Designing 21st Century Curriculum for Bitcoin and Blockchain Studies

Michael Thombs
Business Studies & Economics, Department, Salve Regina University, Newport, Rhode Island USA
thombsm@salve.edu

Amy Anastasia Tillman,
Independent ADJ Consultant, San Diego, California, USA
amytillman414@gmail.com

Abstract

This paper will explore an effort to build an instrument that may be used by curriculum designers to help build a course or series of courses in the Bitcoin, Altcoins, and Blockchain Technologies Space. In October of 2008, a pseudo-individual named Satoshi Nakamoto, sent a white paper (*Bitcoin: A Peer-to-Peer" Electronic Cash System*) attached to an email to a small group of Cyberpunks and Cryptologists and introduced a new form of electronic digital currency named Bitcoin. The fundamental concepts associated with Bitcoin and the Blockchain infrastructure supporting the coin was revolutionary thus creating the potential for flow of digital currency with anonymity. Satoshi had finally solved the "double-spending" problem, a problem that plagued the group for over a decade. As the financial world was beginning to collapse in 2008-2009, the time for an alternative, decentralized, crowd sourced, global financial instrument had arrived. Curriculum designed, with the aid of the instrument, will help students delve into the murky waters of crypto currencies, alt-coins, Blockchains, "Proof-of-work" strategies, and monetary privacy issues. The instrument provides design guidance on topics such as: Bitcoin, Altcoins, Blockchain Technology, Cryptology, private and public encryption keys, Proof-of-Work Strategies, Hashing Algorithms, Hashrate difficulty, Smart Contracts, E-Wallets, Exchanges, Mining Pools, Mining, ERC20 Tokens, The Dark Web, The Silk Road, the philosophy behind Bitcoin, and a history of digital currencies.

Keywords: *Bitcoin, Altcoins, Blockchain, crypto currencies, Hashing Algorithms, Hashrate, Smart Contracts, E-Wallets, Exchanges, Mining Pools, Mining, ERC20 Tokens, The Dark Web.*

Overview

As stated in the abstract, this paper will explore an effort to build an instrument that may be used by instructors, curriculum designers, and textbook authors to help them build a course or series of courses in the Bitcoin, Altcoins, and Blockchain Technologies space. The authors are scheduled to begin teaching a Junior-level (300) undergraduate course on Bitcoin and Blockchain technologies in the spring semester of 2019 and possibly as early as Fall 2018. The new course will be offered at Salve Regina University (SRU), Newport, Rhode Island U.S.A., a small (2,180 undergraduate and 643 graduate students) private institution of higher education offering liberal arts degrees (Baccalaureate, Masters, and Doctoral.) This paper is intended to help users create a course offering by considering each of the elements that make up the instrument. The elements of the instrument will motivate the educator/designer to consider important components and are free to add, change, or delete.

The authors make the following assumptions throughout the paper:

- The word *Blockchain* represents a radical change to the way data is collected, stored and distributed. Blockchain is **NOT** a synonym with the word Database.
- Pertaining to any discussion of Blockchain Technology topics must include decentralized, peer-to-peer networking, distributed data management, global environment, Immutability, Cryptography, and consensus-based decision making.
- Bitcoin and Alt-coins embody a disruptive technology and must **NOT** be treated as another payment system such as PayPal, VISA, or MasterCard.
- There is no shame in using the word Bitcoin or Alt-coin without the word Blockchain as though Blockchain is the adult or guardian of an immature, unruly, or disruptive child that needs supervision or validation.
- The authors will use the term: Crypto Currency (CC) to encompass Bitcoin, Alt-coin, and Blockchain technology.

Course and Textbook Details

The following list of objectives may be considered for a course, workshop, or workbook.

Objectives: By the end of the course, each student will be able to:

1. Discuss the history and evolution of Bitcoin, and digital cash payment systems
2. Define what Bitcoin, alt-coins, and tokens are and how they can be used
3. Describe how blockchain-driven payment systems react in different societies and cultures
4. Make intelligent, well-informed futuristic predictions for the future of blockchain-driven systems using technological, economic, and cultural information
5. Explain in detail how a blockchain functions by describing each of the fundamentally important features of the blockchain and how components interface
6. Discuss taxable events and tax collection issues in paradigms that integrate digital cash systems
7. Discuss the relationship of blockchain technology to The Internet of Things (IOT)
8. Explain the process of mining digital currency, mining pools, and digital coin disbursement strategies
9. Explain the role and purpose of smart digital contracts and be able to identify several examples where they may best be used
10. Discuss three or more alt-coin and token models and ways they are intended to be used, distributed, and stored
11. Compare e-wallet, paper-wallet, and cloud-based wallet storage strategies and associated risks
12. List and describe three or more consumer-related risks and security issues with methods and policies that will increase security
13. Discuss issues of trust, 51% attack strategies, and threats to distributed peer-to-peer, consensus-based blockchain systems
14. Compare and contrast blockchain technologies to traditional centralized database technologies
15. Show several ways that blockchain-based digital currency systems are appropriate in trade, commerce, and business
16. Explain how and where Cryptography is incorporated in blockchain technologies
17. Explain and give example of soft- and hard-forks that can and do occur on blockchain networks
18. Explain how the peer-to-peer networks of a blockchain-based system share data and validates blocks using consensus votes
19. Compare and contrast three or more “proof-of-work” strategies and discuss appropriate applications for each
20. Name or list three or more applications that may benefit from adoption of blockchain technologies

Reading and supplemental Documents:

The following texts were helpful to the authors in determining ways to approach the historical, philosophical, and Technical components of the crypto space. The following texts will help the designer begin formalizing their lists.

Philosophical:

The Internet of Money Part Volume One by Andreas M. Antonopoulos. ISBN: 1537000454

The Internet of Money Volume Two by Andreas M. Antonopoulos. ISBN: 9781947910065

The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order by Paul Vigna and Michael J. Casey, 2006. ISBN-13: 978-1250081551

Historical:

The Book Of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto, by Phil Champagne, 2015. ISBN-13: 978-0996061315

Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money by Nathaniel Popper, 2016. ISBN-13: 978-0062362506

Technical:

Mastering Bitcoin: Programming the Open Blockchain 2nd Edition by Andreas M. Antonopoulos. ISBN-13: 978-1491954386

Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World by Don Tapscott and Alex Tapscott, 2016. ISBN-13: 978-1101980132

Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners by Chris Dannen, 2017. ISBN-13: 978-1484225349

Class Evaluation and Projects

Since the crypto space is fast changing and complete with new unfolding current events, the authors think that in the evaluation section designers consider packaging several assignments into a larger written effort. Students may work in teams and select a main topic for the course and the semester. Students will perform standard review of the literature and possibly include some primary data from surveys, focus groups, or personal interviews. An analysis of the research will be done and finalized in the formal presentation to the class or a special interests group such as a club. Students will write an abstract suitable for submission to an international conference that accepts student papers. The abstract will include appropriate cover-page information. The abstract will be submitted to one or several conferences for consideration. A final paper will be produced that gathers and formalizes all research and analysis. This strategy has been helpful to students because it helps them build a portfolio of their important academic works. The authors have applied this strategy to help students present papers at international conferences since 2006 including: Beijing China, Athens Greece, Hawaii USA, Detroit USA, Las Vegas USA, and Dubai UAE.

Strategic Elements

I. The Philosophy of Crypto-Currencies

In October of 2008, a pseudo-individual named Satoshi Nakamoto, sent a white paper (Bitcoin: A Peer-to-Peer" Electronic Cash System) attached to an email to a small group of Cyberpunks and Cryptologists and introduced a new form of electronic digital currency named Bitcoin (Champagne, 2014). The fundamental concepts associated with Bitcoin and the Blockchain infrastructure supporting the coin was revolutionary thus creating the potential for the introduction of a digital currency. Satoshi had finally solved the "double-spending" problem, a problem that plagued the group for over a decade. As the financial world was beginning to collapse in 2008-2009, the time for an alternative, decentralized, crowd sourced, global financial instrument had arrived.

In the process of designing a course on Bitcoin/Blockchain, setting an appropriate philosophical framework is important. From Satoshi's 2008 white paper, statements from the Bitcoin-QT Core development team, and proponents of Bitcoin/Blockchain technology

such as Andreas Antonopoulos in his book, *The Internet of Money*, a unified theme that describes a disruptive technology (Antonopoulos, 2017a.) Andreas Antonopoulos coined the phrase *Bitcoin un-banks the banked, and banks the un-banked* (Antonopoulos, 2017a). What Andreas is describing is the 2 billion plus people in the world who have no bank and no banking services. A smart-phone, use of Bitcoin, and an Internet connection have the potential of giving this population their own bank. In reverse, approximately 4.5 billion people worldwide have banking services but find that *their* money is tied in the banking system and are not readily available (Antonopoulos, 2017a.) The authors experience three to nine-day transfer delays when moving money to exchanges and banking services come along with significant fees (the authors where charged with a $35.00 transfer fee to wire money using SWIFT wire service in 2017.)

II. History Digital Currencies

The designer may wish to step back and consider starting this section with lessons that first talk about the history of other currencies. The use of gold, silver and other tangible items may provide a solid base for comparison when introducing virtual currencies. Research will show many studies comparing traditional currencies and the introduction of Fiat currencies (physical currency like bills and coins which is deemed legitimate by a government but is not backed by something of value, e.g. Gold/precious metals). Transitioning from solid tangible asset-based currencies, to Fiat currencies, and finally, to virtual currencies may serve to help students better understand the evolutionary path.

Following on with an analysis of the cyber-punk movements and attempts to create digital cash systems shortly after the birth of the Internet would seem to be the next logical progression. The authors think that this section provides some of the best topics for student research and discussion. Students can become excited when examining crypto currencies to other forms of currency in these times of Quantitative Easing (QE), Fiat Money, and government sponsored bailouts.

III. Crypto Currencies(CC)

Several successful strategies may work in a classroom or workshop event. From a lecture only point of view or if time is not abundant, Bitcoin could be the teaching and research model. It would be reasonable to expect students to transfer what they have learned about Bitcoin and apply it to other coins and perform their own dealt analysis. If a lecture/symposium is the classroom model, student presentations can be used to broaden the field of alt-coins covered in the semester. For textbook developers, an approach of using multiple chapter-authors may be appropriate. The authors rely on www.coin marketcap.com to stay informed. This tool shows market cap, volume, has charts, and can be used to show important information about Tokens. www.tradingview.com is another useful tool for performing technical analysis. At the time of this writing, BTC, LTC, DASH, ETH, and BCH are top coins and may be tracked and analyzed for classroom demonstrations. The authors built and maintain a website that may be easily use on a mobile device that captures and renders the top dozen *CoinMarketCap* coins.

IV. Proof-of-work strategies

The designer will consider the basics of Bitcoin's *proof-of-work* strategy and leverage that against several other coins that deviate from the SHA256 hashing algorithm. Examples of alternate hashing algorithms are: Script and X11 (Antonopoulos, 2017b). In addition to proof of work strategies, the designer, time permitting may explore alternatives such as *proof-of-stake* and *proof-of-ownership* (Dannen, 2017). This is a second rich area for student research, projects, and presentations.

V. Monetary and privacy issues

In traditional non-cash money, credit card, and banking transactions, the purchaser's identity must be known. Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations forces banks and, exchanges, and credit card companies to collect, store, and protect customer information. Identity theft can lead to hackers taking control of a person's bank account, credit card, tax refunds, PayPal accounts, securities accounts just to name a few. Though it may be argued that hackers may hack wallets of Bitcoin, alt-coins, and Tokens, these hacks differ because they do not start with identity

theft. The curriculum and course lesson designer may wish to spend lecture and discussion time looking into the pros and cons of trusting a central money/credit source and begin discussing decentralized systems. Because traditional money transactions are tied directly to a person's identity, the systems that support these transactions must be made secure. Securing transactions are expensive when considering time, equipment, and labor. Traditional transactions require sophisticated servers, server farms, point-to-point encryption, firewalls, Intruder Detection Systems (IDS), and high-skilled labor. The designer may leverage these points when considering the alternatives that virtual crypto currencies offer.

VI. Blockchain Technology

There are two main issues about blockchain that the authors wish to note. First, there are many alternative blockchain variants that are becoming popular. Time should be give to allow students to research and report on through the recommended student presentation efforts. The second important issue surrounding discussions of blockchain is fake-blockchain technology. The word blockchain has become well known and system designers may feel the temptation to substitute the word blockchain for the word database (Antonopoulos, 2017a), and offer a new and improved product without any substantial redesign. The designers must provide adequate time to fully define the differences between blockchain and traditional relational or hierarchical databases. The important features that must be included in any treatment of blockchain must include: peer-to-peer, distributed, consensus-based, crypto logically secure, immutable, global, semi-anonymous, and decentralized. Failure to meet any of these important elements should raise suspicion.

VII. Cryptography

In this section on Cryptography, a continuation of the discussion on blockchain technologies, the designer will include a discussion about how Digital Fingerprints are made, how they are used to create immutability and add it to the blockchain. Discussions should include the basic format of each block in the blockchain, which elements are used to create the digital fingerprint, how hash algorithms are used, and begin discussions and research in to public and private keys.

VIII. Private and public encryption keys

This is a continuation of the topics of blockchain and cryptography. Asymmetric private and public keys are an important topic to consider. The designer should pay close attention to Andreas Antonopoulos' book, *Mastering Bitcoin*, to help introduce the following important topics: creating private keys, SHA256, RIPEMD160, elliptic curve multiplication, Base 58 check-encoding, Wallet Import Format (WIF), compressed public and private keys, theory of checksums, hexadecimal and binary encoding, and address creation (Antonopoulos, 2017.)

IX. Hashing Algorithms

Students should be encouraged to explore several different types of hash algorithms use throughout coin-space such as SHA256, Script, and X11. The designer should plan on outlining how hash algorithms are used to creating private and public keys and creating and verifying digital fingerprints. The designer may stimulate discussion and elicit research in subjects such as Gaming Processor Unit (GPU) mining versus Application Specific Integrated Circuits (ASIC). A recent series of articles (Lethos3, 2017) shows how the alt-coin Monero core development team, is threatening to modifying the base code every 6-months to thwart the development of ASIC mining equipment. The authors think that real-time current events will stimulate student involvement, personal identification with the topic and provide stimulus and motivation.

X. Hash rate difficulty

In proof of work systems such as Bitcoin and Litecoin, miners are given a complex mathematical problem to solve. Solving the problem relies on brute-force computational power. The more power a miner commands the better the chance of solving the problem. The miner who first solves the problem, broadcasts the solution over the network and receives a pre-set threshold number of confirmations, writes the block and receives a reward. Rewards vary from coin to coin and from time period to time period and usually consist of a number of coins that are *Coinbase* (not the name of the exchange. Satoshi said in an email, "By convention, the first transaction in a block is a special transaction that

starts a new coin owned by the creator of the block" (Tapscott & Tapscott, 2016). It refers to a transaction with no inputs resulting in free coin to the miner) Students should become familiar with the mining effort, the protocols involved such as Stratum (www.bitcoin.stack3xchange.com) and proof-of-work alternatives. Students should be able to list three or more Hashing methods and link those to specific alt-coins.

XI. Market Caps

Bitcoin, alt-coins, and tokens do not share the same set of fundamental as stocks or securities. Stocks represent a certificate of fractional ownership in a company, some carry voting rights to owners of the security. Fundamental include company metadata such as Percent Earning (PE) ratios, Market Capitalization (Market Cap), and treasury and float volume figures. Bitcoin and most alt-coins have little or no fundamentals. Tokens, especially ERC20 Tokens (the astute student may point out that ERC20 Tokens are based on Ethereum!) are closer to resembling securities than Bitcoin or alt-coins because they may be used to represent fractional ownership in a company, usually a start-up company. It is no coincidence that start-up companies using tokens use the abbreviated term ICO, Initial Coin Offering, and a play on the more familiar abbreviation IPO, Initial Public Offering of a security on Wall Street.

XII. Smart Contracts

Bitcoin developers built in a scripting language that is not *Turing Complete*. This decision protects Bitcoin and other coins from certain types of hacking attacks. For example, iterative loops are not supported in Bitcoin therefore infinite loops cannot occur. Coins such as Ethereum do support fully Turing Compete scripting and guard against hacking attempts in different ways. The designer needs to outline and provide student resource materials along with lectures that focus on smart contract technology. At the time of this writing the DASH development team is build both a level-II and level-III application layer that leverages the original DASH network Layer-I to bring smart contracts to the application layer.

XIII. E-Wallets

Since the basic philosophical concept of crypto currencies is *to bank the unbanked, and un-bank the banked* (Antonopoulos, 2017a.) then every user is a bank. Banks traditionally have secure vaults wherein the money or hard assets are stored. If the crypto currency user is a bank, they too will need a vault. Vaults in crypto-space are called wallets. Wallets do not store coin or wealth as do their material counterparts. Wallets contain Private keys or Private/Public Key combinations. Private keys can be used to lock, unlock Bitcoin transaction in the Blockchain and to crate and verify digital fingerprints. The designer must craft lessons and discussions centering on these basic concepts. This unit may flow naturally from the section on Cryptography and Public/Private Key.

XIV. Exchanges

Exchanges are the gateways to Bitcoin, Alt-coin, and token ownership. Designers must provide adequate coverage of the two ways coins can be obtained: purchase through an exchange or mined via participation in the network as a full-node. Designers should exercise caution that all materials covered do not elicit, motivate, or encourage investing. A good design shows the paths that must be followed to link traditional banks to exchanges and exchanges with other exchanges.

XV. Mining

To pay attention and give adequate coverage of this section, the designer will cover miners, mining pools, mining-pool strategies, hash-rate, difficulty, mining protocols, the 51% attack problem, and mining equipment. The authors recommend using the analogy of the 1850 California Gold Rush (Popper, X). Students may appreciate the comparison of panning, picks and shovels, and tunneling to CPU/GPU mining, ASIC mining, and terra-hash mining equipment heading to the 14 nanometer level. Students may find research and Return on Investment (ROI) worksheets and online calculators satisfying and interesting.

XVI. ERC20 Tokens

ERC20 Tokens are a popular type of token that are built on the Ethereum blockchain and use the Ethereum network. Many ICOs use ERC20 Tokens because it is

easy to build, test, and manage. Student wishing to pursue a deeper and more technical journey may elect to research, build ERC20 Tokens on a test network. The Internet has several good references to turn to for help. The authors think that the Google-based MetaMask Chrome extension is a good place to start.

XVII. The Dark Web, the Silk Road, and the TOR network

The designer may begin their effort with a historical tour of crypt currency and in doing so may elect to include overage of Dark Web (also often referred to as the Dark Net,) the Silk Road, and the TOR network. There are dark areas of the Internet and there are dark areas of crypto currencies. Students with majors in cyber security and administration of justice may enjoy research in this murky area. Students will especially enjoy investigating the FBI seizure of Silk Road in 2013 (Vigna & Casey, 2106).

References

Andreas M. Antonopoulos (2016.) *The Internet of Money Part Volume One.* 29, 86 USA: Merkle Bloom LLC.

Andreas M. Antonopoulos (2017a) *The Internet of Money Volume Two.* 6,11,13 USA: Merkle Bloom LLC.

Andreas M. Antonopoulos (2017b) *Mastering Bitcoin: Programming the Open Blockchain 2nd Edition.* 70 California USA: O'Reilly Media , Inc.

Phil Champagne (2014.) *The Book Of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto.* 351 USA: E53 Publishing LLC

Chris Dannen (2017.) *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners.* Brooklyn New York USA: Apress

Lethos3, Reddit Post, 2017 from https://www.reddit.com/r/Monero/comments/5xfy06/why_the_asic_resistant_cryptonight_in_monero_is/

Nathaniel Popper (2016) *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*, Introduction page X. New York, USA: Harper

Don Tapscott and Alex Tapscott (2016.) *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. 36 New York USA: Portfolio / Penguin

Paul Vigna and Michael J. Casey (2016.) *The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order.* 126 New York USA: St, Martin's Press

About the Authors:

Dr. Michael Thombs and Amy Tillman (BA, MS) were first introduced to Bitcoin in 2010. For the past 12 years, they have coauthored papers and presented their studies all over the world and throughout the US including Hawaii, Detroit, Pennsylvania, New York, Boston, Las Vegas, Dubai UAE, Athens Greece, Beijing China, and now Windsor Canada. Topics have included technology, business, science, cultures and contact all from the global perspective.

During a trip abroad, before beginning her Master's program, Tillman was traveling abroad in Morocco in January 2008. As a single American female traveling in the MENA (Middle East and North Africa) region for the first time, her perception of the world and the people in it understandably was changed in many ways. She began to soak up the Moroccan culture, languages and see the world from a very different perspective. One of the most eye-opening experiences in Morocco was the access to different types of media and news coverage. Upon returning to The United States, Tillman was eager to share her experience of North Africa with Dr. Thombs including her very favorite new news source, Al Jazeera.

To their dismay, Al Jazeera was not accessible in Rhode Island, United States that led them to the questions: Why? What were they trying to keep from the American public or why was there such a lack of interest from within the U.S.? Why were they not willing to make information available about people in the MENA region? Who was keeping this information from the Americans?

After months of digging, Tillman and Thombs were able to find a Free-To-Air (FTA) satellite system that could access Al Jazeera English: a more filtered, western version of Al Jazeera

that Tillman experienced in Morocco. From this satellite system they were able to access different channels, one of which was *The Keiser Report* on Russia Today (RT). Max Keiser, the host, is an internationally known financial expert with years of experience with U.S. Wall Street provides commentaries on international finance and economics. Thombs introduced his university to this satellite system and its array of international channels and shared this discovery with hundreds of university students so they too could see the world from a perspective other than the endless battle of news between CNN, MSNBC, and the FOX News Network. The Keister Report played every day in the lounge between classes and caught the attention of Dr. Thombs when Keiser introduced a new, revolutionary form of digital currency which we now know as Bitcoin.

In early 2010 Bitcoin made another appearance while Tillman was perusing a Master's in Criminal Justice/International Criminal Law at Roger Williams University, Bristol Rhode Island, USA. Through studies of international criminal networks and the dark web, Tillman discovered an online commerce vehicle through an encrypted portal where anonymous individuals could sell anything and everything using a digital form of currency called Bitcoin. This online commerce site was called the Silk Road: named after the ancient network of trade routes throughout Eurasia to the Mediterranean, this online market sought to become accessible to the global arena and protect the anonymity of all users.

The Silk Road quickly became famously known for its online sales of illegal drugs and stolen merchandise but it was so much more than that. Literally anything and everything was being sold on this online forum, some legal, some illegal, and a lot of merchandise in the grey market. The Silk Road could only be accessed through a portal called The Onion Router (TOR) Network. This portal is used to access parts of the darknet not available to users without the downloaded portal access.

Eager to explore this mysterious new form of currency, Thombs and Tillman teamed up to try to figure out exactly what Bitcoin was, where it came from, who was controlling it and how could it be accrued, earned or collected and how could it be truly anonymous and protected. Eight years and the mining of several Bitcoin later, they have discovered that this was just the beginning of the revolution of global currency. The authors have been involved with Bitcoin mining using Raspberry Pi micro-computers, Application Specific Integrated Circuits (ASIC), the ASIC Blade, The ASIC Cube, Ant-miners, and the monster Teri-hash mining unit.