POLICY PROPOSAL

UNIVERSAL BASIC INCOME VIA DIGITAL CURRENCY FOR FINANCIAL SECURITY AND ECONOMIC GROWTH

25 JANUARY 2015

BY JOHN LAROCCO

SUMMARY

Digital currencies, such as Bitcoin and its derivatives (known as altcoins), represent at different approach to money that simultaneously allows entirely novel possibilities. With the automation destroying entire economic sectors, the universal basic income (UBI) may become an essential tool for continued economic prosperity and social stability. The digital currency-based implementation of a UBI program could enable it to be turned into a cost-effective, and even revenue positive, for the country. This proposal details the benefits and concerns of a digital currency-based UBI, as well as related applications of the technology.

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Overview

Digital currencies and automated finance may replace costly bureaucracies while enabling novel possibilities for social investment. The first generation of digital currencies, such as Bitcoin and its derivatives (known as altcoins), were dependent upon a decentralized, peer-to-peer (P2P) computer network to function [1]. Despite a number of hacking incidents on altcoin exchanges [2] [3], an informal economy has grown up around them. Experimentation and new concepts are rife in this field, so the market is still very dynamic.

Digital currencies have been developed for individual nations (such as the Icelandic Auroracoin [4]) and indigenous peoples (such as the Lakota MazaCoin [5]). New digital currency systems, dubbed the Bitcoin 2.0 generation, include platforms such as Counterparty, Ethereum, Ripple, and Stellar. New options pioneered by these systems include software mediated "smart contracts" and virtual corporations. Pioneering digital currencies are already being designed specifically with a basic income included, such as uCoin and Bitnation's new basic income feature.

This proposal describes the development of a nation-specific digital currency (hence fore referred to as the Ubicredit), and novel strategies resolving the legal and security issues with many current digital currencies. In addition, inequality even in previously equalitarian states like New Zealand has widened in recent decades. A universal basic income (UBI) may alleviate this [6].

1.2 Implications

First and foremost, the Ubicredit endeavor would set novel precedents in both addressing inequality and in finance technology. The novel nature of digital currency has dissuaded many budget-constrained governments from experimentation. A limited, trial endeavor could take risks and set precedents before any major public effort was launched. In addition, the project may provide some benefits of public banking without need for increases in government spending. Additionally, the national economy would not be as threatened by automation and even provide some defense against financial attacks. Many of the methods proposed here could potentially cut costs and promote efficiency for charitable and civic organizations. In addition, the concept could potentially spur public interest in information technology (IT).

1.3 Resources

The implementation of Ubicredit would require a diverse range of resources. These would include programmers, financial and legal advisement, and physical data centers. Primarily, a programmer would be necessarily to implement the software. The non-profit or government organization (henceforth referred to as the Foundation) would need to be structured and staffed for the continued oversight. Some relevant suggestions are detailed in the report. However, the scope of this report is to summarize the background issues and propose an implementation for Ubicredit. A basic background of related terms and potential precedents [5] [7] will be provided, followed by goals and benefits, a proposed implementation, and closing thoughts.

2 BACKGROUND

2.1 Summary

Bitcoin was the first digital currency to achieve mainstream recognition. Since its creation by an originator or group of originators using the name "Satoshi Nakamoto," the concept has spurred the development of a diverse online economy and other altcoins [8]. Other altcoins range from currencies similar to Bitcoin (such as Litecoin) to political activism (such as MazaCoin) to media experiments (such as Arscoin) to semi-humorous endeavors (such as Dogecoin) to assisting scientific research (such as Gridcoin) experiments in demurrage-based systems (such as Freicoin). The range of services and products available is no-less broad. While some sites carry illegal merchandise, many more offer legitimate services. Bitcoins and altcoins can be exchanged for traditional fiat currencies at "exchange" websites, although the amounts handled by exchanges are typically smaller than the conventional foreign exchange markets. Traditionally, a "coin" might consist of: a client to run the software, the unit of currency itself, a "wallet" program to store balances, and a network of recorded transactions called the blockchain.

2.2 Basic Traits and Terminology

The first generation of digital currencies, Bitcoin and altcoins, shared many traits and introduces terminology retained by later generations. They can be subdivided to smaller values (e.g., 10E-7 for Bitcoin), allowing for smaller transactions than whole "coin" tokens. A common trait among these digital currencies is the reliance on a decentralized network of devices with the basic software installed [1]. Each device with the software installed acts as a node on the network, often known to other computers only by a random public key. Transactions between machines are verified and encrypted using a ledger stored on each machine in the network [9] called the blockchain.

New blocks of coins are generated at a rate dependent upon a node's ability to perform calculations for the network, a process known as mining. The software is hard-coded with an ultimate limit of "coins," and mining becomes more difficult as the limit is approached. Theoretically, early adopters are rewarded as each individual "coin" gains more value, while later adopters face diminishing returns. The altcoins that award new software token balances based upon processing power are referred to as "proof-of-work" (POW).

Digital currency units are stored in "wallets," addresses where "payment" is sent to. Wallet programs can be found for all manner of electronic devices, ranging from desktop PCs to smart phones to online "wallet" sites. Even in the absence of online connections, digital currency systems could utilize portable devices (e.g., USB drives) instead, although delays could be significantly increased [8]. Other digital currency systems have improved upon this.

A digital currency can be seen as a corporation that is highly decentralized, entirely managed by software, able to subdivide its "shares" into smaller commodities for sale. As such, currency issuance adds new shares at a rate dependent upon the algorithm, transferring them to "shareholders." Just as there are non-profit corporations, a digital currency may serve as the basis for an automated non-profit organization. Also, a digital currency may provide a transaction network and additional security [3].

2.3 Security

The decentralized nature of digital currency networks does grant added resilience against attempts to totally destroy or disable the network. Their security can be compromised,

just as that of any other system can [3]. Often, individual nodes are targeted rather than the entire network, and not all users practice in-depth cybersecurity procedures. Cyber-attacks that allow a hacker to seize control of a device or server with a wallet may "rob" the contents of such.

Encrypting transactions does not mean coins cannot be stolen. Sub-par security utilized by many online exchanges has resulted in a rash of Bitcoin and altcoin "heists," including one at the Mt. Gox exchange totaling $468 million USD [10]. Fraud may also be a concern, as most altcoin exchanges do not offer consumer protections on par with conventional financial services. Security issues are one reason why the price of an altcoin may be extremely volatile.

An innate vulnerability of the POW system is the vulnerability known as the "51% attack." If a single actor contributes the majority of processing power of the entire network, they can disrupt other transactions in the process. An alternative to "proof-of-work" is known as "proof-of-stake" (POS), and is largely resistant to this. POS begins with a baseline number of units created, with issuance and currency creation varying based on the specific implementation. POS can be combined with other systems, such as the POS/POW hybrid Peercoin.

Many of the second generation (or Bitcoin 2.0) protocols utilize consensus-based decision making, which acts as an open electronic ledger. All assets in the system are denoted in terms of a "native token" to the ecosystem (e.g., XRP in Ripple). Consensus-based systems are more centralized than altcoins, but still offer many of the security advantages of digital currencies without the vulnerability to a 51% attack. The primary examples of consensus-based systems include Ripple and Stellar.

Sidechains, or protocols existing in parallel with other digital currencies, are a secondary layer of protocols atop an existing blockchain. New frameworks, such as Ethereum and Counterparty, offer even more complex options for digital equity, contracts, and the like. The Bitcoin 2.0 protocols, based upon consensus and sidechain protocols, allow for complex options, ranging from commodities trading to exchange of fiat currencies to computer-mediated contracts.

2.4 Legality

Different nations have legally responded to digital currency in divergent ways [11] [12]. While the network itself cannot be realistically shut down, exchanges have been primarily targeted. If a government classifies a digital currency as a currency or commodity, certain taxes and fees may be required, as well as licenses on the exchange's part [11]. Requiring exchanges to grant some measure of consumer protection or minimum security may be a more realistic effort than totally banning digital currency. In the case of a government-issued digital currency, a highly relevant framework would be complementary currencies.

A related concern is the use of digital currency to purchase illicit goods and services (e.g., banned substances and illegal weapons). These concerns are often based on misunderstanding, as each node on the network retains a record of transactions associated with a particular public key. If law enforcement officials examine relevant digital devices, the task of associating public keys with the balance of a particular wallet becomes easier [1] [2]. At the same time, identifying the sites through which transactions occur via undercover identities could provide a stronger case than simply trying to block or ban them.

2.5 Universal Basic Income

The universal basic income (UBI) is the concept of paying all citizens, regardless of wealth or employment status, a fixed amount of money. A UBI providing the equivalent of a living wage was recently voted on in Switzerland [6], but costs remain high and potentially include tax raises and cuts to other programs. However, evidence from Namibia, the Native American Cherokee, and Canada shows that even a small amount of money from a UBI program can greatly benefit lower and middle class groups [13] [14] [15].

Automation has the potential to wipe out entire sectors of the economy, including white collar ones. The basic income would ensure that citizens are able to continue education, pursue self-employment, and otherwise contribute to the economy. Additionally, it would promote social stability by ensuring basic necessities for all [13] [14] [15]. The government would have access to more funds indirectly, due to an expanded tax base. New legal precedents would be set [16]. Even employed citizens would have more money of their own to save or use.

3 GOALS AND BENEFITS

The goal of this project is to create a cost-effective and novel approach to UBI for social and economic stability.

3.1 Goals

The policy goals include the framework essential for the system. This will include:

a. Software implementation of a national currency and payment system.
b. Formation of a managing body (e.g., a “Foundation”).
c. Integration with the financial system.
d. Ensuring that the system continues to meet its goals.

3.2 Benefits

The potential benefits would include:

a. Expanding the range of resources for citizens.
b. Providing economic security against automation.
c. Giving additional robustness to the national financial system.
d. Creating new sources of income.
e. Political benefit for the party implementing it.
f. Setting international precedents for digital currency law.
g. Expanding government revenues indirectly via increased tax revenue.
h. Creating predicable, stable demand for the national currency.
i. Building a secure infrastructure for online local businesses.
j. Familiarizing citizens with technology.
k. Facilitating remittances for foreign workers.

4 IMPLEMENTATION

4.1 Technical Implementation

The political, technical, and financial implementations of Ubicredit overlap to a large degree, and this implementation integrates and improves upon several precedents. Technically, the Ubicredit would exist as a series of tokens on the Ripple or Stellar payment networks (or a similar consensus-based ledger system). This means that their issuance would be handled by the Foundation only, and that they already have a versatile and proven network that reduces the need for extensive debugging.

Ideally, the core Ubicredit should be released as open-source software, to allow for public scrutiny of code, as with other digital currencies. A client should be released for Windows, Mac, Linux, and other operating systems as well.

At first, a simple and arbitrary peg between Ubicredit units and fiat currency could occur, which would then be adjusted each payment period. In order to receive Ubicredit payments, an individual should be either:

1) An adult citizen.
2) A permanent resident (18 or older).

Payments would be issued to recipients on a regular basis (e.g., weekly or monthly), with unused balances of recipients wiped clean prior to the issuance of new currency by demurrage. The exception to this would be those seeking to purchase Ubicredit units from the Foundation directly.

At any time, a client could purchase Ubicredit units from the Foundation. If a client holds a minimum balance of Ubicredits for a minimum required time, the client could vote on how a portion of the Foundation's sovereign wealth fund is invested. The minimum balance and minimum required time to hold it would both increase over time, incentivizing early adoption.

However, the ideal payment system should be accessible even for technical laypeople. As such, a debit card compatible with existing payment networks should be implemented. ANX, a Hong Kong-based company, offers Stellar compatible Visa debit cards. The technology would simply be adapted for the country in question, and cards issued to all legitimate recipients. They would then receive a monthly balance on that card.

4.2 Deployment

The Foundation would retain "reserves" of the digital currency for any prospective investors and its own sake, as well as maintain the list of recipients. The system would operate according to this series of steps (assuming a monthly payout):

1) Check recipient list once a month and store addresses.

a) Check if payment from prior month was used by each recipient.

b) If no payment used for fiat currency in 24 months, remove address from list.

c) Clear Ubicredit balances from each recipient address on list, excluding those that purchased Ubicredit units in prior months from Foundation.

2) Check size of Foundation reserves.

a) Ensure reserve size is at least 50% of total Ubicredit units (and “refresh” this value based on the total number of Ubicredits in circulation).

b) Check inflation/deflation using commodity prices and foreign exchange data. Adjust payment size based upon this.

c) Delete or add Ubicredits in reserve as necessary.

d) Redeem a portion of new Ubicredits to generate cash reserves in fiat currency for national wealth fund (this can be done by just having the “official” Foundation address as a recipient).

3) Issue payments for all valid, active addresses.

a) Select a random second in the first minute after midnight of new month.

b) Send out monthly Ubicredit payment size for all valid addresses at that random second. (This is to limit potential arbitrage-based abuse of the system).

b) When user initiates "redemption" of cash for national fiat currency, a small amount (~1%) goes into cash reserves and wealth fund.

c) Wait for next month.

Additionally, recipients may be allowed to vote on how the Foundation’s wealth fund is used or even submit proposals, although the Foundation would retain the final decision. Integration with existing payment and finance infrastructure, such as local banking and transactions systems, is essential. The debit card approach is probably the most intuitive for less tech-savvy individuals.

4.3 Related Issues

The basic Ubicredit system presented here has implications beyond automated basic income. Currency war and financial arbitrage could be drastically changed by using such an approach. Especially important portions of the Ubicredit system would include the security of the Foundation’s recipient and client database, the national wealth fund’s voting protocol, potential shortfalls in estimating inflation/deflation, and the problem of determining an adequate payment size. On the plus side, the digital currency approach may potentially make domestic finance and the process of currency issuance easier to manage.

Other issues could include new venues of financial warfare becoming possible outside of the country. For example, if another party has a substantial amount of the national currency and Ubicredits, they could flood the market or use short sales to drive the price down immediately after a periodic payment. A potential counter to this is have capital reserves on hand as equivalent to the sum of issued Ubicredit to prevent the “bank run” scenario and drive the price back up.

Perhaps most interestingly is the potential to use such a method to gain political and economic leverage over another country. If a digital currency was pegged to a foreign country’s currency in a way that was disadvantageous to that country’s markets (e.g., exports) and then issued to its citizens, that country’s government would find shutting such a system down difficult.

The party launching such an attack, however, would need some reserves of currency or assets to initialize it, although a successful attack might create its own “black market,” offering a large rate of return on a small investment of resources. In this case, digital currency effectively lowers the barriers to entry for financial attacks, much like asymmetric warfare lowers the barriers to entry for non-state actors to achieve objectives.

Such incidents could be performed by countries, but also by corporations, activist groups, or even individuals.

Interestingly, the best defense could be a domestic basic income system. This would mean an attacking party has to spend a much larger amount of resources for substantial economic and financial disruption. Likewise, sustaining such a disruptive attack would require even more resources. Countries holding significant assets and foreign reserves would be well-advised to consider such scenarios.

5 PROPOSED STRATEGY

The Foundation would require the following resources: a software engineer to deploy the system, a hosting service, financial and legal advisors to ensure relevant laws and security protocols are followed, and a well-organized public relations campaign to familiarize people with the concepts. Additionally, distribution of electronic cards would be the most direct and simple way to integrate the Ubicredits into the financial system. The following steps would be taken:

a. Formation of the Foundation.
b. Writing and implementing the software.
c. Determining initial payment size based on cost of living at poverty line.
d. Ensuring card system is compatible with existing financial infrastructure.
e. Implementing automated monthly top-up system for cards.
f. Raising awareness of the program to attract investors.
g. Issuing cards to those who sign up for it.
h. Shifting payment size on a period basis.

6 CONCLUSIONS

Software presents an alternative to the costly bureaucracy currently used in the public and private sectors. Digital currency is merely the tip of the iceberg, and the Ubicredit idea presented here is an example of how a novel commodity can become a cost-effective means of cyber-welfare. By deploying basic income to serve the interest of citizens, the Foundation would familiarize a new generation with increasingly essential skills, address the automation of the economy, and provide vital resources for social development. In addition, a platform like Ubicredit would provide a suitable platform and infrastructure for future improvements. An endeavor like the Ubicredit could be deployed almost immediately using a relatively small amount of resources. A small-scale test may be feasible even in the short term to further hone the concept. The precedents set would be ground-breaking socially, technologically, financially, and legally.

7 BIBLIOGRAPHY

[1] C. Decker and R. Wattenhofer, "Information propagation in the Bitcoin network," *Proc. IEEE Int. Conf. on Peer-to-Peer Computing,* vol. 13, 2013.

[2] F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System," *Proc. IEEE Int. Conf. Privacy, Security, Risk and Trust,* vol. 3, pp. 1318-1326, 2011.

[3] I. Miers, C. Garman, M. Green and A. Rubin, "Zerocoin: Anonymous Distributed E-Cash from Bitcoin," *IEEE Symposium on Security and Privacy,* pp. 397-411, 2013.

[4] Auroracoin Team, "Auroracoin," 2014. [Online]. Available: http://www.auroracoin.org/. [Accessed 14 March 2014].

[5] MazaCoin Development Team, "MazaCoin," MazaCoin Development Team, 2013. [Online]. Available: http://www.mazacoin.org/. [Accessed 14 March 2014].

[6] S. Faris, "The Swiss Join the Fight Against Inequality," Bloomberg Businessweek, 16 January 2014. [Online]. Available: http://www.businessweek.com/articles/2014-01-16/inequality-fight-swiss-will-vote-on-minimum-income. [Accessed 14 March 2014].

[7] B. F. Óðinsson, "Auroracoin Airdrop Blueprint," 2014. [Online]. Available: http://auroracoin.org/blueprint.php. [Accessed 14 March 2014].

[8] P. Singh, B. Chandavarkar, S. Arora and N. Agrawal, "Performance Comparison of Executing Fast Transactions in Bitcoin Network Using Verifiable Code Execution," *Proc. Int. Conf. Advanced Computing, Networking and Security,* vol. 2, pp. 193-198, 2013.

[9] National Institute of Standards and Technology, "Descriptions of SHA-256, SHA-384, and SHA-512," [Online]. Available: http://csrc.nist.gov/groups/STM/cavp/documents/shs/sha256-384-512.pdf. [Accessed 14 March 2014].

[10] J. Wagstaff, "Mt. Gox bitcoin debacle: huge heist or sloppy glitch?," Reuters, 28 February 2014. [Online]. Available: http://www.reuters.com/article/2014/02/28/bitcoin-mtgox-heist-idUSL3N0LX2SP20140228. [Accessed 14 March 2014].

[11] K. Hill, "Federal Judge Rules Bitcoin Is Real Money," Forbes, 2013. [Online]. Available: http://www.forbes.com/sites/kashmirhill/2013/08/07/federal-judge-rules-bitcoin-is-real-money/. [Accessed 14 March 2014].

[12] G. Baczynska, "Russian authorities say Bitcoin illegal," Reuters, 9 February 2014. [Online]. Available: http://www.reuters.com/article/2014/02/09/us-russia-bitcoin-idUSBREA1806620140209. [Accessed 14 March 2014].

[13] Velasquez-Manoff and Moises, "What Happens When the Poor Receive a Stipend?," New York Times, 18 January 2014. [Online]. Available: http://opinionator.blogs.nytimes.com/2014/01/18/what-happens-when-the-poor-receive-a-stipend/. [Accessed 14 March 2014].

[14] C. Haarmann and D. Haarmann, BIG Coalition, 2012. [Online]. Available: http://www.bignam.org/.

[Accessed 14 March 2014].

[15] Forget and Evelyn, "The Town With No Poverty," February 2011. [Online]. Available: http://sociology.uwo.ca/cluster/en/PolicyBrief10.html. [Accessed 14 March 2014].

[16] B. McLannahan, "Japan to class Bitcoin as a commodity," Financial Times, 7 March 2014. [Online]. Available: http://www.ft.com/cms/s/0/a8381228-a5a0-11e3-8070-00144feab7de.html#axzz2vvIPMv00. [Accessed 14 March 2014].