Series: The Ideal Digital Currency (1)

Monetary Policies and Digital Currencies – What Happens when the Dog Catches up to the Car?

Digital currencies that are not tied to any Federal reserve or a governmental authority that control their supply are now part of the economic calculus and have continued to gain a small but increasing share in their use as a transaction medium. As they grow as a share of the economy questions are now being asked about their supply mechanisms, and subsequently monetary control. Let's take a look at the supply side schemes of several digital currencies.

Constant Supply as a Transaction Processing Reward that Decreases in Time until its Zero

In this method, new digital currencies are created as a reward to nodes that processes transactions in blocks. This is the method used by bitcoins, the first and currently most prevalent digital currency. In the scheme, blocks are set to be created roughly every ten minutes, the reward starts off at the outset at 50 BTC and then becomes halved approximately every 210,000 blocks or every four years until exactly 21million BTCs are in circulation. After this point, no new coins are created.

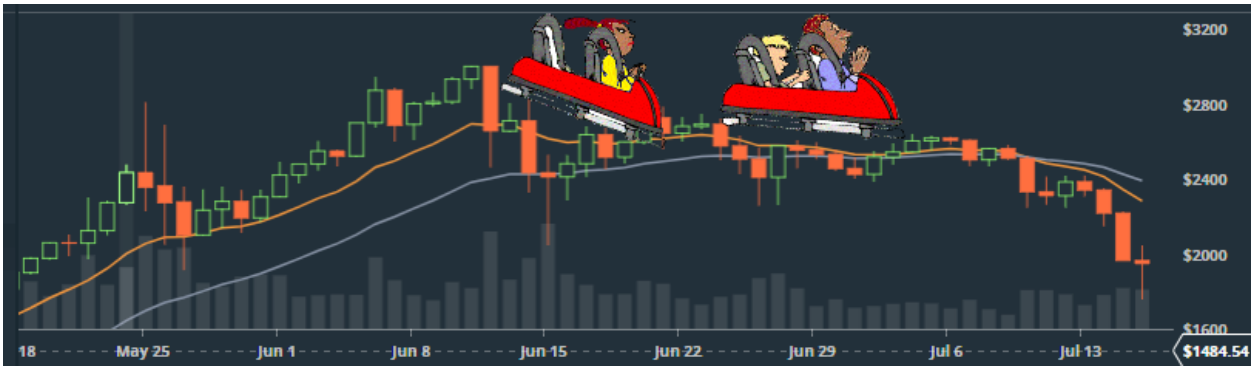
This might initially seem like a very smart idea to combat inflation, especially to inflation-weary inhabitants of excessive fiat currency domains. But let's go on some simple thought experiment.

1. Consider the point where no more BTCs are created, and we really do have 21 million BTCs in circulation. What happens when coins are lost due to lost wallet keys (turns out there is no recourse to recovering the contents of a wallet in that event by the way), demise of the owner without revealing the keys, wallets with little balance that get abandoned, and so on. Slowly, the number of BTCs in circulation would begin to dwindle until there's zero left!

   Note that the deleterious effects of inadequate supply does not need to wait till zero supply before it is being felt. The Economist noted the high deflation inherent in bitcoins and the monetary impacts of that deflation. In an earlier article, I posited that the unusually high increasing net valuation could be accounting for why the currency is not fulfilling one of its touted use cases, and growing as a payment medium. No one would want to spend their currency only to find out in short time that they could have bought twice what they bought for it today. It encourages savings – or we can call it hoarding – and that can ultimately be a problem given a long enough time as the currency would not be serving one of its major use cases. The article showed that historically, bitcoins had been doubling their purchasing power approximately every 231 days.

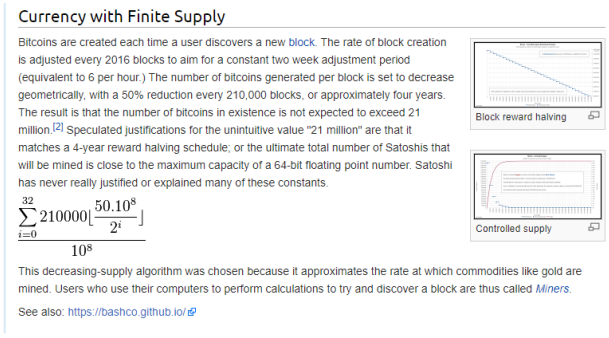
2. Transaction processing nodes are recipients of the only method of supply; even when they barely process any transactions. In fact several times in the past, blocks were mined with no transactions save the coin creation transaction for the miner or processor. Much of the first 100,000 bitcoin blocks were of this type. There has to be something fundamentally inequitable about such an arrangement, and it also ensures that a good portion of the target circulation gets locked in few hands and end up not in circulation after all, with similar effects as in (1).

3. If there is a sudden large demand for the currency, or a sudden dump of the currency due to a current event, there is no mechanism for the currency to adjust so that its holders do not experience sudden halving of their assets for instance, or worse? This has happened several times already within the nine years of their existence, but has not been as big an issue because none of the digital currencies have been dominant in any economy where they serve. Therefore, affected parties have been few, and have had fall back options. What if the digital currency has grown so large that it is the majority denomination in an economy? Such swings can virtually precipitate a run on the currency, or lead to bubbles and recessions faster than if the assets had better supply control methods.



Supply Mechanism for Some of the Existing and Proposed Digital Currencies

Most of the existing and upcoming digital currencies have proposed a reducing to eventually zero supply strategy.


Currency with Finite Supply

Bitcoins are created each time a user discovers a new block. The rate of block creation is adjusted every 2016 blocks to aim for a constant two week adjustment period (equivalent to 6 per hour.) The number of bitcoins generated per block is set to decrease geometrically, with a 50% reduction every 210,000 blocks, or approximately four years. The result is that the number of bitcoins in existence is not expected to exceed 21 million.[2] Speculated justifications for the unintuitive value "21 million" are that it matches a 4-year reward halving schedule; or the ultimate total number of Satoshis that will be mined is close to the maximum capacity of a 64-bit floating point number. Satoshi has never really justified or explained many of these constants.

$$\frac{\sum_{i=0}^{32} 210000\lfloor\frac{50.10^8}{2^i}\rfloor}{10^8}$$

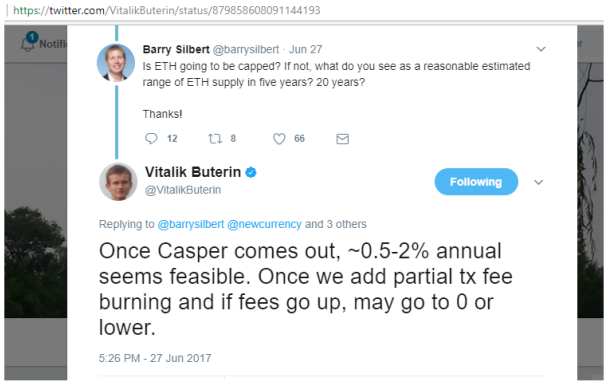
Block reward halving

Controlled supply

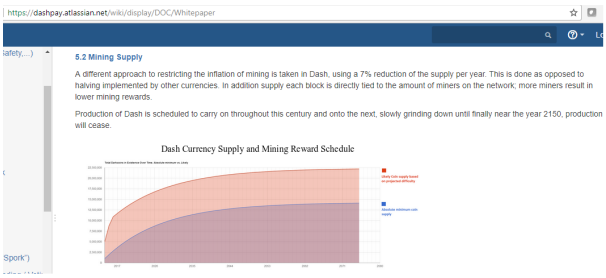
This decreasing-supply algorithm was chosen because it approximates the rate at which commodities like gold are mined. Users who use their computers to perform calculations to try and discover a block are thus called *Miners*.

See also: https://bashco.github.io/

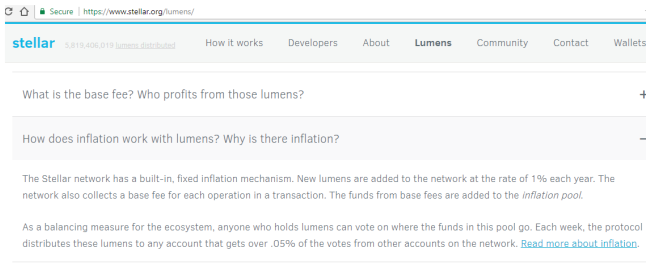
Bitcoin Supply



Ethereum Supply



DASH Supply



Lumens Supply

The fact that they all seem to have followed some version of the simplistic but obviously flawed capped supply is surprising and maybe demonstrates a bit of group-think in the industry. Or much of the designs were based on a short term mindset. It could be that the seeming success of bitcoins in creating value for holders of the currency became the model much of the other implementations aspired to. Eight years is short for a currency, where many fiat currencies have been in existence for over a century. Like the dog that catches up to the car, digital currencies might run into problems where they do not perform in a stable manner due to their lack of monetary stabilizing mechanism. In fact, they probably already are running into such problems.

The Economist described one of such scenarios well: “That other (fiat) currencies remain the medium of account has so far been the Bitcoin economy’s saving grace. If Bitcoin matured into a complete currency, with large numbers of workers using it as their medium of account, then its inflexibility could bring economic havoc. Money-supply “shocks”, like the disappearance of Mt Gox, could set off a systemic collapse. Given a loss of faith in exchanges, users might withdraw their coins in a panic, leading to a dangerous decline in transaction volume.”

Methods of Introducing Healthy Supply Mechanisms into the System

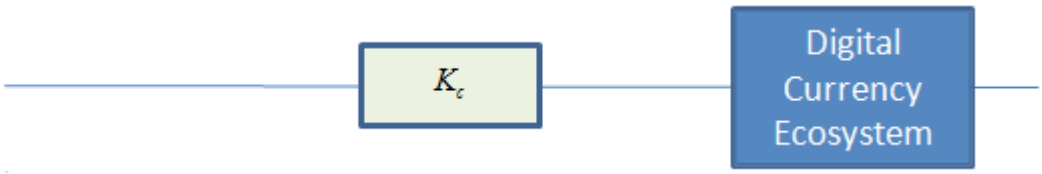
This article is not advocating non transparent, or arbitrary supply methods similar to what currently exists for some fiat currencies. But there could still be transparent, predictable formula introduced to the supply strategy such that the currencies do not eventually begin to dwindle to nothing, and that they maintain some less volatile and more determinate growth profile. The best scenario would be if they were fitted with some control mechanism containing a feedback loop similar to what is used in engineering; and in fact many other fields. At a minimum, the supply could be set to simply roughly match the coin destruction rate when the target number in circulation is reached.

Let's consider several supply methods where the supply is ultimately never set to zero to ensure that the amount of digital currency in circulation does not begin to dwindle slowly.

(Note that in the methods presented below, in place of the circulation, the measured signal could be selected to be the price, or number of unique users using a model [2] to connect those to the supply; with loss in generality of the control procedure. Also, readers not keen on mathematical description can simply read the the first sentence in each of the list below and skip to the rest of the article.)

1. **Supply set to a constant value to match an expected destruction rate**

Instead of the eventual supply to become zero, monitoring of the coin in circulation could allow a supply value to be set to roughly match the destruction rate. This would ensure that the total circulation would not begin to dwindle to nothing. The control model for this method is simple and is shown below:



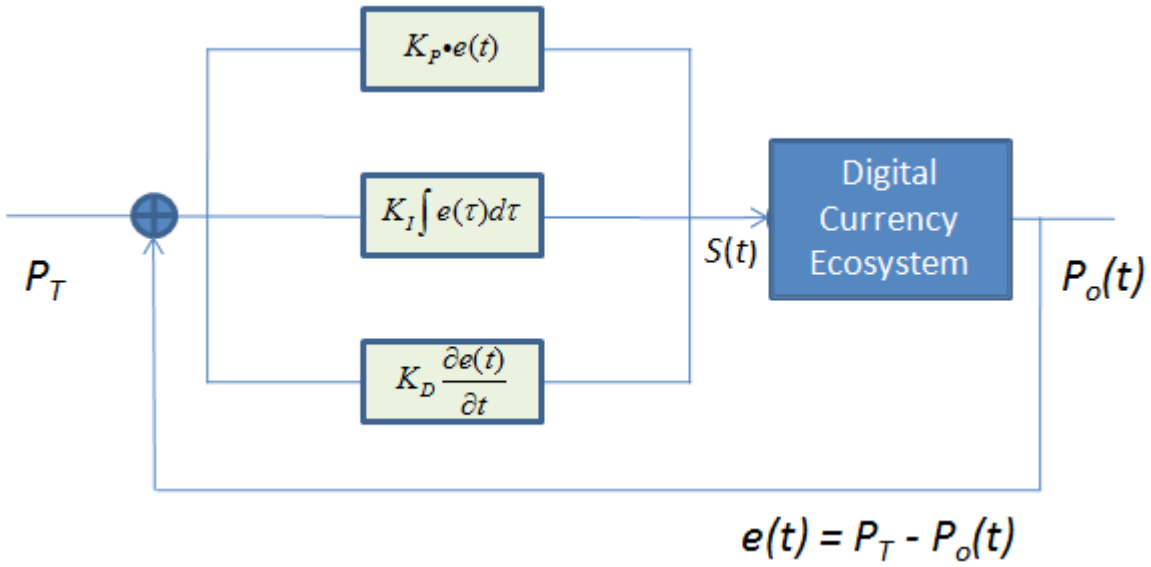
The value of K_c would be set to a miner reward value determined to keep the total amount of currency units in circulation roughly constant.

Apart from possibly exerting some monetary control, this has an advantage over the current formulation of many digital currencies in that transaction processing can continue to be supported by rewards rather than fees ensuring that the levy on individual user transactions remain low – a touted advantage of many of the currency's use cases. This is important because it is doubtful that current fees at the rate at which the hashing difficulty continues to rise would continue to be sustainable for processors without the reward.

For bitcoins for instance, the asymptotic processing reward per block could be set constant at 3.125 BTC. This modification would be a bit easier to implement than the next few ones below.

2. **Supply dynamically set via a closed loop feedback control mechanism**

In this method, a closed feedback loop is created where the gap between the measured supply and a target is brought under control by computing the appropriate supply based on that gap, its rate of change, and its accumulation in time. This control method would fully control the rate of supply $S(t)$ so that the actual output $P_O(t)$ consistently trends towards a target level, P_T, using a proportional integral derivative (PID) controller. The control model for this method is simple and is shown below.

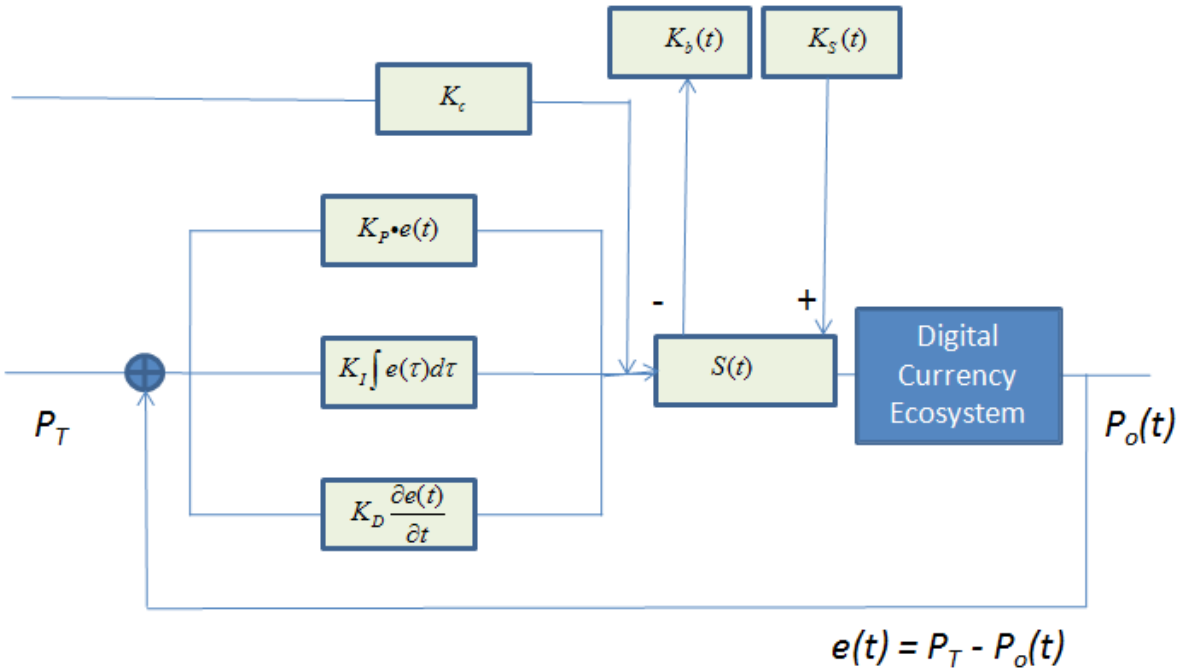


The PID controller works based on the measured gap, $e(t)$, between the actual output and the target output. The proportional portion adds an input supply with amount scaled relative to that gap or the different between the observed and target values. Its proportional constant, K_p, determines how quickly the correction is applied. A value of $K_p = 1$ simply means if the observed output falls below the target by a number e, then e additional units are added in the next cycle. The integral portion is present to incorporate the history of the gap into the control mechanism. The derivative portion is set to incorporate the rate at which the gap is changing, that is increasing or decreasing, into the supply response. Then the supply S(t) is applied based on the following equation:

$$S(t) = K_P e(t) + K_I \int e(t)\,dt + K_D \frac{\partial}{\partial t} e(t)$$

3. Supply dynamically set via a closed loop feedback in combination with other sources and sinks

The strategy here would include a PID controller same as in (2), and persistent constant transaction processing rewards, K_c to ensure transaction fees remain low and capped. However, the control system would also include the model for adding supply when the net feedback, $S(t)$ is positive, or reduce it when the net feedback is negative; which can presumably occur due to negative, transient events.



While the only supply mechanism for bitcoins is miner rewards, it can be noted from the earlier examples that some of the later digital currency implementation allowed some of the newly created assets to be introduced via other means. This includes such dissemination procedures as master node rewards as in the case of DASH, decentralized selection and funding of the currency improvement project, and freezing of asset rewards as in the case of DASH and BOSCOIN, and air dropping or dissemination of free coins to catalyze network effects as in the case of Stellar. These dissemination procedures would be considered sources to a potential control process and are functions of time. The sources are represented by $K_s(t)$ in the above figure.

Under certain extreme conditions, the model includes allowance to reduce circulation or dampen temporary value fears in the ecosystem by actually retrieving or buying back currencies in circulation. This is referred to as a sink, or negative source, and is represented in the figure by $K_b(t)$. Since much of the digital currency implementation are expected to be slightly deflationary, it is expected that the use of this tool would be rare since simply reducing or temporarily halting supply would eventually bring the output back to expected level. There is no application of any digital currency that we know of that contains procedures for rapid reduction of supply by applying a negative source, but it could conceivably be implemented by master node buy back or certain triggers (which increases the master node's stake) or flash increases to staking or freezing rewards.

Introducing some More Intuitive and Innovative Sources

For digital currencies that have miner rewards as the only method of supply, any control system implemented to modulate its supply would inevitably end up providing the rewards of all the economic activity in the ecosystem to the miners. We would have partially traded one system where a none

transparent body printed all the money and kept all the proceeds for another where a transparent group printed all the money and kept all the proceeds. Recognizing that being a source is essentially a creation process, it would seem more natural to have processes that actually create within the ecosystem be processes that are recipients of source privileges. Some of these are listed below.

Purchasing of source or new digital currencies would be similar to the initial coin offering that many digital currencies now use to disseminate genesis currencies, except that they could be auctioned off slightly below market rate, with a predetermined margin that is set in a transparent manner.

- **Agricultural produce and commodity production**
  Producers of agricultural products typically create new economic units. For instance, a farmer that creates 5 tonnes of wheat worth 500 units of currencies from an input of say 100 units of agricultural equipment and other expenses, has created 400 units of currencies in the ecosystem that never hitherto existed in the system. Initial purchase of such items into the system could apply for source units at the preferred rates. The contracts for such new coins may further be written such that they can only be used initially for their requested purposes

- **Physical mining of resources**
  This is similar to above and could be designated source events, depending on the focus of the digital currency.

- **Loans, Grants, and Subsidies**
  These are also source processes. In the case of loans, this becomes obvious when it is considered that the total interest payments as set up for loans typically exceed the principals. Depending on the constitution of the specific ecosystem, the privilege to purchase source currency units may be further determined by the type of loans; for instance agricultural loans, development loans, small business loans could be designated as potential sources.

- **Verifiable Charitable Donations**
  Charitable donations to specific causes could also be designated as potential sources depending on the constitution of the digital currency. The selection and verification procedure will of course need to be done in a transparent and verifiable way in keeping with the original drive behind the public ledger system. There have been blockchain initiatives in the past that have been lauded by members of the community for their charitable activities. There doesn't seem to have been much of a direct effort to directly precipitate it in the blockchains developed; and this could be one way to do that.

- **Interests on Frozen or Staked Assets**
  Any member of the system can also choose to freeze some of their currencies similar to how physical cash can be put into a fixed term deposits. This is referred to as staking in digital currency parlance. Several digital currency networks such as Dash, Pivx, and Boscoin already contain this provision and newly created currency created are apportioned to be split among staked holdings. The positive effect of savings on the overall supply is beneficial to the system and therefore rewarded in this manner.

- **Environmental Conservation Processes**
  This might not seem as obvious as the others. However, environmental issues are actually a sink to most ecosystems – indirectly by destruction of economic units, and sometimes directly by causing the loss of units of currencies. Prevention or mitigation of sink events adds to the ecosystem and such activities could be allowed access to supply at source rates, depending of course on the drive and constitution behind the digital currency. Considering the amount of electricity consumed by some of the blockchains, which might need to be separately addressed, this could be an important item to consider to potentially spur innovation and improvement.

From that last point, it can be noted that transaction processing is also creation process in the sense of taking resources, in this case electricity, and processing transactions for the ecosystem. It can also be noted that this system, well designed, would maintain transparency desired from a public ledger system, not be subject to politics or lobbying, and still accomplish some of the intended uses and behavior of money in an advanced and multi-faceted economic system.

Conclusions

It was pointed out that capping the amount of a currency that is created is a flawed monetary supply strategy since all currencies are subject to some destruction by various means. Some of the ways digital currencies become effectively destroyed includes loss of wallet keys, demise of owner, and abandonment of wallets with little balances. More broadly, the lack of a practical supply-side strategy for many digital currencies could be playing a role in their value fluctuations and volatility in the short term, and causing them to be too deflationary in the long term. The high deflationary settings may attract a lot of investors at the outset but could hamper the networks from performing their actual use cases long term. This could lead to their potential failure later down the road, or more frequent than usual destructive boom and busts along the way.

The good thing is that reasonable supply-side strategies can be introduced that are completely transparent but yet building in market response to ensure a more stable performance, that augurs well for eventual long term success. Either that or future digital currency networks could include more practical but still transparent supply-side strategies, and may prove to be more successful networks in the long run.

References

1. Ken Alabi, May 25 2017, “Why Cryptocurrencies are not yet Making a Big Impact in Payment Processing“, Published on Medium, https://medium.com/@alabi.ken/why-cryptocurrencies-are-not-yet-making-a-big-impact-in-payment-processing-3ea1f71d2dee

2. Ken Alabi, July 2017, “Digital blockchain networks appear to be following Metcalfe’s Law”, Electronic Commerce Research and Applications, Volume 24, July–August 2017, Pages 23-29 https://doi.org/10.1016/j.elerap.2017.06.003

3. Ken Alabi, Jun 16, 2017, “A Macro-Mathematical Model for the Observed Value of Digital BlockChain Networks”, Published on Medium. https://medium.com/@alabi.ken/a-macro-mathematical-model-for-the-observed-value-of-digital-blockchain-networks-23cc8e0dc7ea

4. The Economist, May 15 2014, “Money from Nothing”, https://www.economist.com/news/finance-and-economics/21599053-chronic-deflation-may-keep-bitcoin-displacing-its-fiat-rivals-money

5. “Bitcoin Supply Strategy”, Bitcoin Wiki. https://en.bitcoin.it/wiki/Controlled_supply. Accessed July 12 2017.

6. Vitalik Buterin, Jun 27 2017. Tweet on ETH supply, Internet tweet. https://twitter.com/VitalikButerin/status/879858608091144193

7. Evan Dufffy & Daniel Diaz, June 14 2016,“ Dash: A Privacy-Centric Crypto-Currency“, Dash WhitePaper, https://dashpay.atlassian.net/wiki/display/DOC/Whitepaper.

8. Stellar Lumens FAQ page, 2017, “https://www.stellar.org/lumens/”

9. Michael Del Castillo, “United Nations sends Aid to 10,000 Refugees that utilized the Ethereum Blockchain.” Internet article. http://www.coindesk.com/united-nations-sends-aid-to-10000-syrian-refugees-using-ethereum-blockchain/, Accessed July 12 2017.

10. Vitalik Buterin, Jun 13 2017. “Vitalik Lauds UN Aid to Refugees making use of the Ethereum Blockchain”, Internet tweet. https://twitter.com/VitalikButerin/status/874603372141318145

11. Li, Y. and Ang, K.H. and Chong, G.C.Y. (2006) Patents, software and hardware for PID control: an overview and analysis of the current art. IEEE Control Systems Magazine 26(1):pp. 42-54.

12. Cooper, Douglas. "PI Control of the Heat Exchanger". Practical Process Control by Control Guru. http://controlguru.com/pi-control-of-the-heat-exchanger/, Retrieved 2014-02-27.