Introduction to Cryptocurrency

Gavin Shepherd
Portfolio Construction & Investment Research Manager

What is cryptocurrency?

Cryptocurrencies do not exist anywhere but in a digital database called a “blockchain”.

In its simplest form, a cryptocurrency allows users to transfer money almost instantly, with cheap transaction fees and no third parties involved. Over the years, many cryptocurrencies have moved beyond this core component and built platforms that allow users to transfer anything from money to real-life assets such as cars and property, all using the blockchain technology introduced by bitcoin.

The crypto part in the name “cryptocurrency” comes from the fact that transactions – the act of transferring assets such as currency and digital or real-life assets between a sender and a recipient – are encrypted for security, a process known as “cryptography”. Cryptography is used for three reasons:

1. To protect transactions from being tampered with;
2. To protect the identity of parties acting in a transaction; and
3. To enable the creation of new coins via the mining process.

A brief history of cryptocurrency

Satoshi Nakamoto published a paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System”, in 2008. This was followed by the launch of Bitcoin on the 3rd of January 2009.

Bitcoin has grown to become the number one cryptocurrency available on the market and has given rise to hundreds of cryptocurrencies, known collectively as altcoins. There are now close to 1,000 cryptocurrencies.

Some of these altcoins are little more than copies of bitcoin, but others are attempting to do things with the underlying blockchain technology that not only disrupt the financial sector but also our understanding of apps and website services, all in an attempt to fix today’s problem of centralisation.

The problem with centralisation

Read any literature relating to bitcoin and cryptocurrencies and you’ll eventually stumble upon the concept of decentralisation. To understand decentralisation, you first need to understand the problem with centralisation.

A world of information and data about who we are, what we do and what we like, is held by a few large organisations: private and public corporations and the government. The dataset representing you (financial records, emails, Facebook messages and likes etc) is held on servers that exist in a central location. For example, your financial records, every transaction you’ve ever been a part of, your current balance and all your loans, exist on your bank’s servers. Your bank might have multiple servers for backup and audit purposes, but it still all exists in virtually one location: your bank. All this information and data may be hacked by a malicious hacker.

The Cypherpunks, the community from which cryptocurrencies first arose, understood this bleak scenario and aimed to fix it. Cryptocurrencies are ***said to be decentralised systems because every user of a cryptocurrency keeps a copy of everyone's transaction history.*** The moment you join a blockchain you receive the entire history of that cryptocurrency, including all transactions ever made. If a user disagrees with a transaction (say a malicious hacker changes their wallet value from 1 Bitcoin to 1,000 Bitcoin), a consensus must be reached by at least 51% of the users of that cryptocurrency. That 51% then decides what the correct amount should be.

This automatic consensus is the beauty behind cryptocurrencies and decentralisation. There is no one server that malicious hackers can attack. They would need to convince 51% of all users because every user keeps a copy of the blockchain.

What is the blockchain?

The blockchain is the entire history of transactions made with a certain cryptocurrency. Because the blockchain is the technology behind every single cryptocurrency, it's critical for the understanding of cryptocurrencies.

A block

Whenever two users of a cryptocurrency, say bitcoin, send coins to each other, a transaction is created. This transaction contains, among other details, the wallet address of the sender, the wallet address of the recipient and the amount of currency sent.

These transactions are added to an unverified block, with each block containing the maximum of a pre-specified number of transactions, depending on the cryptocurrency in question. Once the transaction is added to a block, it is said to be immutable: it cannot be edited and cannot be removed.

You can think of a block as a page of a ledger containing a list of transactions. Once the block is filled, miners will verify the transactions (more on mining later) and the block is ready to be attached to the chain.

The chain

Each mined block is then attached to the rest of the blocks in the blockchain. This chain of blocks contains every single transaction executed in the history of the cryptocurrency. The block is given a new identifier and also the previous block's identifier. This attaches the block to the previous one in the chain and so on. Any one block can only be attached to one previous block and can only have one block at any one time.

Advantages of blockchain

The advantages of blockchain include:

i) guarantees the correctness of its past and present data;

ii) guarantees the correctness of its future state and data.

Blockchains replace intermediaries with mathematics. Before blockchains, digital currencies had to run through central servers and be logged by central bookkeepers. Your money had to rely on several single points of failure before it would reach your intended destination. Blockchain solved that problem.

Some key points when using blockchain:

- No geographic borders;
- No banks;
- Anonymity (in bitcoin, the size of the transaction can be seen, but, as an example - *Ronan's* and *Xavier's* names can't be seen. In other cryptocurrencies, there might be much greater anonymity);

- The validation is done by computers that raise their hands and say, “We are miners and will do it for free.” The miners don’t charge transaction costs, but depending on how the currency is designed, they might get more coins depending on how much “work” they do to validate transactions;

- Decentralized. Which is part of the privacy of the transaction and also ensures that no one source is controlling the validation (and then possibly faking transactions or minting more money).

Cryptocurrency mining

The highly important task of maintaining the blockchain, verifying transactions and adding blocks to the blockchain, rests in the hands of miners. Working with very powerful computers running specialised mining software, miners look at unverified blocks and the transactions on them and solve a mathematically difficult, cryptographic puzzle involving everything on the block.

This puzzle can take anywhere between a minute and ten minutes to solve. While the exact process by which miners verify these blocks is beyond the scope of this article, once a miner verifies a block, it’s assumed for all intents and purposes to be valid and ready for attachment to the blockchain.

The miner then pulls the last block’s identifier from the blockchain and attaches it to the new block. He also gives the new block its own identifier. This process makes the new block an official part of the blockchain, and this new information is then propagated to everyone using that particular cryptocurrency.

As reimbursement for this work, the miner receives payment in the cryptocurrency just mined. Some cryptocurrencies choose to award a portion of the transaction fees on the block just mined while others, like bitcoin, generate new coins and those coins are then given to the miner.

The rise of altcoins

Many cryptocurrencies have been attempting to replicate bitcoin’s success, some with better results than others. With just under 1000 altcoins this market does not seem to be slowing down. While most altcoins are merely a copy of bitcoin (with very few modifications or improvements), others are attempting to do new things with the underlying bitcoin technology. However, 95% of currencies are scams and are likely to fail in the next few years. How come? Because in any euphoria, criminals are created. We saw it with internet stocks in 1999; we saw it with hedge funds in the 2000s; we saw it with mortgage-backed securities in 2008 and now we are going to see it in cryptocurrencies.

Some altcoins, like Ethereum (commonly known as Bitcoin 2.0), have been using the blockchain to allow the development of decentralised applications where the data is held by every user of the blockchain instead of a single server. Others, like Monero, have put their focus on anonymity, building on the cryptography used by the bitcoin blockchain to further obfuscate recipient and sender wallet addresses.

What does a cryptocurrency transaction look like?

- *Ronan* wants to send money to *Xavier.*
- He puts together a “transaction” on his computer that describes how much he wants to send.
- The transaction is added to a “block”.
- The “block” is sent all over the network and the network “validates” the transaction by looking at all the prior transactions that led to Ronan having enough validated currency.
- The currency is sent to Xavier. The transaction is now there in the block. And Xavier is now in control of his own “private key” that controls the funds. Cryptography protects Xavier’s funds from A) being duplicated and B) being stolen from him. As long as Xavier takes reasonable security measures, his crypto will be safe. Each new block created on this chain of blocks (hence, “blockchain”) adds yet another layer of difficulty, making it harder and harder to reverse each “one-way” cryptographic problem. Thus, it becomes exponentially more difficult to change the validation of Ronan’s transaction, the more blocks are added. Famed cryptographer Nick Szabo likened this process to a fly getting trapped in amber. The more time passes by, the more the amber accumulates and the harder and harder it gets to remove the fly from the amber. So, a block can be likened to another thin layer of digital amber and the blockchain is the collective depth of the digital amber…or something like that!

Advantages and Disadvantages of Cryptocurrencies

Advantages:

i) A standardized and neutral confirmation policy backed by software that has no human agendas.

What does this mean?

Imagine I want to send Xavier dollars to buy his house. I need to trust all of the middlemen between Xavier and me: local bank, lawyers, governments, Xavier's bank, etc., to approve of this transaction if I do it in dollars. This is OK, but at each step, someone could be untrustworthy. They are all humans, even the government (humans subtly influence the price of the dollar and also share details of the transaction with unfriendly parties). Also, each step in the above has a transaction cost. So, inflation is built into the system. If this were for example, a bitcoin transaction, enough miners need to approve that this transaction is valid. So even if a few miners are not trustworthy, the bulk of them will be, and we can trust that the transaction between Xavier and me is legit. This is the ENTIRE reason for cryptocurrency: to avoid governments, borders, middlemen and extra transaction costs. As well as have high security and avoid forgery. (There is another reason for cryptocurrency, which is to do with more complicated transactions that we can call "contracts" [also known as "smart contracts" without lawyers, etc.]).

ii) Blockchains are incredibly resilient. A blockchain can survive unaffected as long as just one stays alive. So, if there's a catastrophic failure throughout the nodes, it takes just one lone survivor to keep the network running without any loss of data. With bitcoin, nodes are running all over the world. The power is distributed. There's no single vector of attack. To kill it, you have to eradicate it completely, globally, totally, without fail, all at once. This is very hard to do. It's why bitcoin is incredibly strong - the most secure network on Earth.

Disadvantages:

i) Miners approve transactions one block at a time. A block is a set of transactions. A "blockchain" is a chain of these timestamped blocks. If a transaction doesn't make it into one block, it waits a certain period of time to get into the next block. So, there's lag. Blockchains are slow. Blockchains are slow because blockchains are extremely inefficient - especially compared to Visa, MasterCard or PayPal. There's a reason. Decentralization and censorship-resistance. That's what sets Bitcoin apart from traditional payment systems and inefficiency is the trade-off. Blockchains are inefficient.

ii) Another "bad" is that everyone can see the transaction (on bitcoin) although nobody knows it was Xavier and Ronan involved in the transaction. Blockchains aren't inherently anonymous.

iii) Another "bad" is that for certain types of transactions (buying a cup of coffee), the blockchain allows for a layer of software above it to quickly verify before the blockchain protocol validates the transaction... or software to provide other services on the blockchain (e.g. a bitcoin exchange that stores wallets for people). That software layer involves humans (humans are bad), which invites good players and bad players to be involved (hence, the Mt. Gox $400 million theft).

iv) Blockchains are very hard to scale. In exchange for security, trust, fewer middlemen and avoidance of governments and boundaries, society pays in computational costs, storage (the same blockchain stored on millions of computers is a waste) and slower transaction speeds. And the software layer above the blockchain needs to evolve, which it is (the same way internet software evolved post 1991).

Conclusion

For those that may remember, we originally wrote about cryptocurrencies in our May 2013 Newsletter, specifically Bitcoins and Gold. Cryptocurrencies are complicated and rarely understood. In this article I have only scratched the surface and introduced some basic features of cryptocurrencies. It's important to do as much research as possible about the different Cryptocurrencies, especially if you personally decide to invest in this space. If you are interested in learning more about this topic, here are some articles we would recommend reading:

1. Why Bitcoin Matters, by Marc Andreesen (founder of Netscape)
2. By reading this article, you're mining bitcoins, by Ritchie S. King, Sam Williams, and David Yanofsky.
3. Fat Protocols by Joel Monegro
4. The Bitcoin Whitepaper by Satoshi Nakamoto

Contribute to super & claim a tax deduction

A legislative change effectively allows individuals to arrange their own pre-tax salary sacrifice arrangements without going through an employer.

Kate Cramsie
Financial Adviser

It has always been possible to make contributions to super and, upon meeting certain criteria, claim a tax deduction for doing so. Prior to 1 July 2017 one such condition was that less than 10% of income had to come from salary and wages. This has now been removed allowing more people to claim a tax deduction this financial year.

The contributions upon which a deduction can be claimed are taxable to the super fund, so a tax saving will only be achieved where a person's marginal tax rate would otherwise be higher than in their super.

Who is eligible to claim a personal deduction for super contributions?

- Anyone aged 18 to 65 regardless of their work status.
- A person under 18 if they earned income as an employee or business operator.
- A person age 65 to 75 if they meet the work test i.e. have worked 40 hours over 30 consecutive days during the year. If the person turns 75 during the year, then only contributions made up to the 28 days after their birthday can be claimed.

Mark is turning 65 on 15th February 2018 and wants to retire from full time work at the end of February. He will be able to claim a tax deduction on any personal contributions he makes in the year up to 30 June 2018.

What types of contributions can be claimed?

Personal contributions made to a complying super fund in the financial year can be claimed as a tax deduction on the individual's return. You can't claim for the following:

- Contributions made to defined benefit or untaxed super funds usually can't be claimed (check with us first).
- A benefit transferred from a foreign super fund.

Remember that compulsory employer SG payments and voluntary pre-tax salary sacrifice payments are not personal contributions. Non-concessional contributions are personal contributions, but no tax deduction is claimed on them and accordingly they aren't taxed by the super fund.

How much is the deduction?

The full amounts contributed on a pre-tax basis can be claimed. Whilst there is no limit to the deduction that can be claimed, the following should be noted:

- Personal contributions for which a tax deduction is claimed count towards the concessional contribution cap, which is $25,000 for 2017/18. Best not to go over this to avoid additional tax. Remember too that employer SG and pre-tax salary sacrifice contributions count towards this cap.

- The deduction received cannot create or increase a loss. In other words, the amount claimed as a tax deduction cannot be greater than your taxable income.

So, if a person had $10,000 in employer SG payments for the year, they could only claim a maximum of $15,000 for personal super contributions without incurring excess tax on the contributions.

Let's say Max's only taxable income is $10,000 in interest for the year and he has made personal super contributions of $18,000. He would only be able to claim deduction on $10,000 worth of contributions, not the full $18,000.

Personal contributions made and not claimed (or contributions on which a deduction is disallowed) will count towards the Non-Concessional Contribution Cap. So, in the above example, Max's super contributions would be split as concessional contributions of $10,000 and non-concessional contributions of $8,000.

How do you make a claim?

Step 1: Make the contribution to the fund. This must be done prior to 30 June in the year you wish to claim the deduction.

Step 2: Provide written notice to the fund that you wish to claim a tax deduction.

This has to be done by the earlier of lodging your personal tax return, and the end of the *following* financial year. The fund also has to still hold the contributions in accumulation phase, so this has to be lodged prior to rolling over to another fund or starting an income stream.

Most public offer funds have a form for this, or there is one available from the ATO website for SMSF's. Contact us and we will assist you.

Step 3: The fund sends you written acknowledgement that they have received the notice.

Step 4: Lodge your tax return claiming the amount as a deduction. You can not claim the deduction if you have not completed step 2.

CASE STUDY

Fred and Wilma are both aged 62 and retired. They have decided to sell their jointly owned holiday home worth $800,000 which will trigger an assessable capital gain of $60,000 each.

Fred has an account based pension worth $1.65m and super balance of $150,000. Wilma has an account based pension worth $500,000.

Account based pension income is not assessable income. So, Fred and Wilma's only assessable income is the capital gain, and they would ordinarily incur $12,147 each in tax (including Medicare Levy). If they both contribute $25,000 to super and claim a tax deduction for the contribution, then this drops their tax payable to $3,447 each. The contributions will be taxed by their super funds, which if we assume the maximum rate of 15%, would be $3,750. (Many SuperWrap accounts and SMSF's would have a much lower effective tax rate than 15%). Even still, the total tax saving is a min. $9,900 combined.

Note that Fred has already used his $1.6m pension transfer cap and so his contribution will have to remain in accumulation phase. Wilma can not add the amount to her existing pension, but she may be able to contribute $300,000 of the sale proceeds to super by way of NCC's (assuming she has not made any in the previous 3 years). She could then use the $325,000 to start a second pension, or amalgamate her two accounts into a new super pension.

Things to be aware of

- The contribution will be treated as assessable income in the super fund and tax of up to 15% (or up to 30% if you earn more than $250,000) will apply.
- Once the money is in super, it can't be accessed until a condition of release is met – usually retiring after preservation age or reaching age 65.
- Personal super contributions made where no tax deduction has been claimed are treated as Non-Concessional Contributions (NCC). Care must be taken not to exceed the NCC cap.

Scenarios where this is likely to be beneficial

This strategy can help reduce tax payable for those who have savings they are prepared to invest for retirement purposes.

A tax benefit will only occur if you have income over your relevant tax-free threshold, which for Australian residents in 2017/18 are:

- $20,542 (including the Low-Income Tax Offset).
- $32,279 if you are single and eligible for the Seniors and Pensioners Tax Offset
- $28,974 if you a member of a couple and eligible for the Seniors and Pensioners Tax Offset

People with income lower than their tax-free threshold are better to make Non-Concessional Contributions to super (personal contributions where no tax deduction is claimed) if possible, as the contributions are not taxed by the super fund. However, if making further Non-Concessional Contributions is not an option due to having already utilised the cap or having a super balance above the allowable threshold, then these contributions may allow further funds to be added to super.

Non-residents should remember that Australian sourced managed funds, direct shares and deposit accounts will deduct withholding tax and the investment income generated will not provide assessable income in Australia. Hence if this is the only source of income in Australia, there is no benefit in claiming a tax deduction for super contributions.

Further opportunity to come

From 1 July 2018, unused concessional contributions can be carried forward for up to five years, potentially allowing individuals to make higher personal deductible contributions above $25,000. The first year the carried forward contributions can be made is 2019/20 and the person must have less than $500,000 in super in total.

t 02 9328 3322
f 02 9328 3323
e team@lfma.com.au
w www.logicalfinancial.com.au

Suite 21, Level 2, 8 Hill Street,
Surry Hills NSW 2010
PO Box 103
Darlinghurst NSW 1300

logical financial management