



A TREATISE ON XAURUM

v. 1.00
Xaurum Team
22/06/2016

www.xaurum.org

1. INTRODUCTION

Bitcoin's invention is most commonly compared to the time of the American Gold Rush; this analogy is misleading. The analogy equates bitcoin to gold, this is problematic because it forms the view that bitcoins are something closer to gold than fiat currencies, and furthers the confusion between natural and artificial scarcity. An analogy more suitable for reflection and analysis a comparison of cryptocurrencies with early coinage, its invention in Lydia and its adoption by the Greek poleis around 600 BCE. The times of Greek adoption of coinage were an important factor of civilization, as Athens was sustained on the silver slave-mines, used mainly for coinage.

Reflection of historic functions of money used in contexts long since decayed through the ages informs us on their potential improvement and helps us avoid its regressions. The past is not completely gone, it is partially preserved, modified in present conditions, the functions of money are such remnants of history present in the world today and when we exclude historic analysis from the analysis of its present use, we make the mistake of confusing its current use for progress, and miss its regressive moments. The classical definition of money determines four functions; money is a store of value, a medium of exchange, a measure of value, and a standard of value, yet this functions of money are merely the functions of its use, that neglect an important aspect of money creation, that became an evident issue, with the private money creation of cryptocurrencies.

2. A SHORT HISTORY OF MONEY AND ITS FUNCTIONS

Value in general is an aesthetic idea, analogous to beauty, yet used for different purposes. The specific cases of use of the idea of value, moral-value and use-value, and consequently exchange-value, share this essential character. Not only is the idea of beauty, or the beauty of the artefacts in exchange always tightly interwoven with exchange-value throughout known history, it is essentially the same type of idea, one of actual harmony or empirical reciprocity. Idea of value in general is composed of abstraction from some empirical idea reflected with the criterion of identity, its ground is therefore empirical and its essence pure. We consider value as a general idea of a standard of human practice, and consequently as the determination of its potential practice, and the use-value as the idea of value applied to an object. An object has a use value, if it is potentially useful for potential human practice.

2.1 A SEMIOTIC THEORY OF VALUE

Use-value is not the basis of exchange-value, but its ground. Use-value is the mark of possession in general, yet when something is considered without cost it can't be considered a possession, even if it is undoubtedly useful. Potential use of something requires one to possess it, on the condition that its possession is less costly than it is to acquire or create the possession. This consideration is based on actual cost as perceived by the subject, and is only approximately measured by exchange-value.

Without a consideration of cost, a thing is not a possession, but a mere natural thing, that can enter exchange only through mediation of property relations. They are retrospectively considered as use-value, because they are given an exchange-value, yet differ from possession essentially and historically. Land and water are such examples, that can't and did not enter exchange until after property rather than possession started to determine exchange-value. The obverse also holds, to transform a natural thing into a possession or property, it must be given a potential use. For possession, because it is an actual empirical relationship, a cost is necessary, for property, because its mode is representation, it is not. This use can be actual or potential and should not be reduced to consumption, it is its character of potentiality, that differentiates it from its origin in labour, scarcity or cost and it is because of it, that it is not fully determined with it.

Potential use with an idea of cost makes a thing a possession, yet this is not sufficient for exchange-value. When possessions are exchanged directly, there is no exchange-value, no standard of this particular practice, that could determine this intersubjective interaction. Only with mediation can exchange-value gain its autonomy as a specific type of value, as a specialized semiotics that determines the potentiality of practice. This process of specialization is a continuum that requires increasingly complex objectification to progress. It is the semiotic character of exchange-value and its mediating force between the general semiotics of cultural values that is a necessary part of historic analysis of production, as the transformations of practice are essentially ideal and objective, regardless of their implementation in things and relations.

There is no dialectics between use-value and exchange-value as ideas, because they are the same idea, the potentiality of an object for potential practice, and no dialectics of their use as applied to each other, because there is no fully determinant relation. However, because use value as a general idea relates the idea to particularity without mediation, it is bound to

actuality of the object, for this reason exchange-value is not only another mode of use value, but its special case. With exchange-value the bonds of actuality are broken.

The idea of exchange-value is one of relationship between property and possession, grounded in the relationship between potential and actual possession. The peculiarity of this mode of value is evident, when we relate it to use-value as its ground. Use value is the potentiality of an object for potential practice, and as its particular mode, exchange value is the potentiality of a potential object for potential practice. Because it determines practice not with an object, but with a potential object, the object must be replaced with property relations, and because property relations depend on the general idea of value and its implementation in a given society, it therefore relates the particular practice to its generality.

Exchange-value includes the relative measure of cost of the object, yet even in primitive societies, this is not a better more adequate measure of cost, it is a desubjectivisation of this measure, by objectification and therefore a more durable measure. By relating between property and possession, exchange-value rises things to the domain of the concept, and mere causality to the mode of representation, this of course is not an event, but a gradual process far from completion. Exchange-value is therefore a particular mode of use-value, that as its special mode encompasses its totality as its content, this inclusion is particular and empirical and depends on the context of the exchange. This does not mean that exchange-value determines every aspect of the human practice, but rather that potentiality of human practice partially determines exchange-value, and is expressed in it. Because of its indetermination, it can determine itself, the more human practice is itself determined with exchange-value, the more exchange-value can be determined with exchange-value.

Determination of potentiality of practice with exchange-value produces a surplus when made actual, yet because it can be actualized either as additional exchange-value (profit) or additional use-value (productivity), this surplus is indeterminate. When use-value of an object is used to produce exchange-value, there is no determinate relationship, no direct adequate relationship between cost and profit, because there is no relation between the use-value of a particular thing to the exchange-value it occasions. This particular relation is determined by practical adequation of the thing to its extrinsic purpose, productivity. The relation of profit to productivity is necessary for growth of productivity and the growth of productivity for progress. In negative terms, the decrease in loss of exchange-value should be related to the decrease of loss in use-value, risk of losing money to the risk of losing productivity. This relationship is far from necessary in-itself, but necessary to some degree for a society to function, when this relationship is dissolved and the relationship between profit and productivity is lost.

Exchange-value is the idea that encompasses the space between possession and property, and had arguably first entered the world in gift economies of primitive societies. When a society receives a gift, it is confronted with the possession of something that is not its property. A gift is at the same time a thing to possess and an obligation to repay it with another - debt. Spirits of another tribe haunt the society possessing the gift, until it is repaid. To reverse Feuerbach's thesis on alienation; it is not that human essence is alienated and objectified in religion, but rather the objectified form of alienation is given a human essence - it is spiritualized. This spiritualization is coincidental, this objectification had to be represented, yet could not be represented adequately as humanity's knowledge of the world was still inadequate both in its mode and representation. Property used as a distinct idea from possession is first used as spiritualized, yet its essential character of knowledge is preserved

through history. Religion as a mode of knowledge plays the role of organizing societies as the original mode of lawfulness, based on divine reciprocity and law.

Property is actual only when possession can become non-actual, when its actuality is not merely negated, but transformed into potentiality. Yet with progress, additional risk, uncertainty or entropy is created that requires mitigation. Systemic entropy is the way systems are open to their environment, not only does entropy endanger the internal distribution of exchange value, as the element within a system, it endangers the system as a whole, and therefore the use-value of exchange value, and the use-value affected by it. The two dangers are the result of a single mechanism of increasing entropy of practice; for both exchange and production externalities multiply. When externalities can be accounted for and included in the system, they incur growth, when not, their decay.

2.2 POSSESSION, PROPERTY, DEBT, MONEY

It is only by the virtual shadowy double of possession, debt, that property, becomes actual as property, and can therefore be used as property, not mere possession. This use implies property relations and their codification as law and consequently produces antagonisms with the spiritualized codifications of 'natural' or divine law. The antagonism is a driving force of human progress, the complexification of human interaction, creation of new types of interaction and new types of practice facilitated by tool use sometimes occasion a better form. A new thing means a new use, and a new use a new type of human interaction. By using property instead of possession, human interaction can rise in complexity, that changes the world it inhabits. This mechanism of intra-societal gift exchange, we can speculate, works as a selection of societies with potential for cooperation; when a society returns the favour, it demonstrates that it understands reciprocity, and therefore shows itself as possessing the conditions for cooperation. Reciprocity can only be tested when there is a difference between possession and property, this reciprocity is the standard of value necessary for exchange value, that can't arise from barter, where things are directly exchanged, but requires the form of exchange, where the process of exchanging is given a durable form, that can either be completed or not. Risk of non-reciprocity is used to export the greater risk of non-cooperation; particular reciprocity is used to secure a more general reciprocity. The particular reciprocity became the special standard of exchange value, the general reciprocity one of value in general, that was at first spiritualized as divine. Because general concepts are more abstract they elude the imagination of men, so from dawn of civilization, the more concrete tools and concepts of exchange value are used as their allegories, and obverse because the particular order of reciprocity is incomplete, it is supplemented with the divine order.

Barter can be viewed as the solution to mitigate the risk of non-reciprocity, once the risk of non-cooperation is no longer a threat. Proto-money is therefore a semiotic tool, an object used for mediating between property and possession, that creates a specialized thing one can possess. Specialization is a specialization of use, that cannot be complete, because it includes its exterior, human practice in general and therefore both use-value and value in general. The difference between intrinsic and extrinsic money is one of degree, both for the general concept of money, in its historic development, and for the particular case. We can construct two ideal abstract types of money that do not exist, but serve as the representations of the extremes of the spectrum of intrinsic and extrinsic money. Pure intrinsic money, as pure commodity money, where its exchange value is perfectly identical to its use value, and pure extrinsic money, as pure token money, where the function of exchange value is completely

identical to its use value, meaning that its only use is its use as exchange value. When a money is pure commodity money, there is no difference between the value of something used as a commodity, the value of its cost of production, and the value of it used as a currency, and therefore no change of value in its use as money. This is practically not the case, as commodity money is affected by demurrage, a loss of material and value through use, or the cost of its use, and because it could only be made into money by the cost of its creation.

When something is created as money the immediate identity between exchange value and its cost is lost, by the addition of its own use-value and its own exchange-value – money is not a pure medium of exchange. The difference is either negative, that produces undervalued money, or positive that produces overvalued money, in regard to the commodity out of which it is made. True money is therefore no longer a mere thing that emerges from a practice of exchange, but rather a relative formalization of this practice into a system where the money serves as a transmitter. The monetary system includes money as the relationship between possession and property, and is used in a formalized context of laws and regulation. The system includes its exterior as cost and as debt, and therefore actual and potential cost, because debt carries with it the uncertainty of cost. Because the element can't represent the whole in the same way, that it represented some part of practice as proto-money, it merely expresses it and obscures the costs of money creation. The more difference between the cost and nominal value, the more obscure the cost of money. The independence of nominal value through history is the independence of property, and the independence of property depends on the complexity of laws. Because money is used as a measure of value, by obscuring its relationship with cost, the relationship of all economic interaction to cost is obscured. This practical problem, was to be solved by the market, yet in this regard, markets are inefficient, they can at best produce a Nash equilibrium, where risk is the lowest in the given context, yet cannot relate the order of representation to the order of things. The greater the obscurity of costs of production, the more obscure the relation of the system to its exterior, and therefore the lesser efficiency in the system's regulation of this relation.

Civilization emerged with domestication of plants and animals and their use for human purposes that produced a surplus of use-value. The centralized warehouses were likely to function as combination of different social functions, as storage, security, banks and temples. The obsession of early cultures with the connection of the world of men and the world of gods was perhaps not a mere fantasy, but the mark of the knowledge of two distinct orders of reciprocity, or rather the insufficiency of particular actual reciprocity. What the actual exchange lacks must be imagined, not to lessen one's suffering and pacify oneself with the injustice of the world, but to sustain the actual exchange itself. The representation of debt, seals signifying what the granary owes to a person, were likely already used for trade as true money. Symbolic tools for counting, keeping ledgers etc. predate written language, yet accounting remained isolated knowledge, part of the mysteries of the priests. Inter-societal exchange done by individual traders used commodity proto-money, obsidian and precious metal such as gold and silver, while intra-societal exchange used more durable food such as grain and barley. Grain became the medium of exchange, yet because grain has to be weighed to determine its quantity, it was not suitable as a standard of measure of exchange-value, for this function domesticated animals like oxen and cows were used (one can quickly spot, that a third of a cow is missing), so the nominal value was determined in terms of oxen, and paid in grain or metal. The functions of money were separate in proto-money and money, the standard used for unit of account, was not combined with medium of exchange and store of value, the functions are separated in practice because not all could reliably substitute

weighing with counting, the main event facilitating this substitution is the invention, adoption and development of coinage.

2.3 INVENTION OF COINAGE

The Lydian Lions, coined by the Lydian King Alyattes are arguably the first coins, they differ from proto-money such as shells, axes, metal, cattle, obsidian, wives etc. by the distinguishing mark of authority that gives them unity of a standard. While proto-money can function as money, it is not created as money, but rather becomes one through practice and is therefore limited to that particular practice. Coins are of course not the first money, that is perhaps as old as representation of counting, yet it nonetheless represents an important historic event, that sheds light on important aspects of functions of money and a milestone in the unification of the different functions of money. There is evidence to suggest Lydians were not the inventors of coinage, but are merely considered as such by most classical authors because of the proximity to the time and place of its Greek proliferation. It is this proliferation and its conditions that tells us more about money than immediate innovations of coinage.

Lydian Lions were coined as electrum, an artificial mixture similar to the natural alloy of gold and silver from the river Pactolus, and were debased with copper, providing the Lydian king with the profit of money creation - seigniorage. It is likely that Lydian king Alyattes invented coins to tax the ongoing bullion trade, by enforcing the exclusive acceptance of the bullions with his mark for official purposes therefore collecting seigniorage, or perhaps to lessen the cost of the sacrifices made to gods. His son Croesus, reformed the coinage into a bimetallic system of relatively pure gold and silver coins, that became more usable for other purposes, because of a monopoly over the mines of gold, he fixed the ratio between them in a way that extracted seigniorage by overvaluing gold, and did not have to debase the coins themselves. A monopoly over gold supply was necessary for this, along with a strong government that could guarantee the use of overvalued money, the innovation of coinage considered in this way, seems more like an innovation of the use of seigniorage as tax, not as immediate replacement of counting over weighing already done partially by other forms of money.

Seigniorage differs from normal taxation in important ways, it preserves the exchange-value of intra-societal exchange by enforcing the nominal value, and increases the exchange-value of the government, the loss is only the relative loss of individual in inter-societal exchange, mostly affecting the periphery of empires. It is also a tax much easier to collect, value doesn't have to be collected from each and every individual, only its official use must be enforced, as an added benefit, people are of course happier to pay taxes with overvalued money. While early warehouses/banks could perhaps collect seigniorage on issuing their tokens, this seigniorage had to be repaid, with coinage, debt was free. By this exclusion of determination of debt, coinage seigniorage could benefit as-if without cost, increasing the power of the whole, by sacrificing only the individuals when interacting for their own interests – this is the innovation that benefited the Greek.

2.4 ADOPTION OF COINAGE

Coinage did not represent an immediate benefit for trade, as the already existent trade tools served better for economic transactions between individuals. The distinguishing mark of true coins is the mark of authority that provides the coins with the uniform type, this is the function of measure of value that creates for it a common type and serves as a unit of account and the standard of measure. It creates a guarantee that something is money, not merely by making it recognizable and easy to authenticate and fungible, but ensures its practical use as money, by enforcing its use for official purposes. The creation of money as money, produces a formalization of money, and transforms money from a thing used as money, to a system where money is an element of economic exchange with artificial scarcity grounded on seigniorage. It is therefore more interesting for theory to look at the benefits of coinage from the perspective of this shift from money as a thing to money as a system, and focus on the official purposes and seigniorage, than their classical functions that are a question of their practical implementation.

The Greek adoption was facilitated not only by economic use, but mostly by the particularities of the Greek relationship between exchange-value and value in general. The antagonisms between divine law and economic exchange were plaguing the aristocratic Athens. After Theseus unified Attica under Athens, the nobility had the right of property, they owned the lands that could not be sold or purchased and required farmers to pay rent in feudalistic system. The common people of Athens were losing their autonomy by becoming debt-slaves - when they were incapable of paying their debt, they were enslaved by their creditor. This kind of society lacked unity of interests, and produced widespread civil unrest. Draco was appointed to deal with it severely, when he failed, Solon reformed the society, by cancelling debts, making debt-slavery illegal and including common people into politics. He transformed political participation from one based on blood, to one based on wealth, and made political functionaries at least partially responsible for their action. The divine law, on which property was founded, was slowly falling into the domain of men, not only had debt-slavery ended, a new unity of politics was born, and nobility became subjected to law.

Athenian economy prospered as a result of reforms and new interest for wealth. After being ruled by a benevolent tyrant Peisistratos, and his malevolent son Hippias, Cleisthenes reformed Athens based on *isonomia*, equality before the law, that resulted in the first democracy. Around the same time Athens coined its coins, and ushered a new era of exchange. Before this time, aristocrats had no need for coinage, as their land-ownership provided them with sufficient income from debt-slaves, and there was rivalry amongst the noble houses, the common people on the other hand, had no interest in using money with additional transaction costs, flowing into the pockets of the aristocrats. With the inclusion of all free men into politics, the public treasury became a common interest of Athenians, and their participation in politics was paid for with money; this enabled even the poor to attend and enjoy leisure time. An additional use of coinage was the representation of the value of land, that had become property governed by civil law, when the feudal relationship between land and aristocracy was broken. All would-be tyrants were exiled and their land sold. The ground of democracy of Athens was cemented by the use of silver coinage, as the mark of the new form of social contract that practically served as a redistribution of wealth on the grounds of equality. Silver coinage was both symbolic and useful, yet before it could become useful, it was necessary for intra-societal slavery to be abolished. A society where the

interests of the its people were united was required, to employ a tool that benefited them as a whole, and exploited foreigners and slaves. Coinage benefited both Athenians and other trade because of the low seigniorage on pure Athenian owls as the first successful system of coinage. Athens, of course did not have to capture much of seigniorage as difference between cost and nominal value, because the mere use of silver benefited them more, much like with gold of Croesus, it was the relatively costless monopoly of slave-mines of silver that produced the profit of coinage and benefited all free men.

2.5 THE RISE AND FALL OF EMPIRES

The Romans reused the ideas of the Greek, continued with development of law, and used the Lydian bimetalism for their coinage, the use of seigniorage for military payment, and its function for exchange-value surplus recycling was essential for the function of the empire. Soldiers were paid in money and paid taxes, to sustain the growing empire. This could only be done because of the earlier republic had established a common interest of the people as the public commonwealth, that has persisted through the imperial change. Seigniorage is of course not the driving force of history, however there is some evidence to suggest, that the collapse of Rome was partially affected by the inability of the state to efficiently capture seigniorage, when the gold and silver reserves were depleted at the end of the time of *Pax Romana*. The empire lost its benefits of controlling the dominating currency of the world, and could no longer sustain itself.

This mode of monetary system, had, in its lesser forms, survived through medieval times, local lords collected seigniorage for themselves, spent it on conquest. Renaissance's innovation in banking, the double-entry accounting, had to wait for the industrial revolution to transform production, before the beginning of capitalism that slowly replaced the feudal order.

Christianity had to abolish slavery in general and the French revolution, had to abolish feudal bonds, before another systemic change could occur. Early capitalism of Britain, increased the uses of use-value of new technology for the production of surpluses in exchange-value. It revived the commercial practice of fractional reserve banking, as goldsmiths started to issue certificates and paid interest on the storage of gold, while they traded a part of it for profit. This kind of representative money, was the start of modern fiat, as it slowly shed its connection to the thing it represented and banking become included in its creation. The scare of the French Revolution, that had employed full fiat money to sell the land of aristocrats and failed miserably as the neighbouring monarchies were counterfeiting it *en masse* causing hyperinflation strengthened the resolve of monarchies in the use of gold species standard. Circulation of gold coin slowly changed into gold bullion standard, where money represents a fixed quantity of gold and is exchangeable for it, and the gold standard, where a currency fixed its exchange ratio to the currency with bullion or species standard.

The gold standard was abandoned as it potentiated the recession of early 20th century into the Great Depression, and the fractal reserve system was slowly abandoned after governments lost their wealth to the world wars. The modern fiat system is partially

determined by this process of abandonment that provided more and more seigniorage that provides more control over debt and a greater efficiency of monetary policy, done with fractional reserve banking that includes the specific debts of economies into the process of money creation. With this change, the unified functions of money were unified with functions of public and private financial institutions. The system of money is separated from the order of particular things and takes the general thing, the economy, as its basis, money creation becomes fully monetized. This makes seigniorage intrinsic, and with this, the exchange-value becomes fully monetized. With this full monetization, the cost of liquidity is equal to the risk of loss of exchange-value, yet without an increase of regulation and distribution, this risk cannot be correlated with the risk of loss of productivity. Although today the main tool of seigniorage is the change of interest rates, it is not used well for its systemic functions and the inflationary model it uses, presents a progressive tax on the poorest – prices might be sticky, yet wages are stickier still.

The International Monetary Fund was founded after the Great Depression as an international safeguard against the dangers of crises, it had denied the proposal of Keynes, that would enforce a neutral money as international unit of account, and instead supported the U.S. extraction of seigniorage from all the world's economies, and accelerated the dominion of its monetary policy. This worked as long as the systemic functions of seigniorage were used productively, yet the Great Recession had already shown the cracks in the system. Because fiat systems are tied to the particular economies, their use includes private interests of governments, and because they are unified with the private financial institutions, the private interests of individuals. When fiat is used as a reserve currency for another country, it presents a considerable advantage for the economies of the reserve currencies, and antagonisms of interests in both. Much like Athens in the times of Theseus, we already live in a unified world, yet one plagued with intra-and-inter societal debt-bondage, one without equality before law, without a commonwealth and therefore without a common interest. Far from being an apolitical form of money, crypto-currencies enable enforcement of monetary policy without force, and therefore ground the potentiality of politics separated from violence and geography. This is the potential of crypto-currencies, the progression past the limitations and particularities of fiat currencies, necessarily tied to the partial interests of their countries.

2.6 THE POTENTIAL OF CRYPTOCURRENCIES

Current implementations of cryptocurrencies still lack much when considered for their purpose as money, their improvement regarding the classical functions is necessary, along with the progress in implementation of seigniorage for its systemic purpose. The main achievement of Bitcoin, was to produce a distributed public ledger, whose integrity can be protected with means of cryptography and economy alone, its use in finance could decrease the role of shadow-banking and systemic corruption. However, because the population of crypto falls into the intersection of ideological spaces between cypherpunk and libertarianism, the role of public ledger is seen as inessential. Since the invention of Bitcoin, most of the effort is directed at removing the public ledger as the function of public transparency of economic interaction for the benefit of anonymity. Although anonymity is a useful tool for the individual trying to resist a corrupt regime, the abolition of this corruption is the greater cause. The potential of public ledgers to abolish shadow-banking is still far

removed, as crypto-currencies themselves currently fall into this exact category, as viewed from traditional regulatory institutions, and more often than not, rightly so, as the vast majority of interaction in the space of crypto-currencies is one of fraud. Blockchains are the first implementation of a distributed public ledger produced by a synchronous decentralized consensus, it is because synchronicity can't be achieved with cryptography alone, that economic game theory has to be applied for this purpose. There is a lot of technical innovation still required to increase the use of cryptography for the functions that are in current schemes done by economics, however the function of seigniorage will always be determined by economics. The essential technical innovation of crypto is the creation of a public ledger with the ability of codification of property relations, this will without doubt create new forms of relations between property and possessions, yet will also have to preserve some of the old, such as money. Public ledger enables triple-entry accounting, that in addition to the double-entry accounting, that accounts for values as debt and credit respectively, separately accounts for the legitimate change of values. Current implementations of achieving consensus are done by employing the function of seigniorage in an inefficient manner, this means they do not represent an improvement over the implementation of fiat, but rather implement its lower form into a digital context, by this they constitute a progression of monetary technology, but not of money itself.

Money is a practical semiotic tool that determines human practice by relating exchange-value and use-value through relating property, as codified law of society, to possession through debt. It is either productive or unproductive in relating exchange-use and use-exchange, by increasing the potentiality of objects in human practice, cultivating possessions into a more adequate form for our purposes or by increasing the exchange-value of the whole. Because it is a practical semiotic tool that relates property relations to possession, it creates social antagonisms and conflicts with the immediate relation between property, law and subjectivity. These antagonisms multiply especially when the codification of property relations divides the interests of a society. These conflicts affect the sphere of values of societies, the grey spheres of morality, as un-codified values. Money can only relate property to possession through debt, and consequently requires a mitigation of the increase of entropy of this inclusion. Because this inclusion of debt is a function of money creation, that at the same time produces a surplus of exchange-value as seigniorage, the latter therefore has a systemic role in the system, one of mitigation of entropy. In fiat, where exchange-value is fully monetized, this role is crucial, as monetization means that seigniorage becomes intrinsic, and representation stops representing, thus completely abandoning its relation with costs.

Money is a system of the relating of semiotic content to its environment, the regulation of the world with the dominion of law, and its consequence the formalization of useful things to property relations and their regulation. While this process itself depends on empirical forces, on violence, it can never attain universality it requires, no common interest of man in general can be achieved and its role as a general equivalent will always function as the dominion of particular interests. As long as its existence depends on a particular force, particular interests play a determining role, and no common social contract is possible, no common ground. Cryptographically secured public ledgers remove this need for violence, and provide us with the opportunity to base the common grounds on knowledge instead of power.

Seigniorage is the essential property of money as money, a function that connects it to monetary policy and makes monetary policy internal to it, by this it relates property relations to the specific possession of money and determines its value. With cryptocurrencies, a monetary system is possible without the use of force, and consequently without an actual government, yet this lack does not make it apolitical, but rather necessitates a different form of politics for its adoption and use. The particularity of interest that fiat includes as its monetary policy is possible, and because cryptocurrencies only have a minimal economy, it breeds even more particular interests. Despite this, it has a potential for universality like no other type of money before it.

What is therefore required, is the development of monetary policy that would circumvent the reliance of money to economy and use seigniorage for its systemic function, as a mechanism that exports entropy and correlates exchange-value to use-value, using profit of money creation for its productive use. The ideal money, as we view it, is not a currency with a stable value, but one with increasing value, that at the same time distributes exchange-value and distributes the surplus of increased productivity of use-value. A stable currency only means that the value increased productivity has not been distributed and is a structural inefficiency in exchange-value distribution, required for stability of the system. The task of cryptocurrencies is not only the development of technology to provide a better use of money, but also the exploration of the space of monetary policies in these new conditions, to seek improvement in the systemic use of seigniorage. This is the main concern of Xaurum, the unification of the interests of all its users, based on an increasing commonwealth implemented as a cryptocurrency with dynamic and distributed elastic seigniorage.

3. XAURUM

Xaurum is a representative cryptocurrency based on an increasing amount of gold. It is designed as a store of value first, and uses distribution of seigniorage to achieve its goal. Regardless of the technology of its implementation, Xaurum could be summed up as an economic game with the next economic agents: the commonwealth, traders, users, money creators and the foundation. Increase of the commonwealth gold provides the basis of unity of interests of all economic agents, this is the main systemic function of seigniorage, its other functions are used to regulate the particularity of the interests of economic agents into unity. Because the commonwealth is composed of physical gold, that provides the guarantee to be exchanged for xaurum, it requires centralized control over money creation (coinage) and destruction (melting). For this task a legal entity Auresco Institute was created, that sustains itself with the rebate on gold. Certified 999.9 investment gold is bought from Good Delivery refineries and because its retail prices are relatively high, Auresco can charge its fee while still providing lower than retail prices of gold for the commonwealth. Because xaurum in exchange has a higher market value, than the value of its gold base, the difference can be used for increasing the commonwealth and incentivizing coinage (details in section 3.3 Coinage). Market value is used to mitigate counterparty risk, and commonwealth value mitigates market value risk, to ensure its function as the storage of value with the addition of surplus. Commonwealth is sustained by seigniorage, collection of fees of transactions and will seek additional forms of income through economic activity of Auresco.

3.1 FUNCTIONS OF CRYPTOGRAPHIC MONETARY SYSTEMS

(a) consensus

Consensus is a practical intersubjective agreement for a single data value. Distributed consensus is currently achieved for cryptocurrencies in two ways, by proof-of-work and proof-of-stake. Proof-of-work, requires mining, the process of finding blocks, bundles of recent transactions, and verifying them by using computation. Mining blocks, verifies transactions and is rewarded by collecting transaction fees and seigniorage of money creation. Proof-of-stake uses the tokens of cryptocurrency as miners, making them less dependent on electricity, as most of electricity of proof-of-work is not used for useful computation, but competition for seigniorage. Proof-of-stake currencies use quantity of tokens for this competition and unite the interests of users and miners by making possession of tokens sufficient for creation of new money.

- *centralization of seigniorage / division of interests*

The antagonism of proof-of-work and proof-of-stake mechanisms is one between the security of the blockchains and centralization of money creation - the security of a blockchain depends on the distribution of mining/staking, and because mining/staking is collecting all seigniorage, mining/staking is centralizing. Its systemic function is limited to creation of consensus, creating antagonism of interests between money creators (miners/stakers) and users.

- *market loss of seigniorage*

Another problem of capturing seigniorage is potentiated by the increased money velocity of cryptocurrencies, achieved by making the function of money as medium of exchange digital and therefore much more efficient. This increased velocity of money, means a loss of captured seigniorage to the market, as the demand for new cryptocurrency is indistinguishable from a general demand for more exchange-value. The result is the decrease in price that decreases the exchange-value of users and increases the exchange-value of miners in another currency, this is factor is potentiated when real costs like electricity are relevant.

- *commodity loss of seigniorage*

In proof-of-work seigniorage is captured through competition, and therefore partially lost in the form of electricity cost (negative seigniorage mechanism of difficulty), this loss is prevented in proof-of-stake, as their cost is trivial (liquidity), yet this solution has its own problems. The cost of liquidity is equal to risk of value, and because value is correlated to technical innovation it is immediately endangered by competition, these problems are perhaps good short-term initiatives for innovation, yet they reduce their functionality as money, especially as store of value. Xaurum bases all its other functions on its function as a storage of value, and uses the proof-of-stake model, its value is the combination of intrinsic value of the digital asset and extrinsic value as a representation of a physical-asset.

- *end of seigniorage as the base of artificial scarcity*

The other issue of current cryptocurrencies is their two-fold model, that demands the end point to the new money supply in order to produce artificial scarcity. This is a consequence of the halving mechanism used for artificial scarcity, where at a point in time, production of new money supply is halved. Xaurum bases its artificial scarcity differently, not on the quantity of new money supply, but on quantity of gold required for new money supply to enter circulation.

(b) *public ledger*

The blockchains combine the function of consensus with the function of public ledger, they are nonetheless distinct and could be separated in different cybernetic systems. While consensus is used to prevent double-spending by linking new transactions to the history of all transactions, the function of the public ledger is to represent all transactions and distributions in currency, or rather to publicly represent objective information in general. Because the blockchain combines both functions, it requires synchronicity of the system and the whole of the past must be included in every full node.

The true accomplishment of cryptocurrencies, despite the dominant sentiment in favour of anonymity, is the public ledger. This is the practical intersubjective epistemic field, created by consensus that enables the epistemic agents to *know that they know what they know*. Public ledgers are a practical application of the positive introspection axiom of epistemic

logic: “Knowledge of p implies knowledge of knowledge of p.” and useful for every instance of our dependence on objective information, such as property relations, law and money. The classical functions of money that are based on representation, that is unit of account, standard of value, medium of exchange, are easily achieved by public ledgers. Ledgers elevate exchange to the mode of representation, however the function of storage of value remains extrinsic to public ledgers. That is, we can know, the unit of value, the sender and receiver of value, the type of value, but not value itself. For this reason, all cryptocurrencies are representative in the same manner as fiat, or better defined as expressive as the intrinsic value of consensus determines their value, and should be considered as digital commodities first, and money second, as the expression of this value. Expression, however, is not representation and value itself is left undetermined. Because of the essential function of the public ledger, Xaurum will prioritise its functions over others in implementing its policies.

3.2 XAURUM MONETARY POLICY

The main purpose of all Xaurum monetary policy is to sustain the common interest by increasing the commonwealth. The commonwealth is stored as gold reserves that serve as the basis of Xaurum's value, the increase of the commonwealth increases the base value of all Xaurum. This means that the ratio of Xaurum to gold is increasing with coinage, and the users of Xaurum are rewarded with an increase of exchange-value, both as the determined increase of exchange-value in gold and the indetermined increase of exchange-value of its price. Xaurum's main innovation is aliquid, the dynamic distributed elastic seigniorage. Aliquid is used for systemic functions of Xaurum and is the changing ratio between the seigniorage paid to the commonwealth in gold and the seigniorage paid to the money creator in xaurum.

(a) the supply of money

Xaurum's money supply is elastic, coinage of new money supply is determined by demand. Because coinage of new money pays part of seigniorage to the money creator, the demand for Xaurum can be only a cloaked demand for more exchange-value in general, this would mean that seigniorage would not be captured and the commonwealth would not increase. To distinguish between the demand for Xaurum and demand for exchange-value in general, some additional regulation of coinage is necessary. The goal of coinage is sustainability of seigniorage for the benefit of the commonwealth.

- mining

Xaurum mining is done by mining other cryptocurrencies for value, exchanging their value for gold, and issuing Xaurum. The higher the quantity of miners mining, the higher the seigniorage given to them. More miners mean more market activity and consequently more volume, this increase of volume should be proportional to the seigniorage given to sustain the price of Xaurum. The goal of xaurum mining is to find an easy to use distributed mining process (that seems likely with storage mining), to provide a distribution of xaurum for trivial costs to the miner and non-trivial surplus in xaurum.

- minting

Minting requires a masternode, possession of 1000 Xaurum as the proof and guarantee of the common interest that the Xaurum commonwealth requires. Because minter possesses 1000 Xaurum, he has the good of the whole in mind, as he profits both from the increase of the commonwealth and from seigniorage. It is therefore in his interest to sustain the market price both to keep profiting from seigniorage and for seigniorage to profit him directly. Minting is additionally restricted by the last price of minting, as there was demand for new Xaurum at the former minting, we can consider that there is no new demand when the market prices are not higher. Minting also requires a legal entity to be established, to prevent issues

with governments. The goal of minting is to provide a distribution of xaurum for money, lowering the costs of large amounts of new coinage.

(b) availability of money

Because the immediate relation with the market would result in a unsustainable inflation decreasing seigniorage, coinage is restricted by the determinations of coinage, and artificial scarcity mechanism of increasing density, that ensures that coinage does not happen with zero or negative seigniorage to the commonwealth. Through this mechanisms, Xaurum achieves money supply inflation.

(c) cost of money

The cost of Xaurum increases as the ratio of gold to Xaurum increases. With the growth of the commonwealth, each xaurum is exchangeable for an increasing amount of gold, and to create new xaurum an increasing amount of gold is required. To accelerate this process and increase seigniorage the artificial scarcity mechanism of density is applied as the increase of cost for coinage. Through this mechanisms, Xaurum achieves price deflation.

(d) cost of transaction

Every transaction pays a small fee, this fee is excluded from the money supply, further increasing the ratio of gold to Xaurum.

3.3 XAURUM COINAGE

Xaurum Coinage produces new money supply; it is organized as a commonwealth where inflation immediately profits all users by increasing the base value of Xaurum in a greater proportion than it decreases it by money inflation.

(a) *coinage table:*

Name	Symbol	Value or formula	Unit	Example	Explanation
Gold Price	Gp	Gold price	USD/g	52.5 USD/g	The price of 1 g of 999.9 purity in USD, with Auresco rebate included.
Xaurum Ratio	Xr	Determined in previous coinage		1.8	Xaurum ratio represents the quantity of physical gold represented by 1 XAU.
Xaurum Density	Xp	Determined in Xaurum Coinage Density table		1.2	Density ensures Xaurum growth even if Xaurum market price is below base price, it increases with the number of Xaurum coined.
Transmutation limit		100 Xaurum	XAU	100 XAU	There is a maximum of 100 Xaurum per calculation.
Coinage gold	Cg	Gold used for coinage in USD/Gp	g	30 g	Mined or minted gold since last payout.
GoldMine Reward	R	Determined in reward table by Cg		0.66	Goldmine reward, determined in tables. More gold used for coinage the more rewards miners get.
Minting Reward	R	R=1		1	Minting is done by master nodes, at the maximum miner reward.
Aliquid	A	$X_m - X_b * X_p$	USD	53.33 USD	Aliquid is the difference between the market price and critical density price.
Market price	Xm	Market purchase price	USD/XAU	166.50 USD/XAU	Xaurum market price in USD, determined on the exchange with the most Xaurum daily

					volume, as the buy price.
Base price	Xb	$G_p * X_r$	USD/XAU	94.31 USD/XAU	Xaurum base price represents Xaurum value in physical gold.
Critical density price	Xbp	$X_b * X_p$	USD	113.1687477 USD	Base price with density. When Aliquid is equal or less than 0, this is the price of Xaurum Coinage.
Mining price	Xi	$X_{bp} + A * 0.5 * (2 - R)$ if $A < 0$ then $X_i = X_{bp}$	USD/XAU	148.9	This is the price required for 1 Xaurum to enter circulation via mining. When Aliquid is equal or less than zero, the price is equal to Critical density price.
Minting price	Xt	Same as Xi with $R=1$	USD/XAU	139.83	This is the price required for 1 Xaurum to enter circulation via minting. Minting is possible only when Xaurum price is higher than the last price used for minting.
Miner reward	Ir	$X_m - X_i$	USD/XAU	17.6	Discount on market price for miners (USD).
Mining profitability	Ip	$(X_m - X_i) / X_i * 100$	%	11.82	The profitability percentage of minig XAU compared to direct mining (BTC, LTC, ...)
Minter reward	Tr	$X_m - X_t$	USD/XAU	26.67	Discount on market price for minters (USD).
Minting profitability	Tp	$(X_m - X_t) / X_t * 100$	%	19.07	Minting reward in %.

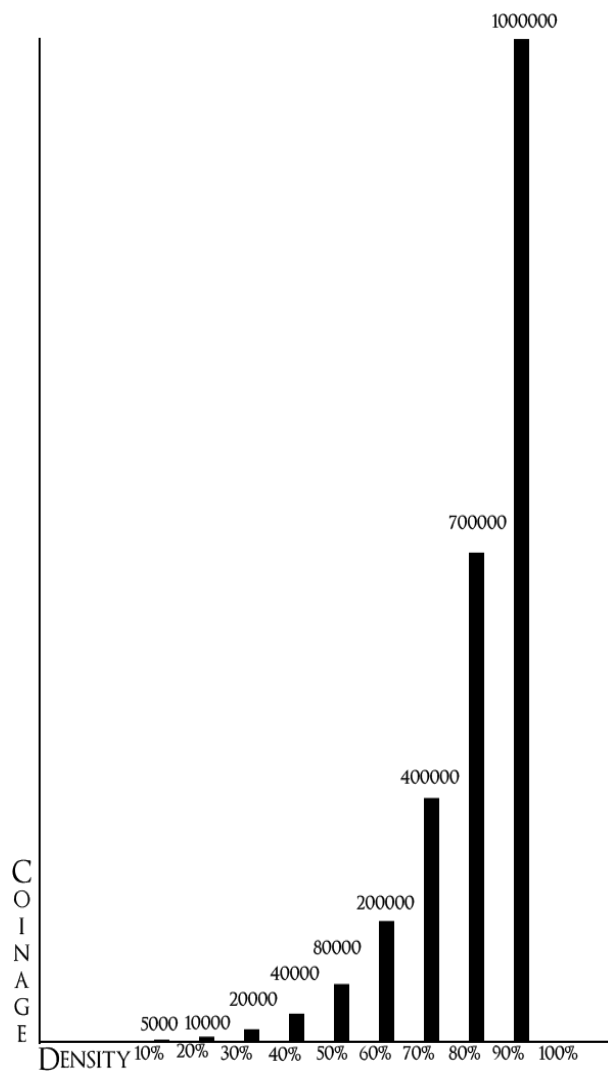
(b) density values

COINAGE (XAURUM)	DENSITY
1000	1.10
5000	1.20
5500	1.21
6000	1.22
6500	1.23
7000	1.24
7500	1.25
8000	1.26
8500	1.27
9000	1.28
9500	1.29
10000	1.30
11000	1.31
12000	1.32
13000	1.33
14000	1.34
15000	1.35
16000	1.36
17000	1.37
18000	1.38
19000	1.39
20000	1.40
22000	1.41
24000	1.42
26000	1.43
28000	1.44
30000	1.45
32000	1.46
34000	1.47
36000	1.48
38000	1.49
40000	1.50
44000	1.51
48000	1.52
52000	1.53
56000	1.54
60000	1.55
64000	1.56

68000	1.57
72000	1.58
76000	1.59
80000	1.60
92000	1.61
104000	1.62
116000	1.63
128000	1.64
140000	1.65
152000	1.66
164000	1.67
176000	1.68
188000	1.69
200000	1.70
220000	1.71
240000	1.72
260000	1.73
280000	1.74
300000	1.75
320000	1.76
340000	1.77
360000	1.78
380000	1.79
400000	1.80
430000	1.81
460000	1.82
490000	1.83
520000	1.84
550000	1.85
580000	1.86
610000	1.87
640000	1.88
670000	1.89
700000	1.90
730000	1.91
760000	1.92
790000	1.93
820000	1.94
850000	1.95
880000	1.96
910000	1.97
940000	1.98
970000	1.99
1000000	2.00

(c) density graph

XAURUM COINAGE DENSITY



(d) mining reward values

COINAGE GOLD (G)	REWARD
1	0.50
2	0.52
4	0.54
6	0.56
8	0.58
10	0.60
12	0.62
14	0.64
16	0.66
18	0.68
20	0.70
22	0.72
24	0.74
26	0.76
28	0.78
34	0.80
40	0.82
46	0.84
52	0.86
58	0.88
64	0.90
82	0.92
86	0.94
90	0.96
94	0.98
100	1.00

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA512

v. 1.00

Xaurum Team

22/06/2016

www.xaurum.org

-----BEGIN PGP SIGNATURE-----

Version: Keybase OpenPGP v2.0.53

Comment: <https://keybase.io/crypto>

wsBcBAABCgAGBQJXarHVAAoJEHJK4jg4BVP+iCciAJ6SkB07ssYcABTFh1aNwRjW
b4LROzyoBDgX2raPua3OYjwZGKYsj8AG7Mib+kVy2yw9sXS/eZovX6syS/TFauGK
ptbtRihV/8EwEqHzUQhwEgHjYGqedY+IXswG5zduOPwrJMkcpGa1A2TJBPLk55f2
O6TYlvRDF061NtsdNP4Mb3gK87qTbLdmkjLRXApXHaoBB6m2QaqEdTg07PQviiM7
aeTYM+z19ma+biPAZoHVzQcHAor++tQsdCdACwjd8RSsGVuk8riXa7coCbuTY8wT
+k75Ru9U9ECE6JeskSkVm1+1CW3BDRq+FcjBCr88lahCQVgkAhX5ENsDQxtixwE=
=aT/q

-----END PGP SIGNATURE-----