digital currency initiative

Discreet Log Contracts. The idea of "Smart Contracts" is one of the exciting promises of digital currency technology, yet the difficulty of getting real world data into the blockchain brings many projects back to similar trust models as the current systems. Trusted oracles are needed to report on real world events and determine the outcomes of smart contracts, and this power can be abused. Discreet Log Contracts (DLC) are a new type of smart contract which limits the information gained and influence of oracles, and can run on the very limited scripting system present in Bitcoin, without the need for more complex languages such as in Ethereum.

Problem. As an illustration of the problems with overly powerful oracles, consider a smart contract which pays out the monetary value of 1000 barrels of oil. This futures contract can be implemented as a 2-of-3 multi signature address, where the 3 signers are the buyer, the seller, and the oracle. The buyer and seller both fund the address at the start of the contract and agree upon an oracle. At the end of the contract, if the buyer and seller agree on the price of oil, they can both sign off on the redistribution of funds without the need for the oracle. In the case of a dispute, however, either party can approach the oracle and request the oracle to sign off on the correct redistribution based on the current price. This is possible but presents problems: the oracle has full visibility and control over the outcome of the contract. Either seller or buyer can attempt to bribe the oracle so that the oracle distributes the funds to themselves. While legal agreements may mitigate this risk, a smart contract system provides little value if it needs to be backed up by external legal systems.

Our Solution. Discreet Log Contracts use a novel cryptographic signature scheme and off-chain transactions introduced in the Lightning Network to reduce the visibility of the contracts and reduce the oracle's influence. The same futures contract using DLC would have only 2 participants: the buyer and seller. The oracle would report the price of oil at the closing date, but would not be aware that the contract exists. In fact, nobody looking at the blockchain after the contract has executed could observe the details of the contract, or that a contract had executed at all; the transaction is indistinguishable from a payment. DLCs can also be layered on top of the Lightning Network so that they occur off-chain, and only the final result of many different contracts is recorded on the blockchain.

Applications and next steps. The DLC protocol can be used for a wide variety of contracts, covering most cases where payouts between parties depend on a publicly known number in the future. We are in the process of implementing futures contracts settled in Bitcoin. Another area for research addresses peer discovery. Before two users can create a contract, they need to find each other. Initially this can be done with centralized matching engines, which would hold no custody of user funds. Fair decentralized peer discovery and matching is a topic for future research.