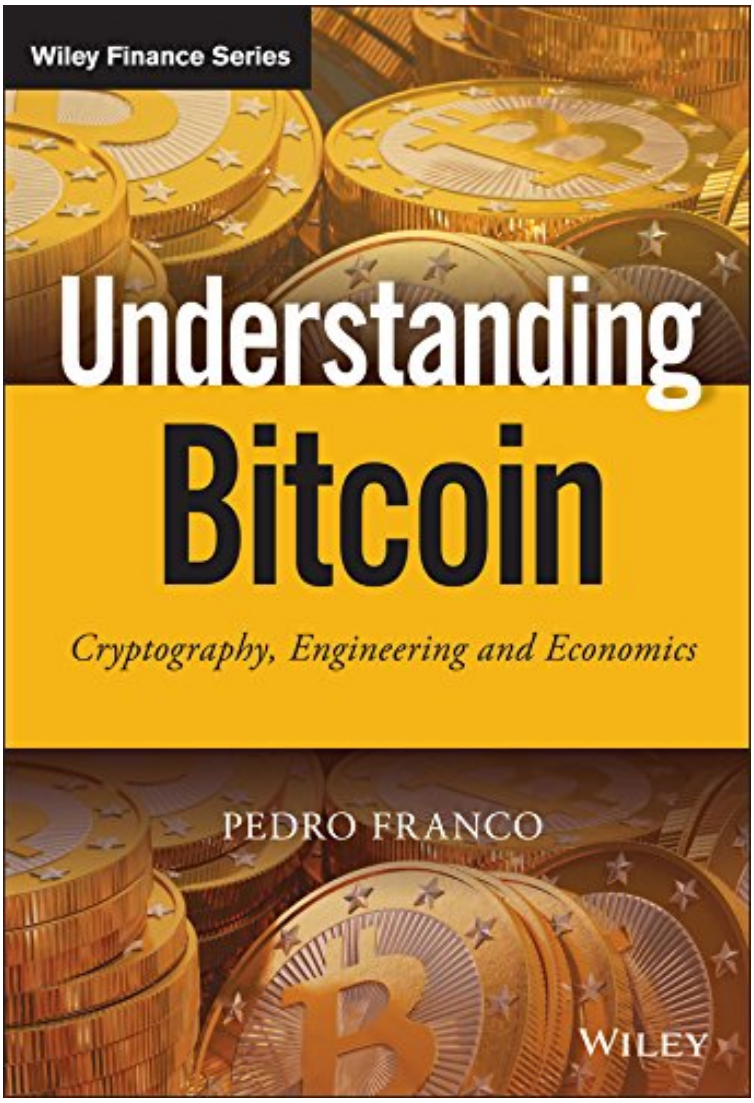
Understanding Bitcoin: Cryptography, Engineering and Economics (The Wiley Finance Series)

Pedro Franco
*DOC | *audiobook | ebooks | Download PDF | ePub*



#414393 in eBooks 2014-10-21 2014-10-21File Name: B00OTJE98C | File size: 23.Mb

Pedro Franco : Understanding Bitcoin: Cryptography, Engineering and Economics (The Wiley Finance Series) before purchasing it in order to gage whether or not it would be worth my time, and all praised Understanding Bitcoin: Cryptography, Engineering and Economics (The Wiley Finance Series):

4 of 4 people found the following review helpful. Perhaps mining for block rewards reminds people of scams like chain lettersBy ian allison/Katy allisonAt the core of this scholarly book is a dissection of bitcoin's biggest achievement. That is the transmission of value over the internet, an inherently insecure channel, without any reliance

on a trusted third party. Even the harshest critics of bitcoin the currency (as opposed to Bitcoin the protocol) would agree the technology has legs, and then some.Pedro Franco, the author of 'Understanding Bitcoin: Cryptography, engineering and economics' begins with a lapel-grabbing analogy: "Bitcoin could be used as an open platform for the exchange of value in much the same way that the internet is an open platform for the exchange of information."He adds that it would have been impossible to predict the importance of social networking in 1994, for example, reminding us we are currently witnessing "the first round of applications in the cryptocurrencies ecosystem".Franco's preface claims that a sceptical view of Bitcoin is perhaps the easiest to understand, which could be taken as a hint at the technical discussions that will follow. The sceptical view he is talking about is driven by a number of issues.It was very important in the beginning, when bitcoin bootstrapped itself into relevance, to rely on its miners to spread the word, to market it. This they did, sending it viral. Added to this hype, is the fact that miners are paid in bitcoin for their work securing the public ledger of transactions.This self-generating style of remuneration, combined with a wildly fluctuating exchange price, earned bitcoin a reputation among some as some kind of carefully wrought confidence trick. Perhaps mining for block rewards reminds people of scams like chain letters. Then there's Satoshi, bitcoin's nebulous mastermind, who also mined about a million bitcoins in the early days.Doubts seemed to be confirmed by events like the collapse of the Mt.Gox exchange, or the closure of Silk Road - formative events which had a seismic impact on the exchange value of bitcoin. Franco doesn't name names, however. He simply states that Bitcoin should not be confused with a Ponzi scheme because it is decentralised and not controlled by any individual.But in the fast-evolving and fiercely polarised world of bitcoin, it's become impossible make pronouncements on the technology's future from an entirely impartial standpoint. Facing off the sceptics is a devoutly anti-corporate hardcore of bitcoin enthusiasts, who would sooner join nodes and declare cyber-geddon on the world's banks than see them squeeze a cent out of cryptocurrencies.Part One: Introduction and EconomicsLiving on bitcoinLondon pair endure forced fasts but survive month-long challengeThe book promises financial professionals a comprehensive guide to bitcoin and other cryptocurrencies. In this regard, Franco's position could be described as a liberal third way. He takes a measured pop at the economic policies of reserve banks, but this is balanced by a passing invitation to the lower orders of the financial services sector, such as those involved in electronic payments.For example, Franco discusses ways of resolving disputes over transactions using funds held in escrow: this facility is built into credit cards, but is lacking from bitcoin. "Credit card processors are good candidates to provide these services, leveraging their expertise in dispute mediation," he says.Bitcoin start-ups are attractive because they seem to be able to hurdle prohibitive barriers to highly regulated financial services industry, such as holding a large capital base.But bitcoin currently inhabits a regulatory grey area. The issuance of private currencies is permitted under US law, provided they don't resemble the dollar. Since bitcoin is a decentralised system it cannot be classed as a money transmitter. However businesses that deal in it can, like payment processors and bitcoin exchanges. These fall under the definition of money transmitters in the US, which require a licence to operate from each state.Recent updates from America's Financial Crimes Enforcement Network (FinCEN) declared that neither bitcoin investors nor miners should be considered money transmitters, but this ruling did not cover web wallet services.At stake here are bitcoin's very low transaction fees. The average fee in the remittance market is reported to be in the range of 8% to 9%, as opposed to bitcoin transactions which cost between 0.01% and 0.05%.Standard anti-money laundering (AML) and know your customer (KYC) regulations cover all money transmitters. These compliance costs are ultimately passed onto customers. In defence of looming regulations, cryptocurrency advocates argue that money laundering using bitcoin would be very risky because all transaction records are kept in a public ledger."A regulatory framework that took into account this transparency could help reduce the compliance costs of money transmitting services," argues Franco.Franco talks about "trust" when comparing the operations of cryptocurrency holdings to the way assets are held by banks. He refers to practices such as fractional reserve banking, where the bank holds only a small percentage of the money deposited and lends the rest back into the financial system."Although nothing prevents an institution from practising fractional reserve banking with bitcoins, it is not clear that users would favour such an institution," he says.Bitcoin exchanges that might have carried on fractional reserve banking are the sorts of companies that users should not trust. Regarding a cryptocurrency lender of last resort, an advantage would be "keeping the monetary authority honest".Bitcoin ATMs will probably fall under same level of regulatory compliance as money transmitters, and might require banking relationships, he states. The obvious future application of these would be using bitcoins to buy currency in foreign countries and therefore avoiding the charges/fees associated with travellers cheques.Part Two: Bitcoin TechnologyRelatedEncryption, ransomware, iPhone hacks and nation-state attacks: Cyber-security predictions for 2015Franco states in his preface that certain of the technical sections of the book can be safely skipped by those who are not attempting to implement the Bitcoin protocol. In any case, he should be praised for his clear and concise explanation of cryptography, which is the subject of the first chapter in the book's technical analysis, despite his admission that "a single chapter does not do justice to the subject, and the treatment here is necessarily shallow and incomplete".He starts by looking at public key encryption: using an algorithm to generate a mathematically linked public-private keypair. Public keys are exchanged and used to encrypt messages, which can only be decrypted by the person holding the private key. A bitcoin wallet is simply a collection of private keys used to sign transactions with the bitcoin ledger, which holds a record of the

amount of funds available to each address.Bitcoin wallets generally offer additional encryption of the private keys they hold, and the wallet itself can be distributed across several devices so that accessing the funds would require cooperation between the devices.Storing private keys offline is also highly recommended. Despite the complexity of cryptographic security, the safest approach in many respects remains the "paper wallet" i.e. printing out bitcoin addresses and private keys on paper and hiding them somewhere safe. Franco makes the point that offline storage on disk or USB can corrupt over time so back them up. Losing the keys generally means you lose the bitcoins.The blockchain technology is an amalgam of cryptography techniques. It borrowed proof-of-work function from Hashcash, which was introduced to curb spam on email, and combined it with linked time-stamping to arrive at a way of securing the distributed database. Franco analyses the useful pieces of technology that are combined to create the blockchain's innovation, and also traces each component back to its "cypherpunk" roots in the 1990s.To prevent two transactions from spending the same funds, the protocol decides that the valid transaction is the one that is time-stamped on the blockchain first. The transaction is further secured as more blocks are piled on top of it. This elegantly adds additional layers of security, backed by the combined computing power of the network.To alter a transaction, an attacker would have to re-mine a given block all the way back to the blockchain head, keeping pace with the rate of new blocks being added by the network. The only sure way to alter the blockchain therefore would be to control over half the total computing power of the network. Thus Bitcoin represents an ever expanding apotheosis of encrypted security.Part Three: The Cryptocurrencies LandscapeHere Franco traces bitcoin's origins back to early experiments in public key cryptography and blind signatures, as set out in documents such as the "Cryto Anarchist Manifesto" (May 1992).He charts a course through innovations such as David Chaum's ecash, an untraceable payment system first mooted in 1982; Adam Back's Hashcash, which ingeniously added computational time and costs to spammers; through to the first published papers by Satoshi Nakamoto in 2008. This was followed by the launch of the bitcoin peer-to-peer network on January 3, 2009.There is survey of some alt-coins that have proposed interesting changes, either technical or to the economics of bitcoin.Litecoin (2011) uses a different proof of work algorithm to bitcoin and its block generation time of 2.5 minutes is shorter. Peercoin (2012) uses a hybrid proof-of-work/proof-of-stake system that requires less computing power, making it arguably a green alternative to bitcoin. Auroracoin (Feb 2014), was 50% pre-mined, so that half its monetary supply could be distributed among the population of Iceland.Alt-coins, which are forks in bitcoin's open source code, can now be created on dedicated websites with just a few mouse clicks, notes Franco.A section on the future applications looks at smart contracts that could in some cases substitute the legal governance: "interactions that today are governed by law could be governed in the future by digital contracts and cryptoledgers".The most commonly cited example of smart property is the car. In this case the car's ownership is represented by a digital asset in the blockchain. The telematics system of the car is connected to the internet and can read the blockchain. It sees that a change of ownership has occurred and updates the public key of its owner accordingly. The new owner can open the car and start the engine by signing a message with his or her private key. This can be sent to the car via a wallet application in a smartphone.More complex transactions are explored: the car could grant an address access for a limited period, say for a rental, or the car could update payment by instalments.Other emerging bitcoin applications include digital bonds or digital shares; the next generation of micropayments and crowd-funding; autonomous agents that can operate Decentralised Autonomous Corporations and so on.We are living though a technological revolution. Who knows what applications will dominate a decade from now? Bitcoin founder Satoshi's predictions made in 2009 are already looking very modest: "I would be surprised if 10 years from now we're not using electronic currency in some way..."Understanding Bitcoin is published by academic research heavyweights Wiley in 2015.5 of 8 people found the following review helpful. IF ONLY THE AUTHOR'S GRASP OF MONEY AND BANKING WERE EQUAL TO HIS UNDERSTANDING OF TECHNOLOGY!By Garrett A. HughesThis is the first book I've encountered that appears to cover the technology of Bitcoin in sufficient detail to make it comprehensible. However, like many other technology enthusiasts writing on the same subject, this author's grasp of money and banking appears to be sorely lacking. (Despite his rather impressive credentials in the financial markets. He should know better.) In the Prologue he states (in an hypothetical conversation) that "Currencies have value because of social convention... Neither euros, dollars, nor Bitcoin are backed by anything." Nothing could be further from the truth (excepting Bitcoin). The author is equating goods and services with a "symbol" for debt - not the debt itself. The fact that someone, somewhere owes you goods and services is a matter of record. It just so happens that euros, dollars, bonds, letters of credit, and more importantly bank account statements make up the records. The records are kept by banks, subject to regulation, whose job it is to keep these records, and more importantly to vet the people who wish to create debt. The records themselves have no inherent value. It is important to make this distinction from the get-go, else this whole business gets off on the wrong foot.Art has value because of social convention (and the society is quite small). Money, on the other hand, has value because it represents the goods and services associated with a particular denomination of money. Money, by definition, is simply debt. Debt has value because it represents readily available goods and services. It is the potential value of those goods and services that give money its value. This is not the whim of a few individuals: this is food, clothing, shelter, protection, etc., to a large number of people who create and own the debt. One can misconstrue the value of these goods and services and call them a basis of

social convention, but that is a long stretch.To correctly value money in terms of the goods and services it represents, is a problem that is solved by markets - the foreign exchange market in particular. Around the world, the debt of sovereign nations is made available in the form of their currency - dollars, euros, kroner, francs... whatever. It's all "money" (debt). Now we get to the important part of valuing money. The value that markets attribute to money depends on perceived notions of the goods and services that the owner of the debt can acquire, relative to the amount of "comparable" goods and service that could be acquired by holding debt in another currency. For example: the euro recently lost value relative to the dollar. One of the reasons (besides speculation and fear) is that the quality and quantity of goods and services that one could acquire by trading a dollar was perceived be greater (and more stable) than that of a euro.At the heart and soul of money is the IOU. Let's see, I need to borrow your plow for a couple of weeks, but at the end of the summer I'll give you 50 bushels of grain in return. Here's my IOU (contract) to that effect. The owner of the IOU is now free to trade his 50 bushels of "promised" grain for a new shed to be built next his barn, and the IOU (the debt, the money) passes into other hands. It just so happens that IOUs have been standardized in the modern world (ancient, as well, as marks on clay tablets) as money in the form of dollars, euros, etc., but the value inherent in those forms will still depend on the quality and quantity of the goods and services that can be acquired by trading that debt.One of the reasons the Eurozone is in such financial turmoil, is that there exists a disparity in the quality and quantity of goods and services that can be acquired in different regions. Just think of the difference in hotel accommodations from one country to the next and you can see my point. Without naming names, if the hotel accommodations in two countries "cost" the same, but the the actual accommodations are much better in one than in the other, then the value of the euro in these two regions is mismatched. So how is the euro then valued overall? Its value is diminished by the disparity, especially if the "buyer" doesn't know a priori what they will be getting when they make the trade of debt - euros - for goods and services.In summary, the value of money depends on the the perceived and generally accepted value of the goods and services that we can acquire with the debt instruments we own. And even within regions using the same currency, large disparities in value can occur. But in the regions in which we live, we bear with this turmoil because it is the best game in town. Now, along comes Bitcoin. It has no goods or services associated with it from any region of the world. Bitcoin is worthless because it is impossible to value it in terms of the goods and services it represents. Until the entire world adopts the same monetary and banking system, and until the entire population of the world is able to exchange comparable goods and services, Bitcoin will be impossible to value. And I have not even begun a discussion of how complex the technology is to make it work. That is the subject of this book. It appears that the author's faith in technology exceeds his faith in markets. Now that is really scary.BTW: I bought this book from . The fact that it is a verified purchase is not showing at the top of the review. That just reinforces my skeptical view of technology in an area as sensitive to error as money. OK - only after I added this last statement to my review did the "verified purchase" statement appear. I guess that's what you call "floating recognition." It's like paying your credit card bill on Friday, and not having it credited until Monday. Now of course any financial transaction today can be verified in milliseconds - yet, the delay still exists: call it banking tradition. Do you suppose Bitcoin transactions can be held up to favor the creditor?2 of 2 people found the following review helpful. Five StarsBy Leisure ReaderWell written

Discover Bitcoin, the cryptocurrency that has the finance world buzzing Bitcoin is arguably one of the biggest developments in finance since the advent of fiat currency. With Understanding Bitcoin, expert author Pedro Franco provides finance professionals with a complete technical guide and resource to the cryptography, engineering and economic development of Bitcoin and other cryptocurrencies. This comprehensive, yet accessible work fully explores the supporting economic realities and technological advances of Bitcoin, and presents positive and negative arguments from various economic schools regarding its continued viability. This authoritative text provides a step-by-step description of how Bitcoin works, starting with public key cryptography and moving on to explain transaction processing, the blockchain and mining technologies. This vital resource reviews Bitcoin from the broader perspective of digital currencies and explores historical attempts at cryptographic currencies. Bitcoin is, after all, not just a digital currency; it's a modern approach to the secure transfer of value using cryptography. This book is a detailed guide to what it is, how it works, and how it just may jumpstart a change in the way digital value changes hands. Understand how Bitcoin works, and the technology behind it Delve into the economics of Bitcoin, and its impact on the financial industry Discover alt-coins and other available cryptocurrencies Explore the ideas behind Bitcoin 2.0 technologies Learn transaction protocols, micropayment channels, atomic cross-chain trading, and more Bitcoin challenges the basic assumption under which the current financial system rests: that currencies are issued by central governments, and their supply is managed by central banks. To fully understand this revolutionary technology, Understanding Bitcoin is a uniquely complete, reader-friendly guide.

From the Inside FlapBitcoin is a revolutionary digital currency that is arousing great interest within the financial industry. Presenting a modern approach to the secure transfer of value using cryptography, this currency also challenges the basic assumptions on which the current global financial system rests. Understanding Bitcoin gives

financial professionals a comprehensive resource and technical guide to the cryptography, engineering and economic development of Bitcoin and other cryptocurrencies.Written by Pedro Franco, this accessible text explores the supporting economic realities and technological advances of the currency, and presents positive and negative arguments from various economic schools regarding its viability. The author includes a step-by-step description of how Bitcoin works, starting with public key cryptography. He goes on to explain how transactions are processed, exploring the blockchain and reviewing how the wallet and mining technologies are structured. This vital resource reviews Bitcoin from the broader perspective of digital currencies and explores historical attempts at cryptographic currencies, all the way through to innovative applications such as decentralized exchanges or autonomous agents. Understanding Bitcoin explores the ongoing tension between those who want to break Bitcoin's privacy by using data mining techniques and those dedicated to creating technologies that will increase its effectiveness. This technical and accessible guide offers a clear understanding of Bitcoin as a monetary phenomenon with dramatic implications for monetary policy.From the Back CoverPraise for Understanding Bitcoin "This book is a one stop source for much-needed information about cryptocurrencies. Finally a single resource for everyone who wants to understand Bitcoin, the technologies it is based on and it's whole surrounding ecosystem. No more googling around and going through wikis and forums." mdash;Pavol "stick" Rusnak, Core developer of TREZOR "Bitcoin is a large domain encompassing many diverse areas of expertise. Franco's Understanding Bitcoin: Cryptography, Engineering and Economics is a welcome endeavour which provides a coherent picture of the framework. His book is a timely reference guide for a hot, quickly evolving, crucially relevant subject." mdash;Prof. Ferdinando M. Ametrano, QuantLib, Hayek Money, Milan Bicocca University, Banca IMI IntesaSanpaolo "Anyone interested in electronic payments will treasure this book for its depth and breadth, as it covers a very wide range of topics ranging from cryptography to software engineering to monetary economics. Pedro has created a comprehensive and very accessible introduction to the world of cryptocurrencies, which is very fun to read." mdash;Jan Pelzl, Author of Understanding Cryptography "Bitcoin is a challenging subject for most people to wrap their heads around. Understanding Bitcoin: Cryptography, Engineering and Economics offers a simple and understandable glimpse into the world of bitcoin that anyone can follow. The book not only explores Bitcoin's potential to transform commerce, but also it's potential to reshape the Internet itself. It's a must read for anyone looking to learn about Bitcoin." mdash;Stephen Pair, BitPay co-founder and CEOAbout the AuthorPEDRO FRANCO holds an MSc in Electrical Engineering from ICAI, a BSc in Economics and an MBA from INSEAD. He has been a consultant with McKinsey and Boston Consulting Group, as well as a researcher with IIT, prior to gaining more than 10 years of experience in financial markets, holding Quant and Trading positions in Credit, Counterparty Risk, Inflation and Interest Rates. He has created various mathematical libraries for financial derivatives, and managed teams of software developers. He can be contacted at pfrancobtc@gmail.com.