U.S. Department of Justice
National Drug Intelligence Center

Product No. 2008-R0709-003

June 2008

Money Laundering in Digital Currencies

This page intentionally left blank.

Table of Contents

This page intentionally left blank.

U.S. Department of Justice
National Drug Intelligence Center

Assessment

Product No. 2008-R0709-003

Money Laundering in Digital Currencies

June 3, 2008

Key Judgment

Digital currencies combine the intrinsic value of gold and other precious metals as well as the designated value of national currencies with the worldwide reach of the Internet to create an ideal mechanism for international money laundering. Users can anonymously fund digital currency accounts, send those funds (sometimes in unlimited amounts) to other digital currency accounts worldwide, and effectively exchange the funds for foreign currencies—often while bypassing U.S. regulatory oversight.

Introduction

Digital currencies provide an ideal money laundering instrument because they facilitate international payments without the transmittal services of traditional financial institutions.[1] Such currencies allow direct access to a remote payment mechanism and can be used to launder illicit funds by sending instant international remittances via the Internet. Many components of the digital currency system are incorporated in offshore and foreign jurisdictions not subject to U.S. regulations; however, their services are accessed in the United States through the Internet. As such, transactions can be completed with less fear of documentation, identification, or law enforcement suspicion. Such emerging electronic payment systems are vulnerable to money laundering and terrorist financing.

Digital currencies are privately owned online payment systems that allow international payments, which are often denominated in the standard weights for gold and precious metals.[2] Each digital currency functions as one transnational currency; however, none of these are recognized as currencies by the U.S. government.[3] Most digital currencies claim to be backed by precious metals such as gold, silver, platinum, and palladium; however, very few can independently prove such backing. Several digital currencies claim to be backed by specific national currencies. Metal-backed digital currency accounts are allegedly valued based on the backing commodity's fluctuating "spot price" at the time of funding or withdrawal;

1. Digital currency account holders may have indirect contact with a depository institution through the digital currency's operating (or "pooled") account.
2. Gold, platinum, silver, and palladium are denominated according to the International Organization for Standardization (ISO) 4217 codes. ISO encourages standardization in order to promote interoperability of international systems.
3. According to the U.S. Department of the Treasury publication *U.S. Money Laundering Threat Assessment*, currency is something monetized by a monetizing authority, generally a central bank. Rather than being used as currency, precious metals are used as a part of a barter exchange (one party agrees to exchange a quantity of gold for various goods or services).

digital gold currencies (DGCs)[4] are by far the most popular type. Metal does not physically change hands in transactions; rather, the transfer is an accounting entry in which only the designation of ownership changes (similar to a stockholder whose shares represent a portion of a company's holdings). According to the Global Digital Currency Association (GDCA), digital currency transactions account for billions of dollars each year—digital gold currency transactions alone increased from approximately $3 billion in 2004 to approximately $10 billion in 2006.

The digital currency system is composed of issuers, digital currency exchangers (DCEs),[5] and the individuals (including merchants) who conduct transactions. Digital currency issuers frequently own or control a digital currency and are generally responsible for maintaining the precious metals used to back currencies or—in the case of currencies not backed by metals or national currencies—managing pooled bank accounts in which users' funds are maintained until withdrawn. Issuers typically process digital currency transactions and maintain online records of users' activities, including funding, spending, fees, and withdrawals. Digital currency exchangers (DCEs) facilitate funding of and withdrawals from digital currency accounts as well as conversion of one digital currency to another. Such exchangers and issuers are usually independent entities; however, an issuer may have a corporate affiliation with one particular DCE. Many DCEs claim to accept any national currency (U.S. dollars, euros, yen, etc.) in exchange for digital currencies, as well as a variety of other payment methods. Because digital currencies operate independently, payments issued by a specific digital currency can be accepted only by merchants or individuals who accept that digital currency, unless the payment is first converted to the appropriate digital currency through a DCE.

Substantiation

Digital currencies allow account holders to electronically manipulate funds similarly to other types of funds transfer services. Digital currency account holders can move funds internationally in a manner that approximates money transfers or traditional wire transfers. The ability to conduct transactions in digital currencies is constantly available, making digital currencies more convenient than other methods of funds transfer, which may be limited by normal business hours and international time zones. Additionally, digital currency transactions can be conducted from any location or device with Internet access. Some issuers also accommodate mobile payments[6] through web-enabled phones. Digital currencies are generally easy to use, and transactions conducted in these currencies are instantaneous and irreversible. Because most digital currencies are denominated into internationally recognized weights of precious metals, inconveniences traditionally associated with international financial transactions, such as calculating international exchange rates for another nation's currency, are eliminated. A digital currency account can function as a merchant account, allowing a digital currency account holder to function

4. Also known as electronic gold currencies (EGCs) or electronic gold.
5. Also known as exchange agents, exchange providers, exchangers, or market makers. Digital currency exchangers (DCEs) are called market makers because they act like wholesalers in the stock market, making a profit from the bid/offer spread. (The bid price is what individuals can sell their shares for; the offer price is what they can buy them for. The bid is always lower than the offer price, and the difference between them is the spread.)
6. Mobile payments are any payments activated or confirmed by a mobile device.

as a front or shell company.[7] DCEs that are automated allow individuals to execute multiple currency-to-currency exchanges in a short period of time and can be exploited to provide an ideal layering mechanism for funds placed into a digital currency account.

Regulatory interpretations and jurisdictional inconsistencies affect the operations of domestic and international digital currency programs that are accessible in the United States. Many digital currency programs in the United States believe that they are not subject to any existing federal or state regulatory structure. This issue is currently being litigated in federal court. Programs with components (servers, bank accounts, corporate offices, etc.) located outside the United States are not subject to U.S. regulations, yet those programs can be accessed within the United States. Issuers and DCEs frequently locate components in international and offshore jurisdictions; this practice enables them to avoid U.S. regulatory oversight and complicates prosecutions.

Anonymity is a heavily marketed characteristic of the digital currency industry. Because digital currency accounts are obtained online and are not subject to the customer identification procedures associated with obtaining a traditional bank account, they often can be opened and funded anonymously. Many digital currency web sites advertise "full anonymity" for transactions. Some issuers require identification, but because users open digital currency accounts online, documents are generally faxed or scanned to the issuer and can be easily altered or falsified. Anonymity continues during the digital currency account funding process, again without face-to-face interaction. Individuals can fund digital currency accounts by making cash deposits directly to an exchanger's bank account.[8] Many DCEs maintain bank accounts in several countries to facilitate cash deposits in various national currencies. Industrywide, exchangers also accept wire transfers, postal money orders, and a variety of other payment types, some of which may make it difficult to determine the source of funds. Illicit users further attempt to conceal their identities by continually opening new digital currency accounts, as often as after each transaction. Digital currency accounts can also be funded with varying degrees of anonymity by mail and over the Internet, using electronic money orders (EMOs), checks, and online banking transfers. Some issuers allow individuals to redeem digital currency account balances in actual precious metals; launderers looking to conduct business in precious metals could exploit digital currencies to acquire them without the paper trail created by the commodities market. Many exchangers will convert digital currency balances into anonymous prepaid (stored value) cards[9] that can be used to withdraw funds by various methods, including at worldwide automated teller machines (ATMs). Digital currencies also may be withdrawn through worldwide wire transfers, mailing third-party

7. Front and shell companies are used to launder money when illicit funds, represented as the proceeds of legitimate business transactions, are deposited to the companies' accounts. Front companies are legally incorporated businesses that participate in legitimate trade; illicit funds deposited to these accounts are commingled with the front companies' legitimate proceeds. Shell companies are legally incorporated businesses that do not engage in legitimate trade; all proceeds deposited to shell companies' accounts are illicit. Front companies, such as import/export businesses and charities, are commonly used to layer funds. Cash-intensive front companies—such as laundromats, salons, and restaurants—and shell companies are frequently used to place illicit funds.
8. Exchangers credit the deposited funds to individuals' digital currency accounts upon receiving proof of the deposit.
9. Prepaid (stored value) cards provide an ideal money laundering instrument to anonymously move monies associated with all types of illicit activity. See NDIC publication number 2006-R0803-001, *Prepaid Stored Value Cards: A Potential Alternative to Traditional Money Laundering Methods*, for complete analysis.

checks to anyone whom the account holder designates, or a variety of other methods.

Various technologies can increase the utility of digital currencies for money laundering by providing additional anonymity and networking abilities. Because digital currency transactions are conducted over the Internet, they can be traced back to individuals' computers;[10] however, anonymizing proxy servers and anonymity networks[11] protect individuals' identities by obscuring the unique IP (Internet Protocol) address as well as the individuals' true locations. Furthermore, mobile payments conducted from anonymous prepaid cellular devices, such as web-enabled phones, may be impossible to trace to an individual. Such portable devices that provide Internet access enable transfers of digital currency; afterward, they can be destroyed, easily and inexpensively, to prevent forensic analysis. Digital currency account holders also may use public Internet terminals or even "hijacked" wireless Internet connections to access their digital currency accounts, causing transactions to appear to originate with the unsuspecting Internet subscriber. Users of digital currency may also use encrypted chat rooms[12] to conceal communications between individuals, making law enforcement scrutiny more difficult.

Because digital currency is increasingly misused to purchase drugs and other illicit materials that are sold online, the proceeds of that activity are essentially prelaundered.[13] Payment in digital currencies makes it easier for traffickers to launder funds that no longer need to be placed into the traditional financial system. Payment can be immediately forwarded to an international digital currency account, perhaps in payment to the original source of supply, or further layered through multiple digital currency accounts and exchangers until reintegrated into the legitimate economy. Online illicit drug sales are now being conducted on bulletin boards, on blogs, and in encrypted chat rooms, and sellers are increasingly demanding payment in digital currencies, specifically DGCs. Additionally, Operation Raw Deal, an Organized Crime Drug Enforcement Task Force (OCDETF) investigation initiated in November 2006, indicates that several Chinese raw materials manufacturers, which supply large-scale methamphetamine laboratories in the United States and Canada, accept payment in DGCs for drugs, precursor materials, and conversion kits for manufacturing finished products. The targeted companies are responsible for mass manufacturing and distributing anabolic steroid raw materials, human growth hormone (HGH), and certain other prescription and counterfeit drugs illegally entering the United States.

10. The origins of Internet activity can often be identified using IP (Internet Protocol) addresses. Each computer on a network, including the Internet, must be uniquely identified by an IP address in order to receive information, such as web pages, requested from remote servers. These servers, including digital currency servers, track and record users' IP addresses.
11. Anonymizing proxy servers and anonymity networks are designed to prevent identification of Internet users' IP addresses. Such proxy servers and networks redirect users' activities so that they appear to originate from a proxy server's or anonymity network's IP address rather than the IP address of an individual Internet user.
12. Encryption ensures that only the intended recipients see the information in electronic transmissions; for security purposes, documents are often encrypted along the way from sender to receiver.
13. During the placement (initial) stage of money laundering, illicit proceeds in the form of cash reenter the legitimate financial system and are most vulnerable to detection. The layering (second) stage consists of a series of noncash transactions designed to distance the illicit proceeds from the source of the funds; i.e., the illicit activity. The integration (third) stage involves the return of the funds—which now appear to have been obtained legitimately—to the economy.

Law Enforcement Case Examples

E-Gold Indicted

On April 27, 2007, a federal grand jury in Washington, D.C., indicted two companies operating a digital currency business and their owners. The indictment charges E-Gold Ltd., Gold and Silver Reserve, Inc., and their owners with one count each of conspiracy to launder monetary instruments, conspiracy to operate an unlicensed money transmitting business, operating an unlicensed money transmitting business under federal law, and one count of money transmission without a license under D.C. law. According to the indictment, persons seeking to use the alternative payment system E-Gold were only required to provide a valid e-mail address to open an E-Gold account—no other contact information was verified. The indictment is the result of a 2½-year investigation by the U.S. Secret Service with cooperation among investigators, including the Internal Revenue Service (IRS), the Federal Bureau of Investigation (FBI), and other state and local law enforcement agencies. According to Jeffrey A. Taylor, U.S. Attorney for the District of Columbia, "The defendants operated a sophisticated and widespread international money remitting business, unsupervised and unregulated by any entity in the world, which allowed for anonymous transfers of value at a click of a mouse. Not surprisingly, criminals of every stripe gravitated to E-Gold as a place to move their money with impunity."

Source: U.S. Department of Justice.

The Shadowcrew Ring

On June 29, 2006, Andrew Montovani was sentenced to 32 months in federal prison for cofounding Shadowcrew.com, an international online discussion forum with more than 4,000 members, many of whom specialized in identity theft and fraud. Shadowcrew members sent and received payments for goods and criminal services through digital currencies. One indicted member, Omar Dhanani, operated an illegal currency exchange, providing members a money laundering service in digital gold by anonymously converting their illicit cash. Dhanani stated that Shadowcrew members used digital gold in order to avoid traditional banking systems. A yearlong investigation by the U.S. Secret Service led to the October 2004 arrest of 21 individuals in the United States, with several other arrests in foreign countries.

Source: U.S. Attorney, District of New Jersey.

Western Express International Currency Exchange Company

On February 22, 2006, Vadim Vassilenko, Yelena Barysheva, and Alexey Baryshev were indicted by the state of New York for operating an illegal check-cashing and money transmittal business from 2002 through 2005. Their company, Western Express International, acted as a currency exchanger, knowingly exchanging criminal proceeds for digital currencies. Through its web sites, Western Express actively solicited overseas clients in eastern Europe, Russia, and the Ukraine to operate illegally in the United States. Clients using fictitious, often multiple identities committed a variety of cyber crimes, such as reshipping, phishing, spoofing, and spamming. Items purchased with stolen credit card numbers were resold for digital gold, which was further laundered through Western Express. A total of $25 million flowed through the company's bank accounts over the 4-year period, in violation of New York banking regulations.

Source: New York County District Attorney's Office, Manhattan.

GoldAge Currency Exchange Company

On July 27, 2006, Arthur Budovsky and Vladimir Kats were indicted by the state of New York on charges of operating an illegal money transmittal business, GoldAge Inc., from their Brooklyn apartments. The defendants had transmitted at least $30 million to digital currency accounts worldwide since beginning operations in 2002. The digital currency exchanger, GoldAge, received and transmitted $4 million between January 1, 2006, and June 30, 2006, as part of the money laundering scheme. Customers opened online GoldAge accounts with limited documentation of identity, then GoldAge purchased digital gold currency through those accounts; the defendants' fees sometimes exceeded $100,000. Customers could choose their method of payment to GoldAge: wire remittances, cash deposits, postal money orders, or checks. Finally, the customers could withdraw the money by requesting wire transfers to accounts anywhere in the world or by having checks sent to any identified individual.

Source: New York County District Attorney's Office, Manhattan.

Some digital currency issuers offer liberal—or even no—limits on transactions, funding amounts, and total account balances, allowing drug traffickers to more easily launder large sums with fewer transactions. Digital currency issuers who impose no limits on total value, funding, and transactions are ideal for large-scale drug trafficking networks and money laundering operations; such financial services make it easier and safer to launder larger amounts of money using fewer transactions.

Federal officials have acknowledged the need to close the regulatory loophole that exists in relation to digital currencies. Despite industry assertions that digital currencies are not subject to regulation, as well as the formation of several trade associations and consortiums attempting to demonstrate industry self-regulation, U.S. Government entities are exploring the application of consistent federal regulation over the digital currency industry—which promotes itself as unregulated and anonymous. Additionally, because the value of digital currency accounts changes with the market performance of the backing commodity, any profits earned (capital gains) during the withdrawal of digital currency accounts may not get reported to the IRS unless the digital currency account holder decides to declare the amount voluntarily.

Outlook

Drug traffickers will increasingly rely upon the digital currency industry to launder and move funds because it enables standardized international financial transactions and operates largely outside the regulatory requirements of the traditional banking system. The ability of individuals and businesses to conduct complex, immediate, and irreversible international transactions with very little financial transparency greatly benefits drug traffickers and other criminals.

U.S. regulatory action alone will not be sufficient to suppress the money laundering threat posed by digital currencies. Even if clear and consistent regulatory measures are imposed, digital currency services established in foreign and offshore jurisdictions—which are not subject to the Bank Secrecy Act (BSA)[14]—can be used to conduct transactions in the United States. Limited international oversight of this expanding financial service is possible through a recommendation of the Financial Action Task Force on Money Laundering (FATF).[15] The FATF has publicly stated the need to monitor the growth of this industry and implement anti-money laundering controls; however, FATF recommendations will have little effect on nonmember countries. It would be nearly impossible to legislate regulatory controls that would allow the U.S. government to prevent completely foreign-based digital currencies from being used in the United States, because these services are available through the Internet.

14. The Bank Secrecy Act (BSA) was designed to do the following: deter money laundering and the use of secret foreign bank accounts; create an investigative paper trail for large currency transactions by establishing regulatory reporting standards and requirements; impose civil and criminal penalties for noncompliance with its reporting requirements; and impose detection and investigation of criminal, tax, and regulatory violations.
15. Founded in 1989, the Financial Action Task Force on Money Laundering (FATF) is an intergovernmental body that sets the international standard for combating money laundering and terrorist financing. The FATF issues recommendations and a list of noncooperative countries or territories (NCCTs). The FATF currently has 34 member countries, territories, and regional organizations.

Sources

Local, State, and Regional

New York County District Attorney's Office, Manhattan

San Diego Law Enforcement Coordination Center

State of New Jersey

Federal

Central Intelligence Agency
- Directorate of Science and Technology
  - Foreign Broadcast Information Service

The Federal Reserve Bank

U.S. Courts
- U.S. District Court
  - District of New Jersey

U.S. Department of Homeland Security
- U.S. Secret Service

U.S. Department of Justice
- Criminal Division
  - Organized Crime Drug Enforcement Task Force
- Executive Office for U.S. Attorneys
  - U.S. Attorneys Office
    - District of New Jersey
- Federal Bureau of Investigation

U.S. Department of State

U.S. Department of the Treasury
- Financial Crimes Enforcement Network
- Internal Revenue Service

U.S. House of Representatives
- House Committee on Banking and Financial Services
  - Subcommittee on Domestic and International Monetary Policy

U.S. Postal Inspection Service

International

Bank for International Settlements

European Monetary Institute

Financial Action Task Force on Money Laundering

International Monetary Fund

International Organization for Standardization

The World Bank

World Gold Council

Other

A1 Guide to Gold Investments

Alert Global Media

American Chronicle

Berkeley Journal of International Law

BusinessWeek magazine

Caslon Analytics

Cato Institute

Computing magazine

Digital Gold Currency Standards Consortium

Digital Money World.com

Electronic Currency Merchants Association

Escape Artist Digital Currencies Index

Financial Cryptography.com

Financial Times magazine

Free Market Monetary Education Association

Global Digital Currency Association

Global Investor magazine

Gold Barter Holdings

Gold Currencies.com

GoldDirectory.com

Gold Economy Magazine

The Gold Institute

GoldMoney Bill.org

Gold Pages Electronic Currency Directory

Government Computer News

The Indomitus Report

Newsday magazine

Single Global Currency Association

St. Petersburg Times

Techwack.com

University of Texas at Austin
Graduate School of Business
Center for Research in Electronic Commerce

U.S. News and World Report

Virtual School.edu

Wifive Investment Corporation S.A.

Wired magazine

This page intentionally left blank.

This page intentionally left blank.

319 Washington Street 5th Floor, Johnstown, PA 15901-1622 • (814) 532-4601
NDIC publications are available on the following web sites:
INTERNET www.usdoj.gov/ndic ADNET http://ndicosa RISS ndic.riss.net
LEO https://www.leo.gov/http://leowcs.leopriv.gov/lesig/ndic/index.htm

061308