Makeit

What is crypto-currency?

How can we have cash without physical notes and coins? **Julian Bucknall** explains

Although we feel we know cash intimately, let's take a deeper look at some of its attributes. First of all, it's represented by a physical object: either a banknote or a coin. If you buy something, you hand over that physical thing to the seller. It leaves your possession and enters theirs. Your net cash worth is reduced by the amount of cash you've handed over.

Second, it's relatively hard to clone your cash. It would be nice if you could just photocopy banknotes (well, at least it would be until everyone started doing it and the global economy crashed a few seconds later) or you could stamp coins more cheaply than you could buy them, but there are various protections to make sure that this is inefficient and costly.

Banknotes are printed on a specific type of paper that is hard to get (in the US, the paper is cotton based and will even survive a trip through the washing machine – something I am loath to try with a fiver) and furthermore the design is created to be extremely difficult to copy or to photocopy. Large denomination coins are designed to be hard to stamp out on simple machines – they have text on the milled edges, they are made from two types of contrasting coloured metal, and so on. Small denomination coins just aren't worth copying: the cost and the work needed will outweigh the benefit of the counterfeit value.

Minting currency

A corollary of that is that cash can only come from those who are authorised to create it: in essence, the government. It's a government department, the Royal Mint, that is charged with replacing cash that's destroyed (say, banknotes that go through the washing machine or coins that get worn and lose their non-clonable features), and with printing or minting more cash to add to the supply.

Third, it's anonymous. There need be no record of cash changing hands, and the only people who would know about a transaction would be the seller and the buyer. As soon as some other representation of money comes into play, say a cheque or a credit card, records are kept of the transaction. Banks would have to be involved to transfer this amount of money from the buyer's account to the seller's. The transaction would become 'known'.

Beyond coins and notes

If we were to design a digital currency, then we would have to replicate these three key features of cash: the ability to transfer it unambiguously from buyer to seller even though it's not a physical object, the inability to clone it (and to limit its creation to those authorised to create it), and its anonymity.

Of these, you'd think the biggest issue would be the cloning problem. We are all aware of how easy it is to duplicate or copy digital objects, from Word documents to MP3s to movies. Even if the digital entity were protected with some kind of DRM, it doesn't take long for someone to work out how to circumvent it. For example, it's how I play DVDs I purchased from England (region 2) here in the US on a region 1 player. If it's that easy to copy and to circumvent digital protection, how could there ever be some kind of digital currency?

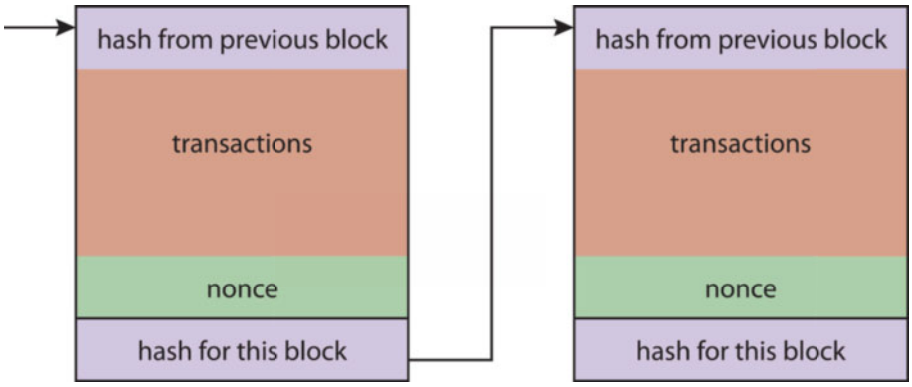
However, notice what I elided there. The digital entities I was talking about have content; we are interested in these objects for what they contain, not for what they are. An Excel spreadsheet is not interesting as an XLS file you can pass around, it's interesting because it's a file that contains data and calculations – information we may not currently have. An MP3 file is only interesting because it's a recording of a track we like and want. But a digital coin is not like that. It has no 'content' – it is a digital object that is interesting because of what it is. And guess what – we already know about digital objects that are fully protected and that are interesting for what they are: digital signatures.

Sign here

Digital signatures are easy for the signer to create and for everyone else to verify, but they are also extremely hard to fake. Knowing this, if we see a digital signature, we know that it can only have come from the signer and no one else. So if I write an email to you for example, and sign it digitally, you know that it can only have come from me and therefore that I have written it. The content of the email could be plaintext or encrypted. It doesn't matter; it's the signature that provides proof of authenticity.

Digital signatures are created through the magic of asymmetric ciphers or public-key cryptography, like RSA. Asymmetric ciphers have two passwords, a private one that only you know and a public one that can be published so everyone else can know it. Data encrypted with the private key can only be decrypted with the public one (and vice versa).

To create a digital signature of a file (or a message), you hash the contents of the file with



▲ **Conceptual view of the Bitcoin block chain.**

a cryptographic hash algorithm like SHA-256 and then encrypt that hash with your private key. The result is your digital signature for the file. Someone can verify this signature for the file by hashing the file with the same algorithm and checking that this hash is equal to the hash obtained by decrypting the signature with your public key. If they are equal then the file has not been changed and you signed it; if not, either the file has been changed or you didn't create the signature.

Using this technology, we can start thinking about how to implement digital coins. Let's suppose we had a central 'bank' dishing out numbers, like the numbers on banknotes (these are unique – each banknote has its own number). The bank hashes the number and signs it with its private key, creating a digital signature for the number. We'll call the combination of the unique number plus its signature a digital coin.

We would have digital coins, yes, and only the bank could create them, but we would still have the cloning problem: I could copy these digital coins all day. Unfortunately, although we can verify that a digital coin is valid, we have no way of determining whether this coin is original or cloned.

Cash register

So the bank needs to track where each coin is – that is, who currently owns it. If I use a digital coin to purchase something from you, I need to inform the bank that I have done so and that you now own that coin. If you like, the transaction has to be registered with the central bank. That way, I can't use the same coin to buy something from you and then from Tom, Dick and Harry as well. It also means the bank is able to tell if I'm trying to use a coin I don't own to purchase something, and can turn down the transaction.

Since we have to worry about someone gaming the system, the purchasing transactions I register with the bank will have to be digitally signed by me. If transactions weren't signed, you could flood the bank with bogus transactions that purported to come from me and that transferred all my coins to you. Therefore, not only are the coins digitally signed (by the bank), but the transactions involving coins are also signed (by the buyer). Of course, that means everyone who uses digital coins has to be registered with the bank so that the bank has copies of everyone's public keys. Remember, in order to verify a transaction, the bank has to decrypt the signature with the buyer's public signature.

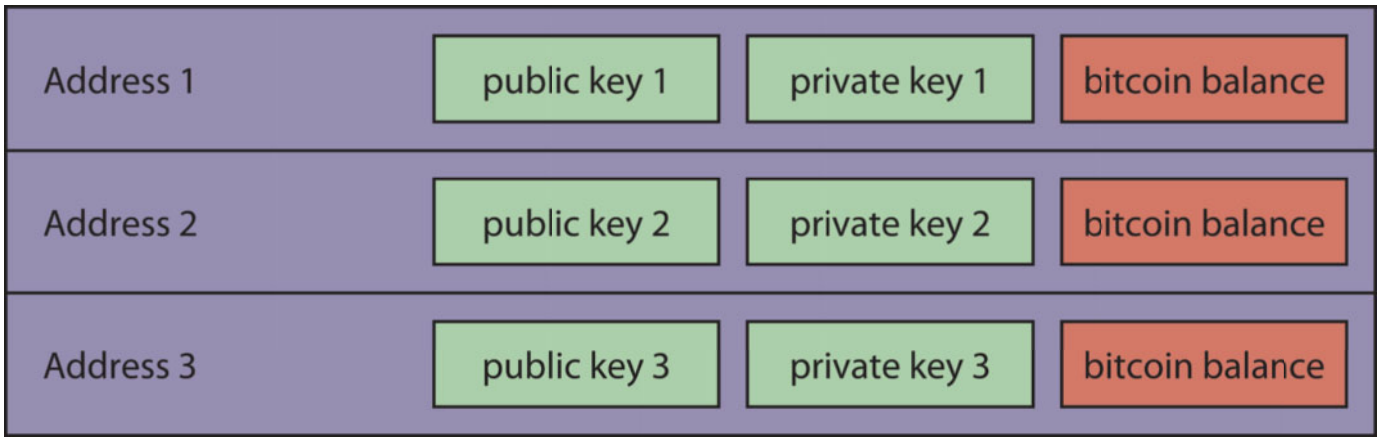
Let's take a break here and recap what we have for our digital cash. We have unique coins, check. Coins can be unambiguously transferred from buyer to seller, check. (Note that even though we can clone coins *ad infinitum*, only one person owns and can use the coin itself.) We have a way of creating more ▸

Bitcoin exchanges

Bitcoins can be used to purchase many goods and services (the most famous 'store' is known as Silk Road, where bitcoins can be used to purchase illicit drugs), but earning them poses a problem.

The first way to get bitcoins is to mine them as described in the main article, by solving time-consuming block problems.

However, most people exchange ordinary currency – dollars, euros, yen – for bitcoins through one of the many exchanges that accept them. After all, bitcoin is a currency, and therefore can be bought and sold through currency exchanges, much like buying euros for your holiday on the continent. The most famous is known as Mt Gox (**www.mtgox.com**), although its fame is mostly due to the fact it was hacked fairly recently and the details of 60,000 users were leaked. Bid/ask prices for bitcoins crashed immediately after this was discovered, and they haven't risen much since. At the time of writing the exchange rate is about $3.15/BTC, down from a high of $17/BTC before the crash). ■



▲ **Conceptual view of a Bitcoin wallet.**

Mining botnets

Miners wishing to generate as many blocks as possible run large computer farms, with each computer running in parallel trying to solve block problems as quickly as possible. After all, it is only through generating new blocks that miners can earn bitcoins, although there is the capability for assessing fees to include a transaction in a block.

Some programmers are already using the GPUs on their PCs to provide extra parallel processing power, and yet others are using botnets to spread the computational processing across many machines. In August this year, Symantec reported the discovery of a special trojan program – dubbed Trojan.Badminer – that infected users' computers in order to add them to a botnet with the sole purpose of mining bitcoins. The resulting botnet was found to be generating roughly $150 at current exchange rates per compromised PC per month. ■

coins by an authorised entity, check. What we don't have – at all – is anonymity. The bank in this situation is all-knowing and all-seeing. It knows who owns every digital coin; it knows every single transaction that took place and the counterparties involved. It's much worse than normal cash in that respect, and it could be argued that it's even worse than cheques and credit cards. Although it has some advantages, this is clearly not a complete solution.

Bitcoin

Enter Bitcoin. The designer of Bitcoin, Satoshi Nakamoto (who may or may not exist or whose name may be a pseudonym), recognised the problem of the central bank becoming omniscient. His solution was radical: make the central bank a peer-to-peer network and make the participants in Bitcoin anonymous.

First things first: with Bitcoin, buyers and sellers are known by their 'address'. A Bitcoin address is a merely a mathematical conversion of a public key from an asymmetric cipher key pair. You can have as many addresses as you want and you store them in a 'wallet', which is a digital repository on your computer. If you lose your wallet (that is, you don't back it up), you will lose all your bitcoins.

The next innovation for Bitcoin is the public network. When you buy or sell, you will generate a transaction as described before. The transaction will be assigned a unique sequential identifier from a timestamp server (actually a distributed timestamp server). This transaction is then broadcast to peer nodes on the network. These peers have a couple of jobs to do when they receive a transaction: they must verify the transaction (in essence, check the digital signature and respond to the sender with a confirmation), and they add the transaction to a special file called a 'block'.

Virtual mining

The block in Bitcoin terms is an intriguing beast. It's generated through a difficult (that is, time-consuming) process. Generating one is how bitcoins are created: you collect a group of transactions, plus a random number (which is known as the 'nonce'), plus the hash of the last validated block, and then you hash the lot. The answer you get has to have a certain number of zero bits at the front. If it doesn't, you alter the nonce and try again. Repeat until you solve the problem. Once you do solve the problem, you broadcast the block to the network so that other nodes can verify it and you get 50 bitcoins for your trouble, which are added to your digital wallet. The system is designed so that the payment for blocks is halved every four years or so.

If your block is validated, it is added to the publicly available block chain. Because your block has a reference to the previous block through that block's hash, the chain is slowly built up. Anybody can verify the chain at any point by following the blocks from the very first (known as the 'genesis block') and verifying the hashes. All blocks are transmitted or synchronised throughout the network, there is no central repository. Blocks are created, on average, about once every 10 minutes (the block chain at the time of writing was 150,955 blocks long and about 600MB in size).

The process of generating a block is known as mining. It is the only way to generate new bitcoins. The system is designed so a maximum of 21 million bitcoins can be generated.

Using this system, we have finally found our digital currency. It's anonymous (participants are known only by their addresses, and each participant can use many addresses). Although bitcoins can be cloned and spent twice, the network maintains information about the monetary value of each address so the double-spend problem is avoided. Finally, transactions of bitcoins are verified and confirmed by the network. PCP

Spotlight on… Scalability

Bitcoin works by copying and synchronising the block chain to every peer in the network. The size of the chain at present is roughly 150,000 blocks, or 600MB. The entire chain has to be synchronised because it is used to verify every bitcoin transaction: you start at the genesis block and verify that every other block in the chain follows on from the previous ones. In other words, you check that the hash for the previous block is used in the hash for the current one. The block chain contains every single transaction made with bitcoins, and therefore the value for every address.

At current transaction rates this is fine, but internet security expert Dan Kaminsky is concerned that this distributed network will break down if the rate of transactions increases. He postulates that if transaction rates reach thousands per second (the rate for services like Visa), the amount of data transmitted and synchronised across the network would be of the order of gigabits per second. Verification would take more and more processing power.

In essence, Bitcoin would develop a system of users and superusers. Superusers would be those who could afford the bandwidth and storage, and who could charge the requisite fees to validate transactions and blocks. Kaminsky called them banks, bringing us full circle again. ■

Julian M Bucknall has worked for companies ranging from TurboPower to Microsoft and is now CTO for Developer Express.
feedback@pcplus.co.uk