The Viridian Project: A digital currency to internalize external costs for a more sustainable economy

Markus Voge

2018-01-28 — v0

Download PDF

Introduction

Among the biggest problems of humanity in the 21st century are environmental crises such as global warming, but also social crises such as inequal distribution of wealth, with some still suffering from hunger. These problems in turn are catalysts for conflicts and migration, putting entire societies under stress. Many experts say that we are pushing the Earth's systems beyond their planetary boundaries [1,2], and that the current lifestyle of the Global North would require more than one planet to survive in the long term.[1]

Most of these problems have to do with economic activity and the underlying monetary systems [4]. One well-known problem is the privatization of profits, while costs, e.g. of environmental damages, are being socialized [5,6]. As a result, often small elites are becoming wealthier, while a majority's well-being is stagnating or even declining. Another result is the acceptance (also by the suffering majority) of environmental damage as an inevitable consequence of economic activity and progress, even when it is risking to destroy the very foundation of life and when healthier alternatives are both available and financeable by society (see [7] pages 12ff., 113ff., 117ff.). One problem of established monetary systems is the inevitability of unlimited economic growth, which is, as many have pointed out [8–11], opposed to the fact of living on a planet with limited resources. The economic growth is largely driven by the financial sector and the habit of paying interest rate and return of investment: companies acquiring money are forced to grow to reel in more than they invested and pay back their donors. For instance, this drives fossil fuel companies to ever riskier extraction practices, such as fracking, deep sea drilling, or drilling in the Arctic, with sometimes catastrophic consequences (see [7] pages 146–48, 332f., 144).

Changing the monetary system

As turned out by Belgian economist Bernard Lietaer [4], all of these problems might be addressed by monetary innovations. One interesting idea is the concept of complementary currencies: Currencies that have limited validity, e.g. only in a certain geographic area or only within certain branches of economy. These currencies are not to replace national or international currencies, but to complement them and thereby strengthen closed circles and reduce extreme aggregation of wealth. The idea of complementary currencies is already actively followed by people from several groups, e.g. the Transition Towns movement [11] that aims to build a post-fossil, sustainable, and resilient economy and by the degrowth movement [12–14] that aims to put an end to unlimited economic growth. Complementary currencies are already in use at some places and prove to strengthen regional and more sustainable value generation. In addition, there are more ideas to redesign our monetary systems, e.g. *The Chicago Plan Revisited* [15,16], a report issued by the International Monetary Fund (IMF) in 2012, suggesting that private banks should only be allowed to lend money that they have in deposits (100% reserve banking), reducing both public and private debt and resulting in a more balanced and stable economy. Another idea is to establish a complementary currency on the national level in each country,

[1] The Global Footprint Network annually calculates the date of the *Earth Overshoot Day*, on which humanity has depleted the amount of natural resources that is regenerated each year, see e.g. the 2016 annual report [3], https://www.footprintnetwork.org/our-work/earth-overshoot-day/, or https://www.overshootday.org/. In 2017, the Earth Overshoot Day fell on 2 August.

distributed to all citizens as a basic income, thereby "insulat[ing] local sustainability and resilience from the deleterious effects of globalization and financial speculation" [14].

Another monetary innovation are cryptocurrencies (the most popular being Bitcoin) based on a distributed ledger or blockchain, which do not require any kind of central institution like a bank [17]. Besides the benefit of reduced cost, a much more fascinating aspect of cryptocurrencies is that of the democratization of money. Instead of restricting the privileges of the creation of new money and the verification of money transactions to few centralized (mostly private) banks, giving them a great deal of power, this power is distributed by giving it to a large group of relatively equal players, which everyone can join. A downside is that cryptocurrencies can only exist digitally and thus require the use of electronic devices. This creates a vulnerable dependency on electricity and might increase resource consumption,[2] which is not good from a sustainability perspective. On the other hand, smartphone devices capable of digital payments are already now almost ubiquitous, even in developing parts of the world.

Cryptocurrencies are not controlled by central institutions, banks and/or governments, i.e. individual people, but by mathematic algorithms carried out by computer software, distributed on all participants' devices. This offers several opportunities: In principle, these algorithms can be formulated in any imaginable way, enabling the easy implementation of a very different monetary system. Also, if designed properly, it might be much harder to break the rules of the currency system, since computers, unlike people, are not corruptible. Especially if manipulation on a majority of devices would be necessary, then this is virtually impossible, which is also what makes Bitcoin a very secure currency.

A new ethical cryptocurrency

The idea is to combine the aim of a more sustainable economy with the benefits of cryptocurrencies. If cryptocurrencies can be designed as one sees fit, then it might be possible to solve the problems of conventional monetary systems.

As a starting point, one can try to incorporate external costs into prices of goods and services. External costs are those that are not part of the economic calculation when a price is determined, however they still arise (sometimes at a different place and/or time, harming third parties) and have to be paid by someone, usually the tax payer or residents of affected areas. Examples of external costs are health damages caused by pollution or costs of disasters that are the result of careless extraction of resources, including more frequent extreme weather events as a result of green house gas emissions. In order to ensure that external costs are taken care of as well as discourage harmful and encourage sustainable behavior, it is better to internalize external costs into the actual price.

Two-dimensional money

The problem is that a (traditional) currency system cannot directly influence the way a business owner determines prices. The currency as a whole can be valued up or down by increasing or reducing the amount of fresh money (i.e. setting the key interest rate), but that does not influence individual trades. However, cryptocurrencies basically consist of transactions between peers and may offer a possibility to interfere right there. A possible idea is to add another dimension to money.

Ever since the invention of money, it has been one-dimensional in its very nature, the single dimension being value, or rather quantity. Money is a single scale, against which almost every thing can be measured. Digital currencies might remove this restriction and could add other dimensions to quantity, for example quality. Not only the mere amount of (physical) wealth would matter, but also the change in quality of life that comes along with the aggregation of wealth.

[2] In addition to increased use of electronic devices for performing payments using cyrpto-wallet apps, an enormous energy and resource consumption can be generated when transactions are verified in a cryptocurrency's network using so-called *proof-of-work* computations. The Bitcoin protocol is based on proof-of-work and the Bitcoin network's global energy consumption is assumed to exceed that of many European countries, including Ireland [18]. There are some ideas on how to replace proof-of-work with less resource-intensive concepts, e.g. the *proof-of-stake* used by the Ethereum blockchain.

To make it more visual, one can think of the new dimension as color:[3] From green, indicating good quality, to red, indicating bad quality. For means of computation, color can be converted to a number between -1 (red) and +1 (green). Since it would be complicated to handle real 2D money (e.g. adding or subtracting money involves vector calculus, which is simple, but not convenient for many people), the color should only come into play during a transaction, on the receiver's side. When the money enters a wallet, it is automatically projected onto a single axis. This means that red money is valued down, while green money is valued up, which corresponds to a diagonal movement in the 2D money space. Figures 1 and 2 visualize the movement in 2D money space for conventional and colorized transactions.

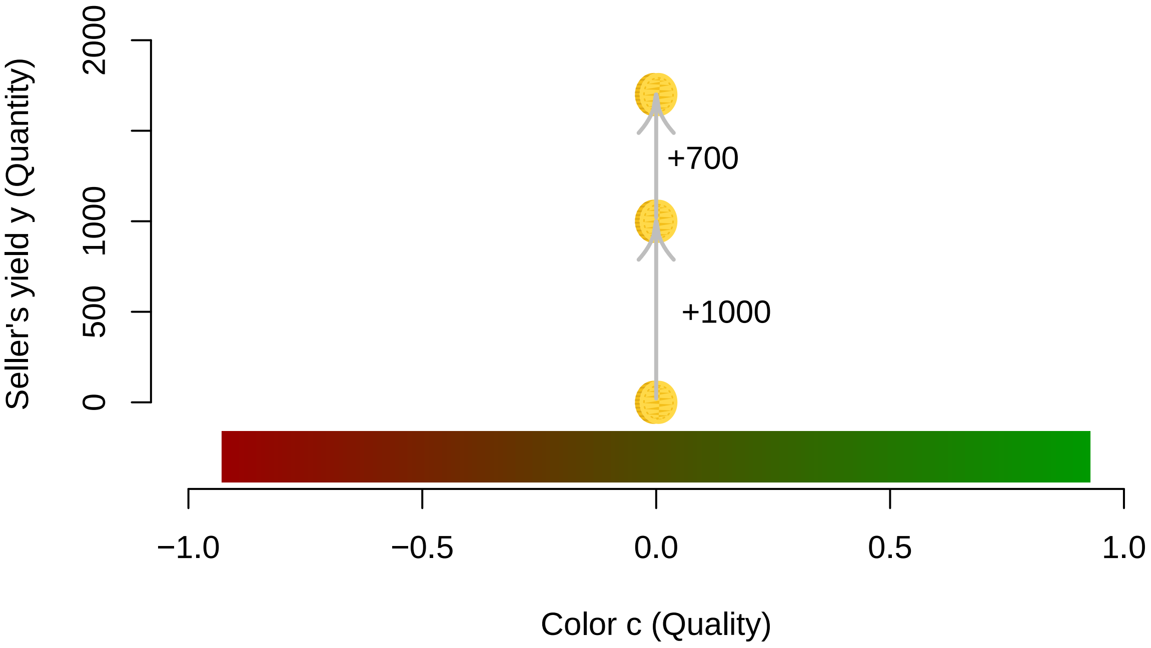

Figure 1: Figure 1: Conventional money transactions are completely one-dimensional. In this simple example, a seller earns first 1000, then 700 coins.

(Icon made by Smashicons from www.flaticon.com is licensed by CC 3.0 BY.)

It can be argued how exactly this projection should be done, e.g. in a linear or non-linear way. It is also debatable if there should be upper and lower limits to the de-/revaluation and what these limits should be. To avoid too extreme value changes, the effect of the color on the transaction should be considered when the color is determined. For now, a very simplistic choice is made: A color c of a transaction changes the value of the reserved money by factor $1 + c$, which can lie anywhere between 0 (dark red, complete devaluation, i.e. selling is prohibited) and 2 (dark green, i.e. duplication of value). This means that there is also "neutral money", which is yellow, $c = 0$, that does not change value, $1 + c = 1$. So, the price p paid by the buyer is changed into the seller's yield y via:

$$y = (1 + c)\ p$$

It is also an interesting question whether there should be more up or more down valuation, which would essentially either create or destroy money, or whether they should balance each other. This could be controlled

[3] Within the cryptocurrency community, already since 2013 there exists the term "colored coins" (see e.g. http://coloredcoins.org/, https://www.coinprism.com/), which has nothing to do with the concept described here. "Colored coins" are bitcoins carrying certain information. They can be used for example to prove ownership of a certain asset. It is called "colored" because a bitcoin is "marked" to make it distinguishable from all other bitcoins. Since the ownership is linked to a cryptocurrency coin, it can be easily transferred to another acount. This enables the realization of "smart contracts", where digital or real world assets can be sold securely using a blockchain. Colored coins are similar to Ethereum, however not using a seperate blockchain, but the bitcoin blockchain.

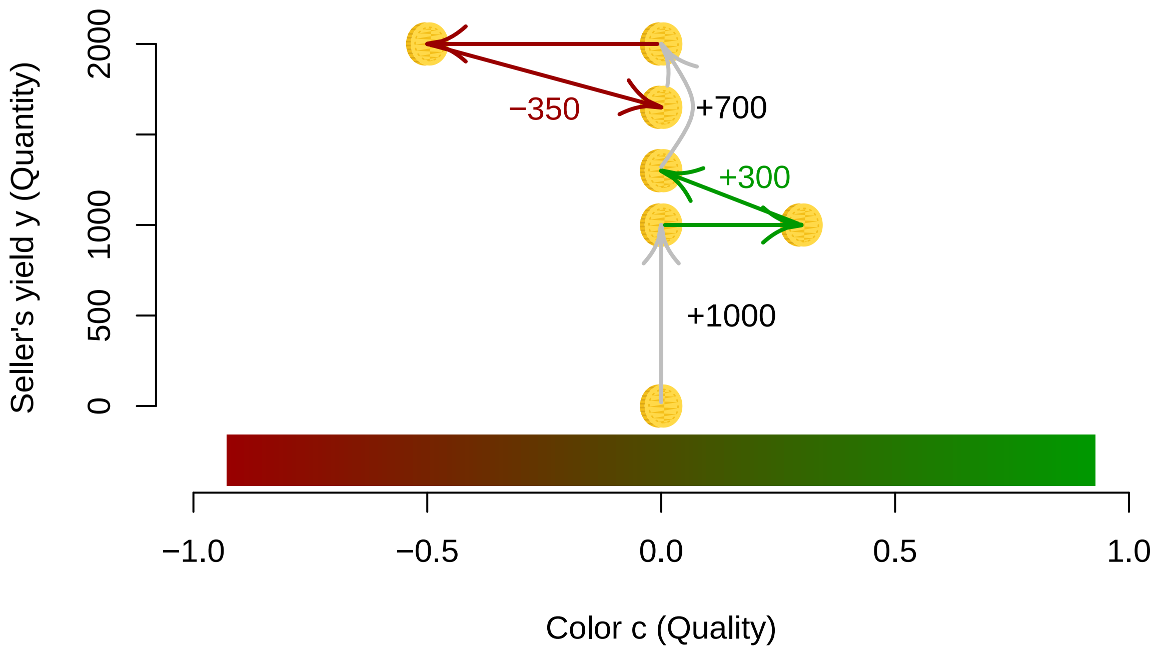

Figure 2: Figure 2: The same example as in the previous figure, but colorized. With colorized transactions, money transactions are two-dimensional: When a seller obtains money, the transaction's color shifts the value to the right or left. A diagonal projection onto the value axis (y-axis) follows, leading to an increased or decreased value.

via a regularly changing overall normalization of the re-evaluation, so that the average change in the total amount of money is constant. Currently in use mainstream currencies constantly create new money via credits, which creates a low inflation rate. Bitcoin on the other hand, the most prominent cryptocurrency, has a fixed volume of 21 million bitcoins. This limited amount of money leads to a deflationary currency. Mainstream economists argue that it is beneficial to have a low inflation rate, because it prevents people hoarding money and creates an incentive to spend the money and bring it back into circulation. This might lead to a more equal distribution of wealth. On the other hand, it might lead to unnecessary consumption of goods and thus be a driver to (excess) economic growth. Degrowth economists therefore might favor a deflationary currency. There are claims that interest rate (and therefore inflation) incentivizes short-term investments, while an interest-free currency system with demurrage (money losing some if its value over time, i.e. negative interest rate, or money "disappearing") incentivizes long-term thinking and promotes a more sustainable economy [4].

An example

As a concrete example for a transaction in the new currency, buying an emission-intensive car with a fossil fuel burning engine might involve red money, while an emission-free electric vehicle is bought with green money.

Let's assume that the seller of the red money car had to pay 9000 coins to buy the car from the producer. The car seller needs a profit margin of 1000 coins, so would sell it for 10000 coins without considering color. The color of the transaction is -0.5, meaning that the yield y will come out 50% lower than the price p. For y to be 10000 coins, p must be $p = y/(1 + c)$, so the car must be sold for 20000 coins.

On the other hand, the green car seller might have paid 15000 coins to the producer and wants to earn 1000 coins as well. The color is 0.1, translating into a price of $16000/1.1 = 14545.45$ coins, making the car cheaper for the consumer even though it was more costly to produce.

Upon entering the seller's wallet, the red money loses some of its value, while the green money is valued up. This effectively means that the fossil fuel car will be sold with a higher price (since the seller gains less), while the electric car gets cheaper. It is like a higher tax on one, while subsidizing the other. The buyer does not even need to know about the color of the transaction or the process of (de-)valuation, only the seller needs to include the color into their price calculation. This makes it easier to adopt for the consumer. This can help cleaner, emerging technologies, sometimes needed as quickly as possible from an ecological point of view, to become marketable much quicker. It can create the right incentives to make good investments and use good practices, while punishing behavior that is harmful to society.

It is important to note that, similar to value added tax, the colorization should probably not be applied multiple times, but only at the end consumer. Intermediate reevaluations must be undone accordingly.

Redistribution of value

All transactions regardless of color should include a small transaction fee that is paid to the color determiners to reward them for their services.

A part of the ("disappeared") money from red transactions may be taken and paid into a fund to alleviate side-effect damages like environmental disasters or increased health costs and can also fund dedicated projects like supporting unemployed people during (necessary) structural change. This would adhere to the principle of "the polluter pays" (see [7] pages 110–19) and would be considered fair by most people.

If one introduces demurrage (s.a.), one could also choose not to simply "destroy" the money, but to redistribute the demurrage evenly across all accounts. This would act similar to a property tax that reduces inequality.

More possibilities

If one wants to, one can incorporate more into the colors than simply social and environmental sustainability. For instance, few large corporations usually create a distorted market situation. Large corporations often have advantages due to their bargaining power and "economy of scale" effects and therefore many sectors of the economy tend towards few huge players. However, when these advantages lead to a monopoly or an oligopoly, there is no fair price determination any more (because it is no free market). Consequences can be too high prices and exploitation.

If one wants to avoid oligopolies and create a more diverse market with many small or medium sized players, then one could add a component to the color that considers the company size (or rather its "market power"). With that, the competetive advantage of large corporations could be reduced or removed so that small companies might enter the market more easily and be more competetive despite of their smaller size.

Managed by the crowd

While a similar effect to that of colored money can be reached by taxation and subsidization, the interesting aspect is that computing technology offers a possibility to do this without a central authority involved.

The main problem with the transformation of the economy towards sustainable development is to do it in a way that is fair and socially accepted by everyone. Past policies have failed to do so and have placed the burden of societal tasks like climate action and recovery from financial crises mostly on the less wealthy majority, even though they are not responsible and not profiting much from the economy that created these problems. Of course, the majority of people will not accept a change that feels like they have to give up their standard of living, while the wealthiest, the ones most responsible, e.g. those profiting from the extraction of resources, are not paying their toll (see [7] p. 118). In this situation, the fear of losing jobs due to a system change is quickly sparked in the public and surely must be addressed, e.g. by dedicated projects. But because governance fails to introduce such projects, which should be paid for by responsible polluters like the fossil fuel companies, system change never comes.

This is why such important decisions like the color of money cannot be placed into the hand of a few privileged, or a single person. It must be done collectively by the crowd, in a way that is acceptable by everyone.

This is an attemt to bypass government and any centralized institutions or elites: Like the Bitcoin miners perform the service of validating transactions and keeping the currency's network secure, dedicated decentralized groups could determine the transaction colors. Much like developers of open source software, there could be groups of people dedicated to auditing certain products or producers in terms of sustainability. Collaboratively, they determine the color in an open and transparent way. There should be an online platform (a "Github of the economy"), where the color determination takes place and is documented. Every interested individual can view how the decision on color was reached and can make suggestions, even though only few have the required experience and the time to actually make decisions.

The hard problem of finding color

Determining a fair color for virtually every product or service that can be bought seems like such a colossal task that it might well be deemed impossible. It might mean performing audits similar to what is done currently for products to obtain certain labels on sustainability or fair trade, but not for some specific products, but for everything. On the other hand, there already exist software tools and databases for performing life-cycle analyses (LCA), which could be leveraged to estimate products' environmental impact, an important part of the color determination. Also, if products consist of components, then the color can partly be a composite. If the same components are used in other products, one can re-use their color.

But still, several problems come to mind: One is the question how the transition to the new currency might be done, a classical hen-egg-problem. If the currency is not in wide use, only very few products will have an adequate color. This means only few products can be bought with the new currency in a meaningful way, which might attract few adopters, leading to very limited usage.

Another problem is that of scalability: while it is in principle possible to determine color, it is very hard to do this completely, including every aspect, and for every product. Of course, perfection is impossible to reach, but one should at least take a closer look, which takes time. A lot of manpower is required to do the audits, which might need to include travels and on-site visits. Some might argue that the work of the auditors would be so expensive that it would be hard for society to pay for it. On the other hand, it should be considered if an ethical and fair (and thus socially stable) economy is worth the price. Thinking in degrowth terms, people in post-industrial economies ought to work only half as much, both because the economy should be less "productive" and because it would free a lot of "off-market" time. This freed time could be partly used for the color determination. But still, any idea to simplify the color determination process and save (human) resources as much as possible would be very welcome.

A third problem is that of changing time: The color of a product can never be constant, but must continuously adapt and react to changes in the production. This is important: to reward producers when they improve, to create good incentives. But also to prevent fraud where producers change the production shortly after the audit. This adds to the colossal nature of the endeavour and makes it a kind of "Sisyphos' work".

A fourth problem is that one must make sure that the system is not corrupted or gamed. Of course, there will be strong motivation to come out "as green as possible", so producers will "do their best", both on legal and illegal paths. The transparency of making all color decisions public on a Github-like platform might help, but probably will not be enough. It is clear that the color determiners would be in an easily corruptible position and it might be a good idea to reward them well to make them more independent from "gifts" from the industry.

Summary of open questions

To summarize the afore-mentioned open questions:

1. *Hen-egg:* How to transition the economy to the use of the new currency? How to attract consumers? How to attract producers?
2. *Scalability:* How to determine color for “everything”? (Too much work?)
3. *Updates:* How to keep track of changes in the real world?
4. *Corruption:* How to prevent corruption and misuse?

This is not meant to be a complete list. There may be many additional issues. For instance, a whole category of open questions revolves around the democratic, decentralized organization of the network. One must find ways to efficiently make collective decisions, without introducing centralized structures and hierarchy that would involve a lot of trust and opportunity for corruption. An interesting idea might be the concept of “liquid democracy” [19–21].

There might be many technical hurdles as well, for example energy-efficient, secure, distributed validation of the blockchain(s).

Attracting a critical mass

If the general public is ever to embrace this new technology, it is immensely important to make it attractive not only to a few people hat are both tech-savvy and care about the planet.

One strategy could be to create a subculture that identifies with this new technology as part of their lifestyle. To make the connection stronger, one could make use of good design, e.g. a very smart name, a fitting logo and a “cool”-looking user interface. The subculture embracing the new technology could cause the public to talk about this new phenomenon, raising more and more interest. Eventually, the subculture may blend into the mainstream and become part of everyone’s lives.

However, more important than appealing design will be usability: ease of use on one hand (paying with the app must be as or even more intuitive than writing a text message), and a perceived gain on the other hand. If the new technology can buy you nothing you can buy with your trusted currency already, and if prices are even higher, then the average customer will not use it, no matter how “sustainable” it is. There must be some advantages to using it. For example, if a new economy would be built around it, there might be products (perhaps highly sought-after innovations) that are only sold in the new currency.

Another interesting strategy would be to create a parallel economy for the new currency that has as many closed circles as possible. This is the concept followed by most complementary currencies. Apart from the new currency enabling access to this somewhat “privileged club”, its use might also have economic advantages. If the alternative currency has more value inside these closed circles than the conventional currency of the outside world, then people will choose to use it. Especially in times of financial crises troubling conventional currencies. This is what happened in some experiments like the Wörgl experiment [22] or the Wära experiment [23], for instance.

It is obvious that it is very important to find early adopters not only among buyers, but even more so among sellers: i.e. producers and merchants (and corresponding auditors). Only if one can buy things, buyers can start using it. Naturally, small companies that already today care a lot about sustainability might be the first adopters. Conservative companies that would be forced to change their behavior will only join when they absolutely have to if they want to survive.

The CoinSence community (see http://coinsence.org/) is similar to the Viridian project and aims to establish complementary social currencies. Within the CoinSence community, there already exist more developed plans on how to attract people and businesses and how to achieve adoption. There might be opportunities to cooperate with CoinSence or to incorporate Viridian into CoinSence.

Challenging the *homo oeconomicus*

On a side note, there are more motivations for people’s actions than selfish advantage. Many surveys have shown that, when being asked openly, a vast majority of individuals agrees to support social or environmental issues (see [7] p. 118; [24]). This is because everyone wants to appear as a “moral”, “good”, and “social” person towards others. One might call this a kind of “social peer pressure”. But this social peer pressure is completely removed from economic activity. Instead, the classical view of economics includes the assumption that every human acts “selfish” in the economy (see [25], Book I, Chapter II, p. 32). This leads, in the absence of peer pressure, to the famous “tragedy of the commmons” [26]. However, communication between individuals, applying peer pressure, can solve this tragedy and it works for many commons across the world [27].

Thus, if some kind of peer pressure would be incorporated into economic transactions by means of cryptocurrency algorithms, it might also help to make economic decisions more balanced and less one-dimensional. The human brain consists of different parts, some of which are responsible for rational, others for emotional behavior. One idea behind the colorization of money is that the process of spending money stimulates the rational side of the brain, so that emotional aspects such as empathy are not considered. However, when people have the task of determining the color of a certain good—without being in the situation of buying it—aspects such as the effect on other people and on the environment will be more important and the emotional side of the brain will be stimulated as well. This might offer a counterbalance to the consumerism of today.[4] Thus, the colorization of money transactions might be seen as an application of social peer pressure (via the color determining community) to trade.

If not using the colored currency would appear immoral and misanthropic, then there might be a strong socio-psychological incentive to use it. The psychological effect might be even stronger when showing the transaction color to the customer before the transaction is carried out.

Possible implementation

From a software architecture point of view, there need to be different components to make the currency system work:

1. A distributed database to store the colors that can be queried during transactions.
2. A collaborative platform, from which the color database can be edited, perhaps similar to Github.
3. The cryptocurrency itself (a distributed ledger storing the transactions), for example as a blockchain.
4. Applications for making transactions and interact with the cryptocurrency.

The color database or “color blockchain”

The color database gives a unique ID to each product. It is updated frequently and always returns the current color when queried. It may or may not be a blockchain. A blockchain would have added benefits like tamper resistance and decentralization as well as version control and traceability. If it is a blockchain, then there would be an “account” for every product and the acount’s balance would be the current color value, which can be changed with “color transactions” by the color determiners, with added meta-data on why the color is changed. Perhaps, it makes sense to store not only the resulting color itself, but also “subcolors” for relevant aspects: social sustainability, environmental sustainability, longevity of the product, size (or “market power”) of the company, etc. Maybe the color database can incorporate user ratings as well, e.g. rating the usefulness or the quality of the product in use. It might also be an option to trace the entire supply chain of a product in the blockchain, giving customers maximal transparency about the nature and quality of the used components.

The separate color blockchain would be managed by the individuals determining colors, the “color miners”. Color mining is a task quite different from the transaction mining, which secures the transaction blockchain. Color mining involves both auditing or LCA work to gather information backing the color value, but also peer reviewing other miners’ “color transactions” before they become a legitimate part of the blockchain.

[4] Bernard Lietaer [28] refers to the duality of *yin* and *yang* from Chinese philosophy and speaks of money being almost entirely associated with *yang* attributes like aggressiveness, strength, competition (considered dominantly male) and not with *yin* attributes like care, empathy, softness (considered dominantly female). Lietaer perceives a lack of appreciation of *yin* values in modern society, caused by the dominance of *yang* money. In this sense, colorized money might add a missing *yin* component.

Each color miner registers an account on the transaction blockchain, to which rewards for their work are transferred.

The collaborative platform

It must be open to anyone. For reading the platform's content, no registration is necessary. Anyone registering on the platform is becoming a "color miner" who helps in the determination of colors. Like there can be "projects" in Github, there are workspaces for each product and service.

One has to make sure that there is only one "genuine" product workspace and that changes to the color of a product are only done by trusted members. For this purpose, one could introduce a user permission system like a "web of trust", where only high rated members have permission to create new work spaces and assign write permissions of certain workspaces to certain members. The downside is that this makes the system more complicated, increases the threshold to add new products and introduces hierarchy. Any better ideas are appreciated.

An interesting idea for the decisions on colors is the use of liquid democracy tools, which represent "a fast, decentralized, collaborative question-answering system, which works by enabling chained answer recommendation" [21]. This would allow a broader group of people to do informed votings on colors, even though only a small group of experts provides the relevant background information (e.g. from audits and visits). When a broader group decides democratically about color, it makes abuse more difficult. Another idea to prevent abuse is to establish peer review within the group of color miners. For example, one could establish that each new information or decision about color has to be approved by at least two other randomly selected independent color miners.

The CoinSence community (see http://coinsence.org/) has developed a working online platform for information exchange, collaboration and the creation and exchange of complementary (social) currencies. They plan to incorporate liquid democracy tools into their community platform (https://community.coinsence.org), so it might be viable to build the color determination platform on top of the CoinSence platform.

The cryptocurrency or "transaction blockchain"

For illustrative purposes and for a more "hands-on" feeling, I will draft a minimal implementation of the cryptocurrency in the Ethereum framework. Keep in mind, however, that the properties of the Ethereum blockchain may not be suitable for the endeavour.

Ethereum is a programming framework for smart contracts. Smart contracts are a generalization of cryptocurrencies, where a blockchain can be used for different purposes. Ethereum is completely independent of the most prominent cryptocurrency, bitcoin, and has its own blockchain and its own cryptocurrency called *ether*, which is not really used as a currency, but merely as a means of carrying out smart contracts. With smart contracts, computer code can be attached to the blockchain, which is executed by the miners when the transaction is validated. Therefore, it can be made sure that the content of a contract is carried out as intended because the code is stored, secure from manipulation and distributed, in the blockchain.

One of the simplest things that can be implemented with Ethereum is a new cryptocurrency. Ethereum features an own programming language for smart contracts (a bit similar to JavaScript): Solidity. Taking a sort of *Hello World!* example of an Ethereum smart contract [29] and changing it slightly, one arrives at a first rather trivial implementation of the new cryptocurrency:

```
contract Coin {
    address public minter;
    mapping (address => uint) public balances;
    Product public product;

    event Sent(address from, address to, uint amount);
    function Coin() public {
        minter = msg.sender;
        product = Product(msg.prod_id);
    }

    function mint(address receiver, uint amount) public {
        if (msg.sender != minter) return;
        balances[receiver] += amount;
    }

    function send(address receiver, uint amount) public {
        if (balances[msg.sender] < amount) return;
        balances[msg.sender] -= amount;
        c = product.getColor();
        balances[receiver] += colorize(amount, c);
        Sent(msg.sender, receiver, amount);
    }

    function colorize(uint amount, double c) public {
        return uint(amount * (1. + c));
    }
}

contract Product {
    address public id;

    function Product(address prod_id) public {
        id = prod_id;
    }

    function getColor() public {
        ... // query color DB
    }
}
```

The application of the product's color is capsuled in the function `colorize()`. This is the place where the used algorithm, here simply $y = (1 + c)\, p$, would be adjusted.

The key function is the still unimplemented function `getColor()` in the `Product` contract. The color of the transaction is an information that must be fetched from the outside non-digital world. In smart contract jargon, a provider of such "external information" is called an *oracle*, e.g. see http://www.oraclize.it/. It is such an oracle that needs to be built in form of the collaborative platform where the colors are determined, stored in the distributed color database, which would be queried by the function `getColor()` to fetch the currently valid color value of the product.

Blockchain validation or "mining"

With the blockchain being a *distributed* ledger, there is no central authority to decide about the validity of transactions. This leads to the famous "double-spend" problem of cryptocurrencies. How to prevent an attacker from spending an amount of money multiple times? When a bank supervises transactions, it is in charge of the only central ledger and can allow the first transaction (emptying the bank account), but will cancel the second transaction (because the account is already empty). With a distributed ledger, there is one copy of the ledger on each node participating in the distributed network. In principle, one could send the first transaction to one node and then, before the first node has had a chance to spread the information, send a second transaction to another node. The second node will not know that the account was already emptied in the first transaction. Therefore, there must be a process of consolidation between all nodes.

Proof-of-work

The ultimate question is: Who is to decide about what set of transactions is accepted (and added to the blockchain)? Because we don't want to trust a central authority, this power has to be spread across the network. Usually, it passes from node to node for each new block, where a block is a small part of the blockchain comprising a certain number of transactions. There are different algorithms to decide about the next node whose turn it is to validate a block of transactions. In Bitcoin [17] and some other cryptocurrencies, this algorithm is called *proof-of-work*. It involves computing a number ("work"), which must have a certain property, by random trial and error. The more computing power one has, the sooner one will (on average) find a suitable number by chance. The fraction of transactions one can validate is proprtional to the owned fraction of computing power of the total network. The result of this is that, given many participants, it is extremely resource-intensive and therefore expensive to gain control over the network. One would need to contribute more than 50% of the entire computing power to take over the network and make it accept fraudulent transactions.[5] In the end, The elegance of this is that Bitcoin stays honest and secure without the need to trust anyone.

One downside is that it is not only extremely resource-intensive to take over the network, it is also extremely resource-intensive to run it in the first place. Because the block validating nodes are rewarded with new bitcoins, they are also called "miners" (they mine for digital gold). The proof-of-work system incentivizes the installation of a lot of computing power because the more computing power one owns, the more often one will validate a block and obtain the reward. The result is an energy consumption as high as an entire country's [18], not for computing anything valuable, but only for winning the right to validate transactions. Another downside is that the system increases inequality: the rich can afford to install a lot of computing power, by which they get even richer because they obtain a large share of the reward. Because of that, there is even a dangerous tendency towards mining monopolies or oligopolies, where big mining farms buy smaller competitors until only few (or one) very large players are left.

Proof-of-stake

A variation of the proof-of-work algorithm is called *proof-of-stake* [30], in which the expensive computation is omitted. The creator of the next block is selected randomly, however favoring nodes that have higher "stakes", i.e. own more of the cryptocurrency. Also, the "age" of the coins can be considered, not just the amount of coins. The idea behind this is that nodes that hold higher stakes (for a longer time) have contributed longer and are thus more trustworthy than recently joined nodes. Another advantage of proof-of-stake is that the owners of the currency are the ones that have the right to secure it. In proof-of-work, the miners might sell their entire rewards for another currency and thus have little incentive to use the complementary currency and invest in its ecosystem.

A disadvantage is that, similar to proof-of-work, rich participants are preferred so that again inequality tends to increase. Most cryptocurrencies that use proof-of-stake, e.g. BlackCoin [31] and Peercoin [32], use mechanisms to prevent too much domination from single rich members, however. The Ethereum blockchain also uses proof-of-stake.

Proof-of-whatever?

It is important to come up with a well-designed validation algorithm that minimizes energy consumption as much as possible (for sustainability), that prevents inequality, oligopolies and centralization, and that is reasonably secure (i.e. not too much prone to fraud).

[5] To understand this, one needs to know that the nodes can disagree on the blockchain validation. If a dishonest node validates a block of transactions containing a fraud (e.g. a double-spend), then the other honest nodes will not accept that block and will create an alternate version of the blockchain where the fraudulent transaction is removed. The blockchain splits into two versions. This is called a *fork*. The nodes will choose the blockchain version that is longer, because it means more nodes have trust in this version. The dishonest attacker needs to add more blocks to the chain than all the honest nodes together, therefore more than 50% of the computing power is needed.

More ideas for improved alternatives to proof-of-work and proof-of-stake exist already. A promising approach may be the *proof-of-cooperation* [33,34] of FairCoin, a cryptocurrency developed by the FairCoop cooperative. Both proof-of-work and proof-of-stake rely on competition between miners. Proof-of-cooperation, however, relies on the assumption that cooperation is more efficient than competition. It works roughly like this: Block creation is evenly shared between nodes. Every node decides independently about the node whose last block creation lies furthest back in the past (by looking at the blockchain history). The node sends a message with its decision over the network. When an assigned node has received enough messages from the other nodes approving it, it goes ahead and creates the new block. This mehcanism could still lead to centralization when a single entity participates with a very large number of nodes. This is currently prevented in FairCoin by validating each node (by talking to them and perhaps even visit them in real life) before it goes online. This validation, as well as decisions about blockchain management, are performed by a single central organization, the FairCoop assembly and administrators appointed by the assembly, which means that it is not truly decentralized and might have a vulnerable point that may be corruptible by very powerful entities. I also suspect that the FairCoin infrastructure does not scale well. FairCoin has a goal of operating 40–50 validated nodes, with a hardcoded maximum of 100 nodes, mostly running on low-power Raspberry Pis. This can hardly be suitable for running the entire world economy. But still, it's a very interesting concept that may be a good starting point.

There are also other ideas, even beyond the blockchain. For example, there are cryptocurrencies that use *directed acyclic graphs* (DAGs), a sort of generalization of the blockchain. The most prominent are currently IOTA [35,36] (https://iota.org/) and Hashgraph [37] (https://hashgraph.com/), however, the latter is patented, which poses a problem for accessibility and wide-spread adoption. IOTA comes from the IOT community as a zero-cost micro-payments cryptocurrency. It claims to be much more scalable than a Bitcoin-like blockchain, with transaction validation becoming faster with the number of transactions, not slower like in Bitcoin. IOTA also claims to be, like FairCoin, cooperative instead of competetive [38].

Interfaces to the "transaction blockchain"

Of course, aside of the blockchain backend, there must be frontend applications ("wallets") for interacting with the blockchain, i.e. for making transactions and paying things. There should also be very easy to use mobile applications available for all smartphone operating systems, in addition to platform-independent computer software.

In addition to conventional crypto-wallet features, there can be features enhancing the information and awareness of the users. The color of the transaction can be made visible, along with information on different components (social, ecological, etc.) of the color decision and maybe even supporting information leading to the decision and the history of the color value.

Conclusion

Leveraging the wisdom of crowds and the power of cryptocurrencies, perhaps one can reach a societal consensus towards a world that is more worth living in for everyone, preserving life for future generations, while not giving up modern lifestyles.

These are the requirements that must be fulfilled by the alternative currency:

1. It must feature a significantly more sustainable and/or fair economy.
2. It must be based on societal consensus to be accepted by (almost) everyone.
3. It must be very easy to use.
4. It must be fun to use and/or provide a real advantage.
5. It must be relatively hard to break the rules or abuse the system.

I assume that (1) would be a consequence of all the other points fulfilled, if the currency would be designed similar to what is described above. (2) is the main problem remaining to be solved: how to determine the external costs of goods in a socially acceptable way? The idea to use crowdsourcing was only vaguely described here. More thoughts on this would be greatly appreciated. (5) would only be partly fulfilled by the use of cryptocurrencies, how to secure the crowdsourcing against abuse is another problem to be solved. (3) and (4) have only been merely scratched at the surface.

Therefore, we are still at the very beginning, but I hope that something good will evolve out of this.

References

[1] J. Rockström, W. Steffen, K. Noone, others, A safe operating space for humanity, Nature. 461 (2009) 472–475. doi:10.1038/461472a.

[2] A.D. Barnosky, E.A. Hadly, J. Bascompte, others, Approaching a state shift in earth's biosphere, Nature. 486 (2012) 52–58. doi:10.1038/nature11018.

[3] M. Wackernagel, others, Global footprint network 2016 annual report, Global Footprint Network, 426 17th Street, Suite 700, Oakland, CA 94612 USA, 2017. http://www.footprintnetwork.org/content/uploads/2017/07/GFN_AR_2016_final_lo.pdf (accessed December 11, 2017).

[4] B.A. Lietaer, Money and sustainability - the missing link : A report from the club of rome - EU chapter to finance watch and the world business academy, Triarchy Press, 2012.

[5] Wikipedia, Externality — Wikipedia, the free encyclopedia, (2017). http://en.wikipedia.org/w/index.php?title=Externality&oldid=814231022 (accessed December 11, 2017).

[6] Wikipedia, Lemon socialism — Wikipedia, the free encyclopedia, (2017). http://en.wikipedia.org/w/index.php?title=Lemon/%20socialism&oldid=807343486 (accessed December 11, 2017).

[7] N. Klein, This changes everything - capitalism vs. the climate, Simon; Schuster, New York, 2014.

[8] D.H. Meadows, D.L. Meadows, J. Randers, W.W. Behrens, The limits to growth - a report for the club of rome's project on the predicament of mankind, Universe Books, New York, 1974. http://www.donellameadows.org/wp-content/userfiles/Limits-to-Growth-digital-scan-version.pdf.

[9] N. Georgescu-Roegen, The entropy law and the economic process, Harvard University Press, Cambridge, Massachusetts, 1971.

[10] F. Schneider, G. Kallis, J. Martinez-Alier, Crisis or opportunity? Economic degrowth for social equity and ecological sustainability. introduction to this special issue, Journal of Cleaner Production. 18 (2010) 511–518. doi:10.1016/j.jclepro.2010.01.014.

[11] R. Hopkins, The transition handbook - from oil dependency to local resilience, Uit Cambridge Limited, Cambridge, 2014.

[12] R. Douthwaite, Degrowth and the supply of money in an energy-scarce world, Ecological Economics. 84 (2012) 187–193. doi:https://doi.org/10.1016/j.ecolecon.2011.03.020.

[13] K. Dittmer, Local currencies for purposive degrowth? A quality check of some proposals for changing money-as-usual, Journal of Cleaner Production. 54 (2013) 3–13. doi:https://doi.org/10.1016/j.jclepro.2013.03.044.

[14] A. Hornborg, How to turn an ocean liner: A proposal for voluntary degrowth by redesigning money for sustainability, justice, and resilience, Journal of Political Ecology. 24 (2017) 623–632. http://jpe.library.arizona.edu/volume_24/Hornborg.pdf.

[15] Wikipedia, The Chicago Plan Revisited — Wikipedia, the free encyclopedia, (2017). http://en.wikipedia.org/w/index.php?title=The/%20Chicago/%20Plan/%20Revisited&oldid=812725885 (accessed December 13, 2017).

[16] J. Benes, M. Kumhof, The chicago plan revisited, International Monetary Fund, 2012. https://www.imf.

org/external/pubs/ft/wp/2012/wp12202.pdf.

[17] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, (2008). https://bitcoin.org/bitcoin.pdf (accessed December 27, 2017).

[18] A. Hern, Bitcoin mining consumes more electricity a year than ireland, The Guardian. (2017). https://www.theguardian.com/technology/2017/nov/27/bitcoin-mining-consumes-electricity-ireland.

[19] B. Ford, Delegative democracy, (2002). http://www.brynosaurus.com/deleg/deleg.pdf (accessed January 20, 2018).

[20] B. Ford, Delegative democracy revisited, (2014). https://bford.github.io/2014/11/16/deleg.html (accessed January 20, 2018).

[21] M.B. -P2P Foundation, Liquid democracy, (2014). https://wiki.p2pfoundation.net/Liquid_Democracy (accessed January 20, 2018).

[22] Wikipedia, Wörgl — Wikipedia, the free encyclopedia, (2017). http://en.wikipedia.org/w/index.php?title=W/%C3/%B6rgl&oldid=809155259 (accessed December 28, 2017).

[23] Wikipedia, Wära — Wikipedia, the free encyclopedia, (2017). http://en.wikipedia.org/w/index.php?title=W/%C3/%A4ra&oldid=788928723 (accessed December 28, 2017).

[24] Special Eurobarometer, Attitudes of european citizens towards the environment, European Commission, 2008. http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_295_en.pdf.

[25] A. Smith, An inquiry into the nature and causes of the wealth of nations, Edited by Sálvio M. Soares, MetaLibri, 2007, v.1.0s, 1776. http://metalibri.wikidot.com/title:an-inquiry-into-the-nature-and-causes-of-the-wealth-of.

[26] Wikipedia, Tragedy of the commons — Wikipedia, the free encyclopedia, (2017). http://en.wikipedia.org/w/index.php?title=Tragedy/%20of/%20the/%20commons&oldid=816926249 (accessed December 28, 2017).

[27] E. Ostrom, Prize lecture: Beyond markets and states: Polycentric governance of complex economic systems, (2009). http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/2009/ostrom-lecture.html.

[28] B. Lietaer, A monetary blind spot?, (2010). http://www.lietaer.com/2010/07/our-monetary-blind-spot (accessed January 23, 2018).

[29] Ethereum, Introduction to smart contracts, (2017). https://solidity.readthedocs.io/en/develop/introduction-to-smart-contracts.html (accessed December 11, 2017).

[30] Wikipedia, Proof-of-stake — Wikipedia, the free encyclopedia, (2018). http://en.wikipedia.org/w/index.php?title=Proof-of-stake&oldid=821368111 (accessed January 20, 2018).

[31] P. Vasin, BlackCoin's proof-of-stake protocol v2, (n.d.). http://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf (accessed January 20, 2018).

[32] S. King, S. Nadal, PPCoin: Peer-to-peer crypto-currency with proof-of-stake, (2012). https://peercoin.net/assets/paper/peercoin-paper.pdf (accessed January 20, 2018).

[33] T. König, E. Duran, FairCoin v2 white paper draft, (2016). https://chain.fair-coin.org/download/FairCoin2-white-paper-V1.1.pdf (accessed January 20, 2018).

[34] T. König, On proof-of-cooperation, (2017). https://github.com/faircoin/faircoin/blob/master/doc/on-proof-of-cooperation.md (accessed January 20, 2018).

[35] Wikipedia, IOTA (technology) — Wikipedia, the free encyclopedia, (2018). http://en.wikipedia.org/w/index.php?title=IOTA/%20(technology)&oldid=821140579 (accessed January 20, 2018).

[36] S. Popov, The tangle, (2017). https://iota.org/IOTA_Whitepaper.pdf (accessed January 20, 2018).

[37] L. Baird, The swirlds hashgraph consenus algorithm: Fair, fast, byzantine fault tolerance, (2016).

http://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf (accessed January 20, 2018).

[38] R. Semko, IOTA: Why free transactions matter most, (2017). https://medium.com/deviota/iota-why-free-transactions-matter-most-f90fd6f4383c (accessed January 20, 2018).