BLOCKCHAIN AND MORE: A LEGAL GUIDE

South Carolina Association of Counties

AUGUST 2019

Thomas K. Potter, III
Burr & Forman, LLP
Nashville, TN
tpotter@burr.com
www.burr.com

Tom Potter is a partner with Burr & Forman, LLP. For over 33 years, Tom has represented business interests in securities, corporate and intellectual property disputes, regulatory-enforcement matters and compliance consulting. He is listed in CHAMBERS USA as a leading practitioner in commercial litigation, and recognized by BEST LAWYERS® for commercial litigation, litigation – banking and finance, litigation – regulatory enforcement, and litigation – securities. Tom earned his B.A. from the University of Virginia and his JD, *magna cum laude* from the Cumberland School of Law of Samford University, where he was Executive Editor of the Law Review. He is a member of the ABA (Sections on Business, Litigation, Business Torts Committee), the Securities Industry & Financial Markets Ass'n (Compliance & Legal Div'n), the National Society of Compliance Professionals and the International Trademark Ass'n.

Burr & Forman, LLP is a southeastern regional firm with over 360 lawyers in 19 offices in Alabama, Delaware, Florida, Georgia, Mississippi, North Carolina, South Carolina and Tennessee: www.burr.com .

I. CRYPTO CURRENCIES, DIGITAL CURRENCIES, BLOCKCHAIN, ETHEREUM, BITCOIN, AND ICO'S[1]

A. The Different Technologies and How They are Related

Distributed Ledger Technology ("DLT") is a shared ledger of transactions or information under which each participant's copy is verified against each other's copy, such that no single "trusted intermediary" possesses or controls the transaction or information record. It is thought to avoid the "trusted intermediary" construct that presents a central authority as a single focal point for fraud, error or other perceived problems.

Blockchain is a type of DLT that uses a cryptographic hash to identify and link together blocks of information in a chain of transactions kept on a Blockchain DLT. When a block is presented to the network, its participants ("miners") use a series of complex algorithms to verify it and bring it on-chain. Blockchains may be "permissionless" (everyone can) or "permissioned" (limited participants admitted by administrator(s)).

Cryptocurrencies typically are digital assets (really, just code) signifying a store or measure of value. They are issued and traded on Blockchain.

B. A Brief Overview: What are They and What are They Used for?

A "digital asset" is an electronic record (simply code) in which someone has a right or interest. A "digitized asset" is an electronic record of an interest in a "real" asset (whether tangible or a recognized intangible right, like a security).

In February, 2018, the Swiss market regulator FINMA adopted a broad framework for categorizing various sorts of digital assets ("tokens") according to their purpose.

---

[1] Portions of these materials are adapted from the author's prior works in T. Potter, *The SEC's State of Play on Cryptocurrency*, 2 J. Robotics, Artificial Intelligence & Law 123 (2019)(©FastCase, with permission) and from materials prepared for The University of Tennessee College of Law, The Clayton Center for Entrepreneurial Law, and Transactions: The Tennessee Journal of Business Law's jointly-sponsored Conference, *Law and Business Tech CLE – Cybersecurity, Blockchain & Electronic Transactions* (Sept. 21, 2018), proceedings to be published in Vol. 20, No. 3 of TRANSACTIONS: THE TENNESSEE J. OF BUS. LAW (© Transactions: The Tennessee J. of Bus. Law, with permission).

FINMA Guidelines for ICOs § 3.1 (Feb. 16, 2016).[2] These categories are widely used, though variable in their definitions:

- ***Payment Tokens*** – synonymous with "cryptocurrencies," they are intended to be used as a store of value to be used for payment, trading or speculation, but do not give rise to any claim on their issuer. *E.g.*, Bitcoin.
- ***Utility Tokens*** – provide access to an application or service through a Blockchain infrastructure. *E.g.* Turn-Key Jet Coin, ERC20.
- ***Asset Tokens*** – represent assets, whether a claim (debt or equity) on the issuer or of underlying tangible assets for trading on-chain. *E.g.*, RMG coin (proposed by the Royal Mint Bullion Co. at 1:1g gold).[3]

Each may be combined with another in **hybrid tokens**. *E.g.* ERC20 (both payment and utility if as "gas").

C. What Industries are Using Them?

DLT and Blockchain use cases encompass any endeavor requiring widely distributed transmission and verification of information:

1. Logistics

Blockchain Wine Pte. Ltd. as an OpChain Solution for tracking and verifying the provenance of vintage wines.

TradeLens, IBM and Maersk's digitized logistics management system for maritime shipping (recently joined by the 2nd and 4th largest shipping companies): https://www.tradelens.com/

[2]https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en

[3] https://www.royalmint.com/aboutus/press-centre/rmg-and-cme-group-tech-partner-announcement/

2. Clearing and Settlement

JPM Coin is the first US bank-backed cryptocurrency -- a permissioned block-chain based technology representing a fiat currency (1:1 US$) to facilitate clearing and settlement between institutional accounts. *J.P. Morgan Press Release* (Feb. 14, 2019); *CNBC News: Finance.*

A **utility settlement coin** under development by a consortium of 14 financial firms (including UBS, Barclays, Credit Suisse, CIBC, Santander and other international banks) for clearing and settlement of cross-border trades. *Wall St. Journal* (June 3, 2019).

But Bundesbank and Deutsche Bourse Blockchain settlement test throughout 2016-2018 tested functional but actually slower than normal process. Similarly, the Depository Trust and Clearing Corporation ("DTCC"), one of the world's largest clearing and settlement businesses, sees DLT as augmenting the books and records functions of, but not wholly replacing, current bilateral settlement systems.[4]

3. Payment Processing

Facebook is expected to announce a payments cryptocurrency (code-named "Project Libra") the week of June 17 and reportedly has lined up over 12 backing companies, including Visa, Mastercard, PayPal, Uber, Booking.com and others. The coin is expected to be a stable-coin pegged to a basket of fiat currencies. *Facebook's New Cryptocurrency Gets Big Backers,* Wall St. J. (June 13, 2019).

TurnKey Jet Coin: In its *TurnKey Jet* no-action letter, the Commission Staff indicated it would not recommend enforcement action over the operation of a private, permissioned, centralized Blockchain network and smart-contract infrastructure for

[4] *Steampunk Settlement: Deploying Futuristic Tecnology to Achieve an Anacrhonistic Result,* DTCC (Q2 2019)(DLT will improve books and records, but cannot improve bilateral settlement systems, analogizing to failed Venetian payment system in 1584). http://perspectives.dtcc.com/downloads/whitepaper/steampunk-settlement-deploying-futuristic-technology-to-achieve-an-anachronistic-result

clearing and payment using a utility-token effectively functioning as a pre-paid jet card (or streetcar token). *See TurnKey Jet, Inc.* (Apr. 3, 2019).[5]

But the Staff long-ago held that similar "Koins" (like Green Stamps) were permissible: *See Kash Koin Enterprises, Inc.*, 1976 SEC No-Act LEXIS 2312 (Sept. 30, 1976), citing *Release No. 33-3890* (Jan. 25, 1958). Kash Koin: An old-school token issue.

BitPay, a cryptocurrency payment processor by AT&T.

Nike, New Balance, Facebook and others are looking into utility token payment systems.

4. <u>Health Care / Medical Records</u>

The "Holy Grail" of Blockchain for electronic health records ("EHR")…

Medicalchain, a Swiss medical-records Blockchain endeavor.[6]

In June, 2018, **Walmart** was awarded a patent for a method of obtaining a medical record stored on a Blockchain from a wearable device.[7]

Vanderbilt University developed a Blockchain-based method for sharing medical records.[8]

5. <u>Other</u>

Three largest Irish banks collaborating on digital wallets for employees' educational and regulatory credentials.

---

[5] https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm

[6] https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf

[7] http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=/netahtml/PTO/srchnum.html&r=1&f=G&l=50&s1=%2220180167200%22.PGNR.&OS=DN/20180167200&RS=DN/20180167200

[8] https://engineering.vanderbilt.edu/news/2018/team-develops-capabilities-more-secure-blockchain/

II. CRYPTO CURRENCY/DIGITAL CURRENCY LAW

A. Introduction to Distributed Ledger Technology

A distributed ledger is a large, multi-party spreadsheet (each participant with its own copy), requiring verification of any proposed transaction by a consensus of participating nodes solving the cryptographic problem required by the technology. It is like the community reputational "distributed ledger" in the stone currency of Yap, but conducted on the internet, with cryptographic protections.

DLT may be public (open to anyone) or permissioned (by a central authority or group in a private network).

Blockchain is a DLT, using the standards described by Nakamoto. Each block contains transaction data. It has a time stamp and is encoded with a cryptographic hash.

The hash applies an algorithm to reduce the block's data to string of alpha-numeric code that can be more easily processed. Blockchain uses a 256-bit Hash. Once hashed, the block is broadcast to the chain for verification. Once verified by consensus of nodes, the block is brought on-chain and appended to the previous block with accompanying cryptography to prevent any change without also changing the whole history of the chain. Each node then updates its copy of the chain.

B. Cryptocurrency Timestamping and Mining Basics

Miners solve the cryptographic problems, add blocks to the chain and receive incentives to doing so (e.g. unearthing new Bitcoins or receiving Ether as "gas"). In essence, they are paid to verify and append transactions to the Blockchain.

The original Bitcoin specified only 21 million Bitcoin could be mined and specified the reward for completing a block. However, that reward is diluted as more Bitcoin is mined. Presently the reward is 12.5 Bitcoin (as of Feb. 2019), but it periodically halves, such that in 2020 the reward will be 6.25 Bitcoin.

To earn it, a person has to mine (verify or solve) 1 megabyte (1MB) of Bitcoin transactions AND be the first miner to do so (why the time-stamp is important). A block header contains its version number, a time stamp, the hash of the prior block, the hash of

the Merkle Root (the hash of all the hashes of the prior blocks), the “nonce” (unique “number only used once”) and the target hash. The randomly-generated nonce is the key to the 64-digit hexadecimal number encoding the entire block and necessary to “unlock” the target hash (the number that block header must be less than or equal to).

The screenshot below, taken from the site Blockchain.info, might shows this information together at a glance. It is a summary of everything that happened when block #580288 was mined. The nonce that generated the "winning" hash was 248102462. The target hash is shown on top. The term "Relayed by viaBTC" refers to the fact that this particular block was completed by viaBTC, a mining pool.[9] They confirmed 2,355 transactions for this block.

Block #580288

Summary	
Number Of Transactions	2355
Output Total	2,293.32021877 BTC
Estimated Transaction Volume	323.82794691 BTC
Transaction Fees	0.35543033 BTC

[9] https://btc.com/stats/pool/ViaBTC

Height	580288 (Main Chain)
Timestamp	2019-06-11 19:45:55
Received Time	2019-06-11 19:45:55
Relayed By	ViaBTC
Difficulty	7,459,680,720,542.3
Bits	388348790
Size	1096.711 kB
Weight	3992.563 kWU
Version	0x20000000
Nonce	248102462
Block Reward	12.5 BTC
Hashes	
Hash	00000000000000000015583d17a9c501dffc2d8a0c91fc0d68f529d182782939

Previous Block	00000000000000000a8ae278af1d2766a0aeeedb6b9d1192960f260aed7da0
Next Block(s)	00000000000000000007f6557ae653c28b86f6346f411981b0618ea423ed5ec0
Merkle Root	d16509f1062975c9a3fcf19f56d93f70effdbb291f0f6bb47f9e66f2f6a512e1

Randomly generating series of nonces to "guess" at a block's target hash requires considerable computing power and energy.

See generally https://www.investopedia.com/tech/how-does-bitcoin-mining-work/

C. The Cryptocurrency Wallet Explained

A "wallet" is where you keep your currency, especially cryptocurrency. Wallets for digital assets may be online (usually hosted by an exchange or other provider), a desktop wallet, a mobile wallet, or an offline wallet (like an offline hardware device, or paper wallet).

Wallets connected to the internet are "hot storage," while offline wallets are "cold storage."

Whatever type of wallet, it stores the users "keys" – both a "public key" (a string of characters denoting the location of the records of the holder's digital assets, the "safe") and a "private key" (another string of characters) that allows individual access.

An exchange or host for an online wallet may also have access to the user's "safe" by possessing the user's or the host's own "private key."

D. Transactions, Exchanges and Swaps

Cryptocurrencies can be traded on exchanges or in P2P transactions, whether "individually" or over matching platforms.

The SEC recently issued an investor alert warning about crypto advisory and trading websites. The alert cautions investors to be especially wary of web-based crypto-currency sites with any of these red-flags:

- Outsized "guaranteed" investment returns.
- Complicated jargon or difficult-to-understand technologies.
- Unlicensed sellers.
- Sounds too good to be true.
- Unsolicited offers.
- Urgency to act.

…in short, the usual hallmarks of many scams. The advisory comes on the heels of an indictment against two Nigerian citizens for wire fraud and conspiracy to commit money-laundering through a bitcoin-based investment websites that also required "processing fees" in order to access bogus investment returns: wealthcurrency.com; boomcurrency.com; merrycurrency.com.[10]

Margin Trading

Margin trading (leveraged trading) uses Smart Contracts as self-executing automated agreements. An early example might be a stop-loss order on an equity: "If GM falls below $20/share, sell at market." For Blockchain applications, it is computer code embodying instructions for fully automated execution (without human intervention, the "smart contract") when certain pre-specified conditions are met, under "if-then" assumptions. Smart contracts rely upon information from external sources, "oracles," as data-feeds to the network. For example, CME Group has a Bitcoin Real-Time Index[11] and the Intercontinental Exchange has a cryptocurrency data feed.[12]

---

[10] DOJ's announcement of the indictment is here: https://www.justice.gov/usao-or/pr/two-nigerian-nationals-indicted-bitcoin-fraud-scheme . The SEC's alert is here: https://www.sec.gov/oiea/investor-alerts-and-bulletins/ia_fraudulentdigitalasset

[11] https://www.cmegroup.com/trading/cryptocurrency-indices/cf-bitcoin-reference-rate.html

[12] https://www.theice.com/market-data/connectivity-and-feeds/consolidated-feed/coverage-list/cryptocurrencies

Smart contracts are regarded as mitigating counterparty performance risk. But some additional inherent risks remain, including: (1) Insufficient pre-transaction specifications; (2) Coding defects, and insufficient ability to intervene, once discovered; (3) Cyber-security risks, including to oracles; and (4) Insufficient "hard-contract" considerations outside of technical concerns.

The CFTC has identified smart-contract use cases including insurance, transportation rental and credit default swaps.[13]

[13] https://www.cftc.gov/sites/default/files/2018-11/LabCFTC_PrimerSmartContracts112718.pdf