DGC Magazine

Breaking News:

H.R. 2487 --the overwhelming new reason to use DGCs instead of a U.S. Bank p.18

August 2010

Recommended Exchanger

SwapGold

fast • secure • global

- official exchanger of all major e-currencies
- trusted by thousands since 2006
- best rate to buy/sell/convert e-currencies
- very fast processing

https://www.SwapGold.com

Are you afraid that your hard-earned money will get...

- ✓ cheated by exchangers who are scammers?
- ✓ mishandled by small & inexperience exchangers who cannot handle large amounts?
- ✓ delayed by exchangers with lousy service & support that takes days to reply you?

Here are 3 top reasons why thousands of customers trust us since January 2006:

1 We are legal & reputable

- We are a legally registered company in Singapore.
- We have been extensively verified by reputable authorities.

2 We are experienced & efficient

- You are served by an experienced team operating daily & serving thousands of customers since January 2006.
- Our team earned 100% praises & zero complaints on public forums & blogs since January 2006.

3 We value your privacy & security

- Your orders are insured with a US$1 million warranty by Comodo.
- We use SSL-encryption on our entire site to protect your privacy & security.

Therefore, you can have an absolute peace of mind when you use our services.

http://www.swapgold.com

https://www.swapgold.com

Pamela Fayed's Alleged Killer Now Under Arrest

Steven Vicente Simmons(the alleged stabber) and Gabriel Jay Marquez pleaded not guilty to murder & conspiracy charges in Los Angeles County Superior Court Wednesday[6/28/10] for the killing of Pamela Fayed Goudie two years ago.

Pamela Fayed was stabbed to death on July 28, 2008, in Los Angeles as she left a meeting between attorneys and James Fayed.

Marquez and Simmons also both face the special circumstance allegations of murder for financial gain and lying in wait. Prosecutors have not yet decided whether to seek the death penalty.

James Fayed, the former owner/operator of Goldfinger Coin & Bullion Inc in Camarillo, parent company of e-bullion.com, and his former employee, Jose Luis Moya, are also charged in the murder-for-hire scheme.

The e-bullion.com website was taken down for a 4-hour "maintenance" window at 1PM Pacific, August 5, 2008 and is now defunct. FBI agents on the case also claimed during a press conference that e-bullion was a ponzi.

Left, James' booking photo and Pamela's DL pic
Below, Pamela and daughter Desiree
Bottom, 2008 funeral services

editor@dgcmagazine.com
Skype IM 'digitalcurrency'
http://twitter.com/dgcmagazine
DGC Magazine is published online 12 times a year. Subscriptions are free. Industry ads are free.

Anybody Seen Our Gold?

The gold reserves of the United States have not been fully and independently audited for half a century. Now there is proof that those gold reserves and those of other Western nations are being used for the surreptitious manipulation of the international currency, commodity, equity, and bond markets. The objective of this manipulation is to conceal the mismanagement of the U.S. dollar so that it might retain its function as the world's reserve currency. But to suppress the price of gold is to disable the barometer of the international financial system so that all markets may be more easily manipulated. This manipulation has been a primary cause of the catastrophic excesses in the markets that now threaten the whole world. Surreptitious market manipulation by government is leading the world to disaster. We want to expose it and stop it.

Who are we?
We're the Gold Anti-Trust Action Committee Inc., a non-profit, federally tax-exempt civil rights and educational organization formed by people who recognize the necessity of free markets in the monetary metals. For information about GATA, visit http://www.GATA.org

GOLD ANTI-TRUST ACTION COMMITTEE INC.
7 Villa Louisa Road, Manchester, Connecticut 06043-7541 USA
CPowell@GATA.org
GATA welcomes financial contributions, which are federally tax-exempt under Section 501-c-3 of the U.S. Internal Revenue Code. GATA is not a registered investment adviser and this should not be considered investment advice or an offer to buy or sell securities.

GATA

WebMoney Keeper Mobile - Stay Paid. Be Mobile.

http://www.wmtransfer.com
http://www.webmoney.ru

telepat
www.telepat.com

Open Spaces

The most successful tyranny is not the one that uses force to assure uniformity but the one that removes the awareness of other possibilities, that makes it seem inconceivable that other ways are viable, that removes the sense that there is an outside.

-- Allan Bloom, "The Closing of The American Mind"

by Paul Rosenberg

As I was planning this article, I received a report that Wikipedia had deleted their page on Bitcoin, a new electronic cash program. I checked and found that the page was deleted by a specialist in glaciers and global warming called 'polargeo.' His reason for deleting it was "lack of third party significant coverage."

I immediately went to AltaVista and found 131,000 hits on Bitcoin. Nope, no significant third-party coverage there!

I've never been inside of Mr. PolarGeo's head, but it's a pretty good guess that he suffers from the usual gatekeeper's syndrome: I must destroy anything from outside.

This is what we're up against in the DGC business – we come from outside, not from inside. That makes a lot of people uncomfortable. Bear in mind that this has absolutely nothing to do with our virtues or lack thereof. We are from outside, and that scares people for deep reasons that they don't understand and can't articulate.

I think most of us understand quite well what outside means: Things that are not within our group's accepted mental and emotional framework; not already approved by the tribe. By early adulthood, almost all of us understand these limits; we know which thoughts are acceptable and which are not. Things outside of those limits are seen as "strange." If they persist, they become "dangerous."

The great problem, of course, is that no progress is possible from inside – Inside is a stasis field.

OPEN SPACES

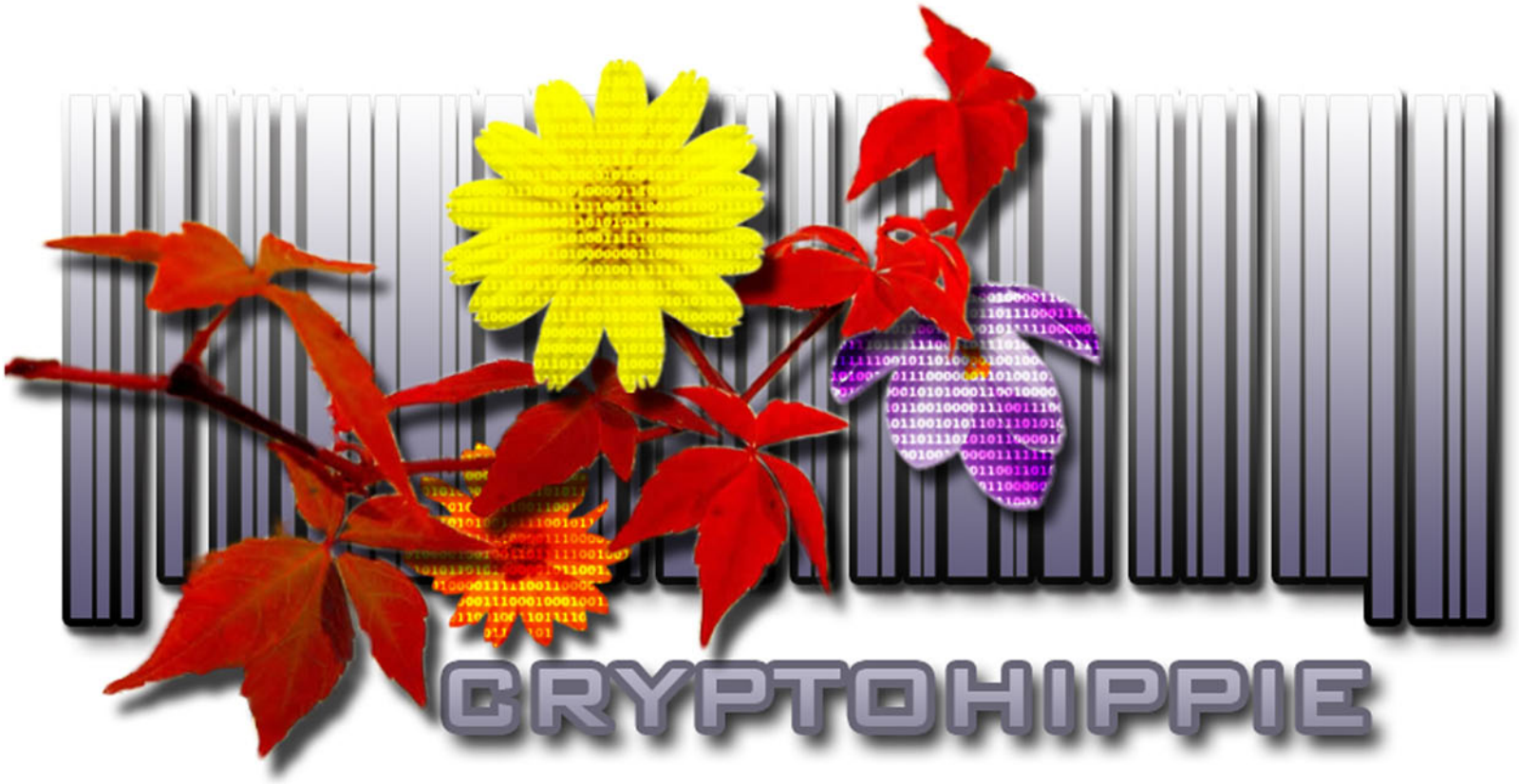
Advances which permit [poverty] to be exceeded… are the work of an extremely small minority, frequently despised, often condemned, and almost always opposed by all "right thinking" people.
-- Robert A. Heinlein

Open space – Outside – is where all the cool and useful things come from. At least in the West, it has always been that way and continues to be that way: Einstein was a hapless patent clerk, Tesla was a crackpot immigrant, Jesus was a wandering teacher without education, backing or respect.

So it goes, as it has always gone. Outside may include a lot of strange flora and fauna, but that's where life actually takes place. Inside features mere survival and endless, enforced mediocrity.

However they can find open space, creative people tend to install themselves there, and they tend to flourish there. Certainly they have their own problems, and success in their endeavors is by no means certain, but at least they have a chance to do something different in the open space.

The great problem facing any creative person in this world lies in finding open space. Sometimes "open space" may be a physical place, such as the America frontier settlements of the 17th and 18th Centuries.



- VPN anonymous surfing
- Anonymous email
- CryptoRouters
- Closed-Group Networks
- Encrypted and distributed data storage
- Multi-hop routing
- Multi-jurisdictional structure
- New products in development

http://www.cryptohippie.com

Peace of Mind – Second to Nothing

Other times it may be an intellectual open space, such as the Scottish Enlightenment. Of course there have been many small open spaces, sometimes as small as a single household.

And, sometimes, there is a period of time, when the old rules crumble in some significant way…

IN PRAISE OF THE 60s

Once upon a time there was a boy named Ted, and when his mother said, "Ted, be good," he would.
-- The Beatles

As much as I complain about the 60s and the early 70s, I'll give them this: They weren't boring. The intellectual life of most people today is unspeakably dull.

Yes, in many ways the idiots and jerks won the big arguments of the 1960s, and a lot of questionable and harmful things were idolized by stupidly rebellious people. But at least there were real arguments. There were communists and objectivists, free-lovers and Jesus freaks, nature-worshippers and NASA nerds, all mixed together. Most people today have no opinions at all, and they definitely have no courage to stand up for anything that hasn't been stamped and approved by the drone-masters. So, give the 60s the credit they are due.

The craziness of the 60s created open spaces where new ideas could form and compete. A lot of those ideas were ridiculous, and the open space gave every wack-job with a re-heated lunacy from the past a chance to trumpet it as a major revelation; but at least they were thinking and saying something!

The young people today are still playing the best songs from the 60s and 70s, and it is not because they are nostalgic for their parents' youth; they would certainly be playing their own music, if most of it didn't stink. Loud and vile is a pretty lame substitute for new and creative. And some idiot girl jumping around shaking her goods isn't music, it's porn.

I hesitate to even mention films. Aside from a few wonderful interruptions like V For Vendetta, Children Of Men and Serenity, they are almost invariably formulaic crap. Swing that camera around fast and blow things up. Maybe a few boob shots too… "Oh yeah, we're pushing the envelope!" It could make you vomit. Hurry, Spider Man 46 is at a theater near you!

The Beatles lyric at the top of this section was sung an insult in the 60s. Now, the televised script induces everyone to put on their bicycle helmets, recycle their plastics, wear the proper colored wrist bands, then find a place in the big game and hold it quietly. It's surprising that more of them don't drive off cliffs out of simple boredom.

We live in a world featuring a hundred substitutes for living, a thousand images of living, endless outward shows of living, but no actual life. Modern citizens (and, yes, I am using that as an insult) never experience more than the mundane. The 60s, goofy as they were, look pretty good in comparison.

WHAT TO DO

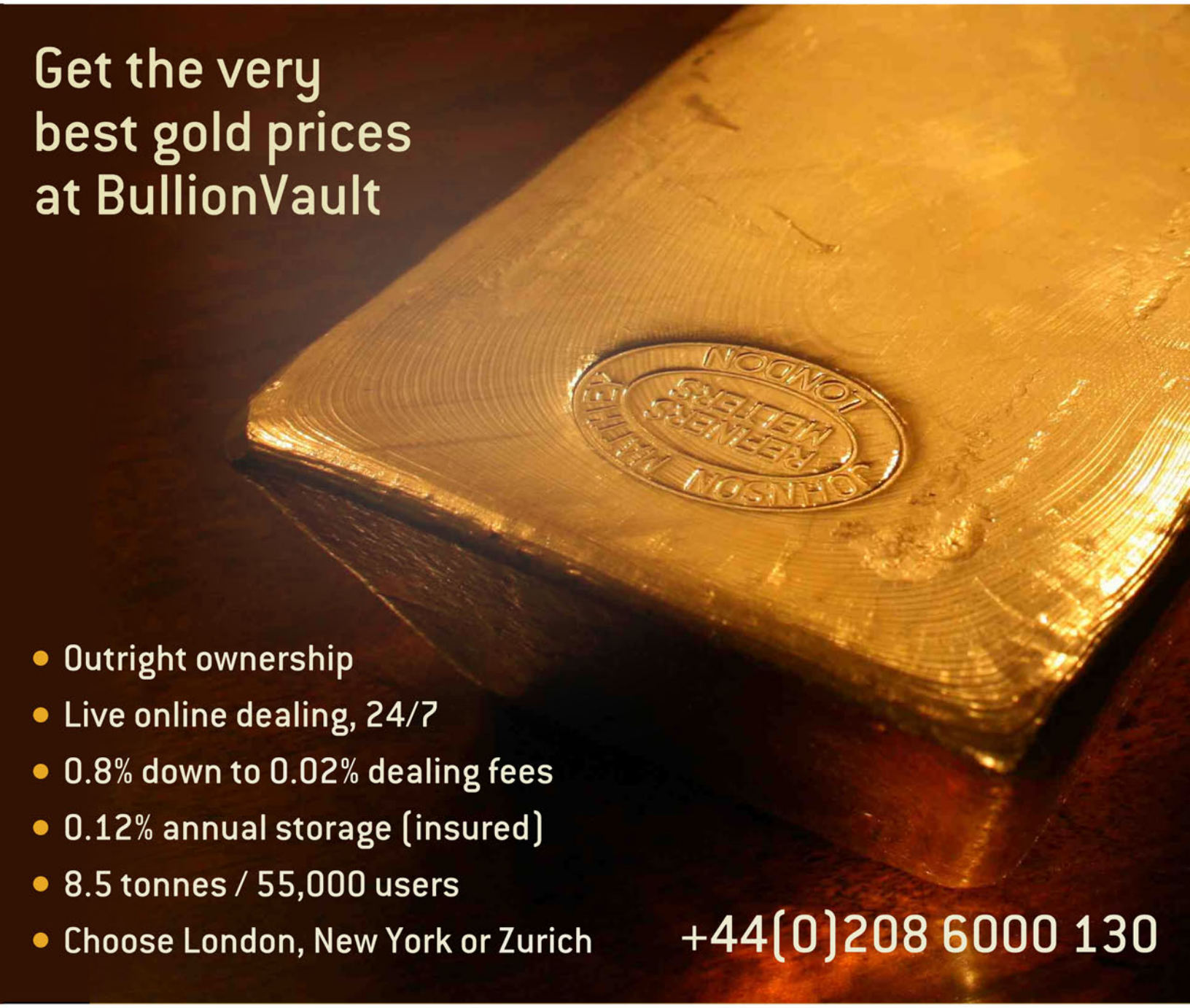
I wouldn't rant like this to many other groups, but the DGC business is full of people who have already stepped away from the televised script – you guys grok my message, if I may play with an old 60s word.

So, let the heathen rage. Let the ignorant and fearful call you names. Just keep moving forward. In so doing, you are being true to yourself and your own, human nature. We are creators, not by vocation, but by our very nature. All humans are, though many have not yet learned this lesson.

Find your open spaces, create new ones at every opportunity, defend them as required, but by all means keep creating. Whether we put this concept into economic terms (creating value), common vocabulary (prospering) or theological language (bearing fruit), we must continue to create – that is the end for which all of us are designed, whether we realize it or not.

Paul is the author of A Lodging of Wayfaring Men, Production Versus Plunder and other books. You can find them at
http://www.veraverba.com

Ready to Buy Gold?



BullionVault.com

Professional Gold for Private Investors

http://www.bullionvault.com

LBMA MEMBER
www.lbma.org.uk

World Gold Council Acquires Equity in BullionVault

Launched in 2005, BullionVault is an online service offering consumers convenient digital bullion accounts. Consumers purchasing gold and silver though BullionVault own the allocated physical gold and silver, not some paper representation. The digital gold platform currently has more than 18,000 accounts and those customers are spread through almost 100 countries around the globe. BullionVault holds 20.168 metric tons of gold for investors in vaults in London, Zurich and New York plus 62.857 tons of silver in London. The precious metal holdings are valued today at about $800million USD. The average holding in any one customer account is said to be around $47,000 dollars.

On June 21st several prominent news services reported that the World Gold Council through the Lord Rothschild-backed Agmentum Capital had completed a £12.5 million investment in Galmarley Ltd., which owns and trades as BullionVault.com. Additionally, Tim Levene, partner at Augmentum, and Marcus Grubb, managing director of investment at the World Gold Council, will join the board of BullionVault.

According the the WGC, Augmentum is a private equity fund focused on technology investments which was formed only last year. The fund is backed by U.K. financier Jacob Rothschild operating through RIT Capital Partners Plc. and RIT trust is listed on the FTSE.

The World Gold Council's new investment in BullionVault is part of its strategy of "increasing its portfolio of successful platforms for gold investment," says Marcus Grubb, managing director of investment at the WGC.

While BullionVault has experienced tremendous success and growth in the past several years it is very small in comparison to the WGC's gold exchange-traded fund which now has around 1,306 tonnes of the metal under management worth more than $50 billion dollars.

As the Perth Mint's Bron Suchecki recently pointed out in an article on the Citizen Economists blog http://www.citizeneconomists.com/, the IAMGOLD Corporation which is also a WGC member is a shareholder in James Turk's GoldMoney. GM is sometimes seen as a competitor of BV.

Congratulations to BullionVault on their new business deal.

http://www.bullionbullscanada.com

GoldMoney

The best way to buy gold & silver

YOUR GOLD HOLDING

Secure • Convenient • Trustworthy

goldmoney.com

Tel: +44-1534-511-977 • Fax: +44-1534-511-988

http://www.goldmoney.com

Bitcoin's Star Is On The Rise

Bitcoin is an open source, P2P network based digital currency which is sometimes called an "electronic cash system" developed by Satoshi Nakamoto

"I've developed a new open source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust."

The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible.

A generation ago, multi-user time-sharing computer systems had a similar problem. Before strong encryption, users had to rely on password protection to secure their files, placing trust in the system administrator to keep their information private. Privacy could always be overridden by the admin based on his judgment call weighing the principle of privacy against other concerns, or at the behest of his superiors. Then strong encryption became available to the masses, and trust was no longer required. Data could be secured in a way that was physically impossible for others to access, no matter for what reason, no matter how good the excuse, no matter what.

It's time we had the same thing for money. With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless.

One of the fundamental building blocks for such a system is digital signatures. A digital coin contains the public key of its owner. To transfer it, the owner signs the coin together with the public key of the next owner. Anyone can check the signatures to verify the chain of ownership. It works well to secure ownership, but leaves one big problem unsolved: double-spending. Any owner could try to re-spend an already spent coin by signing it again to another owner.

The usual solution is for a trusted company with a central database to check for double-spending, but that just gets back to the trust model. In its central position, the company can override the users, and the fees needed to support the company make micropayments impractical.

Bitcoin's solution is to use a peer-to-peer network to check for double-spending. In a nutshell, the network works like a distributed timestamp server, stamping the first transaction to spend a coin. It takes advantage of the nature of information being easy to spread but hard to stifle. For details on how it works, see the design paper at http://www.bitcoin.org/bitcoin.pdf (see the back of this issue)

The result is a distributed system with no single point of failure. Users hold the crypto keys to their own money and transact directly with each other, with the help of the P2P network to check for double-spending.

Satoshi Nakamoto
http://www.bitcoin.org

P2P means that there is no central authority to issue new money or keep track of transactions. Instead, these tasks are managed collectively by the nodes of the network. Advantages:

- ***Transfer money easily through the Internet, without having to trust middlemen.***
- ***Third parties can't prevent or control your transactions.***
- ***Bitcoin transactions are practically free, whereas credit cards and online payment systems typically cost 1-5% per transaction plus various other merchant fees up to hundreds of dollars.***
- ***Be safe from the instability caused by fractional reserve banking and bad policies of central banks. The limited inflation of the Bitcoin system's money supply is distributed evenly (by CPU power) throughout the network, not monopolized by the banks.***

Bitcoin development is hosted at SourceForge.
http://sourceforge.net/projects/bitcoin/

Writing for InfoWorld.com Mr. Neil McAllister has a recent article which includes a nice section on Bitcoin.

Open source innovation: Bitcoin

Alternative currencies for e-commerce have been attempted many times, but never one quite like Bitcoin. Its creator, Satoshi Nakamoto, has dubbed it a "cryptocurrency," because it relies on public/private key cryptography to facilitate electronic trading in a completely anonymous, secure, peer-to-peer fashion.

Read more on page 3 of the article:
http://www.infoworld.com/d/open-source/open-source-innovation-the-cutting-edge-582?page=0,2

The New Liberty Standard has a nice wiki type web site with Bitcoin information. The following info is from this web site.
http://newlibertystandard.wetpaint.com/
Bitcoin is the gold standard of digital currency. The availability of bitcoins can not be manipulated by governments or financial institutions and bitcoin transactions occur directly between two parties without a middleman.

HOW TO
Try using bitcoins the next time you need to send or receive a payment over the Internet.

First, download the Bitcoin software. Once Bitcoin is running, click 'Generate Coins' which will pay you bitcoins in exchange for your computer working to validate bitcoin transactions.

Check the exchange rate to calculate how many bitcoins need to be sent. The payer can purchase additional bitcoins if needed.

The payer's previously generated bitcoins allow for a lower out of pocket payment. The payer then sends the bitcoins to the receiver using the Bitcoin software.

The receiver can then sell their bitcoins for dollars. The receiver's previously generated bitcoins allow a higher dollar payout.

###

The Bitcoin Cottage Industry

An updated list is here: http://www.bitcoin.org/trade

- https://www.bitcoinmarket.com/

Bitcoin Market is a real-time marketplace for the exchange of Bitcoins. It functions like a commodity exchange or stock market, where buyers and sellers continually speculate on the price of Bitcoins.

WHY IS BITCOIN MARKET NECESSARY?
Like all commodities, the value of Bitcoins will fluctuate over time as supply and demand change. This market will create a real-time Bitcoin-to-Dollar exchange rate. Bitcoin Market WILL NOT CONTROL the exchange rate or the issuance of new Bitcoins. It is to bring Bitcoin traders together. The traders' actions will determine the exchange rate. The issuance of new Bitcoins is an altogether separate matter determined by the Bitcoin program.

http://www.anglofareast.com

established 1991

Anglo Far-East.
"The Original"
Gold and Silver bullion custodian.

www.anglofareast.com

Contact:

+1 206 905 9961 USA
+ 507 264 0164 Panama
+ 64 9337 0715 New Zealand
+ 61 8 8334 6855 Australia
+ 41 43 500 4218 Switzerland
+ 44 208 819 3911 UK
+ 852 8124 1265 Hong Kong

Email: astanczyk@anglofareast.com

ARE YOU THE BROKER OR THE MARKET?
Both.

HOW ANONYMOUS IS YOUR SERVICE?
Buyers will send payments directly to sellers. If you don't want the world to know your addresses or account numbers, you may not want to use this service. Generally, I have come to the following conclusion. No exchange method is going to be as anonymous as using Bitcoins exclusively. However, many people choose to be more anonymous or less anonymous depending on the situation. Bitcoin allows you to have as many identities as you deem necessary. The opportunities are bounded only by your imagination.

WHAT IF THE BUYER REFUSES TO SEND PAYMENT?
The buyer does not receive the Bitcoins until the seller confirms payment. If no payment is sent, I will issue a Bitcoin refund to the seller, in the full amount.

TRADING USD FOR BITCOINS? DOESN'T THAT DEFEAT THE PURPOSE OF USING BITCOINS IN THE FIRST PLACE?
No. First of all, Bitcoins are a new currency. No one will trust a new currency unless it can be exchanged for other types of currency. Secondly, all forms of currency are traded relative to other currencies. It's basic human nature to be diversified. Thirdly, Bitcoins are entirely electronic and not physical. Physical payment exists everyday off of the Internet. There will always be a need to exchange Bitcoins for physical currency to conduct physical transactions.

https://www.bitcoin4cash.com/
Welcome to the most anonymous way to buy and sell Bitcoins. If you are new, we recommend that you read the F.A.Q. It will answer most of the questions that you probably have about the service including security, privacy, liability, and legalities.

https://www.mybitcoin.com
MyBitcoin is a web-based wallet service for Bitcoin. With MyBitcoin you can easily send and receive Bitcoin payments from any web-enabled device, including most mobile phones.

https://mtgox.com/
Mt Gox is an exchange. It allows you to trade US Dollars (USD) for Bitcoins (BTC) or Bitcoins for US Dollars with other Mt. Gox users. You set the price you want to buy or sell your BTC for. Mt Gox allows you to trade US Dollars (USD) for Bitcoins (BTC) or Bitcoins for US Dollars. You are trading with other users of Mt Gox. Mt Gox does not act as a counter party to any trades. The price you buy or sell bitcoins for is up to you. If there is no one that will currently except your offer then your offer will be saved and the trade will happen once someone comes along and accepts your offer.

http://www.bitcoin.org/smf/index.php
The Bitcoin Forum
Learn More....What are Bitcoins?
http://www.bitcoin.org

A Message From Mark

Welcome to the USSA?

In the January 2010 issue of DGCmagazine I published an interview with DGCs man of the year, Mr. James Turk. In the interview I asked him this question regarding capital controls.

DGC: In 1963 President Kennedy implemented the Interest Equalization Tax, which, "..was meant to make it less profitable for U.S. investors to invest abroad by taxing[15%] the interest on foreign securities." Wasn't that just a form of capital control, trying to restrict the flow of money in or out of the country and could the U.S. be looking ahead at similar controls in order to keep all those foreign held U.S. dollars from returning to America?

Turk: Yes, that is exactly how I see it. I even mentioned in my October 2003 Barron's interview the likelihood of capital controls being imposed before this bust is over. We cannot predict what form those controls will take, but we can read from monetary history, that rather than reverse course and pursue sound money policies, governments impose capital controls to try to buy more time. The controls you mention from President Kennedy bought time, but only until the Johnson administration, when years of money mismanagement by the Federal Reserve along with new bad policies being imposed caused the dollar to unravel.

On the next page, is the Zerohedge introduction to the 2010 "Capital Control Act". Perhaps this is even the best reason to use digital gold currency instead of a U.S. Bank?

It's Official - America Now Enforces Capital Controls

Source: http://www.zerohedge.com/article/its-official-america-now-enforces-capital-controls 03/28/2010

It couldn't have happened to a nicer country. On March 18, with very little pomp and circumstance, president Obama passed the most recent stimulus act, the $17.5 billion Hiring Incentives to Restore Employment Act (H.R. 2487), brilliantly goalseeked by the administration's millionaire cronies to abbreviate as HIRE. As it was merely the latest in an endless stream of acts destined to expand the government payroll to infinity, nobody cared about it, or actually read it. Because if anyone **had** read it, the act would have been known as the **Capital Controls Act**, as one of the lesser, but infinitely more important provisions on page 27, known as Offset Provisions - Subtitle A—Foreign Account Tax Compliance, institutes just that. In brief, the **Provision requires that foreign banks not only withhold 30% of all outgoing capital flows (likely remitting the collection promptly back to the US Treasury) but also disclose the full details of non-exempt account-holders to the US and the IRS.** And should this provision be deemed illegal by a given foreign nation's domestic laws (think Switzerland), well the foreign financial institution is **required to close the account**. It's the law. If you thought you could move your capital to the non-sequestration safety of non-US financial institutions, sorry you lose - the law now says so. **Capital Controls are now here and are now fully enforced by the law.**

Let's parse through the just passed law, which has been mentioned by exactly zero mainstream media outlets.

Here is the default new state of capital outflows:

(a) IN GENERAL.—The Internal Revenue Code of 1986 is amended by inserting after chapter 3 the following new chapter:

''CHAPTER 4—TAXES TO ENFORCE REPORTING ON CERTAIN FOREIGN ACCOUNTS
''Sec. 1471. Withholdable payments to foreign financial institutions.
''Sec. 1472. Withholdable payments to other foreign entities.
''Sec. 1473. Definitions.
''Sec. 1474. Special rules.
''SEC. 1471. WITHHOLDABLE PAYMENTS TO FOREIGN FINANCIAL INSTITUTIONS.

''(a) IN GENERAL.—In the case of any withholdable payment to a foreign financial institution which does not meet the requirements of subsection (b), **the withholding agent with respect to such payment shall deduct and withhold from such payment a tax equal to 30 percent of the amount of such payment.**

Clarifying who this law applies to:

''(C) in the case of any United States account maintained by such institution, to report on an annual basis the information described in subsection (c) with respect to such account,
''(D) to deduct and withhold a tax equal to 30 percent of—
''(i) any passthru payment which is made by such institution to a recalcitrant account holder or another foreign financial institution which does not meet the requirements of this subsection, and
''(ii) in the case of any passthru payment which is made by such institution to a foreign financial institution which has in effect an election under paragraph (3) with respect to such payment, so much of such payment as is allocable to accounts held by recalcitrant account holders or foreign financial institutions which do not meet the requirements of this subsection.

What happens if this brand new law impinges and/or is in blatant contradiction with existing foreign laws?

The Worlds Local Exchanger

Gold Now

US: +1 (213) 341-1583
CA: +1 (418) 210-3942
MX: +52 (0) 55 535-11-443
UK: +44 (0) 208 150-6659
FR: +33 (0) 4 886-70-302
IE: +353 (0) 766-153-669
AU: +61 (0) 3 9017-1975
NZ: +64 (0) 9 974-2009
US Fax: +1 (213) 559-8555
Skype: goldnow
Email: kelly_clan@fastmail.fm

www.GoldNow.St

CENTREGOLD

Buy digital currency with credit card

Some of the advantages of having gold "in digital form" are the ability of paying with it, the ability of seeing the balance at any time, while also seeing what that balance is currently equivalent to in terms of fiat currency value.

As well as being able to sell it quickly while being located anywhere on Earth, and having no need to physically carry it with yourself.

Get your real gold in digital form, as well as other types of Digital Value Units (or Digital Currency) via http://centregold.ca, where speed and quality merge together.

Update: and now, buy WebMoney with credit cards and bank wires!

http://cg2wm.com.

Update: new and very demanded payment methods are coming.

Go and see it yourself.

http://centregold.ca

‘‘(F) in any case in which any foreign law would (but for a waiver described in clause (i)) prevent the reporting of any information referred to in this subsection or subsection (c) with respect to any United States account maintained by such institution—
‘‘(i) to attempt to obtain a valid and effective waiver of such law from each holder of such account, and
“(ii) if a waiver described in clause (i) is not obtained from each such holder within a reasonable period of time, to close such account.

Not only are capital flows now to be overseen and controlled by the government and the IRS, but holders of foreign accounts can kiss any semblance of privacy goodbye:

‘‘(c) INFORMATION REQUIRED TO BE REPORTED ON UNITED STATES ACCOUNTS.—
‘‘(1) IN GENERAL.—The agreement described in subsection (b) shall require the foreign financial institution to report the following with respect to each United States account maintained by such institution:
“(A) The name, address, and TIN of each account holder which is a specified United States person and, in the case of any account holder which is a United States owned foreign entity, the name, address, and TIN of each substantial United States owner of such entity.
“(B) The account number.
“(C) The account balance or value (determined at such time and in such manner as the Secretary may provide).
“(D) Except to the extent provided by the Secretary, the gross receipts and gross withdrawals or payments from the account (determined for such period and in such manner as the Secretary may provide).

The only exemption to the rule? If you hold the meager sum of $50,000 or less in foreign accounts.

‘‘(B) EXCEPTION FOR CERTAIN ACCOUNTS HELD BY INDIVIDUALS.—Unless the foreign financial institution elects to not have this subparagraph apply, such term shall not include any depository account maintained by such financial institution if—
‘‘(i) each holder of such account is a natural person,and
“(ii) with respect to each holder of such account, the aggregate value of all depository accounts held (in whole or in part) by such holder and maintained by the same financial institution which maintains such account does not exceed $50,000.

And, while we are on the topic of definitions, here is how “financial account” is defined by the US:

‘‘(2) FINANCIAL ACCOUNT.—Except as otherwise provided by the Secretary, the term ‘financial account’ means, with respect to any financial institution—
“(A) any depository account maintained by such financial institution,
“(B) any custodial account maintained by such financial institution, and
“(C) any equity or debt interest in such financial institution (other than interests which are regularly traded on an established securities market). Any equity or debt interest which constitutes a financial account under subparagraph (C) with respect to any financial institution shall be treated for purposes of this section as maintained by such financial institution.

In case you find you do not like to be subject to capital controls, you are now deemed a “Recalcitrant Account Holder.”

“(6) RECALCITRANT ACCOUNT HOLDER.—The term ‘recalcitrant account holder’ means any account holder which—
“(A) fails to comply with reasonable requests for the information referred to in subsection (b)(1)(A) or

(c)(1)(A),
or "(B) fails to provide a waiver described in subsection (b)(1)(F) upon request.

But guess what - if you are a foreign Central Bank, or if the Secretary determined that you are "a low risk for tax evasion" (unlike the Secretary himself) you still can do whatever the hell you want:

''(f) EXCEPTION FOR CERTAIN PAYMENTS.—Subsection (a) shall not apply to any payment to the extent that the beneficial owner
of such payment is—
''(1) any foreign government, any political subdivision of a foreign government, or any wholly owned agency or instrumentality of any one or more of the foregoing,
''(2) any international organization or any wholly owned agency or instrumentality thereof,
"(3) <u>any foreign central bank of issue, or</u>
"(4) any other class of persons identified by the Secretary for purposes of this subsection as posing a low risk of tax evasion.

One thing we are confused about is whether this law is a preamble, or already incorporates, the flow of non-cash assets, such as commodities, and, thus, gold. If an account transfers, via physical or paper delivery, gold from a domestic account to a foreign one, we are not sure if the language deems this a 30% taxable transaction, although preliminary discussions with lawyers indicates this is likely the case.

And so the noose on capital mobility tightens, as very soon the only option US citizens have when it comes to investing their money, will be in government mandated retirement annuities, which will likely be the next step in the capital control escalation, which will culminate with every single free dollar required to be reinvested into the US, likely in the form of purchasing US Treasury emissions such as Treasuries, TIPS and other worthless pieces of paper.

Congratulations bankrupt America - you are now one step closer to a thoroughly non-free market.

Banksy

http://www.e-dinar.com

Protect against Inflation
Use Gold & Silver

buy physical Gold & Silver online

make instant online payments with Gold & Silver

hold Gold Dinar and Silver Dirhams in your hands

e-dinar

www.e-dinar.com

Non Bank Digital Currency Payment Systems: Regulations & Growth

by Mark Herpel
article originally appeared in
e-Finance & Payments
Law & Policy Newsletter
July 10 Volume 04 Issue 07
http://www.e-comlaw.com

Digital currency is often described as money or value that circulates online but does not circulate through a bank or recognized financial institution. Many digital currency companies emerged in the mid to late 1990's with names such as DigiCash, CyberCash, eCash and e-gold. During the 1990's these privately issued digital tokens representing value were not recognized as government issued "money". Consequently, the creation and transfer of the units was not considered a regulated banking operation. This was true for almost a decade.

The "digital currency" unit of the 1990's was an anonymous digital token which could be transferred from one account to another within a closed system. These systems could be described as large accounting programs where one account is debited and another account receives the credit. What makes these systems so special is that from the early 1990's digital currency granted anyone in any country, instant & easy access to the world of online commerce.

In its early days, this industry operated in a brand new unlicensed and unregulated environment. While about a dozen or so companies online today still live in that bubble, the largest companies and the industry leaders have all gone through a period of growing pains and evolved into more modern systems.

However, several popular digital currency companies were intentionally domiciled or re-domiciled in under regulated or obscure jurisdictions lacking sophisticated regulation and Internet oversight. These companies presently transferring funds around the globe each day for thousands of anonymous customers are quite simply flying below the radar. While freedom lovers call it "privacy", international law enforcement does not always hold that view. No matter what your perspective on the situation, this is definitely not conventional online banking.

To open and operate a digital currency account in the late 1990's all you needed was a computer and an Internet connection. Almost all of the early systems operated using a similar type of model. Some companies changed over the years and grown out of that first structure, many have not. Since the mid 1990's, very few have retained all of their original features. Unlike an online bank account "digital currency" is defined by these features. During the past decade, some of these features were popular but have evolved while other features are still widely used.

- Digital currency accounts can be opened and used instantly.

- There were no distinctions between a personal account or a "merchant account". All digital currency accounts were identical whether personal or "merchant".

- All transactions clear instantly, no delays... ever.

- All digital currency transactions are final, no charge backs or reversal of funds...ever.

- To open and use a digital currency account the currency issuer/operator did not require identification, credit check or verification of identity. (GoldMoney was an exception with a

CAP. Webmoney accounts(passports) require ID for anything more than a basic act.)

- There were no age limits, a 10 year old could operate an account with no questions.
- There were no jurisdictional restrictions. Residents of Iran, Cuba, India, South Africa or China were all free to use digital currency.
- Unlike a bank account, there are no minimum deposits required to open & maintain that account. Digital currency accounts can be opened with no deposit and remain open without issue or fee.
- There were no type of business restrictions. Gambling, online pharmacies, pornography, MLMs, investments, pyramid/ponzi schemes and many others were permitted using digital currency. (Exceptions: GoldMoney & Webmoney have restrictions)
- Account holders were always adding withdrawing funds (national currency) through third party independent agents, not the digital currency issuer/operator.
- Because funds could not be reversed, there are never withholdings or reserve funds. 100% of each transaction clears and is immediately available.
- Digital currency transaction fees were and still are extremely low. Compared to credit card processing fees, digital currency transaction fees are often less than 1/5 of the cost.

Digital Currency Differences

For more than a decade, digital currency units denominated in dollars, euros, rubles or backed by precious metal were technically not government issued money. As units moved over the Internet and not through a bank, it was believed digital currency circulated beyond the reach of existing bank regulations.

"In a turbulent world it's good to know there's still a safe and reliable place to store your wealth."

For more than 5 years we have been a leading provider of gold storage services

We offer our customers

extremely strong security,
outstanding customer service,
excellent reliability and
honest transparent governance

We're adapting to change...
How about you?

Join us today

pecunix

Licensed and registered in the Republic of Panama

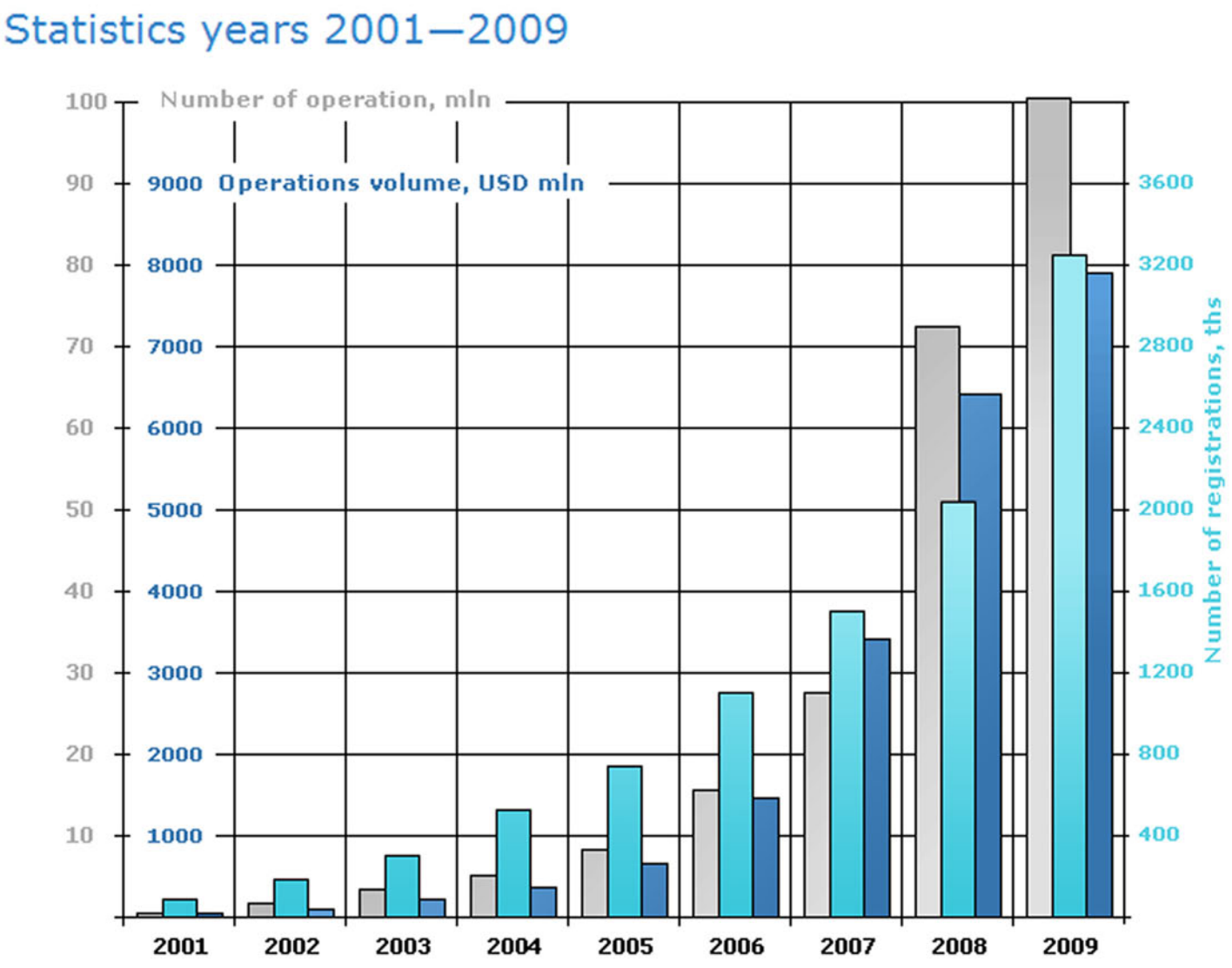
Today, however, this loose concept has evolved and several of the larger countries like Australia, Canada and the U.S. have encircled both the issuers & exchange agents with challenging new regulations along with clarifications of the existing bank laws.

In contrast to online bank accounts, digital currency has more anonymous cash like features. A banker would say, the accounts lack oversight. These digital currency units are issued by a private company and quietly move around the globe with just a few keystrokes. No strict bank regulators or sophisticated AML software is monitoring this account activity. This was true in the 1990's and is generally still true today.
In a recent interview for DGCmagazine with the operator of gBullion, a brand new digital gold currency domiciled in the UAE, I asked, "...if I am transferring 1 million euro a week through my gBullion account, month after month, do you ever ask the account holder for a source of funds on where that money came from and is that information reported to any government organization or tax authority?

The answer was no: "If identification is confirmed and we 'know our client' they can buy or sell gold daily up to amounts of €1.000 000, €2.000 000 or even €10.000 000 per day. This is their right..."

Here is a new online financial business which would permit deposits of €2.000.000 - €10.000 000 per day being deposited and or withdrawn, but never question where the funds originated. Is this freedom & privacy or simply ignorance?

Operators of these early 1990's style digital systems did not have bank accounts and never



accepted direct transactions with retail consumers. All financial transactions between retail public customers were completed via independent third party exchange agents. Retail customers always sent money to a third party and not the operator of the system. This structure provided absolute protection for the assets backing the digital units. Whether the value behind the digital currency was cash, precious metal or anything else, at all times that value remained protected from the everyday risks of doing business. Today, many existing companies still use an identical structure.

This model creates a 'round-the-clock' third party liquid market for the digital units and offers a myriad of payment options in various countries. The ability of a customer to fund or withdraw money from their digital currency account using any number of a dozen local methods is a spectacular incentive for global non bank users. (cash, IBAN, SWIFT, Western Union, Ukash, cashU, Moneygram, Anelik, Zoom, money order etc.) It is doubtful if any type of regulations could ever slow down the growth for this type of third party exchange business.

On the opposite side of the payment spectrum, companies like PayPal are integrated with banks, process credit card transactions and operate as licensed a money transmitters. The PayPal's of the world require all national currency transactions to flow directly through PayPal bank accounts. All customer funds sent to PayPal or withdrawn from those accounts must flow directly through PayPal. No third party exchange transactions have ever been permitted. Unlike digital currency businesses, the big online payment processing companies absorb 100% of the risks when dealing with the public.

In 2002 while PayPal prepared for a public offering, the company's corporate lawyers were quick to secure those important financial licenses required for doing business in the United States. However, during those years between 2002-2005 most digital currency companies were not following that same regulatory path.

Regulation & Growth

It's been said that government regulations lag behind the development of new technology by 3 or more years.

In 2006, concerned with the anonymity of digital currency products, a number of U.S. government agencies began to take a closer look at the industry along with those independent exchange agents which handled the customer transactions. All of companies located in the continental U.S. fell under scrutiny. The following year a number of these businesses were charged with operating as unlicensed money-transmitting businesses.

In April of 2007 a U.S. court ordered seizure forced the e-gold company to liquidate a large number of customer accounts and hand over the funds. The amount of seized money was in the millions. The confiscated accounts mainly belonged to independent exchange agents operating within the United States which had been declared "unlicensed & illegal".

This 2007 action killed 99% of the digital currency business in the U.S., eventually lead to criminal charges for e-gold and forced the closure of payment systems such as 1MDC & Crowne Gold. What is interesting to note regarding e-gold is that during the period of 2005-2008 while they were engaged in a very public legal battle, the number of customer accounts more than doubled as e-gold picked up 3 million new accounts. Since the company never used paid advertising this was the first main stream publicity it had ever received.

Immediately after this action, a few large agents and operators permanently fled the U.S. for more casual business environments such as Central America. Several of them left the business and retired. The industry had seen a similar consolidation resulting from new Financial Services Licensing regulations enforced by the Australian Securities and Investments Commission (ASIC) during 2004. Forced out of business in Australia, some had closed but other larger agents changed jurisdictions and simply moved their business. The world is a very big place.

While regulations and growing pains have becoming the norm for digital currency companies, this has not slowed the industry's growth.

Now in our third year online, we salute all our DGC friends.
Read DGCmagazine, support GATA, and proudly wear your tin foil hat! Cheers.

Global leader Webmoney Transfer has shown dramatic growth each year for the past decade. (as indicated by this chart) The number of users, day to day transactions and funds on deposit have surged as Webmoney has expanded into new territories and offered new products. Webmoney Transfer now has more than 11 million customer accounts and has never required any user to have a credit card or bank account. That digital currency flows through more than 8,000 cities in 70 countries around the globe.

The 2009 e-money industry in Russia had sales of more than 40 billion rubles ($1.3 bil USD). Despite the Russian government's effort to pass new e-money regulation this year which could possibly effect business expansion through higher fees, Webmoney's business is booming. GoldMoney customer holdings have just passed $1 Billion USD in value and there are even several other new digital currency companies new to the marketplace in just the past year.

Outside of the United States proper digital currency regulations compatible with current market models should not slow industry growth. In fact some additional KYC and AML regulations should help bolster the growth of digital currency across major emerging markets.

New consumers entering the digital currency marketplace do not come from credit card companies or banks. In fact it is very difficult to convince anyone to put down their plastic. Digital currency attracts those people in cash markets wanting to do business online. Digital currency speaks to those customers in markets not yet serviced by the PayPal's of the world and new users surface from an ever expanding customer base of non-bank consumers.

The business opportunities that digital currency offers to someone without a bank account or credit card are enormous. In the years ahead we can expect to see more non-bank Internet users and despite additional government regulations the forecast is for a continued boom in these products.

Image comes from Webmoney Transfer, http://www.wmtransfer.com/eng/about/statistics/stat_years.shtml

The Strange Case of The Liberty Dollar

by: Adam Jefferson Kirby

Reprinted with Adam's permission from
http://www.silvermonthly.com/1459/the-strange-case-of-the-liberty-dollar/

Anyone interested in creating coins for use as a medium of exchange would be well advised to become familiar with the foundations of our currency laws; namely, Article I, Section VIII of the U.S. Constitution. It states clearly that "The Congress shall have Power…To coin Money, regulate the Value thereof, and of foreign Coin, and fix the Standard of Weights and Measures; To provide for the Punishment of counterfeiting the Securities and current Coin of the United States."

The Coinage Act of 1792 is the foundation of American legal tender laws. Section 10 specified the configuration of U.S. legal tender coins, establishing the standard against which the authenticity of American currency was measured thereafter:

And be it further enacted, That, upon the said coins respectively, there shall be the following devices and legends, namely: Upon one side of each of the said coins there shall be an impression emblematic of liberty, with an inscription of the word Liberty, and the year of the coinage; and upon the reverse of each of the gold and silver coins there shall be the figure or representation of an eagle, with this inscription, "United states of America" and upon the reverse of each of the copper coins, there shall be an inscription which shall

express the denomination for the piece, namely, cent or half cent, as the case may require. [1] [Emphasis in original.]

A currency only functions as a medium of exchange if a society believes that it truly represents value. The reason why gold and silver have been desirable as money throughout history is because they are highly portable, easily divisible substances which are universally recognized as scarce, which makes them a store of value. The United States utilized gold and silver in some manner or form as the basis for its economy until 1971, when U.S. President Richard Nixon terminated the Bretton Woods agreement of 1944. Under Bretton Woods, which fixed international exchange rates against a gold-pegged dollar, the world's largest economies had a functional relationship within which to trade currencies, and for the purposes of international settlements. Some argued that the gold basis for this system did not allow for enough elasticity in the money supply, and that argument eventually prevailed. In August of 1971, the American currency lost what remained of its direct commodity backing, raising grave concerns about the advent of greater monetary abuse.

In response to what he perceived to be the forced, hidden confiscation of the purchasing power of the American currency by the United States government, self-described monetary architect Bernard Von Nothaus embarked upon a mission to establish a commodity-backed, voluntary barter currency composed of gold and silver. Von Nothaus claims to be the mint master of Royal Hawaiian Mint, (RHM). There is no indication that this is an official state entity. No information exists on RHM other than a few references associated with the Von Nothaus name. RHM is very likely a private entity run by Von Nothaus himself. Regardless of the opaque nature of his resume, Von Nothaus claims over 25 years experience in minting.

Von Nothaus recognized the grave economic threat that is an unrestrained government with the ability to monetize debt indiscriminately. His solution was to create a voluntary barter currency redeemable in silver, issued under the umbrella of a nonprofit entity called the National Organization for the Repeal of the

Federal Reserve Act and Internal Revenue Code, or NORFED, where Von Nothaus has been mentioned in several articles as being its "Senior Economist." [2] In 1998, NORFED introduced the Liberty Dollar, and marketed it as an alternative to Federal

Reserve Notes. The project began with the circulation of warehouse receipts representing a specified quantity of silver held in storage at a private mint. Merchants or consumers who held similar concerns about the longevity of the Federal Reserve Note's purchasing power could circulate these Liberty Dollar receipts amongst themselves as a medium of exchange for goods and services. So long as it was voluntary, and both parties understood what they were doing, the system was untouchable.

According to an article by John Christian Ryter, NORFED was investigated in 1999 by the Secret Service regarding their warehouse receipts but did not file charges, finding that the receipts did not constitute counterfeit currency because they did not contain the language "legal tender", and that there was a sufficient amount of warehoused silver to represent the value indicated on the Liberty Dollar receipts. [3] It was not until the coins themselves began widely circulating that the U.S. Government decided to take legal action. In November of 2007, the U.S. Department of Justice conducted a raid, seizing the assets of NORFED held in a private office in Evansville, Indiana. [4] A concurrent raid was also conducted at the private mint in Idaho where the coins and warehouse receipts were manufactured and stored. [5] In the Justice Department's own affidavit, it cites Von Nothaus' statements to the effect that the Liberty Dollar was intended to be in direct competition with the Federal Reserve Note. [6] This seems to contradict and nullify the counterfeit claim. In spite of this, the Affidavit cited U.S.C. 18 § 492 as justification for claiming probable cause. This section of the U.S. code deals with forfeiture of counterfeit coins, material and apparatus. [7]

To directly compete for consumer market share with a distinctive good or service is one thing. To undermine the legitimate market share of a firm by emitting false or erroneous versions of that firm's distinctive products constitutes the crime of counterfeiting. Von Nothaus made no attempt to overtly counterfeit Federal Reserve Notes or other official U.S. coinage. All of his marketing literature explicitly distinguishes the fundamental philosophical and economic differences between what the U.S. government forces the market to accept as official U.S. currency and what NORFED was offering with the Liberty Dollar. The problem was that Von Nothaus did not make his products physically distinctive enough to avoid confusion.

In fact, knowing full well that the ability for a currency to succeed is incumbent on its acceptability, Von Nothaus encouraged his associates to directly introduce the silver coins into general circulation, trusting that once vendors could physically inspect these coins, that their intrinsic value would be understood. Von Nothaus had faith that his product would indeed be seen as a legitimate medium of exchange and in no way different in function from Federal Reserve Notes. Regardless of their legitimacy, without an explicit understanding that a merchant was undertaking a voluntary barter transaction, any such transaction with Liberty Dollars was fraudulent. No contract between two parties is valid if the terms are not clearly and explicitly articulated.

Strangely absent at the time of the seizures was the issuance of a criminal complaint against Von Nothaus. The U.S. Justice Department did eventually file a criminal complaint against Von Nothaus and three of his colleagues in June of 2009.8 The indictment cited several violations, including U.S.C. 18 § 486, dealing with uttering coins. It states the following:

> ***Whoever, except as authorized by law, makes or utters or passes, or attempts to utter or pass, any coins of gold or silver or other metal, or alloys of metals, intended for use as current money, whether in the resemblance of coins of the United States or of foreign countries, or of original design, shall be fined under this title [1] or imprisoned not more than five years, or both. [9] [Emphasis added.]***

U.S.C. 18 § 486 does appear to create criminal liability for the simple reason that the Von Nothaus product was put directly into circulation without the clear understanding by merchants that they were entering into a voluntary transaction with a medium of exchange not officially recognized by the U.S. government. It was common practice for Von Nothaus and his associates to present Liberty Dollars to merchants unfamiliar with his product without offering the explanation that they were not U.S. legal tender currency, but rather, a voluntary barter currency, one which could not be redeemed at face value for Federal Reserve Notes in any U.S. commercial bank. A video exposé posted originally on the Liberty Dollar website – a short clip from The Learning Channel's show Super Structures – features Von Nothaus personally buying sandwiches with a $10 Liberty Dollar coin, declaring it to be a "new ten dollar silver piece" as he handed it to the bewildered vendor. [10]

However compelling Von Nothaus' philosophical and constitutional arguments may be, this unfortunate, deceptive practice does not lend credibility to the legitimate criticism of the U.S. government's fiscal policy of inflation, nor to the legitimate practice of entering into private voluntary barter using gold and silver as a medium of exchange. Although it can be argued persuasively that the Liberty Dollars are not technically counterfeit, the engagement in the practice of infiltrating the currency market in such a way seems to be tantamount to a kind of economic insurrection, inviting the reprisal of government force. Furthermore, if Von Nothaus wanted his competitive product to be able to vie for

market share of exchange media, the coins should not have been made to so closely resemble U.S. legal tender coins.

The Liberty Dollar coins which were seized by the F.B.I. and the Secret Service contain "impressions emblematic of liberty", namely, the word "Liberty" in bold lettering, appearing in the same manner as on U.S. legal tender coins; the phrase "Trust In God" in a location similar to that of the inscription "In God We Trust", as found on U.S. legal tender coins since the Coinage Act of 1873 [11] ; a profile of a woman's head wearing a crown, similar to that of the Statue of Liberty on the obverse; and what appears to be the torch of the Statue of Liberty on the reverse. The Von Nothaus coins also have the year of mintage featured prominently and similarly as on U.S. legal tender coins. The coins also utilize the "$" symbol to denominate their purchasing power, even though they represent purchasing power from a different philosophical perspective-value which is not in direct correlation with that suggested by the denominations on Federal Reserve Notes.

The best way to convince the American people to accept an alternative medium of exchange is to make sure the terms of use are clearly understood. There is no reason for a monetary architect to obscure his motives, the circumstances of exchange, or the philosophy he espouses. Restoring sound money is an honorable objective considering the widely shared concerns about inflation, and the idea of creating wealth as an alternative to debt is a noble philosophy. The quiet resestablishment of commodity based currencies, including the careful retasking of our nation's old silver coinage, would go far to address the same problems which Von Nothaus and his associates have failed to accomplish due to their lack of clear and explicit articulation of voluntarism.

1. A Century of Lawmaking for a New Nation: U.S. Congressional Documents and Debates, 1774-1875, Library ofCongress Website. Accessed Feb 20th, 2010. http://memory.loc.gov/cgi-bin/ampage?collId=llsl&fileName=001/llsl001.db&recNum=371
2. "Y2K Buck Stops Here" by Will Hoover, December 7th 1998. The Honolulu Advertiser. http://www.libertydollar.org/news-stories/pdfs/1164902770.pdf
3. "FBI Raids Liberty Dollar" by Jon Christian Ryter. November 17th 2007, NewsWithViews.com. http://www.newswithviews.com/Ryter/jon201.htm
4. "Liberty Dollar Office Raided" by Gary Lesnick. November 15th 2007, Evansville Courier & Press. http://www.courierpress.com/news/2007/nov/15/liberty-dollar-office-raided/
5. Verified Complaint for Forfeiture In Rem, United States District Court Western District of North CarolinaAsheville Division, June 26th, 2008, pg. 3.
6. Verified Complaint for Forfeiture In Rem, United States District Court Western District of North Carolina Asheville Division, June 26th, 2008, pg. 6.
7. Cornell University Law School, Legal Information Institute. http://www.law.cornell.edu/uscode/18/492.html
8. United States of America v. Bernard Von Nothaus, others. Bill of Indictment, May 19th 2009. United States District Court for the Western District of North Carolina Statesville Division. http://www.libertydollar.org/legal/pdf/05192009_indictment.pdf
9. Cornell University Law School, Legal Information Institute. http://www.law.cornell.edu/uscode/18/486.html
10. "Fiat Currency versus The Liberty Dollar" exerpt from Super Structures, The Learning Channel, January 8th, 2004. YouTube video posted October 22nd 2007. http://www.youtube.com/watch?v=1VaBX7A9FqA
11. United States Department of the Treasury: Fact Sheets: Currency & Coins: History of 'In God We Trust'. http://www.treas.gov/education/fact-sheets/currency/in-god-we-trust.shtml

Adam Jefferson Kirby is a student at the University of Texas at Tyler. He blogs at http://www.obvi8or.blogspot.com

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

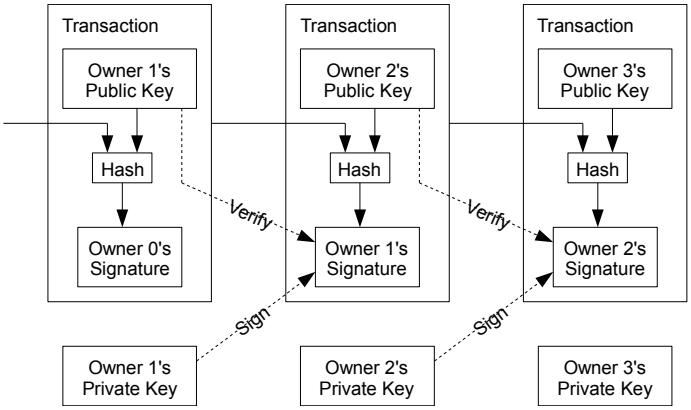
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

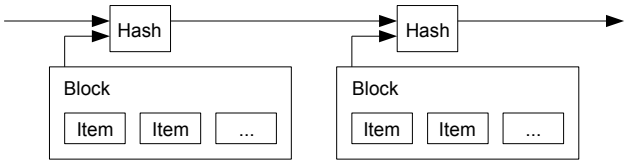


The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

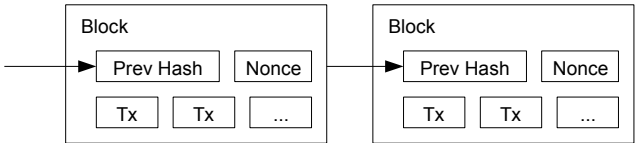
The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. Incentive

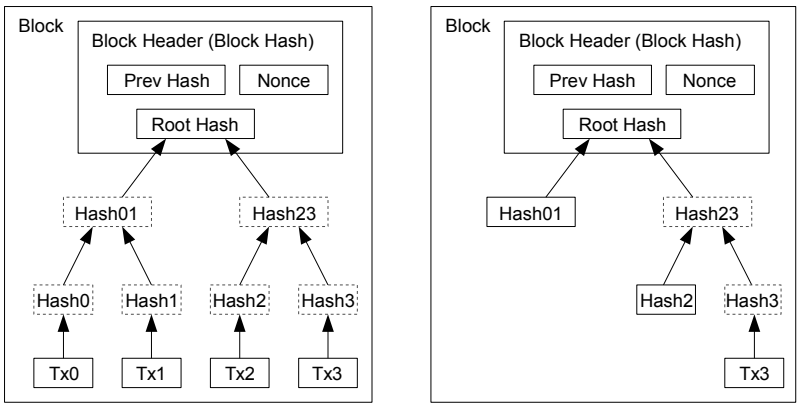
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



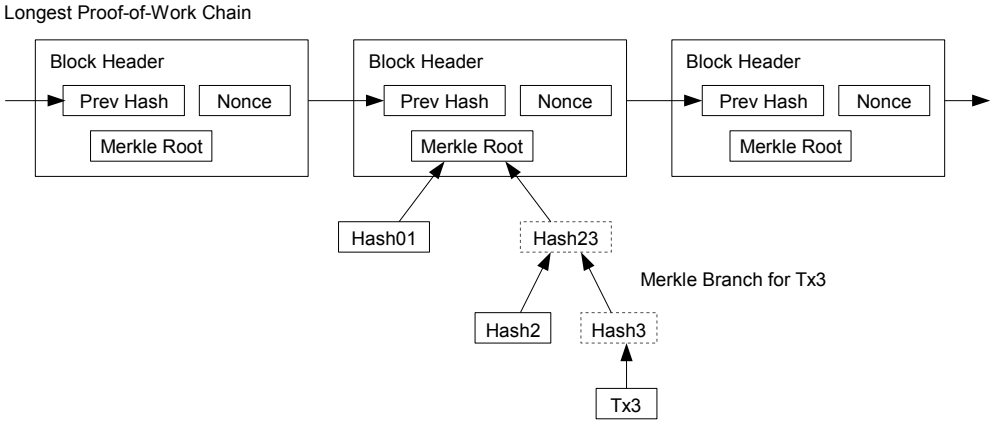
Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

8. Simplified Payment Verification

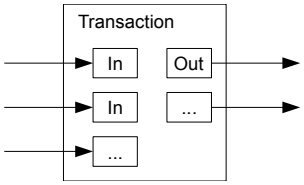
It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.



As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

9. Combining and Splitting Value

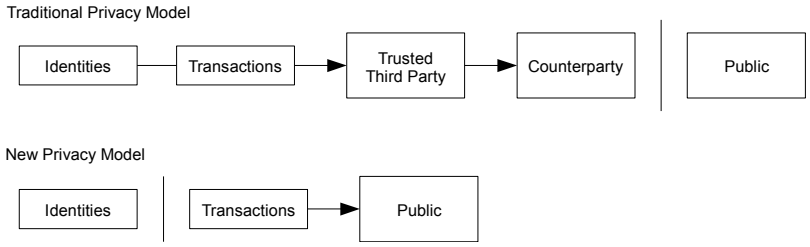
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.



It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z\frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Solving for P less than 0.1%...

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.