BITCOIN & CO: AN ONTOLOGY FOR CATEGORISING CRYPTOCURRENCIES

UDK 004.738.5:336.7456 / JEL E42 ; E58 / REVIEW ARTICLE

JEFF HERBERT
PGDipCIS
SCHOOL OF COMPUTER AND MATHEMATICAL SCIENCES,
FACULTY OF DESIGN AND CREATIVE TECHNOLOGIES,
AUCKLAND UNIVERSITY OF TECHNOLOGY
AUCKLAND, NEW ZEALAND
jeff.herbert@aut.ac.nz

MARTIN STABAUER
ASSISTANT
INSTITUTE OF DATA PROCESSING FOR SOCIAL SCIENCES,
ECONOMICS AND BUSINESS, JOHANNES KEPLER
UNIVERSITY LINZ
LINZ, AUSTRIA
martin.stabauer@jku.at

ABSTRACT

As cryptocurrencies like Bitcoin become more and more influential and widely spread, a steadily growing target audience coming from the most diverse disciplines takes notice and interest in them. There are lots of discussions going on around the globe, whether or not Bitcoin can be considered a "real" currency and how to deal with its ecosystem from a juridical point of view as well as within the borders of monetary policy.

This paper proposes a model and, based thereupon, an ontology for categorising the different manifestations of cryptocurrencies available today. It takes into consideration the relevant publications by the ECB and the US FinCEN and tries to find a common ground. We address various aspects related to the subject like compatible technologies, applications and their interconnections. The findings are consequently tested and validated using appropriate methodology.

Our work results in an ontology implemented in languages of the semantic web that covers many of today's cryptocurrencies and categorises them by the aspects discovered earlier in the paper. This ontology contributes to a fairly new knowledge domain where varying interpretations and misunderstandings are common occurrences.

KEY WORDS: cryptocurrencies, currencies, bitcoin, ontology, semantic technologies.

1. INTRODUCTION

Today it is getting more and more difficult to ignore Bitcoin and other forms of cryptocurrencies. As the former Director of the U.S. Mint Ed Moy states: "Cryptocurrencies will likely play a pivotal role to modernizing the notions of money and finance and help usher in help a new global economy worthy of the 21st century" (Moy, 2015). While it is still unclear where the development will lead, it seems that governments, jurists and financial institutions are well advised to give more attention to the advances being made.

The financial crisis in recent years led to a loss of trust in financial intermediaries, trading platforms and payment systems. One of the most outstanding innovations of cryptocurrencies is their ability to avoid the need for a trusted third party (Blundell-Wignall, 2014). This also includes dramatically lower transaction fees, especially for international transactions. Estimations say that using Bitcoin over traditional payment providers could theoretically save over 100 billion dollars of transaction costs p.a. (Goldman Sachs 2014).

The lack of regulations and legal definitions lead to a very unclear situation. While some governments are starting to recognise cryptocurrencies, they are regulated against by others. The Chair of the Board of Governors of the U.S. Federal Reserve System said "It's important to understand that this is a payment innovation that's happening outside the banking industry. […] The Federal Reserve simply does not have the authority to regulate Bitcoin in any way." (Yellen, 2014). The ECB states that "regulatory responses are likely to be more effective if they are internationally coordinated" (ECB, 2015).

This paper should contribute to clarify the current state by proposing definitions and classifications for various types of cryptocurrency economic systems. In chapter 2 we define common terms that are used throughout the paper and in the following chapters we propose properties for currency schemes and try to find categories that they can be subsumed into.

2 DEFINITIONS

2.1. Money

From an economic point of view, money traditionally is defined as having three primary attributes (ECB, 2012; Surowiecki, 2012):

- It may be used as a medium of exchange in the role of an intermediary in trade to avoid the need for barter.
- It needs to act as a standardised numerical unit of account, thereby measuring the value and cost of goods, services, assets and liabilities.
- It has to be able to store value where the money can be consumed at a later date.

From a legal perspective, anything that is used widely to exchange value in transactions is usually seen as money (ECB, 2015). Money has been historically found in written records since 3000BC, where it was used as a commodity for trade and social exchange. Over time usage of money became more prevalent in scope as it encompassed entire countries, first using the base value of the metal of the coinage as the basis of value, through to the 15th century where paper based money was first used in China. This evolution demonstrates that the value of money depends on the willingness of economic agents to accept it, no matter what material the money is made of. Trust is the central requirement for money where all participants agree to a value of the commodity used as money (Skaggs, 1998; Surowiecki, 2012).

2.2. Currency

There are various definitions of currency. Nelson (2011) defines currency as "a country's currency that is backed by that country's government. This backing can either be by fiat – government regulation or law – or by commodity such as the Gold Standard the U.S. used to use". FinCEN (2013) regulations define currency (also referred to as "real" currency) as "the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of issuance". ECB (2012) states that currency is any legal tender designated and issued by a central authority. Currencies are regulated and centralised, and each country sets out a system that governs how the currency functions and provides monetary policy to the population that determine its monetary value.

Taking the common elements of these definitions into account, we can state that for a currency to exist, it must be written into the government regulations of a country and legally issued by a central authority of that country. This also leads to the conclusion that as soon as a single country accepts any cryptocurrency as legal tender this cryptocurrency becomes a legitimate and lawful currency in that country and as a consequence a foreign currency in every other country of the world.

2.3. Cryptocurrency

"Cryptocurrency" is commonly used to describe blockchain-based transaction systems and economic systems. We acknowledge the entomology of word cryptocurrency as being derived from: (a) cryptography, in recognition of the cryptographic methods employed by the blockchain ecosystems, and (b) currency, in recognition that the blockchain ecosystem is providing a monetary transaction system.

The Oxford dictionary defines cryptocurrency as "a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank: 'decentralised cryptocurrencies such as bitcoin now provide an outlet for personal wealth that is beyond restriction and confiscation'".

However, as cryptocurrencies are not regulated by any government, they cannot be defined as a currency in accordance with the currently accepted definition of currencies as described in 2.2, and as such, the term cryptocurrency is used as a label to describe blockchain-based transaction systems. In addition to cryptocurrency we also use the term "Virtual Currency Scheme" as proposed by the ECB and described in chapter 2.4.

2.4. Virtual Currency Scheme

The ECB uses the following definition for virtual currencies: "a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money" (ECB, 2015). Based thereupon, the term "Virtual Currency Scheme" (VCS) is used "to describe both the aspect of value and that of the inherent or in-built mechanisms ensuring that value can be transferred" (ECB, 2015).

The earlier definition "A virtual currency is a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community" (ECB, 2012) was revoked by this new term. VCS can therefore be seen as a superclass of cryptocurrencies, this is also reflected in our model.

"Virtual Currency Schemes, such as Bitcoin, are not full forms of money as usually defined in economic literature, nor are virtual currencies money or currency from a legal perspective. Nevertheless, VCS can/may substitute banknotes and coins, scriptural money and e-money in certain payment situations." (ECB, 2015)

In comparison, FinCEN guidance focusses on the "convertible" aspect of virtual currencies and the participants involved in the exchange of "convertible" virtual currencies into fiat currency. FinCEN acknowledges the decentralised characteristic of cryptocurrencies, but does not consider types of cryptocurrencies as their focus

is the Administrators and Exchangers of Virtual Currency (FinCEN, 2013). As such, FinCEN guidance does not provide much insight into types of Virtual Currency Schemes.

2.5. Currency Scheme

We define Currency Schemes as inclusive of any type of fiat or local currency or Virtual Currency Schemes used for transactions without necessarily meeting the definition of currency.

3. CRYPTOCURRENCY ECOSYSTEM

3.1. Primer

Developed by Satoshi Nakamoto and first introduced with the creation of Bitcoin, cryptocurrencies are a new form of virtual currency. A cryptocurrency is a purely decentralised peer-to-peer electronic cash system and is the first technology to successfully overcome the requirement for a centralised party to validate transactions. The cryptocurrency ecosystem combines several blended features to provide decentralised money, mint and transaction processing functions, all stored on public ledgers within a quasi-anonymous framework (Brikman, 2014).

Nakamoto defines an electronic coin as a chain of digital signatures in the form of blocks (Nakamoto, 2008), which when chained together cryptographically forms the cryptocurrency blockchain. The blockchain is the public ledger, a database of all transactions ever executed in the currency, and shared by all nodes participating in the cryptocurrency ecosystem.

Cryptocurrencies use public-key cryptography to validate transactions between all participants. The public key can be considered as the participant's account number whilst the private key represents the participant's ownership credentials. All participants have digital wallets that are used to store the private keys, as well as the digital signatures that represent the cryptocurrency bitcoin entitlements that the participants owns. The use of digital signatures ensures transactional integrity and non-repudiation. (Peteanu, 2014)

As a peer-to-peer decentralised technology, cryptocurrencies historically rely on a network of low cost computers called "Miners" which run software that performs the primary functions within the cryptocurrency ecosystem. This software, used by each node, creates new blocks through cryptographic mechanisms (referred to as Proof), incentivises miners for utilising their computing resources by rewarding them with bitcoins when the node discovers a new block, maintains a full copy of the blockchain; and participates in the transaction validation process.

3.2. Transactions

Cryptocurrency transactions are a message between participants, and consists of 3 segments: (i) Signature, the originator's digital signature signed with the originator's private key so that other cryptocurrency nodes can verify the message really came from the originating participant; (ii) Inputs, a list of the signatures of transactions already in the ledger where the originator was the recipient of the bitcoins and the input bitcoins are the funds the originator uses in the transaction; (iii) Outputs, a list of how the funds in the inputs should be distributed. All the funds in the inputs must be redistributed in the outputs, so the originator will pay the recipient the required fund and pay themselves the remainder as change.

As the recipient is identified by their public key, cryptocurrency transactions can be traced through the blockchain through to the beginning of the creation of the bitcoin. This forms the mechanism for checking the ownership of bitcoins. Publically verifiable transactions by any node avoids double spending and provides a high degree of certainty to the participants of the cryptocurrency ecosystem.

When a transaction occurs it is broadcast onto the cryptocurrency network for verification by the nodes to prevent double spending of the bitcoin. As nodes receive the transaction they independently verify the validity of the transaction, and the greater number of nodes accepting the transaction, the less likely it is to be a double spend. Participants can quickly ascertain if there are issues with the validity of the transaction if the immediate responding nodes reject the transaction.

4. PROPERTIES OF CURRENCY SCHEMES AND CRYPTOCURRENCIES

We have created a model for currency schemes based on ECB and FinCEN definitions, and identified the characteristics of the various types of Virtual Currency Schemes. We have applied and extended the initial ECB Virtual Currency Schemes model to include a more properties of existing (and potential future) cryptocurrencies with the outcome of create classes for cryptocurrencies. The following sections describe the characteristics that form the Currency Schemes and cryptocurrency classes.

4.1. Legal Status

Legal Status is a fundamental characteristic of Currency Schemes because a currency by definition must be incorporated into law and issued as Legal Tender by a government of a country, and as such is Regulated by the government. Other Currency Schemes and cryptocurrencies are not under the control of any government, are therefore not Legal Tender, and as such are Unregulated.

4.2. Centricity

Centricity is a new characteristic for Currency Schemes with the advent of the decentralised nature of cryptocurrencies. The peer-to-peer design of cryptocurrencies was intended to mitigate the risks associated with a central party performing transaction processing, as well as reduce threat of shutdown by a targeted attack on a node, distributed denial of service, or shutdown of the cryptocurrency through government intervention. The types of Centricity include: (i) Centralised, where a central entity undertakes transaction processing; (ii) Distributed, there is no central entity and transaction processing is undertaken through the peer-to-peer network of anonymous "miner" nodes, examples including cryptocurrencies such as Bitcoin (bitcoin.org) and NXT (nxt.org); (iii) Decentralised, a central authority controls the transaction processing which is undertaken by a network of authorised ledger nodes, such as Ripple (ripple.com).

4.3. Format

The Format for Currency Schemes is a relatively new characteristic as a result of the digital age of computing. Currency Schemes have historically been based on physical coins or paper, however most Currency today is represented in a Digital format without any underlying association with value of a physical asset (such as the abandoned Gold standard). The ECB also defines Format as shown in Figure 2 in Section 4.1.

4.4. Control & Issuance

The Control & Issuance characteristic defines the authority that controls the monetary policy and supply, and that is allowed to generate units in a Currency Scheme (ECB, 2015). We have identified three types of issuer: (i) Government, where the regulated central banking authority can issue new money; (ii) Private, where the owner of the Currency Scheme can issue new private money into the private economic system; (iii) Network, where the peer-to-peer network can issue cryptocurrency units. For example, Bitcoin network automatically issues bitcoins to miners for successful hash solutions based of Proof-of-Work, whilst the NXT network automatically issues nxtcoins to miners based on Proof-of-Stake. However, SolarCoin uses an incentive-based allocation method for their SolarCoins, which are distributed manually by the owner on the basis that a participant can prove that they have generated 1MWh of solar energy (solarcoin.org), making Solarcoin a privately issued cryptocurrency.

4.5. Validating System

As a characteristic of Currency Schemes, the "Validating System" is defined by the ECB as "the methods used for validating the transactions made and securing the network" (ECB, 2015) with the primary goal of preventing double spending of money. The Validation System is a technical construct or mechanism that validates each transaction. There are three forms of Validating Systems: (i) A Bank computer system, which provides a centralised accounting ledger for debiting and crediting accounts using fiat currency; (ii) A Private system, where a private organisation undertakes some form of centralised function for debiting and crediting accounts using a form of private currency in a private economic system; (iii) Algorithm-based, distributed or decentralised transaction processing of cryptocurrency bitcoins for debiting and crediting accounts within the cryptocurrency economic system.

Cryptocurrencies use a variety of algorithms for validating transactions, the primary algorithms being Proof-of-Work and Proof-of-Stake, and sometimes a combination of the two algorithms. Proof-of-Work cryptocurrencies use specific hashing functions for block discovery, with leveraging a principle of hashing where a digest of a hash is relatively easy to verify, but very difficult to create. Proof-of-Work has had several weaknesses identified including security, scalability, performance, reward system, power consumption (Courtois, 2014; Kaye, 2014), hence Proof-of-Stake algorithms were proposed and implemented in an effort to overcome several of these problems. Proof-of-Stake means proof of ownership of the currency, and requires the owner to hold a certain amount of currency for some time before it is able be used to mint a block (Buterin, 2013; Kaye, 2014). With Proof-of-Work, the probability of minting a block depends on the work done by the miner, however with Proof-of-Stake the probability of solving the block is determined by how many coins have been sitting in the miner's wallet for at least 30 days. Proof-of-Stake is used to build the security model of a peer-to-peer cryptocurrency as part of its minting process, whereas Proof-of-Work mainly facilitates the minting process and gradually reduces its significance (King & Nadal, 2012). Proof-of-Stake also has potential security issues of a different nature to Proof-of-Work that will need to be overcome (King & Nadal, 2012; Vasin 2014)

4.7. Source

Addition of Source as a characteristic is a reflection on the transparency that the Currency Scheme provides to the stakeholders of the Currency Scheme. There are of course two types of Source – Open-Source and Closed-Source. Open Source is widely promoted for allowing anyone to investigate the source code to assess its functionality, quality, reliability, identify security issues and such like (e.g. Money et al., 2012). In order to foster trust in a distributed economic system such as a cryptocurrency, most cryptocurrencies are released as Open-Source. Closed-source maintains all code as private and confidential, and vendors do not release source code to stakeholders. As such, stakeholders must have complete trust in the Closed-source vendor, and cannot easily verify functionality or identify security risks.

4.8. Purpose

As demonstrated in this section, new characteristics are being defined through the introduction of cryptocurrencies into the family of Virtual Currency Schemes as defined by ECB (2012, 2015). Some cryptocurrencies have been designed to overcome specific issues, some have been designed to improve resource utilisation, whilst yet others have a broader vision that use combinations of methods to create new functions and applications that are grounded in cryptocurrency methodology.

Each cryptocurrency transaction includes a script capability that can provide a certain rules-based scripted intelligence to be added to each transaction. This is like each transaction having a Harry Potter ™ "Dobby" house-elf holding a gold coin, and who is able to evaluate various conditions and inputs before committing the spending of that coin. First generation cryptocurrencies such as Bitcoin provides a basic script capability that is used to ensure integrity of the transaction flow for each transaction. However, second generation cryptocurrencies have additional functions that improve the level of Dobby intelligence so that smarter decision making can be implemented without requiring human input. In addition, second generation cryptocurrencies can have capabilities that allow applications to integrate with the blockchain directly and run as distributed applications.

The definition of the Purpose characteristic in the context of this work is to classify any additional benefit over and above the standard transaction function of a Currency Scheme. We have identified three Purposes currently in use, as follows.

(i) Transaction Only Currency Schemes have the sole purpose of debiting and crediting accounts and validating transactions. Examples of Transaction Only Currency Schemes include Fiat Currency, Warcraft Gold, Linden Dollars and cryptocurrencies that are transaction only, such as Bitcoin.

(ii) Transaction and Application type generally applies to second generation cryptocurrencies, where in addition to transaction capabilities, the cryptocurrency has some form of additional application or function integration that is useful outside of the transaction aspect of the cryptocurrency. Third party applications can directly utilise these features in the cryptocurrency blockchain.

(iii) Transaction and Application Platform are second generation cryptocurrencies that provide a "Turing Complete" platform for third party application development and support for distributed applications (DApp), where no central node is running the application.

4.9. Function Integration

Following from Purpose, the characteristic Function Integration is used to further refine two types of cryptocurrencies: (i) those that have Native embedded blockchain applications or function integration; and (ii) those that have External blockchain applications or function integration. This distinction is essential because embedded functionality changes and innovations are provided by the cryptocurrency developers, whilst external functionality and innovations are provided by third party developers.

5. CATEGORIES OF VIRTUAL CURRENCY SCHEMES

While the quantity of established currency schemes (see 5.1.) stays straightforward and stable, the number of cryptocurrencies changes almost daily. At the time of writing, around 600 cryptocurrencies can be distinguished (coinmarketcap, 2015). This is why there is a need to introduce generically applicable categories, which not only cryptocurrencies available today can be sorted into but also are prepared to accommodate future implementations.

While FinCEN (2013) focuses on the distinction between centralised and decentralised virtual currencies, we go more into detail and differentiate even more types. The centralised virtual currency schemes are described in section 5.1. and the decentralised virtual currency schemes described in the later sections.

5.1. Summary of established currency schemes

Clearly, the first category is the established type of fiat money. This type not only includes the physical format in the form of banknotes and coins but also digital formats in the form of government backed E-money (EU, 2009) and commercial bank deposits.

The second category is called LOCAL and is intended for certain types of local currencies that were established in the past decades in various regions. One remarkable example of this category is Freigeld, a local currency established in Wörgl, Austria in 1932. The built-in demurrage of this currency has been transferred to cryptocurrencies like Freicoin. Another currency of this category that has emerged in recent years is the Detroit Community Scrip (e.g. Kavanaugh, 2009).

When it comes to digital-only currency schemes, ECB (2012) differentiates three types:

- Closed money flow schemes with almost no link to the real economy. The virtual currency can only be earned and spent within the virtual ecosystem and traded within the community. One example is Blizzards World of Warcraft Gold.
- Schemes with unidirectional flow where the virtual currency can be purchased using real currency but can not be exchanged back. Facebook credits was one of those until it was removed from the system in 2013. Another example are the frequent flyer programmes of many airlines, these programmes have reached outstanding values, even surpassing the total amount of U.S. dollar notes and coins in circulation (Economist, 2005).

- Schemes with bidirectional flow where users can buy and sell virtual money according to the exchange rates with their currency. One example for this type are Linden Dollars, the currency that can be used for buying and selling goods and services in the virtual world Second Life. However, we exclude cryptocurrencies from this type as our proposed model and ontology have separate characteristics and classes for cryptocurrency Virtual Currency Schemes.

5.2. Transaction only Cryptocurrency

Transaction only cryptocurrencies meet the requirement of being focussed on providing monetary transactions between accounts in the economic system, whilst having a non-master Authoritative Blockchain Verification Method and Algorithm-based Validating System. These are typically the first generation cryptocurrencies such as Bitcoin, Peercoin and Ripple, built to provide the distributed or decentralised transaction validation.

Although these cryptocurrencies provide basic scripting functionality to facilitate transaction integrity, they do not provide any additional application functionality. We define Transaction only Cryptocurrency as type VCS 1.

5.3. Native Blockchain Application

Native Blockchain Applications are defined as Virtual Currency Schemes that provide additional application functionality built into the cryptocurrency or blockchain. By definition, all cryptocurrencies rely on transactions, but this type does not require an application to have monetary use-case. The blockchain has many future applications outside of the monetary context most commonly used, and we expect that many applications that leverage the blockchain will appear. Native Blockchain Application examples include: (i) NXT, with its embedded applications such as its Trustless Financial Ecosystem, decentralised marketplace, and encrypted messages; (ii) Namecoin, with its embedded private domain name service functions; (iii) Maidsafe, providing a distributed network for file storage (Massive Array of Internet Disks). We define Native Blockchain Applications as type VCS 2.

5.4. External Blockchain Application

Similarly to Native Blockchain Applications, External Blockchain Applications also provide additional application functionality to the cryptocurrency or blockchain ecosystem, but do so through an external interface to the blockchain. These applications process the blockchain natively and are programmed to interact accordingly with the blockchain. However, External Blockchain Applications are centralised in nature (they run as a service and require their own server to function) and are under the control of a third party developer.

Examples include: (i) Counterparty, which uses the Bitcoin network to provide a platform for free and open financial tools; and (ii) Gridcoin, which is the first blockchain protocol that works with Berkley Open Infrastructure for Network Computing (BOINC) hosted network, to provide almost any kind of distributed computing process such as SETI@Home (Search for Extraterrestrial Intelligence) and Poem@Home protein folding modelling.

We define External Blockchain Applications as type VCS 3.

5.5. Transaction & Application Platform

A Transaction and Application Platform is defined as a cryptocurrency and blockchain that provides an embedded Turing complete contract language that allows for full Distributed Applications (DApps) to be designed and run on the application platform. This functionality is distinct in that the Turing completeness will allow conditions and loops to be implemented, something that other cryptocurrencies do not support by design.

This capability means that the Dobby attached to each transaction can be programmatically created to provide any level of automated decision making based on any factors or given limitations. An Internet of Things vending machine can negotiate a contract with suppliers for replacement orders, with parameters including pricing, delivery schedules, loading the machine, acceptance and payment. The single example of a Transaction & Application Platform is the Ethereum Project, with its first live release called Frontier on 30 July 2015.

We define Transaction & Application Platform as type VCS 4.

5.6. Regulated Virtual Currency

Besides the possibility of some government accepting an already existing and commonly used cryptocurrency as a legal tender currency (as described in chapter 2.3.), there might also emerge cryptocurrencies specifically designed for central banks maintaining full control. One example of this category is RSCoin (Danezis & Meiklejohn, 2015), which allows for a centralised monetary policy combined with a distributed validating system for prevention of double-spending.

There are distinct advantages of cryptocurrency technology in a government sense, where transactions are taxed automatically at the time of transaction, regardless of the global location of the participants, and taxing of micro-transactions are easily supported. The government could insert various algorithms in a government controlled cryptocurrency to enable and automate many types of financial, health and social support processes. Government interest is expected to grow with comments from Moy (2015), former Director of the U.S. Mint expressing how cryptocurrencies are evolutionary.

As such, this type is a placeholder on our model, and we define Regulated Virtual Currency as Type RVC.

6. ONTOLOGY

Our ontology was built using languages of the Semantic Web. The basic idea of these technologies is to make various forms of content meaningful to computers (Berners-Lee et al., 2001). This starts with very simple and popular techniques like tagging pictures and documents with the intention of enabling the computer to understand what is depicted or written, respectively. More advanced techniques include building whole models of specific knowledge domains and have the computer generate new pieces of knowledge based on the already known by reasoning algorithms.

In our case we used the Web Ontology Language OWL in its 2nd edition (Hitzler et al., 2012) to create a model of currency schemas and their properties. We only make use of basic features of OWL2 in order to keep the ontology comprehensible and universally usable. There always is a trade-off between high-level expressiveness on one side and decidability and the availability of practical reasoning algorithms on the other.

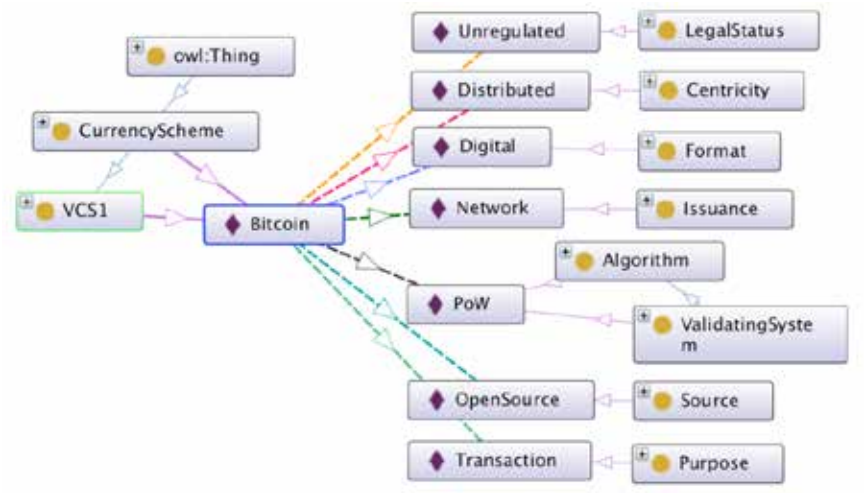
Table 1 shows an overview of the types we built into the ontology. This does not contain all the properties or all tested cryptocurrencies but should give an idea of the model created.

Table 1. Model of Currency Schemes

Legal Status	Regulated	Unregulated								Regulated
Centricity	Centralised					Decentralised/Distributed				
Format	Physical or Digital	Physical	Digital							
Control and Issuance	Government	Private				Network/Private				Government
Validating System	Bank	Private				Algorithm (PoW, PoS etc)				
Source	Closed Source					Mostly Open Source				
Purpose	Transaction Only						Transaction & Application		Transaction & Application Platform	?
Function Integration	Not Applicable						Embedded	External	Embedded	?
Type	**FIAT**	**LOCAL**	**ECB 1**	**ECB 2**	**ECB 3**	**VCS 1**	**VCS 2**	**VCS 3**	**VCS 4**	**RVC**
Definition	Fiat	Local Currency	Closed	Uni-directional	Bi-directional	Transaction only Crypto-currency	Native Blockchain Application	External Blockchain Application	Application Platform	Regulated Virtual Currency
Examples	USD/EUR E-Money	Community Coins Detroit Scrip Freigeld	Warcraft Gold	Facebook credits Frequent Flyer Miles	Linden Dollars	Bitcoin, Peercoin, Ripplecoin, Solarcoin, Zerocash, Primecoin,	NXT, Namecoin, Maidsafe	Omni, Sidechains, Counterparty, Gridcoin	"Turing Complete Platform" "Bitcoin 2.0" Ethereum, Zerocash	RScoin (concept) Future

One of the main reasons for building the ontology in OWL is the ability to create new knowledge based on the known pieces of knowledge. In this case, all we did was give the Individual “Bitcoin” its correct values for all the properties, and the Reasoner automatically categorised Bitcoin as “Transaction only Cryptocurrency” of type VCS1. This can also be seen as a special form of testing the ontology, as one can always see if a certain cryptocurrency is being categorised correctly when inputting the respective properties. 1 depicts some of the main relations of Bitcoin as an exemplary cryptocurrency in the ontology.

Figure 1: Bitcoin in the ontology



Another option is to manually classify a cryptocurrency into a specific type. The Reasoner then automatically assigns all the properties that need to be fulfilled for individuals of that class. This also makes it possible to test the ontology and see if all properties are assigned correctly.

One has to be very careful with OWL and other languages of the Semantic Web though, as they make the so called open-world assumption (OWA). The main idea of OWA is that if a statement is not known, it is not automatically seen as false like it would be seen in relational databases and most programming languages. It is simply unknown, this way there can be a distinction between false statements from missing statements (Grimm, 2010). This can have unexpected effects for those who are not familiar with OWA systems. For example, one can not define VCS1 with the following OWL triples, saying that VCS1 can not have a purpose of Application nor one of ApplicationPlatform:

Class: VCS1

EquivalentTo:

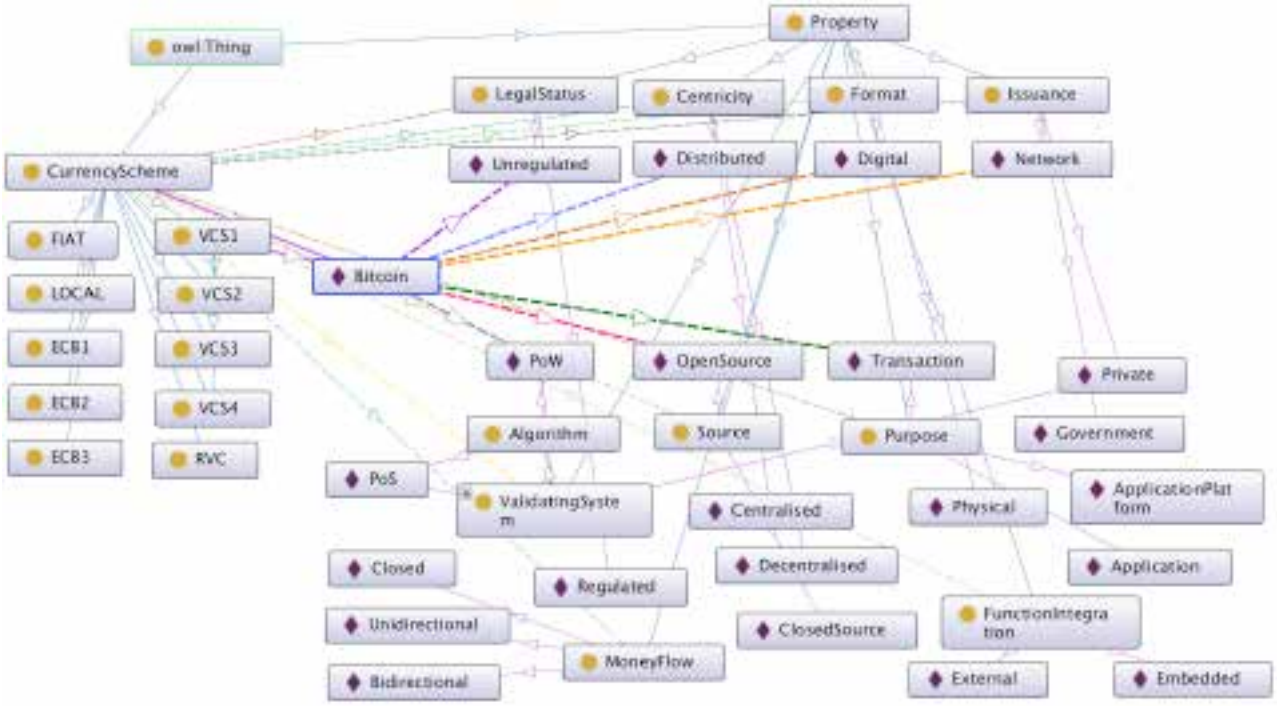
not ((hasPurpose value Application)

or (hasPurpose value ApplicationPlatform))

The reason for this not working is that there will never be an Individual fulfilling this restriction. There can always be knowledge that's not known so far including the knowledge that a specific cryptocurrency has another purpose than transactions. In OWA systems these unknown facts lead to this class being empty.

2 shows the bigger picture, again for Bitcoin as an example.

Figure 2: Ontology



7. CONCLUSION

In this paper, we have presented an ontology for categorising established currency schemes and cryptocurrencies. First we tried to find valid and unambiguous definitions for common terms that are often used not only throughout this paper but also by other parties. We then developed a catalogue of relevant properties that help to distinguish between different variations of VCS and proposed a model of 10 types that they can be fitted into. As diverging as these cryptocurrencies seem to be, they can still be aggregated in a few categories by choosing the right properties.

The approach of this paper is to contribute in clarifying the current state as well as preparing for the possible advances in future applications of cryptocurrencies. In particular, when having a look at current publications of various governments and financial institutions, very diverging points of view come to light.

We also can conclude that although cryptocurrencies are at present correctly defined as "Virtual Currency Schemes", all it would require is for a single country to accept any cryptocurrency such as Bitcoin as legal tender for that cryptocurrency to be recognised as a legitimate and lawful currency.

REFERENCES

1. Berners-Lee, T. et al. (2001) The Semantic Web. In: *Scientific American* May 2001, pp 34-43, New York.
2. Blundell-Wignall, A. (2014) The Bitcoin Question: Currency versus Trust-less Transfer Technology, *OECD Working Papers on Finance, Insurance and Private Pensions*, No. 37.
3. Brikman, Y. (2014) Bitcoin by analogy, http://brikis98.blogspot.fr/2014/04/bitcoin-by-analogy.html (accessed 31.08.2015)
4. Buterin, V. (2013) What Proof of Stake Is And Why It Matters. Bitcoin Magazine, http://bitcoinmagazine.com/6528/what-proof-of-stake-is-and-why-it-matters/ (accessed 31.08.2015)
5. coinmarketcap (2015) Crypto-Currency Market Capitalizations, http://coinmarketcap.com/currencies/views/all/ (accessed 31.08.2015)
6. Courtois, N. T. (2014) Crypto Currencies And Bitcoin, http://www.nicolascourtois.com/bitcoin/paycoin_may_2014.pdf (accessed 31.08.2015)
7. Danezis, G. & Meiklejohn, S. (2015) Centrally Banked Cryptocurrencies, arXiv:1505.06895.
8. ECB (2012) Virtual currency schemes, https://www.ecb.europa.eu/pub/pdf/other/ virtualcurrencyschemes201210en.pdf (accessed 31.08.2015)
9. ECB (2015) Virtual currency schemes – a further analysis, https://www.ecb.europa.eu/pub/pdf/ other/virtualcurrencyschemesen.pdf (accessed 31.08.2015)
10. Economist (2005) Frequent-flyer miles: In terminal decline? The Economist, 2005-01-06.
11. EU (2009) Electronic money institutions, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110 (accessed 31.08.2015)
12. FinCEN (2013) Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf (accessed 31.08.2015)
13. FinCEN (2014a) Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform, http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R011.pdf (accessed 31.08.2015)
14. FinCEN (2014b) Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System, http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R012.pdf (accessed 31.08.2015)
15. Goldman Sachs (2014) All About Bitcoin. In: *Top of Mind 21*, March 2014.
16. Grimm, S. (2010) Knowledge Representation and Ontologies. In: *Scientific Data Mining and Knowledge Discovery – Principles and Foundations,* pp. 111– 137.
17. Hitzler, P. et al. (2012) OWL 2 Web Ontology Language Primer (Second Edition), http://www.w3.org/TR/owl2-primer/ (accessed 31.08.2015)
18. Hofman, A. (2014) NXT – Proof of Stake and the New Alternative Altcoin. Bitcoin Magazine, https://bitcoinmagazine.com/9826/nxt-proof-stake-new-alternative-altcoin/ (accessed 31.08.2015)
19. Kavanaugh, K. (2009) 3 Cheers for Detroit's Local Currency, http://www.modeldmedia.com/features/detroitcheers18809.aspx (accessed 31.08.2015)
20. Kaye, M. (2014) How to Secure a Blockchain with Zero Energy, http://bitcoinmagazine.com/9317/ how-to-secure-a-blockchain-with-zero-energy/ (accessed 31.08.2015)
21. King, S., & Nadal, S. (2012) PPCoin: peer-to-peer crypto-currency with proof-of-stake.
22. Larimer, D. (2013) Transactions as proof-of-stake, http://bravenewcoin.com/assets/ Uploads/TransactionsAsProofOfStake10.pdf (accessed 31.08.2015)
23. Money, L.P. et al. (2012) Open Source Software – Quality Benefits, Evaluation Criteria and Adoption Methodologies. In Journal of Computations & Modelling 2/3, 1-16
24. Moy, E. (2015) Book Review: The Age of Cryptocurrency, http://www.newsmax.com/Finance/Ed-Moy/cryptocurrencies-bitcoin-book-money/2015/05/29/id/647430/ (accessed 31.08.2015)
25. Nakamoto, S. (2008) Bitcoin: A peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf (accessed 31.08.2015)
26. Nelson, J. W. (2011) Why Bitcoin Isn't A Security Under Federal Securities Law, http://www.lextechnologiae.com/2011/06/26/why-bitcoin-isnt-a-security-under-federal-securities-law/ (accessed 31.08.2015)
27. Peteanu, R. (2014) Fraud Detection in the World of Bitcoin. Bitcoin Magazine, http://bitcoinmagazine.com/11599/fraud-detection-world-bitcoin/ (accessed 31.08.2015)
28. Skaggs, N. T. (1998) Debt as the Basis of Currency: The Monetary Economics of Trust. American Journal of Economics and Sociology, 57(4), 453-467. doi: 10.1111/j.1536-7150.1998.tb03375.x
29. Surowiecki, J. (2012) A brief history of money, IEEE Spectrum, Volume 49, Issue 6, pp. 44 – 79. doi: 10.1109/MSPEC.2012.6203967
30. Vasin, P. (2014) BlackCoin's Proof-of-Stake Protocol v2, http://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf (accessed 31.08.2015)
31. Yellen, J. (2014) Fed will steer clear of Bitcoin, http://fortune.com/2014/02/27/janet-yellen-fed-will-steer-clear-of-bitcoin (accessed 31.08.2015)