BUILDING THE NEW ECONOMY

Data as Capital

ALEX PENTLAND, ALEXANDER LIPTON,
AND THOMAS HARDJONO

MIT Connection Science & Engineering
connection.mit.edu

The MIT Press
Cambridge, Massachusetts
London, England

6

THE TRADECOIN SYSTEM

Alexander Lipton, Thomas Hardjono,
and Alex Pentland

6.1 INTRODUCTION

Central to any economy is a medium of exchange and a store of value: money. We often think of money in the context of banks and finance, but some variation on the basic idea of money is critical to supply chains, service businesses, labor contracts, retirement planning, and more. Today, we mostly use fiat currencies issued by national governments, but there is also well-functioning "money" issued by cooperatives, national alliances, and mutual funds.

An example of a cooperative issuing "money" is the Swiss WIR, created in 1934 (during the Depression) by a cooperative of local businesses and landholders in order to spur local development, which is backed by local property and infrastructure. The International Monetary Fund's special drawing rights are backed by a basket of national currencies and issued to countries typically for national development purposes. Exchange-traded funds (ETFs) are digital certificates giving ownership rights to a basket of company stock shares or bonds.

Today, there is tremendous interest in the possibility of using cryptotechnologies and ETF-style assets to replace physical cash and national currencies. Although the notion of electronic cash (eCash) has been around for almost three decades (see, e.g., Chaum[1] and Chaum, Fiat, and Naor[2]), it was the emergence of the Bitcoin[3] system that provided the first working example of a payment system that operated based on a peer-to-peer network and could scale up operations in a decentralized fashion.

In this chapter, we outline an approach to building a consortium of sponsors, who contribute real assets; a narrow bank, handling financial transactions involving fiat currencies; and an administrator, who issues the corresponding digital token in exchange for fiat payments and makes fiat payments in exchange for digital tokens. In short, our idea is to apply distributed ledger technology to give a new lease on life to the old notion of a sound asset-backed currency and to use this currency as a transactional tool for a large pool of potential users, including small and medium-sized enterprises and individuals.

Most recently, we have seen Facebook back the Libra digital currency and the Chinese government back its own national digital currency, as well as a variety of banks beginning to use their own digital currencies in order to transfer money between partner banks. In this chapter, we will describe how to build a currency whose governance is transparent, and thus can be regulated, and encourages legitimate commerce but makes illegal activities difficult.

6.2 THE DIGITAL TRADECOIN (DTC)

In essence, we wish to replace physical cash with a supranational digital token, which is insulated from adverse actions by central banks and other parties because it is asset backed. We believe the DTC is ideally suited as a medium of exchange for groups of smaller nations or supranational organizations who wish to use it as a counterweight to large reserve currencies.

Supranational currencies have been known for two millennia. For instance, Roman, and later Byzantine and Iranian, gold coins were used along the entire Silk Road; Spanish and Austrian silver coins were a prevalent medium of exchange during the Age of Sail. Closer to our time, the British pound was used as the reserve currency for the British Empire and, to a lesser degree, the rest of the world; the US dollar and the pound were used as a reserve currency basket for the world economy in the twentieth century, to which the euro and the yen were added in the late twentieth century; and now the yuan might be used along a revived Silk Road.

Today, for the first time ever, there is the possibility of designing a digital currency that combines the best features of both physical cash and digital currencies, including finality of settlement, partial anonymity, and usability on the web. This currency is largely immune to policies of central banks that control the world's reserve currencies. Such a currency has enormous potential to improve the stability and competitiveness of trading and natural resource producing economies. In the DTC, we propose to develop a trade-oriented asset-backed digital currency aimed at facilitating international trade and making it as seamless as possible. This currency will be based on a proprietary framework combining the most recent advances in blockchain and distributed ledger technology, cryptography, and secure multiparty calculations, together with time-tested methods for preventing double spending. In view of the fact that our framework relies in part on our own research and in part on ideas readily available in the public domain, we do not anticipate specific issues related to intellectual property rights. Unlike Bitcoin, it will be fast, scalable, and environmentally friendly. It will also be transaction-friendly because of its low volatility versus fiat currencies, not to mention cryptocurrencies.

Over the past decade, potential advantages and disadvantages of distributed ledgers or blockchains have been discussed by numerous researchers. (see, e.g., Lipton[4] and references therein). While numerous potential applications of blockchains have been entertained in the literature—including title deeds, posttrade processing, trade finance, rehypothecation, and syndicated loans, to mention but a few, the main use of blockchains has so far been in the general area of payments, more specifically cryptocurrencies.

Worldwide interest in distributed ledgers was ignited by Bitcoin, which is a cryptocurrency protocol operating without a central authority. It was described first in the seminal white paper by S. Nakamoto.[5]

Since then, Bitcoin has inspired the creation of more than a thousand other cryptocurrencies, all with various degrees of novelty and utility (if any). One of the most promising is Ethereum, which is significantly more versatile than Bitcoin, not least because it supports so-called smart contracts.[6] Another interesting and popular cryptocurrency protocol is Ripple.[7] The Ripple system departs from the Nakamoto consensus approach. Because it does not rely on the thousands of anonymous (pseudonymous) mining nodes that form the peer-to-peer network underlying Bitcoin, it is not truly decentralized. Instead, the Ripple system uses a small set of nodes that act more like notaries, validating transactions at a higher throughput and much lower cost than Bitcoin. Unlike

Bitcoin, most entities in the system are known and not anonymous. By their very nature, all these currencies are native tokens residing on a blockchain. Their transition from one economic agent to the next is controlled by the set of rules that are inherent or "hardwired" in the blockchain setup and are needed to maintain the integrity of their blockchain as a whole. However, until now, attempts to build tokens backed by real-world assets—first and foremost, fiat currencies—have been unsuccessful. Yet, until this all-important problem is solved, it is virtually impossible to make cryptocurrencies part of the mainstream financial infrastructure, because otherwise the inherent volatility of cryptocurrencies will severely curtail their usability.

Although the potential application of distributed ledgers mentioned earlier, such as posttrade processing and trade finance, is particularly important, they are technical in nature and lack the revolutionary spirit. However, a distributed ledger can potentially play a truly transformative role and bring a dramatic departure from the past by making central bank digital currency (CBDC) and stable cryptocurrencies a reality.

Here, we propose a stable, asset-backed cryptocurrency, which we refer to as DTC. It can be viewed as a natural extension of a fiat-backed cryptocurrency called the utility settlement coin (USC) (see Lipton, Pentland, and Hardjono[8]). Setting aside operational aspects of gathering and managing collateral assets, we need to design a ledger associated with value transfers. Since, by design, Nakamoto's approach is neither scalable nor efficient, we need to use a different design. Our analysis indicates that combining blockchain with an earlier approach for issuing electronic cash (eCash), developed by Chaum,[9] seems to be promising. Recall that

Chaum introduced a blind signature procedure for converting bank deposits into anonymous cash. On the one hand, Chaum's protocol is much cheaper, faster, and more efficient than Bitcoin. It also offers an avenue toward true anonymity and unlinkability (as in paper cash), as compared to the weak pseudoanonymity of Bitcoin. If true anonymity is not desired, there are variations on the Chaum approach on offer; for instance, anonymity for the purchaser but not for the seller and so forth. However, on the other hand, the basic Chaum model and many of its variants rely on the integrity of the issuing bank. To alleviate this issue, we propose the use of blockchain technology itself to track the relevant transaction parameters, reducing the opportunity for parties to be dishonest. Payments between users are still direct, as in Chaum's proposal.

In the DTC, we propose a solution to the stable cryptocurrency problem, which boils down to assembling a pool of *assets*, contributed by *sponsors*; appointing an *administrator*, who will manage the pool; and digitizing the ownership rights on this pool. In addition, we build a special-purpose *narrow bank*, which facilitates activities of the administrator. By construction, neither the pool itself nor the supporting bank can fail because of market and liquidity risks. Their operations are streamlined as much as possible to limit operational risks. It is worth noting that operational risks are always present; this statement is true not only for the setup we are proposing but also for ordinary cash and bank deposits, not to mention cryptocurrencies, which are notorious for their operational risk exposure. The narrow bank receives fiat currency submitted by the users and passes it to the administrator and ultimately to sponsors, while the administrator issues digital tokens in return. These tokens will circulate within the group of users in a fast and efficient manner by utilizing a distributed ledger mechanism, thus creating native tokens proportionally convertible into the underlying assets at will. Their value is maintained in a relatively narrow band around the value of the underlying asset pool, with the lower bound enforced by arbitrage and the upper bound enforced by the administrator, assisted by sponsors.

The key insight of the chapter is that the properly designed DTC can serve as an international reserve currency, remaining stable in the long run and serving as a much-needed counterbalance to fiat currencies issued by individual nations, which can be easily affected by their respective central banks.

The chapter is organized as follows. Background on asset-backed currencies is discussed in section 6.3. The design of Bitcoin and Ripple, including their similarities and differences, is outlined in section 6.4. CBDC and the closely related USC, respectively, are discussed in section 6.5. DTC is discussed in section 6.6. Section 6.7 briefly discusses the Tradecoin system architecture, and section 6.8 explores the Chaumian eCash model using the assistance of ledgers. Section 6.9 looks at the notion of an environmentally friendly DTC coins. Conclusions are drawn in section 6.10.

6.3 INTRODUCTION TO ASSET-BACKED CURRENCIES

The idea of anchoring the value of paper currency in baskets of real assets is old (see, e.g., Haas et al.[10]). Gold and silver as well as bimetallic standards have been used for centuries to achieve this goal. Two approaches are common: a redeemable currency backed by a basket of commodities or a tabular standard currency indexed to a basket of commodities.

Lowe[11] was the first to explain how to use a tabular standard of value to control price inflation; a similar plan based on a basket of 50 commodities was developed by Scrope.[12] Jevons[13] pushed these ideas (much) further and proposed an indexation scheme based on a basket of 100 commodities, while Marshall[14] proposed a similar tabular standard.

Inspired by developments during the Great Depression, F. Graham[15] developed an automatic countercyclical policy based on 100 percent backing of bank deposits by commodities and goods, while B. Graham[16] proposed backing the US dollar with a basket of 60 percent commodities and 40 percent gold. Hayek[17] advocated establishing a universal basket of commodities, which every country would use to back its currency. At roughly the same time, Keynes[18] designed an international gold-linked multilateral transaction currency, which he called the bancor. Unfortunately, his ideas were discarded by the architects of the Bretton Woods system.

Since World War II, interest in commodity-based currencies has been lukewarm. Still, Kaldor[19] proposed a new commodity reserve currency, which he also called bancor. More recently, Zhou[20] proposed a new international reserve currency anchored to a stable commodity basket benchmark.

The choice of the actual asset basket backing DTC is not an easy one. It is dictated partly by the composition of the sponsors' pool and partly by what assets they actually possess and are willing to contribute. For instance, depending on their resources and abilities, sponsors can contribute oil, gold, base metals, and agricultural commodities. Given that storage of significant amounts of these resources is difficult and costly, it is natural to use collateral, which is in storage already, thus making stored commodities economically productive.

When discussing asset-backed currencies, it is necessary to mention the WIR, which is both an abbreviation of *Wirtschaftsring* (economic circle) and the word *we* in German. This wordplay emphasizes WIR's dual role as an economic circle and a community. According to WIR's statutes, "Its purpose is to encourage participating members to put their buying power at each other's disposal and keep it circulating within their ranks, thereby providing members with additional sales volume." WIR issues a purely digital private currency. Participants can use WIR in combination with the Swiss franc as part of dual-currency transactions. Thus, we can view WIR as an analog precursor of the DTC.

WIR serves small and medium-sized enterprises as well as private individuals. It was founded in 1934 to address currency shortages and global financial instability, receiving a banking license in 1936. In the beginning, WIR's founders followed the theory of Silvio Gesell, which requires that money be free from interest; however, the WIR Bank eventually (and unsurprisingly) renounced Gesell's ideas in 1952 and introduced monetary interest. WIR gradually grew from its original 16 members in 1934 to more than 60,000 today. Total assets are approximately 5.3 billion Swiss francs (CHF), loans 4.5 billion CHF, and deposits of 3.9 billion CHF as of the end of 2016.

A particularly important fact about the WIR franc is that it is an electronic currency reflected in clients' trade accounts and not represented by paper money. Thus, the WIR bank maintains the entire ledger. The initial purpose of the currency was to increase sales, cash flow, and profits for qualified participants. Eventually, WIR created a credit system that issues credit in WIR francs, (over)collateralized by assets, which ensures that the currency is fully asset backed.

New WIR francs are created when a loan is issued, and they are destroyed when it is repaid, but a small amount of interest stays in the system forever and contributes to bank profits. A typical transaction between two members involves payment in both Swiss francs and WIR francs, thus reducing the amount of cash needed by the buyer but without the seller discounting the price of their product or service.

6.4 EXISTING CRYPTOCURRENCIES

In this section we briefly review the Bitcoin and Ripple systems for electronic currency.

6.4.1 Bitcoin

Since it was first announced in 2008, Bitcoin[21] has captured the imagination of the public by proposing the first cryptographic electronic currency having no intrinsic value, issued without central authority, and capable of peer-to-peer digital transfers. Anyone can join the Bitcoin ecosystem, which is both a strength and a weakness.

Because it's currently the best-known form of cryptocurrency, it's worth exploring how Bitcoin works. Financial transactions are made directly between users, without the help of designated intermediaries. Transactions are publicly broadcast and recorded in a "blockchain ledger," which can be seen by all participants.

Once a transaction is broadcast, the "miners" come into play. They aggregate individual transactions into blocks (currently of about 2,000 transactions each), verify them to ensure that there is no double spending by competitively providing *proof of work* (PoW), and receive mining rewards in bitcoins. The proof of work is based on finding a cryptographic random number (called a *nonce*) that makes the hash value of the candidate block of transactions lower than a given threshold. Therefore, the "hash power" (i.e., hardware and software processing capacity) of a node makes a difference in the likelihood that the node will find the match.

It is assumed (but not proven) that there are sufficiently many honest miners that collusion among them (known as a 51 percent attack) is not possible. A transaction is considered confirmed if there are at least six new blocks built on top of the block to which it belongs. The Bitcoin ecosystem is not without very serious issues—it can handle no more than 7 transactions per second (vs. Visa, which can handle more than 20,000 transactions per second), and it consumes enormous amounts of electricity used by miners (by virtue of the underlying PoW computation). Thus, the immutability of Bitcoin's blockchain ledger and the prevention of double spending are achieved through mining based on PoW.

In view of this, bitcoins themselves are just unspent transaction outputs of a long chain of transactions, which can be traced all the way back to the time when they were minted, either to the very first "genesis" block or as part of a "coinbase" transaction included in a block by a successful miner.

Since Bitcoin's inception in 2009, its price has gone up several orders of magnitude, making it the darling of speculators across the globe. However, a word of caution is in order. Since a bitcoin has no value, it can have any price; hence one should not be surprised if its price falls dramatically. Other than for speculative purposes, a bitcoin's uses are rather limited, because its price versus the US dollar and other fiat currencies is extremely volatile, which prevents it from becoming a medium of transaction. In addition, in spite of claims to the contrary, Bitcoin transaction costs are very high and growing.

Although Bitcoin may not be the disruptive force its supporters are claiming, the distributed ledger technology underpinning it has clear potential to transform the financial ecosystem as a whole.

6.4.2 Ripple

Ripple is a money transfer protocol; ripple is the underlying native currency. It is completely different from Bitcoin. For starters, ripples are preminted, while bitcoins are mined. In fact, Ripple is not decentralized at all. The stated purpose of the protocol is to facilitate fiat currency transfers among participating banks. However, because there is a native token, Ripple can be used along the lines of Bitcoin as well. Details of how Ripple works are given in various Ripple promotional materials, including its white paper.[22]

The main ingredients of the Ripple ecosystem are servers, which maintain the ledger; clients, who can initiate transactions; proposers, which can be any server; and the unique nodes list (UNL), indicating parties that can be trusted by the participants in the protocol.

The life cycle of a single transaction consists of several steps. First, a transaction is created and signed by an account owner. Second, this transaction is submitted to the network. If it is badly formed, this transaction may be rejected immediately; otherwise, it is provisionally included in the ledger. Validating nodes propose new ledger updates. Transmitting nodes broadcast the ledger updates to the network. Consensus is achieved by voting of the validators. The result of a successful consensus round is a validated ledger. If a consensus round fails, the consensus process repeats until it succeeds. The validated ledger includes the transaction and its effects on the ledger state.

Ripple's consensus assumptions are that every nonfaulty server makes decisions in finite time; that all nonfaulty servers arrive at the same decision; and that *both* true and false decisions regarding a given transaction are possible.

The Ripple protocol consensus algorithm (RPCA) works in rounds. Initially, every server compiles a list of valid candidate transactions. Then, each server amalgamates all candidates coming from its UNL and votes on their veracity. Next, transactions passing the minimum threshold are passed to the next round. The final round requires 80 percent agreement. In general, RPCA works well; however, it can fail when validating nodes form cliques, which cannot agree with each other.

6.5 CBDC AND USC

In this section we discuss the possibility of central banks issuing digital currencies, in the form of a CBDC or USC.

6.5.1 CBDC

Could and should central banks issue central bank digital currency? Recently, a previously academic question of the feasibility and desirability of CBDC came to the fore (see, e.g., Ali et al.[23] and Scorer[24]). By issuing CBDC, states can abandon physical cash in favor of its electronic equivalent and replace a large chunk of government debt with it. The impact on society at large will be huge.[25] CBDC can obviate the need for fractional banking and dramatically improve the stability of the financial system as a whole. On the other hand, the ability of the banking sector to create money "out of thin air" by making loans will be significantly curtailed and transferred to central banks. It is clear that developments in this direction are inevitable, but their timing and magnitude are uncertain.

Interest in CBDC has been ignited by two unrelated factors—the introduction of Bitcoin and the persistence of negative interest rates in some developed countries. In Medieval Europe, negative interest existed in the form of demurrage for centuries. Recall that demurrage is a tax on monetary wealth. In principle, demurrage encourages spending money rather than hoarding it, thus accelerating economic activity. The idea of demurrage was reborn shortly after World War I, in the form of scrip money, which requires payment of periodic tax in order for it to stay in circulation. Scrip money was proposed by German-Argentinian entrepreneur and economist Silvio Gesell,[26] whose idea was restated by Irving Fisher during the Great Depression.[27] Demurrage was thought to be a suitable replacement for mild inflation. Since in the modern economy demurrage is hard to orchestrate because of the presence of paper currency, its conversion into the electronic form is necessary for making seriously negative rates a reality.[28]

Currently, there are three approaches to creating CBDC on a large scale:

- Economic agents, from enterprises to private individuals, can be given accounts with central banks. However, in this case, central banks would have to execute know your customer (KYC) and anti-money-laundering (AML) functions, tasks that they are not equipped to perform. Besides, under duress, rational economic agents might abandon their commercial bank accounts and move their funds to central bank accounts, thus massively destabilizing the entire financial system.

- Inspired by Bitcoin,[29] CBDC can be issued as a token on an unpermissioned distributed ledger, whose integrity is maintained by designated notaries receiving payments for their services (see, e.g., Danezis and Meiklejohn[30]). Given that notary efforts do not require mining and hence are significantly cheaper and faster than those of Bitcoin miners, this construct is scalable and can satisfy needs of the whole economy. Users are pseudonymous since they are represented by their public keys. Since at any moment there is an immutable record showing the balance of every public key, it is possible to deanonymize transactions by using various inversion techniques applied to their recorded transactions,[31] thus maintaining AML requirements.
- A central bank can follow the Chaumian scheme[32] and issue numbered and blind signed currency units onto a distributed ledger, whose trust is maintained either by designated notaries or by the bank itself. In this case, it would have to rely on commercial banks, directly or indirectly, for satisfying the KYC/AML requirements.

To summarize, by using modern technology, it is possible to abolish paper currency and introduce CBDC. On the positive side, CBDC can be used to alleviate some of the societal ills and eliminate costs of handling physical cash, which are of the order of 1 percent of a country's GDP. It can help the unbanked participate in the digital economy, thus positively affecting society at large. On the negative side, it can give central authorities too much power over the economy and privacy, which can potentially be misused.

While CBDC is absolutely stable with respect to the underlying fiat currency, it does not make the fiat currency stable in itself. For that, we need a carefully constructed DTC.

6.5.2 USC

CBDC is technically possible but politically complicated. Hence, several alternatives have been proposed. One promising venue is USC, which was developed by a consortium of banks and a financial technology start-up called Clearmatics.[33] Initially, USC can be an internal token for a consortium of participating banks. These coins have to be fully collateralized by electronic cash balances of these banks, which are held by the central bank itself. Eventually, these coins can be circulated among a larger group of participants. However, in this case, issuance of USCs has to be outsourced to a narrow bank, which can perform the all-important KYC and AML functions.

Recall that a narrow bank has assets, which include solely marketable low-risk securities and central bank cash in an amount exceeding its deposit base per the regulatory prescribed capital cushion (see, e.g., Pennacchi[34] among many others). As a result, such a bank is impervious to credit and liquidity shocks. However, like any other firm, it can be affected by operational failures, including fraud, computer hacking, inability to solve the KYC/AML problem, and others. These failures can be minimized, but not eliminated, by using proper modern technology. Accordingly, narrow bank deposits would be as close to the fiat currency as technically possible.[35] Ideally, one narrow bank per fiat currency is required. Further details are given in Lipton, Pentland, and Hardjono.[36]

USC is helpful from a technical perspective, but it does not solve issues of monetary policy. We wish to address this issue by building a counterweight for fiat currencies by backing the DTC with a pool of real assets.

6.5.3 Survivability of CBDC and USC

The idea that a blockchain system can withstand a concerted attack simply because it consists of physically distributed nodes is an untested and unproven proposition. The possible types of attacks to a blockchain system have been discussed elsewhere and consist of a broad spectrum. These range from classic network-level attacks (e.g., network partitions, distributed denial of service) to more sophisticated attacks targeting the particular blockchain-specific constructs (e.g., consensus implementations) or targeting specific implementations of mining nodes or notaries (e.g., code vulnerabilities, viruses). An attack on a blockchain system may not need to cripple it entirely, as degradation in its overall service quality (e.g., slower transaction throughput) may be sufficient to disincline users to use the system.

The notion of *interoperability* across blockchain systems is an important one in the light of survivability.[37] The internet was able to expand and allowed *autonomous systems* (i.e., routing domains) to interconnect with one another because of good design principles. The design philosophy of the internet is based on three fundamental goals: (1) network survivability (internet communications must continue despite loss of networks or gateways); (2) variety of service types (the internet must support multiple types of communication services); and (3) variety of networks (the internet must accommodate a variety of networks). We believe the same fundamental goals must be adopted for the current development of blockchain technology—and more specifically they must drive the technological selection for the implementations of the DTC architecture.

6.6 DTC MOTIVATIONS AND REQUIREMENTS

There are several issues, technical and economical, with regards to DTC and ledger-based implementations. We discuss these in the following section.

6.6.1 DTC Motivations

Bitcoin and Ripple protocols can be used as a prototype for a cryptocurrency based on a distributed ledger that is more suitable for financial transactions. Several issues, some technical and some economic, have to be addressed before this goal can be achieved:

- The KYC problem has to be formulated and articulated, and a suitable framework for solving it has to be designed
- An AML mechanism has to be developed
- A highly efficient method for maintaining consensus on the ledger, with industrial-strength transactions per second (TpS) capabilities, has to be built
- A transparent and economically meaningful system for issuing new DTCs and retiring the existing ones has to be implemented
- Most importantly, a satisfactory mechanism for making DTC a stable cryptocurrency has to be designed

Although public ledgers are not truly anonymous but rather are pseudonymous, it is difficult to use them in the KYC/AML compliant fashion. Accordingly, the DTC ledger has to be made semiprivate (but probably not private) in order to solve the KYC/AML problem. At the same time, the right balance has to be struck between privacy and accountability so excessive restrictions do not impede the flow of legitimate commerce.

In order to achieve the level of speed and efficiency we desire, including a TpS on the order of several thousand, the Ripple-style consensus protocol has to be used. Following Ripple's approach, we choose a group of notaries who are known in advance and properly licensed. These notaries are responsible for updating the ledger and maintaining its integrity by ensuring Byzantine fault tolerance (see, e.g., Lamport, Shostak, and Pease[38] and Castro and Liskov[39]). For their services, notaries are paid a small fee, say a percentage of the transaction amount they approve, which is naturally denominated in DTC so that their commercial interest is aligned with their function. If notaries stay inactive or systematically approve invalid transactions, they are penalized financially. In each round, validators create their own versions of the ledger and propose them to the rest of the group. Several rounds of voting take place until a supermajority candidate ledger is selected. This approach is similar in spirit to the well-known Paxos algorithm. In order to increase the TpS number, we use the idea of sharding and assign individual notaries to particular sets of addresses. In this setup, a quorum verifies its own shard, while the full ledger is assembled out of the corresponding shards.

The DTC architecture recognizes that there are two or three types of application-level transactions commonly found in many blockchain implementations. The first is the one-party recording of assets to the ledger. Logically, the DTC represents this on an *assets ledger*. The second type is the two-party transfer transaction, exemplified by the transfer of coins from one party to another. The DTC captures these logically on the *coins ledger*. The third type of transaction is the off-chain transfer of value (i.e., eCash) in a privacy-preserving manner. Here the goal is to allow a limited amount of coin-backed anonymous eCash to be transferred from one user to another, following the classic Chaum approach. Relevant parameters of the eCash flow are recorded on the DTC *tracking ledger* in order to reduce the opportunity of fraud by entities involved in the eCash flows.

This design decision of recognizing the three types of application-level transactions provides the broadest flexibility for the DTC architecture to be tailored for specific use cases and for different implementations of the three ledgers to be chosen according to the requirements of the use case.

6.6.2 Creation and Annihilation of DTC

For now, we consider this pool and its associated narrow bank as given and describe the creation and annihilation mechanisms for the DTC. New coins are injected into the distributed ledger by virtue of the following mechanism. During the initial stage, participants who wish to acquire a freshly minted DTC have to proceed as follows. First, they must have a conventional fiat account, which can be held either directly with the narrow bank or with their commercial bank. Second, they have to open an initially empty wallet ready to accept DTCs. Third, participants transfer the desired amount of fiat currency to the narrow bank. Fourth, the narrow bank transfers these funds to sponsors, who in turn release some of the DTCs created when the asset pool is built to the pool administrator. Fifth, the administrator transfers the corresponding DTCs from its public-key address to the public-key address provided by the participant. Thus, in effect, the participant becomes a shareholder in the pool administrator. Subsequently, participants can acquire DTCs from other participants in exchange for goods and services, so a newborn DTC starts its journey from one address represented by a public key to the next, until it is annihilated by a participant sending it to the administrator in exchange for cash. When a participant in the ledger wishes to receive fiat currency for their DTC, they transfer DTCs from their public key to the public key of the administrator, who in turn sells an appropriate proportion of the assets and deposits proceeds with the associated narrow bank, which in turn credits fiat currency either to the account on its own ledger or to a designated account in a different bank. The corresponding DTCs are destroyed by sending them to the "terminal" public key without a private key.

As a result, the administrator is in possession of real assets, sponsors receive fiat currency, and the general public receives DTCs, which can always be converted into fiat at the current market price.

6.6.3 Mechanisms of Stabilization of DTC

Finally, the value of the DTC is kept relatively stable by virtue of the independent actions of participants and the administrator. If the value of a DTC goes below the value of the fraction of the asset pool it represents, which we call its intrinsic value, then rational economic agents will turn it back to the administrator in exchange for cash. If, on the other hand, the market value starts to deviate upward compared to the intrinsic value, then, after a certain threshold is breached, the sponsors will contribute more assets to the pool, which can come from their own sources or be purchased on the open market, in exchange for DTCs, which they will sell on the open market, thus pushing the market price of DTCs down. These two complementary mechanisms can keep the market price of the DTC in a bank around the market price of the underlying basket.

More precisely, the price P_{DTC} of DTC will be close to (but not exactly at) the market price of the corresponding asset pool, P_M. Indeed, if P_{DTC} falls significantly below P_M, economic agents will give DTC back to the administrator, who will have to sell a fraction of the pool's assets for cash and pass the proceeds to these agents. If P_{DTC} increases significantly above P_M, sponsors will supply more assets to the administrator, who will issue additional DTC and pass it to sponsors, who will sell it for cash, just pushing the price down. This mechanism ensures that $|P_{DTC} - P_M|/P_M << 1$, a very desirable feature, especially compared to conventional cryptocurrencies, which habitually exhibit extreme volatility. At the same time, outright manipulation by central banks is not possible either. Note that the notion of economic agents (e.g., sponsors with assets) is distinct from system entities (e.g., notaries) in the DTC architecture.

6.7 ARCHITECTURE AND DESIGN PRINCIPLES

In order for DTC to be a stable and durable digital currency that can store value as well as provide utility, there are a number of principles driving its architecture. The DTC architecture seeks to be a “blueprint” that allows the DTC to be implementable for various use cases. Some use cases that have been identified are as a reserve digital currency shared by a number of geopolitically diverse small countries as a means of providing local financial stability and as a digital currency operating for a narrow bank that can provide relative stability during financially volatile periods. A number of system design principles are as follows:

- *Unambiguous identifiability and ownership of properties* Assets (represented digitally), coins, and eCash must be uniquely identifiable and have unambiguous ownership at any given time. A corollary of true ownership is that these must be transferable (portable) by their owner.
- *Identifiability of entities and devices* All entities (e.g., sponsors) must be uniquely identifiable using identifiers that are legally recognized (e.g., legal entity identifier[40]). Similarly, all devices interacting on the blockchain must be uniquely identifiable, and each device must have an owner. Additionally, the users and devices must be authenticable.

Anonymity of node devices may lead to concentrations of hash power.[41] In some permissionless blockchain networks, any entity can take the role of a mining node and be identified on the blockchain solely by their public key (i.e., "address"). Although this anonymity may be considered a virtue in some blockchain networks (e.g., Bitcoin[42]), there may be some disadvantages to this approach. One disadvantage is the potential for the amassing (centralization) of hashing power by a handful of anonymous nodes or entities, which goes against the proposition of decentralization of the blockchain paradigm. Such entities could conceivably use this concentration of hash power to skew or manipulate the network over time.

- *Visibility into shared state* Entities in the ecosystem should have visibility into the state of the DTC system and network and have equal access to such information. More specifically, this means visibility into the assets that back the issuance of coins and visibility into the circulation of coins and eCash.

- *Mechanisms implementing monetary policies* In order for the DTC ecosystem to operate according to the desired community behavior, there must be technical mechanisms that allow agreed policies to be carried out in the system as a whole. Such mechanisms can be controlled centrally (e.g., by a single entity), controlled in a group-oriented manner (e.g., by consensus of entities), or a combination of both (e.g., by leader election protocols).
- *Correct, accurate, and unhindered systemwide reporting* Each system component that implements DTC must be unhindered in the reporting of its internal state. Furthermore, there must be ways to validate the reported state so misbehavior can be detected and acted on. Such misbehavior can be the result of human or system error, degradation in system components over time (hardware and software), or active or passive compromises (i.e., attacks).
- *Well-defined operations (limited programmability)* One of the key factors in the success of the Bitcoin[43] system is the very limited number of available operations (op-codes). These operations are geared toward a very specific application of the blockchain: electronic peer-to-peer payments. This is in contrast to the Ethereum system,[44] which was touted to be a highly programmable platform for distributed applications. However, the high degree of programmability may be a double-edged sword in the sense that human error and malicious code can be deployed on the platform and harm other users or applications (e.g., DAO Hack[45]).

These system design principles borrow from a number of key design principles underlying the internet.[46] The need for unambiguous ownership of an asset is an obvious one. The DTC seeks to use standard object identification solutions (e.g., the globally unique identifier (GUID) standard) for digital assets. The legal ownership of assets is a construct that is external to the DTC system and as such must be established prior to assets being introduced by their legal owner (e.g., sponsor) into a given DTC deployment.

The principle of visibility is driven by the need for entities in a DTC implementation to have equal access to data, and it is implemented through the assets ledger and coins ledger. The consortium administration must have full visibility into all operational aspects of a given DTC implementation. Certain DTC implementations may restrict visibility of parts of the systems (e.g., assets ledger) to entities that have “skin in the game” (e.g., sponsors who have actual assets on the DTC assets ledger).

A key aspect of the success of a DTC implementation is the ability of the consortium to carry out monetary policies and other governance rules in the system as a whole. Technical mechanisms can be implemented as “hooks” or control points through which policy decisions are executed. For example, a DTC implementation may require that each sponsor have assets (in the assets ledger) above a given threshold (i.e., reserve ratio) at all times. The actual value of the threshold should be dynamically adjustable according to the consortium-agreed policies and be carried out by the consortium administration as the appointed authority. In this case, the consortium administration can transmit a special “policy implementation” transaction (to the assets ledger and coins ledger) setting the new threshold value. Notaries observe such policy decisions by declining an asset-to-coin conversion transaction from a sponsor if it causes the sponsor’s asset reserves to dip below the new threshold value.

Key to the operation of a DTC implementation is the ability of entities to identify and authenticate each other. We believe this is closely related to the principle of systemwide reporting. Some DTC implementations may choose to deploy advanced cryptographic techniques that provide anonymity and untraceability of entities. However, such features must still satisfy the principle of unambiguous identifiability and mutual authentication.

6.7.1 Sponsors, Consortium, and Users

There are a number of active (human-driven) entities in the DTC ecosystem (figure 6.1):

- *Sponsor* A sponsor is an entity who supplies assets to the DTC ecosystem in return for coins. The community of sponsors forms a consortium tasked with the various management aspects of coins and eCash in the ecosystem.
- *Consortium* A community of sponsors forms a consortium operating under an agreed governance model that specifies the

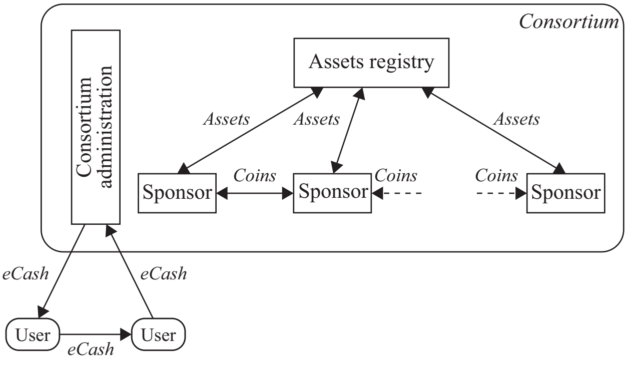

Figure 6.1
Tradecoin entities.

legal, business, and technical operational rules of members of the consortium. In essence, the consortium is a network of sponsors who are participating in the DTC ecosystem.

Additionally, a *consortium administration* carries out the monetary policies of the membership of the consortium. The consortium administration is legally empowered by the consortium membership to implement (centralized) control over certain system functions.

- *Users* A user is an entity that obtains eCash from the consortium for the purpose of making payments for goods and services from other users.

6.7.2 Logical Functions

The DTC architecture logically separates functions into those pertaining to assets, coins, and eCash (figure 6.2). Here, to allow us to focus on logical functions that meet the system design principles stated earlier, we use the term *ledger* generically without calling out specific realizations.

Specific technical implementations of the ledger may include a distributed database system, a peer-to-peer network of nodes, a fully distributed blockchain system, or even an append-only single database system.

- *Assets management* Visibility into the assets that sponsors contribute in exchange for coins represents a foundational requirement in DTC. DTC employs an *assets registry* and an *assets ledger*. The registry records verified real-world assets associated with a sponsor, who forwards that asset to the consortium.

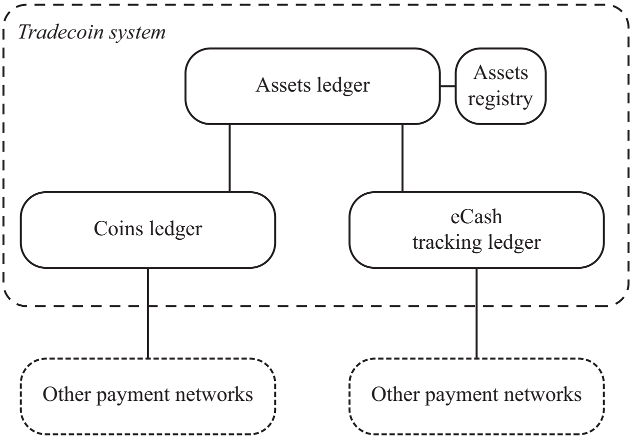

Figure 6.2
The assets ledger, coins ledger, and eCash tracking ledger.

The assets ledger captures the binding between real-world assets (put forward by a sponsor) and the amount of coins equivalent to (proportional to) those assets. The assets ledger also records the proportion of coins that are in the consortium's reserves and those that are in a sponsor's reserve. These coin equivalents are considered noncirculation.

- *Coin circulation* Allowing sponsors to exchange (i.e., sell or lend) their asset-backed coins with each other represents a cornerstone of DTC. The *coins ledger* records the coin movements and transactions in the DTC ecosystem (figure 6.4). The coins ledger is used by sponsors and the consortium administration. Sponsors exchange or "trade" coins with each other on this ledger.

- *eCash circulation* Providing stable digital currency to users also represents a cornerstone of DTC. The eCash *tracking ledger* records the movement of eCash (i.e., cryptographic keys and parameters) between users.

Each of the three ledgers in DTC are independent but are connected in the sense that a transaction in one ledger may refer to (point to) recorded transactions in other ledgers. This independence of ledgers is important not only from the perspective of technological choice (i.e., adoption of new ledger technologies) but also crucial to the operational resilience of the system as a whole.

An example of the connection of the ledgers is the "pushing" (or pulling) of coins into (or out of) circulation by a sponsor following the policies of a given DTC implementation. When a sponsor seeks to have its assets (on the assets ledger) converted to coins and for the resulting coins to be accessible by the sponsor on the coins ledger, the sponsor must transmit a push transaction. This results in a transaction occurring on the assets ledger and a corresponding transaction occurring on the coins ledger. These two transactions—albeit on different ledgers—are related in that one refers to (i.e., carries a hash of) another. In the push case, the transaction on the coins ledger points to a completed transaction on the assets ledger.

6.7.3 Converting Assets to Coins

The purpose of the assets ledger together with the assets registry is to satisfy the design principles with regard to the conversion of real-world assets into their coin equivalent (see figure 6.3).

A key requirement here is the validation of the legal ownership of assets as claimed by a given sponsor. The sponsor must provide legal evidence in such a way that a digital representation of the evidence can be captured and presented within the assets ledger.

Examples of such evidence include a paper certificate and its digital representation that has been digitally signed by the issuer using legally acceptable digital-signature technology (e.g., the Digital Signature Act of 2000). For example, a digital version of a gold certificate (e.g., unallocated gold) could be signed by an authority and presented by a sponsor as evidence. It is the responsibility of the consortium administration to validate the evidence.

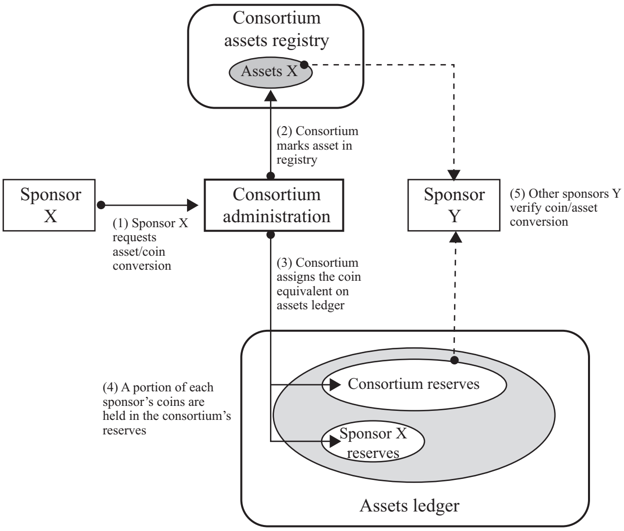
Consortium assets registry
Assets X
(2) Consortium marks asset in registry
Sponsor X
(1) Sponsor X requests asset/coin conversion
Consortium administration
Sponsor Y
(5) Other sponsors Y verify coin/asset conversion
(3) Consortium assigns the coin equivalent on assets ledger
(4) A portion of each sponsor's coins are held in the consortium's reserves
Consortium reserves
Sponsor X reserves
Assets ledger

Figure 6.3
Converting assets to coins.

6.7.4 Pushing and Pulling Coins

The medium for sponsors to exchange coins with each other is the *coins ledger*. The notion here is that coins are bought, lent, and returned among sponsors on the ledger, providing transparency and visibility into the trading behavior of all sponsors in the DTC network.

Prior to having access to coins on this ledger, a sponsor must explicitly request that the consortium "push" the sponsor's coins from the assets ledger (from the sponsor's reserves) into circulation on the coins ledger (see figure 6.4). The consortium administration

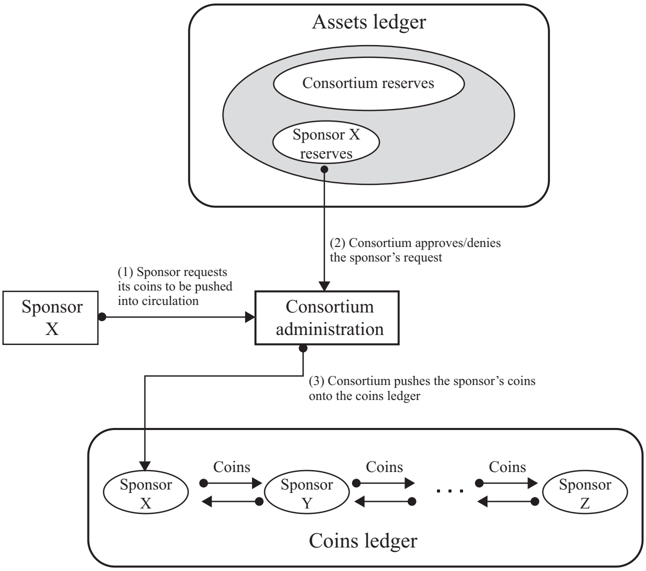
Assets ledger
Consortium reserves
Sponsor X reserves
(2) Consortium approves/denies the sponsor's request
(1) Sponsor requests its coins to be pushed into circulation
Sponsor X
Consortium administration
(3) Consortium pushes the sponsor's coins onto the coins ledger
Coins
Coins
Coins
Sponsor X
Sponsor Y
. . .
Sponsor Z
Coins ledger

Figure 6.4
"Pushing" coins into circulation.

must respond to this request in an explicit manner (request granted, denied, or postponed) on the assets ledger. A request that is granted is followed by the consortium administration transferring coins from its account on the coins ledger to the sponsor's account on the same ledger.

This explicit request-response paradigm is a manifestation of the mechanism to implement monetary policies. It is a "hook" into the system in which the consortium administration—as the representative of the community of sponsors—enforces policies agreed to by the community. A simple example of a monetary policy decision is the *reserve ratio* that must be met by each sponsor on the assets ledger. A sponsor that exhausts its reserves on the assets ledger, thereby violating the policy of sponsors maintaining a minimum reserve, should not be granted a request to push further coins into circulation onto the coins ledger.

A symmetric operation to pushing coins to the coins ledger is that of "pulling" coins from circulation (see figure 6.5). This may occur when a sponsor wishes to enlarge its reserves on the assets ledger by moving coins from the coins ledger to the assets ledger.

6.8 LEDGER-ASSISTED ELECTRONIC CASH

We believe that there are scenarios for Chaumian electronic cash (eCash)[47] in the context of day-to-day consumer usage. In this section, we explore how eCash schemes could be integrated into the DTC model. In general, a *user* (i.e., consumer) is distinguished from a sponsor in that a user does not possess assets in the consortium. The user obtains eCash in exchange for fiat currencies that are acceptable by the consortium. The goal of the user is

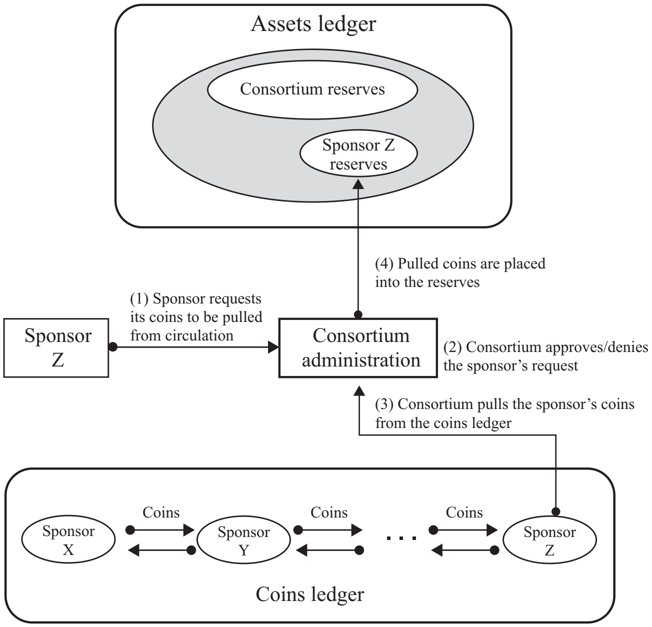
Assets ledger
Consortium reserves
Sponsor Z reserves
(4) Pulled coins are placed into the reserves
(1) Sponsor requests its coins to be pulled from circulation
Sponsor Z
Consortium administration
(2) Consortium approves/denies the sponsor's request
(3) Consortium pulls the sponsor's coins from the coins ledger
Coins
Coins
Coins
Sponsor X
Sponsor Y
. . .
Sponsor Z
Coins ledger

Figure 6.5
"Pulling" coins from circulation.

to utilize a convenient and low-cost (zero-cost) eCash payment method that is stable on a day-to-day basis and can store value over a reasonably long period.

In DTC, the entity that issues and redeems is the consortium itself. This ensures that the stability of eCash is directly related to the stability of coins and assets in the consortium, all three of which are under the monetary control of the consortium as a community. As the issuer of eCash to a user, the consortium enacts monetary policies that govern how much eCash a user can request specifically at any one time. More generally, the consortium can govern how much eCash is permitted to be in circulation at any given moment as a function of the total assets at the consortium.

6.8.1 Background: Key Features of eCash

The notion of *electronic cash* (e-cash) was first put forward in the landmark work by Chaum.[48] One key goal of the original e-cash proposal was that of preserving (as far as possible) the privacy features of paper cash; that is, to prevent third parties from discovering the identity of the payer and payee, the amount, and the time of payment. Therefore, many eCash schemes use cryptographic constructs (e.g., blind signatures, zero-knowledge proofs) that hide an entity's true identity. Another important goal was to prevent collusion of entities from defeating the scheme as a whole. An example would be collusion between the issuer (e.g., bank) and payee (e.g., merchant) that harms the payer. Similarly, a colluding payer and payee must not be able to cheat an honest bank.

In general, e-cash schemes seek to possess the technical features of *blindness* on the part of the bank, which prevents it from seeing what the payer is spending; *unlinkability*, which prevents the bank from correlating e-cash units belonging to the same payer; and *unforgeability*, which prevents payers and payees from creating fake e-cash.[49] Other desirable features include *exculpability* of honest entities (i.e., defend them from being framed by dishonest entities).

The basic flows of currency units in eCash systems are typically three-party. A person, Alice (payer), withdraws eCash from her account at the bank (sponsor) and delivers the eCash *directly* to a merchant, Bob (payee). The merchant must then present the eCash to the same bank in order to get his account credited with the amount. It's worth noting here that the transferal of the e-cash units from Alice to Bob is a direct one, without the mediation of a ledger or third parties.

Aside from the cryptographic complexity of many proposed e-cash schemes, there are a number of practical factors that have prevented their wide adoption over the past two decades. These include:

- *Reliance on a centralized entity* In many e-cash schemes, the bank plays the dual role of the issuing authority and the redeeming (clearing) authority for e-cash. Therefore, for daily use, such e-cash schemes offer little benefit over traditional credit cards.
- *Unmediated peer transferability* Many e-cash schemes suffer from inefficiencies with regard to the multihop transferability (portability) of e-cash units (e.g., Alice to Bob to Charlie) without the mediation of the bank.

The need for the bank entity to be online all the time has often been cited as a stumbling block. However, in the current age of internet connectivity, this may no longer be a factor.

The GNU *Taler* system[50] is one of the more recent practical iterations of Chaum's electronic cash proposal. The Taler system is notable because it provides anonymity only to the payer entity. The payee is assumed to be a merchant and thus for taxation purposes its identity must be disclosed upon redeeming the eCash to the bank.

6.8.2 eCash Support: Motivations and Goals

The following summarizes the high-level goals of the ledger-assisted eCash:

- *Support off-ledger direct payment mechanisms using eCash*
  Provide users to perform payments of eCash without an adverse impact on the Tradecoin ecosystem.
- *Retain visibility into the circulation of eCash in a privacy-preserving way*
  Retain visibility into the circulation of eCash backed by coins while preserving the privacy of the user.
  The relevant entities are prevented from colluding to defraud or damage the Tradecoin ecosystem.
- *Reduce the risk from possible collusion in eCash*
  Provide the necessary mechanisms to prevent collusion by entities in the eCash flow that adversely impact the Tradecoin ecosystem.

6.8.3 Constraints and Assumptions

We impose a number of design constraints on the use of eCash in the Tradecoin ecosystem. These are summarized as follows:

- *Consortium as the issuer of eCash* In Tradecoin, the consortium (administration) is the issuer (source) of all eCash. That is, the consortium plays the role of the bank in the classic Chaum model.
- *Limited three-party flow* The eCash flow follows the classic Chaum three-party flows. This consists of the consortium (as issuing bank); the payer (Alice), who withdraws eCash; and the payee (merchant), who receives payment from the payer. The loop is closed when the merchant deposits the eCash back to the consortium.

- *Limited amounts of eCash withdrawals* Users are permitted to obtain only limited amounts of eCash from the consortium. The amount and rate are subject to monetary policies. As such, this approach provides an early detection mechanism for users who are hoarding large amounts of Tradecoin eCash outside their accounts at the consortium. We believe this limitation is a reasonable constraint that reflects the current paper cash withdrawal limitations imposed in the US banking industry.
- *User anonymity to the merchant only* In the Tradecoin usage of eCash, the user is anonymous only to the merchant. The consortium knows the identities of the user and the merchant.
- *User identification at eCash withdrawal* A user that seeks to withdraw eCash from the account at the consortium must be strongly authenticated by the consortium. This constraint is also reasonable and reflects the current industry practice where a person needs to authenticate themselves at the teller/counter or at the ATM machine before withdrawing paper cash.
- *Merchant nonanonymity* Another constraint in Tradecoin is the nonanonymity of the merchant (payee). That is, the merchant entity is known and identified by the user and by the consortium. This is in line with the recent GNU Taler project.[51]
- *Nontransferability across peer users* Currently, Tradecoin precludes the notion of peer transferability (i.e., multihop transfers) between users. Thus, the payee (merchant) is not able to forward the eCash to other entities without mediation. The merchant has only one option, which is to deposit the eCash to its account at the consortium.
- *Size of eCash circulation subject to monetary policy* An overall constraint is that the total value of eCash in circulation at any

given time is subject to the Tradecoin community's monetary policy.

6.8.4 The Tracking Ledger

The tracking ledger (figure 6.6) is an *append-only distributed log* mechanism. That is, the tracking ledger is read-and-append (read/write) accessible to the consortium and to parties involved in the eCash-related flows (consortium, payer, and payee). It is read-accessible (read-only) for all parties in the Tradecoin ecosystem.

When the consortium issues eCash to a payer or redeems it from a payee, it makes use of the tracking ledger to "declare" these actions. In essence, even though the identity of the user obtaining eCash is anonymized from the rest of the world, the consortium is making an assertion on the tracking ledger that it has issued some eCash units that correspond to a given set of coins.

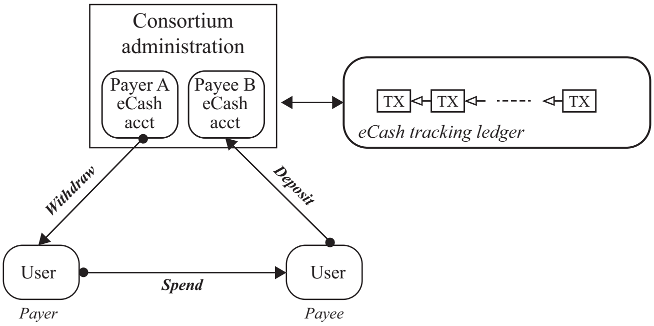

Figure 6.6
Overview of the Tradecoin eCash tracking ledger.

This act of the consortium declaring eCash issuance on the tracking ledger allows the sponsors to have visibility into the size of the eCash units being issued at any given time. It also allows the payer and payee to verify that the consortium has behaved honestly (i.e., has issued the correct number of eCash units to the payer).

6.8.5 The eCash Ledger Identities

In order to preserve the true identity of the payer, it is important that the payer not employ its ledger identity when sending payments to the payee (merchant) and that at spend flow the payer not link to transactions recorded on the ledger that may disclose its identity to the payee.

6.8.6 What Is Recorded on the Tracking Ledger

One purpose of the tracking ledger, among others, is to record the actions taken by entities (consortium, payer, and payee) in such a way that there is a mechanism for the consortium as a whole to observe the flow of eCash in the Tradecoin ecosystem. Since some of the parameters in an eCash system are confidential (e.g., blinded parameters) and are typically exchanged between parties pairwise over a secure channel (e.g., SSL or HTTP/S connection), the tracking ledger relies on the honesty of each entity to record a hash of the relevant parameters to the tracking ledger.

The generic eCash protocol flows that are most representative of the variants of the Chaum schemes consist of three groups: the *withdraw*, *spend*, and *deposit* protocols. The evidence to be recorded on the tracking ledger pertains to pairwise interactions between two entities involved in each of the three Chaum flows. Thus, for example, when a payer withdraws eCash from the consortium administration, both the parameters sent by the administration to the payer and the parameters received by the payer from the administration are recorded to the ledger. That is, both the sender and recipient must log what they sent and received, respectively. This is illustrated in figure 6.7.

The following provides an outline of the states relating to the ledger-assisted eCash protocol flows.

Evidence of the withdrawal When a payer withdraws eCash from his or her account at the consortium (i.e., as the eCash issuer), each eCash unit takes the form of a *serial number* (call it S_{iss}) plus the consortium's signature part over that eCash unit (call it *sigS*). Step 1(a) of figure 6.7 shows the withdrawal stage.

In addition to storing each of these eCash units (i.e., the serial number and the issuer's signature) in its internal system, the

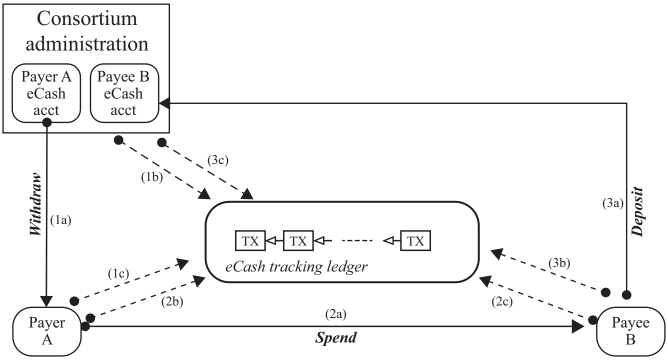

Figure 6.7
The eCash tracking ledger flows.

consortium must record a hash of the following values on the tracking ledger such that they are visible to the other Tradecoin entities:

- Identity of consortium (issuer)
- Hash of signed eCash (serial number S_{iss} and its signature *sigS*)
- eCash denomination (name of eCash scheme)
- eCash unit value
- Time stamp

This is shown in step 1(b) of figure 6.7. The payer may also record on the ledger a hash of what it received from the consortium (step 1(c) of figure 6.7).

Evidence at prespend When the payer has obtained the eCash unit in the form of a serial number S_{iss}, the payer must transform this unit in such a way that it retains some desired properties of the unit (e.g., the payer becomes anonymous at spend time).

We denote this transformation simply as the serial number S_{payer}, where $S_{payer} = F\ (S_{iss})$ for some function F specific to the eCash scheme. These transformed serial numbers S_{payer} are the units that the payer spends or delivers to the payee.

For its exculpability, the payer must record a hash of the transformed serial numbers on the tracking ledger (step 2(b) of figure 6.7) consisting of:

- Identity of consortium (from which the payer obtains the serial numbers)
- Hash of original serial number (the hash of S_{iss})
- Hash of transformed serial number (the hash of S_{payer})
- eCash denomination (name of eCash scheme)
- eCash unit value

- Pointer to corresponding earlier withdrawal transaction on the tracking ledger
- Time stamp

Evidence at spend Typically, the act of spending the eCash units involves a challenge-response exchange between the payee and the payer (step 2(a) of figure 6.7). Here the payee sends a challenge value C_{payer} to the payer. The payer then must prove that the serial number S_{payer} is valid by responding to the challenge with the response R_{payer}.

Evidence at postspend For its own exculpability, the payee must keep a transcript of the challenge-response exchange and also record parts of it on the tracking ledger (step 2(c) of figure 6.7):

- Hash of transcript (the hash of the set of values S_{payer}, C_{payer}, and response R_{payer})
- eCash denomination (name of eCash scheme)
- The spent eCash unit value
- Pointer to corresponding prespend transaction (flow 2) on the tracking ledger
- Time stamp

Evidence at predeposit When the payee (e.g., merchant) deposits the serial number received from the payer into the payee's account at the consortium (step 3(a)), the payee must deliver the values S_{payer}, C_{payer}, and response R_{payer} to the consortium.

For its exculpability, the payee must capture or log the eCash parameters it deposited to the consortium (step 3(b) of figure 6.7):

- Hash of signed eCash (serial number S_{iss} and its signature *sigS*)
- eCash denomination (name of eCash scheme)
- eCash unit value
- Pointer to corresponding postspend transaction on the tracking ledger
- Time stamp

For its exculpability, the consortium must keep a transcript of the exchange with the payee for deposits and also record parts of the transcript on the tracking ledger.

6.9 ENVIRONMENTALLY FRIENDLY DIGITAL TRADECOIN

Climate change has a profound negative impact, visible in a plethora of very unpleasant physical consequences, such as the need to move entire cities (including capitals, such as Jakarta) to avoid perennial flooding, refitting industrial plants on a gigantic scale, and the like. It also has a profound financial component. In addition to utilities, extractive industries, construction, and others, some of the financially oriented industries, including banking, insurance, asset management, and pension funds, will suffer very substantial losses. The *Wall Street Journal* dubbed the recent bankruptcy of the major California utility PG&E "the first climate-change bankruptcy." There is no doubt in our mind that it is not going to be the last. According to the Bank of England, "Climate change poses significant risks to the economy and to the financial system, and while these risks may seem abstract and far away, they are in fact very real, fast approaching, and in need of action today."

Experience suggests that protestations alone are insufficient to convince people to make their behavior more environmentally friendly. Thus, we need to introduce a set of suitable financial tools and incentives that can gently push people in the right direction.

We can achieve that goal by introducing the environmental DTC (EDTC)—an environmentally friendly version of the DTC. We can model such a coin on a coalition loyalty program. A loyalty program can be conceptualized as an amalgamation of several single-issuer loyalty programs so that loyalty points can be accrued and redeemed at a variety of participating businesses. From their humble beginning in the 1970s, when American Airlines launched the first frequent flyer program (incidentally introducing the term itself), loyalty programs have grown exponentially.

The economic value of these programs is enormous. For instance, in January 2019, Air Canada, along with TD, CIBC, and Visa, acquired a loyalty program called Aeroplan, which has about 5 million active members, from Aimia for C$450 million in cash. They also assumed liability for the unused Aeroplan points at an estimated value of C$1.9 billion, at 2.5 cents a mile. Given these facts, the potential benefit of the EDTC-related deployment along the loyalty program lines can be substantial.

A vital part of loyalty programs, including EDTCs, is a platform for business intelligence reporting and analytics, which analyzes member information, tracks purchasing patterns, identifies profiles of loyal members, and aligns its loyalty program with members' preferences. For the EDTC to be successful, the utmost attention should be paid to privacy-preserving measures.

The EDTC ecosystem consists of several components. Its heart is an efficient, precise, and easy-to-use app that records positive actions by program participants. This app is a "money printing press." The next constituent part of the ecosystem consists of individual participants interested in fighting climate change and attracted by suitable financial initiatives. Their natural counterpoint is corporate sponsors—companies and taxing authorities sufficiently concerned about climate change to be prepared to spend money to fight it. Currently, all major companies with exposure to climate change and sustainability have substantial budgets to support environmentally friendly proposals. In turn, environmental DTC presents them with a source of income via attracting more customers and increasing revenues and profitability, cutting costs on sustainability infrastructure, and a tool for reducing climate change bankruptcy risk such as experienced by PG&E. The glue holding the EDTC ecosystem together consists of coalition members, who are prepared to accept EDTCs as partial payment for their goods and services. For instance, a utility provider might allow paying up to 10 percent of utility bills with EDTCs. A coffee shop might charge up to 10 percent in EDTCs and use them for buying environmentally friendly coffee beans or paying its electricity bills. AI-based data collection systems and blockchain technology can be used to record EDTC balances of all activities of participants, sponsors, and coalition members in a robust and reliable ledger.

Since participants earn EDTCs for performing seemingly unrelated activities, such as walking instead of using a car or consuming green electric power instead of using conventional sources, a fair mechanism that brings all these actions to a common denominator is crucially important. There are several possibilities. For example, different activities can be valued based on their reduction in the participant's CO_2 footprint.

Implementation of a robust monetary policy, which determines the rate of disappearance of EDTCs earned by participants over time, is crucial for the stability of the ecosystem as a whole. A comparison with successful loyalty programs suggests that a form of demurrage is the most natural. In simple terms, it means that EDTCs accumulated by participants should expire and disappear after a certain period, the same mechanism that exists in various frequent flyer programs.

It is necessary to design suitable circulation rules by identifying "sources and sinks" for EDTCs. If we follow a strict loyalty point analogy, we must conclude that EDTCs are created at the "source" when individual participants perform environmentally friendly actions and are destroyed at the "sink" when they are used as partial payment for goods and services. This setting is overly restrictive because it obliterates the useful WIR analogy, by which EDTCs should not disappear at all. It appears that an intermediate solution is in order. EDTCs can be both earned by participants and borrowed by sponsors. There is an intermediate level of businesses accepting EDTCs, which also can use them with the participating coalition members as partial payment for their own needs. Finally, there are "super sponsors" who accept EDTCs but destroy rather than recirculate them. Such sponsors may include tax authorities and major multinationals spending part of their climate change budgets on promoting environmentally friendly policies.

6.10 CONCLUSIONS

We have discussed conceptual underpinnings and technical approaches to building DTCs. We have shown that DTCs have several decisive advantages compared to more established cryptocurrencies such as Bitcoin and Ripple. In addition to being a convenient transactional cryptocurrencies for the internet era, DTCs can serve as an important counterbalance to fiat currencies and, when fully developed, can play the role of a supranational currency, facilitating international commerce and allowing groups of small countries to create their own viable currencies.

NOTES

1. D. L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Communications of the ACM* 24, no. 2 (February 1981): 84–88.

2. D. L. Chaum, A. Fiat, and M. Naor, "Untraceable Electronic Cash," in *Advances in Cryptology (CRYPTO 88)*, ed. S. Goldwasser, Lecture Notes in Computer Science 403 (New York: Springer-Verlag, 1990), 319–327, http://dl.acm.org/citation.cfm?id=88314.88969.

3. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008, https://bitcoin.org/bitcoin.pdf.

4. A. Lipton, "Blockchains and Distributed Ledgers in Retrospective and Perspective," *Journal of Risk Finance* 19, no. 1 (2018): 4–25, https://doi.org/10.1108/JRF-02-2017-0035.

5. Nakamoto, "Bitcoin."

6. V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," white paper, 2014, https://github.com/ethereum/wiki/wiki/White-Paper.

7. D. Schwartz, N. Youngs, and A. Britto, "The Ripple Protocol Consensus Algorithm," Ripple Labs Inc. White Paper 5, 2014.

8. A. Lipton, A. Pentland, and T. Hardjono, "Narrow Banks and Fiat Backed Digital Coins," *Capco Institute Journal* 47 (2018): 101–116

9. Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms”; Chaum, Fiat, and Naor, “Untraceable Electronic Cash.”

10. A. Haas, L. J. Ussher, K. Töpfer, and C. C. Jaeger, “Currencies, Commodities, and Keynes” (unpublished manuscript, March 6, 2014).

11. J. Lowe, *The Present State of England in Regard to Agriculture, Trade and Finance: With a Comparison of the Prospects of England and France* (Edinburgh: E. Bliss and E. White, 1824).

12. G. P. Scrope, *An Examination of the Bank Charter Question* (London: John Murray, 1833).

13. W. S. Jevons, *Money and the Mechanism of Exchange*, vol. 17 (New York: Kegan Paul, Trench, 1885).

14. A. Marshall, *Remedies for Fluctuations of General Prices* (London: n.p., 1887).

15. F. D. Graham, “The Primary Functions of Money and Their Consummation in Monetary Policy,” *American Economic Review* 30, no. 1 (1940): 1–16.

16. B. Graham, “Stabilized Reflation,” *Economic Forum* 1, no. 2 (1933): 186–193.

17. F. A. Hayek, “A Commodity Reserve Currency,” *Economic Journal* 53, no. 210–211 (1943): 176–184.

18. J. M. Keynes, “The Objective of International Price Stability,” *Economic Journal* 53, no. 210–211 (1943): 185–187.

19. N. Kaldor, *Causes of Growth and Stagnation in the World Economy* (Cambridge: Cambridge University Press, 2007).

20. Z. Xiaochuan, “Reform the International Monetary System,” *Bank for International Settlements Quarterly Review* 41 (2009): 1–3, https://www.bis.org/review/r090402c.pdf.

21. Nakamoto, “Bitcoin.”

22. Schwartz, Youngs, and Britto, "The Ripple Protocol Consensus Algorithm."

23. R. Ali, J. Barrdear, R. Clews, and J. Southgate, "The Economics of Digital Currencies," *Bank of England Quarterly Bulletin*, Q3, September 2014, 276–286, https://www.bankofengland.co.uk/quarterly-bulletin/2014/q3/the-economics-of-digital-currencies.

24. S. Scorer, "Central Bank Digital Currency: DLT or not DLT? That Is the Question," June 5, 2017, https://bankunderground.co.uk/2017/06/05/central-bank-digital-currency-dlt-or-not-dlt-that-is-the-question/.

25. K. Rogoff, *The Curse of Cash* (Princeton, NJ: Princeton University Press, 2016).

26. C. Ilgmann, "Silvio Gesell: A Strange, Unduly Neglected Monetary Theorist," *Journal of Post Keynesian Economics* 38, no. 4 (2015): 532–564.

27. I. Fisher, *Stamp Scrip* (New York: Adelphi Company, 1933).

28. A. Lipton, "The Decline of the Cash Empire," *Risk Magazine* 29, no. 11 (2016): 53, https://www.risk.net/risk-management/2475663/decline-cash-empire.

29. Nakamoto, "Bitcoin."

30. G. Danezis and S. Meiklejohn, "Centrally Banked Cryptocurrencies" (preprint, 2015), http://arxiv.org/abs/1505.06895.

31. F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System," in *Security and Privacy in Social Networks* , ed. Y. Altshuler, Y. Elovici, A. Cremers, N.. Aharony, and A. Pentland (New York: Springer, 2013), 197–223, https://doi.org/10.1007/978-1-4614-4139-7_10.

32. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms"; Chaum, Fiat, and Naor, "Untraceable Electronic Cash."

33. The lead author is a member of their advisory board.

34. G. Pennacchi, "Narrow Banking," *Annual Review of Financial Economics* 4, no. 1 (2012): 141–159.

35. As always, Shakespeare put it best: "Neither a borrower nor a lender be, for loan oft loses both itself and friend, and borrowing dulls the edges of husbandry." *Hamlet*, act 1, scene 3.

36. Lipton, Pentland, and Hardjono, "Narrow Banks and Fiat Backed Digital Coins."

37. T. Hardjono, A. Lipton, and A. Pentland, "Towards an Interoperability Architecture: Blockchain Autonomous Systems," *IEEE Transactions on Engineering Management* 67, no. 4 (2020): 1298–1309, https://doi.org/10.1109/TEM.2019.2920154.

38. L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," *ACM Transactions on Programming Languages and Systems (TOPLAS)* 4, no. 3 (1982): 382–401.

39. M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," in *Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI)* (February 1999), 173–186.

40. Global Legal Entity Identifier Foundation (GLEIF), *LEI in KYC: A New Future for Legal Entity Identification*, GLEIF Research Report, May 2018, https://www.gleif.org/en/lei-solutions/lei-in-kyc-a-new-future-for-legal-entity-identification.

41. T. Hardjono and N. Smith, "Decentralized Trusted Computing Base for Blockchain Infrastructure Security," *Frontiers Journal—Special Issue on Finance, Money and Blockchains* 2 (December 2019): 1–15, https://doi.org/10.3389/fbloc.2019.00024.

42. Nakamoto, "Bitcoin."

43. Nakamoto, "Bitcoin."

44. Buterin, "Ethereum."

45. D. Siegel, "Understanding the DAO Attack," *CoinDesk*, June 2016, https://www.coindesk.com/understanding-dao-hack-journalists.

46. Hardjono, Lipton, and Pentland, "Towards an Interoperability Architecture."

47. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms."

48. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms."

49. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms"; Chaum, Fiat, and Naor, "Untraceable Electronic Cash"; J. Camenisch, S. Hohenberger, and A. Lysyanskaya, "Compact E-Cash," in *Advances in Cryptology—EUROCRYPT 2005*, ed. R. Cramer (Berlin: Springer, 2005), 302–321.

50. C. Grothoff, "GNU Taler—a Privacy-Preserving Online Payment System for Libre Society," July 27, 2016, https://grothoff.org/christian/fsfe2016.pdf.

51. Grothoff, "GNU Taler."