亦来币（ELA）区块链开发文档二

亦来云区块链开发组 2017 年 7 月 3 日

Comprehensive Strategy Document for the Construction of ELA

1. Overview

Elastos Coin (ELA) will be a virtual currency marketed in conjunction with, and optimized to work with, the Elastos
secure operating system invented by Chen Rong. Given that the future trajectory of BTC has been unstable as a result of
ongoing social and technical disputations, and that major figures within the BTC community of the PRC have already
expressed hope and support for the Elastos family of developments, there are some high expectations in store for ELA. In
particular, the currency and its associated technical system must satisfy the dual goals of somehow replacing BTC while
also working alongside BTC, serving to bolster and to stabilize it. The currency is set to benefit from certain abstract
reconsiderations in the design of virtual currencies, such as have been imagined by Dr Xu Gang, and are slated to be
further explored along the course of the project, as part of its overlapping phases for development and research.

In order to secure the timely delivery of a usable product, such as will be deployed both to server farms under Yuan
Engineering or under the management of Han Feng, as well as to interested large-scale commercial parties, it is
necessary to focus the development team's efforts upon a clean, well defined, well tested core program written in C,
which is targeted towards the platform of choice among the enterpreneurial and mining community of the PRC, namely,
Windows AMD64 (also known as sixty-four bit Windows), among others.

This core program will access a modular framework, whose policies may be implemented in a language agnostic manner, such
as with the help of mixed compilation technologies, in order to experiment with different concepts accrued from the
research section of this project, which as mentioned above, will be overlapping with the development portion and largely
instigated by a separate team. This team may be led, or at least closely advised, by Dr Xu, in its efforts to specify,
and to verify, well defined mathematical functions or subroutines, such as may

constitute an implementation of: smart
contracts, side-chains, NAT hole punching, internet filtration avoidance, inflationary economy, founder's reward
mechanisms, merge-mining, quasi-hard-fork, and other subgoals which may be raised by interested parties during the
project's course.

The dead-line of the project is not exact, owing to the ongoing nature of the project and the yet unclearly delimited
scope. However, every attempt will be made from the technical side, led by Yuan Xun, to have 1) a deployable product no
later than 1 August 2017, 2) a test-net up and running no later than 26 July 2017, 3) executables suitable for beta
testing no later than 19 July 2017. Every attempt will be made to neatly modularize the subgoals mentioned above, such
as UDP hole punching and support for side-chains, so that these features may be cleanly deferred as required by
schedule, and in accordance with the order of priorities of the marketing campaign.

Ideally, every subgoal should be modularized to the extent that the entry of new teams possessing minimal communication
with existing teams may be dispatched to work on subgoals individually. In fact, seeing that the project at hand is a
community-based venture, and that the PRC is a nation renowed for the breadth of its human resources, and not to say the
least, human merits, it would make sense that we are working to create the world's first truly modular virtual currency
platform, one which is all-at-once accessible to the masses by means of its transparency and wide-spread support, and
which has no need of the knowledge-control of a particular interest group to continue to function and to thrive, an area
where BTC and ETH have sadly both fallen short.

With the ubiquity and safety of Elastos the operating system, combined with the modularity, scalability, and correctness
inherent in the design of ELA, the road may finally be paved for the technical and financial community of the PRC to
unleash, in the full view of the world, and to their surprise, the next generation of advancements foretelling the smart
economy's arrival.

2. Personnel

I have the intention of hiring some or all of the following people on a part-time basis, depending on their
availability, having met these people through the Blockchain Lesson held in Beijing, of which I was the instructor:
Zhang Na, Yu Shunan, Li Taotao, Dong Yuanfang.

I expect that the following colleagues or former colleagues of mine in America may be available for this project, these
being some of the most skilled programmers I have known: John Matthew (PhD), David Huang, Matthew Seman, Data Brezack.

The following people will be employed full-time in Changping District of Beijing: Yuan Xuegui, Li Changli, Shi Yu. I am
seeking two more individuals for full-time employment as well: one engineer and one technician.

3. Method: Construction Phase

Week 1-2. Strongly typed interfaces and bare-bones implementations will be completed for Protocol A, B, and C. There will
be simple proofs-of-concept for the file-management component, the network-management component, and the verification
component. It is understood that the rules for verification may not be permanently established by this point. Thus, a
modular framework for verification must be provided so that the rules can be easily changed.

Week 3-4. An executable prototype will be ready for launch. The first test-net will be launched by the end of the second
week. Even within a given iteration of Protocol A, B, and C, there can be several test-nets, each of them with a
specific genesis block which may be triggered based on a command-line option. There will be finite-state-machine
routines for introspecting the node implementations and verifying their correctness. There will be a stripped down ASCII
notation for network transactions based on nc(1) so that testing individual transactions by hand may be simplified.

Week 5. At this point, there will be a series of refinements to the existing code and well as experiments with different
versions of protocols. For each version of Protocol A, B, and C, a separate set of headers can be made, and swapped into
the compilation folder so that they can be included during the compilation process. There will be active communication

with Dr Xu Gang and others within the Bitcoin community, such as the personnel of Wu Jihan, to ensure that protocols
arrived at may satisfy the wishes of various parties and be easy to configure for, and to build against.

Week 6. Further experiments will continue. There will be rigorous testing by dedicated unit-testers and integration-
testers at the company. At this point, the details of deployment will be considered, as well as the ease of
verification, and the ability to deploy the program to end-users, and also remotely, and in an automated fashion. The
author aims that the resulting program may be distributed as a single executable.

The resulting executable will target two major platforms, Windows AMD64 and Linux i686. The former was chosen because it
is the platform of choice for miners and node operators within the PRC. The latter was chosen because it is, by the
estimation of the author, the most stable platform, and the one which he would prefer to use for test-nets during
iterative experimentation and testing, and for the seed-servers for public use, upon there being an authorized version
of ELA scheduled for public release.

4. Mile-stones

A. Completion of the File System Component
B. Completion of the Network Component
C. Completion of the Command Line Parser
D. Completion of the Controlling Finite State Machine
E. Completion of the Policy Framework
F. Completion of the First Working Node
G. Deployment of the First Test Net
H. Deployment of Later Test Nets with Changes in Policy
I. Testing and Verification of A (Ongoing, Segmented)
J. Testing and Verification of B (Ongoing, Segmented)
K. Testing and Verification of C (Ongoing, Segmented)
L. Testing and Verification of D (Ongoing, Segmented)

5. Questions for Research (Ongoing)

What will be the byte-level format of an individual block within ELA?
How will ELA be connected to BTC?
How will inflation be implemented within ELA?

Will there be a means of adjusting inflation within ELA without a hard-fork?
How will smart contracts be implemented within ELA?
How will ELA support side-chains?
What would be the cost of creating a side-chain?
How much time would be required to create a side-chain?
Will ELA support Simplified Payment Verification (SPV)?
Will units of ELA be automatically delivered to owners of BTC?
If not, what steps would be necessary to submit a claim to ELA ownership?
What steps may be taken to prevent a hard-fork to delete the founder's reward?

6. Note Concerning Protocols

The following protocols exist for BTC and for all node programs of a similar nature: Protocol A, which describes the
structure of the block-chain and the procedure needed for verification, 2) Protocol B, which describes the means by
which an application, including a mining program, can communicate with a node, and Protocol C, which describes the means
of communication between two nodes. Protocol C is the most complex because it concerns low-level details of transmission
along the network, including difficulties with the discovery of peers and with timing, that is, the maximum allowable
time elapsed between communications before changes occur in the network, such as peers ejecting one another or deeming
one another invalid. Protocol C under ELA will be subject to attentional requirements, namely:

1) BTC does not provide a means for UDP hole punching, but this is a necessary feature for casual end-users to be able
to run their nodes upon home computers, so that they may be plugged into the network, thereby increasing the network's
capacity, robustness, and interconnectedness, which may further facilitate communication with applications such as
wallets, commerce programs, and visualization programs.

2) BTC uses magic identifying strings in order to initiate connections, but this carries the risk that a motivated
obstructor, such as the operator of a firewall, may use detection routines to systematically preempt connections
relating to BTC, thereby disrupting the flow of traffic between residents of a given domain and residents outside of
that domain. Certain techniques need to be utilized in order to avoid the use of magic identifying strings, such as
having a rotating key-ring.

7. Subgoals for Research

A number of subgoals, or special features, such as to distinguish the upcoming currency from its competitors, have been raised by Dr Xu and were further explicated over several hours during the first meeting of the figures of the new Elastos project, which occurred on 25 July 2017 in Beijing. The following section will be used to illustrate the benefits, constraints, and tentative implementation plans for each of the following features or functions.

A. Smart Contracts

While Ethereum introduced the second generation of block-chains with built in support for smart contracts, it had the disadvantage of pooling the entire world's resources in the pursuit of simulating a single computer. There must be ways in which a number of computers or processor cores may be simulated on the network, and that not all nodes will have to bear the burden of simulation, but only those nodes which act as arbitrators, as well as the interested parties themselves.

B. Side Chains

A form of segregated witness will need to be implemented so that side chains are implementable, and that such may be achieved at a low overhead, and transprent to the structure of the rest of the chain.

C. NAT Hole Punching

NAT hole punching is necessary in order to allow a machine which is not directly connected to the internet, but connected through a router, to be able to run server programs (programs which use the listen(2) system call) as opposed to merely client programs (programs which use the connect(2) system call). This is necessary for the wider adoption and proliferation of nodes of ELA. Both BTC and ETH suffered from the flaw of not having built-in UDP hole punching, which placed casual users and node-operators of scarcer means at a disadvantage in terms of exposure and participation within the community.

D. Internet Filtration Avoidance

In the same vein as above, there are network considerations necessary in order to prevent a blanket ban upon network
traffic emitted by this currency. New means not generally explored for protocol design will need to be established, such
as to create instance-based protocols which rotate between value markers, as opposed to having a single magic string
which signals a formal start of communication or start of specific functions.

E. Inflationary Economy

There needs to be a way to compound the inflation every X amount of time, such as monthly or yearly, as well as
protocols to handle the inflation in the event that, for some reason, a block should not appear for an extended period
of time (unlikely) or that the time-stamps of an individual block or a series are all significantly skewed (more
likely). There needs to be a way to store the inflationary bonus in a special account similar to a smart contract or a
Decentarlized Autonomous Organization (DAO), so that half of it may be allocated to purposes specified by the founders.
Steem and a few other currencies have inflationary economies

F. Founder's Reward

Having a hard-coded founder's reward, as with the case of ZEC, was not that difficult to implement, but the harder part
is to create a system for the founder's reward engrained in the protocol in a way so that it wouldn't be so trivial to
remove, in the case that rival factions would wish to destablize ELA by straightaway creating a fork of it.

G. Merge Mining

Merge mining refers to the ability to collect money upon a given chain by means of proof-of-work which was originally
performed on another chain. The chain where the labor takes place is called the host chain, whereas the chain where the
labor is given additional recognition and reward is called the guest chain. The most famous merge-mined virtual currency
is currently Namecoin. There are several major questions when implementing a merge-mining system, including the format

of the special string in question, which must necessarily be inserted into the host chain, such as to activate the guest
chain's recognition, and to lead to credits flowing into the target's account. Another question is whether every
full-node of ELA will need to store a separate copy of the BTC block-chain such as to verify that a given amount of work
was done upon BTC. If so, this would impose significant hard disk and band-width challenges, the costs of which must be
defrayed through other feats of engineering.

H. Quasi Hard Fork

For the first time in virtual currency history, according to the understand of the author, there will be a quasi hard
fork, namely, that a new currency will be created, but in such a fashion as to credit holders of an older currency.
There will be difficulties in the performant execution of a claims system, or the bridging of UTXOs between the guest
and host chain, such that coins occurring in the past system will be accessible in the current system.

The leaders of Elastos may choose a sort of automatic policy whereby all previous possessors of BTC are credited with
ELA, or else, there may need to be a manual claims system as mentioned above, whereby within a certain time limit, or
indefinitely, a person may submit a special record to be held in the guest chain, which verifies that a given set of
UTXOs as possessed in the host chain, before a given cut-off block, have been set into a redeemed state, and that these
are considered just as valid currency as new currency being mined.