UNIVERSITY *of* NICOSIA

MSc in Digital Currency

DFIN-511: Introduction to Digital Currencies

Session 6
Alternative Uses of the Blockchain I

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 the upcoming 2 sessions we aim to introduce a few different potential applications.***

Agenda

1. Purpose of the Blockchain
2. Alternative uses of the Blockchain – Privacy Coins, Asset Management, Sidechains, Contracts
3. Blockchain solutions for various industries
4. Conclusions
5. Further Reading

1. Purpose of the Blockchain

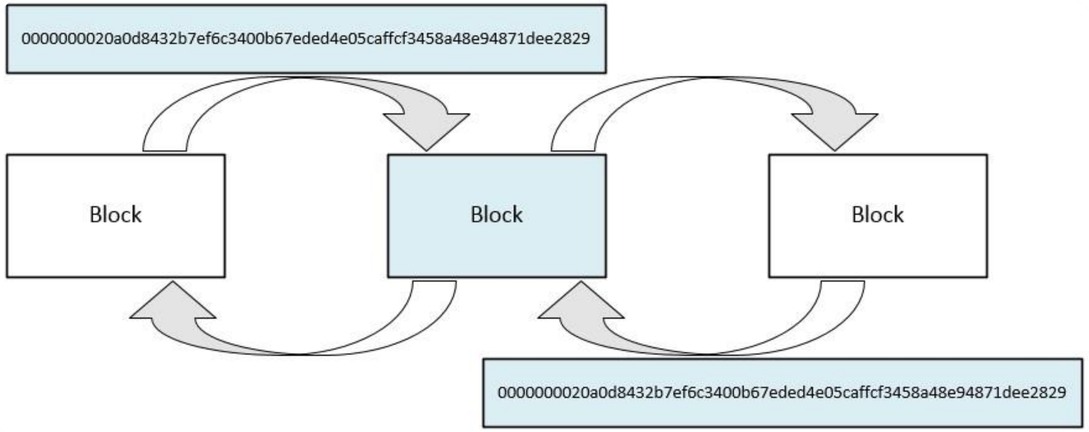
Purpose of a blockchain

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 and immutability 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 in the areas of:

- Meta-coins
- Sidechains
- Asset Registration
- Colored Coins
- Solar Energy Distribution
- Academic Certificates

- Smart Contracts
- Smart Property
- Financial Contracts and Instruments
- Digital Rights Management
- Supply chain
- Real Estate Management

Source: gigaom.com

Privacy 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 user identities from their payment patterns/habits
- Zerocoin achieves its goal by employing zero-knowledge mathematical proofs (see next slides). 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 - significant time taken by nodes to verify the proofs

Source: Wikimedia Foundation

Alt-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

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 (now forming the Zcash team) point out that Bitcoin 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 Zcash works

Zcash

- “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, Zcash 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 (it only takes milliseconds).
- *“A Z-to-Z transaction appears on the public blockchain, so it is known to have occured and that the fees were paid. But the addresses, transaction amount and the memo field are all encrypted and not publicly visible. Using encryption on a blockchain is only possible through the use of zero-knowledge proofs. More information on these proofs and Zcash’s implementation of zk-SNARKs is available.*
- *The owner of an address may choose to disclose z-address and transaction details with trusted third parties — think auditory and compliance needs — through the use of view keys and payment disclosure.*
- *Transactions between two transparent addresses (t-addresses) work just like Bitcoin: The sender, receiver and transaction value are publicly visible. While many wallets and exchanges exclusively use t-addresseses today, many are moving to shielded addresses to better protect user privacy.*
- *The two Zcash address types are interoperable. Funds can be transferred between z-addresses and t-addresses. However, is important that users understand the privacy implications of shielding or de-shielding information through these transactions. More information on the various transaction types is available.”*
- Source: https://z.cash/technology/

Zero-knowledge proofs

- This concept aims to solve fungibility issues. Zcash addresses are either private (z-addresses) or transparent (t-addresses). Z-addresses start with a “z,” and t-addresses start with a "t.“
- Have a look at Zcash’s blockchain.
  - Approximate only 5.3% of funds are held in z-addresses, which are private addresses enhancing zero-knowledge proofs
  - Approximately 94.7% of the transactions are not private
  - The process of creating a transaction with zero-knowledge proofs (zk-SNARKs) is not default and sometimes slow and costly – requiring a full and up to 4GB of RAM
  - Users using privacy features usually hold large amount of funds and/or sensitive information so they may draw interest from malicious parties to be attacked

Grin Coin

- Since we are discussing privacy coins, "Grin" has been a recent implementation of the MimbleWimble protocol, aiming to be a scalable and private coin that has no addresses, no amounts with limited storage requirements. Grin is ASIC-resistant, so GPU and CPU are the methods to mine. Grin was launched on January 15th, 2019.
- *MimbleWimble changes this bitcoin model by creating one multisignature for all of the inputs and outputs. The parties involved in a transaction create one public multisignature key that can verify the transaction. There are no addresses in the system because two parties engaging in a transaction share what's called a "blinding factor" where only those two parties know they are engaging in a transaction; keeping the privacy of the network.*
- *A blinding factor is a shared secret between the two parties that encrypts the inputs and outputs in that specific transaction as well as the transacting parties' public and private keys. MimbleWimble utilizes a Pedersen commitment scheme where full nodes subtract the encrypted amounts on the sending side of transactions (inputs) from the encrypted amounts on the receiving side of transactions (outputs).*
- *A balanced equation means that no coins were created out of thin air – **and the node never has to know what the transaction amounts were.***

https://cryptobriefing.com/grin-coin-mimblewimble-introduction/

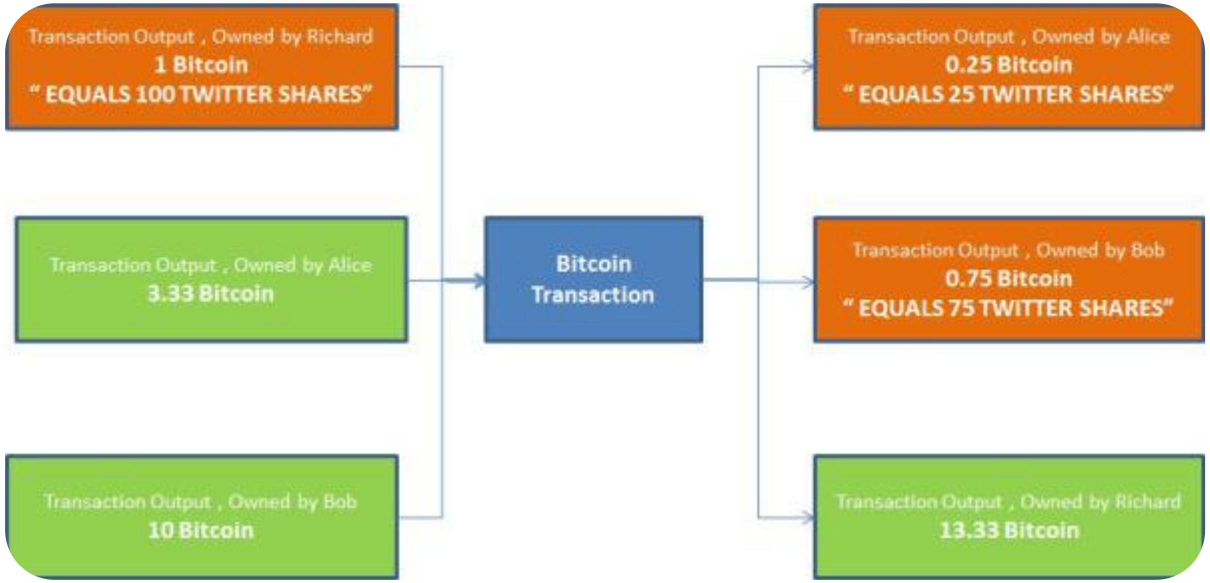
Grin Coin

- Notice the last sentence of the previous slide. The only verification needed is that no new coins have been created and that the parties in the transaction have ownership of their keys. Other than some exchanges, the official Grin wallet (i.e. full node) can be used to manage Grin coins which and provide full control to the user.
- Grin is community driven and it enhances PoW, but with a different algorithm – Cuckoo Cycle.
- Development Funding - https://grin-tech.org/yeastplume.html
- Grin's Monetary Policy
  - Supply of 1 coin per second with no maximum limit - each block takes 1 minute to mine – therefore 60 grin will be produced as block coinbase reward per minute.
  - Divisible to 1,000,000,000 nanogrins
  - It enhances a linear emission rate, therefore certainty and predictability for miners and investors
  - No ICO. Grin mined will become available organically to the market.
  - Transaction fees are low with the only intention to prevent spammers. They are priced proportionately to the costs incurred by the network when accepting a transaction
  - Alternative assets enhancing differing cryptography and policies are to be soft forked into the Grin protocol in the future.

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).

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


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

Asset registration

- Blockchain technology is also able to address the issuing of shares and bonds, or the creation of 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 is now a forgotten concept as better alternatives have emerged.

Colored Coins

- Instead of building other blockchains (sidechains), colored coins allow attaching metadata to bitcoin transactions. These coins now represent other real-world assets which can be traded on the bitcoin blockchain
- The value of such assets (Securities, shares, bonds, cars, documents, smart keys, digital rights etc.) is tied to a real world promise (contract) by the asset issuers that they are willing to redeem digital tokens for these assets
- This concept takes advantage of blockchain immutability and transparency
- Example: Color 1 btc – each satoshi is tied to 1 share of XYZ stock. XYZ stock can be traded on the btc blockchain, not the stock market
- Disadvantage: Real world promise is a contract done outside of blockchain. So trust must be built. If I have 10k satoshis and go to XYZ company to take my shares, they are not forced by the protocol to give me the shares.
- Coins can be tracked. Anyone can color. But a special wallet is needed to check b/ces and distinguish which bitcoins are colored. Colored coins are staying irrelevant because other solutions emerge which do not depend on bitcoin blockchain e.g. ERC 20 Tokens
- An examples of a Colored coins-enabled wallet is the ChromaWallet

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.
- https://counterparty.io/projects/
- A counterparty protocol for the Bitcoin cash network is being created
  - https://news.bitcoin.com/crypto-derivative-platform-counterparty-is-coming-to-the-bitcoin-cash-network/

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.

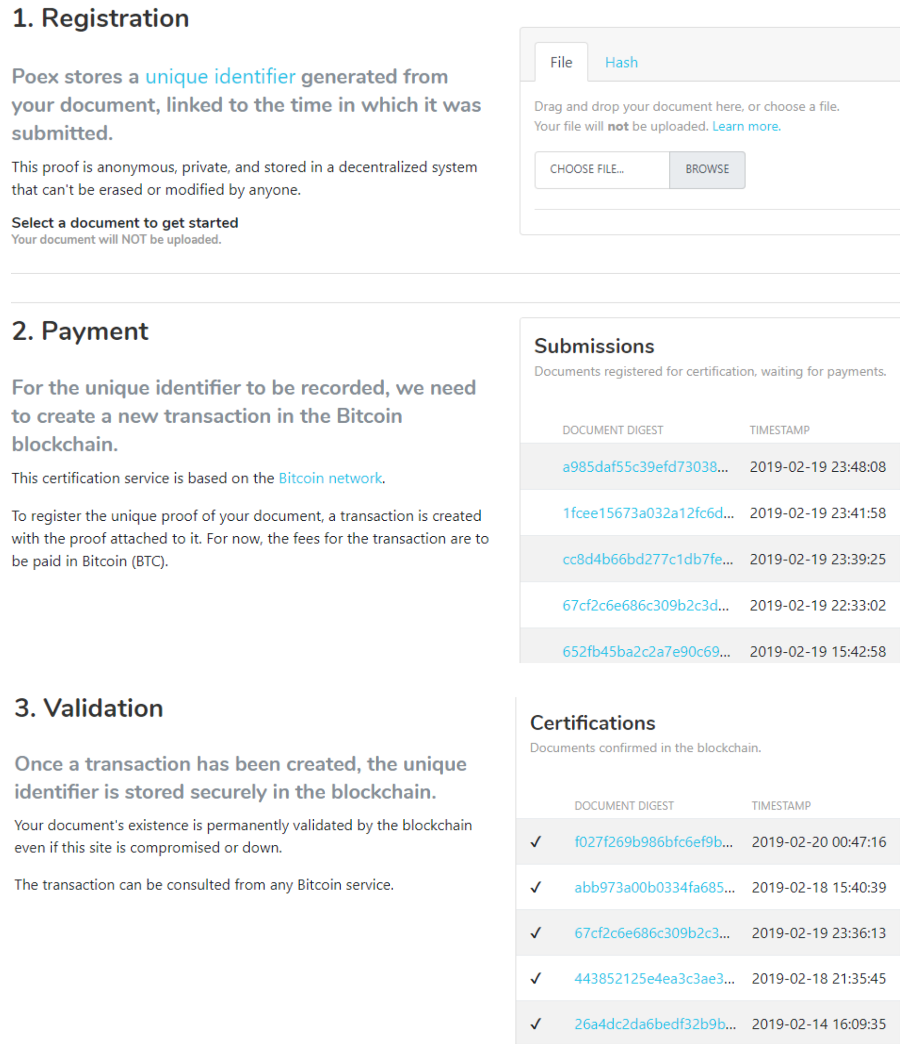
Counterparty – in detail

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

Proof-of-Existence

- **Proof-of-Existence: https://poex.io/**
- Anonymity, integrity and security by storing an online distributed proof of existence for any document
  - Documents not stored in any database or the Bitcoin Blockchain
  - No need to trust any central authority
  - By demonstrating data ownership without revealing actual data, copyrights and patents can be safe
- Abstract from website: *"The document is certified via embedding its SHA256 digest in the bitcoin blockchain. This is done by generating a special bitcoin transaction that encodes/contains the hash via an OP_RETURN script. This is a bitcoin scripting opcode that marks the transaction output as provably unspendable and allows a small amount of data to be inserted, which in our case is the document's hash, plus a marker to identify all of our transactions. Once the transaction is confirmed, the document is permanently certified and proven to exist at least as early as the time the transaction was confirmed"*



1. Registration

Poex stores a unique identifier generated from your document, linked to the time in which it was submitted.

This proof is anonymous, private, and stored in a decentralized system that can't be erased or modified by anyone.

Select a document to get started
Your document will NOT be uploaded.

Drag and drop your document here, or choose a file.
Your file will **not** be uploaded. Learn more.

2. Payment

For the unique identifier to be recorded, we need to create a new transaction in the Bitcoin blockchain.

This certification service is based on the Bitcoin network.

To register the unique proof of your document, a transaction is created with the proof attached to it. For now, the fees for the transaction are to be paid in Bitcoin (BTC).

Submissions

Documents registered for certification, waiting for payments.

DOCUMENT DIGEST	TIMESTAMP
a985daf55c39efd73038...	2019-02-19 23:48:08
1fcee15673a032a12fc6d...	2019-02-19 23:41:58
cc8d4b66bd277c1db7fe...	2019-02-19 23:39:25
67cf2c6e686c309b2c3d...	2019-02-19 22:33:02
652fb45ba2c2a7e90c69...	2019-02-19 15:42:58

3. Validation

Once a transaction has been created, the unique identifier is stored securely in the blockchain.

Your document's existence is permanently validated by the blockchain even if this site is compromised or down.

The transaction can be consulted from any Bitcoin service.

Certifications

Documents confirmed in the blockchain.

	DOCUMENT DIGEST	TIMESTAMP
✓	f027f269b986bfc6ef9b...	2019-02-20 00:47:16
✓	abb973a00b0334fa685...	2019-02-18 15:40:39
✓	67cf2c6e686c309b2c3...	2019-02-19 23:36:13
✓	443852125e4ea3c3ae3...	2019-02-18 21:35:45
✓	26a4dc2da6bedf32b9b...	2019-02-14 16:09:35

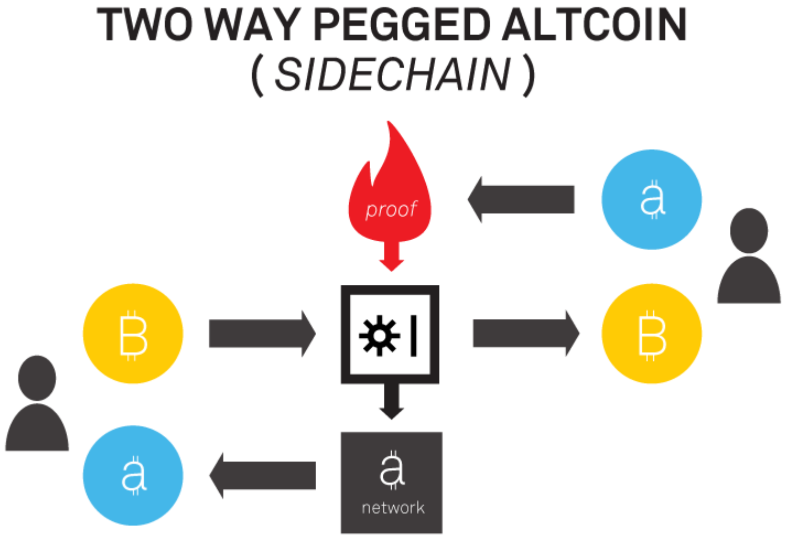
Another use of blockchain technology - Sidechains

- Sidechains: Blockchains completely independent from the main bitcoin blockchain
- Allow bitcoin or other assets to be transferred between blockchains
- Can be the architecture for new type of products/services by combining functionality/popularity of bitcoin with flexibility of other blockchains
- <u>Problem solved: How to advance the functionality of bitcoin without affecting the network</u>
- Sidechains become source of innovation and extension of the bitcoin blockchain - Can be built on top of any blockchain
- Process:
  - Assets are transferred at a fixed or otherwise deterministic exchange rate
  - Coins “leave” the bitcoin network(in reality sent to a special address), so they are actually frozen not leaving the network
  - When a tx is confirmed – bitcoin owner sends a message to the sidechain containing verification of ownership
  - Sidechain creates an equal amount of pegged bitcoins(or other specified tokens) and send to the owner
  - These coins can be involved in transactions in the sidechain under whatever rules the sidechain has
  - Pegged coins can be redeemed back for bitcoins in the same way. Sidechain will destroy the pegged coins and bitcoins will be released on the main blockchain
- **<u>Advantages:</u>** Extensions to original bitcoin capabilities with other capabilities - Environment for innovation - Better performance on parent chain because of offload transactions in sidechains - Increased privacy

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 that 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.



Source: cryptobizmagazine.com

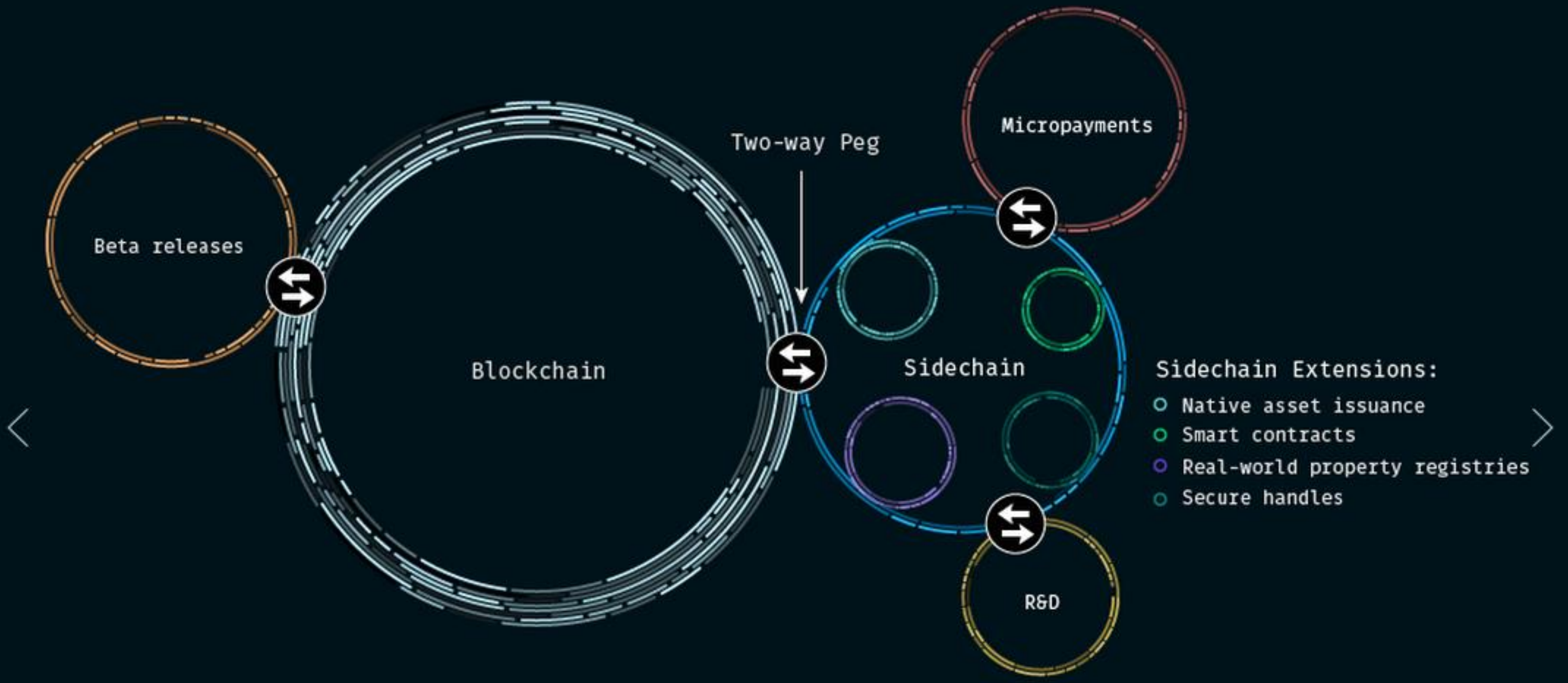
Sidechains – in detail

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

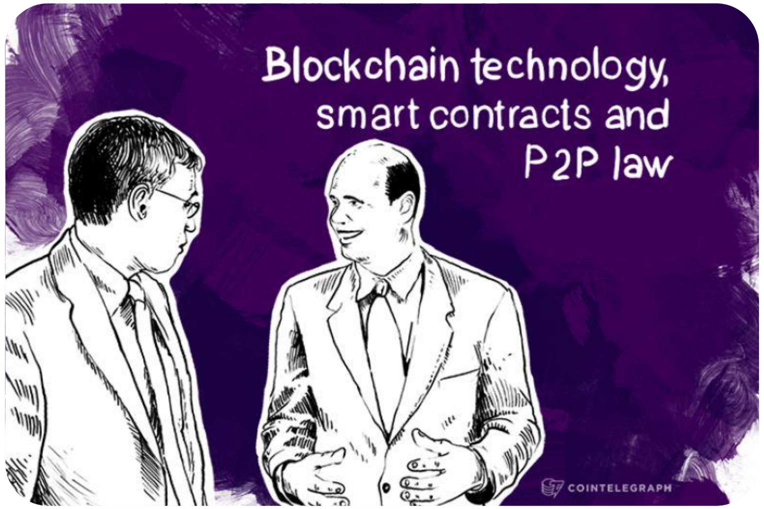


Sidechains can have other sidechains for things like micropayments. They allow for experimentation and pre-release versions of future sidechains or even a beta version of Bitcoin itself.

https://www.bitcoinmarketjournal.com/what-is-a-bitcoin-sidechain/

Smart contracts – to be examined on the next session

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

- See here for some interesting solutions empowered by smart contracts technology
- 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 Contracts - 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 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

- “Smart Contracts” can also be defined as “Smart Agreements”. Most financial instruments are essentially a contract/agreement 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. Since these third parties are costly and time-consuming, 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.

- Let’s imagine that 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.

A sidechain based protocol aiming to offer equivalent and compatible smart contract functionality, is Rootstock.
Rootstock evaluation: https://medium.com/novamining/rootstock-rsk-smart-contracts-on-bitcoin-9ef28e135193

3. Blockchain Solutions for Various Industries

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
  - Trusts
- **Other uses**, for instance:
  - Certifications (like our university uses to store certificates of MOOC completion)
  - Medical records (like the Hashed Health initiative)

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

https://ujomusic.com/

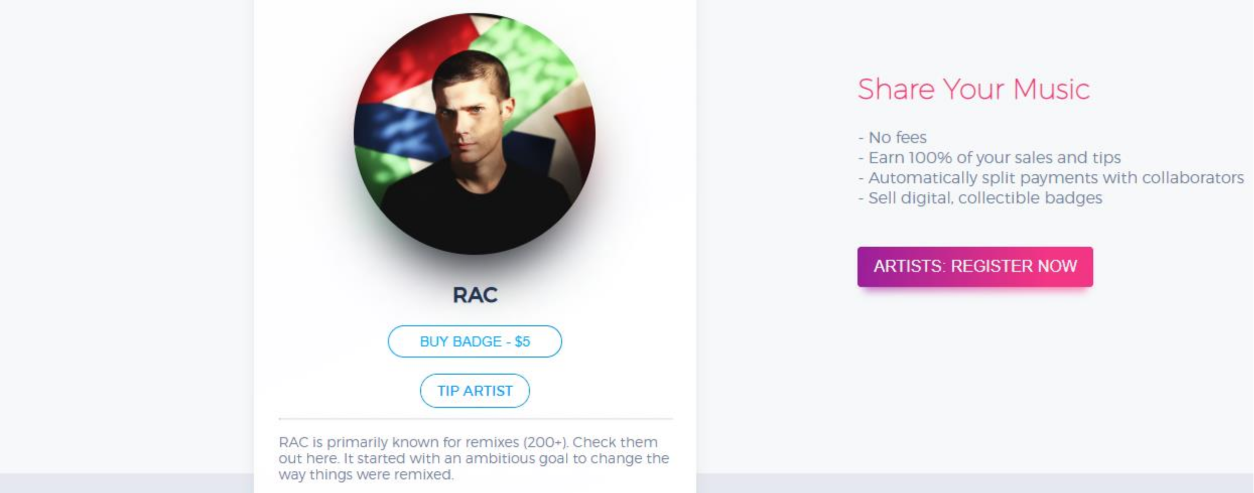
http://myceliaformusic.org/

- Ownership is registered permanently therefore no need for record labels to have a share of the artist's work
- UjoMusic - 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

Imogen Heap's 'Tiny Human' was the only track available on Ujo as an initial attempt. (almost 150 purchases)

You would need to set up Metamask in order to access Decentralized Applications

Ujo's interface

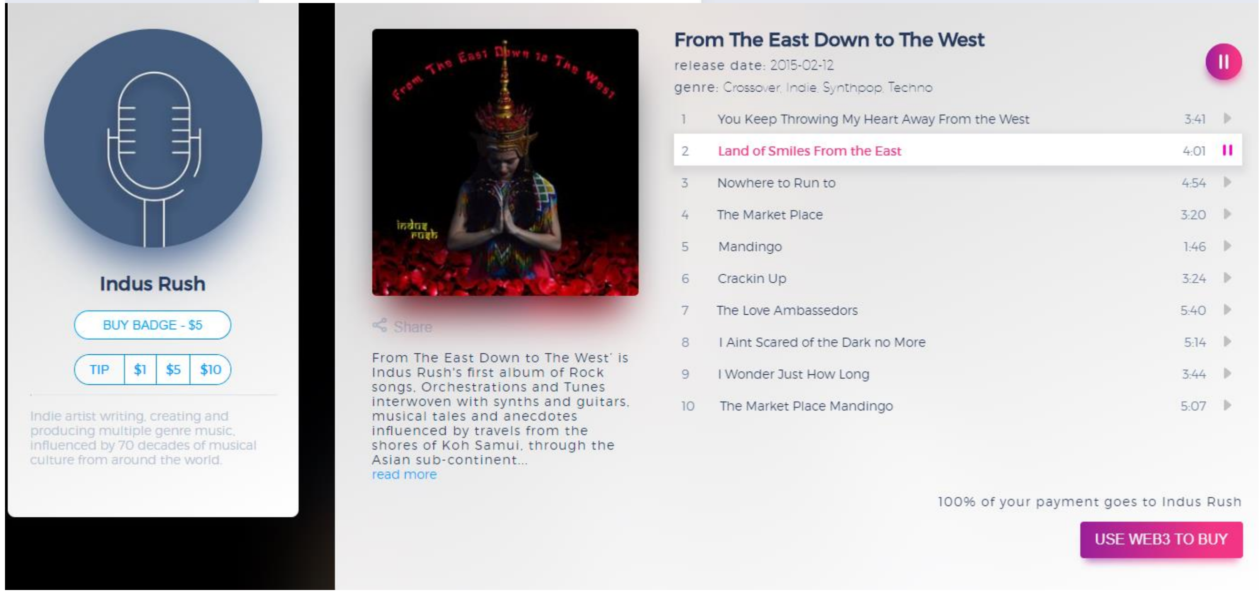


RAC is primarily known for remixes (200+). Check them out here. It started with an ambitious goal to change the way things were remixed.

Share Your Music

- No fees
- Earn 100% of your sales and tips
- Automatically split payments with collaborators
- Sell digital, collectible badges

Artists can register and list their work



Indie artist writing, creating and producing multiple genre music, influenced by 70 decades of musical culture from around the world.

From The East Down to The West' is Indus Rush's first album of Rock songs, Orchestrations and Tunes interwoven with synths and guitars, musical tales and anecdotes influenced by travels from the shores of Koh Samui, through the Asian sub-continent...
read more

From The East Down to The West

release date: 2015-02-12

genre: Crossover, Indie, Synthpop, Techno

1	You Keep Throwing My Heart Away From the West	3:41
2	Land of Smiles From the East	4:01
3	Nowhere to Run to	4:54
4	The Market Place	3:20
5	Mandingo	1:46
6	Crackin Up	3:24
7	The Love Ambassedors	5:40
8	I Aint Scared of the Dark no More	5:14
9	I Wonder Just How Long	3:44
10	The Market Place Mandingo	5:07

100% of your payment goes to Indus Rush

Fans can reward their favourite artists via blockchain technology

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
- The University of Nicosia solution: https://block.co/our-product/#how-it-works-nav

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.
- Example: Bitfury and Republic of Georgia

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
- Example: IBM & Maersk

Image Source: https://www.sgkglobal.com/

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.

https://www.energymatters.com.au/panels-modules/choosing-solar-panels/

4. Conclusions

Conclusions

- The concept of blockchain can be employed to solve more advanced problems than just serve as a payment mechanism.
- 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. Ethereum (more details next week) looks like the most promising platform at the moment to host disruptive decentralized applications
- Besides the material presented on this session, you can also check out next week's additional material posted on MOODLE, which will provide an overview of consortium blockchain use cases like Hyperledger and R3. These communities work to provide distributed platforms and frameworks which are able to innovate procedures within many industries.

5. Further Reading

Some Further Reading

- Overview of Colored Coins paper, Meni Rosenfeld

https://bitcoil.co.il/BitcoinX.pdf

- 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

- Fidelity is lunching a digital assets trading platform

https://www.coindesk.com/fidelity-reveals-cryptocurrency-and-digital-asset-trading-platform

- Community Discussion on non-Bitcoin applications of blockchain technology

https://www.quora.com/What-are-non-Bitcoin-cryptocurrency-applications-of-blockchain-technology

- Grin Coin

https://grin-tech.org/

https://blockonomi.com/grin-mimblewimble/

Some Further Reading

- Blockchain Land Registry in the UK

https://www.coindesk.com/uk-land-registry-begins-new-phase-of-blockchain-research-project

- Ethereum-based decentralized applications

https://www.stateofthedapps.com/

- Enabling Blockchain Innovations with Pegged Sidechains, Blockstream

https://blockstream.com/sidechains.pdf

- Sidechains: Why These Researchers Think They Solved a Key Piece of the Puzzle, Amy Castor

https://bitcoinmagazine.com/articles/sidechains-why-these-researchers-think-they-solved-key-piece-puzzle/

- Smart Contracts Switch “I agree” to “I negotiate”, Andreas Vlachos

https://www.linkedin.com/pulse/smart-contracts-switch-i-agree-negotiate-andreas-vlachos

- Blockchain for 2018 and Beyond: A (growing) list of blockchain use cases

https://medium.com/fluree/blockchain-for-2018-and-beyond-a-growing-list-of-blockchain-use-cases-37db7c19fb99

UNIVERSITY *of* NICOSIA

Questions?

Contact us:

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