Chameleon: A scalable distributed cryptographic information and value transfer architecture

Alfred Noble

Abstract -The world wide web and internet of things together with the explosion in cryptographic currency peer-to-peer networks has lead to an enormous richness and complexity of associated features and data. An architecture is proposed to allow the mapping and connection of arbitrary distributed systems and associated data. The connection is proposed as a peer-to-peer service layer providing coordination, access and update capabilities from the connection layer itself as well as between distributed systems. In this way the vast and disparate heterogeneous data systems and network can be coordinated and allowed to efficiently enhance each other's capabilities through an open source peer-to-peer network.

I. Introduction

Since the advent of Bitcoin in 2009 [1], numerous alternative blockchain-based cryptocurrency networks have been formed; many being highly derivative in nature in that they differ only superficially from Bitcoin. Conversely, some have sought to provide their own unique features or enhancements that set their projects apart as being of interest in their own right. In addition to the method of securing the bitcoin blockchain using the *Proof-Of-Work* (*PoW)* protocol where hashing power is used to mine blocks, other methods have developed including *useful* forms of proof of work, for example searching for twin primes or prime pair with given difference. This can include, for example, computation of Brun's constant [2] and also the general case of a given difference for prime cousins. Using the power available for hashing blocks for exploring a particular field of application with potential value obviously represents a tremendous leap in terms of usefulness in return for the computational power deployed and consequently what is a potentially enormous electricity usage. In addition there has been an increase in the deployment of a second major blockchain protocol to date known as *Proof-Of-Stake (PoS)*. PoS aims to secure the blockchain by means of randomized attempts to establish a so-called coin stake kernel transaction from among the user's coins. This has a major advantage not only in terms of energy efficiency (the computational load is comparable to CPU scavenging methods). This method of securing the blockchain allows a much wider distribution of stake holders in the peer-to-peer network to contribute to securing the blockchain. Having the possibility for a much wider contribution to the security of the blockchain is an inherent major advantage over PoW; where there exists a strong tendency towards condensation of network hashing power among a privileged set of miners thus tending towards increased centralization. Numerous cryptocurrency projects have further specialized in providing a number of specific or unique features that may be regarded as forming an additional feature layer over the existing possibility for value transfer over the peer-to-peer network. In particular, I/O Coin (IOC) has taken the lead in encrypted communication technology after beginning with the provision of an aliasing feature to provide human readable or logical names for native I/O Coin base58 addresses known as *DIONS* (Decentralized Input Output Name Server). In 2015, they created fundamental new capabilities in communication and delivered the world's first pure blockchain peer-to-peer encrypted message system using AES 256 over RSA negotiated channel endpoints within the block chain itself. The peer-to-peer encrypted communications of I/O Coin takes the form of graphs consisting of endpoints within the blockchain providing immutable encrypted records of communications and elimination of any third-party: e.g. cloud based server resources. This mechanism facilitates peer-to-peer instant encrypted communications as well as encrypted file upload and transfers all through encrypted channels. In 2018, they have extended their graph model to the general case of groups providing a unique encrypted group communication feature fully decentralized on the blockchain. Other projects, such as Siacoin, have specialized in data storage fragmenting files over the network and rewarding peers that store file data fragments. A tendency for competition between many blockchain projects of a certain type, driven by marketing to a large extent, has developed such that they try to include as many features as possible often leading to a poorly implemented system at best as they strive to attract users new to cryptocurrencies. A core of cryptocurrency networks remains amid this tendency that provide their own specialized chain features and attempt to focus on these aspects to a high working standard of operation and effectiveness. A question naturally arises is: how these disparate systems might be used to best effect in conjunction with the features that the other better currency networks offer.

II. ABSTRACT API

Within any distributed system where peers run on standard ports and with a common interface what are termed as *Agents* may be run. These will be, by their nature transparent to their network peers and will expose an interface allowing an external system to interrogate or modify the state of the network or data. An agent will expose an abstract interface to the Chameleon network. Messages are relayed and distributed by the Chameleon peer-to-peer network specifying a target class of agent nodes. Message content decoding and processing is then handled by the particular concrete class instance of the agent.

The flow of transactional requests and responses in the Chameleon peer-to-peer network are sufficiently flexible to allow inter connection of blockchain networks and potentially arbitrary extensions. Messages map to agents running concrete implementations of an exposed interface definition. With this, a great diversity of heterogeneous networks and respective protocols may be adapted such that their state may be interrogated or modified.

III. CHAMELEON

The Chameleon peer-to-peer network operates on agent nodes by means of requests and responses to interrogate or manipulate the state of the targeted network or data. Requests are submitted to the network and relayed to agent nodes in the target network. Chameleon provides a connection layer between any number of networks or data sources together with a connection mapping of context specific messages to concrete network implementations. Transactions are issued which act as triggers for defined activity on a given network. This may include any network connected to Chameleon as well as the Chameleon network alone. The Chameleon network cryptocurrency that will be used to pay for the use of all features supported by the Chameleon peer-to-peer network will be termed *Cham*. Cross-network requests may be issued from within the Chameleon network and mapped to an agent of the target network and processed. Responses from agents are relayed to Chameleon asynchronously and correlated with the originating request. Chameleon peers earn fees for processing the requests and correlated responses.

The Chameleon protocol will be such that peers are rewarded that take part in validations of transactions. Only after a threshold number of validations using disparate sub graphs of nodes making up the network are the transactions deemed valid. Rewards are then distributed among the peers and weighted according to data share, frequency and regularity of validations and number of Chameleon coins held. Rewards are weighted in addition by supporting feature sets embodied by inter-operation targets of particular value. As Chameleon is launched, IOC will play a key role as the base currency. Chameleon holders of IOC who support the network validation protocol will then be rewarded additionally with IOC holdings.

IV. RELIABILITY FROM POTENTIALLY UNRELIABLE AGENTS

Agents in target networks will have the incentive to run reliably in support of the integrated network features that are collated and coordinated under the Chameleon connection network. In addition, agents will be rewarded for providing consistently reliable information and network confirmations. A principle incentive to run reliable agents is the collective or community goal of combining the best of high value coin networks and, in the wider sense, other potential open data sources that may be brought into play with Chameleon into a single abstract overview. As requests and responses are relayed through the network agents, providing consistent results may be rewarded while unreliable agents rejected.

V. OPTIMAL BALANCING OF SPECIALIZED PEER-TO-PEER NETWORKS

Several peer-to-peer networks provide functional layers that go beyond what constitutes an electronic cash system alone. Some blockchain networks provide file storage while others may provide computational power in the attempt to solve scientific problems. I/O Coin has emerged and has achieved world firsts in the field of blockchain-based encrypted communication with its peer-to-peer encrypted messaging and now fledgling encrypted group chat functionality.

It is natural to consider that such specializations are enhanced by means of transparent connection via an abstract API provided by agents in the target systems. In this way, networks can perform the roles they do best without unnecessary blockchain bloat or bottlenecks that are inevitable in systems that seek to converge services over ranges which overreach their original design and performance aims.

VI. APPLICATION: COLLATING INFORMATION FROM THE INTERNET OF THINGS

I/O Coin(3) introduced DIONS in 2015 and it was fully implemented into the IOC blockchain via a protocol update in December 2017. I/O Coin was the first cryptocurrency in the world to implement and release peer-to-peer AES encrypted blockchain chat. Also part of DIONS is the ability to store encrypted files. These are facilitated via an API that may have *Decentralized Applications,* or Dapps as they are referred to from here on, which are designed to adapt external business logic or applications in other domains to make use of the encrypted messaging and data storage features of DIONS. Dapps may be built to easily receive and relay data from external devices such as base stations and access modules. Here again is an example of making use of a specialized blockchain technology and allowing the API to be exposed to the Chameleon connection layer. As a result, information from the IoT may be collated and used in conjunction with other specialized chains. For example, pattern or error detection in the resulting data from the end communication devices perhaps using a blockchain that is specifically suited to scientific computation.

VII. BIG DATA

With the collation of data from potentially millions of IoT devices, further data may be accessed from such fields as medical research, consumer analytics, and in the field of telecommunications, in particular network element status messages, warnings, and alarms. When network equipment, for example, enters an error condition it will typically result in forward propagation to interconnected equipment so that for a single network element alone that is in error, many thousands of alarm messages may be generated. Reinforced learning, neural network approaches, and pattern recognition can reveal underlying patterns in the generated alarms that detect the character of the problem and probable cause. The enormous scale of data which is publicly available is inherently such that agents may be deployed using an abstract API to be interrogated or data flows updated or mapped to data in other systems using, for example, a key value pair. Thus updates to, as an example, a consumer statics database may be mapped to some internet device to report on the update history. The reverse is also true with documents being prepared and transmitted through a scanner directly to a data storing blockchain which results in one or more triggers being fired by the agent.

Potential applications to the field of deep learning would be the possibility of creating and training neural networks using back-propagation.

VIII. IMPACT ON BLOCKCHAIN-BASED PEER-TO-PEER NETWORKS

Currently with the huge number of blockchain networks publicly available there is inevitably a great deal of duplication or very slight variations on other coin networks. A specific core of blockchains have over the past five years actively sought to innovate and provide within their own fields of emphasis; highly developed technological solutions for specific use cases. The advantage of a connection layer coordinating many currently independent chains to make them interdependent is clear. It is anticipated that many derivative technologies will lack the essential motivation to support having inclusion in a connected eco-system of blockchains covering an essential and meaningful field of application. As a result, it is expected that with the success of Chameleon many derivative networks will either atrophy or die of completely thereby reinforcing distinctive and innovative blockchain networks.

IX. SMART CONTRACTS

Various blockchains implement what are known as smart contracts. For example, Ethereum with its Ethereum Virtual Machine (EVM), smart contracts are compiled into byte code and stored in the Ethereum blockchain. The code then may be executed on the EVM. A more flexible approach is proposed in this paper that smart contracts may be stored not only in the chain but also in an external container which may be sand-boxed. An abstract smart contract class and inheritance will allow a polymorphic mechanism for recognition of the underlying form of a smart contract. Polymorphic classes define a smart contract container and a finite state machine is constructed by inheriting from the framework. Virtual base classes define a set of signals that control state some of which may be overridden by the writer. Transition between states is controlled by request / response sequences so that the contract becomes an implementation of a finite state machine. Fees may then be associated with a well-defined state transition sequence. The underlying smart contract framework may be based on Sun Java byte code for execution on the Java JVM or an adaptive framework exposing a set of C++ virtual base classes. Through the connection layer formed by Chameleon, smart contracts may be invoked not only from within Chameleon but may be implemented within more specialized sub networks for invocation by means of transactional requests triggered across potentially any other network. Making use of the Sun Java JVM is particularly practical in that it will give access to the very wide range of existing JDK class packages.

X. RANDOMIZED DISTRIBUTION OF TRANSACTIONS

Instead of replicated copies of the ledger over every node in the network, what is proposed here is a highly randomized fragmentation with redundancy over the whole network such that as the network grows in size the probability is high that all parts of the ledger are represented by the network as a whole at any given time.

Transactions making up the ledger are distributed over the peer-to-peer network uniformly and such that multiple peers may leave the network at any given time and the information making up the ledger remains complete over the network as a whole. In this way any given peer will see only part of the ledger. As the network scales to very high levels of transaction volumes, it is required to balance the distribution over the network peers. Also as the network scales to high transaction volumes, the distribution becomes dense over the network peers giving a high level of fault tolerance. The term fault is applied here in generic terms. This means either a node simply leaves the network temporarily for maintenance or network reasons or integrity of the node has become degraded in some way.

XI. MECHANISM OF TRANSACTION VALIDATION - THE MOLECULAR LEDGER

It is evident with existing blockchain based cryptocurrencies that the mode of each node replicating the ledger will not scale to very high transaction volumes. In addition, the current way in-which blocks are mined by a single node to be accepted by the rest of the network, whether proof of work or proof of stake, constitutes both a bottleneck to scalability and also a degradation of the fundamental goal of decentralization.

It is proposed for Chameleon a different approach that does not involve block mining as has been done to date by other cryptographically based electronic currencies. Transactions submitted to the network are regarded as propositions and the network attempts to carry out a validation which may also be regarded as a proof. Transactions may be validated completely by single nodes simultaneously or partially validated in parallel by many nodes. The greater the number of independent validations or fragmented validations the greater the confidence level of the transaction due to the wider distribution of network peers involved. Security from double spend attacks derives from the statistical properties of the ledger distribution making it exceedingly difficult for a single actor to achieve the necessary wide distribution of nodes involved in a conspiracy to degrade the ledger integrity. When the statistical density of validations is achieved the transaction is considered by the network as validated and accepted. With no mining of blocks, as in the case of Bitcoin, there is not the tendency for centralization in terms of the concentration of mining resources. The network as a whole engages in validating or proving transactions. With a highly scaled and balanced network, security derives from statistical complexity of the system as a whole. The validation is the form of logical operations carried out in parallel over several peers. Following cross-correlation over a threshold level of sub graphs the transaction is validated. What underlies the network security is essentially its inherent entropy: a physical property. Given the stochastic aspects and thermodynamic parallels, the Chameleon ledger is termed for short *The Molecular Ledger*.

In the degenerate case when the network undergoes a scale reduction, statistical signatures combined with neural networks identify deviations in the distribution from some norm and redistribute elements.

XII. INITIAL PHASE: CROSS-CHAIN INTERCONNECT PROOF OF CONCEPT

The initial phase of Chameleon will be concerned with cross-chain interconnection and the focus will be on agent communication and request response mapping. For this purpose, DIONS will provide a suitable basis given the extensive communication and data payload capabilities that it already has. Thus this initial phase will be a proof of stake chain built on DIONS as a solid foundation and interconnection with the I/O Coin proof of stake blockchain. Initially for focussing on interconnection features there will be two separate blockchains: I/O Coin and Chameleon. Two separate and distinct networks.

XIII. CONCLUSION

With many disparate blockchain networks and the specialized features they have to offer and the potential extension of these systems to, for example, external device interaction, processing of results based on big data from a vast array of sources such as telecommunications monitoring, it is clear that a transparent decentralized mechanism for mapping functionality across all systems would not only provide effective access and coordination of feature sets and strengths but collectively enhance the individual features offered. The Molecular Ledger of Chameleon was proposed - validations depend on entropy and near instant logical operations running in parallel. The validation is analogous more to proving a statement coupled with the inherent complexity of the network. There is no block mining with its inherent design tendency to condense within the network. Under normal conditions a given node will not hold the entire ledger - only fragments.

REFERENCES

[1] Nakamoto, Satoshi (24 May 2009). “Bitcoin: A Peer-to-Peer Electronic Cash System”

[2] Brun, Viggo (1915). "On the Goldbach Conjecture and the number of Prime-pairs". Archiv for Mathematik og Naturvidenskab. B34 (8).

[3] I/O Coin (IOC) A decentralized cryptocurrency and blockchain ecosystem