Cryptocurrency

```
Research Plan
Author = Jasper Haasdijk
         s4449754
Topic  = Cryptocurrency
Academic year::2017-2018
```

Topic

The topic of my research is cryptocurrency. In this paper, I will try to specify and answer the question "What makes a good cryptocurrency?". Using this answer, I will create a first draft for a standard specification, with which I will then create my own altcoin (Investopedia 2017). During this process I will document each and every step, in the hope that this will provide one of the first of the many steps needed to lower the barrier for creating a formal specification.

Problem

Cryptocurrency. Digital money powered by encryption (Forbes 2011). A topic which has been gaining interest for quite a while now (Trends 2017a), and the hype is far from over. Apparently even Russian president Vladimir Putin has taken an interest in the subject (Cryptocoinsnews 2017). This means that this topic attracts, and will keep attracting an increasing amount of people who don't know what it is, or how it works (Trends 2017b). This is not very surprising since, at the time of writing, there are a total of 1175 different coins out there on the market (Coinmarketcap 2017a). Some proving to be more successful, *Bitcoin* (Coinmarketcap 2017b), than others, *Megacoin* (Coinmarketcap 2017c). With this growing interest, the need for a standardized formal product specification becomes more and more apparent. If we want to see cryptocurrency succeed in the long term, it is of vital importance that we lower the entry barrier for novice users. But how do we go about creating such a formal specification? In this paper, using the following questions as an outline, I will propose a first draft. These questions are:

- What distinguishes currency A from currency B?
- What do all these fancy charts actually mean?
- What makes it that some have a higher chance of success than others?
- How does the design process look like and what are some of the big design choices that need to be made?
- What does it bring us to create our own?
- Why are we not satisfied with what is already available?

Background

Looking at the research that is already out there, we notice that it is primarily focused on the specific implementations, like bitcoin (Barber et al. 2012) (Eyal and Sirer 2014) (Mitsuru Iwamura et al., n.d.) and zerocoin (Ian Miers et al., n.d.). In this paper however, just like with (Delmolino et al. 2016), I will try to refrain from diving in specific implementations and instead give a more top-level overview. This is more suitable since we are not trying to determine the value of a single currency, but instead are interested in a formal specification for cryptocurrencies in general.

Indisputably, cryptocurrency is a new trend in the financial sector. One that is not likely to go away any time soon. Accompanying this trend is a lot of fluctuation in the perceived value of the individual coins. People are introduced to these coins on a price basis, which leads to them investing because of a fear of missing out. Often times they are not even interested in the underlying technology or see any benefit in the possibilities of the blockchain technology (d'Anconia 2017). This makes it very risky for people who are new to the scene to invest their hard earned money. While there is no detectable population-level consensus on which currency is the "best" (ElBahrawy 2017), there is a huge gap in perceived value between the high - and somewhat lower ranked currencies. How then do we determine this value? While there exists a draft for a cryptocurrency security standard (Cryptoconsortium 2017), there is no current formal product specification. By constructing such a specification, I hope to provide a factual ground point for people to make an informed decision. This, I hope, will improve the overall health and stability of the community.

Method

The research will be split up in different strategies. The first section will consist of a literature review. Here I will try to answer the aforementioned questions (See Problem). During this literature review I will form a specification with which I will then create my own currency. This latter part will consists of the typical design and creation methodology. Obviously this will most likely not be a hard split. Most likely I will end up in an iterative cycle where I interleave *literature review* with *design and creation*. Afterwards I will reflect on this process and its end product using the finished specification draft, both as a way to give an example on how this specification could be used in the real world and as a way to review my currency. This last step will also point out possible missing properties which I can then reflect on.

Planning

Please take a look at the following Gantt chart for my estimated time schedule. Please note that as I've mentioned earlier, I will most likely end up in an iterative cycle. Therefore the scheduled time in my chart is to be considered more as a general flow than precise deadlines.

Some side notes with regards to the chart

- Gathering papers; Here I will scour the internet looking for relevant material on the subject.
- Reading papers; Here I will read the gathered papers.
- Reviewing papers; While reading I will also categorize them on subject and add a small summary so that at a later point in time I can easily remember what the paper was about.
- Refine sub questions; While reading and reviewing the papers I will most likely notice some things about my current questions. They are too vague, they need further specification, they are not in the scope of this paper, or something entirely different. That's why I have given myself this time frame where I can still adjust my questions without delaying the overall work too much.

- Answer sub questions; This one is quite self explanatory. I will try to answer the sub question as best I can.
- Form specification; This is quite an important one, which explains why I have given myself some time to work on this. This is where I start working on the draft of the standardized formal product specification.
- Research; Before writing my first line of code, it is important to find out what goes into creating your own altcoin. Here I will look into the design process of creating one. This research process will not stop until I have a finished product. You will always keep on reading, keep on learning and keep on adjusting your implementation until the deadline. There is always something that can be improved.
- Design; As the title says, here I design an implementation. I will sketch out the choices I make and substantiate my claims.
- Create; Here I start working on the actual implementation. You'll notice that time frames come together here, this is due to the fact that I suspect the variation of actually starting to work on some code will be a welcome change. Also I find that actually implementing something is the quickest way to find the shortcomings in your design.
- Peer Review; After finishing my implementation, I will post it on an open source forum for other people to review. This will (hopefully) provide me with some pointers which I might have missed and some suggested improvements which I can then still work on to improve my implementation.
- Analyse and Update; Here I analyse my product so far and conclude my research. I will finish up any loose end and provide an answer to the originally asked research question.

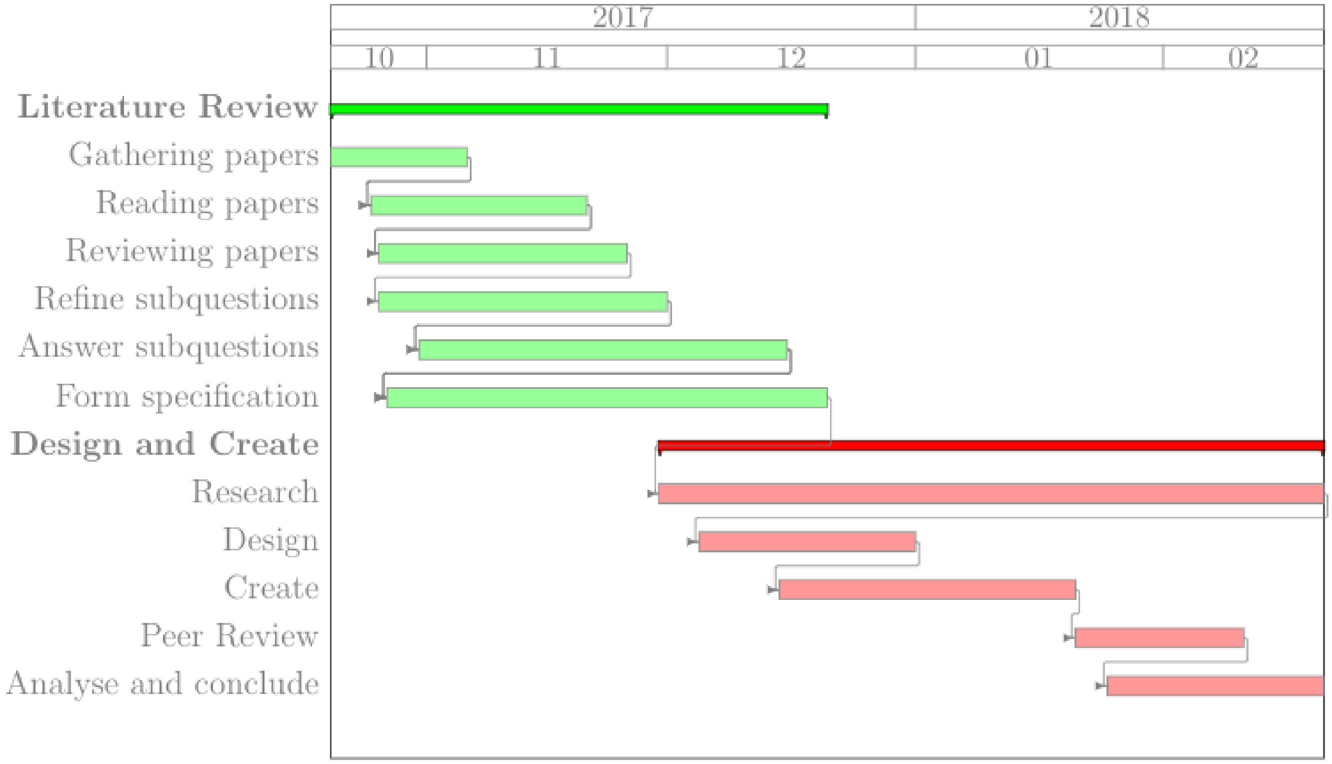

Figure 1: Gantt-Chart

References

Barber, Simon, Xavier Boyen, Elaine Shi, and Ersin Uzun. 2012. “Bitter to Better — How to Make Bitcoin a Better Currency.” In *Financial Cryptography and Data Security: 16th International Conference, Fc 2012, Kralendijk, Bonaire, Februray 27-March 2, 2012, Revised Selected Papers*, edited by Angelos D. Keromytis, 399–414. Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-642-32946-3_29.

Coinmarketcap. 2017a. “Altcoin Market.” Coinmarketcap. https://coinmarketcap.com/all/views/all/.

———. 2017b. “Altcoin Market.” Coinmarketcap. https://coinmarketcap.com/currencies/bitcoin/.

———. 2017c. “Altcoin Market.” Coinmarketcap. https://coinmarketcap.com/currencies/megacoin/.

Cryptocoinsnews. 2017. “The Cryptoruble.” cryptocoinsnews. https://www.cryptocoinsnews.com/putins-orders-russia-will-national-cryptocurrency-cryptoruble/.

Cryptoconsortium. 2017. “Cryptography Security Standard.” Cryptoconsortium. https://cryptoconsortium.github.io/CCSS/.

d’Anconia, Frisco. 2017. “Bitcoin Bubble.” Cointelegraph. https://cointelegraph.com/news/bitcoin-price-growth-is-speculation-bubble-will-burst-macleod.

Delmolino, Kevin, Mitchell Arnett, Ahmed Kosba, Andrew Miller, and Elaine Shi. 2016. “Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab.” In *Financial Cryptography and Data Security: FC 2016 International Workshops, Bitcoin, Voting, and Wahc, Christ Church, Barbados, February 26, 2016, Revised Selected Papers*, edited by Jeremy Clark, Sarah Meiklejohn, Peter Y.A. Ryan, Dan Wallach, Michael Brenner, and Kurt Rohloff, 79–94. Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-662-53357-4_6.

ElBahrawy, Alessandretti, A. 2017. “Bitcoin Ecology: Quantifying and Modelling the Long-Term Dynamics of the Cryptocurrency Market.” University of London. http://openaccess.city.ac.uk/17657/1/1705.05334v2.pdf.

Eyal, Ittay, and Emin Gün Sirer. 2014. “Majority Is Not Enough: Bitcoin Mining Is Vulnerable.” In *Financial Cryptography and Data Security: 18th International Conference, Fc 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers*, edited by Nicolas Christin and Reihaneh Safavi-Naini, 436–54. Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-662-45472-5_28.

Forbes. 2011. “Cryptocurrency.” Wikipedia. https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html.

Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin. n.d. “Zerocoin: Anonymous Distributed E-Cash from Bitcoin.” In.

Investopedia. 2017. “Altcoin Explained.” Investopedia. http://www.investopedia.com/terms/a/altcoin.asp.

Mitsuru Iwamura, Yukinobu Kitamura, Tsutomu Matsumoto, and Kenji Saito. n.d. “Can We Stabilize the Price of a Cryptocurrency?: Understanding the Design of Bitcoin and Its Potential to Compete with Central Bank Money.” In.

Trends. 2017a. “Cryptocurrency Trends.” Google. https://trends.google.com/trends/explore?q=bitcoin,ethereum.

———. 2017b. “What Is Bitcoin?” Google. https://trends.google.com/trends/explore?q=how%20to%20buy%20stocks,how%20to%20buy%20bitcoin,what%20is%20bitcoin.