UNIVERSITY of NICOSIA

MSc in Digital Currency

DFIN-511: Introduction to Digital Currencies

Session 6
Alternative uses of the blockchain

DFIN-511: Introduction to Digital Currencies

UNIVERSITY of
NICOSIA

Objectives of Session 6

- Understand the original purpose of Bitcoin's blockchain
- Explore some alternative uses of the blockchain (e.g. colored coins, smart contracts, etc.)
- Glimpse at possible future uses of the blockchain

Before we begin with this session, we need to clarify that boundaries between concepts are not always 100% clear in an area of constant innovation. Being able to understand each innovation is more important than agreeing what label should be given to its category.

Bitcoin is at its core, a technology that enables a series of achievements that were not possible before, and not just "magic internet money". Decentralized consensus can create more robust systems in a multitude of ownership or attestation related roles. Currency is the first "app" of this technology and definitely not the last. In this session we aim to introduce a few different potential applications.

Agenda

1. Purpose of Bitcoin’s blockchain
2. Alternative uses of the blockchain
3. Future of the blockchain
4. Conclusions
5. Further Reading

1. Purpose of Bitcoin’s blockchain

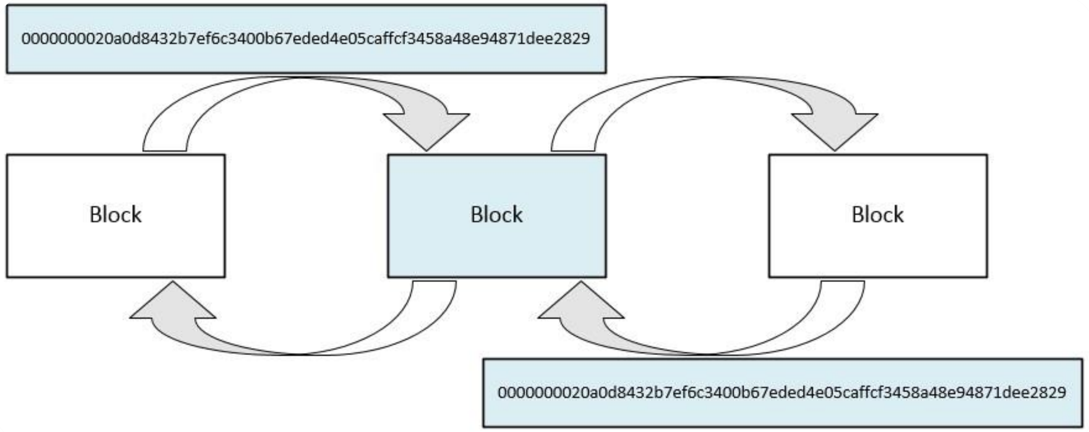
Purpose of Bitcoin’s blockchain

The blockchain is the public record of all transactions and it is shared and is collaboratively maintained through global consensus by all nodes participating in the Bitcoin network. In Bitcoin, the blockchain specifically serves a dual purpose, as it is used to:

- Prove the permanence of all transactions (e.g. against modifications)
- Prevent double-spending (i.e. Prevent malicious users from spending their bitcoins to two different recipients at the same time)

As we have seen, each block in the Blockchain contains:

- A block header, and
- Transaction data for all transactions


0000000020a0d8432b7ef6c3400b67eded4e05caffcf3458a48e94871dee2829
Block
Block
Block
0000000020a0d8432b7ef6c3400b67eded4e05caffcf3458a48e94871dee2829

Source: www.bitparticle.com

All blocks in the blockchain are chained together via header hashes; as a result, the name "blockchain" seems to be more than appropriate.

2. Alternative uses of the blockchain

Alternative uses of the blockchain

As we have already discussed in session 2, Bitcoin has provided a practical solution to the Byzantine General's Problem through its use of the blockchain. Since BGP is a general problem in distributed systems, the same concept can be employed for other purposes.

We will explore the following alternative uses of the blockchain:

- Meta-coins
- Asset Registration
- Colored Coins
- Mastercoin
- Attestation
- Smart Contracts
- Smart Property
- Financial Contracts and Instruments
- Political Speech

Source: gigaom.com

Meta-coins – Zerocoin

- Meta-coins utilize the existing Bitcoin blockchain infrastructure to extend Bitcoin with further features through meta-data. Meta-coins differ from Alt-coins (to be studied in Session 7) in that the latter are based on the Bitcoin implementation, yet differ in many details. Like colored coins, meta-coins provide additional functionality on top of the blockchain.

- A notable example of a meta-coin is Zerocoin, which aims to further enhance the privacy of Bitcoin payments by obfuscating the deduction of user identities from their payment patterns/habits.

- Zerocoin achieves its goal by employing zero-knowledge mathematical proofs (see page 12). Unfortunately, Zerocoin had the disadvantage that it introduced additional bloat and delay to the existing Bitcoin network, as it requires storing its proofs in the blockchain, and due to the significant time it takes for nodes to verify the proofs.

Source: Wikimedia Foundation

Meta-coins – Zerocash

Due to the limitations of Zerocoin, its original authors created an improved implementation called “Zerocash” (an Alt-coin). Zerocash addresses Zerocoin’s performance and bloat issues and provides further functionality, such as:

- Obfuscating payment history
  (e.g. payment destinations, amounts)
- Zerocoin hides a payment's origin, but not its destination or amount

Zerocash

Source: zerocash-project.org

While some users may currently work around some of Bitcoin’s privacy issues by employing multiple addresses for separate payments, transaction graph analyses are still possible.

- The authors of Zerocash point out that Bitcoin currently exhibits the following privacy concerns:
- It is *less* private than a traditional bank account (due to its public ledger)
- It makes your transaction history public for anyone to see (i.e. user identity can be deduced)
- It introduces privacy-intrusion concerns (e.g. data-mining by third parties, etc.)

Over the next page we will see briefly how Zerocash works.

Meta-coins – Zerocash in detail

According to its protocol specification, Zerocash:

- Creates a separate anonymous currency called “zerocoins”, whereby non-anonymous bitcoins (referred to as “basecoins”) are the base currency.
- Dictates a different method of Bitcoin payment transaction assembly and verification.
- Extends Bitcoin with two new types of transactions:
  - **Mint transactions** – used to convert existing bitcoins to the equivalent zerocoins.
  - **Pour transactions** – which enable anonymous/private payments by using existing user coins to produce new coins, using zero-knowledge proofs.

The basis of Mint transactions is a “cryptographic commitment” (see next), which is itself generated using the SHA-256 hash function. This commitment is based on the coin’s value, a unique serial number, and the owner’s address. While these data are protected by the commitment, any user can later demonstrate ownership of the commitment through its de-committed values.

Meta-coins – Zerocash in detail

A "cryptographic commitment" is a binding scheme enabling one party to commit to a value or statement, while keeping it a secret from any other parties. Later on, the original party has the ability to reveal (or de-commit from) the committed value, which can then be verified by another party. Thus, a commitment scheme consists of two phases:

- **Commit phase** – whereby a party commits to a value that is unknown to any other parties
- **Reveal phase** – whereby the value is revealed and verified

An example of such a commitment would be:

1. Alice claims to Bob that she can predict next week's winning lottery numbers.
2. Alice commits by writing the winning numbers on a piece of paper, locking the paper in a safety box, and giving the box to Bob for safekeeping (Commit phase).
3. Finally, next week, Alice gives Bob the key to the safety box, so that Bob can verify that Alice's prediction was indeed correct (Reveal phase).

Zerocoin and Zerocash apply these principles in Mint transactions.

Zero-knowledge proofs

“Zero-knowledge proofs” allow one party (e.g. the sender) to prove to another (e.g. the receiver) that a given statement is true, while not providing any further information beyond the fact that the statement is true.

For performance reasons, Zerocash uses so-called “zero-knowledge Succinct Non-interactive ARguments of Knowledge” (or zk-SNARK), which are mathematical proofs that are short and easy to verify.

Zerocoin and Zerocash apply these principles in Pour transactions.

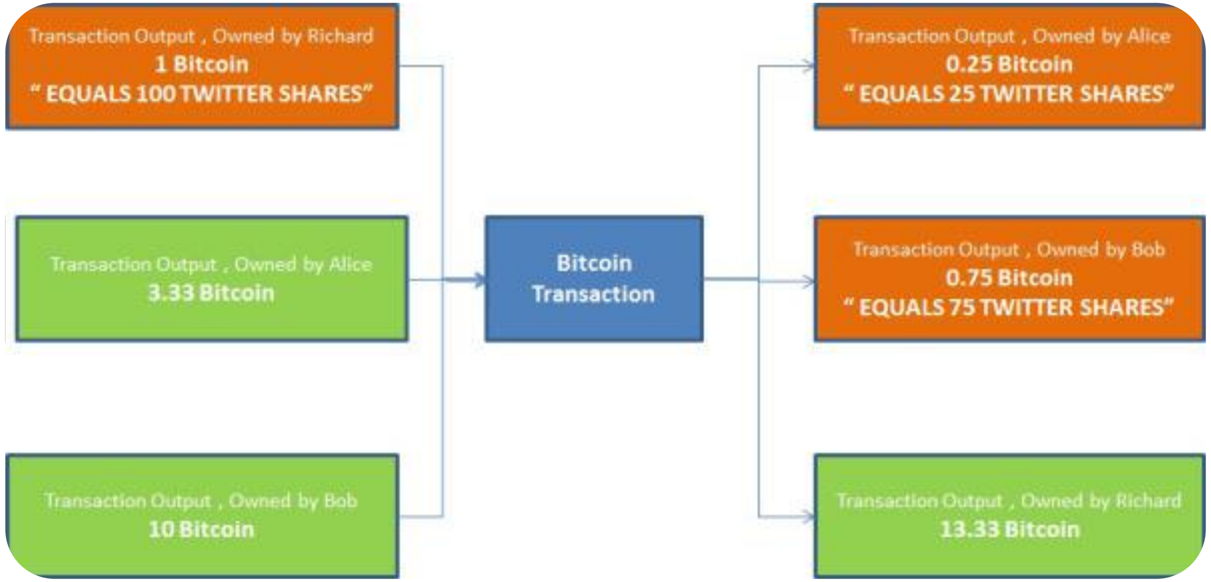
Zerocoin developer team and zk-SNARKs have since moved to work on a cryptocurrency named Zcash, aiming to solve fungibility issues in cryptocurrencies.

Asset registration

Global asset registration is another interesting use of the blockchain. For instance, a number of shares (i.e. assets) could be matched to their equivalent worth in bitcoins (e.g. 1,000 shares of XYZ company could be worth X bitcoins).

Two interesting meta-coin projects that aim to provide a consistent way of employing the blockchain to support, among other uses, global asset registration are:

- Colored coins (see next)
- Counterparty (see page 18)


Transaction Output , Owned by Richard
1 Bitcoin
" EQUALS 100 TWITTER SHARES"
Transaction Output , Owned by Alice
3.33 Bitcoin
Transaction Output , Owned by Bob
10 Bitcoin
Bitcoin Transaction
Transaction Output , Owned by Alice
0.25 Bitcoin
" EQUALS 25 TWITTER SHARES"
Transaction Output , Owned by Bob
0.75 Bitcoin
" EQUALS 75 TWITTER SHARES"
Transaction Output , Owned by Richard
13.33 Bitcoin

Source: gendal.wordpress.com

The US stock exchange NASDAQ, has begun experimenting with the using the blockchain to trade assets on it's pre-IPO arm, NASDAQ Private Markets.

Asset registration

What if the blockchain could be used to do more than exchanging money? Like for instance, one could also be able to issue shares and bonds, or create alternative currencies? The blockchain records an ownership state of an abstract value (unspent outputs). If a group agrees that a certain amount of these represent another value altogether, can they potentially use these "designated" bitcoins to transact in this value?

The **Colored coins** concept employs Bitcoin's existing blockchain Infrastructure to achieve these goals. Colored coins extend (or "color") bitcoins with further properties, effectively turning them into tokens which can be used to represent anything (e.g. specific coins that represent 1,000 shares of a company, or deposits of physical gold in one company's warehouse, and so on). Trading those specific coins is essentially trading the issued asset.

Source: coloredcoins.org

Colored coins work as an "overlay" network on top of the traditional Bitcoin infrastructure, as we will see over the next pages.

Colored coins – in detail

- *To create* a new color, a "genesis transaction" with specific rules for transaction inputs/outputs must be created. Specifically:

- Input rules:
  - **Non-reissuable colors**: In this case, inputs are ignored, and only outputs are considered.
  - **Reissuable colors**: In this case, only the first input is used, where the issuer sets it to a secure "issuing address" (responsible at most for 1 color). All other inputs are ignored.

- Output rules, consisting of a set of outputs, specifically:
  - Outputs used to send colored coins to their original owners
  - A data output (which among others, encodes the color)
  - "Change" outputs used to send any excess bitcoins back to their original owners

Colored coins – in detail

To *transfer* colored coins, a “transfer transaction” must be created, which follows a “tagging-based coloring” algorithm. The latter algorithm tags each input of a transaction based on its sequence number and uses this tag to determine which outputs the coins will go to.

The tagging algorithm provides several advantages, such as:

- Minimal per-transaction meta-data is stored
- Multi-color support (i.e. a transaction may contain bitcoins of many different colors, or asset types)
- No minimum sending amount is enforced (i.e. a transaction can send 1 color value if so desired)

Further details on the specific implementation of the “tagging-based coloring” algorithm are outside the scope of this Session.

Examples of Colored coins-enabled wallets include: Coinprism, ChromaWallet, and Coinspark. Check out the Colu platform for more.

Omni

The Omni project (formerly Mastercoin) was proposed to enable the existing Bitcoin network to be used as a “protocol layer” upon which further applications can be built, one of them being, for example, smart contracts. The “Mastercoin protocol” built upon Bitcoin has the following characteristics:

- Like Bitcoin’s “Genesis block”, Mastercoin’s starting point is an “Exodus address” (1EXoDusjGwvnjZUyKkxZ4UHEf77z6A5S4P), a bitcoin address from which the first mastercoins were generated in August 2013.
- Initial distribution of mastercoins occurred by sending bitcoins to the Exodus address (whereby 1 bitcoin was equivalent to 100 mastercoins).
- Updates to the protocol and it’s state can be found here: http://blog.omni.foundation/2015/05/19/state-of-the-layer-all-hands-may-19-2015/

Source: http://www.omnilayer.org/

Counterparty

"Counterparty" is an open-source meta-coin that extends Bitcoin to build a fully decentralized digital currency exchange service and among others, support asset registration, allow issuing of dividends and create contracts for difference.

Counterparty has the following features:

- It uses its own currency (called "XCP"), which is issued through "proof of burn" (see below)
- XCP is used to create new assets, derivatives, etc.
- XCP represents the value of the network

The "**proof of burn**" method employed by Counterparty works by sending bitcoins to a special address which renders the coins permanently unspendable. A notable asset issued on Counterparty are "LTBCoins" which can be used to pay contributors to the Let's Talk Bitcoin podcast show.

Developers from Counterparty were working with Overstock to create a system that could disintermediate the transfer of stocks and securities via the Counterparty protocol, but have left to form Symbiont.

Source: counterparty.io

Counterparty – in detail

Counterparty uses the existing Bitcoin blockchain to timestamp and publish its messages. Counterparty messages encode the following attributes:

- **Source address** – a bitcoin address which will send a quantity of assets
- **Destination address** – a bitcoin address which will receive a quantity of assets
- **Asset Quantity** – the quantity of specific assets to send from source to destination address
- **Miners' fee** – The fee paid to miners which will manage to add the transaction to a block
- **Data** field prefixed with the UTF-8 string "CNTRPRTY"

Some of the message types supported by Counterparty are:

- **Send** – used to send any quantity of an asset from a source to a destination address.
- **Order** – used to "exchange" a particular quantity of an asset for a quantity of another asset.
- **Issue** – used to issue an asset with a unique name and quantity.
- **Bet** – used to support wagers and contracts for difference.

Counterparty – in detail

Counterparty transactions are "overlayed" over Bitcoin transactions that have the following characteristics:

Inputs:

- Source of funds (i.e. source address)

Outputs:

- Destination output (i.e. destination address)
- One or more data outputs (used to store Counterparty-specific data)
- Optional "charge" outputs – generally ignored by Counterparty

Counterparty assets have the following properties:

- Assets may be divisible for up to 8 decimal places, or indivisible
- Assets may be "callable" (i.e. may be called back by their issuer after their call date)

The developers of counterparty have moved on, to creating a smart contract platform in the same manner that Ethereum has, with compatible contracts

Attestation

Attestation or *"Remote attestation"*, as it is commonly referred to, is the ability of authenticated nodes to monitor the behavior of another node participating in a distributed peer-to-peer network. If malicious or uncooperative behavior is detected by other nodes, the misbehaving node could be disconnected and/or banned from the network through global consensus.

Remote attestation is currently used for Bitcoin transactions and is achieved through global proof-of-work and the blockchain, as it is impossible for malicious users to introduce invalid transactions that will be included in the blockchain.

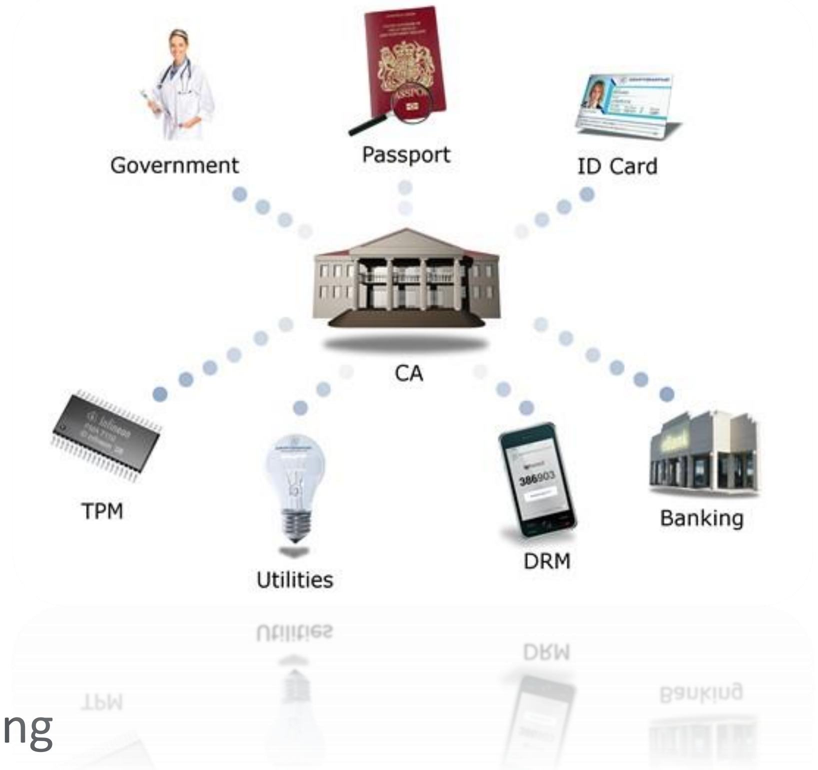
Source: bitcoinexaminer.org

As we will see over the next pages, remote attestation has further interesting applications, from building decentralized certificate authorities to supporting network-centric warfare.

Attestation and Certificate Authorities

A **Certificate Authority** (CA) is a centralized entity that is authorized and trusted to issue and certify ownership of digital certificates, based on the Principles of Public-Key Cryptography (see Session 3).

Digital certificates serve as proof of ownership of a Private-Public key pair by the subject identified on the Certificate (i.e. the owner). A trusted third party (i.e. the CA) certifies to any interested party that a digital certificate is indeed owned by the subject.

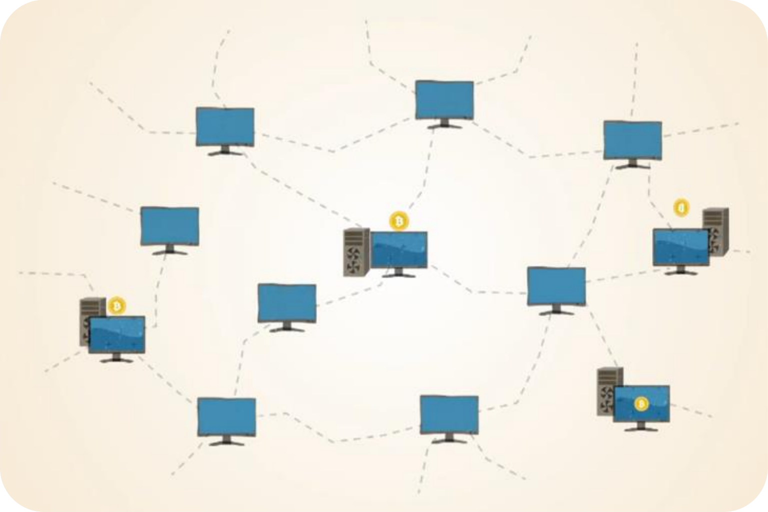


To perform this "*certification*", the CA uses the corresponding private key of the digital certificate. The most common example of a digital certificate are SSL certificates which are used for secure web browsing (e.g. on Bank websites, etc.).

Image Source: www.cryptomathic.com

Attestation and Certificate Authorities

But, what if we could build decentralized certificate authorities? By leveraging the concepts of "Decentralized Anonymous Attestation" (which provides a scheme for decentralized certification), zero-knowledge proofs, and the Bitcoin infrastructure, it is possible to create such a decentralized digital notary.



Source: www.straight.com

A notable example of a blockchain-based notary is the alt-coin Namecoin, which allows domain name registration and transfer in a completely decentralized manner (i.e. creating a decentralized DNS for .bit domains).

namecoin

Source: namecoin.info

Other notable examples are Blockstack the ProofOfExistence and BTProof digital notary projects, which allow users to certify any document by using the blockchain.

Proof of Existence

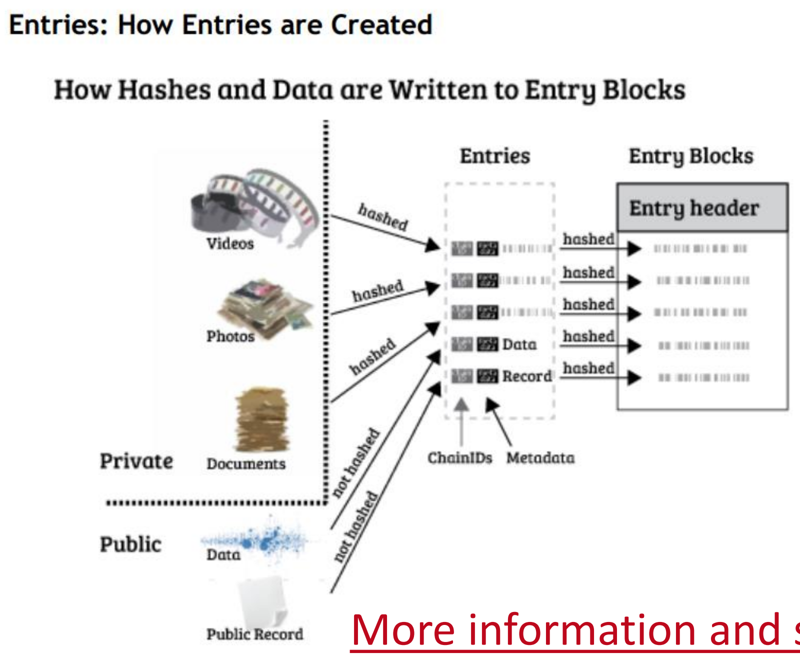
Proof of Existence is an open-source digital notary project which uses the blockchain to certify and prove that a document existed at a certain point in time. The original idea for this project was to protect against censorship and to be used by any party (e.g. a journalist) handling a "certified" document to verify its integrity. Proof of Existence has the following characteristics:

- The SHA-256 hash algorithm is used to generate a hash code for a given document
- A document's hash code is created client-side in the user's browser, and no document is uploaded on the blockchain
- A special transaction is created which embeds the document's SHA-256 hash code and the special marker "DOCPROOF"
- Any bitcoins associated with a Proof of Existence transaction are lost forever, due to the way transactions are created – thus transactions are rendered provably unspendable
- Once a transaction is confirmed, the document becomes permanently certified and proven to exist at least as early as the time the transaction was confirmed.

Data Layers on Top

Projects like Factom are trying to scale these principles to a complete system that can create a data layer over the Bitcoin blockchain, without adding bloat. They have since moved to their own blockchain which will tie with several other blockchains.

Since any amount of data can be turned into a unique hash, trees of these data, or combinations of hashes (merkle trees) can convey a very large amount of provably existing information. In this manner, Factom aims to create a separate, faster blockchain to store the hash data and occasionally insert hashes of these data in the Bitcoin blockchain (every ten minutes). Different from Bitcoin though, “miners” here, are tasked with both recording the entries and auditing the entries for validity (making sure the data matches the hash according to the application’s requirements and rulesets).



More information and source

Factom is working with Chinese digital notarization services to collaborate on a “smart cities” initiative.

Sidechains

Sidechains (or “pegged sidechains”) are a new concept which capitalizes on the innovations developed by Bitcoin to enable users to not only transfer bitcoins to individuals, addresses, and centralized services, but also to other blockchains. Sidechains will operate in a completely independent and isolated fashion - they are separate systems running in parallel to and taking advantage of the existing Bitcoin blockchain (referred to as “the parent chain”). As such, Sidechains do not introduce any side effects, like the probability of malicious or unintentional damage.

By using the existing Bitcoin architecture, currency, and the blockchain, Sidechains will provide the following benefits:

- Changes or fixes to Bitcoin can be introduced as part of a Sidechain, while preserving the original Bitcoin architecture (e.g. by introducing improved payer privacy)
- They minimize additional trust on the original Bitcoin model
- They allow creation of alternative chains with coins (or other assets, such as smart contracts) that derive their scarcity and supply from Bitcoin

Sidechains (cont)

A transfer of bitcoins (or assets) occurs as follows:

1. A transaction which locks the assets is created on the parent chain (the blockchain)
2. A transaction with inputs containing a cryptographic proof that the lock was done correctly is created on the sidechain; inputs are tagged with an asset type (e.g. genesis hash of the originating blockchain)

Note that no new assets are created, but simply, existing assets (or coins) are transferred.

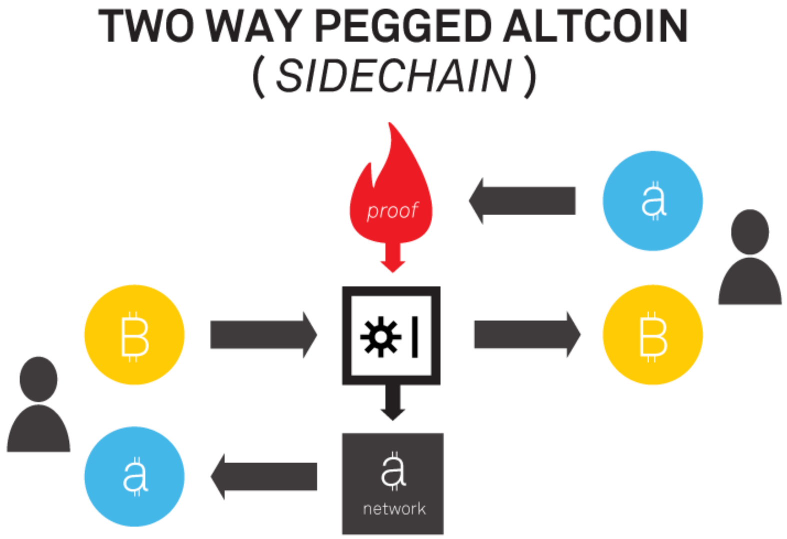
Let's delve into more details on Sidechains (see next page).

Sidechains – in detail

The technical basis of Sidechains is a “two-way peg”, whereby bitcoins can be transferred between any chain (i.e. parent and sidechains) at a deterministic (or fixed) exchange rate.

In addition, *“SPV (Simplified Payment Verification) proofs”* play a vital role in Sidechains. SPV proofs, allow verifiers to check thaat some amount of work has been committed to the existence of a special output, and to determine history by trusting that the longest blockchain is the correct longest blockchain.

You can read a more detailed post about Sidechains and a tutorial of Alpha Sidechain from one of our MSc graduates : here



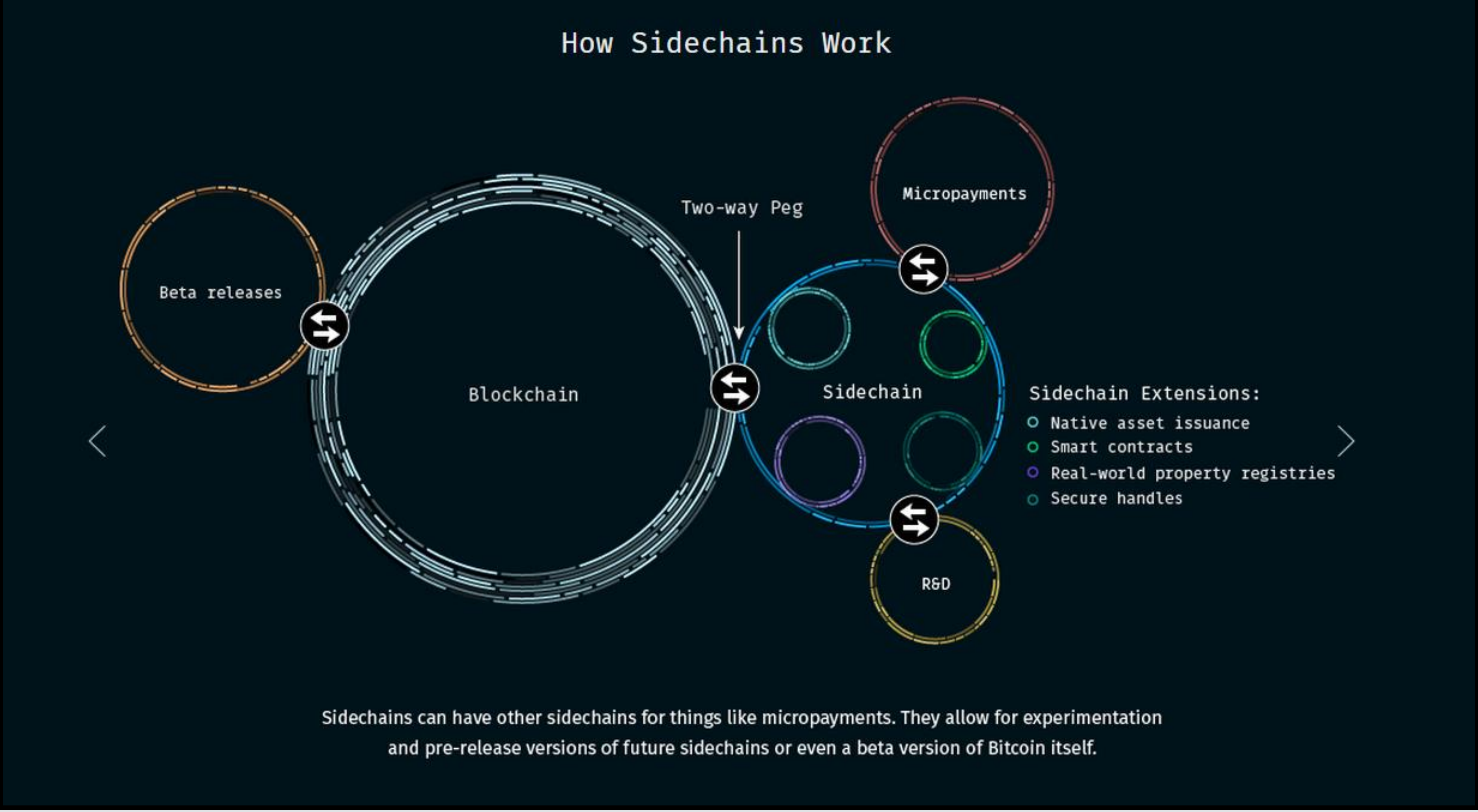
Source: cryptobizmagazine.com

Sidechains – in detail (cont)

There are two suggested models for Sidechains:

- **The *"Symmetric two-way peg"* model**, whereby the transfer mechanisms between any chain are the same and are based on SPV proofs. To transfer coins from the parent chain to a sidechain, the coins are sent to a special output on the parent chain that can only be unlocked by an SPV proof of possession on the sidechain. Furthermore, to synchronize the two chains, two waiting periods are used: (a) A *"confirmation period"* during which a coin remains locked on the parent chain before it can be transferred to the sidechain, and (b) A *"contest period"* during which a newly-transferred coin may not be spent on the sidechain.
- **The *"Asymmetric two-way peg"* model**, whereby each user can independently fully validate the state of the parent chain, without requiring SPV proofs, because all users are aware of the state of the parent chain.

In order to use Sidechains, special SPV-aware Bitcoin clients must first be developed. Spearheading the sidechains development is Blockstream, co-founded by Adam Back, the developer of Hashcash and the PoW principle that Bitcoin uses.

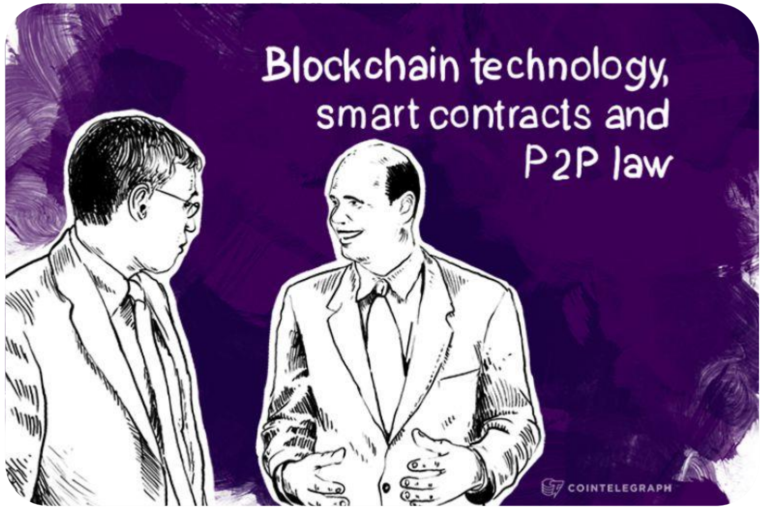


How Sidechains Work

Sidechains can have other sidechains for things like micropayments. They allow for experimentation and pre-release versions of future sidechains or even a beta version of Bitcoin itself.

Smart contracts

A **smart contract** is a contractual agreement that is implemented using software. Unlike a traditional contract where parties may seek remedial action through the legal system, a smart contract is self-enforced (possibly also self-executed), depending on whether specific conditions, that are monitored through software, are met. Due to the way the Bitcoin blockchain works, a "layer" can be built upon the existing infrastructure to support smart contracts.



Source: cointelegraph.com

Smart contracts may provide several benefits, for instance:

- They may automatically enforce power equality of all parties involved
- They protect an individual's rights by enforcing reasonable expectations for the signee
- They eliminate the possibility of any signatory defaulting on their obligations

Smart Property

Cryptographically protected physical ownership is commonplace in car immobilizers, phone PINs and access controls. Nick Szabo first suggested the idea of "smart property", as a means of cryptographically enforced ownership which is digitally transferable and which can be liable to an arbitrary set of contracts between the provider/owner and a customer/lender.

Much like a vending machine is a low risk automated contract with the vendor and the customer, the ownership transference that the blockchain provides, is a dis-intermediated way to enable digital contracts that depend on specific parameters. These could be used to "access control" services and actual property including cars, home keys, etc. Szabo uses this example in his paper:

1. *A lock to selectively let in the owner and exclude third parties;*
2. *A back door to let in the creditor;*
    - *(3a) Creditor back door switched on only upon non-payment for a certain period of time; and*
    - *(3b) The final electronic payment permanently switches off the back door.*

At the same time, these contracts could enable a multitude of novel loan and collateral applications, but also in comparison with oracles (independent digital arbitrators) a large array of property or financial instruments.

More information can be found at : https://en.bitcoin.it/wiki/Smart_Property

Financial Contracts and instruments

Most financial instruments are essentially a contract depending on the issuer and the set of rules or dependencies set by them. In regulated markets, the relevant security and exchange authorities monitor the compliance of the issuer and user of the contract/instrument to the rules set. What if we could replace these with math? Oracles, in this case, can act as the authority that determines compliance and adherence to the rules set.

Alice and Bob want to play rock, paper, scissors and the winner of 3 games wins a bet of 1mBTC.
In this case, an oracle can:

- hold both their funds in escrow until a winner is determined
- make sure that both players do not know what choice the other player commits to before they commit their own
- have a rule set that determines that rock beats scissors, paper beats rock, and scissors beat paper
- keep account of the winner of each game until someone wins three times
- pay out the full sum to the final winner of the 3 games

All these can be done objectively, transparently and without trust between Alice and Bob. The same can take place for more complicated financial instruments which rely on various external conditions.

Financial Contracts and instruments

Such external conditions could be nearly anything that can be quantified and digitized. The variable in this case would have to be retrieved from a source that is ideally verifiable and objective. Applications could include:

- Stock Market or Commodity Indices, taken from the exchanges themselves
- CFDs on weather variation in a city, taken from a central weather service
- The results of a soccer match
- The exchange rate of a currency at a point in time, as reported from Bloomberg or other service

Ethereum, and Augur which we will go into in Session 7, is poised to create a more robust contract base that could enable increasingly complex contracts.

At the same time, work is underway for a sidechain based protocol to offer equivalent and compatible smart contract functionality, called Rootstock. You can find a more detailed presentation and the roadmap of Rootstock in Sergio Lerner's talk in MIT here.

Political speech

BitCongress tried to implement a blockchain-based decentralized voting system, making use of some of these principles. BitCongress was itself based on Bitcoin, Counterparty, and Smart Contracts all operating under a voting and legislation tool called Axiomity.

Unfortunately there are no updates to the project since 2014.

Source: www.bitcongress.org (no longer available)

3. Future of the blockchain

What is the future of the blockchain?

As we have seen, the Bitcoin blockchain can be used for various purposes. Amongst other things, experts envision that the blockchain concept may be further used to keep:

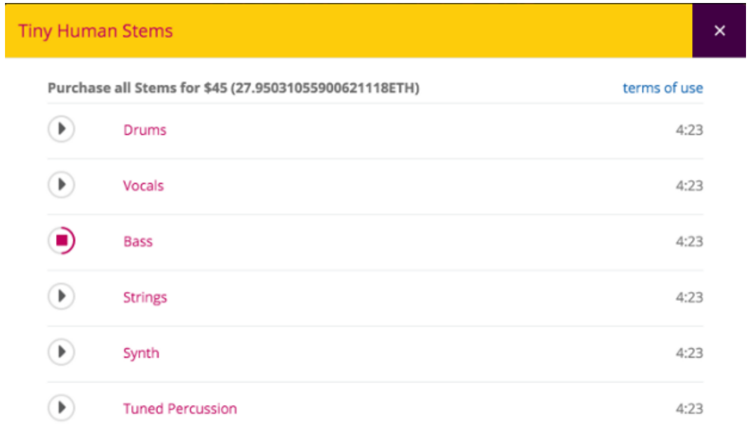
- **Public Records**, for instance:
  - Land titles (as is currently explored with Factom)
  - Criminal records
  - Voter records
  - Court records
- **Private Records**, for instance:
  - Wills (as explored by Third Key Solutions)
  - Trusts
- **Other uses**, for instance:
  - Certifications (like our university uses to store certificates of MOOC completion)
  - Medical records (like the MedVault project)

Music Industry - Prove Ownership and get Compensation via Blockchain

- Blockchain can store a cryptographic hash representing a new song's:
  - Artist
  - Composer
  - Title
  - Official Video/Audio
  - Any other relevant information
- Ownership is registered permanently therefore no need for record labels to have a share of the artist's work
- UjoMusic is based on the Ethereum blockchain and allows artists to publish their work immediately after uploading and manage licensing on their own terms.
- Users fund their accounts with Ether
- Smart Contracts technology allows artists to set automated payments to them based on licenses they design themselves
- https://ujomusic.com/

Imogen Heap's 'Tiny Human' is the only track available on Ujo as an initial attempt

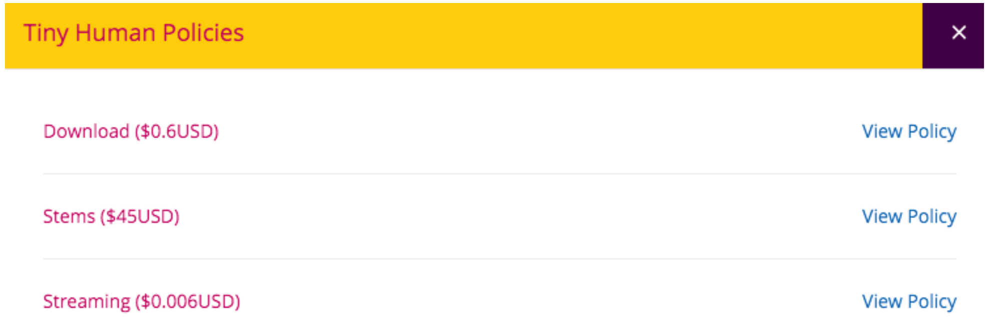
Ujo’s interface



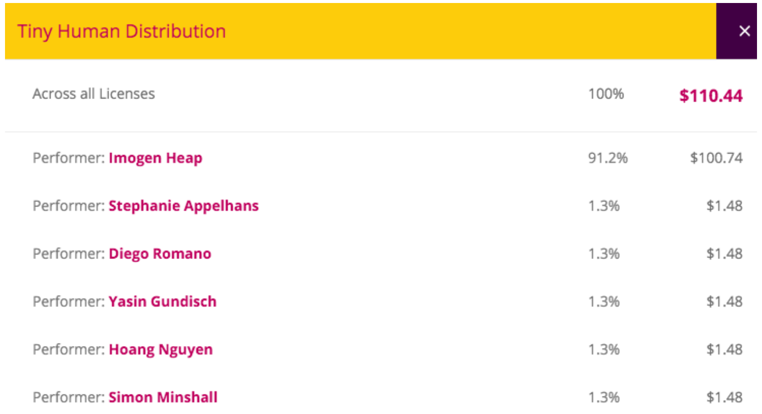
Purchase all Stems for $45 (27.95031055900621118ETH) terms of use

▶	Drums	4:23
▶	Vocals	4:23
■	Bass	4:23
▶	Strings	4:23
▶	Synth	4:23
▶	Tuned Percussion	4:23

Each stem of the song can be individually purchased

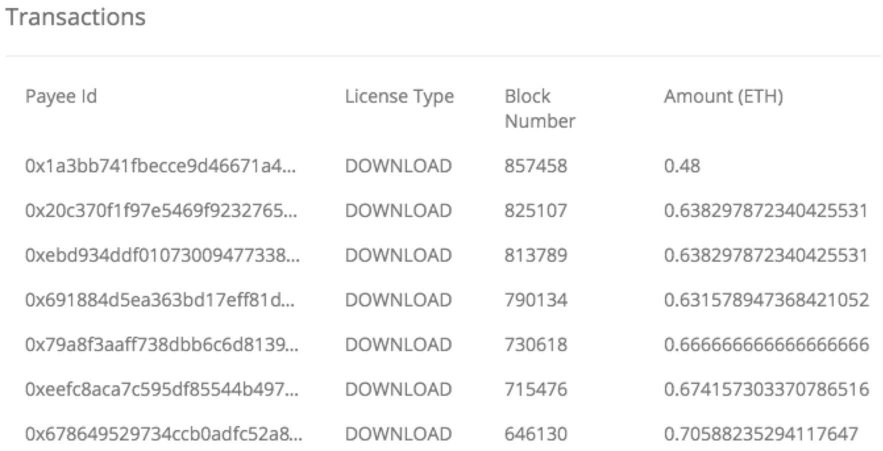


Download ($0.6USD)	View Policy
Stems ($45USD)	View Policy
Streaming ($0.006USD)	View Policy



Across all Licenses	100%	**$110.44**
Performer: **Imogen Heap**	91.2%	$100.74
Performer: **Stephanie Appelhans**	1.3%	$1.48
Performer: **Diego Romano**	1.3%	$1.48
Performer: **Yasin Gundisch**	1.3%	$1.48
Performer: **Hoang Nguyen**	1.3%	$1.48
Performer: **Simon Minshall**	1.3%	$1.48

Ownership and artist compensation is publicly visible in a “smart contract”


Transactions

Payee Id	License Type	Block Number	Amount (ETH)
0x1a3bb741fbecce9d46671a4...	DOWNLOAD	857458	0.48
0x20c370f1f97e5469f9232765...	DOWNLOAD	825107	0.638297872340425531
0xebd934ddf01073009477338...	DOWNLOAD	813789	0.638297872340425531
0x691884d5ea363bd17eff81d...	DOWNLOAD	790134	0.631578947368421052
0x79a8f3aaff738dbb6c6d8139...	DOWNLOAD	730618	0.666666666666666666
0xeefc8aca7c595df85544b497...	DOWNLOAD	715476	0.674157303370786516
0x678649529734ccb0adfc52a8...	DOWNLOAD	646130	0.70588235294117647

Every transaction is publicly available

Academic Certificates - Blockchain Solutions

- Ease of Publication & Distribution
- Independent validation
- Immutable Records - Digital fingerprints (hashes) of the individual certificates issued, are placed permanently in a blockchain transaction
- Reduced time to issue Certificates
- Costs of re-issuing certificates in the case the hard copy is lost are minimal
- Ease and instant authentication by interested parties (e.g. employers) even if the application used or the institution's website no longer exists. Operational costs minimized
- Universities and issuing authorities protect their brand names from being tarnished
- Employers can examine job applications more efficiently, ensuring that a candidate employee is presenting true information, without long waiting times or processing costs
- Our solution: http://block.co/our-approach/

Real Estate Management - Blockchain Solutions

- Authenticity: Property holders could digitally prove and transfer ownership immediately without the need to pay and wait for third-party verification

- Eliminate fraud and costs: Funds of sender and recipient can be logged using the multisig technology and be triggered upon smart contract execution i.e. transfer a land title when funds are received. A “digital ownership certificate” cannot be replicated, and can be linked to one property in the system, making selling or advertising properties you don’t own almost impossible. No further middlemen, paper work and delays

- Transparency: Creation of unique digital IDs for real estate assets, buyers and sellers. Enable faster mortgage process and transfer of ownership. For the buyer, credit history and income could be instantly verifiable, avoiding time-consuming tasks involving banks, lawyers and estate agents. Homeowners can prove ownership and time of residence within a property. For assets, digital identities could be assigned, which would include the chain of ownership, list of repairs etc.

- Examples: Bitfury & velox.re

Supply Chain Shipping – Blockchain Solutions

- Digitize Supply Chain Process
- Track the paper trails of shipping containers
- Reduce time spent in transit and shipping process
- Enhance transparency and security of product information exchanged between parties
- Reduce costs and complexity
- Improve stock management
- Reduce fraud and errors on the quality of products
- Examples: IBM Watson (play the demo)

Solar Energy Management - Blockchain Solutions

- Example: The Brooklyn Microgrid
- **Transparency** through the whole process
- Decentralized and direct buying/selling of energy among participants(mostly electricity) – Independence from a third party power provider
- Storage of transaction data and recording of electricity generated per participant within a network
- Smart contracts application on distribution upon smart devices recordings
- Blockchain technology can allow a neighborhood or a region to put together an energy trading system derived from solar panels, to record transactions between locals. This would *save them money and hassle*
- Users can trade excess energy between them instead of selling it back to the power company. Participants will be able to access the transparent ledger any time they wish. Participants can decide **how much, at what price and to whom to sell their excess energy**, while all the transactions will be recorded on the Blockchain.

4. Conclusions

Conclusions

- The concept of the blockchain can be employed to solve more advanced problems.
- Meta-coins extend the existing Bitcoin protocol and depend on the existing Bitcoin infastructure. On the other hand, Alt-coins are based on the Bitcoin concept while differing in their implementations.
- Meta-coins enable more advanced applications, such as smart contracts, asset registration, remote attestation, voting, etc.
- Future uses of the concept of the blockchain will increasingly give birth to a large number of promising applications and further concepts.

5. Further Reading

Some Further Reading

- **Bitcoin: A Peer-to-Peer Electronic Cash System**, Satoshi Nakamoto https://bitcoin.org/bitcoin.pdf (The original paper of Satoshi Nakamoto)
- **Overview of Colored Coins** paper, Meni Rosenfeld https://bitcoil.co.il/BitcoinX.pdf
- **Enter The Blockchain: How Bitcoin Can Turn The Cloud Inside Out**, J. Evans, TechCrunch
- **Bitcoin Series 24: The Mega-Master Blockchain List**, Ledra Capital LLC http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list
- **Zerocash: Decentralized Anonymous Payments from Bitcoin** http://zerocash-project.org/paper
- **Decentralized Digital Asset Registers – Concepts**, Richard Brown, http://gendal.wordpress.com/2013/11/10/decentralised-digital-asset-registers-concepts/
- **Bitcoin Cooperative ProofofStake**, Stephen L. Reed http://arxiv.org/pdf/1405.5741.pdf
- **Principles of Remote Attestation** http://web.cs.wpi.edu/~guttman/pubs/good_attest.pdf
- **Decentralized Anonymous Credentials**, Johns Hopkins University https://eprint.iacr.org/2013/622.pdf

UNIVERSITY *of* NICOSIA

Questions?

Contact us:

Twitter: @mscdigital
Course Support: digitalcurrency@unic.ac.cy
IT & Live Session support: dl.it@unic.ac.cy