Chapter Fifteen The World's First Decentralized System for Financial and Legal Transaction

By Chris Odom

Chris Odom is Co-Founder and CTO of Monetas, the world's first decentralized system for financial and legal transactions, and the creator of the Open-Transactions digital finance suite that Monetas is based on. Open-Transactions features industry-leading innovations that solve critical problems in digital finance and addresses urgent needs in the Bitcoin economy.

The Legacy Banking System

Legacy banking systems and their associated technologies such as ACH, wires, credit cards, and merchant accounts have left users frustrated. Long durations before clearing (3-5 business days for ACH), ATM fees, temporarily inaccessible funds, regulatory burdens, and in the case of credit cards and merchant accounts, high costs and hassle, are all examples of how 20th century technology is ceasing to be tenable in the Internet age.

How did such an anachronism last so long in the first place? Would it be possible in a free market?

Regulatory capture, a form of political corruption where regulatory bodies merge with the entities they are meant to police,

has resulted in the corruption of our money. Everywhere we see rigged markets, bureaucratic banks, cycles of inflation and deflation, excessive fees, bailouts, loss of privacy, capital controls, confiscations of bank deposits (as happened in Cyprus), housing bubble, education bubble, sovereign debt bubble, and of course, unhappy users. Yet as unhappy as their customers are, banks are nevertheless reporting all-time high profits. How can this be?

Central bankers insist that "policy" must be used to "stabilize" the value of currency, and regulators insist their purpose is to "protect consumers," not to stifle competition. But if all this bureaucracy is truly superior to a free market, then why does it have to be forced onto people in the first place?

The New Money that is Coming

New technologies in money are inevitable, and will eventually work their way throughout the entire economy. Just as "software is eating the whole world" -- just as electricity did a hundred years ago -- so also new technologies in money will change our lives and our world in unfathomable ways.

What are some of the features of the money that is coming in the near future?

- Secure.
- Irreversible.
- Censorship-resistant.
- Instantaneous, Inexpensive, and International.
- Private, Apolitical and Multi-Jurisdictional.
- …yet will “embrace and extend” the legacy system.
- Extendable.
- Convertible.
- Automated.
- P2P.
- Federated.
- Largely self-enforcing.
- An eco-system.

- Will become an essential piece of infrastructure within a short time.

Convertible and Automated

Imagine being able to store your money in gold, move it in Bitcoin, and spend it in dollars, to a merchant who only receives in euros… seamlessly.

Imagine having wallet preferences with a list of accepted currencies, audited transaction servers, trusted issuers, Bitcoin pools, P2P credit lines, insurance policies, trusted auditors, pseudonymous identities, asset allocations—yet perhaps not even having to deal with those directly, because your software is self-balancing, based on your rules or rules you have subscribed to.

In the future,

- Users will be able to store their money in any currency or allocation of currencies.
- Users will be able to convert into any form, transfer in any form, and spend in any form.
- Merchants will be able to receive in any form.
- …And there will be seamless, automated currency exchange between them all.

An Eco-System

The system that is coming is not based on any one company, or any one piece of software, or in any one jurisdiction. Rather, it's an eco-system composed of many disparate entities including digital gold currencies, Bitcoin, legacy banks and fiat currencies, virtual currencies, LETS systems, and so on.

The most important pieces of the ecosystem, in no particular order, are:

- Legacy banking and fiat currencies.
- Legacy finance.
- Digital gold currencies.
- Transaction Servers.

- Business agreements and enforcement.
- Local currencies and LETS systems.
- Blockchain-based currencies such as Bitcoin. (Due to their inherent censorship-resistance.)
- Virtual game currencies. (Including, but not limited to, online gambling.)
- Currency and stock exchanges.
- Asset-based currencies (with private issuers.)
- Commodities markets.
- Derivatives markets.
- Prediction markets.
- Labor markets.
- Auction markets.
- Real Bills.
- P2P credit lines (such as Ripple.)
- Illegal markets (such as for drugs, arms, porn, or pirated products.)
- Software APIs.
- Retail merchants.
- E-Commerce.

The transformation will occur first in those areas where the new money is the most enabling, and will then be adopted by each subsequent area of the economy with increasing rapidity due to the network effect.

An Essential Piece of Infrastructure

This eco-system will become an essential piece of infrastructure in a short period of time. Just like Amazon EC2, or optical fibre, or roads, or trunk lines, or wireless spectrum.

As various different pieces of software begin to take advantage of APIs for instant, secure, seamlessly convertible, apolitical money, many different parts of our economy will quickly take advantage of the new capabilities this will provide.

The ability to transmit money in this way, at the instant API

level, is comparable in importance to the ability to transmit data itself.

As these pieces become closer and closer integrated, it will become impossible to tear down this ecosystem. Even successful attacks on individual pieces, will not disable the eco-system as a whole. It will become a basic infrastructure connecting many aspects of our economy, that could not be torn up, any more than highways or power lines would be torn up. Instead, that infrastructure will simply become a part of the fabric of reality, accepted as a fact of life by government agencies, corporations, individuals, and even software APIs.

Strong Cryptography

Strong cryptography is what makes this possible. In the 1990s, national governments were scrambling to put the "strong crypto" genie back into its bottle, but to no avail. Today, libraries like OpenSSL and GPG are built into a plethora of different products used to protect lives and data all around the world.

But some very critical capabilities, made possible only by strong crypto, have yet to make their way into common usage. The new open-source library Open-Transactions includes some of these new features:

- Unforgeable transactions, made possible using digital signatures and signed receipts.
- Un-changeable balances. Conventional "account-keeping" systems (such as PayPal or E-Gold) are able to change your account balance simply by changing an accounting entry. But Open-Transactions servers cannot change your balance, because they cannot forge your signature on the receipt.
- Untraceable cash. Open-Transactions uses "Chaumian blinding" to provide truly untraceable cash.
- Destructible receipts. In double-entry bookkeeping, the record of transactions is necessary to calculate the balance.

But Open-Transactions is able to prove which instruments are valid, and which transactions are closed, without storing any transaction history, except for the last signed receipt.

The Age of Apolitical Money

Features of new systems like Open-Transactions, such as untraceability, destructible account history, separation of powers, and jurisdictional arbitrage, all add up to much more financial privacy than has been available for decades to the typical plebe in our society. And this privacy will be enforced by mathematics and protocols, instead of legislation and courts.

Many currencies are purely virtual, and others, based on physical reserves, will be cross-jurisdictional. Entities using physical reserves (such as digital gold currencies) already employ a strategy of splitting their reserves across storage companies in multiple countries.

There are several other reasons why the ecosystem, as a whole, is 'apolitical':

- The power of strong crypto, and the inability of democratic processes to compromise or bribe it.
- The function of Bitcoin as the "universal medium" allowing fast, easy, unrestricted movement of funds in-and-out of various different systems.
- The "jurisdictional arbitrage" that occurs when you have many issuers in many different jurisdictions.
- The use of basket currencies (with insurance) to distribute a single currency across multiple issuers.
- The use of surety bonds for providing anonymous security, as that seen in the e-Cache experiment.
- The ability to have many transaction servers, with these servers also able to operate in many jurisdictions, and even on anonymous networks, in the case of "low-trust servers."

- The use of multiple jurisdictions for storage facilities of physical reserves.
- The existing services providing convertibility between virtual currencies and Bitcoins, between Bitcoins and fiat money, between Bitcoins and digital gold currencies, and between digital gold currencies and fiat, in a multitude of jurisdictions -- and in no jurisdiction at all.
- The natural competition between jurisdictions.
- The power of P2P credit lines, which will allow users to circumvent any "gatekeepers" for access to the system, by simply going through their friends. Hawala is one ancient example of this concept, which is still a powerful force in the world today.

What will ultimately happen with the U.S. Dollar of the 20th century? Nixon closed the gold window in 1971, and so our current experiment has been active for just over 40 years. History teaches us that of the 775 fiat currencies that have existed, 599 are no longer in circulation. The median life expectancy for defunct currencies is 15 years, and the average is 34 years. 1 in 5 fiat currencies have ended in hyperinflation, and even the most successful examples have lost over 99% of their original value.

What is Money?

Money is any substance that provides utility as a unit of account, a medium of exchange, and a store of value.

Over history, as people have bartered and traded, some substances have been selected for the role of money by natural market forces, based on their relative utility as a unit of account, a medium of exchange, and a store of value.

The first gold and silver coins of the Grecian age were struck in Lydia around 700 BC (in the form of electrum.) Later, silver was refined and coined in its pure form. For thousands of years, many nations used silver as the basic unit of monetary value. In some languages, such as Spanish and Hebrew, the same word means

both silver and money. In German, the same word means both gold and money.

Even today, gold is valued for monetary purposes. The largest gold depositories in the world are controlled by central banks in the major nations of the world, and it is common for portfolios to include a gold allocation for hedging against crisis, inflation, and downturns in the stock market.

The Properties of Gold

Regarding gold, it's important to keep in mind that it doesn't exactly have "intrinsic" value. Rather, gold is valued by men for its unique properties.

Gold is:

- Divisible.
- Fungible.
- Value dense.
- Recognizable.
- Durable.
- Zero counter-party risk.
- Stable in supply, yet minable.
- Liquid.
- International.
- Non-manipulatable. (Non-centralized.)

The above properties all contribute towards making precious metals uniquely suited for use as currency.

Let's compare gold to other forms of value:

- Diamonds, while valuable, are not evenly divisible, nor are they fungible. (Fungible meaning that any unit is interchangeable with any other unit, just as any dollar is identical in value to any other dollar.) Therefore we'd expect gold to be selected over diamonds by the invisible hand, for use as a currency.
- Water, while valuable and divisible, is not value-dense enough to compete with gold as a form of money, on the

free market.

- Food, while valuable, is not durable. Though neither is fiat money, in many places. (In Argentina, they say, "Cash rots faster than bananas.")
- Dollars, while liquid, do not represent zero-counter-party-risk (rather, they are debt-based.)
- Dollars, while recognizable, are not stable in supply (inflation is a worry).
- Dollars are also not minable. Control over production is limited to a banking cartel, versus gold, which anyone can produce.
- Food, which anyone can produce, cannot provide liquidity as a currency, especially in comparison to dollars or gold.
- A dollar can be manipulated in value. Even while you hold it in your pocket, the Federal Reserve board nonetheless retains the ability to manipulate its value from afar. This is not the case with gold.

The Invisible Hand

It becomes very clear that gold was never "declared" to be a form of money by any "authorities" but rather, became money due to natural market forces. The invisible hand was all that was necessary, historically, for gold to rise and to reign as money for thousands of years.

Authorities have uniformly acted, historically, to muzzle the trade of gold, to monopolize seignorage of silver, to inflate the silver via increasingly less-valuable alloys, to replace gold and silver with paper money, and even outright confiscation. But despite these pressures, gold and silver remain as premium currencies, and as veritable strongholds of wealth the world over, even into the modern day.

Artificial Forces

If gold became money strictly due to natural market forces as

a result of its unique properties, then the only reason it can have been supplanted by dollars is due to artificial restraints imposed on the market by government forces, such as legal tender legislation, tax legislation, capital controls, and money laundering legislation.

Such forces must be constantly active, otherwise, natural market forces would immediately resolve back to gold again as they have for thousands of years.

But what will happen once the forces of censorship are no longer able to restrict how we use our money?

The Rise of Bitcoin

In 2009, Satoshi Nakamoto released his landmark paper, "Bitcoin: a Peer-to-Peer Electronic Cash System." Bitcoin is not merely a new currency -- it's a whole new technology, and a commodity, rolled into one.

By early 2014, Vice President of the Federal Reserve Bank of St. Louis David Andolfatto had released a report on Bitcoin. Among other things, his report stated that Bitcoin is a "threat [to] money and payment systems" and that "enforcing an outright ban is close to impossible…. [Bitcoin] will force traditional institutions to adapt or die."

Let's consider Bitcoin's unique properties:

- Divisible.
- Fungible.
- Value dense.
- Recognizable.
- Durable.
- Zero counter-party risk.
- Stable in supply, yet minable.
- Liquid.
- International.
- Non-manipulatable. (Non-centralized.)

As we can see, Bitcoin's unique properties are like those of

gold. Additionally, Bitcoin is:

- Non-confiscatable.
- Accounts cannot be frozen.
- Anonymity is possible.
- Instantly digitally transferrable.

These new properties (non-confiscatable, non-freezable, potentially anonymous, and digitally transferrable) all serve to route-around the artificially-restrictive monetary forces in operation today that depend on government collusion with banks, and on their collective monopoly on the ability to issue, store, freeze, confiscate, track, and wire fiat money.

Does it Work?

Typically digital currency systems have a central server that controls the balances and signs off on the transaction. But Bitcoin is decentralized. Like Bittorrent, it is composed of its users who communicate directly to each other on a peer-to-peer network. So then, how is the Bitcoin network able to arrive at an agreement regarding which balances are correct and which transactions are valid?

Quite simply, other users on the Bitcoin network handle the duties of signing off on the transactions and the changes in account balance. These users are known as "miners." But how can we trust those miners to do so without lying? We cannot. Bitcoin is designed to work even when other peers are not trusted.

When a miner signs a transaction, he has to perform a proof-of-work algorithm in order to do so. Basically this means that he has to *expend some effort.* He has to *spend some money.* Put another way, he has to *crunch some numbers*. Other miners can prove whether or not he actually did his work, and if he didn't, they will ignore his message. And if the transaction is invalid in any other way, again, the other miners will just ignore it. And notice: it costs him money to be dishonest -- money he'll never get back.

Whereas if a miner operates in good faith and properly signs

transactions, he will be rewarded with transaction fees from the users, and with new coins that are uncovered by the mining process.

In short: miners are likely to *earn money* if they tell the truth, but if they lie, it will *cost them money.* Based on this principle, we may assume that more people will be telling the truth, than lying. Or more to the point, more computing power will be telling the truth, versus lying.

On the Bitcoin blockchain, the more confirmations that a transaction has, the more trustworthy it becomes. The longest chain of confirmations becomes the "truth."

A List of Things to Come

It's useful to view new technologies from the perspective of what they actually enable us to do, that we were not able to do before.

We all remember when Napster, a centralized file-sharing network, was shut down. But soon after, Bittorrent came into existence--and Bittorrent cannot be shut down, because it is decentralized. We know that if it were possible to shut it down, then it would have been shut down already. (After all, that's what happened to Napster.) But Bittorrent is censorship-resistant, and thus it cannot be shut down.

Similarly, Bitcoin provides us with a censorship-resistant, digital version of gold. It is valuable for use as money, but most importantly: it cannot be shut down.

To understand what this means, consider the now-defunct Silk Road market, and its many successors which operate on the Tor anonymous network.

Numerous sellers hawk illegal wares, mostly drugs, on these sites. Product advertisements blatantly display photographs of cocaine, crystal methamphetamine, ecstasy, and so on. If these sites were operating on a normal web server, they would immediately get shut down. But because they operate on Tor, an anonymous

network protected by strong cryptography, it's anonymous and it's extremely difficult to discover where it actually is.

Similarly, if such sites were using, say, PayPal for their payments, the sellers would all be arrested in short order. But because these sites operate using Bitcoin, no one can shut down their payment system -- it's censorship-resistant.

This is an extreme example, but that gives us a taste of the impact of this new technology in the real world. Before Bitcoin, one could not have a website selling drugs. The authorities certainly would shut down such an abhorrent operation, if they were able to. Therefore, Bitcoin is truly censorship-resistant, just as Bittorrent is. Otherwise it would have already been shut down.

Natural Law

But it would be a grave mistake to think of Bitcoin as merely a tool of for drug dealers and money launderers. This is what the media always tells us. But the currency used most by drug dealers, by far, is the U.S. Dollar, and the biggest money-launderers are conventional banks, which were (for example) recently caught laundering billions of dollars for drug lords south of the border. If the current, over-regulated financial system is not able to prevent money laundering, even with its draconian violation of our privacy, then how can it be a solution?

Bitcoin's primary feature is specifically its immunity to manipulation by bankers. This understanding is key: Bitcoin is ushering in natural law. It enables people to do things which are not in violation of natural law.

Another example is instructive: Imagine that I walk into a coin shop, and hand them a 1-ounce gold coin. They, in turn, send some Bitcoin (digitally) to a coin shop in South Africa, where my relative walks in and picks up a 1-ounce gold coin. (Paid for by the Bitcoin transfer.)

The point? Bitcoin is not just an "alternative" to gold, but rather, Bitcoin can be used for *sending* gold. In fact, it can be used

for sending any sort of value; it's a generic value-transfer mechanism. This sort of power is a great boon to the people, and a symbol of the coming democratization of wealth of the 21st century.

The real vision is a future where people have complete and total control over their own money. A future where every kind of value can easily and quickly flow from one person to another, and even from one software API to another, or from one robot to another, changing form as necessary, and stored in whatever asset allocation each user sees fit.

We're entering a future where value, like information, is able to be free.

Irreversible. The May Scale of Monetary Hardness describes the relative "hardness" of monetary instruments, based on how reversible they are.

Hardness Item

1. Street cash, Bitcoin, Gold/Silver Coins (Hard)
2. Western Union and other money transmitters
3. Account based electronic currencies fire walled away from banking system (e.g. Liberty Reserve)
4. International wires
5. bank checks
6. ACH, personal checks
7. Consumer-level electronic account transfers (e.g. Dwolla, AlerPay), Bitcoin sellers (BitInstant, MtGox etc.)
8. Business-account-level retail transfer systems, credit cards (brick and mortar) (soft)
9. Credit cards (via internet or phone)
10. PayPal (Ridiculously soft)

One of the most hated aspects of legacy payment systems is forced reversibility, which is used as a tool by the banking system to clamp down on "harder" currency systems, in favor of "softer" ones.

An example of this:

1. Customer purchases Bitcoins using dollars on credit card.
2. Merchant sends Bitcoins to customer.
3. Customer files chargeback, gets dollars back.
4. (Merchant has now lost coins AND dollars.)
5. Merchant goes out of business.

In this way, reversibility is used to clamp down on certain forms of commerce in the West. But in other parts of the world, reversibility is only an option.

For example, Alipay is the largest payment processor in China, and their transactions are irreversible by policy. Escrow *is* available, but only as an optional feature, which is used in about half of all Alipay transactions.

In the new, crypto-based currency systems such as Bitcoin and Open-Transactions, transactions are irreversible because they are based on protocols built with strong cryptography, and thus much harder currencies become available.

For example, a website for exchanging virtual game currencies can easily allow users to withdraw balances from the server in Bitcoin, since there is zero risk of chargeback. Before the invention of Bitcoin, such servers would not be able to risk the chargebacks, and thus could not allow withdrawals from the server. They could only operate using "server credits" that could not be withdrawn back out as money again. But Bitcoin solves this.

As harder currencies such as Bitcoin come into mainstream use, reversibility will be provided through escrow systems at higher layers. Escrow will be a useful option, instead of a forced property of the currency itself.

Largely Self-Enforcing

Most new business capabilities will be the sort that is able to operate without needing access to the traditional court system, due to technologies such as:

- Signed receipts and digital cash.
- Smart contracts. These provide automated enforcement of

agreements between multiple parties.

- Leading to: Virtual corporations. Software will enable corporations to issue stock, pay dividends, appoint agents, and have security over funds, all without requiring any access to legacy markets and banking systems.
- Cash-streaming protocols. When any software API needs to acquire resources from an entity it does not trust, it can simply purchase these resources in small quantities, and then purchase more when supplies are running low. Larger quantities can be purchased at a discount, as trust is built.
- Reputation tracking systems, such as web-of-trust and P2P credit lines.

Fiat money is usually instituted through legal tender laws, which consist of a government refusal to enforce any debt when the dollar-value of that debt has been paid in dollars. For example, if someone owes me an ounce of gold, and if gold is $1200/oz. on the market, then the court will consider the debt paid as long as the debtor has paid me $1200 in dollar form. Tax laws are similarly used to impose fiat money, since taxes must be paid in said fiat money.

However, Bitcoin and Open-Transactions are already able to process "smart contracts," which are custom, scripted agreements between the users, protected by strong cryptography.

This means that complex legal agreements, as well as dependable, predictable outcomes, are now possible, without requiring access to the existing court system in order to protect the security of agreements.

For the many agreements that can be processed in this way, instead of via the legacy court system, a considerable expense is avoided. Business in many areas will thus be able to operate at much lower levels of risk, especially wherever business processes and payments can be built into the software directly.

The Untraceable Future

In 1983, David Chaum released his seminal paper, "Blind signatures for untraceable payments" which outlined a method for using public key cryptography to make a truly untraceable form of digital cash. The technology lay dormant under patent for several decades, and its greatest promise seemed undone by its Achilles heel: the fact that digital cash systems still required a legal entity to serve as the currency issuer. After all, someone has to hold the gold.

This plain fact, that "someone still has to hold the gold," was the undoing of e-Gold, Ltd, a formerly-promising Internet-based gold currency, who eventually saw their customers' gold confiscated by federal authorities. But new systems, like Open-Transactions, are being designed to enable separation of powers, basket currencies, and jurisdictional arbitrage. And some systems, like Bitcoin, have no physical reserves at all.

Further complicating matters was e-Gold's database and resulting ability to track and reverse payments, which stuck them with the liability of tracking and reversing any "fraudulent or suspicious transactions" which had occurred on their system. The founder of e-gold, Douglas Jackson, is still wearing an ankle bracelet for his trouble. But the persecution of Jackson only served to drive the development of systems that were not so vulnerable; these new systems are being designed specifically to reduce liability for operators.

Limited Liability

Newcomer Voucher-Safe proposes to reduce operator liability through a separation of powers between the transaction servers and each actual currency issuer. After all, if the currency, once issued into circulation, passes entirely outside of the control of its issuer, then that issuer cannot be held liable for how its currency is used after that point, any more than the Federal Reserve itself could be held liable for how its dollars are used, once they have

passed into general circulation.

The persecution of older systems like e-Gold is what drove the development of new systems such as Voucher-Safe, in the same way that shutting down Napster drove the creation of Bittorrent. And this process is accelerating, as a wave of financial crisis sweeps the world. The more that authorities devalue their fiat currencies, and clamp-down on their movements, the more that technological alternatives are driven to grow and adapt -- and the more their adoption is driven in the general population.

Homomorphic Cryptography

Untraceable cash, based on blind signatures, is just one form of homomorphic cryptography. But it's also possible to encrypt transaction amounts as well, so that a piece of software can process transactions without even being able to see the amounts that are being transacted.

E-Gold was made responsible to report on account balances and transaction amounts. But what if, due to homomorphic crypto, the "e-Gold of the future" is able to process transactions, without even knowing what the amounts and account balances are?

E-Gold was held liable to report on where payments were coming from, and to whom they were going. But what if, due to blind signatures, the "e-Gold of the future" is unable to see such things?

Even more: what if the "e-Gold of the future" is itself able to operate anonymously on darknets such as Tor? What if these systems can serve us, yet without having to trust them?

An Epoch in History

The new money that is coming is likely to succeed first in developing countries, where it adds the most value; where currency inflation is most prevalent, where price-gouging is commonly perpetrated by remittance services, and where Rule of Law is generally less accessible to the common man.

We stand at an epoch in history. The typical person today is Han Chinese, earns around $10,000 per year, and does not have a bank account -- yet he does have a mobile phone.

If the availability of value-transfer software on that device makes it easier to store and exchange value than legacy alternatives, then it will only be a matter of time before that device usurps the role entirely. Already 95% of Kenyan adults use M-Pesa, a phone-based currency system, as their primary form of money.

70% of new smartphones are already running the Android operating system, where any user can already download Bitcoin and related applications. How long before destructive events such as the Zimbabwean Inflation become mere artifacts of history?

Magic Technologies

The various properties of these digital cash algorithms can also be combined with one another, creating a whole greater than the sum of its parts.

For example, Bitcoin mixer services have already sprouted offering digital cash instruments that combine the censorship-resistance of Bitcoin with the untraceability of David Chaum's digital cash. Different technologies will be layered together, creating an eco-system with far more power than any of its constituent parts.

It's hard to predict what will happen to the social and political landscape, once the "common man" has easy access to untraceable and censorship-resistant money, and when such money is built into everything around us. Automated resource allocation will impact all sectors, and shape the growth of up-and-coming industries such as robotics, 3D printing, and self-driving cars.

...And it's coming soon.