CRYPTO-CURRENCY AND E-FINANCIALS

Stanković B. Ivica
Faculty of Business Studies and Law, Belgrade, Serbia
ivica.stankovic@fpsp.edu.rs
Mihajlović R. Aleksandar
MI-SANU, Belgrade, Serbia
Mihajlović A. Radomir
NYIT, New York, USA

Abstract: *In this paper we present a formal view of the general session, transaction, value, market and currency. Based on the presented view we examine validity of the digital crypto currency while focusing on the particular example of Bitcoin. As the most important problem associated with any currency based transaction, we discuss main security issues, indicating the US government as the major potential source of a threat to any crypto currency system.*

Keywords: *Protocol, session, transaction, crypto currency, digital currency, ecommerce, e-financials.*

1. FUNDAMENTAL REMARKS

We define a general session as a joint activity of two or more active entities having one common goal, purpose or application. A minimal session that requires only two cooperating or communicating active entities has a cardinality of two and may be considered a binary session. We shall restrict our discussions to binary data or message exchange sessions that some may call information sessions. In such sessions, each message *m* has certain semantic content meaningful to both entities involved and defined (statically specified) by what is known as a protocol. According to our definition, a protocol represents a session's static activity scripts, message format or syntax with actionable message meaning or semantics.

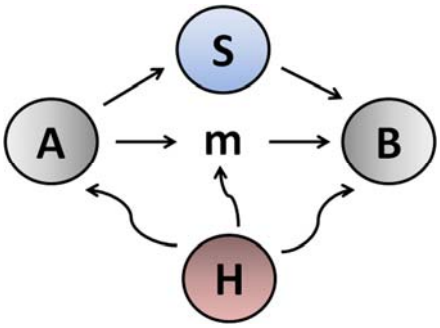

Figure 1: Secure binary session elements.

We distinguish the terms *session* and *transaction.* Each transaction is a session while the opposite does not always hold. For example every business transaction requires a session between business partners. A transaction is assumed to be one completed, i.e., closed, session with all protocol activities performed as specified by the defining script. Figure 1 illustrates a simple one way information session with two parties A and B, where A sends message *m* to B. All elements of this session maybe exposed to an attack by some intruding third party H (a hacker). A secure session is possible if all entities involved, (A, B and *m*) are protected.

In the case of Web 2.0, common protection against these attacks is based on a set of cryptographic protocols involving the third trusted party S, (See Figure 1). The implicit or explicit existence of the authoritative security or supervisory party S is found in most e-commerce system designs. The authoritative party S connects A and B via parallel security side (out of band) session. Such a security session is an overhead to each application session that is unavoidable whenever application session execution involves public communications infrastructure such as Internet. Mandatory involvement of the third security party imposes certain static and dynamic restrictions on the principle application session parties A and B. Statically, both A and B are required to preregister or be pre-configured with S. Dynamically, during the session, both A and B may be required to communicate with S, engage in the security meta-session, waste time and slow down the main application session. The static limitations are limiting the freedom of both parties A and B. Party A cannot initiate arbitrary secure or trusted peer-to-peer session with any party B unless both are previously identified and pre-configured to use S security services. A simple passing of the message *m* relevant to the application protocol is not enough. It seems to us that this fundamental problem of the lack of freedom to initiate unsupervised peer-to-peer session will be solved with the next-step Web, i.e., the true Web 3.0[1]. The session freedom that Web 3.0 promises translates into a freedom with almost endless possibilities of yet to be designed and implemented Web application protocols.

2. COMMERCE AND MARKETS

By some ad hoc definition, the term business defines all individual or collective activities relevant to acquisition or production of goods, as well as the trade of goods and/or services. The terms of acquisition and trade implicitly assume existence of trading parties, traded entities, trading transaction, and trading session.

The most elementary trading session would be a two-way (bilateral) and binary in nature involving two parties exchanging traded entities. For example, let us consider a session where party A is offering entity *x* and party B in return is offering entity *y*. Upon the evaluation and value matching of the traded entities *x* and *y*, party A delivers *x* of certain value *v* to the party B and party B responds by delivering to A element *y* of the same or approximate value *v*.

A domain of physical or logical space offering certain trade related convenience or service, a domain where trading parties may engage in trade can be considered as a market. Acting as a trade transaction context, probably the best trading services that market can offer are:

- Easy and fair value v measurement or pricing of the traded entities *x* and *y* [2],
- Trade agreement or contract enforcement upon A and B, and
- Trade secure transaction protection from the intrusion by H.

Trading on a larger market scale is commonly accepted as commerce, and trading electronically, e.g., via Internet as e-commerce. In addition, any market where logical fungible value equivalents are traded may be considered as a financial market.
Apparently, besides being physical in nature, markets also can be logical. Financial markets are sort of logical markets. Some may observe that the e-commerce market digitally implemented on the Internet dedicated, for instance, to the trade of digital or information goods is an example of the logical market too. In addition, Web based auction sites appear as markets too. In such markets trade transactions can take place entirely online and two trading parties A and B do not have to physically meet.
In modern economic theory, all goods can be:

- Tangible aka physical, and
- Intangible aka logical.

For example, an automobile is a tangible object, while downloaded video clip belongs to an intangible class of logical or digital goods that can be consumed by means of an electronic device such as computer or television set.

3. TRADING AND VALUE

To facilitate fair trading of mismatched entities, e.g., commodities, x and y, a fungible substitute value representative entity z must be introduced. For z to act as an interface entity, the minimal unit of z must be set with such a fine grain that certain number of such units, a price, can be equated to the value of z or of y. It appears that all entities z of such properties represent trade interface entities or value measures.
One legacy representative fungible entity used through the ages is gold. By definition, fungibility, is the property of a good whose individual units have an equivalence property, i.e., are capable of mutual substitution. For instance, since a given gram of gold is equivalent to any other gram of gold, gold is fungible, and as such may be used as trade element. Examples of other fungible entities are crude oil, silver, copper, soy beans, or papers of value such as shares of stocks, bonds or currency notes known as money. Apparently, fungible entities may be physical or logical. The convenience of using logical fungibles is their convenient physical handling properties, i.e., ease of storage and transportation. The most widely used logical fungible value measure is known as currency or money. As a value representative currency was traditionally and conveniently used in commerce.

4. CURRENCY

As a medium between the provider A and consumer B of some goods or services, currency enables optimal value matching. Due to the logical, understanding based value of currency, the enforcement of the value understanding must be executed by some third authoritative party. The virtual nature of currency implies that the lack of the physical currency value, (e.g., paper currency), is transparent and that currency is accepted by the trading parties as having agreed upon value. Commonly found third party in charge of the currency recognition and virtual value enforcement are governments of countries or unions such as European Union with its own currency.

Besides being a medium used to connect mismatched parties that are trading goods and services, currency may be treated itself as a form of logical good. Namely if the consumer intends to consume certain currency the producer may be compensated in another type of currency. Such a transaction is commonly known as currency exchange transaction. To most people, the term "currency" is self-explanatory. Currency or money is a generally accepted form of virtual value, or value representative that includes coins and paper notes, which are issued by a government to be used within an economy in trade sessions.

5. DIGITAL CURRENCY

The ancient Greek philosopher Aristotle (384 BC – 322 BC) analyzed and formulated the question of measuring and matching value also known as the problem of commensurability [3]. He wondered how a fair equating and exchange of mismatching and non-comparable goods could be set. Aristotle said that objects of money and currency can be used as a common value measure of all tradable goods and services, making them commensurable, i.e., capable of being matched and equated. Aristotle stated that money or currency is a substance that has a *telos,* a purpose or application, which is "value measurement". In addition, Aristotle specified the following four basic characteristics of money:

1. Durable, i.e., it must stand the test of aging and hostile environment, (It must not fade, corrode, or change through time),
2. Portable, i.e., it must small in size and light,
3. Divisible by a common unit without remainder, i.e., it should be easy to combine the same as well as smaller and larger units. This feature is an extension of the fungibility principle, (A good or service is fungible if the same unit objects cannot be distinguished one from another).
4. Intrinsically valuable, i.e., the money or currency value just by itself should be apparent to users (people) independent of any other tradable good or service.

Modern definitions of money [4] ignore the fourth Aristotelian characteristic and list three additional characteristics:

5. uniformacy,
6. limited supply, and
7. acceptability.

In response to diminishing sixth property of modern world currencies, an anonymous mathematician Nakamoto Satoshi [5] has proposed special digital crypto-currency named Bitcoins. One of the inventors of the Web, Ted Nelson [6], declares in his video presentation that behind the name Nakamoto Satoshi stands brilliant Japanese mathematician Mochizuki Shinichi, [7].
Regardless of the identity of Nakamoto Satoshi, the Bitcoin protocol has started in 2009 a real digital financial revolution, i.e., e-financials has been born.

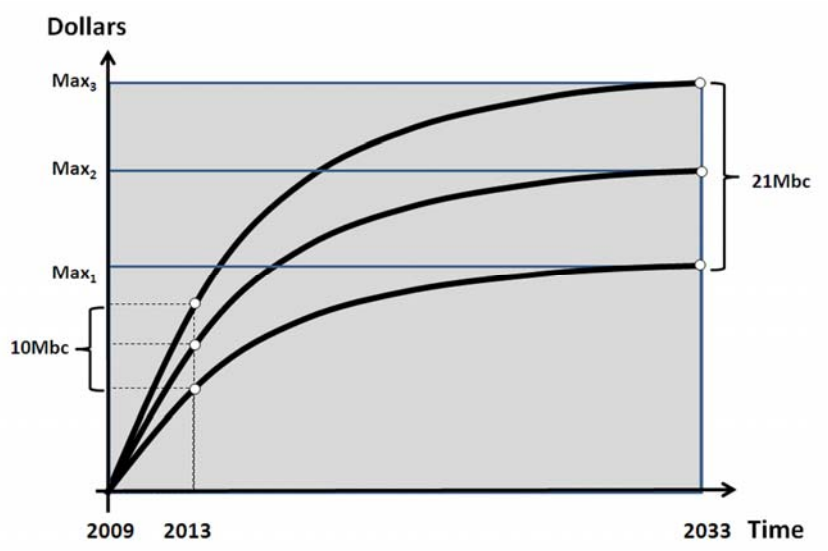

Figure 2: Floating dollar value of the total Bitcoin volume available.

The bitcoin protocol limits the total number of all possible Bitcoins. Initially every block of transactions introduced b=50 new coins in the system. With every additional 210,000 blocks the number of introduced coins would be halved, so that the total maximal value would be:

$$ax = \sum_{t=0}^{\infty} (210000 \, x \, 50) / \; 2^{t} = \frac{1}{1-\frac{1}{2}} (10{,}500{,}00) = 21{,}000{,}0$$

As Figure 2 indicates, by 2013, half of the maximal value was released, and all coins will be released, i.e., mined by 2033 [8]. Although, it looks as Bitcoin is deflationary crypto currency, the floating price (See Figure 2), of individual coins and the fine grain unit of 1 Satoshi = 1/100,000,000 Bitcoin, makes the maximal potential dollar value of all Bitcoins more than large enough to cover entire global trade. Inflationary nature of the fiat paper currency such as dollar has been complemented by the deflationary counter currency.
Bitcoin has over 100 rival currencies that are accepted by much smaller number of people, In March of 2014 there were 12,540,000 Bitcoins released with about $600.00 per coin price, representing 7.5 billion dollars in ecommerce power [9].

6. DIGITAL CURRENCY SECURITY

Security problems are important whenever any value is traded over the public infrastructure such as Internet. Our analysis indicates that periodic collapse of crypto currency exchanges such was Mt Goxex change bankruptcy are not due to any defects in the crypto currency protocol but due to the plane critical password theft and other standard systems security defects.

The problem of multiple spending of the same crypto coin was elegantly solved by the proof-of-work algorithm and the support of the massive coin mining global computer network. The coin mining network helps approve each coin based transaction and in the process release new coins into the system. The main vulnerability of the Bitcoin system is in the fact that a supercomputer of the power comparable to the coin mining network can devastate the coin system. By shutting parts of the network and by activating supercomputer system, governments such as US government can crush any crypto currency system even as large as Bitcoin. Larger crypto currency systems are harder to crush, which means that almost 10 billion dollar Bitcoin system is much stronger than any of the smaller competitor systems.

7. CONCLUSION

It seems that the unstoppable trend of wide acceptance of crypto currencies is in its full swing. After credit card revolution, and after having trading parties identified by their mobile phone number, use their SMS messages as a form of electronic digital currency, the problem of stronger anonymity in trade transactions, greater convenience and lower cost of payment processing was solved by the digital crypto currency systems.
Fiat currency regulatory bodies and the banking system are still necessary to measure the value of the digital currency, but vice versa boomerang effect is possible too.

REFERENCES

[1] Mihajlovic, R.A., Mihajlovic, A.R.: *Web 3.0, Ecommerce 2.0 and Internet Neutrality.* 4th Intl. Conf. LEMIMA 2014.
[2] Mihajlovic, R.A., Gregorek, M.J., Jafari, A., Mihajlovic, D.V.: *E-Commerce Contract Modeling and the Contract Law,* DCCA 2007, The 1st Intern. Conf. on Digital Communications and Computer Applications, 621–629.
[3] Shiner, R.A.: *Aristotle's Theory of Equity,* 27 Loy. L.A. L. Rev. 1245 (1994)
[4] Natelson, R.G.: P*aper Money APER Money and the Original Understanding of the Coinage Clause,* Harvard Journal of Law & Public Policy, Vol. 31, No.3, 1017-1081, 2008
[5] Nakamoto, S.: *Bitcoin: A Peer-to-Peer Electronic Cash System,* 2009., Available at: https://bitcoin.org/bitcoin.pdf
[6] Nelson, T.: *I Think I Know Who Satoshi Is,* Available at: https://www.youtube.com/watch?v=emDJTGTrEm0
[7] Mochizuki, S.: *CV* Available at: http://www.kurims.kyoto-u.ac.jp/~motizuki/Curriculum%20Vitae.pdf
[8] Driscoll, S.: *How Bitcoin Works Under the Hood,* Imponderable Things, July 14, 2013, Available at: http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html
[9] Website: *Bitcoin Watch,* Available at: http://bitcoinwatch.com/