SECOND EDITION

BEYOND BITCOIN

THE FUTURE OF DIGITAL CURRENCY

SEAN WORTHINGTON, PhD ABD

BEYOND BITCOIN

the future of digital currency

by

Sean Worthington

Published by

CloudCoin Consortium

Contents

Envision a new future...

Imagine, if you will, a future where there will be no banks—except the banks on your cell phones and computers.

There will be no tellers, vaults, loan officers, or buildings to house them. Accountants will become a profession of the past as software takes care of all of your accounting and banking.

Tax systems will all but disappear—no one will pay taxes. Only taxes on land and homes will be possible.

People will be able to trade by verbally passing codes, and store their money in their minds, where it cannot be seized or detected.

Governments will go into decline as they are forced to limit their income to fees, bonds, and donations.

Politicians who once got elected by delivering largess to their supporters will be out of business.

You will receive your income by email, text message, and website download, and it will go directly into the bank on your desktop.

This bank will pay your bills automatically, on the dates you specify, by sending emails to those you wish to pay.

Your banking software will also automatically send any unused money (via email) directly to investment pools where you can withdraw it in seconds should the need arise. These investment pools will give you a chance to earn a respectable interest on your savings, and allow the great inventions of the future to be funded.

Funds like these will also provide home and auto loans, all without the government—or anyone else—knowing about it. These pools will be controlled by anonymous people located all around the world. These pools will be run by virtual organizations and will be part of a growing nation known as the Cloud People.

You will be able to buy anything from anyone in the world using your computer. All laws dealing with customs and tariffs will all be ignored and useless. Virtual global organizations made up of people unhindered by bureaucracy will flourish.

The CEO of a multi-billion dollar company may be completely anonymous and work out of his home office.

Labor laws will be futile.

But who will make sure things are done fairly and without fraud?

It won't be governments. Free market institutions will form to fill this niche.

When someone in the future is convicted of a crime, the information will be available to anyone in the world and criminals will be shunned.

Theft of money will disappear. People will be able to store their money in their minds. They will be able to retrieve their money at any time by combining their biometric information with the passwords they have memorized.

Is this future possible?

Defining a monetary system

Any monetary system is an information system.

Such a system helps us economize*, and economy is vital to our survival.

The most important part of any monetary system is the human mind. If people don't have the math skills to be able to understand prices and costs, or to judge how much money they have in order to plan and budget, then monetary systems simply will not work.

Monetary systems allow us to make decisions regarding how we will coordinate and optimize our actions.

Money is data.

Data must be accurate if it's going to give us insight into the true state of things. With accurate data, we can make educated decisions. In computer science, data is true when it has integrity.

There are two major types of data integrity, physical and logical, and these apply to money as well.

Money tells us how we should act, where we should work, what we should buy, and what we should make and sell.

---

* *The word* economy *originally referred to the management of a household. It later evolved to suggest a wise use of resources and avoidance of waste.*

Without money, our populations would not be able to grow beyond 150 people—about as many people as a barter system can support. Money allows millions of us to work together, each providing value to society.

Without money, civilizations would collapse. Without money, most of us would literally starve to death.

Money is the data we use to coordinate all activities.

Good money means good coordination, which I call **emergence**. Bad money means **submergence**. You may have heard the term emergence in other fields of study.

Life emerges from trillions of lifeless atoms and molecules by using DNA. Consciousness emerges from billions of neurons by using connections. An economy emerges from millions of humans by the use of money.

Entropy tears down and disorganizes. But with money, we can build things up. With a perfect money, we could reach unimaginable levels of prosperity. Without money, or with a bad money system, our economy dies—and we die with it.

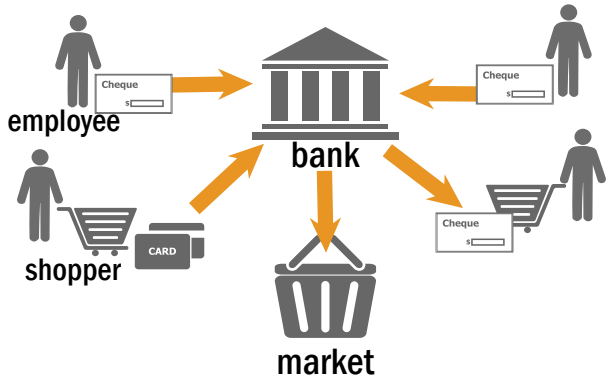
Knowing what a monetary system is and knowing its purpose, we can start to design the perfect money by understanding what makes perfect data and a perfect information system. We simply apply the rules used in information systems and computer science to a monetary system and to its units of money.

Societies can have two major types of currency:

- **Money based on centralized data**, such as Bitcoin or the stone money used on the island of Yap, or

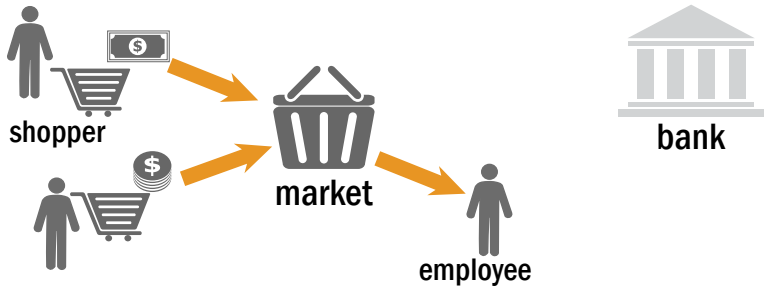
- **Money that is decentralized**—like most modern money, including cash, gold (historically), silver, and most recently, the CloudCoin™.

CENTRALIZED MONEY SYSTEM



With a centralized money system, it's easy to track all of your transactions through ledger records.

DECENTRALIZED SYSTEM



A decentralized system provides privacy for your transactions.

Centralized currencies require a public ledger or central village square to display money. Decentralized money is spread out in everyone's pockets. In centralized money, most administrative

efforts go to managing transactions, and the transactions must be public.

With decentralized money, transactions can be private, and most of the administrative costs go toward preventing counterfeiting.

CloudCoin™

I have invented the first counterfeit detection system that fully allows for a decentralized digital currency. I call this counterfeit detection system **RAIDA***, and I call the currency **CloudCoin**.

In this book, I will explain why we *must* be interested in digital currencies. I will cover the problems that digital currencies face.

And I will tell you how these problems have been solved by this new counterfeit detection system, and how RAIDA technology has been used to create CloudCoin.

There are nightmare possibilities in our future right now, but we don't have to go there. We now have what I know is a clear path to securing our liberty so that these nightmares never come true.

* *Redundant Array of Independent Detection Agents*

The promise of digital currencies

We now stand at a portal that has been opened by digital currencies, and are only just beginning to understand the profound consequences of the technology of digital currency.

Money commands us all.

It tells us which job is our most efficient work by rewarding us with the highest salary for taking it. It tells us which products are most efficiently produced by giving us a price.

Money can organize our civilization and allow us to economize. Without money, society would fall apart.

However, money can lie. Money can be used against us. It can be used to steal from us.

Digital currencies like Bitcoin have become today's hot topic as people make millions off their meteoric rise in value.

Digital currencies allow us to trade with anyone in the world. It's like spending cash directly from our own computers.

In theory, there are no banking fees and no worries about identity theft. You have privacy, and your money is protected from any government's inflating currency.

When Bitcoin came out, most of us didn't buy any. We didn't get involved. And we missed the significance of this technology.

It's time to wake up!

Money calls us, and we would be fools not to listen. For now there is something new.

It's not the blockchain, but RAIDA. It's not Bitcoin, but CloudCoin. And it is something new, something that solves those problems inherent in a digital currency.

Bitcoin is an amazing technology, but CloudCoin will change everything. And this time we are not going to miss the opportunity.

More specifically, *you* should not miss this opportunity.

A new future expanded

Let's take a look through that portal into the future and see what the world might look like with digital currencies.

In the past, the people who physically had the money owned it. But in the future, the people who know the money will own it.

Charities will rise to take the place of government social programs and safety nets, and will do a much better job. The power and influence of governments will wane. The capacity of a government to maintain standing armies and fight wars will also cease to exist.

You will be able to make financial decisions, including owning stocks and bonds, without anyone knowing you own them.

You will be able to gamble, buy prescription drugs—without a prescription—take a taxi that is not a taxi, stay in secret hotels, or see a doctor who is not a doctor.

Government regulations will become unenforceable.

Federal Reserve Notes and other government-based currencies will go bust. Their value will slowly drain until they are worthless pieces of paper. In the end, they will be overrun by counterfeits as the cost of counterfeiting goes down and the cost of policing goes up.

The new digital currencies will be privately administered and much more efficient.

We will see more economic equality among people as the rich and poor who once milked the system no longer have a system to milk.

All people will work harder. All people will make better decisions. All people will economize and become more efficient.

The end result is that a new economy will emerge, along with a new class of citizens who will be powerful and able to control the governments so that those who wish to stay in power will not try to infringe on the money rights of others.

Constitutional rights will be restored.

Women who wish to stay home with their children will be able to afford to do so again, as they will no longer be required to work to prop up the military and state apparatus. There will be less marital strife and fewer divorces, and more equality between the sexes.

There will be a move from the cities to the country as people will no longer need the services that cities once provided. They will not need cubicles, banks, or retail stores, and they will not need to be in close proximity to others.

Everything administrative will be done digitally, online, and people will want to get away from the crowds, traffic, stress, prices, pollution, and crime.

The prosperous will move from the cities and the poor will flock to them because the cities will become like today's Detroit: inexpensive to live in. This will cause the cities to become even more undesirable and dangerous places to live until the cities become nothing but large squatter communities.

When the value of the dollar collapses, manufacturing will return to the cities of America because minimum wage laws will no longer be relevant, and the unused space, along with a labor force that's ready to work, will bring manufacturing to a local level. Incomes around the globe will begin to equalize.

In the future, insurance companies will make a huge comeback—but they will all be virtual and unauthorized by governments. Instead of having one medical insurance company to choose from, you will have thousands. They will provide real insurance as opposed to trying (unsuccessfully) to manage a government program like today's insurance companies are forced to do.

The cost of healthcare will plummet as people become insured for real problems. The ill and injured will have access to doctors, medicines and treatments from all over the world—all virtually over the Internet, and all paid for with digital money.

A new theory of money will be taught in the economics departments to supplant the teaching of Keynes, Marx and Socialism. Instead, economists will turn to information systems theory.

Economics will no longer be a subjective behavioral science; it will be a hard science—and the importance of unfettered money will be very clear.

Homeschooling will become the norm as school districts force the kids into their homes to save money, and place the responsibility of education directly on the shoulders of the parents. This will result in children who are better educated. Colleges and universities, faced with the demand to reduce budgets, will cut gender studies, environmental studies and ethnic studies instead

of cutting computer science, biology and nursing. The campuses will become much more conservative.

In the future, the number of people working as government regulators will drop off because they will be paid with worthless Federal Reserve dollars instead of a digital money that maintains its value.

Terrorists, unfortunately, will be able to send money anywhere in the world. The only way to stop them will be to physically isolate them.

Child porn and many other crimes will persist, but the overall welfare of children and people in general will increase as the new monetary systems bring about a new prosperity. Instead of going after the money, law enforcement will go after the criminals who use the money. There will be significantly more resources to stop them, thanks to the charities that are now able to fund private detectives, private courts, and private punishments.

In the future, digital currencies will improve everything and make nothing worse.

As a species, we will become more intelligent and less violent, with greater harmony among the races.

As individuals, we will become happier and more satisfied with life. We will have much less tolerance for tyranny and a greater sense of community.

The theory of a perfect money

While I have heard theories of "ideal" money, to my knowledge, mine is the first theory of **perfect money**.

And while I wrote it, the truth is that the ideas have been lifted from the theories of good database design practices developed in the field of information systems. I honestly believe this theory should be placed in every Economics 101 text book.

Monetary systems have a job, and money has a specific role within monetary systems. **The job of the monetary system is to track what value an individual adds to the economy and ensure that more value is received than is put in.**

If a monetary system does not do this, then it is unjust and people will "defect" from using it .They may use it if forced to, but they will avoid it if they are able.

With the invention of digital currencies such as CloudCoin, many more people will be able to enjoy high-integrity monetary systems as they defect from the fiat currencies that governments and banking cartels offer.

What a perfect money would offer

The perfect monetary system would be **run by system administrators**, not bankers, governments or even computer scientists. This is because monetary systems are information

systems, and have little to do with banking, government or computers.

The perfect money has **perfect integrity**. This integrity can be classified under three headings:

- Physical integrity
- Logical integrity
- Preferential integrity

Integrity

In practice, physical integrity means:

- No counterfeits
- No loss
- No theft
- No possibility of system-wide failure

Logical integrity addresses:

- Users must know who the money belongs to (entity integrity).
- The money must all be of the same stuff (domain integrity).
- The money must refer to something that is actually there (referential integrity)

With preferential integrity, the system must:

- Be private
- Be scalable
- Be fast to transact

- Use whole numbers (or at least fractions that are easy to understand)
- Have high availability (no downtime)

Physical integrity

A monetary system must allow people to prove to others that they added value to the monetary system, and that they deserve to get some back. If a person gets money through counterfeiting or theft, or by taxing, they are able to prove something that is not true.

Data and money must be true. That is what integrity is about.

And if the system becomes unavailable (fails), then no one can know the truth. That must not happen in a monetary system.

Money has to be there to do the job. If the money just disappeared, we would not have a monetary system. If some of the money disappeared, then it may still be usable but flawed. The money must not disappear, must not be able to be destroyed, lost or unreadable, and must not appear out of nowhere to be perfect.

Loss

As of this writing, over 17 million Bitcoins have been mined, and over 4 million of them have been permanently lost.

What happens when the losses exceed the coins mined? The monetary system dies.

The major problem with loss is that it fails to accurately reward people who created value. You may not think of this as a big problem until it happens to you.

Anyone can lose money, but it is unfair when it happens. In a perfect monetary system, it is impossible to lose money.

Theft

Some currencies are more susceptible to theft than others. The cryptocurrencies are probably the most susceptible because of their private keys that control the money in the accounts. We can dramatically reduce theft of most currencies by simply not putting all our eggs in one basket—by reducing the systematic risk. I could go into great detail about this, but I am now in the process of making CloudCoin unstealable even with quantum computers. In a perfect monetary system, there should be no theft.

Shutdowns

In the 1990s, people in California put their gold together in one vault, then issued digital currency against it. They did billions of dollars worth of trade using this e-Gold. But then some state government bureaucracy decided to kick down the doors and take the vault and all the gold. The system did not have physical integrity.

If your currency can be shut down, then it does not have physical integrity and it will not last. Bitcoin was the first digital currency to achieve this physical integrity, but it will not last for long. Quantum computers will put an end to this and other cryptocurrencies.

The cloud can be made quantum-safe. A perfect monetary system is always available, and works right every time.

System risk

There are two types of risk: **systemic** (the risk of collapse of an entire financial system or market) and **unsystematic** (risk contained within a single company or industry).

Digital currencies must be able to eliminate all systemic risk. CloudCoin has done this.

Logical integrity

There are many parts to logical integrity. The first is entity integrity.

Entity integrity means that each money must belong to an entity.

This also assumes that an entity must be able to prove that ownership. Money without an owner is lost, and loss is not allowed in a perfect monetary system. Entity integrity is only an issue when it comes to transferring ownership. In a perfect monetary system, ownership is clear.

Another part is **domain integrity**. This means that all the money must fall within the same "domain." Systems based on silver, copper, gold and nickel coins do not have domain integrity. They are all made of different stuff (domains), and this stuff does not have the same value.

Even systems that mix paper money and coins lack domain integrity.

It is possible that the metal in the coins could be worth more than the numbers printed on them and much more than the numbers printed on the paper.

Digital currencies generally do not suffer from lack of domain integrity. In a perfect monetary system, the money is all cut from the same material—it belongs to the same domain.

Regarding **referential integrity**: Often with money, the data is written on something with physical properties that reflect the value.

For example, a dollar was originally defined as the modern-day equivalent of 24.057 grams of less-than-pure silver, so with a silver coin that's labeled as a dollar, you would expect that coin to contain 24.057 grams of silver.

However, you can write the word "dollar" on anything, including pieces of toilet paper. If we accept the original definition of a dollar, then put the word "dollar" on paper and that money loses all referential integrity.

If we change the meaning of "dollar" to a monetary unit used by the Federal Reserve Bank, then we get the referential integrity back.

We have seen referential money like the U.S. silver certificates, which are no longer in circulation. These pieces of paper referred to an ounce of silver that was supposed to be safely vaulted away. The problem was that it was not true—the silver certificates did not possess referential integrity.

There are now many digital currencies, such as Tether*, that claim referential integrity by binding to a currency such as the U.S. dollar. But, as history has shown, monetary systems that work on referential integrity always fail sooner or later. In other words, if you invest long in referential money, you will lose your ass.

Perfect money has 100% referential integrity. This means that it says what it is and there is no doubt as to what it is. A CloudCoin is 100% a CloudCoin. Bitcoin also enjoys 100% referential integrity.

---

* *Tether is a blockchain cryptocurrency that is backed one-to-one, by fiat currencies.*

Preferential integrity

It may be possible for a monetary system to keep all of its data straight, and to track who added what and who should get what out. But there are other important things that must be addressed.

What people *prefer* might not fall under the strict science of data, but these are also important. One aspect of this is **privacy.**

Imagine that when you went to buy something it was posted on Facebook so that everyone could see everything you bought and where you bought it.

Imagine getting lectured by your boss, coworkers, family members and even your kids on what to buy and what not to buy, where to shop and where not to shop.

The better the privacy, the better decisions we make, the more we economize, the more civilized we become. If you have to sign up for an account to use your money, it's not private.

You can obtain a pseudo privacy with cryptocurrencies, but if someone finds your private key, they can prove how much money you have and all the trades you have made.

Real 100% privacy means no accounts, no logins, no passwords, no private keys and none of the other things that publicly attaches you to the money you own.

Scalability means that a system does not slow down when more people use it. Think of cars on a bridge. The bridge is not scalable—the more traffic it gets, the slower the traffic moves.

The world is looking for a global currency that can handle the entire world's trades. It would be a crushing blow to get invested

in a currency that stops working because everyone else wants to use it too. But that is what happened to Bitcoin and Etherium.

Blockchains in general are just not scalable. I would even suggest that if you are using a currency that claims to be blockchain-based *and* scalable, it is either not really blockchain or not really scalable, because the two don't match.

Perfect money is scalable.

Speed of transactions is also very relevant. During the height of the Bitcoin bubble, it took an average of 20 hours for a transaction to complete. That is not going to work for someone who wants to buy a soda at the corner store. People don't care if it is 500 milliseconds or 250 milliseconds, but the slower you get, the more people will complain. I assume that anything over 20 seconds is dead when it comes to retail.

Perfect money trades fast.

The **fractions** a coin can break down to is also a vital point.

The most important part of a monetary system is the human mind. We need to be able to think about what the numbers mean to us. We have to know how much we have, how much we need, and how to plan our spending. Thinking in whole numbers may be easier than mixing whole numbers and fractions. It is easer to think of 5 CloudCoins than 5.6789958443 Bitcoins.

What level of precision (number of decimals) does a monetary system need to be accurate? That, I admit, I do not know. But I am putting my money (CloudCoins) on whole numbers.

In terms of preference, a perfect money should be **easy to use**. It should always be available, transact at any time, and have high portability.

A perfect money must meet the preferences of its users.

———

This is the first time in history that my theory of "perfect money" has been published. I left this out of the first edition of this book to allow CloudCoin to have an advantage over other currencies, but I will be very interested to see how these arguments stand the test of time.

Will I receive the Nobel prize in economics? Or will I be diagnosed with mania and grandiose delusions? Maybe both!

Blockchain vs. RAIDA

The table below will give you a better idea of how to measure their fundamental values.

Feature	Crypto Currency / Blockchain	Cloud Currency / RAIDA
Spending Speed	Spending takes 40 minutes or more to update public ledger and confirm.	Takes milliseconds to check authenticity.
Theft	Can be stolen.	100% safe if encrypted. Theft can be stopped if owner updates the RAIDA before the thief.
Loss	Loss is permanent.	Loss can be recovered.
Counterfeits	Can be mined.	Number of CloudCoins does not increase or decrease.
Privacy	Pseudo-anonymous.	100% anonymous.
Software Required	Requires exchange for purchase and wallet for storage.	A single user-friendly interface.
Time to get started	Takes over 24 hours to download blockchain.	No downloads required.

Feature	Crypto Currency / Blockchain	Cloud Currency / RAIDA
Public ledger of all transactions	Uses public ledger available to the entire world, including KGB, CIA, China, etc.	No public ledger or centralized database.
Safe from quantum hacks	Bitcoin is not quantum safe.	Yes! Totally quantum safe.
Importable	Bitcoin cannot be imported into video games or other apps.	CloudCoin is the only real currency that can be imported/exported with other software, including video games.
Fractions	Bitcoin uses insane fractions like .000002	CloudCoin uses only integer denominations (whole numbers, like customary money). It doubles if it becomes too valuable to scale to user's needs. Comes in denominations of 1, 5, 25, 100 and 250 CloudCoin units.
Environmental Impact	Bitcoin requires millions of dollars in electricity.	CloudCoins use very little electricity.
Bottom line	First decentralized eCurrency.	Next-generation decentralized eCurrency .

Comparing integrity in different money systems

The next table shows how CloudCoin stands up against other familiar monies:

	Gold	Bitcoin	CloudCoin	Fed notes
Physical integrity				
Can the currency be counterfeited (mined)?	Y	Y	N	Y
If it can be counterfeited or mined, can the counterfeits be made at a fast rate?	N	N	N	Y
Can the currency be permanently and easily lost?	Y	Y	N	Y
Is the infrastructure self-funded, meaning that it does not require fees? [1] *Requires billions in taxes*	Y	N	Y	N[1]
Can the cost of the infrastructure exceed the revenues needed to support it?	N	Y	N	Y
Does it require more bandwidth, storage space, processing power and electricity than other comparable options?	Y	Y	N	Y
Is the currency quantum-safe?	Y	N	Y	Y
Is the truth of the coin dependent on consensus (consensus is not truth)?	N	Y	N	N
Can a government, hacker or natural disaster shut down the system?	N	N	N	N
Does the currency mix logic with data and expose risks? [2] *This would be yes for Etherium*	N	N[2]	N	N
Is it controlled by one entity that can be sued, taxed or closed?	N	N	N	Y
Is it scalable? Can it transact for the entire world's population?	Y	N	Y	Y
Logical (entity) integrity				
Can an owner of the currency demonstrate ownership without spending?	Y	Y	Y	Y
Is there a low systemic risk of theft, or can the risk of theft be distributed?	Y	N	Y	Y
Is there a low systemic risk of loss, or can the risk of loss be distributed?	Y	N	Y	Y

	Gold	Bitcoin	CloudCoin	Fed notes
Does one secret control the entire amount owned?	N	Y	N	N
Logical (domain) integrity				
Does the money use different mediums of storage (gold, silver, paper, copper, nickel, hard drive), or different units?	N	N	N	Y
Logical (referential) integrity				
Does the currency refer to something that may not be there (like a silver certificate refers to silver)? [3] *But it once did.*	N	N	N	N[3]
Logical (preferential) integrity				
Does it transact in less time than is humanly noticeable?	N	N	Y	Y
Can it transact at any time? Day night, holidays etc.	N	Y	Y	N
Can it transact over any distance (Globally)?	N	Y	Y	N
Does it use incomprehensible fractions?	N	Y	N	N
Does it require an account (100% private)?	N	Y	N	N
Are transactions recorded?	N	Y	N	N
Are transactions readable to the public?	N	Y	N	N
Is it highly liquid? Can it be quickly exchanged for goods, services and other currencies? [4] *Slow* [5] *Not yet*	N[4]	Y[4]	N[5]	Y

The Story of King O'Keefe

In the 1800s, an Irish-American captain sailed his ship to an island in the middle of the Pacific Ocean in search of copra.

What he found on the island of Yap was a form of money made of huge carved stones. The stones came from a nearby island, and had to be transported back to Yap. The islanders had no metal tools, so once they transported them, carving a single stone into the shape that represented money required massive amounts of the islanders' time.

But Captain O'Keefe had an idea. He sailed to the island that had the right type of stones, then using his iron tools, he carved the stones to mimic those of Yap. He took the stones back to Yap and asked if he could purchase one of the smaller islands with his stones. The islanders happily agreed to the trade.

Soon the captain was back for food, labor, shelter and more. The islanders saw this as a boon, so they quit farming and dedicated their time to building the sailor's home and furniture. They could always buy food later with the new stones they would earn.

But things did not work out well. With no farmers, the food ran out. With more money than products, their monetary system collapsed.

The villagers were dismayed at how the price of food skyrocketed. The children were hungry. The women complained to their husbands.

They all suspected that the sailors had something to do with it, and they all complained to the chief.

After much thought, the chief called everyone together and said, "Listen closely to what I'm about to say. You are cannibals. Follow your heritage. Eat the bastards!"

The problem with Bitcoin

The future that digital currency promises is grand, but there are big problems in the road to reaching the best possible future.

But first, what is a blockchain?

Blockchain defined

A blockchain is a database that is duplicated thousands of times across thousands of servers as it tracks transactions.

These transactions usually involve a specific cryptocurrency, although blockchains can also be used to track and secure other types of information.

Digital currencies like Bitcoin use blockchain technologies to provide what computer scientists call **physical integrity**—the manner in which data is physically stored.

This means the currency is secure, and won't disappear. And even governments can't touch it.

Or can they?

How safe is Bitcoin?

Supercomputers—known as quantum computers—are now being developed. These computers are just like your desktop computer, except they have 10 to the 8th power more processing capability. This means they are 100 million times more powerful. In theory, a

quantum computer could break a blockchain's 128-bit encryption in under two minutes. Quantum computers are just coming onto the market—but it's safe to assume that governments around the world already have them in secret. This means they can already secretly track cryptocurrencies.

But that's not the only problem. Cryptocurrencies use a system of **proof-of-work** and **consensus**.

Proof-of-work (PoW) is a way of verifying a Bitcoin (or other crypto) transaction. Consensus is a broad agreement among the people managing a cryptocurrency blockchain for the rules that PoW will follow.

In theory, the Chinese government could put up 6,000 servers and use their combined computing power to take over the Bitcoin blockchain. Significantly fewer servers would be needed if they were using quantum computers.

The blockchain uses **pseudo-anonymity**—an apparency of anonymity but not true anonymity—to track every transaction that occurs. If your name is linked to your **public ledger address**, anyone can find out everything you have ever bought or sold through that blockchain.

It can take days to set up an account on a blockchain, because the **exchanges** (sites where you can buy and sell cryptocurrencies) are very intent these days on verifying your identity before they'll let you set up an account. You may have tried to buy Bitcoin and given up; it's just too danged difficult.

But this isn't the end of the problems inherent with a cryptocurrency like Bitcoin.

How Bitcoin is “minted”

The entire Bitcoin blockchain is funded by “counterfeiters” who are euphemistically called **miners**.

When Bitcoins were first created, there were a finite number of coins. Miners are people who “solve” the mathematical problems (PoW) used to keep transactions secure, using powerful computers and specialized software. When a problem is solved, new coins are created and given to the first miner who solved the problem, but he doesn’t receive it until a number of other miners have come up with the same answer.

It takes huge amounts of costly electricity and tens of thousands of high-powered servers to run this Bitcoin blockchain. Bitcoin mining alone consumes as much electricity as an entire mid-size state, like Nebraska or New Mexico. Due to these costs, the system is becoming much more centralized. One missile to a single mining site in Iceland (where massive Bitcoin mining is done because of the low cost of power) could stop the whole transaction process.

Why Bitcoin transactions are slow

But the worst aspect of Bitcoin is that it takes minutes or hours to confirm a purchase, and soon it will take days. Imagine waiting days to buy a soda. Bitcoin is simply impossible for retail use.

The blockchain isn’t **scalable**. This means that the more people who use it, the slower it gets. The algorithm is doomed by its own success.

And now, companies are charging transaction fees, and the exchanges are becoming extensions of our governments.

Countries like Japan, Bahrain, and India are even setting up official government-run blockchain digital currencies.

Bitcoins are like the stone money found on the island of Yap. In Yap they have a village square where all the big stone coins are kept in a physical public ledger for everyone to see. There is a raised platform for each family. If your platform is empty, you are broke. The blockchain is a digital version of this public ledger system.

And yes, there is a better way.

Centralization

Remember that monetary systems are information systems. So when we talk about centralization, we could be talking about data centralization, or system administration centralization.

First, we'll look at **data centralization**.

In monetary systems, money is data. There are two major approaches to money as data—**ledger (centralized)**, or **physical tokens (decentralized)**.

Gold, silver, and paper money are all physical, token-based forms of money.

The electronic data used in CloudCoin also takes up storage space (as all stored data does), so CloudCoin uses the physical token model. With physical tokens, including CloudCoin, the money is dispersed across its users, and is extremely decentralized.

Bitcoin, PayPal, and the stone money of Yap use the ledger approach, and the data is centralized. Bitcoin and Yap use a public ledger to stop unauthorized transactions. PayPal has a private ledger, but still maintains a centralized record.

Stone money (photo by Eric Gunther)

In the case of Yap's stone currency, the money is all located in the village square. How many servers are required to run Bitcoin? In theory, just one. And everyone must have access to it, just like with the village square.

The fact that Bitcoin copies its public ledger to many servers has no real effect on the centralization of the data, but instead affects the centralization of its administration.

When we get to **centralized system administration**, things get a little more controversial.

Monetary systems need system administrators. That is why I say that the monetary systems of the future will be run by system administrators. In distributed-token systems like dollars or CloudCoin, the main administrative effort goes toward fighting counterfeits.

In public ledgers, there is less concern about counterfeits and more about **entity integrity** (knowing who owns what). On the island of Yap, they must move the stones from one place to another to show ownership, and they make sure no one moves stones without authorization. With Bitcoin, numbers must move from one account to the next to show ownership and prevent unauthorized moves.

The Federal Reserve System requires a significant amount of administration, primarily due to threat of counterfeits. Page after page of laws and international agreements have been drawn up to administer the fiat currency of any land.

Try to make a photocopy of any paper money in the world and you will see your copy machine do an odd thing. It has a little brain in it that recognizes when you are trying to copy money, and it will—on behalf of the Federal Reserve—stop making copies. This gives you a stark window into what you can expect if governments make their own digital currencies.

How can governments reach as far as controlling how copy machines and scanners work? Clearly, the Federal Reserve System is centrally administered—and they are doing a lot of it.

Centralization is dangerous, and we must fight against it.

In CloudCoin, we are also primarily concerned with detecting counterfeits. My invention, the patent-pending RAIDA technology, is the novel idea that makes this digital currency possible. RAIDA stands for Redundant Array of Independent Detection Agents.

Bitcoin does not have a central administrator, but it has a design flaw that results in the administration becoming more centralized as the value of Bitcoin goes up. The Bitcoin miners are the administrators, and as more people have access to Bitcoins, and more coins are generated, it takes more power to administrate the blockchain.

And so the number of administrators for Bitcoin is falling.

To be a Bitcoin administrator (or miner), you need to know how to run servers. You need to keep them running with the right software. Because of the economics of Bitcoin mining, we are seeing it become more expensive to mine (counterfeit) Bitcoins, and so the only miners are people who have an economic advantage.

There are now warehouses full of servers in Iceland. Iceland has a cold climate and cheap electricity, which makes it one of the best places on earth for mining. The truth is that there is only one "most efficient" Bitcoin administrator in the world. That is why Bitcoin's administration will naturally become more centralized as this currency becomes more popular.

And the more centralized it becomes, the more vulnerable it is to attacks, both physical and digital.

The second mover advantage

A **second mover advantage** is the advantage a company has when it’s not first to market.

Unlike Satoshi Nakamoto, who had no precedent, I could look at all the Bitcoin blockchain mistakes and find ways to avoid them. With the wisdom of hindsight, I was able to determine those things that do not work and remedy them.

Solving the physical integrity problem

The most important property of money is its physical integrity, and the most important part of that is its ability to avoid being counterfeited.

For something to be useful as money, it should either cost more to counterfeit than its value, or it should be impossible to counterfeit.

This is why we've used gold as money in the past. Gold was not used because it was valuable, but because gold coins are difficult to counterfeit. If you want to create a gold coin, you have to mine the gold. Gold mining is so difficult that it cost more than the money was worth.

The real value of money comes from its integrity as data.

Humans form a **superorganism*** that we call a society or an economy. This superorganism emerges through the use of money.

Because money is data, any data corruption will lead to the submersion of the economy. An example of data corruption is counterfeiting. **Submersion** refers to the economy becoming weaker and more disorganized.

Today we are seeing cryptocurrencies that cannot be counterfeited because of the encryption they use. In a good monetary accounting system, we do not want data (money)

* *A social unit with division of labor. Individuals are highly specialized and cannot survive on their own for extended periods of time.*

appearing out of nowhere, disappearing, or in any way becoming corrupted.

When corruption does happen, the monetary system becomes inaccurate, and will prevent people from making efficient decisions.

Imagine a person who shows up with a bag full of cash and offers to buy your house for what seems like a very good price. You sell the house.

As you drive off, you realize that the road is filled with cash, and there's a helicopter above dropping more.

People are picking it up in wheelbarrows. The bag of cash sitting next to you suddenly doesn't seem to be as valuable as it seemed a few minutes earlier.

Down the road, when you're ready to buy a new house, you discover that your bag of cash will no longer even cover a month's rent!

You made a very bad decision based on bad money. Now multiply this by millions of people.

Physical integrity of money

Let's compare the physical integrity of different types of money.

First let's imagine the worst type of money we could use.

Suppose we decided to use ice cubes for money.

It's obvious that this would be a terrible mistake because anyone with a freezer could add new money to the system, thus corrupting the accounting. Ice cubes would melt, causing

everyone's hard-earned money to disappear. In a short time, everyone would make poor decisions, and poverty would become the norm.

Now compare that to silver coins.

Silver coins make good data (money) because they add physical integrity to a monetary system. However, a monetary system based on silver coins is still not perfect. Although difficult, it is still, like gold, possible to counterfeit silver coins.

A case in point is the historic Spanish Price Revolution that occurred between 1470 and 1650 when silver began to pour into Europe from the New World. This caused a rampant inflation that lasted for over 100 years, with decidedly negative effects.

Wages lagged behind prices. Landowners and the rich—along with anyone with something to sell—benefited from this inflation. But for most people, the accounting system did not function properly. They made bad decisions and become poorer even though more silver was readily available.

What about paper money?

Paper money is difficult to counterfeit unless you are the central bank and own the printing presses. In this case, it is very easy to increase the supply.

As with silver during the Spanish Price Revolution, this helps the government, the rich, the landowners, and anyone with something to sell.

Paper money has much less physical integrity than a metal currency, and is far from a perfect money.

The integrity of Bitcoin

Now let's take a look at Bitcoin.

You may think that it's impossible to counterfeit Bitcoin. But, in fact, Bitcoin mining is counterfeiting. Counterfeiting is necessary to make bitcoins work because the operation of the servers that hold the public ledger depends on counterfeiting (mining) to pay for the system's administrators (miners).

It is also possible to lose Bitcoins. You may work very hard for your Bitcoins and then lose them. And sorry, but you will not be compensated for your lost value. That is not a feature of a good monetary system.

For Bitcoin to work, it is necessary to have a public ledger stored on someone's hard drive that is publicly accessible.

But what if someone accidentally deleted the public ledger? To prevent this from happening, the public ledger is mirrored (duplicated) on many computers, and anyone can download it and keep a copy of it on their own computer if they choose to. This gives Bitcoin physical integrity because storing duplicate versions of the data on separate computers protects it from loss.

But what if someone were to tamper with the information? They could change the row that represents the total amount of Bitcoin they own and make it bigger. This is where the blockchain comes in. To prevent corruption, every transaction is recorded and encrypted. These encrypted transactions are also encrypted, then added to a chain.

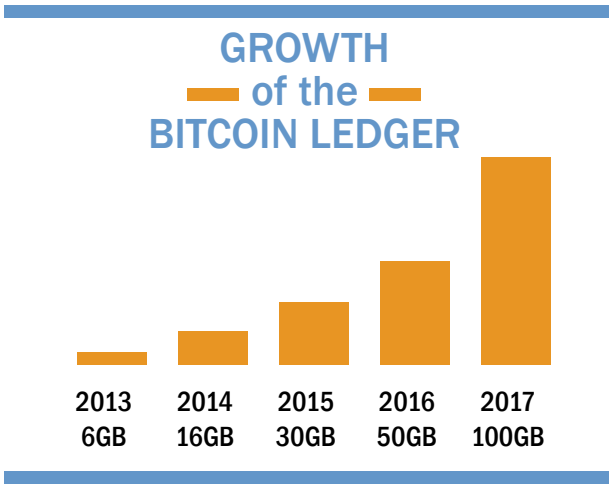
This system requires vast amounts of computer processing power and electricity to encrypt transactions, but it works and it allows for the funding of the physical infrastructure.

Even so, there is still some vulnerability to Bitcoin's physical integrity.

First, Bitcoin requires encryption, and is not quantum safe. When quantum computers become widely available, in a very short time, Bitcoin will become hackable—first by governments, then by common hackers. When this happens, Bitcoin is finished.

The second vulnerability is that the Bitcoin infrastructure is paid for by bitcoin miners. As time goes by, it is becoming harder and harder to make money mining Bitcoin, and this puts the entire infrastructure at risk as fewer people will be able to provide computers to store the public ledger.

Another issue with Bitcoin is that its ledger is growing. Right now, it is 100GB. Who knows, with more accounts and more transactions, we may see it grow to a terabyte in just a few years. If the blockchain is too big to fit on a hard drive, this threatens the physical integrity of the coins.



The space demands for storing the Bitcoin blockchain ledger are growing rapidly, and the ledger is becoming more unmanageable every year.

The best way to maintain physical integrity is by not depending on encryption alone, but by utilizing the newest technology: the Cloud.

RAIDA and integrity

I have taught networking and system administration for over seventeen years and, having finished all of the coursework for a doctoral degree, I am all but dissertation (ABD) for my PhD in Computer Information Systems.

I can imagine an endless collection of new privacy technologies that could change the world. But I don't want to write about them, I want to implement them.

I have a patent pending on a new cloud-based counterfeit detection system that I call the Redundant Array of Independent Detection Agents, or RAIDA. What is the easiest way to monetize this new technology? By creating a new currency. And that currency is called CloudCoin, because it is based on the cloud.

You are likely to see many more inventions from me in the future, but for now, let's review what RAIDA is.

RAIDA is a global counterfeit-detection system that is indestructible and cannot be hacked or tampered with. Nuclear bombs, comet strikes, world wars, dictatorships and government hackers cannot not bring down RAIDA.

RAIDA is quantum-safe, self-healing, simple, fast and reliable.

And RAIDA can detect the authenticity of a CloudCoin within milliseconds. That's right, milliseconds.

Trust

The essence of money is that it can't be counterfeited.

The purpose of money is to help us economize.

The value of money is based on its physical and logical integrity (trust).

CloudCoin takes our trust in a currency to the highest level yet.

Using the patent-pending RAIDA technologies (with a patent intended to keep just one cloud-based currency), independent system administrators from all around the world can leverage thousands of servers and networks to create an unbreakable system that no single entity or organization can dictate.

Note that the RAIDA does not create, store, transmit, track or broker CloudCoins or any other digital currency. The *only* function of a RAIDA cloud is to detect the authenticity of a CloudCoin.

Like a blockchain, RAIDA does not have a central administrator.

If I get hit by a bus, the RAIDA keeps going because it doesn't depend on an individual to run it.

I am sad to say that we had a RAIDA administration (Nick Burges) die during the proof-of-concept test. His death was a great loss to everyone—including CloudCoin. But his death did accomplish one thing that may have a lasting impact on humanity—it showed that the RAIDA technology works, and proved that it is fault tolerant.

Fault tolerance, by the way, is another concept from computer science. **Fault-tolerant computing is a key concept in systems design that ensures the system will continue working even in the presence of faults** in the hardware.

Not only is RAIDA fault tolerant, but, unlike blockchain technology, the more its popularity and value grow, the more decentralized it becomes. (A blockchain will always move toward becoming more centralized as the associated value goes up.)

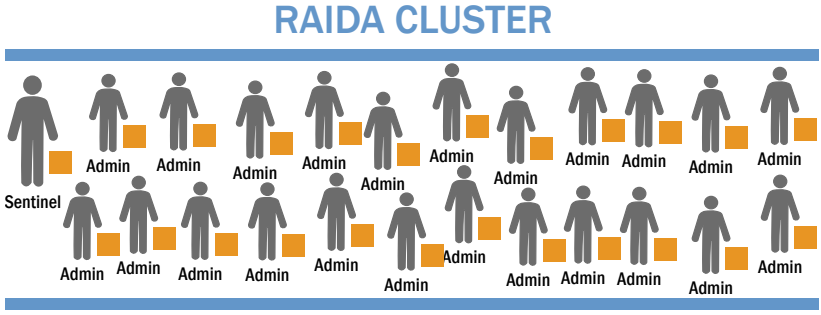
The CloudCoin™ structure

A **RAIDA network** is composed of 25 RAIDA clouds.

A single **RAIDA cloud** can have up to 32 administrators and one sentinel. The **sentinel** is responsible for making sure data stays true and available,

Each cloud is a **cluster**—a group of separate but connected or virtually connected data storage units.

A **node** is a single machine or group of machines in a cluster.



Each cluster has at least one sentinel, and not more than thirty-two admins. In each cluster, the sentinel is responsible for insuring data integrity.

The administrators need to be able to fund their operations. But, unlike Bitcoin, which requires rooms full of servers, the needs of RAIDA are minimal.

In the full 800-node configuration (up to thirty-two admins for each of the twenty-five clusters), each node (single admin) is in charge of only 21,000 CloudCoin notes. This means that

the admin only needs 25MB of database storage, a minimal processor, and very little network bandwidth. (Compare this memory usage to the size of the Bitcoin ledger in the previous chapter.)

The system requirements to support RAIDA are so minimal, in fact, that RAIDA can literally run on a Raspberry Pi*.

RAIDA node on a Raspberry Pi device on the left. Compare to a blockchain node on the right.

We have one RAIDA that has been running on a Raspberry Pi for months. These little servers are well under $100 each, and you can literally fit one in your pocket!

Unlike the Bitcoin network, it is entirely within the realm of possibility that the RAIDA could be run by volunteers. However, to ensure that there *is* money to pay the RAIDA admins, these admins are allowed to receive coins for discovering coins that have been otherwise permanently lost—one CloudCoin for every 25 found.

** A Rasberry Pi is a small, inexpensive computer developed for teaching computer science in schools, and for use in developing countries.*

RAIDA clouds

Each RAIDA network is composed of many redundant servers, networks and databases that are interconnected via the Internet. Such arrangements of hardware are often referred to as **clouds**.

The databases are mirrored in multiple physical locations, with multiple servers to keep the cloud readily available.

Multiple locations also allow for such **catastrophic failures** as a meteor strike by keeping the system operational, no matter what.

Governments may try to suppress RAIDA servers some day.

It is likely that in time RAIDA clouds would become a target for thousands of highly trained hackers from around the world.

It is also likely that RAIDA would be targeted for **Denial-of-Service (DoS) attacks*** by the worst attackers imaginable.

But with this structure, if some of the components fail or are attacked, the RAIDA system keeps going.

A self-healing system

A **fractured CloudCoin** is a CloudCoin that failed authenticity on one or more RAIDA nodes. These nodes can "compare notes," and in doing so, repair the fractured coin. This process is invisible to the coin owner.

* *A (DoS) attack is when hackers attempt to block legitimate users from accessing a service, usually by overloading the network or server with invalid communications.*

Expanding CloudCoin

When the value of CloudCoin goes up, the entire RAIDA can be cloned multiple times. Each time this happens, the whole system becomes even more fault tolerant than before. If the value were to go up the way Bitcoin has, I can imagine the system growing to 60,000 micro servers—and still remain completely free to use.

What this all means

RAIDA does everything that a blockchain does, only much faster, more reliably and far more efficiently.

The only thing RAIDA does not do that Bitcoin does is to track your transactions.

RAIDA is scalable. More nodes and networks can be brought on as needed to perform transactions within milliseconds. The work is distributed among more nodes rather than requiring each node to do more work (like blockchain).

Costs are paid through recovery of lost coins, so there are no transaction costs for the user. Every CloudCoin is owned by someone who knows its authenticity numbers (passwords).

However, if no one knows a CloudCoin's password, it is considered lost. We can identify these lost coins because they have not been re-authenticated in two years.

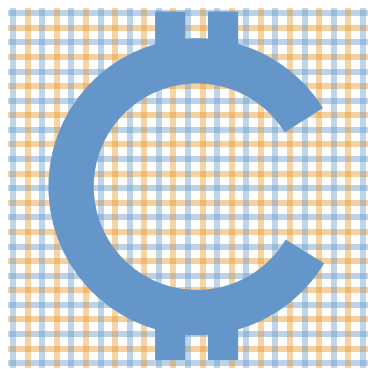
However, RAIDA itself is only a counterfeit detection system. The data for the money is stored within the CloudCoins themselves.

The world's first cloud currency

CloudCoin is designed to be the first perfect money. CloudCoin data is not stored on the network, only authenticated. The Cloudcoin owner stores the data, which means it has no central administration.

A **RAIDA network** is made up of 25 RAIDA clouds. A **RAIDA cloud** is a virtual network of up to **thirty-two administrators** and one **sentinel**. Each administrator has his or her own computer, or **server**, that does not share data with any of the other servers. A single server requires only 25 MB of storage space, which is very minimal.

The number of CloudCoins available in a network is fixed at 1,428,160,512 coins spread across 16,777,216 notes of varying denominations.



A CloudCoin sentinel verifies the authenticity of only a single stripe or shard in a coin. The other twenty-five stripes are verified by other sentinels.

Each CloudCoin has **400 bytes*** **of random numbers** embedded in it. These 400 bytes are divided into **25 stripes** and **25 shards**.

Each stripe is called an **AN** (**authenticity number**). Each shard represents the coin's **serial number**.

You can think of it as a table of information. The stripes represent columns of numbers, while the shards represent rows. The contents of these tables are spread across the RAIDA network. None of the information is centralized.

There are 1,428,160,512 coins total per network. This number was chosen to keep the value of CloudCoins low enough to make hacking unattractive.

The total number of CloudCoins in a single RAIDA network will never increase or decrease. However, if the value becomes too high, (more than the equivalent of $2.00 USD), CloudCoins can be split so that every coin then becomes more coins.

CloudCoins are designed so that splitting, doubling, or in any way multiplying CloudCoins also multiplies the networks, infrastructure and the fault tolerance of the coins.

Because every CloudCoin is split at the same time for the same amount, this monetary inflation is proportional, and the monetary system will not provide inaccurate information to its users. Instead, the split provides benefits for the users by keeping the unit of accounting at a usable value.

Bitcoins, on the other hand, require insane fractions of a coin to be spent. A loaf of bread at your local supermarket might cost 0.00068157342 BTC. Very few retailers have the equipment to process such small figures—let alone make change!

* *A byte is a unit of information on a computer made up of eight bits. A bit is usually a 0 or a 1. A byte most often represents a number.*

Bitcoins and CloudCoins

Now let's compare the physical integrity of Bitcoin and CloudCoins.

CloudCoins do not depend on encryption. Instead, the data is divided or shredded into data clouds all over the world that are managed by completely independent operators.

But what if one of these operators decided to give himself some CloudCoins by altering the records? Because the data is spread over 25 different data clouds, a RAIDA administrator could only take control of 1/25 of a CloudCoin. This would be instantly detectable and would cause the coins to be replaced immediately.

RAIDA administrators make their money by recovering lost coins, so anything that they could do to cause the value of CloudCoins to decrease would be self-defeating.

RAIDA operators are highly incentivized to keep the value of CloudCoins up, and that means keeping the money **true**.

What if a government or hackers were able to obtain the data from their RAIDA servers by force? The problem for the hacker is that once hackers are detected, the RAIDA clouds are replaced, and the RAIDA is designed so that all of the information about a CloudCoin is stored in the coin itself, not in the RAIDA network.

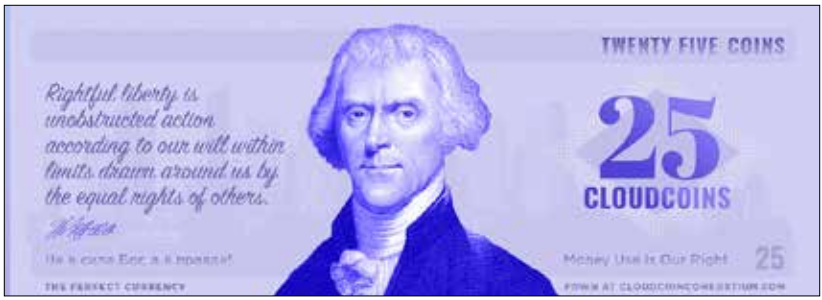
The CloudCoin notes

CloudCoin notes come in denominations ranging from one to 250.

There are actually two images used for the One CC note. The first is of **Stefan Molyneux.** *Molyneux is the founder of the YouTube channel* Freedomain Radio*. As of April 2018, he had over 768 thousand subscribers. (See* Acknowledgments *for more on Stefan.)*

The second is **Tank Man** *(also called the Unknown Protester or Unknown Rebel). On June 5, 1989, he bravely blocked the passage of tanks in Tienanmen Square. This incident was filmed and seen around the world.*

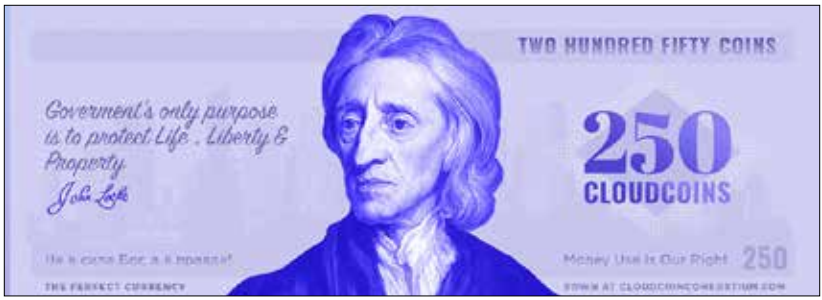
Adam Smith *(1723–1790) was a Scottish economist and philosopher best known for his work,* The Wealth of Nations*, published in 1776. His demeanor graces a 5 CC note.*



One of the Founding Fathers and principal author of the Declaration of Independence*,* **Thomas Jefferson** *(1743–1826) is found on the 25 CC note.*

Like the One CC note, the 100 CC note has two alternating images. The first is author **Ayn Rand** *(1905–1982). Her novels dramatized the philosophy she developed known as Objectiveism.*

The second 100 CC note shows **Alexander Nevsky** *(1220–1263). Nevsky, who lived in Russia in the 13th Century, was legendary for his victories over invaders, and was later canonized as a saint of the Russian Orthodox Church.*



The largest CC note, for 250 CC, has the image of **John Locke** *(1632–1704), commonly known as the Father of Liberalism.*

The CloudCoin experiment

With the success of Bitcoin and other cryptocurrencies, two central questions have driven the research for what has evolved into CloudCoin:

- What is the essence of money?
- What would be a perfect electronic currency?

I employed an information-systems approach toward a monetary system based on the two key points of **trust** and **integrity**.

From this, I implemented a group of cloud networks. The resultant system performs better than Bitcoin. Anyone can easily manage CloudCoins. You don't need an account with an exchange, and you don't need to download a huge 100 GB blockchain.

CloudCoins are faster to transact. While Bitcoin transactions must synchronize over thousands of public ledgers, requiring 40 minutes on average, CloudCoin only needs to be checked for counterfeit, and this process takes milliseconds. Real-world tests have authenticated 50,000 CloudCoins in just 3.5 seconds.

CloudCoins are 100% anonymous, while Bitcoins are pseudo-anonymous, meaning that if people figure out your account number on the public ledger, they can track anything you have bought or sold.

Bitcoin administration (mining) is consolidating. while CloudCoin admin should disperse.

Bitcoin is not quantum-safe and can be hacked with government quantum computers. CloudCoin does not rely on encryption to keep it 100% quantum-safe.

CloudCoin requires servers the size of a deck of cards while Blockchain requires rooms full of servers that consume huge amounts of electricity for performing encryption.

Money is data

The first hypothesis is that money—the tokens we hold, the coins, bills and numbers in our bank accounts—are actually part of a bigger system, an information system.

Specifically: **Money is a distributed database that is physically implemented among people.**

Each one of us is in charge of holding a small part of the data.

Each of us use our minds to process the information provided by our own money in order to economize.

We communicate key information to each other via prices. The interaction between the money and our behavior allows us to spontaneously organize our behavior to create an efficient economy.

No counterfeits—an essential characteristic

The second hypothesis is that the value of money does not come from the substance it is made of, but from the effort required to counterfeit it, and its integrity as data. Gold coins, paper dollars and electronic Bitcoins are all made of different stuff, and yet they are all used as money—and all of them are valuable.

Monetary systems made of gold, paper money and Bitcoins are very difficult, although not impossible, to counterfeit.

Gold can be mined and minted into duplicate coins. Paper money can be printed by expert counterfeiters and by a treasury itself. Bitcoins can be "mined" by solving puzzles.

Perfect money, however, cannot be counterfeited.

CloudCoins are composed of codes embedded in files, stored on paper or digitally, or remembered in your mind. These codes can only be used once.

When a CloudCoin changes hands, a new set of codes is generated. This makes it impossible to counterfeit, mine, double-spend or destroy a coin.

The total number of CloudCoins never changes—unless CloudCoin becomes too valuable, in which case, it splits, and everyone's CloudCoin doubles.

Unlike Bitcoins that can be mined into existence, CloudCoins were minted, then the mint was destroyed. There are exactly 16,777,216 notes in denominations ranging from 1 to 250. The number of notes cannot be increased or reduced because the number is based on the length of the Serial Number for each note.

Experiment design

Building on the hypothesis that the essential attribute of money is that it can't be counterfeited, a process was developed and implemented for the detection of counterfeits.

Assuming that the hypothesis "money is data" is true, a monetary system should be designed to give its money integrity in the same way a database would be designed to give its data integrity.

To achieve the general goal of data integrity, a redundant and robust system of clouds, governed by a consortium of independent multinational organizations, was designed. The end result is called RAIDA.

A patent has been filed for a cloud-based authentication system, a CloudCoin Consortium was created, and a digital currency was minted and deployed in a RAIDA.

For more details on the technology behind CloudCoin, see the Appendices at the end of this book.

Powning

Sometimes, when you develop a new technology, you have to find new words to describe it.

Powning (pronounced *PŌN-ing*) is the act of proving ownership. It derives from **proof of owning**, or **password owning**.

Information for a single CloudCoin can be contained within a **JPEG** image. However, for CloudCoin notes worth more than one CloudCoin, the information is contained in a text file called a **stack**.

With CloudCoin, ownership is proven by who has the password, and this ownership is passed electronically from one person to another. How this transfer occurs is mostly invisible to the CloudCoin user, but the steps below are what occur in the background during a transfer:

- The current owner transfers the CloudCoin as one or more **JPEGs** or text files (called **stacks**) to a recipient.
- The recipient opens the CloudCoin file in his CloudCoin software, checks that the denomination on the note matches what it should be. This thwarts any attempts to pass off lower denominations as higher denominations.
- The recipient's software sends a **Counterfeit Detection Request** to the twenty-five data-holding RAIDA clouds. Embedded in the request are the denomination, serial number, and corresponding authenticity number for each

CloudCoin. The RAIDA clouds determine if the authenticity data received agrees with the denomination and serial number the RAIDA has stored.

- If the numbers match, the response is that the currency is **authentic**. If they don't match, then the response is that it is **counterfeit**.
- Once the currency has been proven as authentic, the recipient can take full ownership. The recipient's software generates twenty-five **random PANs** (**Proposed Authenticity Numbers**) to replace the existing **ANs** (**Authenticity Numbers**).
- Now the recipient's software sends a **take-ownership-request** to the twenty-five RAIDA clouds. Embedded in each request is the denomination, serial number, the corresponding AN, and the PAN.
- The **detection agents** (the clusters of nodes that make up a RAIDA cloud) determine whether the authorization number data matches the denomination and serial number that the note has stored.
- If the numbers match, then the stored authenticity numbers (ANs) will be replaced with proposed (new) authenticity numbers (PANs).
- Now only the new owner (or his software) knows the new numbers, so the recipient becomes the new owner.

The interface for the CloudCoin Consumer Edition software is very easy to use. All of the procedures described above are handled automatically when you add a stack of CloudCoin to your account.

It is likely that not all RAIDA clouds will be available 100% of the time. This is not an issue, as **only ten of the twenty-five RAIDA clouds are necessary for authentication**.

The RAIDA cloud does not save any ownership information. It is the responsibility of the CloudCoin user to back up his or her CloudCoin data.

> “Annual income 20 pounds, annual expenditure 19 pounds, nineteen and six, result happiness.
>
> “Annual income 20 pounds, annual expenditure 20 pounds ought and six, result misery.”
>
> — Charles Dickens

Putting theory into practice

The theory behind CloudCoin was worked out. The next step was to put the theory to the test.

- Twenty-five RAIDA administrators of different nationalities were recruited. Twenty-five clusters were set up in the following countries:
  - Australia
  - Bulgaria
  - Canada
  - Colombia
  - France
  - Germany
  - India
  - Luxembourg
  - Macedonia
  - Philippines
  - Romania
  - Russia
  - Serbia
  - Singapore
  - Sweden
  - Switzerland
  - Taiwan
  - Ukraine
  - United Kingdom
  - United States
  - Venezuela

  The objective was to include as much geographical diversity as possible, and still keep the administrators within those countries that have mostly liberal governments.
- The operating systems used were either Microsoft® Windows or one of several versions of Linux operating systems.
- The CloudCoins were created, and authenticity codes were embedded in them.

- Software applications were developed to validate the ownership transfers, and CloudCoins were passed by email through five different people using the applications. Each person took ownership of the CloudCoins.

During the experiment, RAIDA5 went down. Because of this, RAIDA5's data became unmanageable. RAIDA5 was taken out of the RAIDA network and a new RAIDA5 was implemented. The CloudCoins in the test became fractured, or **fracked** (because, in this case, not all slices in the coins could be authenticated).

However, within seconds, each CloudCoin was able to fix itself—as the system was designed.

The experiment concluded on February 4, 2017.

This experiment demonstrated that CloudCoin *is* viable as an electronic currency, and that the RAIDA invention works stably as a new fault-tolerant authentication system.

- RAIDA performed much better than the blockchain used by Bitcoin because RAIDA required less than two seconds to perform a transaction.
- RAIDA required no user accounts or large software downloads.
- The transactions were 100% private, as opposed to semi-private as with Bitcoins.

A patent has been filed for the RAIDA technology with the United States Patent and Trademark Office. A trademark claim has also been filed for the term CloudCoin.

The CloudCoin Consortium is now preparing to provide CloudCoins as a global currency, and transactions will be offered free of

charge as the RAIDA will be funded by the scavenging of lost CloudCoins.

The proof

The concept of a cloud currency has features that make it superior to cryptocurrencies.

Cloud currencies such as CloudCoin do not require user accounts, and do not collect or track user data (except the month of the CloudCoin last transaction). This makes CloudCoin potentially more private than Bitcoin.

Because CloudCoin does not depend on encryption, CloudCoin is much faster to confirm.

It appears to be impossible to double-spend CloudCoins.

It also appears that CloudCoins are safe from quantum computer decryption, which may become an issue in the near future.

The infrastructure of CloudCoin can be self-funded by allowing RAIDA administrators to scavenge lost CloudCoins (CloudCoins that have not been spent or checked in two or more years) to pay for their operations.

> "The system of banking [is] a blot left in all our Constitutions, which, if not covered, will end in their destruction... I sincerely believe that banking institutions are more dangerous than standing armies; and that the principle of spending money to be paid by posterity... is but swindling futurity on a large scale."
>
> — Thomas Jefferson

Blockchain Socialism

Once there were two countries, each with a society of about 10 million people. Every day, the citizens of each country would go to work, earn money, trade with other citizens, and try to economize.

This was the natural state of things until one day the President of one country noticed that some families were very good at working and had collected a lot more money than the other families.

The President, who was interested in creating a just society—wanted all people to have equal money, so he said to his most trusted advisor, his brother Brutus, "You will create a blockchain-based digital currency and assign everyone an account. You will include an algorithm so that all people will end up with the same amount of money. You will take from those with abundance and give to those who have less so that all families can be economically equal. Take some of the money for yourself."

Brutus devised the system, and it was implemented.

When some of the citizens got paid at the end of the month, they were delighted to find that extra money had almost magically appeared in their accounts. Other citizens, however, rushed to tell the President that they had been robbed. "A thief has hacked our account and stolen our money!" But the President assured them that it wasn't theft, but sharing, and that the country had become a more just society because of it.

Now this country, which had introduced a blockchain-based socialism, soon grew poor. Not only were there fewer people who worked (Brutus redistributed instead), there were also unintended behavioral changes among the country's people.

People who used to work hard to make money grew tired of all their toil being taken by someone else, so they only worked half as much and brought home less money. Some of the people stopped working altogether because they learned that they would still get money even when they didn't work.

Some of the more talented workers and traders were so mad that they packed up their families in airplanes and flew off to their neighbor country, while homeless people slipped quietly across the borders, wanting to become a part of this "just society."

Then the President's brother, Brutus, started skimming a little extra from the algorithm for himself, and he was soon the richest citizen in the country (a fact he hid from others by using many secret accounts).

The blockchain socialist country grew poorer and poorer. The system required large amounts of expensive electricity to run, and trades grew slower and slower too. People now had to wait in line.

Meanwhile, in the naturally free country that used CloudCoin, all the citizens had to work for their money. They knew that if they did not work hard they might end up hungry or worse. They worked so hard that some of them even had surplus money.

Soon they found that surplus money could be used to allow some citizens of the country to research new ways to work and trade more efficiently. The research paid off, and the total product and

trade grew with each new technology invented. They soon called the people with surplus money who performed this research "CloudCoin capitalists" because they were using their heads (since they knew "capital" means head). They called their system CloudCoin Capitalism, but many just called their system the free market because this is what happens when people are free to act naturally.

It was only a matter of time before the CloudCoin capitalist country grew so economically powerful and the blockchain socialist country grew so poor that it became clear to the blockchain socialists they needed to change.

So the President of the blockchain socialist country called for a vote to see if the people wanted to change. But brother Brutus liked the system and knew the people would vote against it.

He murdered his brother and canceled the election.

To keep the talented people from leaving the country, Brutus (who was now running the country based on the influence of his enormous wealth), outlawed emigration.

He declared laws to limit the natural rights of people. He kept them from communicating, collaborating or making weapons that could be used to overthrow the socialist system.

All of this worked very well for Brutus. He lied to everyone and told them that their system was "just."

But in reality, he stole from hard-working people and gave the money to laggards, including the greatest laggard of all—himself.

The economy became submerged because the money no longer sent signals to people to economize. In the end, hackers with

quantum computers were able to take the system down and the people were freed.

The moral of the story is that the blockchain can be used for evil just as easily as it can be used for good.

We need good money to make good economic decisions. The Blockchain requires accounts. Like Ayn Rand said, "Civilization is the progress toward a society of privacy."

The blockchain can do the exact opposite because every purchase anyone has ever made can be tracked, and the system can even be used to redistribute. The blockchain could be used as a powerful tool for repression.

This story avoids sharing the gruesome details of hundreds of millions of victims of democide* who were killed or starved because their monetary system was controlled by a central government.

Monetary systems must be decentralized and privatized to work.

* *The murder of any person or people by their government, including genocide, politicide and mass murder.*

The future of your enslavement

RULE: The perfect money is perfectly private.

One of the inherent problems facing all modern currencies is the way in which new money is created, and who gets this newly created money.

According to my theory of money, the perfect money cannot be created or destroyed, except at its inception (minting), unless the money is split so that all people end up with the exact same proportion of money—just more of it. The primary purpose of money is to track who gets what proportion of the total output based on their total input.

The opposite of this is a system where money (data) is created and introduced to the system at the expense of everyone else. These types of systems (which dominate the world now more than ever) inadvertently cause logical errors, negative feedback loops, and submersion of the economy.

In economics, these phenomena are often known as **inflation**, **price inflation** or **bubbles**.

Sometimes economists argue about what inflation is.

Is it something that occurs when there is more money? Is it something that happens when prices are higher? Both of these assumptions are wrong, and economists need to turn to information systems to understand the situation.

Remember that money is data. If data appears without valid input in an information system, we call this an **anomaly**.

This incorrect data will be processed by our human minds and will cause logical errors. We will see opportunities in things that are not opportunities. Likewise, we will avoid true opportunities because we cannot recognize them. This can cause a feedback effect in which errors are compounded.

Ants have their own information systems. They use pheromones. Their antennae are specially designed to detect these pheromones. For ants, these pheromones are like money. They tell the ants what to do.

Do you want to mess with ants? Spray some pheromones in places they are not supposed to be. The colony will collapse into chaos. What would happen to human civilization if you dropped money from helicopters?

The same thing happens when money is dropped into the economy in random places. It causes crazy behavior, including the housing bubbles, and booms and busts.

Some parts of the economy may be unaffected, but other parts go into hyper-mode. This will not last long though. Soon, areas of the economy become neglected.

Because an economy is built on itself, each part is essential in some way. Neglecting any part will cause the entire system to grind to a screeching halt.

As often happens, food and energy are neglected, causing starvation and even death for millions of people.

This is what I call **sluck**. It is a concept based on "submersion due to logical errors caused by anomalous data injection." So instead

of saying that the Federal Reserve is causing inflation, it is better to say that the Federal Reserve is slucking our economy.

Sometimes we just need new words.

But wait, isn't our economy improving? Slucking makes us think things that are not true, and while it may not stop growth, slucking causes the economy to improve more slowly than it may otherwise.

Emergence and submergence

This brings us to the idea of **emergence**.

Human civilization is not possible without money. If you take away all the money, people don't know what to do, and they don't know how to economize.

Without money, we are stuck with the next best thing—**barter**.

Simple barter systems can only support a few hundred entities before they become too complicated to work. There is only so much people can process in their minds. Money makes commerce easy.

When there is good money, an economy emerges. We call this an economy, a civilization, a nation, or a society. But we can also think of it as a hive, a **superorganism**.

The concept of emergence becomes clear when we look at what comes out of a large number of smaller parts. There are trillions of atoms in a human cell. From these atoms, life emerges. We have billions of neurons in our brain. From this network, our consciousness emerges. There are billions of people in the world, and from these populations, nations emerge.

Only from money can nations emerge. If there is a lack of good money, they will submerge. Having good money is of paramount importance to all of us. With the digital currencies of the future, we can expect our economy to emerge like never before. If that digital currency turns out to be evil, expect great tragedy.

In science, diversity is inequality

Some think that free-market capitalism creates inequality. However, inequality is part of the natural world, part of the diversity of the human species, and part of every other life form on the planet.

Any scheme that tries to make everyone economically equal goes against nature and God and against the nature of the Universe.

Trying to create a situation where people have equal amounts of money is a form of **hacking**. It takes a lot of work and it goes against society.

Hacking is theft

Hacking is the action of gaining unauthorized access to or manipulation or exploitation of a computer or network for an illicit purpose. But computers are not the only thing that can be hacked.

There are people who know how to hack our monetary system.

These hackers get money that they did not earn. Because they are able to get undeserved money, the monetary system is not perfect. I do not blame these people because they probably don't even understand what they are doing.

But this kind of hacking happens at both the top and bottom of society.

Some of these hackers are really rich and are what I would call the true **PhD hackers**. They have found vulnerabilities, and they have exploited them. They do not share their secrets with others.

At the other end of this spectrum are the **script kiddies***. These social hackers are generally stupid and uneducated. They either don't know how to make a living or don't care enough to bother, but they do know all about government programs and how to exploit them.

So, who are the hackers?

You are probably like most people; you work your ass off and get the shit taxed out of you and wonder why things get a little more challenging with each passing year.

But the hackers don't work their asses off and don't pay taxes. With a perfect currency, they would be unable to do this.

With a flawed currency, you are being victimized—and you might not even realize it. It is like a virus that uses you without killing you. It wants to keep things so low-grade that you don't even notice you are sick. But you are, in fact, like a farm animal to them. You will be milked, and they don't give a dang if you don't like it.

If you don't resist, you condone it. We need to stop the hack, we need to upgrade to a more secure information system—a

---

* *Script kiddies are a class of wannabe hackers who don't actually know enough to write code that can hack a system, but who use existing code that they get from someone else. Script kiddies are dangerous primarily because of their stupidity and carelessness.*

monetary system that cannot be hacked. Digital currencies give us a way to resist. They give us a way to fight back.

They give us a way to stop the hacks.

A global PayPal

Most people do not realize that PayPal is a monetary system.

While Bitcoin has a public ledger, PayPal has a private ledger.

Bitcoin's blockchain is distributed over many systems while PayPal's is centrally controlled, which makes it both more efficient and more scalable.

Could PayPal be brought down? I think it will last longer than Bitcoin.

The PayPal system was the great invention of the Libertarian Peter Theil. Theil believed that PayPal would be a big step toward freedom, and that it would especially help people in authoritarian countries.

He was absolutely correct.

PayPal has been a great achievement, and has opened up the world to commerce. I know of very few people in Venezuela who do not have a PayPal account, and this allows them to survive despite their socialist, money-destroying government.

But many people do not like PayPal.

For many of us, PayPal has become an extension of governments, a system that helps to regulate us.

Plus it has some annoying features. I have certainly had my account frozen many times.

Of course, this happens with debit cards too. I go to the store and fill up my cart, only to find that my card has been declined at the register, even though I have plenty of money in the account.

And why does this happen? The answer is **referential integrity**.

Your bank account is not *really* full of real money. Your money isn't actually in PayPal. These systems just reference real money with what are called **pointers**.

If money is data, then your debit card is **metadata***. It is like one of those old silver certificates, which originally represented an amount of silver in a vault.

One money system must reference the other. It becomes a problem when it does not. At this point, it lacks referential integrity.

PayPal must freeze your account to make sure that the money that you have is actually there. PayPal lacks referential integrity.

CloudCoin does not reference anything else. Therefore, it has 100% referential integrity.

And another problem is that sometimes they (the bank or PayPal) can't figure out who the owner is. This is called **entity integrity**. They think you may be committing identity theft when you use your debit card, so they freeze your account to stop anyone from stealing.

I remember when Target's servers were hacked and everyone's credit card information was stolen. The banks started locking everyone out because they didn't know who was using the information.

---

* *Metadata is a set of data that provides data about other data.*

There will most certainly be an attempt by governments in the future to create a global PayPal-like system, but you are not going to like it.

Not only will you be frozen out of your accounts just like you may have been with PayPal, but governments can do much, much worse.

They will be able to seize your money because you don't own it—you just own a reference to it—and they will be able to violate that reference with ease.

Your blockchain address is your Social Security Number. But suppose a government wants to make sure that everything you buy and sell is tracked, and there is no way (short of a quantum computer) to make changes. The blockchain is perfect at this. They can use your government ID number as the unique identifying number on the public ledger.

The problem is that people need privacy to make efficient decisions.

Imagine if, every time you went to the store, everyone was watching what you purchased. Or imagine if you were compelled to publish your receipt on Facebook for every purchase. You would begin to behave differently.

CloudCoin is completely anonymous. With CloudCoin, you are free to be you.

Artificially intelligent dictators

Once we have government-controlled digital money, it will be easy to add a little artificial intelligence to *really* mess things up.

If you think about it, the human brain is the most intelligent thing we know of, and we have 7 billion of them on planet Earth—all working in parallel to manage the economy.

We humans have tried **central planning***, and it does not work. A government lacks the computational power to run things.

Command and control economies** have never even come close to the performance of **free markets*****.

Much of the success from past experiments in command and control has come from theft or cannibalization. Sure, if you kill millions of your citizens, the cost of labor will go up and the price of homes will go down.

If you put people in gulags, you can create a free labor pool. But eventually, like the Russian Empire, things will collapse.

But what about quantum computers?

Each quantum computer has the computing power of approximately one billion desktop PCs. Can't we put a quantum computer in charge of things?

Can't these supercomputers tell us where to go each day so we're always most efficiently employed? Can't they provide the healthiest food choices for us? Who'd need money? We'd be living in a future utopia, right?

** An economic system where the government takes control of production of goods and services, instead of letting consumers' needs drive business production.*

*** Direct regulation of an industry or activity that states what is permitted and what is illegal.*

**** An economic system where prices for goods and services are driven by supply and demand, without government intervention or price control through a monopoly.*

The truth is that we know very little about the human mind or quantum mechanics. It is within the realm of possibility that our minds are already quantum computers using some unknown mechanism. And a quantum computer will never be as powerful as a human being using a quantum computer.

The reverse is not going to work for us either. Artificially intelligent computers do not fear death or hell. To an AI, human life will never have any more value than we give to characters in video games. Mathematically, there is much to gain from killing us off.

Stalin was a rational atheist who believed in communism and equality. It made sense to Stalin to kill tens of millions of people and ruin the lives of tens of millions more.

He was, in his own mind, thinking rationally. Had he been an AI computer, it would have made sense for him to kill *everyone*.

> "Civilization is the progress toward a society of privacy...."
>
> – Ayn Rand

The problem with the Federal Reserve

Thousands of years ago, tribes of Paleolithic peoples who lived by the sea collected rare blue cowry shells.

Members of all of the tribes loved these shells. They used them for jewelry, and decorated their clothing and hair with them. They even integrated them into their crafts, weaving shells cleverly into their baskets.

The shells were so popular that the people began to use them as money. They knew that it took about an hour of searching to find a cowry shell, so each was worth about an hour of their time.

The use of these shells as money soon led to an economic boom.

The money allowed the islanders to practice **division of labor** for the first time, where each person could specialize in tasks at which they were adept. This opened up new jobs.

Sometimes they would use other shells for money. The red cowry was very common and only took about fifteen minutes to find, so it was worth 25% of a blue cowry. The purple cowry, on the other hand, was extremely rare and could take days to find. It was worth 100 blue cowry.

The economy grew substantially as the islanders became more productive at everything they did because of their division of labor.

Within all of the tribes, there were innovative people who made new inventions.

One person came up with the fishing net. He knew that his idea would work, but it would take a lot of time and effort to turn his idea into reality.

He told a friend about the idea, explaining how time-consuming it would be to gather the fibers, weave them into string, then tie them into a net. It would take many days, and in those times, people needed to spend their time gathering food just to subsist.

The inventor's friend thought about how to make this project work, and in the process, inadvertently invented a bank: He asked his neighbors to loan him shells for the project, and he promised to pay them back with even more shells later.

With this primitive banking system, the fishing net was developed into a working tool. And yes, it really worked—and created a boom in fishing!

Two things happened because of the fishnet invention.

- The price of fish in cowry shells dropped because fish could be caught with less effort, thanks to the new technology.
- The value of the cowry shells went up because people could buy more fish with them.

After buying the cheaper fish, the people had extra money to buy other things. This provided opportunities for other tribal members to create new ways for others to spend their cowry shells—other jobs and specialties were created in the economy.

The fishermen who caught the fish were getting far less per fish, but had many more fish to sell, and so were making more profit.

And since fish were cheaper, that meant some of the money that had previously gone to buying fish went instead to the people who had risked their shells to support the development of their inventions.

Soon came the professional investors, and these investors had an incentive to make investments—they wanted to get lots of shells so they too could buy lots of stuff. And soon inventive ideas all around the islands were being funded by the bankers who only needed to use their heads to work (the Capitalists).

Unfortunately, there was crime. No matter what they did, there always seemed to be someone who would try to steal someone else's shells. The newly formed banks built vaults to help alleviate crime by providing safe places to store shells.

But then things changed.

One of the tribes was headed by a war-loving chief named Brutus. Brutus wanted to go to other tribes, attack them, and take all of their goods.

But war is expensive. He needed soldiers, weapons, and supplies.

Brutus would need the help of the other tribal members to build his army. He needed the guy who made fishing spears to make fighting spears instead, and give the spears to him.

He needed the fishing boat builder to build war boats instead of fishing vessels.

Brutus needed people who would fight—but the only way he could get men to become fighters was by offering them many shells in return.

Attacking neighbors was going to be expensive, but he could sense that it would be profitable. So he began asking the tribe members to give him some of their blue cowry shells.

But the other tribe members didn't like the idea. They remembered how they had lost money the last time Brutus attacked their neighbors and lost.

Brutus wanted to force people to give him shells. He said it was of national importance, and that the tribe should have a tax.

But the people rebelled against Brutus, and Brutus was forced to quit taxing the tribe out of fear that he himself could be attacked.

Finally, Brutus came up with a plan to ensure that he could always have enough shells for his military adventures. He would create a **Reserve Bank**. This Federal Reserve Shell Bank would make certain that there were always enough shells for him to borrow anytime he wanted.

To create such a bank, he had to do some work, and he needed to get the other banks to go along with it too.

First, he had to create some paper money, which he called Paper Shells, with pictures of shells on the bills.

Then he would outlaw private ownership and trade of shells. Everyone with shells would have to exchange their shells for Paper Shells. Then all the real shells would be placed in Fort Shell Knox—a very secure location.

The banks would all become voting members of a government-sponsored cartel, which would be called the Federal Shell Reserve.

In exchange for their cooperation, the banks would also be able to borrow as much money as they wanted, anytime they wanted.

When the banks wanted to loan money, or when Brutus wanted to borrow some—Paper Shells would simply be printed up for them at everyone else's expense.

They would need to be careful. They were smart enough to know that printing too much too quickly could cause the economy to sluck, and even give the people a reason to overthrow the banks and Brutus.

But the new Federal Shell Reserve immediately began wreaking havoc with the economy.

First there was the invention of the bow and arrow. This invention allowed a hunter to kill many more animals than the traditional spear could in the same amount of time.

Normally, without the Federal Reserve, the best hunters would be the first to receive the new technology, and it would take more time for the invention to be implemented broadly. But with the invention of the bow and arrow under the Reserve system, all the hunters in the tribe showed up on the same day wanting a loan to buy the new productivity-enhancing tool. The banks ordered more Paper Shells printed and all the hunters were given a loan for the cost of the tool on the same day.

All the hunters took their Paper Shells to the bow maker. They all wanted a bow, but the bow maker only had a few bows on hand so he boosted his price dramatically. He raised the price so much that it was hardly efficient for the hunters to buy them.

The bow maker quickly hired a bunch of people to make the bows, and they worked all day and night making bows—and they made

a lot of money. But after all the hunters bought one, the entire market demand for bows collapsed, and all but a few bow makers were laid off.

Meanwhile, the hunters collected so much meat that the price of meat collapsed (which was good for everyone except the hunters).

Soon many of the hunters couldn't pay back the money they owed on the bows because the bows were now worth less than the money they had bought them for.

So the Federal Reserve had the following impact:

- Markets boomed and busted much more dramatically and with huge price fluctuations.
- Things that were purchased with freshly borrowed money went up in price dramatically.
- As the freshly minted money circulated through the system, all things (minus the new technology) would go up in price slowly but surely.
- Money was now available to pay for wars that would otherwise be unaffordable.

And that's what's wrong with the Federal Reserve.

Protecting our civilization

From the Gospel of Matthew, Chapter 25:

14 For the kingdom of heaven is like a man traveling to a far country, who called his own servants and delivered his goods to them.

15 And to one he gave five talents, to another two, and to another one, to each according to his own ability; and immediately he went on a journey.*

16 Then he who had received the five talents went and traded with them, and made another five talents.

17 And likewise he who had received two gained two more also.

18 But he who had received one went and dug in the ground, and hid his lord's money.

19 After a long time the lord of those servants came and settled accounts with them.

20 So he who had received five talents came and brought five other talents, saying, 'Lord, you delivered to me five talents; look, I have gained five more talents besides them.'

21 His lord said to him, 'Well done, good and faithful servant; you were faithful over a few things, I will make you ruler over many things. Enter into the joy of your lord.'

---

* *A talent is a type of money used by ancient Babylonians, Sumerians and Hebrews.*

22 He also who had received two talents came and said, 'Lord, you delivered to me two talents; look, I have gained two more talents besides them.'

23 His lord said to him, 'Well done, good and faithful servant; you have been faithful over a few things, I will make you ruler over many things. Enter into the joy of your lord.'

24 Then he who had received the one talent came and said, 'Lord, I knew you to be a hard man, reaping where you have not sown, and gathering where you have not scattered seed.

25 'And I was afraid, and went and hid your talent in the ground. Look, there you have what is yours.'

26 But his lord answered and said to him, 'You wicked and lazy servant, you knew that I reap where I have not sown, and gather where I have not scattered seed.

27 'So you ought to have deposited my money with the bankers, and at my coming I would have received back my own with interest.'

28 Therefore, he took the talent from him, and gave it to he who had ten talents.

29 For to everyone who has, more will be given, and he will have abundance; but from he who does not have, even what he has will be taken away.

From this parable, you can see that Jesus was a Free Market Capitalist and so is God. Without the freedom to make mistakes,

we cannot do good, for those who are compelled to act are never fully responsible for their actions.

If you want to be good with God, let freedom ring. Do not let governments or banks get between you and God. Money is the Voice of God. It commands us, it tempts us, it makes us free so we may do good and so that we may do evil. It is part of the test that God puts us through here on Earth.

Use of money is our divine and sacred right. We must be willing to fight to defend it. And you must defend the rights of others to use money too, for if you will allow others to stand alone, then you can expect to stand alone yourself. And by your division from others, you will be conquered.

Begin with the end
in mind.

—Stephan R. Covey

The prehistory of money

I am about to speculate about how money came to be.

I considered leaving this part out because it is so odd that you may find it unbelievable. But I have been right about other things, so just go with me on this for a bit.

Besides, what I'm about to explain is all evidence-based.

Looking at the evidence

Let's go back 50,000 years, to Europe.

There was no farming. On the ice age tundra, there was nothing to eat except mammoth and other plant-eating mammals. Money wasn't needed.

The nomadic people of the Paleolithic era cared only about food, shelter, and sex. They were interested in tools, but they really couldn't afford to put much effort into research or development of new technologies.

People would live their whole lives without experiencing any changes in the way things were done, and would never see a new invention.

Like today, men and women differed in interests, but all were interested in companionship and friends. Female humans, unlike almost all animals, had sex socially.

In theory a woman could copulate almost all year long, but with only one fertile day a month. But because sperm can live for up to five days, the actual fertility window was a little longer.

Fifty thousand years ago, people were constantly on the move. They lived in small family groups and they created temporary camps. In the camps lived the very young, the women, and the very few who were lucky enough to grow old.

Adult men, however, did not stay in the camps much, except for a small group of what we might call Alpha males. These Alpha males were probably chosen by the matriarchs and were expected to guard the camp but they also impregnated the fertile women.

It was that elite class of Alpha males who did all the impregnating. I surmise that only 20% of men in those days ever had children. (With the invention of money, this would later increase to 60% and give money users a biological advantage over non-users. Genetic research supports this.)

Women were probably pregnant most of the time, but when they were not, they had to act accordingly.

Back then, for one week a month, the women would —like mindless zombies—stop having sex with the Beta males and coax the Alpha males to secret rendezvous. They may have even blocked out the memories of these trysts to make it easier to lie about it to the Beta males to prevent them from becoming jealous.

The Beta males were expected to go out and do the very dangerous work of hunting mammoths and other large game. Women and the Alpha males probably did all the construction of shelters, crafting of tools, and making of weapons, clothing and

shoes, while the Beta males were away doing all the dangerous killing of wild animals.

The fact that women did not have to hunt increased the number of children that were born because the women didn't have to take risks, and stayed in camp to raise children.

The Beta males would trade meat for sex and companionship. It wasn't prostitution, but more like an open marriage.

However, the Beta males did not get any women pregnant. For Beta males, there was only a 1 in 30 chance that they would get a woman pregnant— if she wasn't pregnant already. And since the Beta male was off hunting quite often, she probably was.

If she was ovulating, she would stop having sex with all but the Alpha males. If the Beta males could slip some sperm in a few days before ovulation, he might have a small chance.

But either way, the woman would eat well without the risk of hunting.

Over 144 Paleolithic figurines of the female form, referred to as **Venus figurines***, have been found that date to 35–11,000 years ago.

Some think that these are goddess figures. But some figurines show a woman as bound—not what you would expect for a deity.

These figures meet all the requirements of money, and support the hypothesis that money has been around in Europe for tens of thousands of years.

---

* *A Venus figurine is any carved or molded figure of the female form that dates back to Paleolithic times. The name has no connection to the Roman goddess Venus.*

This Venus figurine, shows a woman with bound hands.

They also represent what was really valuable in the Stone Age.

The Beta males had a problem because, when they killed a mammoth, there was too much meat to carry back to the camp, and too much meat for the camp to eat before it went rotten. Most of the meat simply went to waste.

This was a problem because killing mammoths was a dangerous endeavor, and wasting meat meant that the Beta males would have to risk their lives more than was necessary.

Money—in the form of Venus figures—would come along and change this.

Back at the camps, tribal members would create Venus figurines of each of the attractive females and give these figurines to the Beta males who went hunting.

If they ran into Beta males from other families who had been successful in hunting, they could trade the figurines for the location of the kill. This allowed the Beta males from one family to get meat from the Beta males of another without having to carry out the risky business of making the kill.

And what did the new owner of the Venus figure get? He got to lie with the woman the figurine represented—perhaps on days of the month when she was likely to get pregnant. He also risked his life less, so there were more chances of getting a woman pregnant in the future.

Most men never had a chance to have children back then, but the Venus figures gave them an advantage!

Now the top Beta males who were good hunters could have access to the women of other tribes, and have a chance at reproduction. Each figurine was worth $25,000 in food in the equivalent of today's economy, but cost very little to create.

Over time, the men who used this Venus currency had more children.

And why would women back then want to sleep with Beta males from other tribes?

In most cases, the women were already pregnant with the children of Alpha males and really had nothing to lose by having sex with the Betas. (The alpha males back then were more like today’s pimps. They were oversexed. They had all the women they wanted, and they did not hunt or do dangerous work.)

It was the women who wanted the Alpha sperm, and the Alphas learned that they could demand meat in exchange. This forced the women to trade with the Beta males to get meat to pay off the Alphas. The women exchanged meat for cooking, shelter, comfort, companionship, and sex. Any tribes that did not use this money were not as successful and thus did not carry their genes into future populations.

That human females don't get pregnant every time they have sex is a unique feature shared with a short list of species that includes bonobos monkeys and some species of bats. This behavior allows for social sex, or sex for the purpose of building social relationships.

When did this system go out of fashion? Around 10,000 years ago the mammoths died off and the system no longer worked.

By that time, societies had evolved to accept other monetary systems, and those other systems were put in place.

When farming was invented, the Betas were able to capture and keep their own women, and the rate of men having children went up substantially, to nearly 100%. The Alphas were locked out, except for their own wives.

Fifty thousand years ago, humans could have all the babies they wanted because humans were killed so often by predators that there was no chance of them having too many children. They had an **r-reproductive strategy*** as opposed to the **k-reproductive strategy** that we have today.

---

* *An r-reproductive strategy is one that focuses on reproducing in a high volume that will ensure survival of the species. A k-reproductive strategy occurs in a stable or predictable environment where competition for limited resources is crucial.*

Women gave birth to many babies over a short life span. If a male wanted to sire a child, he needed a woman's token.

The first coins were not made of silver, but of mammoth tusk.

They did not have the heads of state on them—they had vulvas.

A mammoth tusk coin found in the Paleolithic tomb of a male. From Czech Republic, circa 26,000 B.C.

I believe these coins were used to purchase sex, with coins obtained by selling the location of a mammoth kill.

Much of a civilization's wealth and prosperity depends on the monetary system it uses.

The superorganism

A superorganism is an organism made up from many organisms. The term is used most often to describe a social unit of **eusocial*** animals or insects, where division of labor is highly specialized and where individuals are not able to survive by themselves for extended periods.

Money is absolutely necessary for humankind to exist in numbers. Even if we were forced to use crappy inflated money (like the Venezuelan Bolivar and its runaway inflation) we would still use it because bad money is better than no money.

But there is a question that I don't know the answer to:

Does the society create the money,
or does the money create the society?

Just in case the money creates the society, I have created the Constitution of the CloudPeople. This Constitution builds on everything we have learned since the framing of America's Constitution. If you plan on overthrowing your government, you may want to check out this constitution because it is just about guaranteed to make your country as rich, prosperous, and happy as humanly possible. You can find it at:

www.CloudCoinConsortium.org/Constitution

---

* *An eusocial group is one where specialized activities are segregated for increased efficiency.*

The right to use tools, including money

One thing that separates human beings from animals is our use of money, and money is critical to our survival.

Money provides a system of justice for people who participate in trade—justice in the sense that people should get what they deserve, and that those who work efficiently deserve to have more economic rewards than those who are not as efficient or productive.

Much of a civilization's wealth and prosperity depends on the monetary system it uses. By choosing the correct system, not only can America be much wealthier than other countries, we can also develop new and innovative types of money that propel us into even more wealth.

Later I will discuss the most ethical and prosperous monetary and banking systems. Here we establish the fact that people are money users and money use is our natural right.

Note that there needn't be a government to have money, and that money existed long before governments.

As humans, we have a nature. We are thinking animals. We have evolved with large brains that allow us to survive in a variety of habitats.

Since the Age of Reason and the American Revolution of 1776, fueled by the Deist* philosophies of John Locke, Thomas Jefferson, and Thomas Paine, liberal societies have come to understand that reason and rational thought are the most ethical means for us to organize and rule ourselves. In stark contrast are

* *Deism is the belief in a supreme being (God) coupled with the belief that God does not interfere in the activities of Man.*

the Islamic Jihadists who believe that their magic book gives them the authority to slaughter anyone who dares so much as draw a cartoon of their leader.

We rational Libertarians understand that we must debate all aspects of the decisions we make and look carefully at the facts, keeping our emotions at bay, resisting mindless religious, and political ideology, and instead embrace reason.

We must be skeptical and question everything.

When someone (teacher, parent, preacher or politician) tells us what is true—we should not just accept it. Look at what the critics say, and examine all sides of the argument. As Thomas Paine said, we must not think that something is true just because it is tradition.

Remember that solutions to problems sometimes seem very strange at first. If the solutions were obvious, we may have thought of them long ago. Do not avoid conflict.

We must challenge each other's thinking. We Americans questioned everything during the American Revolution, with good results.

Let us start by declaring who we are and what we want.

Freedom provides the possibility of failure, and freedom is necessary for human happiness and the long-term evolution of our species. That is why it is ethical and good to make certain that no other humans are given control of our lives—and that we may be independent and live on our own terms, free to fail and always in control of ourselves.

A natural declaration

We humans have evolved with certain adaptations, abilities, instincts and behaviors that provide us with natural advantages in our environment.

Among these are the ability to communicate, cooperate, and use tools, and the instincts to live and live well.

Let us call these adaptations our natural rights, human rights, genetic rights, or simply our rights.

Important traits that we have evolved with include our opposable thumbs, vocal cords, and large brains. These endowments were inherited from our parents, and ultimately from God, or as a phenomenon of the natural Universe.

These natural rights are inalienable and are inseparable from us. Even if we should have our tongues cut from our mouths—by force—we will still possess the just claim to communicate because the urge to communicate is sequenced in every DNA chain in every single cell in our bodies.

Therefore, our rights came before there were governments, constitutions, or laws, and our rights are a direct result of God, our biology, and millions of years of evolution. We Homo sapiens have obtained our rights simply by being born human.

We are all equal in our claim to our own natural rights.

We all, every member of our species, short or tall, smart or simpleminded, have a just claim to seek out the best for ourselves, and use our parent-given genetic rights to try to achieve our goals and pursue happiness independently.

Within the human population, there is much genetic diversity. Males and females have different chromosomes, and every person has unique genetics based on a unique ancestry.

The pursuit of happiness and other rights are not related to our race, gender, sexuality, or religion.

Because of our diversity, humans may not succeed equally—but all people have the right to pursue happiness in an environment where institutions do not discriminate against, or grant preferential treatment to, any individual or group on the basis of race, sex, color, or ethnicity.

Our rights are self-evident, meaning that they are obvious to us because we are humans and we experience our life in bodies every day. We know what it means to be human; we know our universal needs, wants, and desires. And we know how to use our human skills to help us reach our goals.

However, in this modern age, we humans are our own worst enemies. The history of mankind is a history of war, death, and carnage. History has shown that when humans control other humans, those being controlled do not live long. Humans will often deny each other's rights to further their own welfare or force their beliefs of how humans should behave on others.

Humans often suppress the rights of other humans to achieve their own selfish goals. Even when humans have good intentions, they may inadvertently take the rights of others, thinking that it is righteous, fair, equitable, or scientific to do so.

Freedom provides the possibility of failure, and freedom is necessary for human happiness and the long-term evolution of our species. That is why it is ethical and good to make certain that no other humans are given control of our lives—and that we may be independent and live on our own terms, free to fail and always in control of ourselves.

Simply put, I have no more right to control your life than you have to control mine.

We the humans have the right to institute governments to protect us from the human tendency to dominate, enslave, coerce, cannibalize, socialize, and even murder other humans.

Humans will dissolve governments that do not protect rights, liberty, and individual sovereignty, as well as those that seek to tax, control and indebt the people they claim to own.

Beginning with the view that the purpose of money is to provide justice in each person's claim to economic production, a system that provides the most justice is the most ethical.

When people intelligently decide to get an education, and to work efficiently, we would expect them to have some money. Those people who decide to play video games all day and refuse to work should have no money. That is justice.

People who invent something special that makes everyone's lives easier may be expected to have the right to a lot of money, and those who steal and cheat can be expected not only to have no money, but also to be punished.

An unjust system would allow the cheaters to get rich while the inventors are poor. In an unjust system, the inventors stop

inventing, the producers stop producing, and everyone gets poorer.

The Communist idea of "From each according to their ability, and to each according to their need" is the exact opposite of justice. So here are some laws.

Natural Selection's Bill of Rights

Premise 1: We are born with adaptations, such as vocal cords, thumbs, brains, and instincts that, taken together, are uniquely human.

Premise 2: Nature selects for traits that give advantages to a species, and these traits are passed on to offspring.

> **Inference:** The use of vocal cords, thumbs, brains, and instincts gives humans a natural advantage.

Let's call the things that give humans natural advantages natural rights, human rights or simply rights.

Keep in mind that in science, diversity is inequality. Therefore a diverse population (like the Earth) can expect to see inequality in income.

These inequalities were not caused by free markets or capitalism, so do not blame free markets and capitalism for inequality.

It is worth taking a page in this book to describe other rights that we should defend. Here are some excerpts from the CloudCoin Constitution:

Here are what I believe to be our rights with regard to money:

We the people have evolved naturally with rights. These rights include core rights that we share with many other life forms, and include:

1. **The right to the preservation of life**

   Like all life forms, we have evolved with a strong drive to avoid death, and to do those things that prolong our lives and help us to live well.

2. **The right to seek happiness and pleasure**

   We have the right to strive for those things that make us happy and give us pleasure. We require freedom to act in ways that enhance our well-being, and therefore we need freedom and independence to be happy.

3. **The right to self-ownership, independence, and liberty**

   We have a just claim to self-ownership, with all its associated privileges, and the responsibilities of independent people. Labor, consumption, marriage, sexuality, offspring, medical treatment, death, and drug use are some of the areas in which you have the right to choose your own actions, and you must live with the consequences.

   Slavery, serfdom, and forced debt repayment are absolutely inhumane.

4. **The right to property, money and capital**

   Humans are territorial animals, and will establish and defend territories, even to the death. Property ownership is part of being human, and includes ownership of land, and tools such as money.

Humans are the only animal to use money and trade it for goods and services. Individuals have the right to choose what they consider money and the value that they place in it.

People shall not be forced to accept specific kinds of money.

We have the right to become wealthy, and to own many things, or at least try to.

Like separation of church and state, there must be a separation of economy and state. The state shall not pass laws that grant monopolies, give advantages to certain businesses, or provide preferential treatment to any group.

5. **The right to communicate**

Humans are communicators, and must communicate for survival. We have a right to communicate, and to employ communication technologies. It is unethical for anyone to infringe on our right to communicate.

6. **The right to use tools**

Humans are tool users, and would become extinct without tools. Our economy is tool-based, and we have the right to use tools, and to be innovative in tool creation.

Tools include medicine, money, and weapons for self-defense.

7. **The right to cooperate**

Humans cooperate and work with each other to further their survival beyond what they could achieve alone.

People should only be forced to respect the rights of others.

8. **The right to hold beliefs and to advocate**

Humans form belief systems (including religions) that create the strategies we employ to further our survival and happiness. Freedom to choose a belief systems or religion cannot be ethically denied by any entity.

The State shall not impose religion. The State shall not take on any church-related role, and church and state shall be strictly separate.

9. The right to collectively defend rights

Humans are social animals who live in hierarchical societies (nations) with leaders and followers.

There may be government, but the only ethical purpose of government must be to protect liberty and justice for all people.

Government may need to fund combatants in order to protect the liberty of the people. Governments are to serve people in general, and not specific people or Gods. Government should not pass laws that only apply to certain people, such as the lawmakers themselves, or the rich and powerful.

Humans have a just claim to dissolve their governments and to organize private militias.

Humans have engaged and will continue to engage in some very bad things, including genocide, slavery, and war. To reduce these actions, governments should have limited control over people, and should instead protect liberty.

10. The right to offspring

We have the right to choose our mates, and to pass our genetics on to our young.

We have a just claim to control of our own DNA.

11. The trivial rights

Humans have many more rights that are too numerous to list but should still be recognized as rights. These would include the right to cook food, wear funky pants, and eat peanut butter.

A new currency and new freedom

Economists say that money is a store of value, a medium of exchange, and a unit of account.

I hate to insult the entire branch of study, but it seems these economists aren't much into science.

Let's do a little empirical study of money. Take a dollar bill from your wallet and examine it closely. If you are observant enough, you will notice something very important: It is just a danged piece of paper with numbers on it.

But it is not that simple.

There has to be something special about these pieces of paper with numbers on them. And there is: They are very difficult to copy convincingly.

And so we come to a new definition of money: **Pieces of paper with numbers on them that are difficult to make realistic copies of.**

This is true, but why is it so important that money be difficult to counterfeit?

The reason is that money has a job to do. It is supposed to tell us things that are true about the state of the world.

Money can tell us:

- Who has created the most value in our economy

- If there is a shortage of rubber
- When we should grow more tomatoes.
- Whether we should work as a doctor or an artist.

All of this is **data**.

Data is "things known or assumed as facts, which make up the basis of reasoning or calculation."

And this brings us back to my definition of money:

Money is data used in a monetary system to track the contributions of each person and to help people economize.

The paramount importance of privacy

The philosopher Ayn Rand once said, "Civilization is the progress toward a society of privacy." I promise that if we all could do anything we want (with the exception of violating the rights of others) without anyone knowing about it, then we would be much happier, wealthier, and the entire society would be better off for it.

We should all strive to pursue our own happiness, and we should be able to do it privately.

Today there are people in the world who want to tell us what we can do and what we can say. This is wrong, and a violation of our innate rights.

Digital currencies give us a chance to break free of their tyranny and live as we ought. No doubt these people will try to control money for their own selfish reasons.

Now is when we must fight to establish within our societies the precedent of free and private use of digital currencies.

We must also use this money to fight against government tyranny and bureaucracy.

I urge you to learn about and use digital currencies. In doing so, you will make the world a freer place.

The future is happening now

A traditional database system has one owner. Facebook owns its databases. Your company owns its databases.

But RAIDA, blockchain and the DNS (Domain Name System, that database that makes it possible to find websites on the Internet) are forms of a new type of database that I have coined a term for: the **superbase**.

The superbase belongs to all of civilization. It belongs to the superorganism. A superbase cannot be destroyed by individuals, hackers, or even governments.

The RAIDA superbase has a huge amount of potential uses that can and will serve all of humanity. We have created **RAIDAQ** (www.RAIDAQ.com) to develop these possibilities and promote freedom. Here are some ideas we are working on:

National currencies Last year, the U.S. spent over eight-hundred million dollars producing Federal Reserve notes. More was spent combating counterfeiting.

RAIDAQ has already been contacted by interested nations that want a better currency. And no, these currencies do not need to be created by governments, but can be created by the people themselves. These deals are for hundreds of millions of dollars.

RAIDA is the only technology that can stop counterfeiting and handle the transactions of entire populations. RAIDAQ will save

nations billions each year and cause their economies to explode in productivity.

And people will have 100% privacy, with no more bank control or government manipulation.

Digital collectibles An attempt was made to use blockchain technology for digital collectibles (CryptoKitties), but the attempt failed as it overwhelmed the capacity of the Etherium network.

RAIDAQ has already partnered with Digital Frontier Marketing LLC to create Celebrium—the world's first counterfeit-proof digital memorabilia.

With this, we are now poised to dominate the $370-billion memorabilia industry.

But this is just one digital collectible possible.

Global inventory tracking A variant of RAIDA can provide a simple low-cost global tracking system that allows the ownership of goods to be tracked privately, even as those goods pass from owner to owner, ensuring that the end user gets what the supplier sent.

Private stock markets The RAIDA allows for new types of stock markets and securities. Securities that can be based on individuals, families, non-profit groups, corporations and projects. These securities can be traded privately.

Counterfeit detection in the pharmaceutical industry With the help of nano technology, we may be able to embed chips smaller than the size of a human hair that can be safely ingested.

These chips will allow for consumers of medicines to know if they are counterfeit or authentic. Knowing that a drug is real will create stronger value for the market, and will increase privacy.

Stopping the counterfeit of any physical or digital item
Using the RAIDA technology, a fool-proof method of counterfeit detection can be applied to any physical item (shoes, watches, purses, and other branded items frequently counterfeited), and to digital items (software, video games, in-game items, and movies).

We can even embed data that would allow us to determine who leaked information should digital information be stolen.

Cross-over currencies Because currencies such as CloudCoin (enabled by RAIDA) separate logic from data, it is possible to use these currencies to go from the real world into the virtual world and back (extending our economy into virtual reality).

RAIDA Data: stop the hack and keep it private Imagine that you have the addresses of one-trillion hiding places in the Internet, and that you shredded the data into stripes.

Now envision each stripe going to a different hiding place. Only the person with the addresses to these hiding places could find the data.

The addresses are kept secure with an authentication process (RAIDA) that utilizes three-factor authentication. To access your keys, you must have a certificate, a pin number, the correct biometric information. If you lose your keys, they can be sent to your email—loss proof!

The protocols for this have already been designed.

Distributed social networks Tired of having Facebook use your private information? We are now creating systems that allow

users to keep their data in un-hackable storage systems, and off of servers that can be mined.

Users will have much more privacy.

Voting systems RAIDAQ is developing new technology that can be used in elections to ensure only real voters vote, and that they only vote once.

Accounting systems CloudCoin is the first currency that can be imported into accounting systems. Already, RAIDAQ's CloudBank software will allow deposits, withdrawals, check writing, check cashing and bill pay.

This is one of RAIDAQ's major assets. But there is more.

RAIDAQ has re-invented the split tally stick—a way to record bilateral exchanges and debts privately—but in a digital version.

The hope is that it can be used to create the perfect accounting system where, internal records of debits and credits are never out of balance. It should also eventually be able to be used to create private contracts for debits and credits.

The superbase When I invented the RAIDA, I also noted that there were at least twelve other exotic data structures that have yet to be invented and developed.

We can combine the blockchain, RAIDA and these twelve others to create a new type of superorganism-owned database that will do amazing things for humanity.

RAIDAQ.com RAIDA can be used in almost any industry.

Do these ideas intrigue you? Do you have ideas of your own? All hands on board the freedom train!

Raidaq is a research corporation that is developing new technologies to further human privacy and liberty.

To find out more about this new wave of innovative products, visit

www.RAIDAQ.com.

Key words and definitions

Sometimes, when developing a new technology, it's necessary to develop a new nomenclature to describe it.

The following words are in key word sequence (instead of listing alphabetically) for easier understanding. Later definitions build on understanding of earlier definitions. If you find a term here that doesn't make sense, make sure you didn't skip over an earlier definition.

MONETARY SYSTEM	An information system. Money is data. A monetary system collects and organizes that data.
EMERGENCE	Emergence is when a collection of entities work together for enhanced survival. This is how nations develop. Emergence supports specialized skills and the development of new technologies. A good monetary system is vital in providing the organization needed for consistent and constant emergence.
SUBMERGENCE	Submergence is the the opposite of emergence. When a society has a bad monetary system, it slides into entropy and chaos because of faulty information.
CENTRALIZED MONEY	Money that's controlled from a central point. Bitcoin is an example of a centralized money system. This kind of system requires a public ledger of some sort. With this kind of system, it's very easy to track and report on any transactions. It does not provide a strong measure of user privacy.

DECENTRALIZED MONEY	Money that is not controlled from a central point. Examples are cash, gold, silver and CloudCoin.
DIGITAL CURRENCY	Currency that exists only in digital format. There is no printed version of a digital currency.
BLOCKCHAIN	A database that is duplicated thousands of times across thousands of servers as it tracks information. It is the duplication of the data, over and over, that keeps the information secure from counterfeiting.
BITCOIN	A digital currency that uses a blockchain technology to store transaction information. Bitcoin was the first digital currency.
CRYPTOCURRENCY	A digital currency that depends on encryption techniques to regulate transactions. Bitcoin is a cryptocurrency. The downside with digital currencies that depend on cryptography (encoding) is that sooner or later someone will figure out how to hack them, and they can then be stolen by the hacker.
MINT	To create new currency. The United States Department of the Treasury mints USD bills and coinage. Bitcoin is minted by miners (see below).
MINER	Someone who uses specialized software that runs on powerful computers to solve complex equations. When these equations are successfully solved, new Bitcoins are generated and awarded to the first miner to come up with the correct answer, but only after that answer has been validated by a number of other miners.
CLOUDCOIN	A perfect money system. It cannot be counterfeited, mined, overspent, or destroyed. It also fully protects the privacy of the currency's owner, as well as all transactions.

RAIDA	Redundant Array of Independent Detection Agents. This is the proprietary system that forms the basis for CloudCoin security and privacy.
RAIDA NETWORK	This is composed of 25 RAIDA clouds (clusters).
RAIDA CLOUD	A virtual network of administrators. There are twenty-five RAIDA clouds, consisting of one to thirty-two administrators for each, and a single sentinel. With RAIDA, a cloud is a single cluster.
CLUSTER	A group of separate but connected or virtually connected data storage units.
NODE	A single machine or group of machines in a cluster.
ADMINISTRATOR	Someone who administrates (manages) a single cluster in a RAIDA network.
SENTINEL	The person in a RAIDA cloud responsible for ensuring that the data stays true and available.
CONSUMER EDITION SOFTWARE	CE software is the user-friendly interface developed by the CloudCoin Consortium for the management of CloudCoins.
CLOUDCOIN JPEG	A file containing a single CloudCoin. Only 1 CC notes are JPEGs. Larger notes are stacks (see below).
CLOUDCOIN STACK	A text file containing information for multiple CloudCoins. Stack notes are available in denominations of 5, 10, 25, 100 and 250.
INTEGRITY	Integrity means *wholeness*. It comes from the Latin *in-*, meaning *not*, and *tangere*, *to touch*.
PHYSICAL INTEGRITY	In practice, physical integrity means no counterfeits, theft, loss, or possibility of system-wide failure.

LOGICAL INTEGRITY	This means that users must know who the money belongs to (entity integrity), the money must all be of the same stuff (domain integrity), and the money must refer to something that is actually there (referential integrity).
DATA INTEGRITY	Integrity means wholeness or validity. Data integrity refers to the overall accuracy, consistency, and completeness of data.
ENTITY INTEGRITY	Integrity means wholeness or validity. In a money system, entity integrity refers to knowing who (an entity) owns what.
COUNTERFEIT	An imitation of something that was created with the intent to deceive.
FAULT-TOLERANCE	A key concept in computer information system design that ensures a system will continue working even in the presence of faults in the hardware.
SUPERORGANISM	An organism made up from many organisms. The term is used most often to describe a social unit of eusocial animals or insects, where division of labor is highly specialized and where individuals are not able to survive by themselves for extended periods.
EUSOCIAL	An eusocial group is one where specialized activities are segregated for increased efficiency,
SLUCK	A concept based on “submersion due to logical errors caused by anomalous data injection.” So instead of saying that the Federal Reserve is causing inflation, it is better to say that the Federal Reserve is slucking our economy.
SUPERBASE	A database containing information that is not privately owned. RAIDA, blockchain and the DNS (Domain Name System, that database that makes it possible to find websites on the Internet) are examples.

Appendix A: How RAIDA is constructed

WARNING: Appendices are in GeekSpeak. If you're not familiar with programming terms and concepts, you might want to skip this part.

But for those of you in touch with your inner geek, you will find this stuff interesting.

———

We start by building on the **TCP/IP protocol** that forms the Internet. This technology was developed in 1973 to allow messaging even in the event that nuclear bombs wiped out major parts of the world's communication networks.

TCP/IP is a nuke-proof technology.

The Internet has never gone down on a global scale, and it never will. The TCP/IP shows us the value that good protocols can have for humanity. On top of this, we use SSL technology. **HTTPS SSL** (secure sockets layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remains private and integral.

SSL allows you to know that the servers you connect to are, in fact, the ones you want to connect to. RAIDA uses only HTTP Strict Transport Security and only passes data that is impossible to infer.

RAIDA's HTTPS usage is unhackable, and there are no known vulnerabilities. With the coming of quantum computers, this will change. But don't worry, we split the request into 25 different streams that are worthless if decrypted individually.

Also, the main goal was to make the system more expensive to hack than is worth it, and one way we will achieve this is by keeping the nominal value of CloudCoins low.

A **content delivery network** (**CDN**) is a system of distributed servers (network) that delivers web pages and other web content to a user based on the user's geographic location, the origin of the web page, and a content delivery server.

Our CDN also provides **DDoS protection** (our enterprise-class DDoS protection network has 20 times more capacity than the largest DDoS attack ever recorded.) And we are making a backup just in case.

We wish to conceal the locations of our RAIDA so that they are less vulnerable to attack. To accomplish this, we use **layers of reverse proxies**. A reverse proxy allows a server to hide. When someone requests service from the RAIDA, they go to the public server. This public server then relays the message to another server. The other server relays it to yet another, which relays it to yet another. This makes it exceptionally difficult for an attacker to even find the RAIDA.

If entire RAIDA clusters are taken offline, they can be replaced and repaired using the **Fix API.** This API repairs fractured CloudCoins. **A fractured CloudCoin is a CloudCoin that has some RAIDA servers failing authenticity**. The CloudCoin owner can request that the fractured server ask its trusted servers (neighbors) to vouch for them.

By default, each RAIDA requires three servers to vouch for a CloudCoin in order to self-repair. There are four combinations of servers that each RAIDA will trust. They will trust the three "corner" RAIDAs on any of their four corners.

With the numbers arranged in a circle like a clock, and the RAIDA that requires repair at zero, the three servers needed to trust are -1, -5, -6, or +1, -4, -5, or -1, +4, +5, or +1, +5 and +6.

RAIDA12, for example, will trust RAIDA11 AND RAIDA7 AND RAIDA6 together, OR the three other combinations of three servers. Note that the administrator for each RAIDA can change the servers that their RAIDA trusts.

To learn more about this technology, visit
www.CloudCoinConsortium.org

Appendix B: How CloudCoin works

Each CloudCoin is a JPEG image with twenty-five random **GUIDs** (**globally unique identifiers**) embedded in it that only the **password owner** can know.

Each RAIDA cloud knows only one of the twenty-five GUIDs.

When an authenticity request is sent, ownership is proven by authenticating the GUIDs in parallel with the RAIDA, using simple, free, open-source software made by the CloudCoin Consortium.

Components of the cloud currency

The three major components of the system are the **eMint**, **CloudCoin** and the **RAIDA**.

eMint: The entity that creates the CloudCoins, disperses them to the initial owners, and registers them in the RAIDA.

After the minting process is complete, the eMint is destroyed, along with any resulting data.

Once minting is complete, the number of CloudCoins in a single RAIDA network will not increase or decrease.

CloudCoin: JPEG images used as electronic money that contain codes to prevent them from being counterfeited.

The codes include:

- **SN (Serial Number)** A 32-bit number displayed in dotdecimal, like an IP address (e.g. 1.210.84.52).

The SN is used to determine the denomination of the money and help the RAIDA clouds store and protect it. The **first octet** of the SN is the network address that **shows which RAIDA** the CloudCoin belongs to. (Currently, there is only one RAIDA network. However, should CloudCoin become too valuable, the networks will be replicated so that all owners will have twice as much money as they had previously. This doubling can occur as many as eight times, with each iteration adding more fault tolerance to the system.

The **second octet** is the subnet. This allows users and software to **identify the denomination of the currency** and take measures to protect more valuable currencies.

The **last two octets are the address**. The length of the address fixes the exact amount of monetary units in the system.

- **ANs (Authenticity Numbers)** These are randomly generated binary numbers that are 16 bytes in length and only known to the owner of the currency and the disparate RAIDA Clouds.

  There are 25 ANs—one for each primary RAIDA Cloud. Parity information could be calculated based on these ANs to be stored by the RAIDA parity clouds.

- **Denomination** There is a fixed amount of each denomination of currency in the system. These denominations correspond to the subnet portion of the SN. For example, any currency with a subnet between 96 and 255 is a 250 CloudCoin unit. Denominations come in 1s, 5s, 25s 100s and 250s.

RAIDA (Redundant Array of Independent Agents)

This is a distributed storage system that works as a counterfeit detection system and provides fault tolerance, high availability

and decentralized management in order to create trust in the CloudCoin. The RAIDA has twenty-five clouds, and is designed so that if clouds go offline, new clouds can quickly be brought in to replace them.

Each cloud has a sentinel cluster that hides thirty-two detection agents behind it.

At least nine of an exact arrangement of cloud operators would need to collude, undetected, to corrupt the system. The RAIDA is unique because, unlike other authentication systems, there are twenty-five unique CloudCoin slices that authenticate in parallel. The coin need not authenticate with all of them.

RAIDA has the following components:

- **PAN (Proposed Authenticity Number)** A randomly generated 16-byte binary number created by the person taking ownership of the purportedly genuine CloudCoin.
- **RAIDA Cloud (Counterfeit Detection Agent)** A cloud-based service that verifies a CloudCoin's Authenticity Number, and that can replace it with the Proposed Authenticity Number during CloudCoin exchanges.

  The exchange process is called "password owning," which was shortened to **pown** to describe it.

  The RAIDA is logically arranged for self-repair by adding a system of triple Kerberos that allows fracked RAIDA clouds to change their stored authenticity numbers by trusting three other RAIDA clouds that also do authentication.

  The purpose is to ensure that data is not lost even if a RAIDA cloud is destroyed or unavailable. The word **fracked** was

coined to refer to a RAIDA cloud that does not authenticate a coin while all other RAIDA clouds do.

- **Counterfeit Detection Request** An encrypted message that triggers counterfeit detection and ownership change. The message includes the Denomination, Serial Number, Authenticity Number and Proposed Authenticity Number.
- **Counterfeit Detection Response** An encrypted message that tells the client whether the CloudCoin is counterfeit or authentic.

To learn more about this technology, visit
www.CloudCoinConsortium.org

Appendix C: RAIDA protocols

The RAIDA Authenticity Detection Protocol is an extremely light protocol that requires only milliseconds to execute, and sends and receives just a few hundred bytes of data.

Clients send authenticity requests in parallel to 25 RAIDA clouds. Thanks to the speed of light, it only takes milliseconds for signals to travel to the other-side of the planet and back. Each RAIDA cloud responds either with a “pass” or a “fail”.

The RAIDA protocol requires no sessions or cookies. The conditional GET method is used to reduce unnecessary network traffic.

Authenticity Request

Field	Sample
Serial Number	56298
Authenticity Number	D32BCE8DF8926EE00E1233D8C6B1363C
Proposed Authenticity Number	ACC42CDF54A5E-06A59B282799408B4B3
Denomination	1

Sample Authenticity Request

```
https://RAIDA1.cloudcoin.global/service/
detect.html?n=1&sn=56298&an=D32BCE8D
F8926EE00E1233D8C6B1363C& pan=ACC42CDF54A5E-
06A59B282799408B4B3&denomination=1detect.
```

Authenticity Response

Field	Sample
Server Name	RAIDA-12
Status	pass
Message	The unit presented is an authentic 1 unit CloudCoin.
Time	2016-09-18 15:08:07

Sample JSON Response

```
{
    "server":"RAIDA-12",
    "nn":"1",
    "sn":"56298",
    "status":"pass", "message":
    "Authentic: The unit presented is an
    authentic 1 unit CloudCoin.",
    "time":"2016-09-18 15:08:07"
}
```

RAIDA Self-Repair Protocol (Triple Kerberos)

At times, sentinels will be unavailable. Once they become unavailable, sentinels are restored or replaced.

The CloudCoins can restore them because all the authenticity data is stored in the CloudCoins themselves.

The repair protocol could be called "Triple Kerberos" because it uses three tickets. Kerberos is a network authentication protocol that works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. It is designed to provide strong authentication for client/server applications by using secret-key cryptography.

RAIDA does everything that Blockchain does, only much faster, more reliably and far more efficiently. RAIDA is scalable and more

nodes and networks can be brought on to perform all the world's transactions within milliseconds. Work is distributed among more nodes instead of requiring each node to do more work (like a blockchain).

The cost of operating one network is $40,000 per month because the there are fewer server requirements. All data can be stored in RAM.

RAIDA is 100% quantum-safe and does not use encryption. The system is fault-tolerant and can withstand government attacks, natural disasters, hackers and even internal subversion.

RAIDA is consumer-ready and does not require any client downloads except for a web page or a small client software application (under 1 MB).

RAIDA sentinels

Each CloudCoin can be sliced into 25 parts. There are 25 sub-clouds (called "crypts"). Each is responsible for one CloudCoin slice. One sentinel cluster guards each crypt. The sentinel clusters hide behind content management systems. Sentinels are distributed around the world and are located mainly in countries that are mostly liberal. The IP addresses of the sentinels are hidden, and only the content management systems know their IPs.

The sentinels each hold a directory of all the IP addresses of the detection agents in their crypt. Only the sentinels know the IP addresses of the detection agents so the locations of the detection agents are obscured. The sentinels will query the detection agents on behalf of the CloudCoins to detect counterfeits and fix fracked coins.

Independent Detection Agents

Each sentinel and detection agent is controlled by a different person. Each sentinel may use a different algorithm for dividing the load among the detection agents. Some sentinels may **shard** (divide by rows) the CloudCoin authentication data between the detection agents. Some sentinels may use a **hash or random lookup table** to divide the load.

Detection agents do not know the serial numbers of the CloudCoins that they are detecting. When random lookup tables are used, it is impossible for RAIDA administrators to assemble the CloudCoins back together.

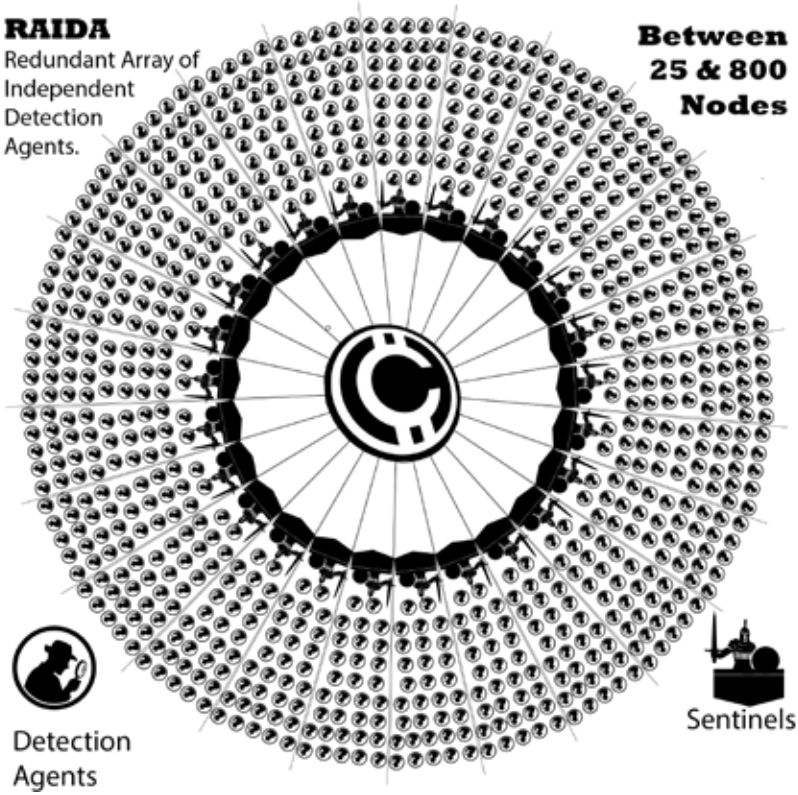
Independence: RAIDA Clouds operate under different controllers, which are not beholden to each other, but instead function as peers (equals). The clouds can use a variety of different technologies, such as Linux, Windows, PHP, C#, Java, Apache, Tomcat, IIS, MySQL, Microsoft SQL, Oracle, etc.

Distributed: With few exceptions, RAIDA Clouds are located in different liberal nations. The word "liberal" is used in the classical sense, as it was used by Philosopher John Locke to describe nations that protect life, liberty, and property. This guards the RAIDA against the actions of governments. Electricity can travel across the globe in milliseconds with no performance issues.

Redundant: RAIDA Clouds all do the same basic job. In theory, they could all go down and as long as one still worked, the CloudCoins would still be operational.

Fixability: The assumption under which this system was developed was that all of the RAIDA Clouds could potentially fail completely and have all their data hacked. That is why it is

possible to simply discard RAIDA Clouds and rebuild new ones elsewhere. The CloudCoins themselves hold the data.



Each CloudCoin is divided into 25 slices. Each slice goes to a different sentinel. Each sentinel has a directory that holds the secret IP addresses for between 1 and 32 detection agents. Each node is controlled by a different and independent entity. The sentinels and the detection agents are located in different jurisdictions. The sentinels can each decide how data is stored among its agents.

Acknowledgments

I would like to acknowledge the impact that modern-day philosopher **Stefan Molyneux** has had on my life, my family, and the ideas I've presented in this book.

After listening to Stefan Molyneux's YouTube channel for many years, I decided to self-study philosophy with my 11-year-old daughter, Victoria.

We bought a copy of **The Philosopher's Way, by John Chaffee**, and spent a year reading and talking about it. This gave me the ability to analyze old problems in new ways and make some incredible breakthroughs.

The lesson I have learned is that it is possible to drastically increase your mental abilities by learning the tools of the mind.

I would never have thought to study philosophy at the age of 47 had it not been for Molyneux. I would encourage everyone to follow him on Youtube because it could change your life too.

In this book I have borrowed some things from Stefan. The chapter title, "The Future of Your Enslavement," is a play on Stefan's Youtube video, "The Story of Your Enslavement". "In Science, Diversity is Inequality" are the words of Stefan Molyneux, and I have added my own perspective to his thoughts on this subject.

I would also like to acknowledge the writings of **Peter Schiff**. I bought his book **How an Economy Grows and Crashes** to read to

my daughter, and it made me think of my own little stories that could be told to explain difficult concepts, which I included in this book.

I hope that Stefan and Peter will find something of value here in return.

About the author

Sean Worthington is a tenured faculty member in the Computer Science Department at Butte College in Northern California. He is also a PhD candidate (all but dissertation) in Computer Information Systems.

In addition to teaching, Sean is also an inventor, with multiple patents and trademarks pending.

His unique theories on monetary systems and digital currency as a "perfect" currency are grabbing the attention of every form of media, from television and radio to social channels like Instagram.

Sean wrote his first line of code at the age of 14, on an Atari 400—one of the first home computers to hit the market.

At 16, he entered an international scientific contest. When he won, he was awarded a three-month scientific expedition to previously unvisited areas of the Australian Outback.

After serving six years in the U.S. Air Force, where he became licensed to repair jet engines (not rocket science, but pretty darned close), Sean studied Economics at California State University Chico, and later worked as an economic technician for the Yuba-Sutter Economic Development Corp.

But the pull of computer technology was strong, and he eventually returned to school for his Masters in Computer Information Systems Management.

Shortly after, he began to teach computer science while at the same time running his own network administration business.

While working on his PhD in computer science, he began to focus on counterfeit detection systems, and it was while researching for his dissertation that all the pieces of his varied past began to shape into what became a new approach to money systems, and eventually, the development of his own digital currency, CloudCoin.

Published by the CloudCoin Consortium
www.cloudcoinconsortium.org
www.cloudcoinconsortium.com

Beyond Bitcoin, the future of Digital Currency is available in trade paperback or PDF format. For additional copies, please contact cloudcoin@protonmail.com.

Please direct any other queries to cloudcoin@protonmail.com.

Published in the United States

Second edition published April 2018
First edition published October 2017

Printed in the USA

This book was produced by Precision Wordage Inc.

Cover design by Strategic Light LLC

FIND OUT MORE AT
www.CloudCoinConsortium.com