cyber•Rating:
Crypto Property Evaluation

Dima Starodubcev[†]

Abstract. Crypto-property is one of the most rapidly growing classes of economic assets nowadays. There are several protocols that determine working principles of the cryptocurrencies as well as several protocols that enable creation and accounting of crypto assets. Owing to unique value proposition, an explosive growth of crypto property is inevitable. The new emerging class of economic assets and corresponding economic system have early stage problems such as lack of clear definitions of basic terms, weak understanding of the value proposition, lack of understanding of how to assess risks and evaluate potential growth. The widely-used corporate credit rating methodologies such as S&P, Fitch, Moody's based on IFRS, GAAP, and sovereign accounting report systems are not applicable to crypto property and thus cannot solve the above issues. This paper defines some basic terms for crypto property, outlines basic approach to their risk assessment, and proposes a decentralized solution for the evaluation of crypto property without the necessity for expensive audit procedures.

KEY WORDS

1. Evaluation. 2. Reporting. 3.Rating. 4. Crypto property 5. Risks

1. Introduction

Currently, at least 20 crypto assets are created every day using NXT, Counterparty, Open Assets, Colored Coins, and Ethereum alone. At least 3 new cryptocurrencies are announced every day on Bitcointalk [1]. Even though plenty solutions ([2], [3], [4]) try to solve the problems of the crypto property evaluation, it does not look like any of these have gotten there, as none of them provide data critical for investors, namely, compliance criteria, methodology for a cap calculation, transactional analytics, health of networks, level of adoption, and ranking system sustainable for Sybil attacks and simple to comprehend.

Traditional methodologies, such as S&P, Fitch, and Moody's, can not be used to access crypto property because they:

(1) are based on expensive reporting systems such as IFRS and GAAP that could not be applied for blockchain-based systems;
(2) are debt-based whereas existing decentralized entities are designed to rely on intrinsic value of underlying token rather than on system's debt;
(3) focus on creditworthiness and don not take into account the growth potential that is much more important at this stage;
(4) do not distinguish between permissionless crypto property and permission state-based property;
(5) rely on the existing legal system and do not take into account censorship-resistant incentivized pre-programmed rules. Blockchain systems could exist independently of the legal state-enforced systems;
(6) are not designed to work automatically as defined by the algorithm;
(7) are managed by centralized authorities;
(8) are subjective.

The above facts necessitate building a reporting system to enable trustworthy rating of the blockchain-based systems thus providing tools to the investors into crypto property.

[†] Dima Starodubcev (d@cyber.fund) is economist, entrepreneur and architect of cyber•Fund.

Bitcoin:14FBqyoP8uidAsak8uHEbwnxSSZizs293h PGP:F69E 4343 8E99 4ACC 3819 EE43 4EC7 4465 2CAA 89D4

2. Definition Challenge

Cryptocurrency, decentralized autonomous organization [5], decentralized application [6], distributed collaborative organization [7], blockchain, distributed ledger [8], cryptoassets, consensus computer [9]. This is not the exhaustive list of terms used for blockchain systems. Although all these terms are viable, they emphasize different aspects of such systems. In this paper, we propose the definitions for crypto property and its subclasses: a cryptocurrency for an independent blockchain system and cryptoassets for a dependent blockchain system. In the traditional economy, assets are any objects of any value that we believe reflects nature of discussed topic.

These definitions are not supposed to fit into existing legal framework. They are proposed to facilitate and clarify the communication between blockchain system developers and investors.

Crypto property is the possession of digital cryptographically protected data [10] those ownership can be proved by digital signature and whose existence in time can be proved by independent blockchain system. The acceptable synonyms are *digital tokens* or *tokens*, and internal capital.

There are 3 requirements that exist for independent blockchain systems:

(1) The node network should be established and uniquely identifiable via Genesis ID

(2) A system should have internal capital, a cryptocurrency that will provide healthy and competitive network consensus and immunity to double spending attacks.

(3) The core code that enables network consensus should be open source, buildable and executable by at least one open source operating system

Any system that follows these requirements can be treated as an independent blockchain system. The acceptable synonyms are decentralized autonomous organization or decentralized autonomous corporation.

These requirements have to enable a proof of ownership and a proof of existence for any crypto property. Crypto property in the form of internal capital that is an inherent component of an independent blockchain system could be defined as *cryptocurrency*. Independent blockchain systems are decentralized databases, so they can store any kind of data. This forms a universe of dependent blockchain systems.

There are 3 requirements that exist for dependent blockchain systems:

(1) They should be registered in an independent blockchain system and be uniquely identifiable via Genesis ID

(2) Registration protocol should be defined by a code, e.g. protocol markup extension: NXT AE and Monetary System [11], Standardized Contract APIs [12]) and/or natural language (protocol specification such as Open Assets protocol [13], AGS [14] or BitAlias [15]

(3) Purpose of registration should be described by a code, e.g. solidity smart contracts [16], Ricardian contracts [17], and/or natural language, e.g. digitally signed shareholders' agreement [18], NatSpec [19], etc.

Crypto property in the form of internal capital that is an inherent component of dependent blockchain system can be defined as *cryptoassets*. The acceptable synonyms are a decentralized application, DApp, cryptoassets, blockchain asset.

Cryptoproperty-based economic relations form a new economic system that overcomes limitations of the traditional economics. So, we propose to define this *cybernomics* system as it is related to crypto property. Cybernomics is in fact a working implementation of a perfect markets concept and the first economic system designed for economic operations between robot and robot, human and robot. The synonyms are crypto-economics, blockchain economics, cybernetic economic system.

Blockchain, distributed ledger and consensus computer definitions are also acceptable for crypto property but reflect technological part of it.

3. Value Proposition

There is a lack of clarity on the value proposition of blockchain systems and their product - crypto property. Hence, crypto property possesses the features that legacy state-based systems fail to grant:

(1) Efficiency: not taxable without owner intention, have no transactional limits, transactions need no settlement or reconciliation and are fast: from 1 second to 10 minutes depending on the underlying technology; tiny transaction fees, no real estate needed for decentralized network operation, no enforced compliance costs.

(2) Transparency: the underlying code is fully open source, all operations accounted on a blockchain or consensus ledger since inception and could be accounted virtually forever.

(3) Intelligence: programmable and autonomous, so it could exist by itself and be secured by math, not physics.

(4) True property: possessed by private key holders, cannot be enforced by a counterparty without private key holder's agreement; holders can choose from a variety of consensus algorithms regardless of their citizenship, residence, nation, belief, gender and even matter holder are made.

Given this, any type of economic interaction is more efficient in cybernomics than in traditional state-based economy. Cybernetic Economy Report 2015 [20] and 2015H1 [21] contains detailed analytics and cases.

4. Risk Assessment

We distinguish risks of (1) crypto property in general, (2) cryptocurrency specific, (3) cryptoassets specific and (4) for different subclasses of both currencies and assets, their own specific risks may exist. (2), (3) and (4) are beyond this paper's scope and the subject of further research. The following is the analysis of (1):

Inherent risk. The risk of weaknesses or exploitable breakthroughs in the field of cryptography. Advances in code cracking, or technical advances such as the development of quantum computers, could present risks to public-key cryptography in general. This risk is almost impossible to mitigate as the entire internet and existing financial infrastructure are built using the same public-key cryptography principles such as RSA and ECDSA. Recent researches prove quantum resistance of Lattice-based Cryptography [22] combined with Merkle-Winternitz signatures [23]. Thus, cryptography of existing networks can be upgraded to meet quantum resistance requirements on demand.

Loss risk. The risk of losing access to crypto property due to loss of private keys. As noted above, any ownership of crypto property is the possession of corresponding private keys. Private keys are usually stored in simple files and can be encrypted. In this case, there is a risk of losing a password from encrypted private keys alongside with losing a private key itself. Such risk could be mitigated using password managers, specialized hardware wallets, multi sig wallets, time-locked wallets, programmatic wills and zen brain exercises that allow owners to not forget or lose information that is impossible to restore. Regardless of zen in order to get sure at least one password allowing to decrypt another data should be stored in the crypto property owner's brain and is never to be written, pronounced, shown, or recorded. The author acknowledges that at the time of writing there are no software solutions that are (1) robust, (2) open source, (3) usable (4) functional and (5) programmatically bequeathable. Dashlane fails to meet (1) and (2), LastPass, 1Password do not meet (1), (2), and (5), Encryptr and Keepass do not compy with (1), (3) and (5). In any cases the use of web services usage needs to be extended with 2-factor auth software such as lke Authy, Duo or Google Auth that make all existing password solutions not functional enough (4). Thus, this risk remains the most critical for crypto property owners and can be mitigated only through education until software/hardware solutions will not be delivered by market forces.

Theft risk. The risk of crypto property theft. Hackers or intelligence agencies may succeed in stealing crypto property in 3 cases: weak brain wallet is used, access to your operation system is gained, or hardware/software backdoors are implanted onto a device. The most zen approach is to store private keys on a computer that (a) has never been connected to the internet and (b) has both open source hardware and software. Transactions are signed offline and then moved using a physical device connected to the computer. Currently, (b) is nearly impossible to implement as government agencies have significant influence on proprietary hardware and software companies. This risk remains the most significant one related to crypto property. Recent hardware developments, e.g. Trezor [24], help successfully mitigate this risk in case of usability and compatibility, though.

Regulatory risk. The risk of regulatory action in one or more jurisdictions. Crypto property has been under regulatory scrutiny by various regulatory bodies around the globe. Regulators cannot block or prohibit physical access to censorship-resistant classes of crypto property; however, regulatory actions could cause panic selling event followed by a significant loss of value versus to fiat currencies. This risk can be mitigated by hedging some portfolio equity using cryptoassets pegged to fiat currencies or commodities such as gold.

Miscomprehension risk. Different digital currencies and assets can have very different set of properties. For instance, Ripple is not censorship-resistant, whereas Bitcoin is. Ripple transactions are final, but Bitcoin transactions need at least 6 network conformations to get high grade of assurance. Some classes of cryptoassets are not decentralized and have issuer risks despite the crypto property per se being is secured by the underlying independent system. Continuously developed cyber•Rating methodology is geared against this risk.

5. Evaluating Approach

Risks and growth capabilities of crypto property based systems are defined by the following criteria: consensus fault tolerance, CAP theorem balance, cost efficiency, transactional performance, network scalability, decentralization grade, anonymity, strength of cryptography, censorship resistance, self-governance, computation capabilities, wealth distribution, storage capabilities, operational transparency, implementation quality, incentive structure, distribution algorithm/approach, monetary policy and consensus dependency.

This criteria should be evaluated against the system's declared market purpose and intrinsic fault tolerance requirements. Though this list cannot be considered exhaustive, we state it sufficiently comprehensive for early evaluation. purposes.

These components are divided into 3 logical groups:

(1) Computable albeit expensive: e.g. wealth distribution
(2) Computationally intractable: e.g. monetary policy
(3) Undecidable: e.g. CAP theorem balance

Thus, we can state that exhaustive and objective valuation is impossible to achieve. In order to solve this, we distinguish the objective and subjective parts of the evaluation. Proposed rating is a five-star system and includes both components with embedded feedback loops between each other.

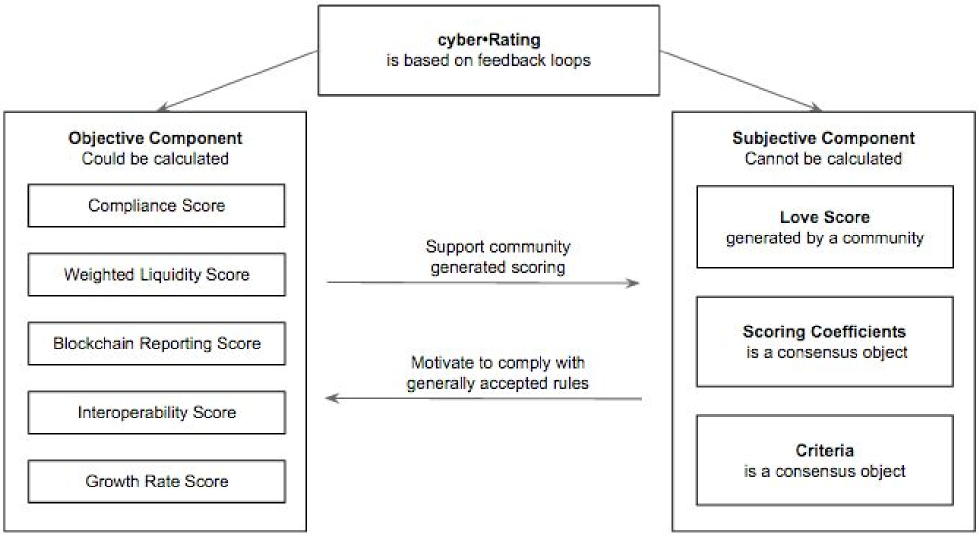

Fig. 1. cyber•Rating components

cyber•Fund's mission is to make digital investments comprehensible, accessible, easy, and safe. The objective part’s logic stems from these requirements and initially includes 5 evaluated components:

(1) Compliance Score. Compound metric reflecting availability of mandatory and recommended infrastructure. It is a set of simple “yes”/”no” statements.
(2) Blockchain Reporting Score. Compound metric showing the quality of compliance with Decentralized Reporting Standard [31].
(3) Weighted Liquidity Score. Daily turnover grade is evaluated against market cap grade.
(4) Interoperability Score. Reflects the support of universal blockchain libraries.
(5) Growth Rate Score. Scoring of compound monthly growth rate. Eventually, the most important metric that show a return on investments. Is not used in proof-of-concept implementation and is a subject to further research.

The subjective part is straightforward and is based on simple metric reflecting how people *love* a given crypto property. There is a saying in technological entrepreneurship, "Make what people love". So we propose a simple way to define what people love. To solve this, we need to propose a system of community-generated scoring (Section 7) and define a reporting system (Section 8) to support community due diligence.

In a proof-of-concept implementation [25], the centralized community generated scoring of cyber•Fund app has been used. Initial weights defined in Scoring [30] are opinionated.

To solve the problem of objective criteria definition and scoring weights between components we suggest a self-governance system (Section 13) that enables defining them at the consensus level.

So as to make proposed rating closer to real life, we should define different score weights for different lifecycle stages and types of crypto property.

6. Lifecycle and Types

Different criteria are important during the system’s lifecycle. Understanding of lifecycle stages is crucial to better understand potential risks. Having observed decentralized systems being born we can formulate the following lifecycle stages:

(1) *Project*. Triggering event is the release of a white paper and/or proof-of-concept code. At this point in time, a code or a paper are not tied to any crypto assets or cryptocurrency yet. However, a project needs tracking, because that is the earliest possible stage when you can access potential investments. A good case is Ethereum before crowdfunding started. We were sure that it has a strong foundation: proof-of-concept code and white paper and a system has economics incentives -

tokens. These are sufficient grounds to anticipate the emergence of this cryptoproperty and to evaluate it scientifically and based on the strength of the founding team.

(2) *Private*. Triggering events are the establishing of a physical network for an independent system or registering of a token for a dependent one. At this stage, all crypto property supply is in the possession of a limited group and market price cannot not be defined yet. A good case is Bitcoin: it was undergoing a private stage before the first market price appeared in 2010 on MtGox.

(3) *Pre-public*. Triggering event is a finished auditable crowd investing campaign. At this point in time, market evaluation of a cryptoasset or cryptocurrency is available, but is fixed until it becomes transferable. A good example is Ethereum during the first year of development.

(4) *Public*. Triggering event is listing on a public exchange and formation of a market price.

We propose to distinguish independent and dependent systems. That stems from the fact that these types of systems have different underlying risks, as dependent ones inherit consensus properties of a system or system(s) it depends on, but independent ones inherent it properties from underlying consensus logic. Also, independent systems need physical storage and computation network, whereas a dependent one can be build virtually on top of such a network. This two-tier architecture ensures simpler due diligence for investors and makes this abstraction layer easier to use by developers. A good analogy: state-based legal system with underlying currency and organizations that use that legal system with underlying assets. Existing rating agencies also distinguish these types of organizations.

7. Community Generated Scoring

Crowdsourcing has proved its efficiency in solving complicated problems. We suggest evaluating crypto property by the community of investors. One could say that the current market price contains all necessary information. But this price is not available during the project, private and pre-public stage. After entering into the public stage, at least 3 techniques are used to effectively manipulate the market price: obscure initial distribution, uncontrolled issuance and collusion with centralized exchanges. Analysis of manipulation art in cryptocurrency space is a subject of a standalone research. What is needed is a simple way to define what investors love. We define love as the intention of an individual to focus their attention on something in the future. This mechanic is successfully used for repository rating by Github, for signal calculation by AngelList, and in fact by any successful web service. We suppose that graph of paid by token actions which mark a crypto property as favorite could be a trustless source of proposed evaluation.

The following 3 approaches could be implemented in order to calculate a score that is resistant to Sybil attacks:

(1) *One account one vote*. This approach requires paid account registration to make the rating system resistant to Sybil attacks.

(2) *Votes weighted by token holdings*. It requires massive Augur like [26] initial distribution to make it work.

(3) *Votes weighted by a share in the economy*. Failsafe approach, although its require implementation would be complicated, as addresses and their balances should be proven for every user for every blockchain.

In our proof-of-concept implementation, we use the first approach based on twitter accounts to minimize possible Sybil attacks, and it demonstrates interesting results [25]: the most advanced cryptocurrencies are rated higher than the most capitalized. This means lower risks and higher probability of a profitable long-term investment decision. In the first version of cyber•Fund protocol, the first approach will be implemented also using blockchain registered accounts. Votes could be positive or negative. Proof of this hypothesis shall need time and is a subject for future research.

8. Blockchain Reporting System

Transparency is critical for investment decision making. Developers of decentralized systems both independent or dependent ones should realize that lower system's transparency means lower probability of a positive investment decision. Traditional finance is based on quarterly reporting and annual auditing. That makes no sense whatsoever for blockchain entities as they report every block with some reorganization probability and are no fit for consensus ledgers, whose state is always final. Thus, reporting could be much more frequent, precise, and free from the necessity to audit.

To understand blockchain reporting, all data necessary for decision making needs to be categorized into 3 groups based on availability principle:

(1) *Blockchain data*. Blockchains are hardly optimized per se, therefore do not store data not required for consensus and data possible to calculate from it. Moreover, the diversity of blockchain software and blockchain APIs make it hard to run and integrate all of them for any single service.

(2) *Calculated data*. Even critical information for decision making, such as current supply of tokens, are often not provided by core API, but rather has to be calculated from unspent transaction outputs of coinbase transactions.

(3) *Off-chain data*. Decentralized nature of blockchains enables the creation of centralized services that lock user's private keys and track transactions off-chain. Presently, virtually all trade happens off-chain. The situation does not seem to change soon even with the help of projects like Sidechains, Eris/Tendermint, ChainDB, OpenChain, Multichain, and Strato. Hence, off-chain data is critical for evaluation.

Thus, comprehensive understanding requires that every client wishing to observe aggregated blockchain reporting on a set of entities should (1) store and sync every block header of every chain in order to verify it, (2) redo immense amount of calculations locally, and (3) parse significant amount of trusted data. Still, (4) designing such software takes a lot of effort. (1) and (2) are not acceptable by the market due to continuously increasing demand for mobility, (3) needs a costly audit procedure, though (4) seems unfeasible for any given single entity.

Developers of autonomous systems are motivated to provide as much as possible effortless experience as possible for investors of any kind, but there is no agreed solution to guide coordinated movement.

We can use EVM based smart contracts to verify block data in a trustless way. In the case of Bitcoin that uses SHA-256 for proof-of-work verification is feasible inside EVM and already has working implementation [27]. But verification of proof-of-work like scrypt or X11 is computationally expensive. Proof-of-stake or consensus ledgers verification require full implementation inside EVM that is also expensive - and still leaves us with a huge chunk of data we have to trust and/or calculate. The only way to solve this problem is to reject the idea of trustless reporting until consensus computers become significantly cheaper, and implement the roles of reporter and observers who will be incentivized to report truthfully.

We are going to solve (1) through (4) by providing (a) simple and flexible reporting requirements in a machine-readable format by any trusted service of any decentralized system in a way that (b) reporters will be motivated to report truthfully, and (c) any other observer will be able to use this reporting and claim on a quality of observed reporting. Thus, the market will be able to reach an equilibrium state of reality without storing (1) and calculating (2), the necessity to audit (3) and in a highly decentralized and distributed manner (4).

To solve (a) we can take xBRL as a basis. xBRL [28] is a business reporting standard that is being actively developed and adopted by businesses and governments. But xBRL has some obvious downsides: it is very difficult to understand, as it has more than 100 specifications providing high-level abstraction layer and describing *how*, rather than *what* must be reported; also, it is based on cluttered XML, whereas current web development is based on JSON. We propose Decentralized Reporting Standard, or DRS (Section 9), which is one page long, precisely describes the domain area and is JSON based. In fact, DRS could work as an extension to xBRL and, if needed, can be deterministically and programmatically converted to xBRL.

To solve (b) we assume that any reporter that operates using any given crypto property is motivated to see the value of a given crypto property grow and could collude and/or provide corrupted reporting. Proposed incentive structure includes the opportunity to earn a part of transactional fees generated by a protocol and a penalty for providing corrupted reports. Every reporter should have a collateral to be granted the ability to report. The amount of that collateral is a consensus variable and can be different for different grades of crypto property. Collateral have a vesting period. Observers of blockchain reporting have the ability to cast positive or negative votes on reporters. Votes can be positive and negative. Votes are weighted by token holdings. Earned fees are split between reporters based on contribution, vested collateral balance, and gained positive/negative votes. Depending on the resulting score, collateral balance increases or decreases every distribution round. The reporters are able to revoke reports in case of unforced errors but have no ability to hide corrupted facts.

Observers votes assuming that every observer can verify blockchain data, calculated blockchain data, and trust the off-chain data. Trusted off-chain reporting create the demand on the part of observers for better transparency and verifiability of this particular data. If a reporter and a data provider are not the same entity *TLSnotary* mechanism [29] could be used by reporters to make such reporting from trusted data providers verifiable.

9. Decentralized Reporting Standard

Decentralized Reporting Standard is built on 2 assumptions:

(1) Markets and blockchains are essential sources of reliable reporting

(2) “Transactional fees” is the only viable business model

Instead of traditional “down-top” reporting when an entity must aggregate and proof information on all transactions in order to obtain market capitalization, DRS could be used in both directions. On the one hand, it allows investors use capitalization without having any proofs except market price, supply and the fact of existence. On the other, it ensures sufficient level of confidence for all operations if an entity has taken effort to provide relevant data. Definition of an approach is due to market forces. We distinguish 3 types of possible reporting information: critical, important and recommended.

Without critical information, no investment decision can be made. Availability of such information answers the question, “What happens”, as it allows to calculate market capitalization and provide proof that any given entity still exist. This information includes:

(1) *Genesis ID*. ID of a blockchain, ledger, asset or record that could uniquely identify the object of reporting and programmatically bind reporting with blockchain/ledger data deterministically.

(2) *Block Proof*. This includes block/ledger height, unix timestamp, block/ledger hash, previous block/ledger hash, block/ledger merkle root; varies for different consensuses. This data is required for the potential user in order to verify reporting data.

(3) *Current Supply*. The amount of tokens that exists at a given height. This amount includes token supply that can be released unpredictably by any single person or a small group. Tokens to be released or created in future by consensus protocol are outside the scope of this metric. Current supply could be treated as generally accepted shares outstanding definition.

(4) *VWPA* or *Volume Weighted Price Average* for the majority of markets. This metrics is difficult to aggregate.

Important information is basically essential data since it allows to understand underlying network economy and compare it with another network. This information allows to give basic comparative foundation to answer the question “Why that happens”:

(1) *Token Flow*. Explains why token supply has been changed. Includes sources (emission or harvesting), and allocations of tokens (mining, burning, etc).

(2) *Transactional Performance.* Explains operational performance in terms of transactional load, averages, and margin.

Recommended information is usually system specific, which means it cannot be reported, but is needed in order to understand unique transaction structures, deep economy and health of the physical or virtual network.

(1) *Transactional Structure*. Amounts, averages and margins of transactions by types such as asset creation, account registration, arbitrary messaging etc. In order to solve the problem of extracting semantic meaning similar to HTML Blockchain Markup Language could be developed later.

(2) *Performance Metrics*. E.g. processing time, block size or broadband.

(3) *Consensus Variables*. Should be reported for each consensus algorithm that has been used to create a particular block: difficulty, hash rate, active delegates, gas limit, gas usage, gas price etc.

(4) *Value Velocity.* Includes days destroyed and a structure of money velocity.

(5) *Accounts Analytics.* Includes amount of addresses used, the total balance of addresses used in native tokens, distribution structure and Gini Index.

These parameters are key to understanding how the network operates. By analyzing in a way similar to financial reporting comparison, investors could make more accurate decisions. In order to define reporting structure, we represent the domain of crypto property as a simple graph, whose edges are systems with their states, and vertexes are exchange ratios.

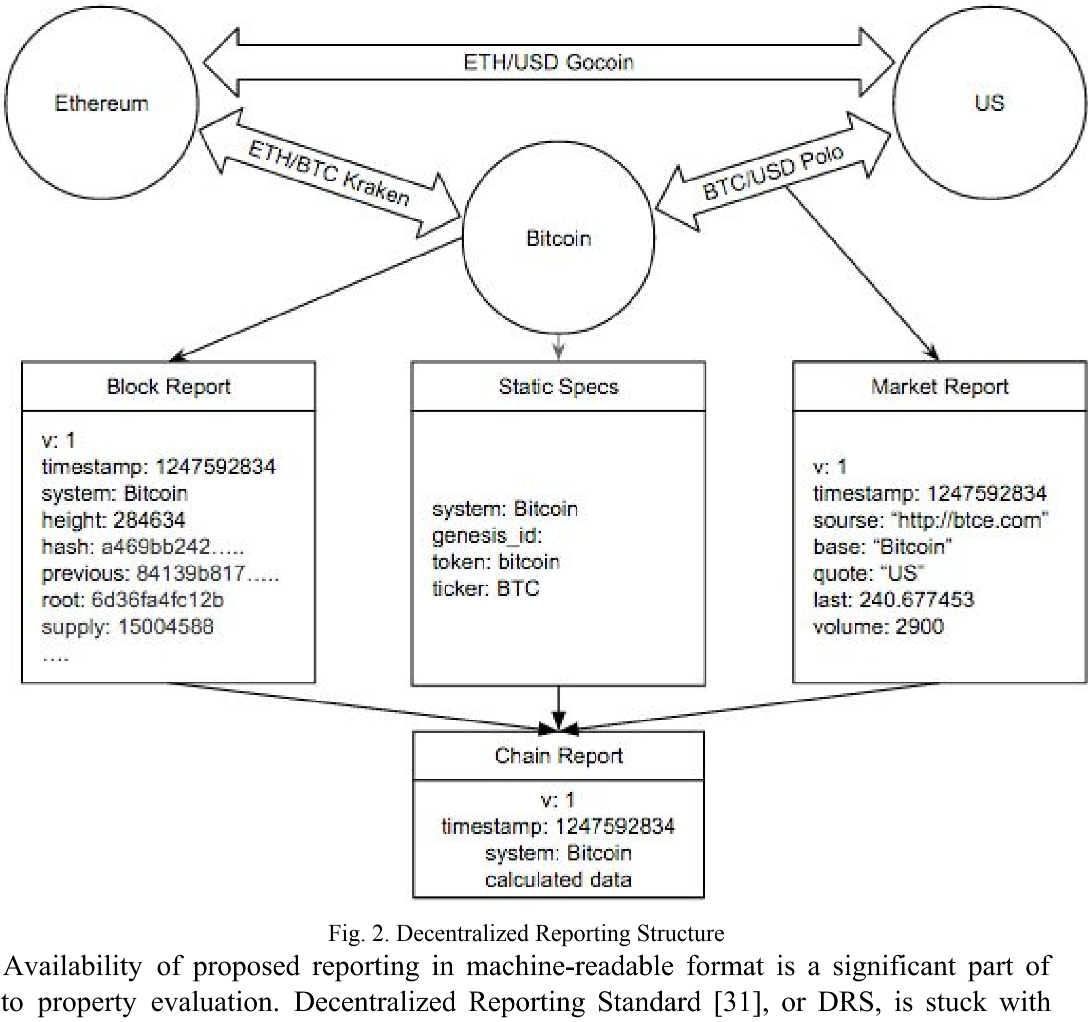

Fig. 2. Decentralized Reporting Structure

Availability of proposed reporting in machine-readable format is a significant part of crypto property evaluation. Decentralized Reporting Standard [31], or DRS, is stuck with semantic versioning and inherent component of cyber•Rating. We propose 3 type of reports: market report, block report and chain report.

10. Market Report

Price data is continuous by nature and is complex to aggregate, as hundreds of markets may exist, each one with varying liquidity levels. The key purpose of the market report is to gather information necessary to calculate volume-weighted price average. Every market report reflects last observed price in the form of a "base vs quote" ratio from a particular market and trade volumes for last 24 hours. The market report only contains facts and no valuations. It can be supplied by the market provided or by a third party reporter. WVPA is calculated based on all market reports trusted by reporter using chain report.

11. Block Report

Blockchain data is discrete by nature and is in a certain state. Existing cash flow classification to processes observed in cybernomics is suggested for better understanding of a block report..

(1) *Investment Activity.* Any operation involving emittance or burning of tokens.

(2) *Operational Activity*. Any operation involving a fund increase or reduction that is maintained by consensus. Transactional fee collecting is considered as *revenue*. Rewarding participants for proof-of-work, proof-of-stake, proof-of-research or any other automated tasks are considered a *cost* because these activities are mandatory for autonomous entity operations.

(3) *Financial Activity.* Any operation entailing a debt fund increase or reduction that is maintained by consensus. This type of activity has not been used by blockchains as there is no technical and organizational foundation exist yet. But we do not exclude that possibility in the future.

A closer look at Bitcoin reveals presence of investment and operational activity. At the time of writing, 25 bitcoins are emitted per block as an investment. An average of 0.2 bitcoin is collected as revenue from transaction fees. Investments and revenue form a virtual budget 25.2 bitcoins. All of this budget is immediately spent as costs of mining. In line with consensus, Bitcoin budget is always 0. Dash is more complicated example. 4 dashes are emitted per block as an investment. ~1 dash is collected as revenue from transaction fees. Investments and revenue form a budget of 5 dashes. 45% of this budget is instantly allocated to miners and 45% to master node operators as costs of operations. Remaining 10% is added to the budget which has an embedded consensus mechanism of spending every superblock. Budget varies depending on revenue and development needs. BitShares has an even more complicated structure, but the logic remains the same.

Every block report reflects a state of a particular chain in a structure understandable to investors. Block report should contain critical and important information. Block report may contain recommended information. This simple approach allows to compare key blockchain operations provided that valuation against a unit of account is conducted periodically.

12. Chain Report

Chain report is needed to observe evaluated discrete blockchain data against continuous market data. Reporters can calculate it on per-block, per-hour, per-day basis, depending on a level of transparency a given entity intends to reach. We recommend evaluating operations against US dollar and bitcoin. For dependent blockchain systems, valuations against cryptocurrency of a blockchain it depends on is also recommended.

13. Self-governance

We propose a system where all critical parameters will be defined by consensus of token holders. We are going to use the generalized concept of consensus variables.

Every token holder can register a variable and define validation rules. Every token holder can set desired value on every registered variable. In order to solve voting apathy problem, we are going to use delegation of voting rights. Votes are weighted by token holdings. This mechanism is already being successfully used by BitShares. In our case the following variables will be defined by consensus:

(1) Hard forks of the core contracts
(2) Transaction fee per actions
(3) Scoring coefficients definition
(4) Requirement for the collateral

Funding and its use are beyond this paper's scope, and so are other necessary components of a proposed cyber•Fund investment protocol.

14. Conclusion

We have proposed a system for crypto property evaluation without relying on centralized rating agencies and expensive audit procedures of accounting and bookkeeping. We started from the analysis of conventional rating and reporting approach and concluded on the impossibility to use it as a basis for crypto property evaluation. We have defined the basic terms of domain research, analyzed risks specific to crypto property, and disclosed downsides of existing tools. Our proposed system is a decentralized methodology of rating calculation and decentralized reputation-based system of blockchain reporting. The system is technologically agnostics and does not rely on any counterparty. It is modular and can be improved as such.

References

[1] No Author. "Announcements (Altcoins)" (accessed 22 December 2015) https://bitcointalk.org/index.php?board=159.0

[2] No Author. "Crypto-Currency Market Capitalizations" (accessed 22 December 2015) http://coinmarcetcap.com

[3] No Author. "360 degree Overview of Cryptocurrencies" (accessed 22 December 2015) http://coingecko.com

[4] No Author. "Coincap" (accessed 22 December 2015) http://coincap.io

[5] V. Buterin. "Ethereum: A Next Generation Smart Contract & Decentralized Application Platfrom" http://blog.lavoiedubitcoin.info/public/Bibliotheque/EthereumWhitePaper.pdf

[6] Johnston D. et al. "The General Theory of Decentralized Applications" https://github.com/DavidJohnstonCEO/DecentralizedApplications

[7] Valkenburgh P., Dietz J., Filippi P., Shadab H., Bollier D., Xethalis G., "Distributed Collaborative Organisations" http://bollier.org/sites/default/files/misc-file-upload/files/DistributedNetworksandtheLaw%20report,%20Swarm-Coin%20Center-Berkman.pdf

[8] Swanson T. "Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems" http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf

[9] Luu L., Teutsch J., Kulkarni R., Saxena P. "Demystifying Incentives in the Consensus Computer" https://eprint.iacr.org/2015/702.pdf

[10] No Author. "Digital Data" in Wikipedia (accessed 22 December 2015) https://en.wikipedia.org/wiki/Digital_data

[11] No Author. "Whitepaper:Nxt." (accessed 22 December 2015) http://wiki.nxtcrypto.org/wiki/Whitepaper:Nxt#Asset_Exchange

[12] No Author. "Standardized Contract APIs" https://github.com/ethereum/wiki/wiki/Standardized_Contract_APIs

[13] Charlon F. "Open Assets Protocol" https://github.com/OpenAssets/open-assets-protocol

[14] Amazon. "Announcing AGS & BitShares Allocation." Bitsharestalk (accessed 22 December 2015) https://bitsharestalk.org/index.php?topic=1863.0

[15] Georgiev Malahov Y. "BitAlias I Aka Usernames for Bitcoin." Medium (accessed 22 December 2015) https://medium.com/@yanislav/bitalias-7b66bffed9d8

[16] No Author. "Solidity." (accessed 22 December 2015) http://solidity.readthedocs.org/

[17] Grigg I. "The Ricardian Contract." http://iang.org/papers/ricardian_contract.html

[18] Starodubcev D., Guryeva M., Lvov V., Lomashuk K. "cyber•Fund Genesis Agreement" https://cyber.fund/cyberFund_Genesis_Agreement.pdf

[19] No Author. "Ethereum Natural Specification Format." https://github.com/ethereum/wiki/wiki/Ethereum-Natural-Specification-Format

[20] Starodubcev D. Lomashuk K. "Cybernetic Economy Report 2015" https://cyber.fund/cyberep

[21] Starodubcev D. Lvov V. "Cybernetics Economy Report 2015H1" https://cyberep.cyber.fund

[22] Micciancio D., Regev O., "Lattice-based Cryptography" http://www.math.uni-bonn.de/~saxena/courses/WS2010-ref5.pdf

[23] Buchmann J., Dahmen E., Ereth S., Hulsing A., Ruckert M. "On the Security of the Winternitz One-Time Signature Scheme" https://eprint.iacr.org/2011/191.pdf

[24] Goodman L.M., "Tezos: A Self-Amending Crypto-Ledger" http://tezos.com/position_paper.pdf

[25] No Author. "Tracking" (accessed 22 December 2015) https://cyber.fund/tracking

[26] Peterson J., Krug J. "Augur: a Decentralized, Open-Source Platform for Prediction Markets" http://augur.link/augur.pdf

[27] No Author. "A bridge between the Bitcoin blockchain & Ethereum smart contracts" (accessed 22 December 2015) http://btcrelay.org/

[28] Engel P., Hamscher W., Shuetrim G., Kannon D., Wallis H. "Extensible Business Reporting Language" http://www.xbrl.org/Specification/XBRL-2.1/REC-2003-12-31/XBRL-2.1-REC-2003-12-31+corrected-errata-2013-02-20.html

[29] No Author. TLSnotary - a mechanism for independently audited https sessions https://tlsnotary.org/TLSNotary.pdf

[30] D. Starodubcev, V.Lvov, “cyber•Rating Scoring” https://github.com/cyberFund/cyberrating/blob/master/scoring.md

[31] D. Starodubcev, V.Lvov, “Decentralized Reporting Standard”. https://github.com/cyberFund/cyberrating/blob/master/DRS.md