b-money

Wei Dai

1998

I am fascinated by Tim May's crypto-anarchy. Unlike the communities traditionally associated with the word "anarchy", in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It's a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations.

Until now it's not clear, even theoretically, how such a community could operate. A community is defined by the cooperation of its participants, and efficient cooperation requires a medium of exchange (money) and a way to enforce contracts. Traditionally these services have been provided by the government or government sponsored institutions and only to legal entities. In this article I describe a protocol by which these services can be provided to and by untraceable entities.

I will actually describe two protocols. The first one is impractical, because it makes heavy use of a synchronous and unjammable anonymous broadcast channel. However it will motivate the second, more practical protocol. In both cases I will assume the existence of an untraceable network, where senders and receivers are identified only by digital pseudonyms (i.e. public keys) and every messages is signed by its sender and encrypted to its receiver.

In the first protocol, every participant maintains a (separate) database of how much money belongs to each pseudonym. These accounts collectively define the ownership of money, and how these accounts are updated is the subject of this protocol.

1. The creation of money. Anyone can create money by broadcasting the solution to a previously unsolved computational problem. The only conditions are that it must be easy to determine how much computing effort it took to solve the problem and the solution must otherwise have no value, either practical or intellectual. The number of monetary units created is equal to the cost of the computing effort in terms of a standard basket of commodities. For example if a problem takes 100 hours to solve on the computer that solves it most economically, and it takes 3 standard baskets to purchase 100 hours of computing time on that computer on the open market, then upon the broadcast of the solution to that problem everyone credits the broadcaster's account by 3 units.

2. The transfer of money. If Alice (owner of pseudonym K_A) wishes to transfer X units of money to Bob (owner of pseudonym K_B), she broadcasts the message "I give X units of money to K_B" signed by K_A. Upon the broadcast of this message, everyone debits K_A's account by X units and credits K_B's account by X units, unless this would create a negative balance in K_A's account in which case the message is ignored.

3. The effecting of contracts. A valid contract must include a maximum reparation in case of default for each participant party to it. It should also include a party who will perform arbitration should there be a dispute. All parties to a contract including the arbitrator must broadcast their signatures of it before it becomes effective. Upon the broadcast of the contract and all signatures, every participant debits the account of each party by the amount of his maximum reparation and

credits a special account identified by a secure hash of the contract by the sum the maximum reparations. The contract becomes effective if the debits succeed for every party without producing a negative balance, otherwise the contract is ignored and the accounts are rolled back. A sample contract might look like this:

> *K_A agrees to send K_B the solution to problem P before 0:0:0 1/1/2000. K_B agrees to pay K_A 100 MU (monetary units) before 0:0:0 1/1/2000. K_C agrees to perform arbitration in case of dispute. K_A agrees to pay a maximum of 1000 MU in case of default. K_B agrees to pay a maximum of 200 MU in case of default. K_C agrees to pay a maximum of 500 MU in case of default.*

4. The conclusion of contracts. If a contract concludes without dispute, each party broadcasts a signed message "The contract with SHA-1 hash H concludes without reparations." or possibly "The contract with SHA-1 hash H concludes with the following reparations: ..." Upon the broadcast of all signatures, every participant credits the account of each party by the amount of his maximum reparation, removes the contract account, then credits or debits the account of each party according to the reparation schedule if there is one.

5. The enforcement of contracts. If the parties to a contract cannot agree on an appropriate conclusion even with the help of the arbitrator, each party broadcasts a suggested reparation/fine schedule and any arguments or evidence in his favor. Each participant makes a determination as to the actual reparations and/or fines, and modifies his accounts accordingly.

In the second protocol, the accounts of who has how much money are kept by a subset of the participants (called servers from now on) instead of everyone. These servers are linked by a Usenet-style broadcast channel. The format of transaction messages broadcasted on this channel remain the same as in the first protocol, but the affected participants of each transaction should verify that the message has been received and successfully processed by a randomly selected subset of the servers.

Since the servers must be trusted to a degree, some mechanism is needed to keep them honest. Each server is required to deposit a certain amount of money in a special account to be used as potential fines or rewards for proof of misconduct. Also, each server must periodically publish and commit to its current money creation and money ownership databases. Each participant should verify that his own account balances are correct and that the sum of the account balances is not greater than the total amount of money created. This prevents the servers, even in total collusion, from permanently and costlessly expanding the money supply. New servers can also use the published databases to synchronize with existing servers.

The protocol proposed in this article allows untraceable pseudonymous entities to cooperate with each other more efficiently, by providing them with a medium of exchange and a method of enforcing contracts. The protocol can probably be made more efficient and secure, but I hope this is a step toward making crypto-anarchy a practical as well as theoretical possibility.

Appendix A: Alternative b-money Creation

One of the more problematic parts in the b-money protocol is money creation. This part of the protocol requires that all of the account keepers decide and agree on the cost of particular

computations. Unfortunately because computing technology tends to advance rapidly and not always publicly, this information may be unavailable, inaccurate, or outdated, all of which would cause serious problems for the protocol.

So I propose an alternative money creation subprotocol, in which account keepers (everyone in the first protocol, or the servers in the second protocol) instead decide and agree on the amount of b-money to be created each period, with the cost of creating that money determined by an auction. Each money creation period is divided up into four phases, as follows:

1. Planning. The account keepers compute and negotiate with each other to determine an optimal increase in the money supply for the next period. Whether or not the account keepers can reach a consensus, they each broadcast their money creation quota and any macroeconomic calculations done to support the figures.

2. Bidding. Anyone who wants to create b-money broadcasts a bid in the form of <x, y> where x is the amount of b-money he wants to create, and y is an unsolved problem from a predetermined problem class. Each problem in this class should have a nominal cost (in MIPS-years say) which is publicly agreed on.

3. Computation. After seeing the bids, the ones who placed bids in the bidding phase may now solve the problems in their bids and broadcast the solutions.

4. Money creation. Each account keeper accepts the highest bids (among those who actually broadcasted solutions) in terms of nominal cost per unit of b-money created and credits the bidders' accounts accordingly.