques.

Ethereum is the most well-known platform that implements smart contracts. However, because Ethereum's smart contracts are stored on a public blockchain, their underlying code, along with their state and all inputs and outputs, can be read and analyzed by anyone.

Hawk is a framework originally designed to complement the Zerocash protocol for creating private smart contracts. It achieves this by creating a public contract, which runs on the public blockchain, and a private contract, which is executed "off-chain." As is typical, there is a trade-off which, for Hawk, requires a "manager" to execute the private contract.

Enigma is another alternative that is a decentralized computation platform for processing encrypted data. In its current form, Enigma is primarily a protocol for enabling distributed processing of confidential data, as opposed to a smart contract protocol. No implementation has been released yet, and we have not yet seen whether Enigma could be adapted to provide support for smart contracts in the same way that Hawk does.

The guidelines for the security industry broadly look to proven solutions that have been tested at length in an open forum. With the newness of blockchain-related technologies, little such testing has occurred. However, in the public blockchain space, several applied theories are being run in production that will provide battle-tested validity of the technologies.

This paper successfully enables the reader to logically understand the trade-offs and technologies, so he or she can make informed decisions in order to have the most private and confidential platform for his or her needs.