Demystifying Crypto
From Bookkeeping, Ledgers, to Blockchain

Jang-Vijay Singh

Singhpora Consulting

Abstract

The meteoric rise of the price of bitcoin, and its accompanying wild fluctuations, has piqued the interest of many investors and speculators. Cryptocurrency has often been hyped as a gold-like replacement for fiat currencies by virtue of its "finite" supply. There have been many publicised stories of the early stage "miners" who "solved puzzles" (as they put it) on their computers to "mine" bitcoin early on, who then went on to cash-out with spectacular windfalls. The underlying "blockchain" technology and proposed applications designed to be built "on the blockchain" also received much attention and, reportedly, investor funding. This paper will first attempt to clarify these terms, explain some of their working based on the author's research, and then examine these claims. It will attempt to answer a simple question: where does the actual "value" for a unit of crypto come from? This should help both potential investors and users of applications based on these concepts to make more informed decisions.

Contents

List of Figures

1 The Evolution of Distributed Ledger Technology

How is “value” attached to a unit of something - be it “one dollar” or “one gold coin”, or “one share” of Apple Corporation? What is behind the price of a Bitcoin? And finally, what is the biggest value addition from its underlying technology called *blockchain*, and how is it an evolution of existing concepts like ledgers. We examine all this by first exploring some basic concepts around value and money, examine how distributed ledger technology evolves from existing concepts, and how it adds value.

1.1 Introduction

People have their views on why they consider something to be of value. For instance, the value of one dollar for the buyer in a transaction could be attached to the amount of bread it can be exchanged for, and for the seller in the same transaction, the value of the same dollar could be in another commodity that the seller might exchange it for. There is a lot of subjectivity involved in this. For simplicity, we consider a unit of currency or money to be a “primitive” similar to natural numbers. The natural number five is a five, and represents five discrete, countable things in the real world.

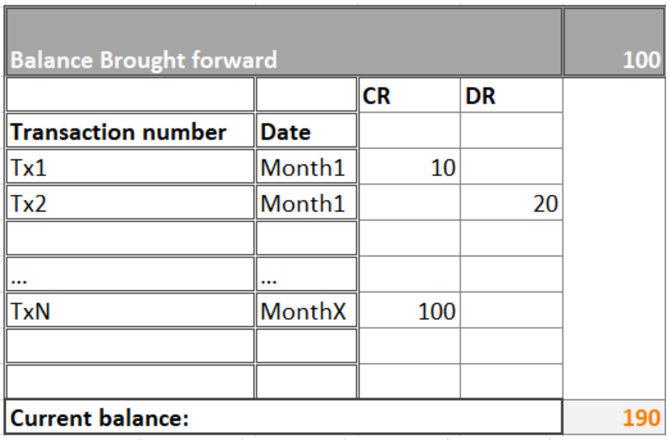
Starting from this abstraction, we are able to determine the “value” of one share of Apple Corporation somewhat more meaningfully in terms of a monetary amount. Apple Corporation owns a number of assets, like intellectual property, factories, research laboratories, liquid funds to run its operations, and much more. These assets by themselves have a value. Apple Corporation, as a going concern, makes use of these assets to produce and sell gadgets at a profit. A combination of its past record of profitability, and profits expected in future, determine the overall value of Apple Corporation. An investor who owns one share owns a fraction of this value and also a proportional share of its yearly profits. This value may or may not be reflected in the “price” of Apple stock. As with the price of any asset or commodity, price at any given time is less deterministic than value, as it can fluctuate with supply, demand, sentiment, and perceived value under different circumstances.

Unlike a share in a corporation, a unit of money performs a few other important functions: it can be used as a medium of exchange, and in some contexts, also an asset (if, say, it is invested to earn interest or profit). But, on its own, the value of currency, unless invested, is considered to deteriorate over time, as a result of inflation, as overall supply of money can increase with no known upper limit. Concepts like fractal reserve banking, debt, stimulus, and quantitative easing explain why.

To serve its function as a medium of exchange for any non-trivial purposes, use of currency is associated with an activity commonly known as “bookkeeping”. Individuals, corporations, and governments, are able to operate with money by being able to track transactions involving the transfer of money. Banks require reliable and trustworthy details of each transaction, so that they can tell their depositors precisely how much balance each account has. Regulatory requirements mandate this for corporations, which also need this record to determine if they have enough cash to meet their operational expenses, to analyse what their money is being spent on, and to ascertain if they are actually able to turn a profit. From this discussion, we arrive at these two concepts: a unit of value that can be owned, stored, or transferred in exchange for something, and the record of its transfer from one party to another. These two concepts are "money", and "bookkeeping".

1.2 Principles and History of Ledgers and Bookkeeping

Complex organisations and applications can operate efficiently when they are supported by ledgers - trustworthy, ordered, and immutable or at least tamper-evident record of their financial transactions. Before exploring the sophisticated concepts from this area that are in vogue today, we need to understand the idea of ledgers and then "distributed ledgers" from its basics. A ledger (like an accounting ledger or what is often simply known as 'book'[1] in a 'bookkeeping' practice) is a collection of sequential records, typically monetary records, that starts with a certain initial value (such as initial money in a bank account or even zero). Over an agreed period, such as a financial year or even a day, various transactions either credit to or debit from the base amount. Books are said to "balance", when certain conditions are met. The most important condition is that the final balance in a bank account at the end of the period must match the sum of all credit and debit transactions. Any spurious credit or debit entry, and any missing entry, would cause a mismatch and be easily detectable, as intended. We could represent a simplified book of accounts for a business as a set of dated entries that either credit to or debit from the "current balance" (fig. 1.1). A real book of accounts would be far more complex. A balance sheet for even a small business would account for all its receivables, record values of any physical items or assets it owns, debit their depreciation, taxes and much more. Each transaction is entered consecutively and dated. Verifying totals requires tedious manual effort and focus. This is a very oversimplified view to help us understand what features and functionality present systems aim to achieve. Historically, such accounts were for centuries maintained on thick bound paper based books, or sheep skin and clay tablets, before paper was invented [Harford, 2017]. The bound ledger books with consecutive entries would involve painstaking



Balance Brought forward				100
		CR	DR	
Transaction number	Date			
Tx1	Month1	10		
Tx2	Month1		20	
...	...			
TxN	MonthX	100		
Current balance:				190

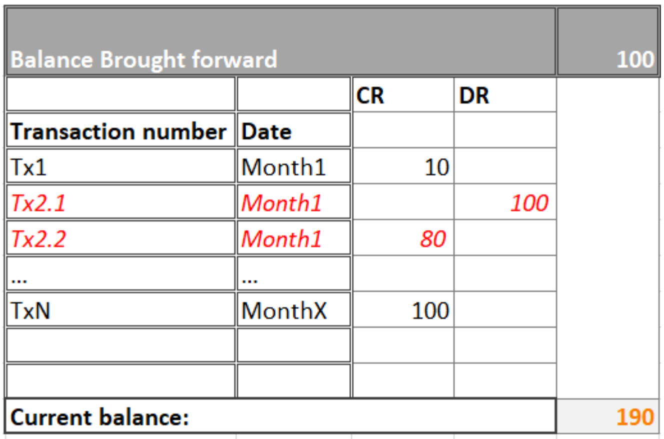
Figure 1.1: A simple book of accounts

[1] In accounting and project management software, it is common to find terms like book of accounts. In popular media, accounting scandals are often described as "clever accountants" fudging or "cooking" the "books"

effort in “balancing” books or auditing, especially if this required checking historical records or detecting errors. There could be various motivations for a malicious attempt to tamper with such accounting record. Not recording an entry altogether might have been possible in the past and harder to detect. Making fraudulent entries could be another one with the motive of siphoning off funds. In modern times, the Enron accounting scandal was essentially perpetuated by fraudulent accounting practices and possible tampering of accounts. Such frauds were not undetectable by audits but the detection could be made harder by sophisticated tampering and collusion. The basic principle of “double-entry bookkeeping” has been used since middle ages to account for money and materials, with sophisticated accounting and audit methods developed with time to detect theft or prevent “disguise” of theft of sensitive material like nuclear material [Lim and Huebel, 1979]. The goal of double-entry bookkeeping in all these use-cases remains:

> *...to ensure accuracy and integrity of records, the accounts are balanced... so that the fundamental account equations of* assets = liabilities *and* credits = debits *are satisfied. Any imbalance causes a* ***book balance discrepancy****... [Lim and Huebel, 1979]*

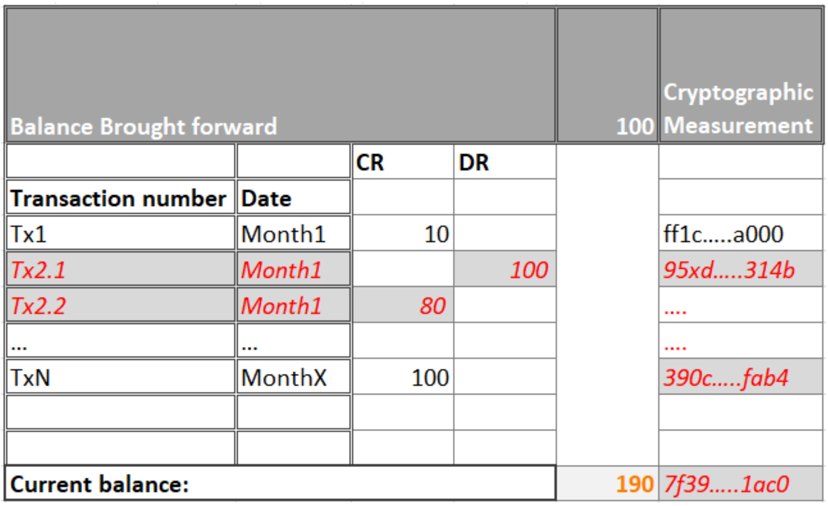
Although the previous example works as intended, it is not tamper-evident, as a *combination* of credit or debit transactions could obfuscate tampering without impacting the overall total. For an adversary, this tactic could be used to tamper with records in a way that can avoid detection by ensuring that the malicious entries do not cause a book-balance discrepancy. The simplistic example in figure 1.2 may or may not cause actual harm, but shows an example of a tampered book of accounts which can be a serious matter. If we were to treat “current balance” as “state” of the ledger, for any given period, we ought to be able to replay the set of credits and debits on an initial “balance brought forward” figure, and arrive at the same figure every time for every date including intermediate dates. In a tampered ledger, this might be possible for the overall period, but not for *all* intermediate dates.



Balance Brought forward				100
		CR	DR	
Transaction number	**Date**			
Tx1	Month1	10		
Tx2.1	*Month1*		*100*	
Tx2.2	*Month1*	*80*		
...	...			
TxN	MonthX	100		
Current balance:				190

Figure 1.2: A tampered accounting book without book balance discrepancy

If, however, all individual entries were to be stored alongside a unique cryptographic measurement (a hash), and, each subsequent entry in the ledger was a hash of the previous hash, current entry, and some unique temporal values like timestamp and nonce, then, the ledger would be more tamper evident. This would make each entry not just a standalone numeric value, but also based on a unique calculation that links it to every single chain of preceding values like a chain. Although what figure 1.3 depicts can only be implemented realistically



Balance Brought forward				100	Cryptographic Measurement
		CR	DR		
Transaction number	Date				
Tx1	Month1	10			ff1c.....a000
Tx2.1	*Month1*		*100*		*95xd.....314b*
Tx2.2	*Month1*	*80*			....
...	...				....
TxN	MonthX	100			*390c.....fab4*
Current balance:				190	*7f39.....1ac0*

Figure 1.3: A simple tamper-evident ledger

as a digital ledger, attempts to secure the integrity and even confidentiality of physical ledgers can also be found in history. A patent (US954791A) from year 1909, for instance, describes a device to physically secure the contents of a ledger to avoid inspection and tampering.

1.3 Distributed Ledgers

In the previous section, we explored the theory behind how a simple ledger could be tampered with, and how linking each record with every previous record can deter tampering. In this section, we explore how this can be implemented digitally, and why multiple *distributed* copies of the ledger make this even more tamper-evident. In physical ledgers, attackers could use different methods in a malicious attempt to tamper with old entries - erasing previous writing, or replacing a whole sheet of paper with one that includes tampered entries. Digital records without safeguards can even make tampering easier, as in practice, simple digital records don't have the limitations or natural tamper-evidence of physical ink and paper.
As a means to increase ledger integrity, if instead of one, multiple identical copies of sensitive ledgers were maintained, this could make tampering harder, though not impossible if the book-keepers happen to collude with one another and with the adversary. Yet another level of complexity could be introduced by geographically separating the ledgers and somehow making it impossible for them to communicate with one another except with a limited set of information:

- Contents of the new transaction (CR/DB x from current state) to be applied to the ledger and,
- The new value of the ledger.

A transaction could be said to get *confirmed* if all these hypothetical (and somewhat improbable) bookkeepers could agree on the new value via a previously agreed protocol (consensus?) for deciding what the current value total of the ledger is. Even if some of the bookkeepers become corrupt or make a mistake, the protocol could be defined to still work with a certain percentage of tolerance for corrupt book-keepers.

What if the ledger and its contents were all public? Surely, any tampering could be detectable if the precise state of the ledger was part of public memory and therefore, any tampering would immediately be detected. Such a system would work with various assumptions:

- That all members of the public or a significant subset of them would be *interested* in doing this or "someone" might incentivise them to do so
- The general public or those who participate in this system are *capable* of doing this accurately and precisely. This would need a high degree of skill and commitment, as we could be dealing with financial accounts, and even other complex transactions or transaction chains like in land records/transfers, corporate share issuance/ownership/transfers (to potentially help prevent cases like sale excess shares of Bear Stearns [Nofer et al., 2017]), or even maintaining inventory of nuclear material [Lim and Huebel, 1979].
  If not 100% capable, at least there should exist some way of determining what most (or most credible) record keepers have to say about the state of the current balance after the application of a transaction
- The records can be made public or at least, the public version of the records can be provably tamper-evident without disclosing content that is intended to be private (one would assume the ledger for nuclear material inventory is highly confidential)

Because of the complexity needed to meet these conditions for both physical and digital ledgers, we note that there is not a completely fool-proof and practical means of ensuring ledger integrity manually. But this is the nature of conditions that the distributed ledger technology enabled by blockchain networks meets.

Without blockchain technology, the conditions described above are not met merely with a digital ledger - perhaps the complexity and magnitude of the problem is compounded without additional safeguards. Digital records could on the one hand introduce additional checks and balances to improve *integrity* and *confidentiality* - audit entries, timestamps, authenticated access and so forth. Redundancy and disaster recovery combined with data replication are standard Software Engineering techniques that are used widely to improve the availability of sensitive data such as important ledgers.

Digital records offer certain advantages: Many auditing mechanisms can be made easier or fully automated. Computer programs are exceptionally good and fast at it, and once developed, they can run over and over again - facilitating both record-keeping and compliance. There are sophisticated and functionally complex business systems that offer this functionality today at large scale. On the technical side, measurements (hashes) of system backups have been a tested means of ensuring system integrity used by systems administrators or database administrators.

All these means still do not offer sufficient (mathematically provable?) fool-proofing against malicious tampering. Two or more redundant copies of a key database are still vulnerable if their administrators (book-keepers) collude to change details that favour an adversary. Timestamps, audit records, everything could be altered in a sophisticated attack. Numerous techniques are employed to enhance properties like availability, consistency, integrity, transaction speed/throughput/response time of data persistence systems (databases), many of which rely on distribution of the system across multiple network nodes. These mechanisms involve tradeoffs between consistency, availability, and partition tolerance, (the CAP theorem [Stonebraker, 2010]), leading some Big Data systems to describe themselves as achieving *"eventual consis-*

tency”.

1.4 Distributed Ledgers on Blockchain

To understand how distributed ledgers implemented on blockchain protocol offer us the desirable properties of immutability and tamper-evidence better than paper or digital ledgers, we go back to the list of assumptions in the previous section. Each *node*, i.e. a computing device, participating in the network is like a book-keeper. Its job is to *confirm* transactions by constantly calculating the measurement of each transaction in combination with a measurement of *all previous transactions*. This process is called *mining*, but this is done by multiple, globally distributed nodes simultaneously, with the goal of arriving at the *same* new *state* for the ledger after the transaction is applied. The final value or state of the ledger is the state confirmed by multiple nodes independently, and each transaction (in reality a block of transactions) is *linked* to each previous transaction (block), forming a chain of blocks, or the *blockchain*. With no centralised control (except for the protocol with which nodes communicate with one another), and no way of determining which nodes actually confirm transactions, collusion is impossible. Tampering of past records is also infeasible because that would mean an inconsistent state in the ledger. [Bashir, 2017] is a good reference to understand the working of blockchain in deeply.

Coming back to our simple account book of figure 1.2, we note that a slight alteration in the sequence or number of entries led to an undetectable change in the ledger (in this simplistic example, the total figure remained unchanged but the spurious transactions could have caused damage - they could represent an illegal loan or asset transaction for which profits were siphoned away). This isn’t an impossible problem to detect via an honest audit (or even prevent when all the bookkeepers are honest) - but we work with the assumptions that the system needs to continue working with reliable results when some of these actors (nodes), and it could be any of them, turns corrupt. This problem is formally described as the Byzantine General’s problem. The pioneering blockchain based system, the Bitcoin distributed ledger in 2009 was the first to apply a *“Practical Byzantine Fault Tolerance”* algorithm called *“Proof of work”* [Bashir, 2017] as a mechanism to achieve consensus. Transaction throughput and scalability has always been difficult to achieve, with different variants of distributed ledger consensus algorithms achieving different results in terms of throughput while retaining the essential design goal of being a decentralised linked list of blocks of transactions. At this point, it is worth adding that the concept of *smart contracts* also gained hype recently. For why this was highly premature, the reader can refer to [DuPont, 2017], as the present article only attempts to share a simplified understanding of the evolution of distributed ledger technology, and how it led to the development of cryptocurrencies.

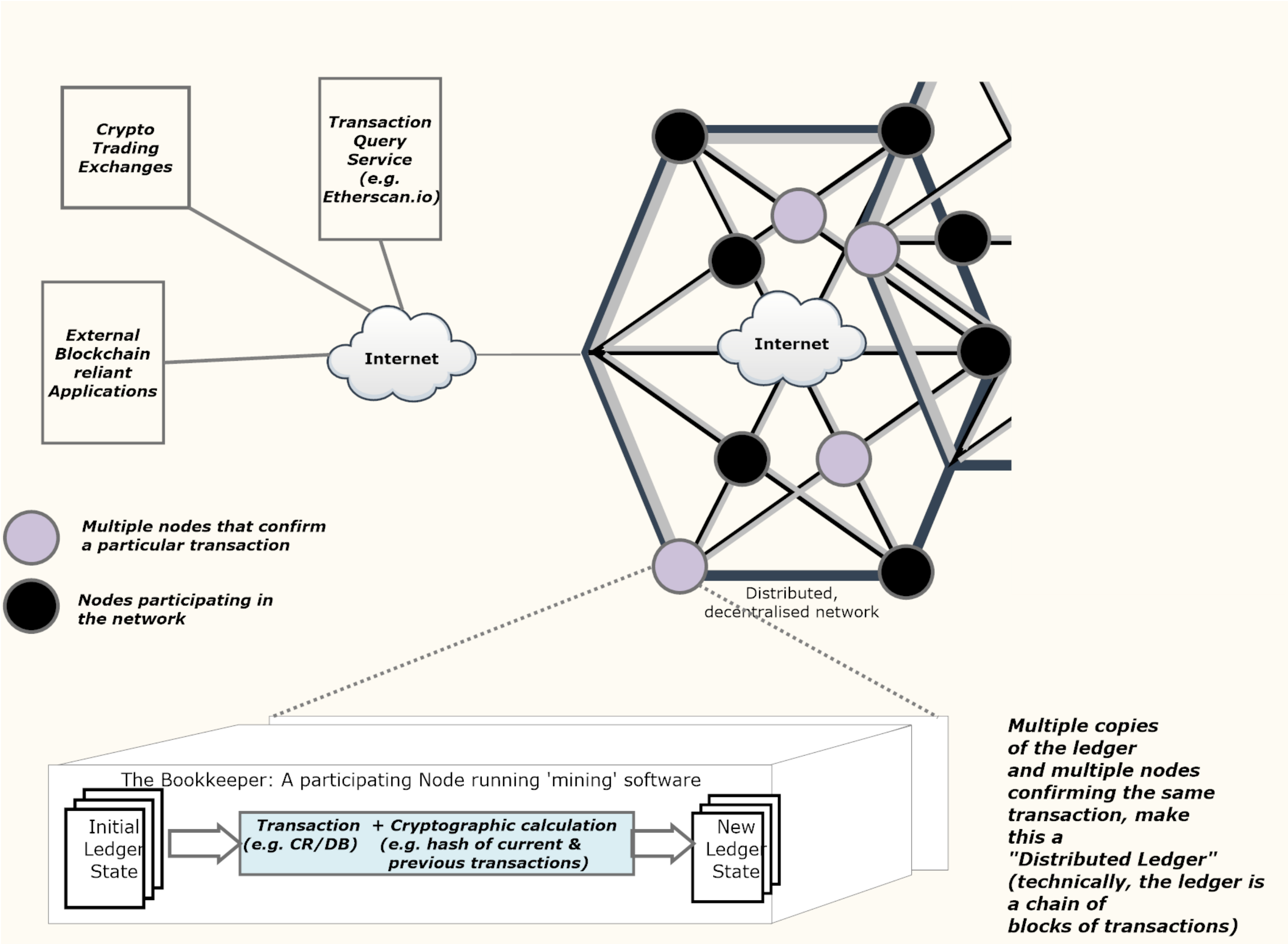

Crypto Trading Exchanges
Transaction Query Service (e.g. Etherscan.io)
External Blockchain reliant Applications
Internet
Internet
Multiple nodes that confirm a particular transaction
Nodes participating in the network
Distributed, decentralised network
The Bookkeeper: A participating Node running 'mining' software
Initial Ledger State
Transaction (e.g. CR/DB)
+ Cryptographic calculation (e.g. hash of current & previous transactions)
New Ledger State
Multiple copies of the ledger and multiple nodes confirming the same transaction, make this a "Distributed Ledger" (technically, the ledger is a chain of blocks of transactions)

Figure 1.4: Depiction of a blockchain network, depicting how a Distributed Ledger is maintained

2 Concluding Notes

We understood that the terms in vogue today, actually have a long history behind them. The two concepts: *money* and double-entry *bookkeeping*, that facilitate much of today's economic system, both have centuries of history. Cryptocurrencies and blockchains of today do *not* reinvent these concepts, but they do offer a new technological paradigm, and demonstrable value addition with immutability and automatic tamper-evidence. More importantly, as explained in sections 1.2 and 1.3, digital distributed ledgers offer a step evolution from traditional forms of physical and digital record-keeping.

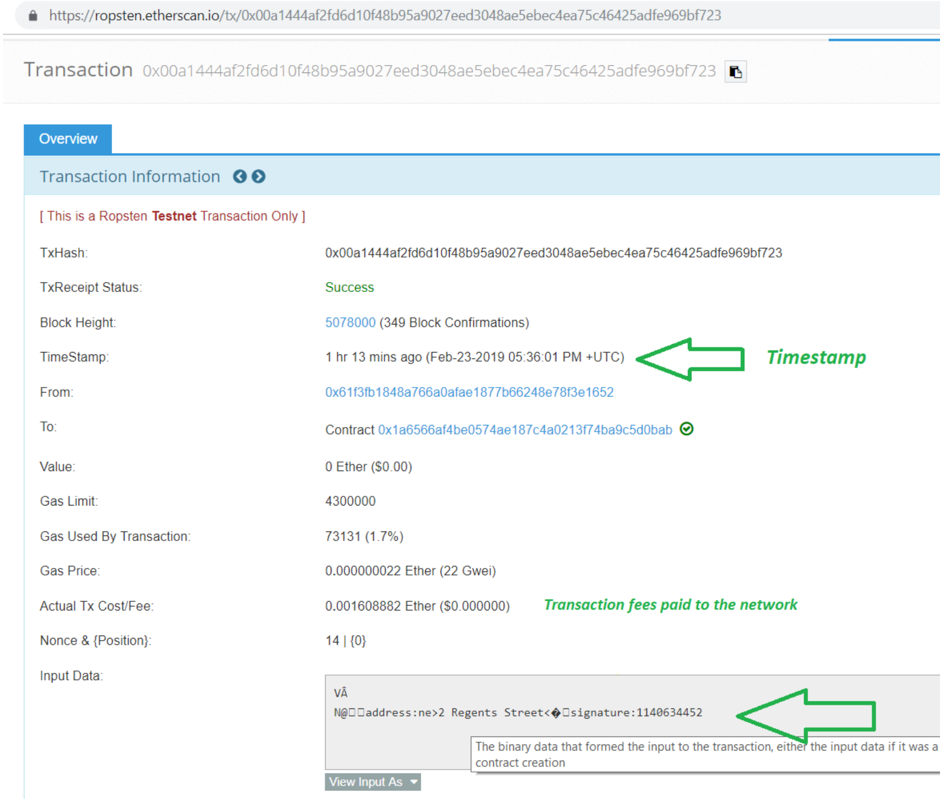
2.1 The Making of Money

A unit of traditional money comes into being as a result of debt. This means, when a government issues debt bonds, its central bank quite literally *creates* an equivalent amount of money that it expects to be repaid with interest (Till early twentieth century, a certain amount of gold had to be deposited with the central bank, but this criteria was removed decades ago to fuel post-war growth). The money thus borrowed or created, is used to fund various government expenses, indirectly supports profit-making enterprise that in turn leads to expansion of the economy or value creation, finally allowing the debt to be paid back with interest. Governments and monetary systems also need to strike a good balance. If they borrow or create too much money, that could lead to uncontrolled inflation or loss of value of the currency. To quote from Sveriges Riksbank's website [Sveriges-Riksbank, 2017]:

> *"The Riksbank is Sweden's central bank. We ensure that money retains its value and that payments can be made safely and efficiently. We also issue banknotes and coins."*

Unlike traditional currency, units of cryptocurrency like Bitcoin and Ethereum, come into being when a node, a computer participating in a blockchain network, successfully confirms a transaction and is paid a certain amount of cryptocoin for it by the network. This is the point when the new amount is said to be created or *mined*, and the first transfer is made to the *wallet* of the node(s) that did the work. This payment is coded into the network software that runs the blockchain network, and has an upper limit that varies by the blockchain network. This is why cryptocoins are advertised as being finite in quantity, like gold, but unlike fiat currencies. Confirming transactions, or more precisely, calculating hashes of blocks in combination with previous blocks so they are linked, is the whole job of participating nodes. This requires work performed by using computing power. More objectively, it requires electricity to run these nodes, and other costs involved like the capital overlay in purchasing and setting them up, and operational costs like maintenance, Internet connectivity, and so forth..

Actual users and applications who rely on these networks for their ledger functionality to record their transactions, or to simply use their crypto-coins as a mode of payment (which also involves recording transactions), are then meant to pay a fee for each transaction (see figure 2.1). The price or transaction fees that users pay to use these networks, therefore, need to at least cover the transaction confirmation costs. The fees involved here have no bearing on the prices of cryptocoins that we see in the headlines and the purpose of this article is not to comment on whether it is fair, but to try and understand if a more deterministic correlation between their price and value is even possible.



https://ropsten.etherscan.io/tx/0x00a1444af2fd6d10f48b95a9027eed3048ae5ebec4ea75c46425adfe969bf723

Transaction 0x00a1444af2fd6d10f48b95a9027eed3048ae5ebec4ea75c46425adfe969bf723

Transaction Information

[This is a Ropsten **Testnet** Transaction Only]

TxHash:	0x00a1444af2fd6d10f48b95a9027eed3048ae5ebec4ea75c46425adfe969bf723	
TxReceipt Status:	Success	
Block Height:	5078000 (349 Block Confirmations)	
TimeStamp:	1 hr 13 mins ago (Feb-23-2019 05:36:01 PM +UTC)	*Timestamp*
From:	0x61f3fb1848a766a0afae1877b66248e78f3e1652	
To:	Contract 0x1a6566af4be0574ae187c4a0213f74ba9c5d0bab ✓	
Value:	0 Ether ($0.00)	
Gas Limit:	4300000	
Gas Used By Transaction:	73131 (1.7%)	
Gas Price:	0.000000022 Ether (22 Gwei)	
Actual Tx Cost/Fee:	0.001608882 Ether ($0.000000)	*Transaction fees paid to the network*
Nonce & {Position}:	14 | {0}	
Input Data:		

```
VÂ
N@□□address:ne>2 Regents Street<�□signature:1140634452
```

The binary data that formed the input to the transaction, either the input data if it was a contract creation

Figure 2.1: A transaction confirmed on a testbed blockchain network showing the transaction fee charged

2.2 Cryptocoin is Speculation, not Investment

A person or entity that owns a certain number of crypto-coins, could use it directly as a mode of payment where feasible, but could sell it in exchange for traditional currency. The question here is, how much traditional money is worth paying for one Bitcoin or Ethereum 'coin'. Clearly, there has been a tangible cost incurred in generating it in the first place, and there is some value in it serving as a medium of exchange of value that should determine its true value. The property of it being in finite supply might seem appealing, but there is not much barrier to new blockchain networks spring up and issueing their own crypto-coins. The very low traction and prices of newer cryptocoins might just be the equivalent of inflation, but without a central bank doing anything about it. This might not be the case in future, if one or two blockchain networks and their associated cryptocoins becomes de-facto payment standards on online payment gateways or retail points of sales *and* transaction confirmation times and fees on blockchain networks can match or better traditional payment systems. For this, major challenges around transaction costs and processing times would need to be solved first, and this would be a heavy impediment in their mainstream use as methods of payment. From this, we can conclude that for the foreseeable future, crypto-currencies appear to be targets of heavy speculation, inflated hype, rather than meaningful investments. Furthermore, like traditional currency, it is important to distinguish between their role as medium of exchange, store of value, or as an asset class by themselves. It is more likely that in the near future, electronic versions of traditional currencies like the Swedish E-Krona [Sveriges-Riksbank, 2017] might have a more viable future as an incremental next step.

Bibliography

[Bashir, 2017] Bashir, I. (2017). *Mastering Blockchain*. Packt Publishing Ltd.

[DuPont, 2017] DuPont, Q. (2017). Experiments in algorithmic governance: A history and ethnography of the dao, a failed decentralized autonomous organization. In *Bitcoin and Beyond*, pages 157–177. Routledge.

[Harford, 2017] Harford, T. (2017). How the world's first accountants counted on cuneiform (bbc world service). `https://www.bbc.co.uk/news/business-39870485`. [Online; accessed 08-Jun-2020].

[Lim and Huebel, 1979] Lim, J. and Huebel, J. (1979). Tempering of accounts and records to disguise snm theft. Technical report, California Univ., Livermore (USA). Lawrence Livermore Lab.

[Nofer et al., 2017] Nofer, M., Gomber, P., Hinz, O., and Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, 59(3):183–187.

[Stonebraker, 2010] Stonebraker, M. (2010). Errors in database systems, eventual consistency, and the cap theorem. *Communications of the ACM, BLOG@ ACM*.

[Sveriges-Riksbank, 2017] Sveriges-Riksbank (2017). E-krona. `https://www.riksbank.se/en-gb/payments--cash/e-krona/`. [Online; accessed 08-Jun-2020].