UOB

Right By You

CONTENT

Demystifying Blockchain

Information as of 14 November 2023

Global Economics & Markets Research
Email: GlobalEcoMktResearch@UOBgroup.com
URL: www.uob.com.sg/research

Demystifying blockchain

Blockchain, a concept that has grown in prominence recently, has come to be associated with innovation, disruption, and transformation. Initially invented to be the digital currency for the Internet, it has since become clear that blockchain has many other potential applications with Banking and Finance leading the way.

In this deep dive report, we will explain what blockchain is, how it works, why it is so important, and its future potentials.

Key takeaways:

- History and motivations behind the invention of blockchain
- The technology and building blocks of the blockchain
- Security and challenges of blockchain technology
- Applications in banking
- Benefit and challenges of blockchain
- The road ahead

Morgan Chia
UOB Blockchain & Digital Assets (BCDA)

1 The beginning of blockchain

We shall start with the problem statement and the motivation behind the invention of the blockchain.

1.1. What problem was the blockchain trying to solve?

Blockchain was invented to allow people to send digital money to each other directly (peer-to-peer) without a trusted third party. This idea was first thought of in the 1990s before online payment was invented.

1.2. The birth of blockchain

In the 1990s, a group of computer scientists invented the first blockchain. However it was not able to gain traction because it was not able to solve the ***double spending*** problem. In a traditional centralized environment, the financial institution keeps records and debits the account balance when money is spent. Without a centralized bookkeeper, it is extremely difficult to prevent anybody from altering the transaction ledger after the transaction was recorded and spend it again thereby committing double spending.

Later in 2008, Satoshi Nakamoto invented the Bitcoin blockchain that solved this problem. Satoshi Nakamoto released a whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System." This document introduced the world to a new form of digital currency, Bitcoin, and the revolutionary blockchain technology.

You can refer to section 3.7 that explains what double spending is and how it is solved.

1.3. The motivation

Bitcoin, the first public blockchain that gained mass adoption, was created in response to the financial crisis of 2008, aiming to provide an alternative to traditional banking systems. Nakamoto wanted to create a decentralized, trust-less payment system that could operate without intermediaries.

The first block of the Bitcoin blockchain, named the "genesis block," contained a message referencing a headline from The Times newspaper: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." This message underlined the motivation behind Bitcoin's creation.

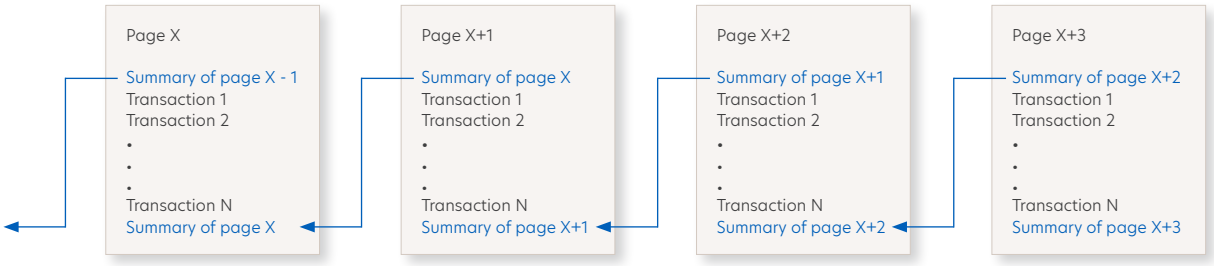
2 The basics

In this section, we will cover the basic concepts that underpin the blockchain technology.

2.1. What is a blockchain?

The blockchain is a system for recording transactions in a secure and transparent way where everyone maintains a full copy of the ledger that is constantly updated with new transactions. Imagine everyone maintains a book with many pages of records. Each page begins with a shortened summary of the page before it. If someone changes anything on an earlier page, he needs to change the summary for all the pages coming after it. If we call these pages "blocks", having each block linked to the previous block forming a continuous chain, we have a blockchain.

Diagram 2.1a



Source: UOB Blockchain & Digital Asset

In this analogy, the book represents the blockchain, each page represents a block and the "summary" is the chain implemented using cryptographic hash. Once added to the blockchain, the transactions cannot be altered or deleted. This immutability and transparency are the core principles of blockchain.

Throughout this report, there will be references to public blockchains such as Bitcoin and Ethereum. Although their use cases are different from enterprise blockchains used by corporates and financial institutions, the concepts and underlying technology are mostly the same. In this report, the terms 'crypto' and 'cryptocurrency' are used interchangeably to refer to the digital currency that is native to a blockchain.

2.2. Key components

Key components of a blockchain include:

- **Transactions:** Transactions are the actions recorded on the blockchain that could represent the transfer of digital assets from one user to another. Each transaction contains details such as the sender's and recipient's wallet addresses, the amount transferred, and a digital signature for verification. It is worthy to note that, contrary to common belief, transactions on the blockchain are not encrypted.

- **Blocks:** These are containers for transactions. Each block is like a page on a book that contains a unique identifier called a cryptographic hash and a reference to the previous block's hash, creating a chronological chain.

- **Nodes:** Nodes are participants in the blockchain network that runs the blockchain software. They are responsible for verifying the transactions and adding new blocks to the network.

- **Consensus Mechanisms:** These are software protocols that ensure that all participants in the network agree on the state and contents of the blockchain. Consensus mechanism ensures security and integrity of the blockchain and thus helps to provide trust for the network in an untrusted setting. Common consensus mechanisms include Proof-of-Work (PoW) and Proof-of-Stake (PoS). Many blockchains have moved from PoW to PoS to reduce energy consumption.

2.3. Decentralization vs distributed

Decentralization is a basic element of blockchain technology. Traditional banking systems rely on central authorities, such as banks and governments, to facilitate and validate transactions. In contrast, blockchain operates in a decentralized manner, where no single entity has control.

Blockchain is a type of distributed ledger technology (DLT), which means that a copy of the ledger is distributed to all nodes in the network. Despite being "distributed", blockchain is more like a decentralised computing system and we shall discuss the differences below.

In a distributed computing system, a problem is divided into small tasks that are processed by multiple computers(nodes) in parallel to make the computation faster and more efficient, the results are then combined in a centralised server to produce a final solution.

On a decentralised network, all nodes work on the same problem using the same[1] complete set of source data; having more nodes does not make the system faster but it does make it more secure and resistant to failure.

In summary, the main difference between decentralised and distributed computing is that decentralised computing such as a blockchain is not designed to be as efficient as possible. Instead, it is designed to be secure and resistant to failure.

1: all nodes are working to solve the math puzzle on the same set of transaction data

3 Building blocks of the blockchain

Blockchain is fusion of multiple technologies cleverly integrated to create a secured and immutable network. In this section, we shall delve into the components and how they interact to form the blockchain.

3.1. What is a digital signature?

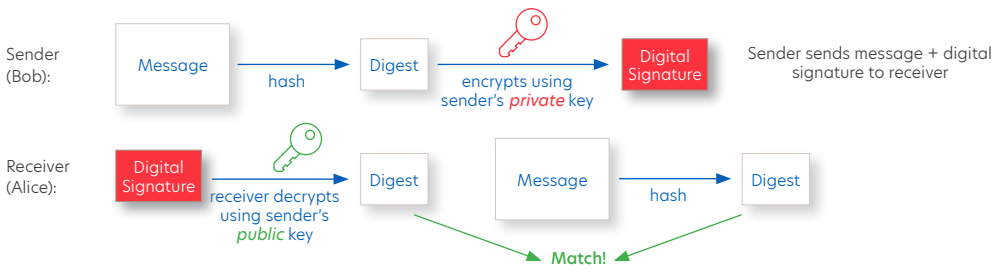
A digital signature is an cryptographic stamp on a digital document that can be used to prove the document originates from the signer and the content has not been altered.

They involve two keys: a private key and a public key. The private key is kept secret and used to sign transactions, while the public key is shared with others to verify the signatures.

Digital signatures use complex mathematical algorithms to create a unique signature for each transaction. This signature ensures that only the owner of the private key can authorize a transaction - it is used on the blockchain for this purpose.

A digital signature also confirms the data is unaltered and originated from the signer.

Diagram 3.1a



Source: UOB Blockchain & Digital Asset

How this works: Bob writes an email and uses the private key to generate a digital signature for the email. The message and digital signature will be sent out together. The receiver, Alice, can use Bob's public key and digital signature to verify the email is authentic. Changing any part of the message, even adding a comma, will cause (hash) verification to fail.

Digital Signature is the mechanism used in blockchains such that only the person holding the private key for that wallet can control the funds / assets inside that wallet. Blockchain mining/validating checks the content of a transaction is signed by the correct wallet owner.

The Bitcoin and Ethereum blockchains use the Elliptical Curve Digital Signature Algorithm (ECDSA) to generate the private/public key pairs. Other blockchains may use other digital signature algorithms for signing transactions, more details can be found in section 5.2.

3.2. Signing transactions

On the Blockchain, the private key is used to sign a transaction by appending a digital signature. With the transaction data and the digital signature, the public key can be used to verify the transaction matches the signature. Hence, when the owner of say Wallet A signs a transaction to send 1 crypto to Wallet B, it will create a transaction (Wallet A sends N crypto to wallet B), signs using his private key and appends the signature to this transaction and broadcasts it to all the nodes for validators to add to the next block.

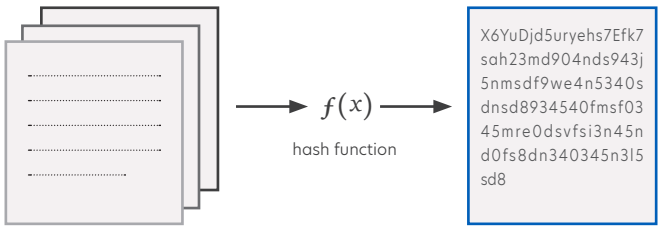
3.3. Validating transactions

The validators will then use the Wallet A's public key and the transaction data to validate the digital signature. Only after this validation is correct will the transaction be included to the next block, otherwise this transaction will be discarded.

3.4. Hashing

A hash is a mathematical function that transforms any amount of data into fixed length of output typically 64 alphanumeric characters. Hashing is a one-way function such that the output cannot be reversed engineered back to the original content. Hashing is also deterministic meaning that an input will always get the same output hash. Hence, without disclosing your content, you can prove you know the content by hashing and compare the hashes.

Diagram 3.4a



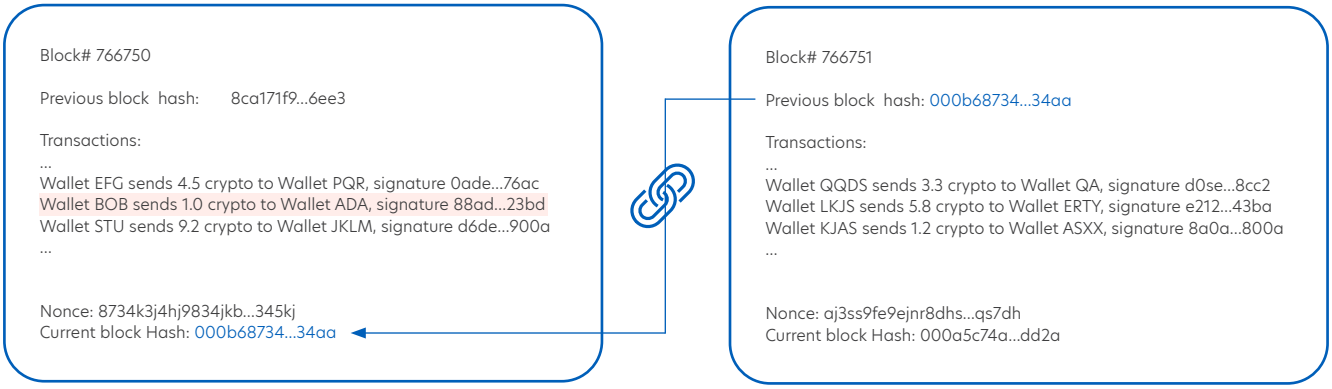
Source: UOB Blockchain & Digital Asset

Hashing is widely used to store hashed passwords on computer servers, so when users login with their passwords, the passwords are hashed and compared against the stored hashed copy on the servers. Passwords are often stored hashed to prevent hackers and support staff from gaining access to them.

Hashing can also be used to ensure the input data has not been altered. For example, if you want to check if the content of a website has been changed over time, you can download the web page and compute a 64-character hash and store it. Sometime later, you can redo the steps by computing the hash and compare against the previously computed hash. If the hashes match, the content of the web page has not been altered.

Hashing is used in the Blockchain to create the wallet address from the public key. It is also used on the entire content of a block of transactions and the hash result is added to the body of the next block, which goes on and on. This hash written into the block is the "page summary" we mentioned earlier in the introduction section.

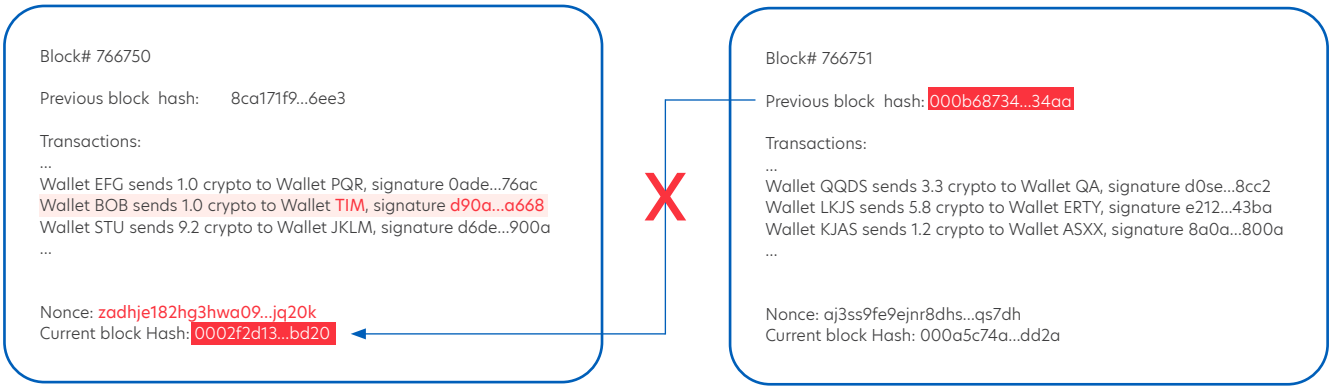
Diagram 3.4b - The hash forms a chain linking a block to the previous block



Source: UOB Blockchain & Digital Asset

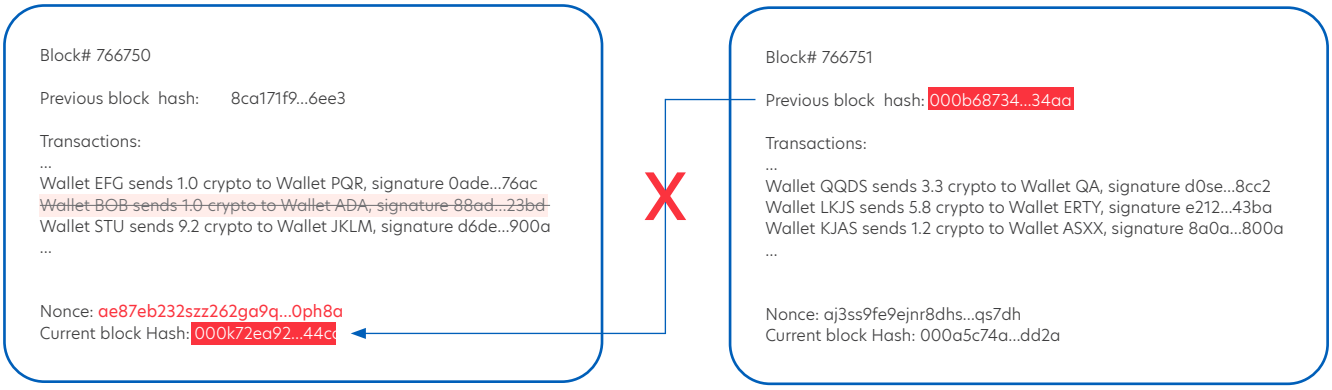
The hashes form an immutable chain. If anyone changes a record on any of the earlier blocks, the hash on that block will be changed, causing the "chain" to break as it will no longer tally with the hash embedded in the following block. In the example below, Bob changes the transaction on a previous block to send a crypto to another person, causing the chain to break.

Diagram 3.4c - Chain is broken when the hash of previous block is changed when the content is altered



Source: UOB Blockchain & Digital Asset

Diagram 3.4d - Chain is broken when the hash of previous block is changed when a transaction is removed



Source: UOB Blockchain & Digital Asset

Checking the hashes of the previous blocks is one of the activities done by the miners/validators to ensure the integrity of the chain they are working on. This effectively prevents double spending.

To summarize, the blockchain contains transactions which are signed by the private keys owning the wallets where the transaction originates; while the chains are the block hashes of the preceding block which is embedded into the body of the following block. The miner / validator checks the digital signatures and the chains' hashes to ensure the blockchain's integrity.

3.5. What is a blockchain wallet?

We have mentioned wallet earlier without explaining it, in this section we shall discuss what a blockchain wallet is.

A blockchain wallet is a digital tool that stores private keys and allows users to manage their crypto and token holdings.

Cryptos and blockchain tokens exist as transactions on the blockchain and are not stored in a wallet. The blockchain wallet is a virtual address that indicates where cryptos and blockchain tokens should be transmitted. An alphanumeric string is used to represent it. Unlike a normal wallet, it does not store cryptos or blockchain tokens but provides access to them.

A blockchain wallet should minimally support the following functions:

1. Storing the private key(s) for wallet(s) on one or more blockchains
2. Signing transactions using the Private Key
3. Sending and receiving cryptos and tokens
4. Display balances of cryptos and tokens

More advanced features of blockchain wallets may include:

5. Buying and selling cryptos and tokens
6. Importing tokens and Non-Fungible Token (NFTs)
7. Converting between different cryptos and tokens

3.6. Relationships between private key, public key and wallet address

A private key is a random sequence of alphanumeric string of characters, and it is used to generate its public key via a digital signature algorithm. The public key is then one-way hashed and truncated to form the wallet address. As a result, these three components are mathematically related, but it is not possible to reverse engineer the wallet address to get the private key.

Private key ► Public key ► Wallet address

You might be interested in the fact that a wallet address can be used on another blockchain that has the same address encoding, hashing function and digital signature function e.g. Ethereum and Polygon. More information is provided in the section 5.2.

The private key is the most important part of the relationship between private keys, public keys, and wallet addresses. It is used to sign transactions and prove ownership of funds. The public key is used to verify signatures and generate wallet addresses, but it cannot be used to reveal the private key.

Therefore, it is essential to keep your private key safe and secret. If you lose your private key, you will lose access to your funds.

3.7. What is double spending, and how consensus mechanisms solve the problem?

Double spending refers to spending the same unit of currency more than once, and it is a critical issue in digital currencies. Double spending causes the system to lose its integrity and the asset to lose its value when a blockchain asset is spent multiple times over.

Without a trusted third-party keeping records, it is extremely difficult to prevent double spending.

Consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS), solve the double spending problem by ensuring that transactions cannot be altered or removed once added to the blockchain.

PoW involves ***miners*** solving complex puzzles to validate transactions, while PoS relies on ***validator's*** stake in the network to validate transactions.

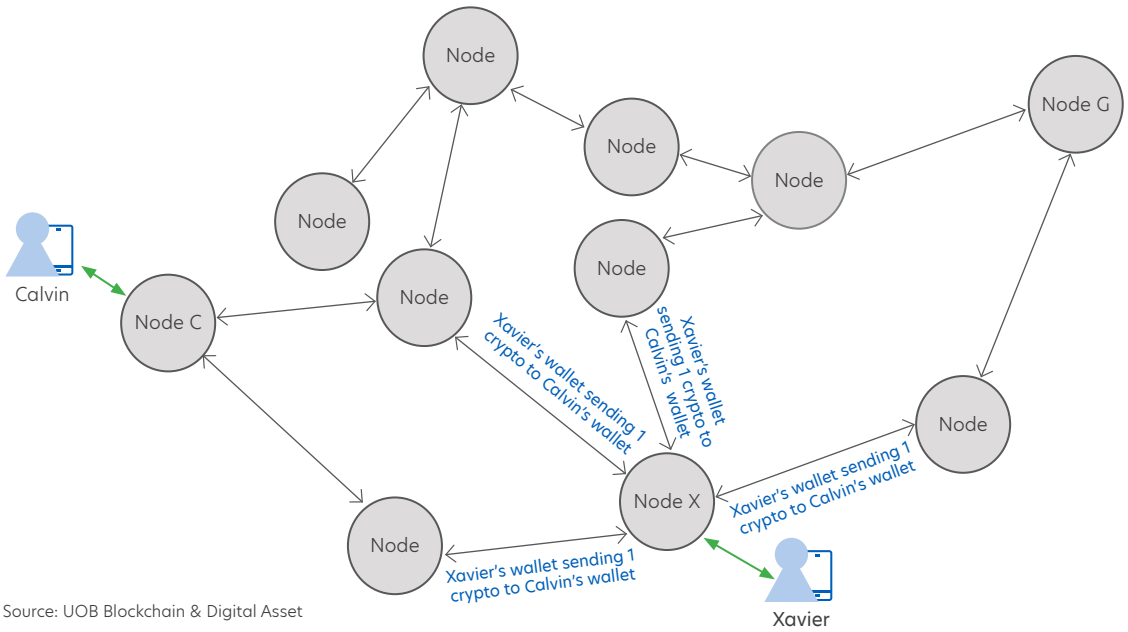
There are 2 ways double spending can be performed by a bad actor:

1. Alter the content of a mined block - The bad actor spends a crypto, and after it is accepted by the recipient, alters the recipient to another person or remove the entire transaction. Refer to diagrams 3.4c and 3.4d.

2. Simultaneously send the same crypto to 2 recipients - The blockchain is maintained by thousands of nodes and not all of them are connected directly and thus some nodes need others to forward the transactions to them. Network latency could also cause some nodes to receive published transactions later.

   Below diagram shows how a normal transaction will be published when a transaction takes place such as when Xavier sends a crypto to Calvin.

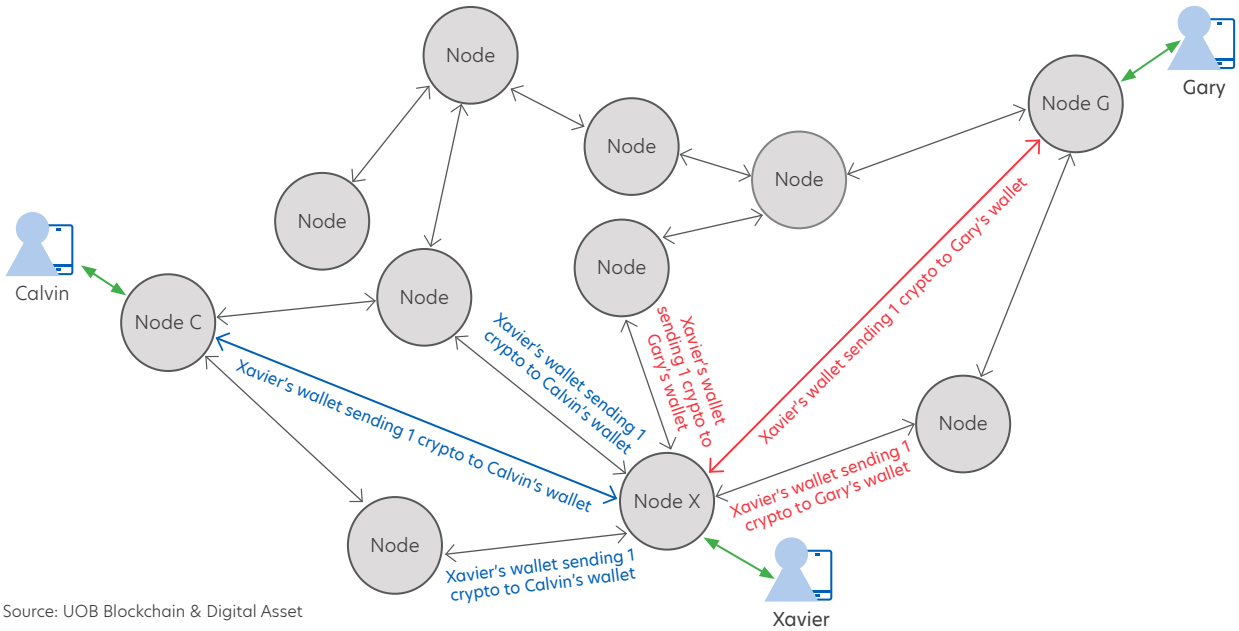
Diagram 3.5a



Source: UOB Blockchain & Digital Asset

This is how Xavier can simultaneously spend 1 crypto twice. Say Xavier is using node X and he wants to send 1 crypto to Calvin and Gary who are using wallets connected to node C and node G respectively; Xavier could publish one transaction "Xavier's wallet sends 1 crypto to Calvin's wallet" to node C and simultaneously publish another transaction "Xavier's wallet send 1 crypto to Gary's wallet" to node G. Doing so node C will add Calvin's transaction to the latest block and Calvin will see his wallet reflecting the new crypto; as for Gary, his transaction will be added to node G's block and reflected on this wallet.

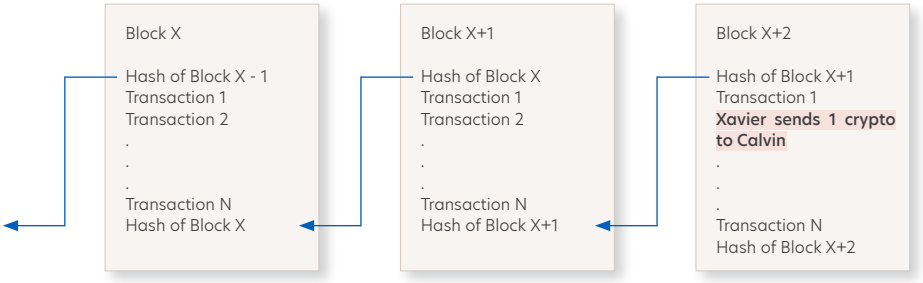
Diagram 3.5b



Source: UOB Blockchain & Digital Asset

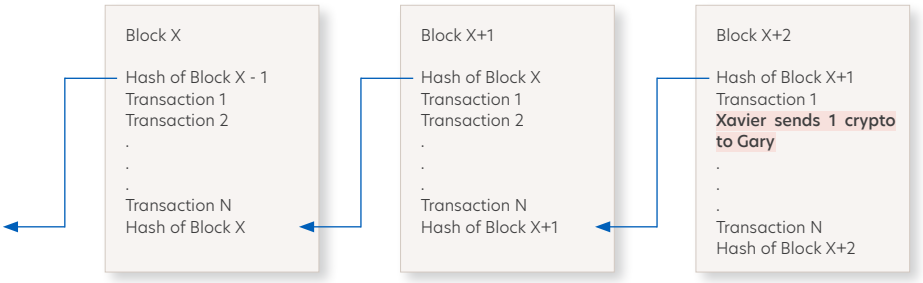
This has effectively created 2 chains on the network.

Diagram 3.5c



Source: UOB Blockchain & Digital Asset

Diagram 3.5d

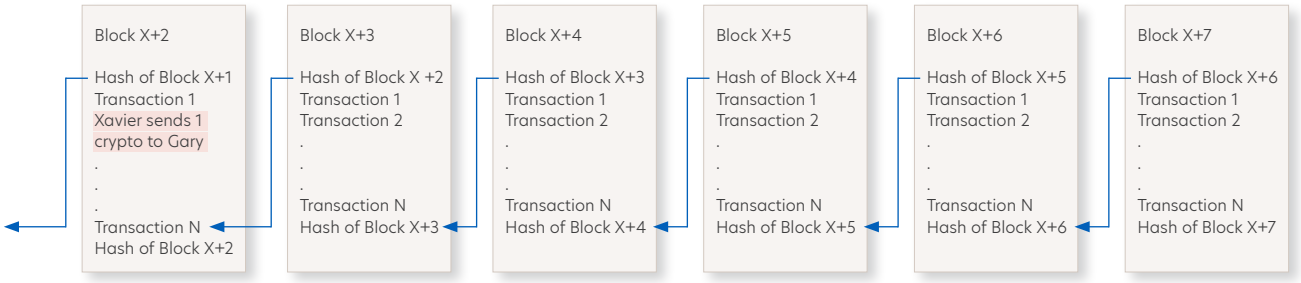


Source: UOB Blockchain & Digital Asset

To resolve this issue with multiple chains, the consensus mechanism will work on the longer chain and discard the shorter chain.

This is because the longest chain, as explained in the Nakamoto's Bitcoin whitepaper, has expended the highest computation power and hence the most trusted chain. After several blocks of mining, the winner chain will emerge and only 1 of the 2 transactions will be retained. It is safe to assume finality is achieved after 6 blocks are mined (including itself) because the chances of a bad actor altering blocks so far behind is exceedingly low.

Diagram 3.5e



Source: UOB Blockchain & Digital Asset

3.8. How do public blockchains provide trust in an untrusted environment?

Satoshi Nakamoto invented the first blockchain, which is a public blockchain that is open to all users. Nobody has the power to restrict who can participate or do what on a public blockchain. Anyone may join without requiring KYC. This means the bookkeepers may be anonymous, so how can you trust unidentified parties to keep the books honest?

The answer lies in the consensus mechanism. Let's discuss using Bitcoin and PoW to illustrate.

When transactions are consolidated to form a block and they are validated against the digital signature and mined expending computing power to guess the special number called nonce such that the resulting block hash satisfy the block difficulty. The derived hash is included in the current block and also added to the next block.

The amount of work needed to mine a Bitcoin block requires billions of computations per second for 10 minutes.

If someone tries to alter the transactions in any block, he needs to expend computing power to mine that block again and also mine the following blocks because the block hash has changed. This makes it extremely difficult because the rest of the miners on the network are already working on the next or following blocks. Hence it would be almost impossible for a dishonest participant to mine an existing block and catch up with the rest of the miners i.e. mine faster than all the miners on the network.

This difficulty makes the blockchain immutable and tamper-free, preventing double spending.

To break the consensus mechanism, you need to overwhelm the blockchain with the majority of computation power i.e. launch a 51% attack, which is a very expensive exercise. More details can be found in section 6 below.

Similarly, for Proof-of-Stake PoS blockchains, the validators are kept honest via the consensus mechanism. For PoS blockchains, the process is similar except a validator node is chosen randomly based on the amount of crypto that is staked. The chosen validator must stay honest otherwise a portion of his staked crypto will be slashed.

Bottomline is, participants trust the digital assets and transactions are secured by:

1. The digital signature validation that provides assurance the assets are only accessible by the person holding the private key

2. The math of the consensus mechanism that makes manipulating the blockchain very difficult and extremely expensive resulting in no single entity controlling the blockchain,

On the other hand, the blockchain does not provide "trust" that the transactions published are legitimate or sent to the correct recipient and participants do not need to trust any individual, organisation or government to maintain the blockchain.

3.9. Gas fee and Transaction fee

Gas fees are the transaction costs associated with using the Ethereum and compatible blockchains. Gas is used to pay for the computational on the Ethereum and compatible blockchains. Gas fees represent transaction costs, serving as compensation for miners or validators responsible for validating transactions. Gas is the metric that quantifies the computational effort needed to execute specific actions within the Ethereum network. Therefore, the amount of gas required for different operations may vary.

In Ethereum-based blockchains, gas is a necessity for "writing" operations to the blockchain, for tasks like transferring cryptos or tokens, deploying smart contracts, creating tokens, and destroying tokens. It's important to note that checking a balance is categorized as a read operation and thus does not consume gas.

Gas fees are settled using the native cryptocurrency of the blockchain, such as ETH or MATIC. The calculation for gas fees is as follows:

Total Gas Fee = Units of Gas Used * (Base Fee + Priority Fee)

The "Units of Gas Used" vary depending on the operation, and in general, the more complex the activity, the more units of gas will be required.

The base (gas) fee is mandatory, while the priority fee is an optional tip often given to validators to prioritise your transaction. It's worth mentioning that validators only receive priority fees, as the base gas fee is permanently removed from circulation.

On networks that do not have programming capability such as Bitcoin and Litecoin, transaction fee consists of purely the base and priority fee. Hence the calculation of transaction is as follows:

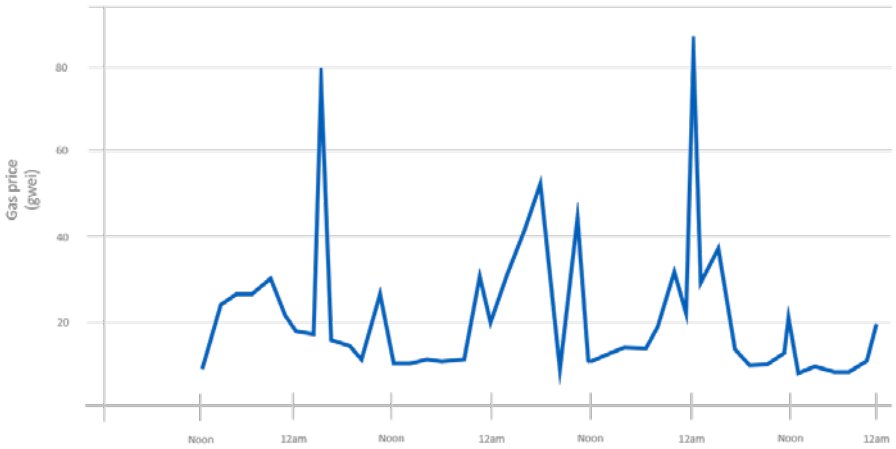
Total Transaction Fee = Base Fee + Priority Fee

3.10. Gas price

Gas prices fluctuates during the day based on demand, so it's a good idea to select a time when gas prices are at their lowest if you want to minimize the total gas fee you'll incur. On weekdays, the most affordable ETH gas rates are typically found between 12 PM and 4 PM (SGT).

Efficiently managing gas fees means choosing the appropriate fee and transaction priority. The maximum gas fee represents the highest amount you're willing to spend on a transaction.

Diagram 3.9a - Typical intraday Gas price on a weekday



Source: UOB Blockchain & Digital Asset

Let's explain this with an example:

> Albert wants to send some ETH to his friend. The standard transfer operation requires 21,000 units of gas while the gas price (base fee) is 20 gwei (a billionth of a ETH) and he added a 5 gwei tip.
>
> Hence the Total Gas Fee will be 21,000 x (20 + 5) = 525,000 gwei or 0.000525 ETH.
>
> Assuming the price of ETH is USD1,630, the total transaction fee will be USD 0.85575.

4 Smart contracts

Smart contract was introduced in 2015 with the launch of Ethereum blockchain. It brings programmability to the blockchain creating many interesting use cases such as decentralized apps, DeFi, NFTs, stable coins and CBDC.

A smart contract, despite its name, is not a legal contract but a computer program that is deployed and run on the blockchain. Smart contracts are self-executing programs with the terms of the contract directly written into software code. They operate on blockchain platforms and automatically execute when predefined conditions are met.

Once written to the blockchain, the code cannot be changed, with the smart contract address finalized at the point of deployment; the tokens created can be used by importing (referencing) that address into a blockchain wallet. While not all smart contracts create new tokens, smart contracts could function as autonomous application to facilitate other transactions such as loan.

Some differences between a smart contract and a normal computer program:

Smart Contract	Normal Computer program
Cannot be changed after it is written to the blockchain	Can be replaced or removed
Has a smart contract address on the blockchain	No address but a file location on the computer
The program code and the variables are "public" for all parties who have access to the blockchain	The program code and variables are hidden from parties using the computer program
There is a 24KB limit on the size of the smart contract	There is not fixed limit on the size of a computer program, it varies based on the language used, the operating system and virtual memory available. Typically programs that run on a desktop computer could vary from a few megabytes (MB) to 10s of gigabytes (GB) in size.
Runs on the Ethereum Virtual Machine restricting the ability to perform tasks such as reading the internet	No restriction as long as there is network connection
Requires gas fee to execute transactions that updates the blockchain	No gas fee is required

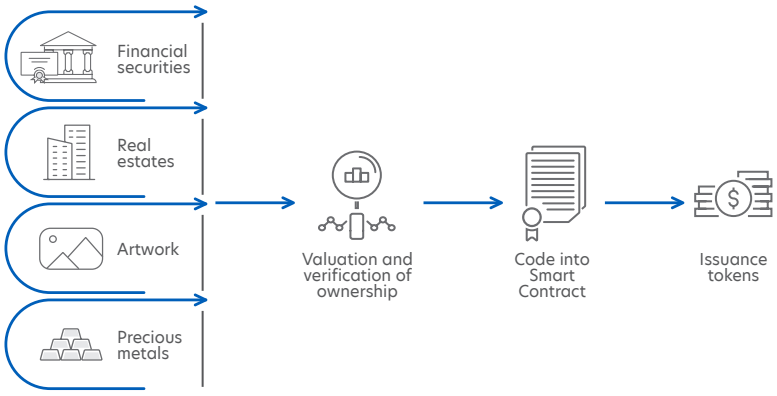
Source: UOB Blockchain & Digital Asset

Smart contracts are a relatively new technology, but they have the potential to revolutionize many industries. For example, smart contracts can be used to automate complex financial transactions, create new types of decentralized applications, and even streamline supply chains and trade finance. It will be interesting to see how smart contracts will develop in the years to come.

4.1. What is security / asset tokenisation?

It is the process of converting the ownership of an item of value into a token usable on the blockchain and the token is created by a smart contract.

Diagram 4.1a - Asset Tokenisation Process



Source: UOB Blockchain & Digital Asset

Imagine you have an expensive piece of artwork that is valued at $1 million. You can write a smart contract, to represent the ownership of that artwork, which create 1 million tokens and price each token $1. The owners of the digital tokens will have legal ownership to a portion of the underlying asset.

Examples of security tokens include equity token, debt token, real asset token and many other assets including precious metals, commodities and even artwork.

Some advantages of securities tokenisation include:

- **Fractionalization** - split the asset into small portions to lower the barrier of entry
- **Increased liquidity** - having small portions make it cheaper to invest in, similar to stock splits
- **Reduced intermediaries** - use of smart contracts can automate many portions of asset lifecycle and reduce intermediaries

4.2. How is a blockchain token created?

Blockchain tokens can be created by smart contracts.

A smart contract developer writes a smart contract, deploys it on a blockchain and mint the tokens. Once the smart contract is deployed, the address will be finalised, users can reference this address to find the smart contract and interact with it. Subsequent tokens that are minted from this smart contract will have the same address.

It should be noted that token names like USDC are not unique on the blockchain. Anyone can create blockchain tokens and name them whatever they like; the smart contract address is what distinguishes them.

For example, the USDC stable coin's Ethereum blockchain smart contract address is 0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48, and if someone else produces another blockchain token and names it USDC, the new smart contract address will be different. This is similar to how the URL of a website is unique.

A smart contract could also be deployed on all ERC compatible blockchains as long as the creator has access and permission on the blockchain to deploy it.

ERC stands for "Ethereum request for comment," which is the standard for defining blockchain tokens and smart contracts.

The most common language used for writing smart contract is Solidity, which is used to write smart contracts for Ethereum Virtual Machine (EVM). The EVM is the software that executes the smart contract. For other blockchains that are not EVM compatible, other languages such as Go (for Hyperledger Fabric) and Rust (for Solana) are also used.

Let's say I have a digital SGD smart contract written in Solidity, it could be deployed on Ethereum, and other EVM compatible blockchains such as Polygon, Hyperledger Besu and Quorum.

There are many readymade templates available for creating smart contracts, the most common are ERC-20 (used for asset tokens and stable coins), ERC-721 (NFT), ERC-1155 (asset tokens and NFT) and ERC-1400 for security tokens.

In Singapore, the central bank is piloting Purpose Bound Money (PBM), for specific usage such as learning credits for citizens to improve their skills or helping in mid-career switch. The PBM is a "wrapped" version of the digital SGD issued by the banks. It is created by having a PBM smart contract accepting digital SGD tokens and creating equivalent value of PBM token and sending the PBM to the digital SGD sender in the same process.

So, if you want to get a $10 worth of PBM, you have to deposit $10 worth of digital SGD into the PBM smart contract and it will create a $10 PBM token and send to your wallet. This PBM tokens have new properties such as restriction of usage to certain merchants, more rules can also be embedded such as restriction of product code, and time/date of purchase etc.

Merchants can redeem the digital SGD by sending back the PBM to the smart contract to get back equivalent value of digital SGD and off ramping these digital SGD from the local banks for fiat.

4.3. Usages of smart contracts

Besides security tokenisation, smart contracts also have applications in areas like decentralized finance (DeFi), supply chain management, legal agreements, and more.

In the banking sector, smart contracts have numerous applications such as:

- Loan Origination: Smart contracts can automate the loan application, approval, and disbursement process, reducing paperwork and processing time.
- Insurance Claims: When an insured event occurs, smart contracts can trigger automatic claims processing and payouts, streamlining the insurance industry.
- Supply Chain & Trade Finance: Smart contracts can facilitate trade finance by automating payment settlements and documentation handling in international trade transactions.

Despite being a relatively new technology, smart contracts have the potential to have a major impact on our world. As smart contracts become more sophisticated and widely adopted, we can expect to see even more innovative and groundbreaking applications emerge.

4.4. Pros and cons of smart contract

The following are some benefits and drawbacks of smart contracts:

Pros:

- Efficiency: Many tasks can be automated by smart contracts, doing away with the need for middlemen. This can save time and money and lead to cost reduction.
- Security: Smart contracts are secured by cryptography and blockchain technology, which makes them very difficult to hack or tamper with.
- Transparency: All transactions on a blockchain are transparent and visible to everyone. This helps to build trust and accountability.
- Accuracy: Smart contracts are very accurate because they are executed automatically by the computer code. This helps to reduce the risk of human error.

Cons:

- Complexity: Smart contracts can be very complex to write and deploy. This means that there is a risk of errors, which could lead to unexpected and unintended consequences.
- Lack of flexibility: Smart contracts are immutable, meaning that they cannot be changed once they are deployed. This can be a problem if there is a need to change the terms of the contract.
- Legal uncertainty: Despite its name, smart contracts are not legal documents and hence does not have any legal backing.

In general, smart contracts provide many advantages, but it is important to be mindful of the associated risks and take steps to mitigate them such as getting qualified professionals to review the codes before deploying them.

5 Under the hood

In this section, we will explore more advanced concepts of blockchain, shedding light on aspects that are often overlooked or misunderstood. Our aim is to provide a comprehensive understanding of the blockchain technology.

5.1. What is mining and how is cryptocurrency created on the blockchain?

Crypto is created through a process called mining. The PoW consensus mechanism is used to secure the Bitcoin blockchain and ensure that all transactions are valid where miners compete to solve a computationally difficult puzzle. The first miner to solve the puzzle gets to add a new block of transactions to the blockchain and is rewarded with newly created bitcoins.

It is worthy to note that if you want to purchase a crypto, you do not need to mine the coins yourself. You can just purchase it from a reseller or from a miner. Similarly you don't need to grow crops yourself, you can purchase them from a farmer or grocery store.

The puzzle that miners solve is based on the SHA-256 hash function. To solve the PoW puzzle, miners need to find a number that, when hashed, produces a value that is less than or equal to a target value. The target value is a constantly changing number that is determined by the difficulty of the mining network. The more computation power there are in the network, the more difficult the puzzle becomes.

The process of solving the PoW puzzle is very computationally expensive. Miners need to use powerful computers and specialized software to try billions of possible solutions per second.

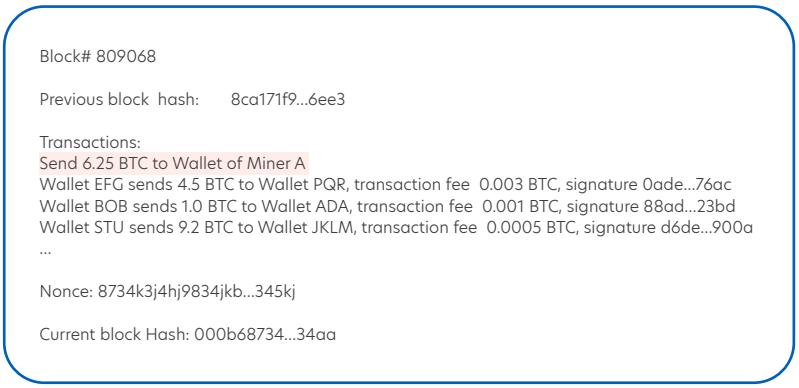
The PoW consensus mechanism is reliable way to secure the blockchain. However, the PoW mechanism is also very energy-intensive which has led to concerns about the environmental impact of blockchain mining.

The detailed process of PoW mining is as follows:

1. The miner writes the first transaction on the block to create and send new N (this N is the block reward for bitcoin that started with 50 and halves every 4 years, this reward is now 6.25 in 2023) crypto to his own wallet address. All the other transactions on the blockchain have a sender address and a receiver address, only the first transaction does not have a sender address, this is how new crypto is created.

   Note: BTC is the symbol for bitcoin.

Diagram 5a - Miner puts his own wallet address on the first transaction to receive the block reward
(Some details of a block are excluded from the diagram)



Source: UOB Blockchain & Digital Asset

2. Miners gather all the transactions (from the mempool - a waiting area for transactions to be confirmed) that have not yet been added to the blockchain.

3. Miners sort the transactions based on transactions fees offered to prioritise those transactions offering higher transaction fees.

4. They create a block for these transactions and find a random number called "nonce".

5. They use a hashing algorithm to compute a unique string of 64 alphanumeric characters hash of the block content.

6. The miners will keep changing (brute force guessing) the nonce until they find a hash that meets the difficulty requirements of the network. The difficulty requirements are automatically adjusted every 2,016 blocks (every 2 weeks – this duration is known as the difficulty epoch) to ensure that it takes an average of 10 minutes (block time) to find a new block. Please be aware the difficulty epoch and block time differs between blockchains and the difficulty epoch is not applicable for PoS blockchains.

7. The miner who finds the first hash that meets the difficulty requirements gets to add the block to the blockchain and is rewarded with cryptos as per point 1.

   To explain further, say miner A puts his wallet address in the first transaction while miner B put his own wallet address. If miner A solved the puzzle by finding the nonce first, his block will be added to the chain so the first transaction in that block will create and send new N crypto to A's wallet will be part of the blockchain - this is how miner A is being rewarded with new crypto. Also, the miner who wins the race will get all the transaction fees inside the block.

For Proof-of-Stake (PoS) blockchains, the process is similar except a validator node is chosen randomly based on the amount of crypto that is staked. With PoS, brute-force guessing of nonce is no longer required and hence electricity usage is drastically reduced. The chosen validator must stay honest otherwise a portion of his staked crypto will be slashed.

5.2. Is there a standard for generating the private / public keys across blockchains?

Blockchain uses public key infrastructure (private/public key) for digital signing. The private key is usually a randomly generated 32bit number (64 hexadecimal numbers), it is then mapped to a public key using the Elliptic Curve Digital Signature Algorithm (ECDSA).

Here's a table listing some common blockchains, their consensus mechanisms, digital signature algorithms, and hashing algorithms.

Blockchain	Symbol	Layer	Digital Signature Algorithm	Hash (chaining the blocks together)	Private Key length	Wallet Address Format (encoding)
Bitcoin	BTC	1	ECDSA / Secp256k1 (curve)	SHA-256	256 bits or 64 hexadecimal characters	P2PKH(0x00), P2SH(0x05), SegWit('bc')
Ethereum	ETH	1	ECDSA / Secp256k1 (curve)	Keccak-256	256 bits or 64 hexadecimal characters	ChecksummedHex starting with 0x
Ripple	XRP	1	ECDSA / Secp256k1 (curve)	SHA-256	29 alphanumeric characters*	Ripple
Solana	SOL	1	EdDSA / curve25519	SHA-256	256 bits or 64 hexadecimal characters	Base58
Cardano	ADA	1	EdDSA / curve25519	Blake2	256 bits or 64 hexadecimal characters	Bech32, base58, or hexadecimal
TRON	TRX	1	ECDSA / Secp256k1 (curve)	SHA3-256	256 bits or 64 hexadecimal characters	Base58 starting with T
Litecoin	LTC	1	ECDSA / Secp256k1 (curve)	Scrypt	256 bits or 64 hexadecimal characters	P2PKH(0x30), P2SH(0x32), P2SH(0x05), SegWit('ltc')
Dogecoin	DOGE	1	ECDSA / Secp256k1 (curve)	Scrypt	256 bits or 64 hexadecimal characters	P2PKH(0x1e), P2SH(0x16)
Polygon	MATIC	2	ECDSA / Secp256k1 (curve)	Keccak-256	256 bits or 64 hexadecimal characters	ChecksummedHex starting with 0x
Arbitrum	ARB	2	ECDSA / Secp256k1 (curve)	Keccak-256	256 bits or 64 hexadecimal characters	ChecksummedHex starting with 0x
Optimism	OP	2	ECDSA / Secp256k1 (curve)	Keccak-256	256 bits or 64 hexadecimal characters	ChecksummedHex starting with 0x
Tether	USDT	ERC-20 token on Ethereum blockchain created by a smart contract	NA	NA	NA	NA
Circle	USDC	ERC-20 token on Ethereum blockchain created by a smart contract	NA	NA	NA	NA
Wrapped Bitcoin	WBTC	ERC-20 token on Ethereum blockchain created by a smart contract	NA	NA	NA	NA

Source: UOB Blockchain & Digital Asset

It is worthy to note that the private/public key pairs generated for a blockchain could be used in another blockchains sharing the same key length, encoding, digital signature and hash algorithms.

As Ethereum, Polygon, Arbitrum, and Optimism use the same wallet address encoding format, digital signature and hash algorithm, you can use the same keys and wallet for these blockchains.

5.3. Differences between native cryptocurrency and ERC tokens?

Native cryptocurrency is the native asset of a blockchain. It is created by mining/validating and used to pay for transaction fees and gas fees, and it can also be used as a store of value or traded on exchanges.

ERC tokens are tokens that are created on the Ethereum blockchain via smart contracts. They can be used for a variety of purposes, such as representing digital assets, creating new applications, or used to facilitate payments.

Here is a table that summarizes the key differences between native cryptocurrency and ERC tokens:

	Native Crypto	ERC Tokens
Examples	Bitcoin (BTC), Ethereum (ETH), Polygon (MATIC), Avalanche (AVAX), Cardano (ADA), Litecoin (LTC), Dogecoin (DOGE)	USD Coin (USDC), Tether (USDT), Shiba Inu (SHIB), Uniswap (UNI), NFT
Created by	Created every time a block is mined / validated as the Block reward. The block reward is embedded within the Blockchain protocol; the amount is fixed.	Created by smart contracts. There is no limit on the number of smart contracts that could be created while each smart contract can create up to 1.158 x 10^77 ERC tokens.
Used for	Store of "value", trading, transaction fee and gas fee.	Store of "value" and trading
Uniqueness	There is only 1 native crypto for each blockchain	Can have unlimited ERC tokens in each blockchain. Can even have ERC tokens having the same name but each smart contract can only have 1 address. For example, there could be a DSGD ERC token in address 0xABCDE.... and another DSGD ERC token in address 0XEFABC123456. They could be created by different parties for different usage which may not be related to each other.
How to differentiate them?	Does not have an "address"	Has a smart contract address for ERC token
Max supply	21 mil for BTC(hardcoded in the Bitcoin protocol), infinite for ETH	Limited by the variable size recorded in the smart contract. Approx 1.158 x 10^77
Approx 1.158 x 10^77	There is only 1 native crypto for each blockchain	Can have unlimited ERC tokens in each blockchain. Can even have ERC tokens having the same name but each smart contract can only have 1 address.
Can be destroyed?	No, see below for explanation	No, see below for explanation

Source: UOB Blockchain & Digital Asset

5.4. Can digital assets such as cryptocurrencies or blockchain tokens be destroyed?

To understand that, you need to know how the cryptos are created. Cryptos are created "out of thin air" during every block creation process (refer to the section 5,1). When a block is created, the miner or the validator gets the block reward by adding the first transaction in the block to send the block reward to his own wallet address. So, this is how crypto is created.

Let's go back to discuss how a crypto can be destroyed. The answer is that cryptos cannot be destroyed because they exist only as entries on the blockchain ledger.

However, you can render them unusable by losing the private key of your wallet or by sending them to a "burn address" where there is no private key to access those cryptos; essentially sending them to oblivion, removing from circulation. While these methods are effective, they do not really destroy the cryptos. You can still see them in the blockchain, it's just that no one can spend them.

5.5. Why are blockchain assets (such as native crypto or tokens) unrecoverable if they are sent to a random wallet address?

Recall that to control any blockchain asset, you need to have the private key of that wallet address. Say if you accidentally sent your asset to a random address 0xaCE7656EC7ab88b098defB751B7401B5f6d8922E, if you want to recover it, you need to have the corresponding private key for this wallet address. As we know, there is no way to derive the private key address from the wallet address, hence the asset is considered lost forever.

You may ask, is it possible this random wallet address is owned by someone else? The answer is that is practically impossible because there is approximately 2^160 or 1.46 x 10^48 unique wallet addresses an absolutely mind-boggling number. To put thing into perspective, the chances of winning first prize in Singapore lottery (49 choose 6) is only 1 in 14 million or 1.4 x 10^7; thus, it is almost impossible for you to stumble across an address already in use by someone else.

Therefore, your private key is safe if it is properly stored, because there is no way a hacker can reverse engineer and derive your private key from your wallet address (refer to section 3.6).

You can store your private key using a reputable blockchain wallet app. Make sure you install anti-virus software and do not download unlicensed software as it may come with viruses or trojan horses that can steal your wallet password and your private key.

6 Security vulnerabilities of blockchain

While blockchains are known for being secure, it is not entirely without vulnerabilities. We shall discuss some of the security concerns associated with the blockchain technology.

6.1. The 51% attack – attacking the consensus mechanism

A 51% attack occurs when a single entity or group of entities gains control over the majority of a blockchain's mining power. This enables them to manipulate transactions and disrupt the network's integrity. The 51% attack is on the consensus mechanism i.e the PoW or PoS. This is achieved by having more computation power or stakes to create a longer chain with false transactions to overrun the legitimate chain.

Below shows how difficult it is to launch a 51% attack on the public Bitcoin blockchain:

1. To dominate the Bitcoin network and force a change to the ledger, you would need to control at least 51% of the network's hash rate. This means that you would need to control more than half of the computing power that is used to secure the network.

2. The Hash rate is the measure of the computational power in a Proof-of-Work (PoW) crypto network. As of Jun 2023, the Bitcoin Hash Rate is 353 ExaHash/s. That is 353 quintillion or 353 x 10^18 hash computations per second.

3. Doing a quick search on websites for mining rigs, one can find the average price of the most powerful rig listed can achieve 255 TeraHash/s (255 trillion hash computations per second) costs approximately USD4150+ and requires 5304W of energy.

   Using that as reference, to achieve 353EH/s in order to gain 50% computation power on the Bitcoin network, we will need at least 1,380k rigs costing USD5.73bil. Additional investments will include electricity and datacenter costs.

4. Even if the attacker is able to achieve this, it is unlikely that he will be able to maintain control of the network for long. Other miners would quickly notice that he is trying to manipulate the network and would increase their hash rate in order to take control back.

5. Even if the attacker finally managed to beat all other parties and gain 51%, it will destabilize the system and cause all the participants to leave the network because investors will lose faith in the network once someone has gained power to manipulate the network.

For Proof-of-Stake (PoS) Ethereum network, validators need to stake their crypto in order to get their chance to validate a block, the more stake they put in the higher the chance. As of Sep 2023, there are some 25.3M ETH staked - so to gain majority, an attacker needs to stake at least the same amount of ETH which costs approximately USD 41bil based on ETH price of USD1,630.

As you can see to launch a 51% attack on the public Bitcoin and Ethereum blockchains is prohibitively expensive and hence this is the trust you can derive from the public blockchains.

6.2. Quantum computing – attacking the digital signature

Recall from section 3.6, that there is no way to reverse engineer to derive the private key from the wallet address or public key generated using digital signature algorithm. ECDSA, the most commonly used digital signature algorithm for blockchain, relies on integer factorization and discrete logarithm which are difficult to solve. With Shor's algorithm it is possible to break ECDSA using quantum computers. The solution is to migrate to quantum-safe digital signature algorithm such as XMSS when the quantum computers become powerful enough to break the digital signatures.

Quantum computers pose a potential threat to blockchain security by potentially breaking the encryption algorithms used to secure transactions. This highlights the need for ongoing research and development in quantum-resistant cryptography.

6.3. Is it possible to claw back stolen cryptocurrencies or tokens?

Transactions on the blockchain comprises source and recipient wallet addresses, the amount to transfer the sender's private key signature. Once a transaction is written on the blockchain it is immutable meaning it is permanent and cannot be reversed. The only way to recover stolen funds is to ask the recipient to send them back.

One drastic method to recover stolen fund is to rollback the entire blockchain to remove those offending transactions. This may be possible on a private chain controlled by a few entities, but it is very difficult to do on a public blockchain. Moreover, this may not solve the issue because if the criminal has already stolen the private keys of the wallet, they can simply steal the funds again after the rollback. This is not recommended unless the loss is so significant such as in the case of the 2016 DAO hack, which caused the Ethereum blockchain to hard fork to 2 distinct chains: Ethereum (with the invested money transferred to a new DAO without the software bug and returned to the investors) and Ethereum Classic (with the old DAO and funds stolen by the hacker).

6.4. Is it possible to add a backdoor to a public blockchain to claw back stolen digital assets such as cryptocurrencies and tokens?

There was a proposal to add a backdoor to the public blockchain for law enforcement to claw back stolen cryptos or tokens.

It may be possible via changing the validation mechanism (in section 3.3). In addition to validating transactions are signed by the corresponding private key for that wallet, the amended protocol can also accept signatures signed by a whitelist of law enforcement private keys i.e. "Master" keys from the law enforcement's wallets.

Proposed steps:

- Per current protocol, the miner/validator will check the transaction signature against the public key of that sender's wallet during mining/validation.
- If that fails, it means the signature wasn't not created by the private key from the sender's wallet and this transaction will be discarded.
- With this new enhancement, when the first validation fails, the additional step is to check the signature against the public key of law enforcement's wallet. If the signature passed, this means the transaction originates from the law enforcement and the transaction will be accepted.

This approach should work on both PoW and PoS blockchains. To implement this, the core consensus of the blockchain must be amended to incorporate this major update.

Drawback of this approach is, anyone holding those Master keys will have absolute power on the blockchain to move assets from any wallet. The existence of such Master keys will cause the public to lose faith in that blockchain.

7 Applications in banking

Blockchain technology has the potential to reshape banking as we know it. In this section, we will explore various applications of blockchain in the financial sector.

7.1. Central Bank Digital Currency (CBDC)

CBDC is a digital version of a country's currency that's issued and controlled by the central bank that is intended to be legal tender. A CBDC's value is equivalent to the country's fiat and is regulated and backed by the central bank. Unlike public cryptocurrencies such as Bitcoin or Ethereum, which are decentralized, CBDCs are centralized and maintained by the central bank.

There are 3 types of CBDC:

- Retail CBDC: for businesses and general public to make payment to other people, in store and online. Like fiat, CBDC could be used for investment, saving and earn interests.
- Wholesale CBDC: for financial institutions to settle large and high-value payments.
- Cross-border CBDC: for remittance using wholesale CBDC

MAS is leading the industry with Project Orchid, a multi-year, multi-phase exploratory project, examining the various design and technical aspects pertinent to digital Singapore dollar, from its functionalities to its interaction with existing payment infrastructures. Though MAS has assessed that there is no urgent need for a retail CBDC in Singapore at this point in time, MAS seeks to facilitate ongoing learning and advance the financial infrastructure in Singapore.

Objectives of the project includes:

- Develop the technology infrastructure and technical competencies necessary for digital Singapore dollar (such as Central Bank Digital Currencies and tokenised bank deposits)
- Explore potential use cases for a programmable money in Singapore

The first phase of the project aims to uncover potential use cases for a programmable digital SGD and the infrastructure required. Subsequent phases of Project Orchid will investigate the optimal ledger technology as well as its integration to the existing financial market infrastructure[1].

1 https://www.mas.gov.sg/schemes-and-initiatives/project-orchid

7.2. Security tokenisation

As mentioned earlier, security tokenisation is the process of converting items of value into blockchain tokens.

MAS is leading the financial industry in Singapore in Project Guardian to tokenise traditional securities. UOB is collaborating with HSBC, Marketnode (a joint venture between Temasek and SGX) and ADDX (a licensed digital exchange) to tokenise short term Structured Notes to distribute to UOB private bank clients.

In June 2023, HSBC, Marketnode and UOB have successfully concluded a technical pilot on the issuance and distribution of a digitally native structured product. The pilot successfully demonstrated the potential for lower issuance and servicing costs, reduced issuance and settlement times, deeper customisability, and broader distribution for participants within the structured product chain.

Looking ahead, these FIs aims to embark on further pilot on the issuance of multi-currency and debt/equity linked structured notes under HSBC's existing issuance programme, tokenised by Marketnode's multi-asset issuance platform, and distributed by UOB for its wealth management activities[1].

1 https://www.mas.gov.sg/schemes-and-initiatives/project-guardian

7.3. Identity verification, verified credentials and KYC

Know Your Customer (KYC) processes are integral to the banking industry. However, the traditional KYC process involves collecting and verifying customer information repeatedly, leading to inefficiencies and security risks. Blockchain can enhance identity verification and improve security.

Blockchain transforms identity verification:

- Immutable Records: Once identity information is recorded on the blockchain, it cannot be altered or deleted without the owner's consent, reducing the risk of identity theft and fraud.
- Permissioned Access: Individuals have control over who can access their identity data, ensuring privacy and compliance with data protection regulations.
- Streamlined Verification: Banks can verify customer identities quickly by accessing blockchain records, eliminating the need for redundant verification processes.

One use case of identity verification is Verifiable Credential (VC). VC is a digital document containing the credentials of the subject which is digitally signed by a trusted or reputable issuer such as the Immigration Department. Examples of VC include digital identity cards, digital birth certificates, and digital education certificates. When a person displays the VC, the verifier checks the VC content and the digital signature. These are verified against the public key of the issuer which is widely available to confirm the authenticity.

Websites also use digital certificates for HTTPS connection. A trusted certificate authority (CA) assures users the website they are visiting is legit, like the green checkmark on Twitter and Whatspp.

7.4. Supply chain finance

Blockchain's transparency and traceability make it a valuable tool in supply chain finance. Supply chain finance involves providing funding to businesses based on the value of goods in transit. Blockchain can optimize this process by providing real-time visibility into the movement of goods.

Blockchain can also be used to digitalise trade documents. Singapore's Infocomm Media Development Authority (IMDA) is working with the industry using NFT (Non-fungible token) to store the hash of trade documents.

Blockchain offers critical benefits to supply chain finance:

- Reduced Risk: Banks can monitor the progress of shipments and verify the authenticity of goods, reducing the risk associated with supply chain financing.
- Faster Transactions: Automated smart contracts can trigger financing when predefined milestones are reached, accelerating the financing process.
- Increased Transparency: All stakeholders in the supply chain, including banks, can access real-time data, reducing disputes and fraud.

Blockchain is transforming supply chain finance by reducing risk, accelerating transactions, and increasing transparency.

8 Benefits and challenges of blockchain

Blockchain technology offers several potential benefits to the banking industry, but it also presents challenges that must be addressed for widespread adoption.

Potential benefits of Blockchain:

- Single source of truth: On the blockchain, each participant receives an identical copy of ledger. This reduces the need for reconciliation among participants, and thus it was predicted blockchain will be widely adopted by back offices within a decade.
- Decentralization: A decentralized network is less susceptible to single points of failure. Even if some nodes fail or are compromised, the network can continue to operate.
- Efficiency: Blockchain may help remove intermediaries and automate transactions using smart contracts, more details below.
- Transparency: All transactions on the blockchain are visible to participants and all participants hold the full transaction ledger. This transparency enables traceability and auditability of the transactions.
- Security and Trust: Blockchain uses digital signature algorithm to ensure transactions originate from the rightful owner and consensus mechanisms to provide strong security features. Participants in a blockchain network develop trust by using these security measures in addition to the transparency, traceability, and auditability that the blockchain provides.
- Immutability: Blockchain uses cryptographic techniques(hashing) to secure transactions and data. This makes it highly secure and resistant to tampering.
- Atomic Settlement: Blockchain makes it possible to do atomic settlement, delivery vs payment, when both legs of the transaction involve blockchain assets such as security tokens and cryptos.

Some key challenges include:

- Complexity: Blockchain is complex and can be difficult to understand for most people. This limits business and corporate adoption of blockchain solutions.
- Keys handling: Blockchains are decentralized, meaning that there is no central authority to manage user accounts and funds. This means that users are responsible for their own private keys, which are used to access and spend their funds. If a user loses their private key, or if it is stolen, they could lose all of their funds which is may not be recoverable.
- Scalability: Scaling blockchain networks to handle higher transaction volumes becomes essential as they expand.
- Interoperability: Different blockchain networks often use different protocols making it difficult to communicate and move data between different blockchains. More information can be found below.
- Security Threats: Blockchain may become a target for more complex cyberattacks as it gets more widely used.

8.1. The potential for efficiency

One of the primary benefits of blockchain in banking is the potential for increased efficiency. Traditional banking processes often involve manual tasks, intermediaries, and multiple reconciliations. Blockchain can streamline these processes, leading to cost savings and faster transactions.

How blockchain translates to real efficiency gains:

- Reduced Settlement Times: In one of the Project Guardian tech pilots conducted, the over-the-counter settlement of the structured note transaction has been reduced from 14 to 5 days. Stock exchanges and clearinghouses can use blockchain to settle trades in real-time, reducing settlement times from days to minutes.
- Lower Costs: The elimination of intermediaries and the automation of processes can significantly reduce operational costs.
- Enhanced Accuracy: Blockchain's immutable ledger reduces the risk of errors, fraud, and data inconsistencies removing the need for data recon in the process.

8.2. Regulatory hurdles

While blockchain technology has the potential to transform the banking industry, it also raises regulatory questions and concerns. Regulators must strike a balance between fostering innovation and ensuring compliance with existing financial laws.

- AML and KYC Compliance: Blockchains are often used to make anonymous transactions, which raises concerns about their use for money laundering and other criminal activities. Financial institutions using blockchain must adhere to anti-money laundering (AML) and KYC regulations to prevent illicit activities.
- Consumer Protection: Regulators must protect consumers from fraud and ensure that blockchain-based financial products are transparent and secure. In Singapore, the central bank has put up measures such as banning advertisements and crypto machines to protect the retail investors from speculating in cryptos.
- Taxation: Taxation rules for cryptos and blockchain-based assets need to be defined clearly.

8.3. What use cases are not suitable for blockchain?

Blockchain is a powerful technology with many uses, but it is not suitable for all use cases. Some use cases that are not suitable for blockchain include:

- High performance or low latency: Blockchain transactions can be slow and expensive, so blockchain is not suitable for use cases that require high performance, low latency or fast confirmation. For example, blockchain is not suitable for high frequency trading, streaming video or making real-time payments (recall that you may need several blocks to be mined, up to couple of minutes, to achieve payment finality).
- Privacy: Public blockchains are transparent, so all data on the blockchain is visible to everyone unless they are encrypted before recording on the blockchain. This is not suitable for use cases that require privacy, such as storing healthcare records or classified government information.
- Small Data Storage: Storing very small amounts of data, such as a few kilobytes, on a blockchain can be inefficient and costly compared to traditional databases.

Overall, blockchain is a powerful technology with a wide range of potential applications. However, it is important to carefully consider the requirements of a use case before deciding whether to use blockchain.

8.4. Blockchain interoperability

Blockchain interoperability refers to the ability of blockchains to communicate with other blockchains or move assets across them. Interoperability has been one of the common pain points for users.

8.4.1. Blockchain bridges

A blockchain bridge is one of the solutions to address interoperability across blockchains. It can be used to bring an asset from a blockchain to another. To do so, you can setup a smart contract to collect the asset from the source chain and then mint a "wrapped" version of the asset of equivalent quantity in the destination chain and send to your wallet there.

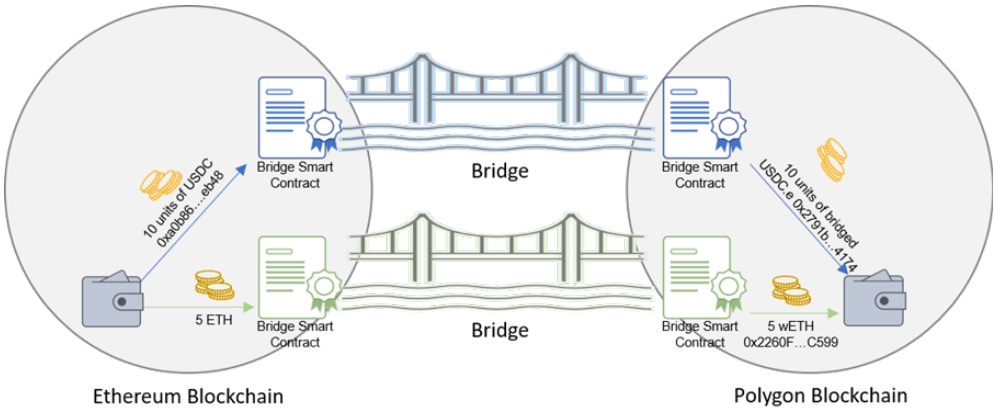
Strictly speaking the asset is locked up in the smart contract on the source blockchain and not transferred to the destination blockchain. This is like the ADR (American Depository Receipt) or VIE (Variable Interest Entity) structure for availing shares in another exchange.

Do be aware the bridged smart contract address in the destination blockchain may be different from the source chain.

For example, the USDC stable coin is a ERC-20 token created on the Ethereum blockchain with smart contract address 0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48. After bridging to the Polygon blockchain, the bridged token has a new address 0x2791bca1f2de4661ed88a30c99A7a9449aa84174. The stable coin issuer could name the bridged token the same as the original token but they appended ".e" and named it USDC.e to indicate this token is bridged from Ethereum.

Similarly, a bridge could be created for sending ETH to Polygon blockchain, where the wallet on the destination blockchain receives a "wrapped" ETH in the form of a blockchain token.

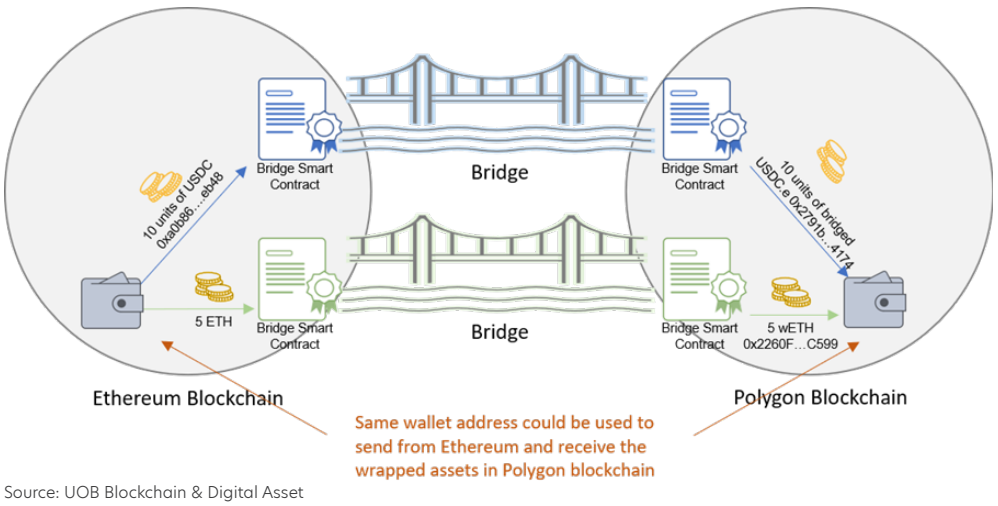
Diagram 8.4a - Bridge linking 2 blockchains to facilitate asset "transfer" between them



Source: UOB Blockchain & Digital Asset

Recall in section 5.2 that the wallet address encoding, digital signature and hash algorithm for Ethereum and Polygon are the same and hence the *keys and wallet address* in Ethereum can be used for Polygon as well. Therefore, when sending the tokens and ETH across to Polygon, you can use the same wallet address to receive the "incoming" bridged USDC.e and wrapped ETH.

Diagram 8.4b - Same wallet address can be used on both Ethereum and Polygon blockchains



Source: UOB Blockchain & Digital Asset

8.4.2. Off-chain connectivity

Besides building bridges to move blockchain assets across chains, there is another way to assess those assets by connecting your wallet to the desired blockchain directly rather than via a bridge.

With this, you will be able to access the assets on other blockchains from your wallet. This is equivalent to signing up with a broker that has connectivity to both the US and Singapore markets, allowing you to trade Apple and UOB shares. You do not need to bring the Apple shares to SGX (Singapore Stock Exchange) to trade them.

9 The road ahead

Blockchain technology is still evolving, and its integration into the banking sector is an ongoing process. In this section, we will explore the path ahead for blockchain in banking.

9.1. Deploying blockchain solutions

The transition to blockchain is not without its complexities. Banks have invested heavily in existing systems and integrating blockchain with legacy infrastructure requires careful planning and execution.

A smooth transition is key:

- Hybrid Solutions: Banks can adopt a phased approach, gradually integrating blockchain into existing processes while maintaining legacy systems.
- Collaboration: Collaborative efforts with blockchain partners can facilitate a smoother transition. The bank has worked with ADDX and Marketnode to tokenise bond issuance.
- Education and Training: Bank staff must be trained in blockchain technology to ensure effective implementation. On this end, the bank's blockchain team has been actively conducting Blockchain 101 trainings to various functions in the bank to bring people onboard with the vision.

9.2. Collaboration with the central bank and the industry

As blockchain technology continues to evolve, we can anticipate several transformative developments in the banking industry. Various functions within the bank are participating in high profile projects with MAS and other banks to ensure we are on top of the blockchain wave. This collaboration drive innovation and technology knowhow which will benefit the bank as a whole.

10 Conclusion

In this report, we have explored the blockchain technology and its potential usage in banking and finance and other industries.

Blockchain is a powerful technology that began as the technology behind Bitcoin, but now has many other uses, such as central bank digital currencies (CBDCs), security tokenization, cross-border payments, and identity management.

Bank and financial institutions will need to adapt to this landscape to stay competitive. Blockchain has the potential to revolutionize many aspects of the digital world, and its journey is just beginning.

The Team

Morgan Chia
FVP, Blockchain & Digital Assets
Chia.Morgan@uobgroup.com

Heng Koon How, CAIA
Head of Markets Strategy
Heng.KoonHow@uobgroup.com

Tan Lena
Business Data Designer
Lena.Tan@uobgroup.com

Right By You

Right By You

Head Office
80 Raffles Place
UOB Plaza
Singapore 048624
Telephone: (65) 6533 9898
Facsimile: (65) 6534 2334

www.uobgroup.com