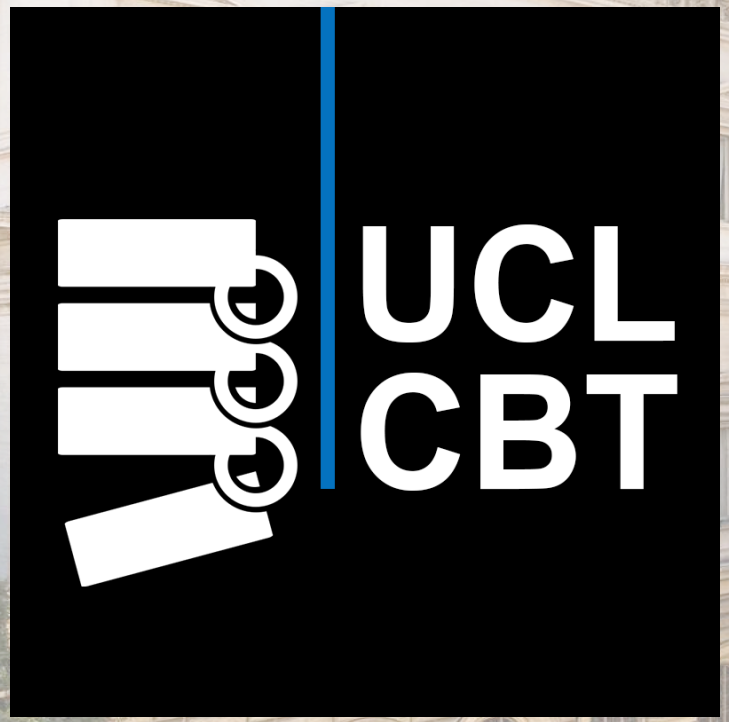
Beyond Digital Currencies
Alternative Blockchain Applications



Paolo Tasca

Convegno Banca d'Italia

La tecnologia blockchain: nuove prospettive per i mercati finanziari

- **What can actually blockchain do ?**

"While the Bitcoin hype cycle has gone quiet, Silicon Valley and Wall Street are betting that the underlying technology behind it, the Blockchain, can change…

- **What can actually blockchain do ?**

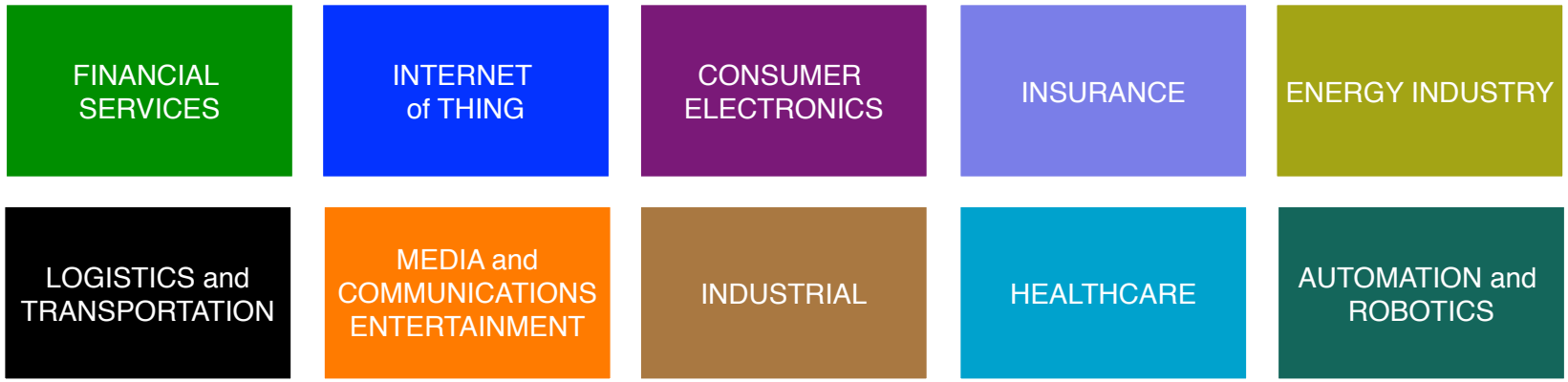
"While the Bitcoin hype cycle has gone quiet, Silicon Valley and Wall Street are betting that the underlying technology behind it, the Blockchain, can change…
well everything"

- **What can actually blockchain do ?**

"While the Bitcoin hype cycle has gone quiet, Silicon Valley and Wall Street are betting that the underlying technology behind it, the Blockchain, can change…
well everything"

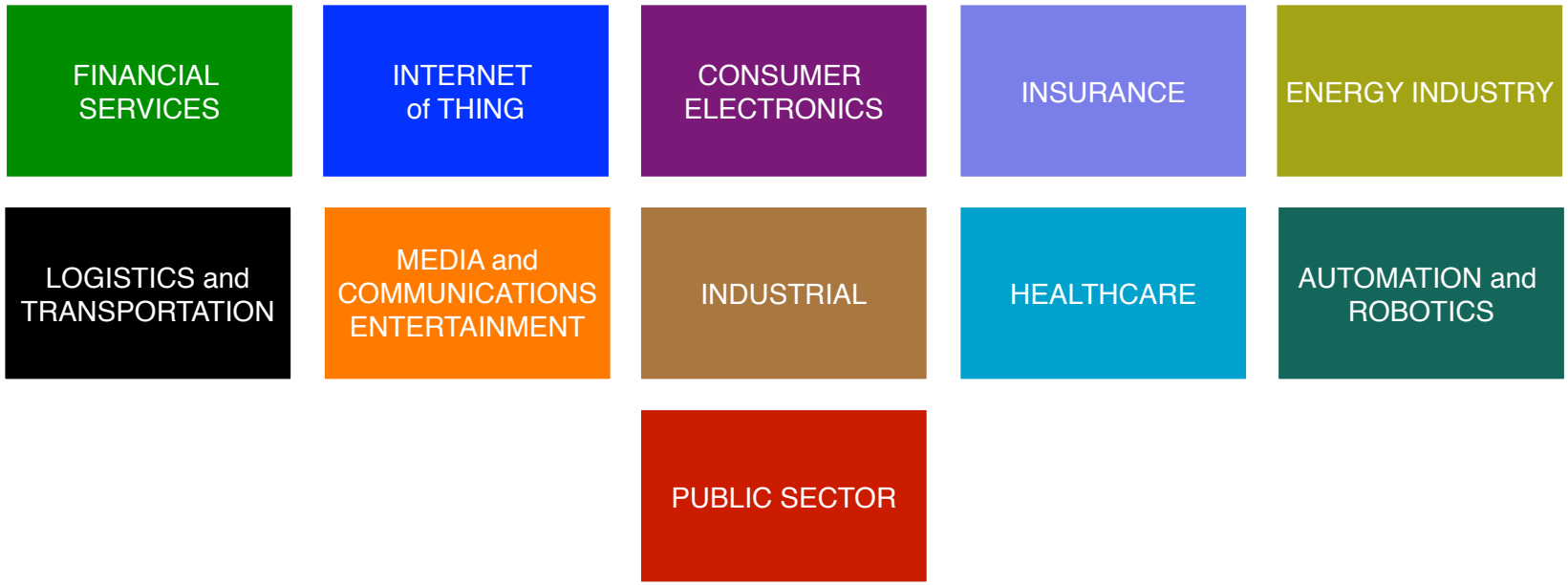
Goldman Sachs
(December 2015)

- **What can actually blockchain do in finance ?**



Sectors that will be affected by the blockchain technology

- **What can actually blockchain do in finance ?**

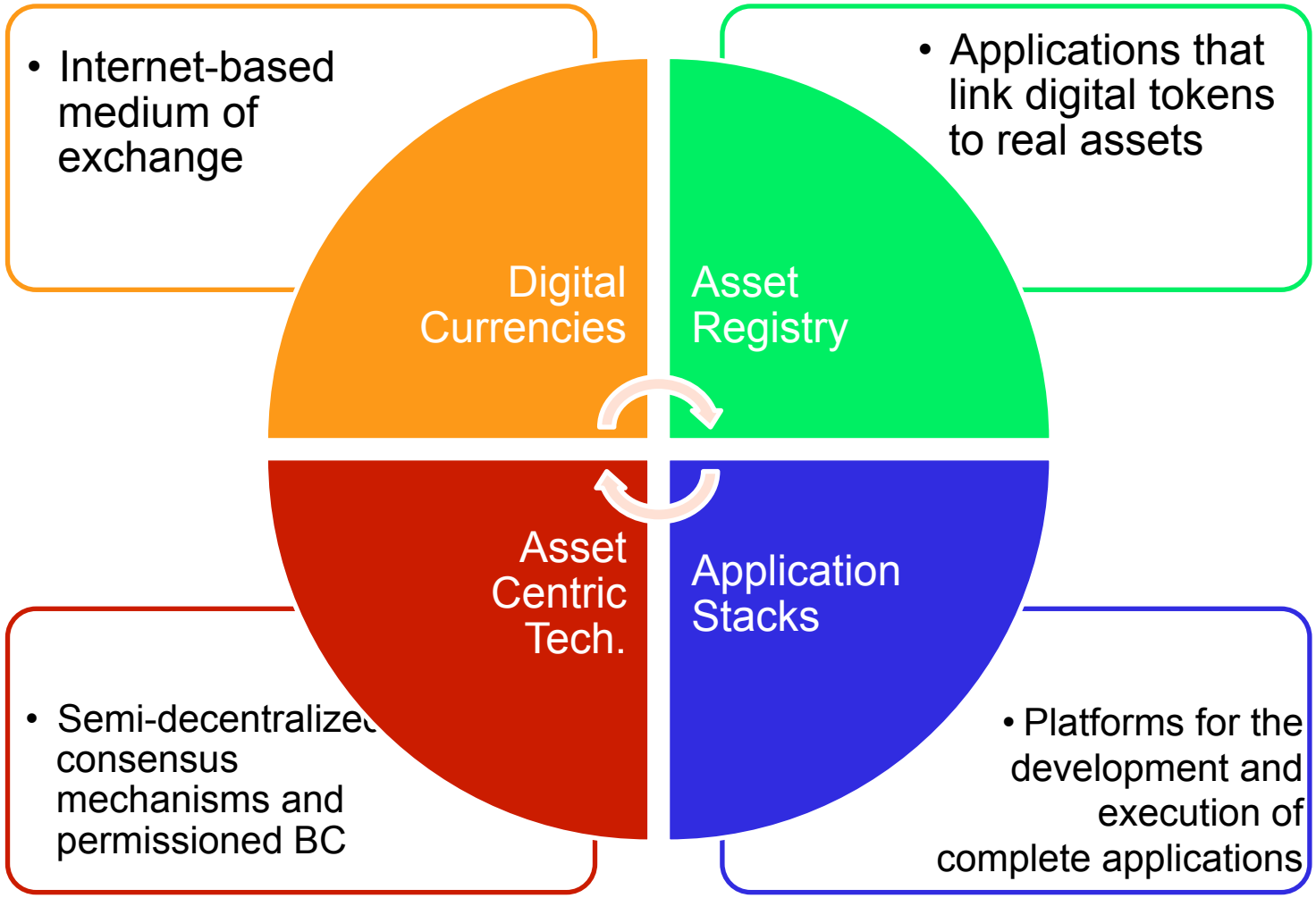


Sectors that will be affected by the blockchain technology

What can actually blockchain do in finance ?

Clearing and settlement Post-trading payments and transactions	Governance and monitoring Rating, grading and voting systems	Risk Management	Distributed and, or decentralised immutable data storage
Rewarding and incentive mechanisms	Refereeing, arbitration and notarization	Human ATM networks based on blockchain	Securitization and re-insurance activities
Digitalization of real assets such as stocks, bonds, land titles, and frequent flyer miles	Blockchain IDs for access in apps and websites, and digitally sign documents	Tamper–proof decentralization of controlling and auditing activities	Smart contracts for IoT applications
Correspond banking, trade finance, remittance and payments	Trust & custody Funds holding, and asset management	Shared private blockchain for efficient automatic invoice reconciliation and tracing	Decentralized applications to prevent frauds and thefts

Which blockchain technology ?



Digital Currencies

Decentralised No central bank or clearing mechanism. The trust is devoted not to one single entity but to the network

Secure The database is an immutable (tamper-proof) and records are irreversible

Trusted Record The distributed nature of the network requires nodes to reach a consensus. The consensus protocols govern the update of the blockchain with new blocks

Publicly/Privately Auditable Computer servers (miners) maintain the ledger entries (blocks) and every node sees the transactions when blocks are created (transaction traceability)

Automated Without the need for human interaction, verification or arbitration, the software is written so that conflicting or double transactions are not permanently written in the blockchain

Metadata Blockchain scripting languages have the potential to store small amounts of metadata on the blockchain

Digital Currencies / Use Cases

Remittance via Mobile

Region	Q1 2013	Q2 2013	Q3 2013	Q4 2013	Q1 2014	Q2 2014	Q3 2014	Q4 2014	Q1 2015	Q2 2015
East Asia & Pacific	8.97	8.88	9.00	8.28	8.52	8.38	7.92	8.12	8.13	8.11
Europe & Central Asia	6.77	6.70	6.68	6.29	6.49	6.35	6.17	6.22	6.11	6.02
Europe & Central Asia excluding Russia	8.43	8.35	8.41	7.93	8.18	7.92	7.67	7.54	7.20	7.18
Latin America & Caribbean	7.77	7.28	7.26	7.02	6.21	5.57	6.02	6.03	6.14	6.78
Middle East & North Africa	7.81	7.83	7.61	7.80	8.32	8.29	8.25	8.63	8.41	8.21
South Asia	7.16	7.02	7.12	6.58	6.56	6.45	5.97	5.94	5.96	5.74
Sub-Saharan Africa	12.2	12.1	12.3	12.6	11.7	11.6	11.3	11.5	10.2	9.74
Global	9.05	8.88	8.93	8.58	8.36	8.14	7.90	7.99	7.72	7.68

Fig: Total avg. remittance cost by region of the world. World Bank remittance pricing report June 2015

- Remittance: USD 200 bn in 2004 to USD **1 tn in 2018** (estimate)
- According to the **World Bank Global Findex** (2014 data), two billion people - equating to **38%** of the world's adult population - do not use formal financial services
- The **73%** of poor people are unbanked because of costs, travel distances and the often-burdensome requirements

Digital Currencies / Use Cases

Remittance via Mobile

From 2014 peer-to-peer remittance or "Human ATM network" where individuals can cash out money sent from other users via blockchain technology.

- **Abra** is a mobile phone app which allows both cash-in and cash-out via registered individuals or businesses, called Abra Tellers, who turn their mobile into an ATM and help consumers convert their paper cash into digital cash and vice versa[1]

- **37coins** has developed a novel means of making the Bitcoin network accessible to phones that only have a text (sms) functionality by sending a text message to a local smartphone that triggers the running of the 37coins gateway application

1. Deposited currency is transferred immediately to bitcoin, which is held on the individual's smartphone. By holding value in bitcoin, the company currently avoids any regulatory requirements for transmitting payments. Bitcoin run on the backend

Digital Currencies / Use Cases

Brand Currencies

Community-based digital currencies used in open-form environments as tools for:

- **Citizens coordination and opinion voicing**
  - **e-Estonia:**e-voting, digital contracts, e-tax declaration. Estonia is creating a transnational digital identity will be coupled with Nasdaq's blockchain technology in an experimental shareholder e-voting scheme
- **New Central bank monetary policy and payment infrastructure**
  - **RSCoin**: Ordinary people could by-pass the commercial banks and hold balances directly with the Central Bank[1]
  - **e-$:** Breaking Through the Zero Lower Bound and Electronic Money proposed by Ruchir Agarwal (IMF) and Miles Kimball (University of Michigan)
  - **FEDCoin** (and beyond). Federal Reserve Bank of St. Louis may be collaborating with IBM to develop a new decentralised payment and monetary infrastructure

1. Somehow in line with the Chicago Plan promoted by Adam Smith, put forward by US economists in the 1930s and never enacted

Asset Registry

What: Applications that link digital tokens to real assets. “Ledger within a ledger”: ledger is embedded within the other and parsed independently

How: Blockchain scripting languages have the potential to store small amounts of metadata on the blockchains

Applications:

1 ColoredCoins (“fake” addresses)
2 Counterparty (PoB, XCP, mutisig)

Problems:

1) Authenticity of the underlying assets/services
2) Risk about the issuer creditworthiness and risk of losing the underlying assets/ services[1]
3) Blockchain bloating

3 Mastercoin (saving addresses, PoB, MSC)
4 Namecoin (DNS namespace, messaging)

1. Coins can accidentally be uncoloured if the order-based coloring rules are not correctly implemented in the coins-aware clients. Metadata hosted on the issuer’s own server

Asset Registry / Use Cases

Calibration Health Insurance Risk Models[1]

A health insurance company could emit colored coins depending on the level of your health behavior. E.g.,

- Every time you go for a run, your smartphone app gives you some coins dependent of your performance
- Every time you do a routine check-up at your doctors you get some coins

Property Rights and Land Applications[2]

Land information management, where the land registry serves as a database of all property rights and historical transactions. Uses cases under dev.:

1) Time stamping of transactions akin to virtual notarization
2) Disaster recovery as the system does not rely on a single data center;
3) Multisignature Transactions[3]

1. **Gem.co** applies blockchain technology to addresses the trade-off between personalized care and operational costs by connecting the ecosystem to universal infrastructure
2. Companies working on this area: **ProSoft Alliance Blockhain** (Integration and Chain of Title Review), **Factom** (Beta Factom Protocol), **Epigraph** (Discussions with Govt. of Honduras), **Ubitquity** (Released Prototype), **Bitland** (Blockchain Capacity Building in Ghana)
3. To secure women's property rights when it comes to marital property

Asset Registry / Use Cases

Settlement

Settlement Risk: 1) one leg of the transaction may be completed but no the other [1] or 2) the settlement agent will fail to perform. Asset Registry technology can be used to:

1. Shorten settlement and reconciliation time (T+0) ⏎

reduce **costs**[2] and the amount of cash and **collateral** needed to be held

US	
Cash Equities	T+3
Equity Options	T+1
Equity Futures	T+1
Gov't Bonds	T+1
Corporate Bonds	T+3
Loans	T+20
Exchange-traded FICC Derivs	T+0
OTC FICC Derivs	T+2*
Europe	
Cash Equities	T+2*
Equity Options	T+1
Equity Futures	T+1
Loans	T+20
Exchange-traded FICC Derivs	T+0

Source: ICE, OCC, SIFMA, World Federation of Excha

1. Bliss & Steigerwald(2006)
2. Autnonmous Research (2016) estimates blockchain could reduce settlement costs by **30%** by 2021

Asset Registry / Use Cases

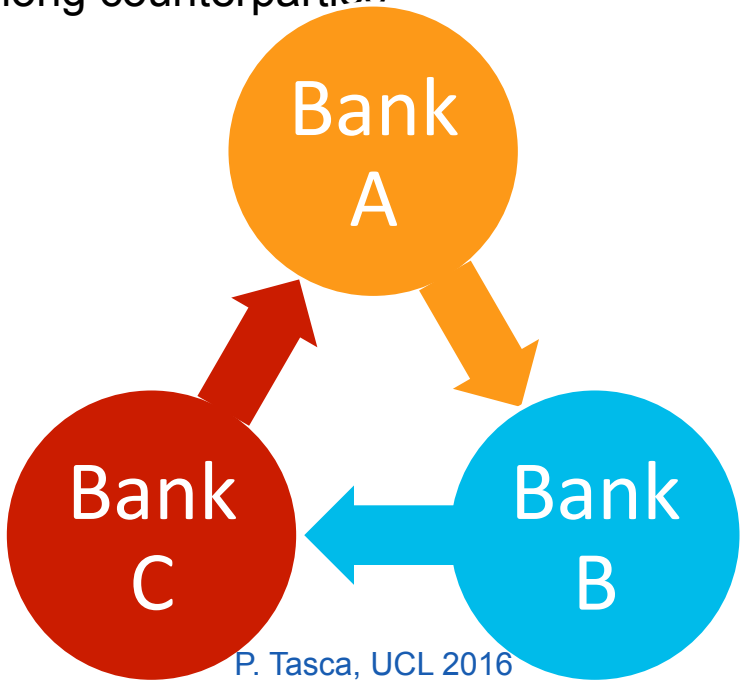
Settlement

Settlement Risk: 1) one leg of the transaction may be completed but no the other [1] or 2) the settlement agent will fail to perform. Asset Registry technology can be used to:

1. Shorten settlement and reconciliation time (T+0) ⏎

reduce **costs**[2] and the amount of cash and **collateral** needed to be held

2. Cut credit paths among counterparties



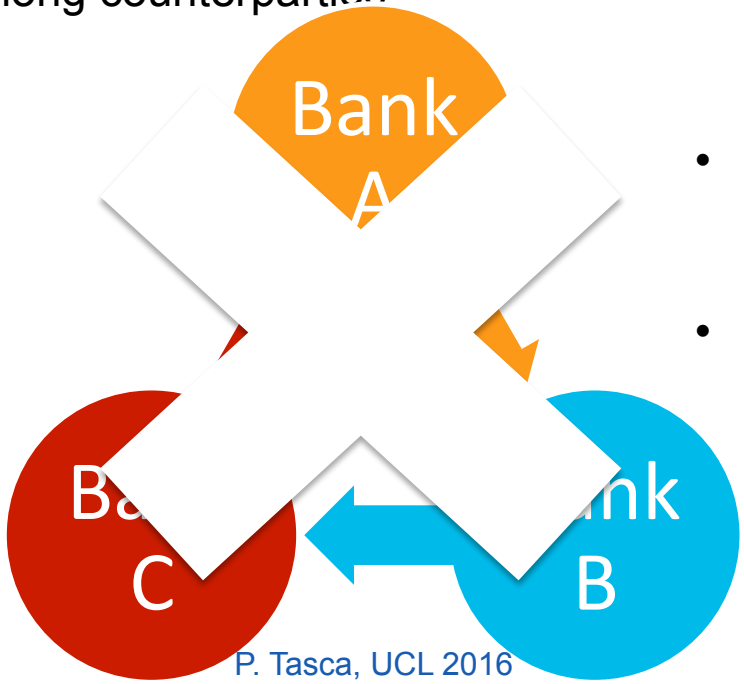
1. Bliss & Steigerwald(2006)
2. Autnonmous Research (2016) estimates blockchain could reduce settlement costs by **30%** by 2021

Asset Registry / Use Cases

Settlement

Settlement Risk: 1) one leg of the transaction may be completed but no the other [1] or 2) the settlement agent will fail to perform. Asset Registry technology can be used to:

1. Shorten settlement and reconciliation time (T+0) ⏎
reduce **costs**[2] and the amount of cash and **collateral** needed to be held
2. Cut credit paths among counterparties



- **Trade compression** by pooling risks together
- **Netting effects** when a bank default its obligation are netted with those of the counterparties

1. Bliss & Steigerwald(2006)
2. Autnonmous Research (2016) estimates blockchain could reduce settlement costs by **30%** by 2021

Asset Registry / Use Cases

Settlement

Business / Projects

Symbiont http://symbiont.io/

Coinprism / Open Asset https://www.coinprism.com/

Omnilayer http://www.omnilayer.org/

Blockchain Clearing Corp http://blockchainclearing.com/

Tzero https://t0.com/ (Issue stocks over Blockchain)

Digital Asset Holdings http://digitalasset.com/

Clearmatics http://www.clearmatics.com/

Setl https://www.setl.io/

BankChain https://www.bankchain.com/

Counterparty http://counterparty.io/

- New Research Group - CME Group, Euroclear, LCH.Clearnet, LSE, Soc Gen, and UBS: http://bit.ly/CMELSEBlockchain

- Goldman Sachs Files Patent Application For Securities Settlement Using Cryptocurrencies (Oct. 2014) https://bitcoinmagazine.com/articles/goldman-sachs-files-patent-application-for-securities-settlement-using-cryptocurrencies-1449000967

- NASDAQ enables private securities issuance using Blockchain Technology: http://bit.ly/nasdaqblock

- Australian Stock Exchange announced that is building a blockchain for clearing and settlement: http://bit.ly/ASEblock

- The Estonian bank LHV Bank is experimenting with coloured coins called “Cuber”, as a “cryptographically protected” certificate of deposit

Application Stacks

What: Non-currency[1] blockchain-based platforms for the development and execution of complete applications

- Autonomous Agents
- Smart Contracts
- Decentralized Application
- Decentralized Organizations
- Decentralized Autonomous Organiz.

on top of decentralised networks

Applications

1 NXT (data transfer, voting system, asset exchange)
2 Ethereum (programmable blockchain to build and run smart contracts)
3 Eris (open source blockchain database and smart contract machine + application server)

1. Used only as "gas"

Application Stacks / Use Cases

Trade Finance and Letter of Credit[1]

In presence of lack of trust, this tool generates the assurance that payments will take place once goods are exchanged according to certain rules

Problems:

- Current solutions suffer from a lack of transparency along the chain
- Paper-based documentation slow and open to fraud
- Working capital is tied up from when goods are manufactured to when they are paid for – 30 to 90 days after delivery[2]
- Taxes and Duties need to be accounted for each country
- Compliance costs (incl. KYC) : Only the most profitable customers get banked
- Messages need be reconciled and this normally takes place overnight
- Information is required to be in Roman characters, meaning a significant amount of translation takes place

1. Global Trade Payment US$22,000 billion
2. A reduction of processing time could result in a **$6 trillion improvement in working capital**

Application Stacks / Use Cases

Trade Finance and Letter of Credit

Documents

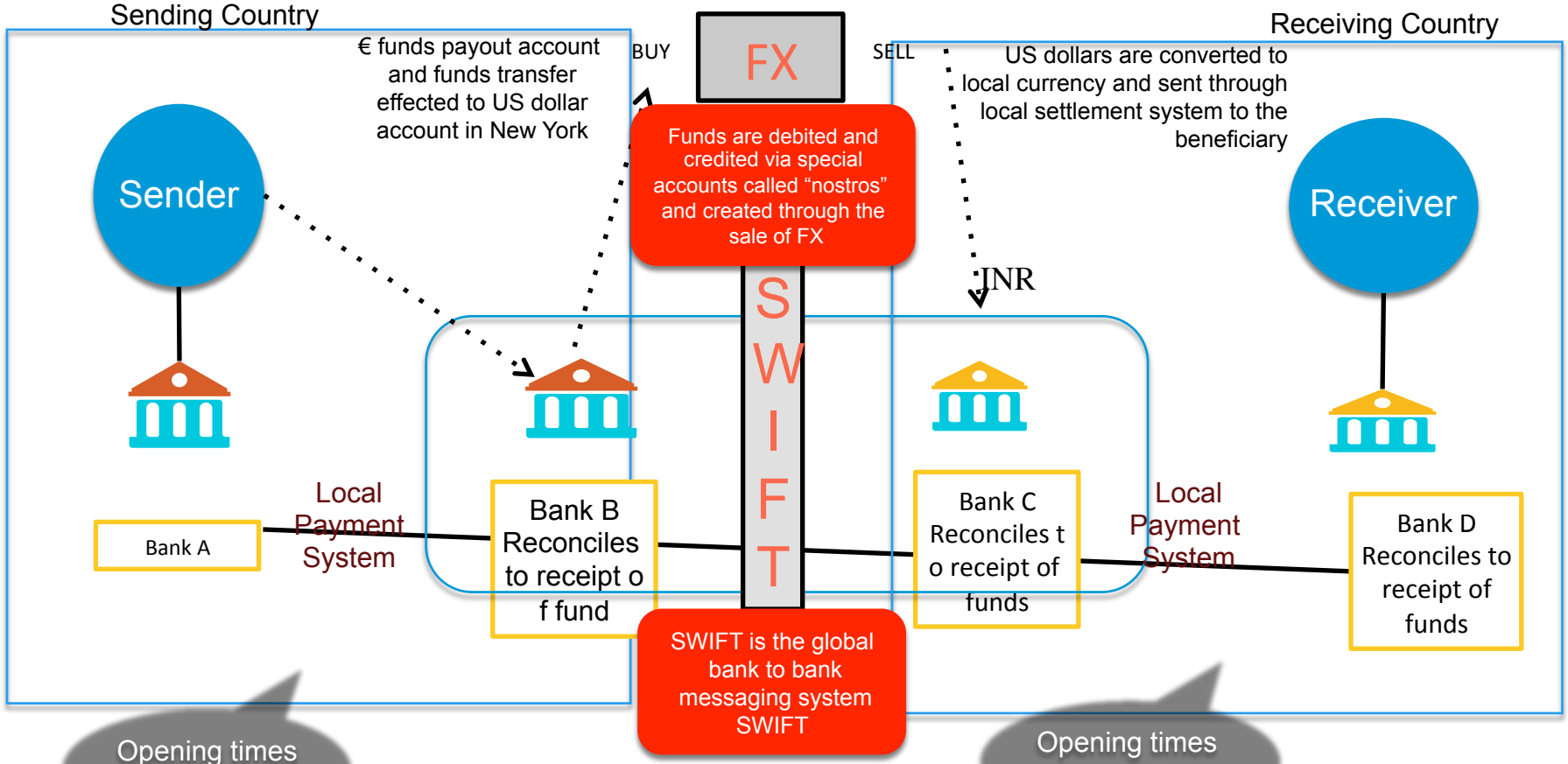
- Request for Quote
- Quote
- P.O.
- ASN
- Invoice
- Approved Invoice
- Bill of Lading
- Packing List
- Payment Instruction

Involved Parties

- Export Port Authority
- Insurer
- Import Customs & Tax
- Homeland Security
- Import Port Authority
- Freight forwarder
- Shipping Agent
- Export Customs & Tax
- Import Bank
- Advising Bank
- Export Bank
- Confirming Bank
- Risk Participant
- Buyer
- Retailer
- Wholesaler
- Domestic Financier
- Courier Company

Application Stacks / Use Cases

Trade Finance and Letter of Credit



Asset Centric Technologies

What: Exploit the properties of public distributed ledgers like Bitcoin but

- have semi-decentralized consensus mechanisms
- are (generally) permissioned

Applications:

1 Stellar (decentralised exchange of digital credits, native token, gateways)

2 Ripple (XRP, decentralised exchange, gross-settlement system, remittance, IOUs, RPCA → UNL)

3 Hyperledger (No native token → no-mining, no-fees and no spamming, multiple interoperable private ledgers, PGBA)

4 Tendermint (Combination of BGA and Proof of Collateral. Different from PBFT used by Hyperledger, Tendermint also works for "consortium" or "public" blockchains)

Asset Centric Technologies / Use Cases

Foreign Exchange (FOREX) Transactions

PSPs in different jurisdictions can act as gateways and once set bilateral trust they can transfer in real-time any currency exploiting a consensus mechanism similar to the Hawala payment systems[1]

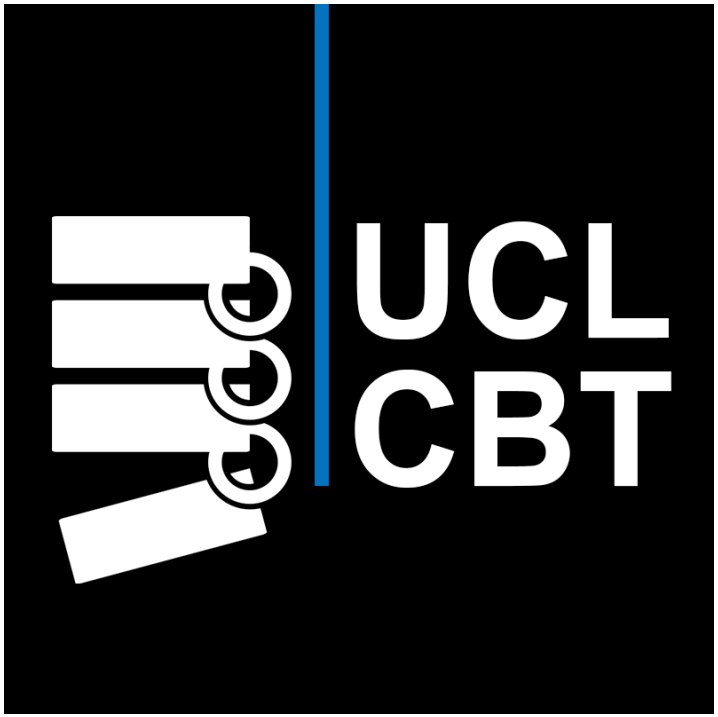
- **Fidor Bank** from Germany (Since 2014) has been offering to its customers instant Euro/USD FX transactions at low cost by implementing an open-source, internet-based settlement technology from Ripple Labs

Cloud-based banking

These are software as a service platforms based on asset centric technologies that allows to connect financial intermediaries

- **Oradian**, is an example of the a cloud-based banking software company, which use the Stellar network to connect microfinance institutions in Nigeria[1]

1. The transaction is the transaction taking place entirely on the honour system
2. 300,000 Nigerians registered in the system can cheaply transfer money between (microfinance institutes) MFIs (that works as gateways) over the Stellar network



Paolo Tasca

P.Tasca@ucl.ac.uk