2014-2019 **ANIMECOIN TEAM**

Development Report

August 02, 2019

Introduction

This document aims to outline the goals and the technological background of the proposed solutions for the ongoing Animecoin project.

Animecoin is a free open source peer-to-peer electronic cash system that aims to stay true to the original Bitcoin design principles:

- decentralization: no need for a central server or trusted parties;
- cryptographic basis: same blockchain mechanics that allow users to transact with each other protect the genuineness of funds.

Animecoin aims to be a payment and secure deal method for the developers of new technologies in the animation and 2D graphics, talented newcomers and animators, as well as a method of promotion of the anime culture in general, especially in the crypto community.
The following chapter describes the issues such a project must be able to solve to be considered successful.

Common Cryptocurrency Design Problems

Blockchain parameters

Values such as total supply and average block time should be chosen carefully. Many coins aimed to be faster and cheaper than the original Bitcoin and failed while arbitrary coins with well-chosen constants became widely adopted solely for that reason. This problem, for the most part, breaks into the following aspects:

Supply issue: bigger supply means cheaper coin value, as dictated by market laws.

Fees issue: cheaper coins, on the other hand, mean the absolute value of transaction fees will also remain low.

Psychological issue: people tend to be more comfortable with sums like 1000 coins rather than 0.001 coin, even though technically this might be the same amount of information. Overly big amount of zeros in either case, however, remains undesirable.

Speed vs overhead issue: faster block generation means faster transactions, but also increases the amount of blocks in the blockchain.

Decentralization

While the network itself has no trouble running without any central server, users still tend to rely on trusted parties to secure deals. While the Bitcoin core technology offers simple and flexible tools to overcome this, most cryptocurrency projects have, strangely enough, never addressed this issue or rely on much more complex solutions.

What did Animecoin initially offer

Well-balanced supply. Roughly 2 billion coins have been generated before the final subsidy halving, and about 8 million is generated annually since that point. Required transaction fees never exceeded 0.02 coin/kB so far.

Fast block generation. Average block time is just 30 seconds, which means the transaction confirmation is extremely fast.

Next Animecoin Generation

Starting with 0.10 release Animecoin will include a Multitool, aimed to make multisig transactions as simple as ordinary ones.

This chapter outlines the rough roadmap for this solution and its relevance to the problems mentioned above.

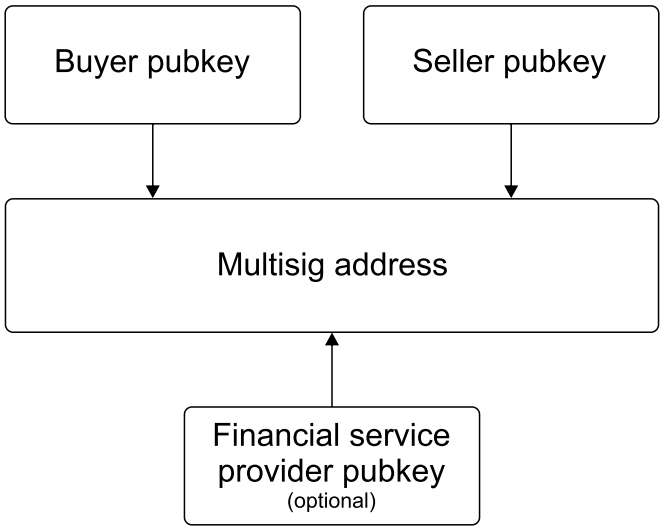
Secure the Keys

The pay-to-script method Animecoin supports can be treated as the simplest form of a self-executing contract. While this remains the basic Bitcoin functionality, most existing wallet software offers no means to use this beyond the RPC calls.

The above figure shows the naive implementation of such a contract.

It's simple: multisig address can be funded by anyone, just like an ordinary address. Its balance can be tracked by all parties but cannot be spent without knowing all the required private keys.

It's secure: only the public keys are required to create such a contract. This requires, realistically, at least the 'buyer' and 'seller' pubkeys, and optionally an 'arbiter' (such as a financial service) pubkey which may sign the deal in case of a dispute.



Signing the deal: unlocking the funds (such as transferring to the seller's ordinary address) will require all the private keys set as required at the contract creation. Each party, however, can sign the transaction separately without exposing its private key.

An incomplete transaction script can be transferred between parties directly or with the help of a financial service.

Keeping it simple: Animecoin 0.10 will provide users with the convenient interface to create multisig addresses of any complexity and exchanging partially signed transactions between parties.

Secure the Deal

There's a major design flaw in the naive contract approach described in the above chapter: namely, if the required number of participants never sign the deal, the funds will remain locked forever.

In order to make multisig contracts truly usable, a simple deadline option is required. The most basic solution is implemented in Bitcoin Improvement Proposal #65 (henceforth BIP-0065). This improvement adds a new OP_CHECKLOCKTIMEVERIFY (CLTV) opcode to internal script language, allowing the contract security measures including:

Refund/overdue: in case a party never signs, funds are unlocked to the other party past the deadline. This can also be treated as an example of a unidirectional payment channel.

Scam protection: in case a financial service acting as an arbiter, service signature may only be accepted past certain deadline to guard against possible service+seller or service+buyer conspiracy.

External verification: a financial service may protect user's funds with an additional verification layer, or the contract signing may release an additional decryption key in case of selling data. Using a CLTV-based deadline ensures the funds/keys will be unlocked for the user/buyer in case the service/merchant disappears.

And more. Activating the BIP-0065 will require a soft fork in the Animecoin network, which will be automatically activated once the majority of miners update to 0.10 release. The user interface providing easy access to BIP-0065 secured contracts will be added to Animecoin Multitool in 0.11, which is to be released following the soft fork successful activation.

Extending the Possibilities

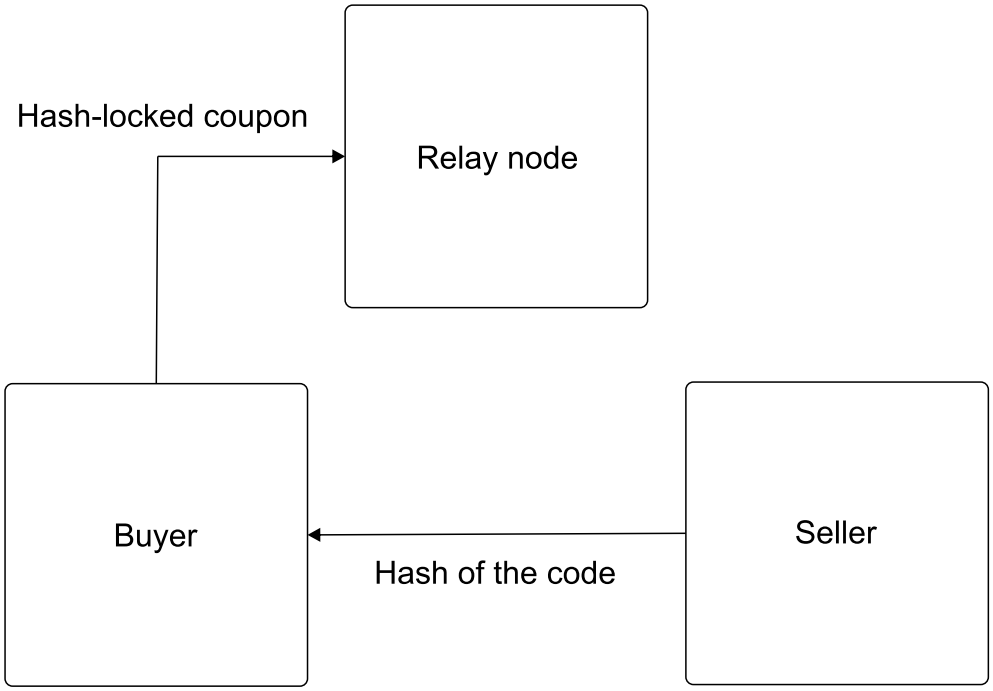
While BIP-0065 remains an absolute necessity for the contract security, the improvement that makes pay-to-script truly shine is Bitcoin Improvement Proposal #112 (BIP-0112). It is aimed to be implemented in Animecoin 0.11 along with the more flexible versionbits soft fork mechanism.

BIP-0112 includes another new opcode, OP_CHECKSEQUENCEVERIFY (CSV), which allows the contracts to include more versatile and more precise timeout options. This unlocks numerous new possibilities for the payment scenarios:

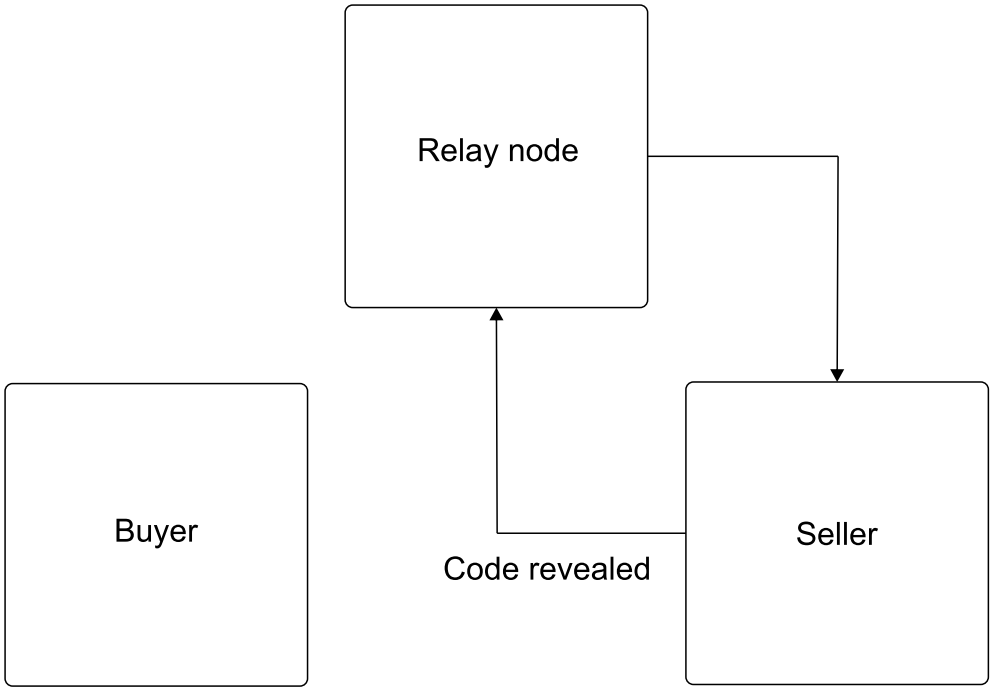
Hash Time-Locked Contracts (HTLC) act a lot like pregenerated coupons: a user knowing the code may instantly import the funds without the massive overhead of importing a private key, alternatively, the funds may arrive as a normal transaction, or be refunded if time expires.

Routable payment channels: combining a CLTV payment channel with the above technique allows the third party to relay the funds through their wallet without unlocking them until the deal is finalized and retain the speed advantage.

As the name suggests, just the hash of the secret code is required to lock the HTLC. Said hash can be shared without security risks to allow other parties to lock the funds without knowing the code itself:



The buyer-to-relay and relay-to-seller routes are secured by CLTV payment channels. Once the seller unlocks the funds, the code is set to be automatically disclosed by the contract:



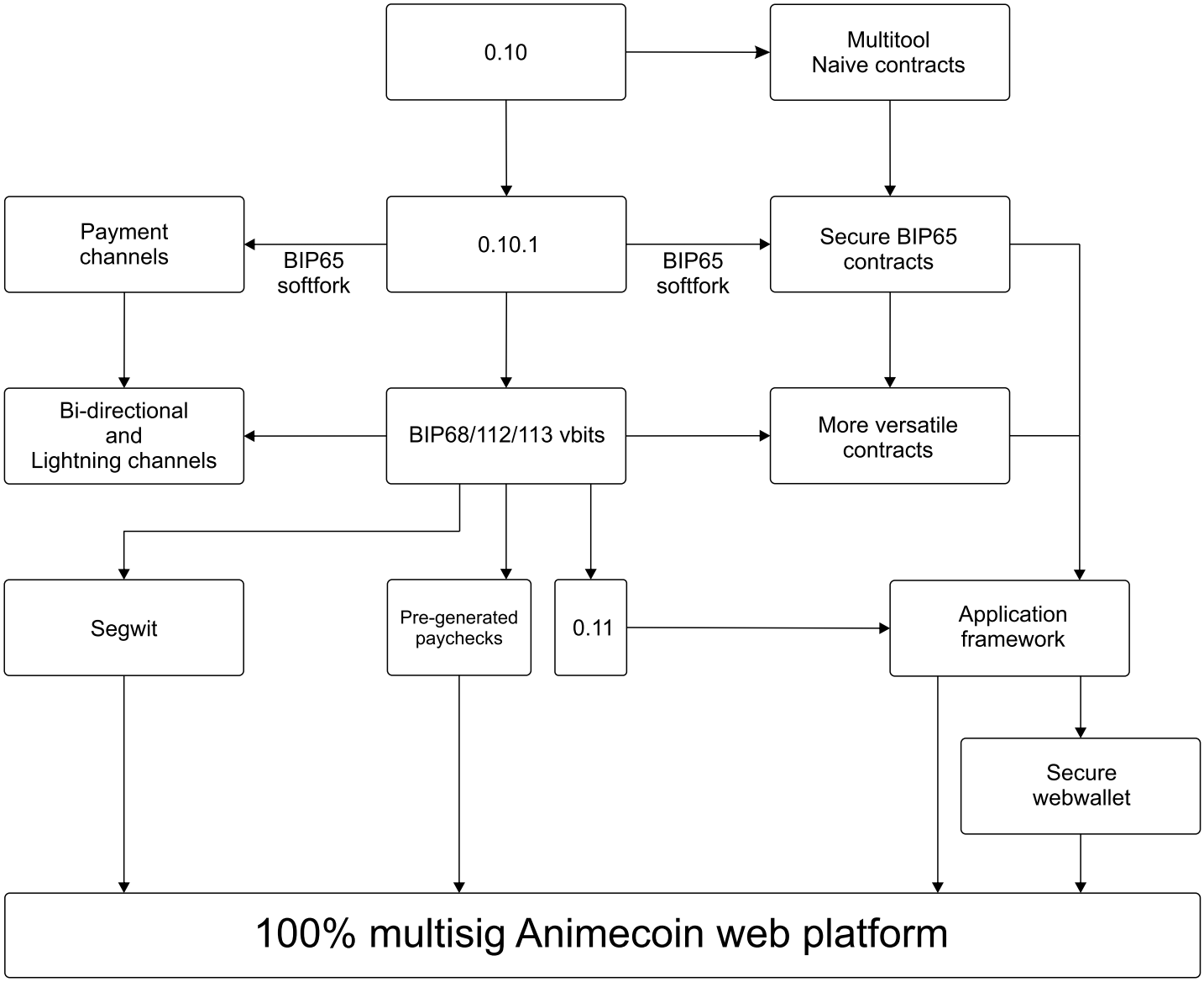
This technique lies in foundation of high-throughput network extensions, such as Lightning Network.

More straightforward scripting: in many simple cases, CLTV may be replaced by CSV. Unlike CLTV which starts ticking immediately, CSV only activates when deposit confirms.

Growing Infrastructure

A convenient HTLC interface is to be added before 0.12 release along with the new CSV-based Multitool options. The accompanying web framework will also be released, allowing to build simple and secure Animecoin-based financial services.

Dvelopment flowchart



Milestones

- Q1 2020: 0.10 release, Multitool for naive contract development.
- Q2 2020: BIP-0065 soft fork activation.
- Q2 2020: 0.11 release, CLTV-based secure contracts.
- Q2 2020: Web framework preview, secure web wallet.
- Q3 2020: BIP-0009/0068/0112/0113 vbits kick in.
- Q4 2020: 0.12 release, CSV/HTLC interface.
- Q4 2020: Web framework release, donation platform demo.

GitHub project page
https://github.com/Animecointeam