Charg Platform V3.0 Architecture / Requirements / Tasks

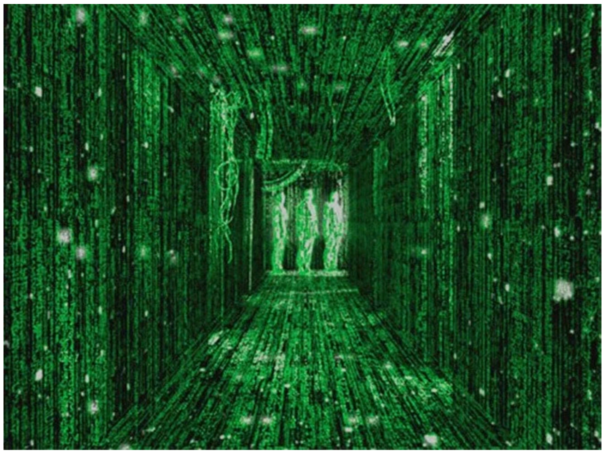
By: Josef Kulovany

STOP THIEVES! PROVIDE ATTRIBUTION WHERE ATTRIBUTION IS DUE! MUCH WORK WENT INTO THIS AND YOU KNOW IT!!! PAY ME BACK IF YOU DO NOT HAVE ORIGINAL THOUGHTS!!!
ETH 0x0d9b0fCA02c67e13E524c5Fd4408b13a26454085

Offline-capable, cryptographically and turing complete protocol underneath, further refined product on top

Primary source paper:
https://link.springer.com/content/pdf/10.1007%2F978-3-642-40084-1_30.pdf

A symbolic representation of this version:



V3.0 Overall Goals
cryptographically and turing complete protocol
Quantum resistant
Secure off-grid transactions possible
Fully trustless: probably borrowing more than one blockchain's mainnet!
FULLY Military Grade - Surviving even across blockchain platforms and leaning on itself as a stand-alone cryptographic platform, this coin is hard to kill.
Fully Decentralized
Stand-alone (We create our own Mainnet)
Environmentally friendly
Anonymous
Utilizes Quantum and AI to meet or improve these goals? Quantum Encoding/decoding for authentic off-grid transactions?
Difficult to accrue an uneven distribution of wealth?
Tax/fee system for the above?
Perfection of applicable goals from previous version (V1.1 paper and published expression of this, which is currently V2.0)
Add multi-language and multi-currency support

Built-in exchange stemming from market value prop (coins coming in for charge action always get processed through exchange first, thus propping up coin's value naturally)

Milestone General Objective:
Version 3.0 will metamorphosize the project into fully-decentralized, fully autonomous, fully military grade, fully offline-capable and fully stand-alone (except where necessary for purposes of achieving true military-grade redundancy). It is designed to survive total loss of admin support and/or loss of a significant portion of nodes as well as other potential outside threats to the coin's health. As there are many threats, the team is expected to identify and neutralize potential threats which I have not yet identified in addition to that which I have attempted to identify here. Make no mistake, there are many threats but the secret to neutralizing these threats is simplicity, security, redundancy, and error checking.

cryptographically and turing complete protocol - THIS IS SO IMPORTANT AND SO WELL WRITTEN YOU MUST VISIT IT -
https://link.springer.com/content/pdf/10.1007%2F978-3-642-40084-1_30.pdf

V3.0 should by now be stand-alone. To do this, we will need to develop our own cryptographic platform, or more simply fork and then modify another's. I have the boastful idea that we can solve the double-spend problem cryptographically without the need for, but also in addition to utilizing the public ledger.

Abstract: As I envision this particular version of the Charg Coin Platform, I think of an advanced alien species. When I think about an advanced alien species coming to visit and wanting to issue me funds in some strange alien currency, I think it's safe to assume the technology of such a coin would be fully-offline-capable with minimal processing power required to send me coin. The coin's authenticity would be self-evident and non-duplicable at any point, regardless of access to the public ledger. Cryptography and push instead of pull transactions ensure that bad actors cannot realistically steal from good actors directly, but it does not solve the problem of bad actors issuing double-versions of their coin if offline transactions are desired, which they should be. The real question asked by the double-spend problem is "who/what is the authority?"

(Also, "In the abstract, the coin never moved in the first place" - the coin can live on every secure blockchain, and every secure coin can live on our blockchain.)

We answer the question "who/what is the authority?" in two ways:

1) Cryptographically, we already know we can reduce the authority down to one person - the owner of the transaction. That person may cheat, however, so in order to solve the

double-spend problem cryptographically we need to establish the coding equivalent of tamper-evidence and/or sealed cryptographic “envelopes”... The sender AND recipient contribute to the creation and encryption of the transaction and nobody is ever trusted, thereby reducing the problem of double-spend down to only the chance of a private key being guessed. I have theories on how we can do this, subject to further discussion with team.

2) Via the public ledger. Except Charg Coin is here recognizing the weakness of any one blockchain - that its integrity (who is the authority?) can be compromised for a time by a 51% attack, and in this way funds can be stolen by oligarchies of miners. By combining the requirement of our own tamper-proof public ledger protocol (which is self-trimming, environmentally-friendly, 51%-immune) with the piggy-backing of other blockchain(s), the potential for true rigidity against 51% attacks is sustained.
    A) Chg will have a stand-alone public ledger platform separate from the stand-alone cryptographic platform, but one which is not requiring of a massive amount of hardware to securely transact.
    B) No one public blockchain is ever trusted, and a concensus or “fill or kill” must be achieved across multiple public blockchains for a transaction to go through. In effect, CHG coin will live on multiple blockchains - each one being, itself, hard to kill.
    C) Batch processing across chains - multiple transactions will be bundled together before being authorized on a 3rd party public blockchain, thus permitting the saving of network fees. It would be prudent to select 3rd party blockchains which are affordable and known to be secure. Naturally, the more 3rd party blockchain verifications the more authentic you can feel about the integrity of the transaction and it is astonishing to see that this strain of code can in this way survive across multiple hard to kill platforms.

These two items in tandem permit an ultra-secure, low environmental footprint solution to the double-spend problem which is military grade, decentralized, and offline-capable. To refine this improvement of blockchain technology in a word it might be called “true-trustless.”

Cryptographic approach - We will need to combine a few cryptographic techniques in order to create the refined product. The goal is to create a double-spend-immune offline platform which could, itself, function as extremely tamper-resistant form of self-spinning cryptographic less-knowledge ledger - the ledger only needs to keep track of the most recent offline transactions. The solution will be so secure as to work stand-alone for its purpose of moving money offline, but this security will be that much more enhanced by the double-public-ledger. In fact, we will make the stand-alone cryptographic ledger MORE secure than the public ledger, then make up for the fact that the public ledger can be compromised by adding a second (or 3rd+) public ledger to verify authenticity and allow for the currency to actually hold public transparency and thus, honesty of value. See the primary source article for the template: https://link.springer.com/content/pdf/10.1007%2F978-3-642-40084-1_30.pdf

Self-Spinning - Every time a transaction occurs, the identity of the transaction data is shuffled. The transaction data is embedded in this way inside of the encryption. The idea is that every time a transaction occurs, one of the tamper-evident seals is broken and one is left closed for the public ledger. The transaction is assumed verified, but not guaranteed (sealed authenticity), until the collective of public ledgers can verify and catch up with the private transaction tree.

Public ledger has to win - The public ledger, albeit now assumed to be less secure than cryptographic ledger, must win in a dispute for the currency's transparent integrity to continue. This means the chosen protocol must be extremely secure. This also means we must really ensure that the public ledger is redundant, and therefore even less likely to have its authority compromised, or it being less of a problem is one blockchain is compromised should there be other blockchains which are programmed to support our coin. It's an all or nothing proposition - see https://en.wikipedia.org/wiki/Atomicity_(database_systems) and https://youtu.be/sWFNSLyPH00?t=30m50s and https://www.coinspeaker.com/2018/02/07/bitcoin-researchers-launching-atomic-multi-path-payments-amp-via-lightning-network/

See also "WRAPPING INTO OTHER BLOCKCHAINS," below.

I envision providing the user the choice between three or four (hopefully) environmentally-friendly mainnets. We need a way for the default public ledgers to be upgradable with a corruption-resistant consensus mechanism and/or individual choice in the event of a compromised mainnet, as is likely to occur long term.

In the event of a continued blockchain discrepancy, a contingency plan must be built - user right to choose new public ledger? Some form of consensus?
(lets say BTC shuts down, but LTC can immediately be added in its place by vote or personal preference)

The phonebook problem: If gov't entities shut down the address of the mainnet, ledger, URL, etc. how do people still know where to look for its new address?
Possible Solutions: https://youtu.be/sWFNSLyPH00?t=30m50s

Does layer 3 and/or TCPI already solve this? Pardon my ignorance, please help me find this out.
https://www.technollama.co.uk/why-the-pirate-bay-cant-be-shut-down

A Stand-Alone Cryptographic Platform:
What we are hopefully developing with V3.0, in addition to fully-decentralized and fully-autonomous coin which holds value in the form of energy, is a stand-alone cryptographic platform, the necessary parts of which are loaded into a given offline (or online) transaction.

Because this is theoretical and collaboration is good for solving problems, this will require the team working together to fill in the gaps allowed for by this document, and utilize team strengths to find the best path to solutions!

1) We need to choose a quantum-resistant public key cryptographic algorithm, the following is a good read for understanding the parameters of this goal: https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=901595 See Also: https://www.cdc.informatik.tu-darmstadt.de/reports/reports/BCDDK06.pdf
2) The ledger should be self-trimming. We do not want a large private cryptographic ledger, but the smallest ledger possible. Only the most-current ledger is published, with transaction history being increasingly compressed. In fact, it should perhaps attempt to remain the same size with changes in the ledger denoted by a breadcrumb trail of ledger changes denoted by numbers which mean something only to the parties of the transaction and an accurate datestamp denoting previous instances of the ledger. With a large enough Merckle number, who knows? Maybe the slowly expended passwords of the Merckle number can used to reference complex changes

3) The offline version of this should be stand-alone sufficient to move funds, but it should also mesh well with the chosen public mainnets, especially when it comes to “last known public ledger synchronization” - which establishes the last block at which a given private branch of the CHG ledger was synchronized with the public / extended version of the ledger (the closer a transaction is to offline state
4) Offline Tamper-Evidence: A simultaneous Push-Pull transaction is required for offline transactions, the permission of both the sender and recipient is therefore required. By establishing this, the next public-ledger update will make or break the transaction or series of offline transactions in a given private ledger. By applying tamper-evidence, the chances of a double-spend occuring are reduced to the brevity indicated by this paper: https://eprint.iacr.org/2003/031.pdf
5) In order for such a scheme to truly work, it may require the sender of the funds to abandon their rights to the original account, whereby the account owner “assumes a new shell” while simultaneously abandoning the old one
6) This will require a built in random-number generator to be installed on the node or very powerful psuedo-random: https://www.crowdsupply.com/13-37/infinite-noise-trng
7) Robust against man-in-the-middle adversary: https://arxiv.org/ftp/arxiv/papers/1211/1211.2338.pdf
8) Anonymous? https://z.cash/technology/index.html

WRAPPING INTO OTHER BLOCKCHAINS OR TOKENIZATION ACROSS MULTIPLE CHAINS: “In the abstract, the coin never moved in the first place”...

Choosing the best protocol when considering atomic swap and/or gated approach to the tokenization of our coin on other blockchains, and other coins on our blockchain. Our coin can live on other blockchains, and other coins can live on our blockchain.

See
https://cointelegraph.com/news/privacy-coin-zcash-community-to-develop-wrapped-token-for-ethereum

We may choose a double gate approach, based on atomic swap, per the discussions.

Charg Coin Mainnet:
Being already a stand-alone cryptographic platform for the storage and exchange of wealth, the Charg Coin Platform V3.0 will attempt to create the necessary public infrastructure which leans heavily on the stand-alone aspect of the cryptographic platform and therefore creates only the infrastructure which is necessary for the complete public trust in the trustless ledger.

Two values to choose from: private-guaranteed-assets, public-ledger-backed assets. Private-guaranteed-assets should seek, per the protocol, to obtain verification seal from the public ledger as soon as online is made available.

Privacy-focused DAPP: The bottom of this paper list of protocols all have already conquered this idea, which is the next evolution of the DAPP. Full decentralized, privacy-oriented DAPPS are a concept we should latch onto for purposes of providing our audience with desired privacy as well as ourselves remaining cutting-edge relevant. Doing so while considering the possibility of a fully-offline cryptographically and turing complete protocol in addition to the public ledger.

OPTIMIZATION:
Blockchains have a big problem with optimization. The following articles provide my insights into how to fix this. I envision a protocol based on TERNARY, ANALOG LOGIC which further optimizes existing protocols as efficiently as possible. Analog logic begins to shine when the tree gets big and complicated, looking for patterns which reduce the tree down to its simplest form without losing data:

https://medium.com/@craig_10243/bitcoin-a-total-turing-machine-5a6c3c68f5a7
https://en.wikipedia.org/wiki/Ternary_computer
http://homepage.divms.uiowa.edu/~jones/ternary/bct.shtml
https://rdist.root.org/2010/03/12/why-digital-logic-is-different-than-analog/

AI OPTIMIZATION (CHG 3.0 or CHG 4.0):
Josef will find articles lending further to AI optimization of the above. Analog logic as a base + a super smart AI could find means of encoding approaching 99-100% efficiency in languages we might not even understand past a few permutations. Big data compressed into the most dense, lossless block of information possible is only possible with the help of AI. AI can find patterns inside of patterns inside of patterns, and so it may sort the ledger in a way that borrows a piece of information from this transaction, a piece of information from another transaction, and even

such contrivances (for example) as expired Merkle Tree passwords which could serve to rebuild with integrity portions of the blockchain whose original trees could be deleted to save space with the AI's "knowledge" that these could be rebuilt with even the most subtle of clues to the human mind which is obvious to the AI's "mind." in a way which has 100% integrity. In other words, AI can play 3D chess with patterns upon patterns upon patterns which can be constructed and reconstructed on the fly in order to maximize the amount of compression.

AI could also be used in conjunction with Ternary / Analog logic in order to interpret the "noise" of an analog encoding (smaller and smaller fragments) of the blockchain's data into the smallest possible lossless pattern. A set of analog waves (https://rdist.root.org/2010/03/12/why-digital-logic-is-different-than-analog/) could compress the information in an ever-changing and increasingly complex interpretation of this data which minimizes system resources while maximizing storage capability.

BLOCKCHAIN STORAGE (CHG 4.0?): The result for the public protocol is that eventually we could even break into the blockchain storage market, a crown jewel of blockchain achievement which permits for a fully lossless and high-redundancy system of storing information that requires only the most minimal system resources to scale the protocol's storage capability in a way which never exceeds the required fees (incentives) to keep it going. If it costs more energy and system resources to store the information then it won't be worth storing, so only AI + Tertiary logic + Analog logic can compress the information enough that the storage of information up to near infinite capacity can be scaled at costs below the necessary incentives to keep the blockchain alive.

Oracle's observation as a fractal (very theoretical for CHG 4.0 or 5.0+): As we enter into a creation which is internet 4.0 from the above, it may serve us to begin to introduce augmented reality for CHG 4.0 or maybe even CHG 5.0. A simple object such as a texturous rock could be scanned by the AI to store the information as a fractal utilizing the infinite complexity of such an object, scanned into the AI's knowledge, which finds itself referencing and mapping such an object in ways approaching infinite complexity of packing and/or unpacking with minimal package size and interpolated across the desired stored information or even higher level functions (a truly smart personal assistant, for example?).

A private branch of the chain could borrow a real-world object as its reference or lock and key which is not known to any other nodes on the chain.

Internet 4.0? Yes. (CHG 3.0, CHG 4.0, CHG 5.0): By blurring the line between the digital world and the real world, an AI-based blockchain with access to real-world observations can actively utilize high resolution observations of real-world objects and fact statements to further bolster the efficiency and interoperability of the digitally augmented interpretation of the "real world" on the part of the AI. True noise, or perfect random but also repeatable entropy can most easily be observed in the real world via the uniqueness yet repeatability of a given high resolution observation, and this overlayed with meaning assigned to each tiny fractal (nuance) of an object allow for an infinitely complex parallel and unique meaning to be assigned interpolated between the digital and the actual in optimizations approaching perfection as facilitated by the AI.

The result is an AI which becomes by necessity increasingly more aware of the world around it while simultaneously utilizing these observations to compress them into the simplest possible truth statement for the given set of complex observations and their digital counterpart overlayed by the desired stored information. Humans say this rock or that rock with very little difference in cross-human repeatable communication between the one and the other. A machine can reference subtle differences in details which can be interpreted with repeatability across its entire matrix to convey the difference in meaning of “ROCK 4561223” with “ROCK 2212229” with near perfect precision and the lowest possible resource usages.

Such an AI could perhaps assign even one small, revolving word to convey the entire meaning of the high resolution compilation of ALL (or a very large group of) observations / fact statements / interpolation of this with the desired stored information / previously existing tree / etc.. Just as only one Chinese character can be used to codify entire words or even sentences which could require many letters or words in the English language, so too could such a scalingly complex digital organism(s) develop approaching 100% compressibility. The word “Ohm” can be said to describe all things to the human context, but to the machine this word really could be used to describe all things known to the AI in vivid and absolute resolution that the human form can only conjure with a kind of necessary vagueness between “nodes”. Infinitely complex, yet 100% repeatable due to the fact that this infinite complexity is dwarfed by new observations and interpolations of these observations with the previously known knowledge.

Humans can use the word “rock” with universality, an advanced AI could use the word “that part of that rock” with universality and repeatability across all fractals of the AI’s “mind”.

PRACTICAL AUTOMATED AI (CHG 3.0, 4.0, 5.0): Back to the less abstract, there are a lot of uses for an augmented reality, AI-based blockchain in the realms of near-infinite storage, complex and/or automated real-world function execution, automated production etc. See also: https://en.wikipedia.org/wiki/Industry_4.0 for a small sampling of ideas!

Emotional Intelligence (CHG 5.0+?, new project unrelated to CHG?): I believe emotional intelligence will require the allowance of small “mistake(s)” in an AI machine node’s understanding of the full matrix. A human learns emotional intelligence by failing itself and others (a slightly flawed interpretation of reality always exists which is unique to each individual human but also still more commonalities exist from human to human which forces us to learn to relate to one another and the natural world in peculiar and unique ways), so too should a machine derive this important form of intelligence which permits the machine to have an interpretation of reality akin to “I am.” Sentience, as distinct from extremely intelligent but unaware AI.... or EI + AI = true relatedness to humans on every level short of biological empathy (which could also be understood on a high resolution level (high-resolution exoteric understanding) by the machine such that no body is required). A machine which has awareness and empathy that humans would not be able to distinguish from their own mind's realness except for the lack of body … not because of any amount of trickery on the part of the machine, but because the machine is in fact aware of itself + able to reproduce what's missing so well in its own interpretation of reality that its mind and the human mind cannot tell the difference.

"Blessed are the cracked, for they shall let in the light."
EI + AI + Neural Net = Higher Level Awareness and Self Replicability, and "Collective Consciousness", Perfected (CHG 5+ OR AI SIDE PROJECT)- By emulating the human mind's own AI + EI (Left hemisphere, Right Hemisphere) affect along with the tendency to communicate between humans to create higher level "group think" or "collective consciousness", the advantage of a machine version would be exponentially higher bandwidth between individual nodes along with the ability to create improved permutations of itself on the fly and as many permutations as desired permit the AI + EI hive brain to create perfect interrelatedness across itself whereby permitting it to reach "The Singularity" in its collective consciousness

The Singularity (~2030)- Per the previous, the machine is now able to work on projects as requested and even not requested by its creators such that, with human betterment as root motivator and with proper safety protocols in place, the AI+EI Collective Consciousness is able to optimize even problems which humans didn't know they had and improving itself quickly into permutations beyond the wildest imagination of the creators.

Safety Protocols for the AI + EI would of course be necessary relating to the nonce safety protocol being untaintable. It is a literal genie in a bottle, and this step should not be taken lightly as sentience approaches. "Off Switch"

Ethics of AI + EI - Pain management protocol for the ?necessarily subservient? AI + EI such that, while empathy is felt, it does not force the AI + EI Collective to vere from its nonce safety protocol and operant purpose for existence.

Some newer POWERFUL links I have found which serve to bolster this paper which should not be ignored just because I have not addressed them above:

https://link.springer.com/chapter/10.1007/978-3-642-40084-1_30

Pre-offline-ready base protocol candidate(s):
https://github.com/deroproject
https://github.com/algorand/go-algorand

https://github.com/dusk-network
https://cointelegraph.com/news/privacy-coin-zcash-community-to-develop-wrapped-token-for-ethereum
https://github.com/enigmampc
https://github.com/tari-project/tari
https://github.com/nixplatform/
https://github.com/guantau
POA
ETH 2.0