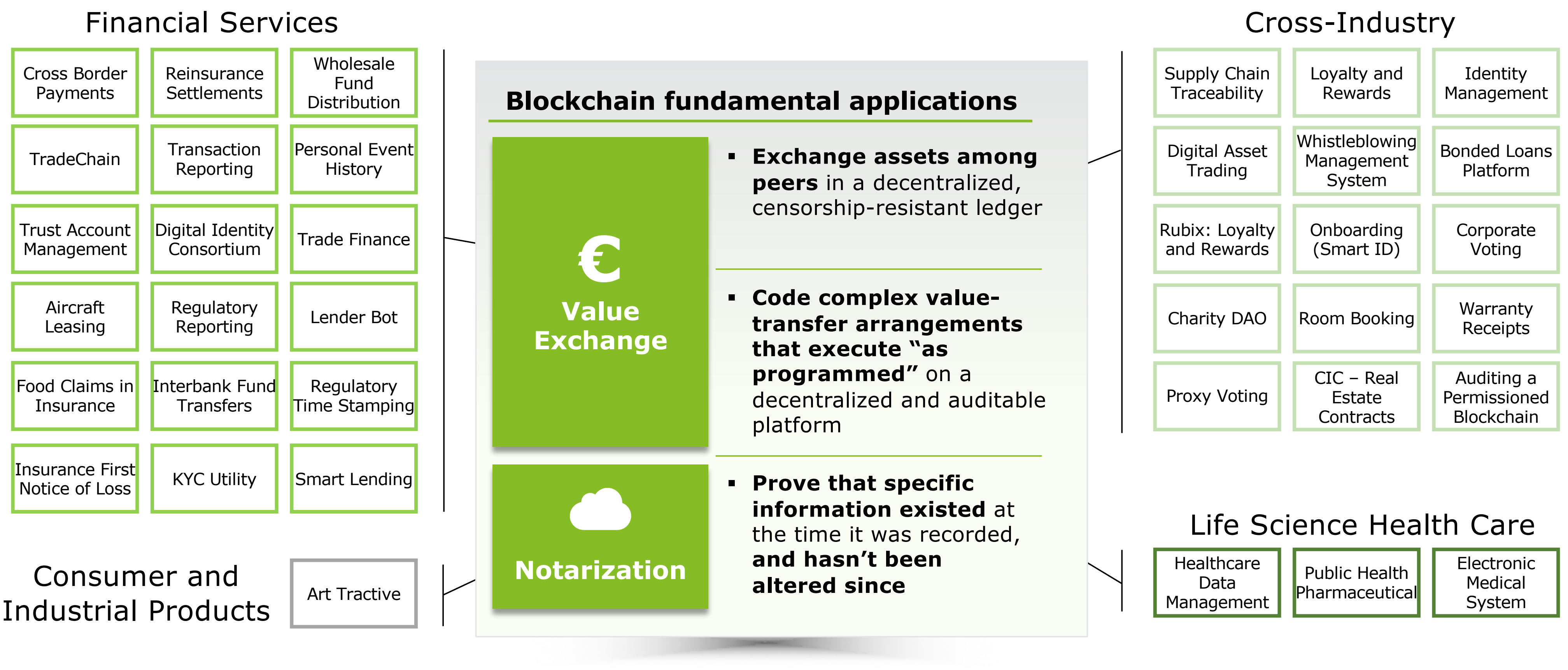
Three practical and prominent blockchain cases: Digicash, Timestamping and ICO

Paolo Gianturco
Senior Partner - Fintech & FSI Tech Leader, EMEA Blockchain Lab Co-Leader

February 1st 2018

A wide range of use cases from different industries



Financial Services

- Cross Border Payments
- Reinsurance Settlements
- Wholesale Fund Distribution
- TradeChain
- Transaction Reporting
- Personal Event History
- Trust Account Management
- Digital Identity Consortium
- Trade Finance
- Aircraft Leasing
- Regulatory Reporting
- Lender Bot
- Food Claims in Insurance
- Interbank Fund Transfers
- Regulatory Time Stamping
- Insurance First Notice of Loss
- KYC Utility
- Smart Lending

Consumer and Industrial Products

- Art Tractive

Blockchain fundamental applications

Value Exchange

- **Exchange assets among peers** in a decentralized, censorship-resistant ledger
- **Code complex value-transfer arrangements that execute "as programmed"** on a decentralized and auditable platform

Notarization

- **Prove that specific information existed** at the time it was recorded, **and hasn't been altered since**

Cross-Industry

- Supply Chain Traceability
- Loyalty and Rewards
- Identity Management
- Digital Asset Trading
- Whistleblowing Management System
- Bonded Loans Platform
- Rubix: Loyalty and Rewards
- Onboarding (Smart ID)
- Corporate Voting
- Charity DAO
- Room Booking
- Warranty Receipts
- Proxy Voting
- CIC – Real Estate Contracts
- Auditing a Permissioned Blockchain

Life Science Health Care

- Healthcare Data Management
- Public Health Pharmaceutical
- Electronic Medical System

□ Financial Services Industry □ Cross-Industry □ Consumer and Industrial Products Industry □ Life Science Health Care Industry

Some are currently live (albiet in a PoC stage)

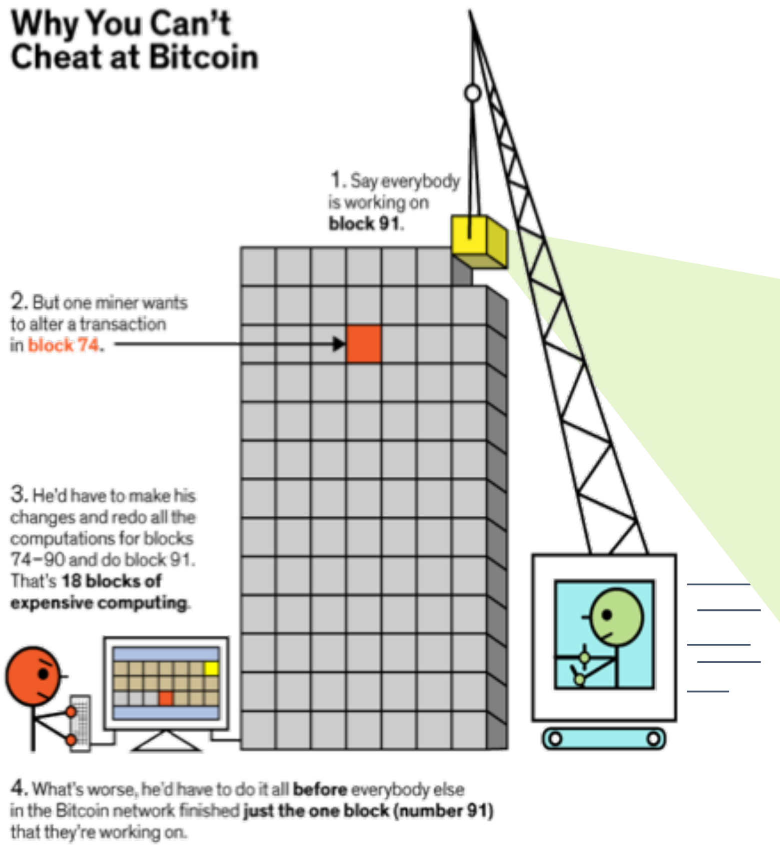
1. Timestamping
2. Digitizing Cash
3. Initial coin offerings

What is a timestamp?

It’s information that provides a temporal order among a set of events that cannot be corrupted.

How proof-of-work blockchains reach consensus, and why they are ‘immutable’

To be able to add a new block to the chain, miners need to solve a computationally-intensive puzzle. Re-writing history is very expensive!



Why You Can’t Cheat at Bitcoin

1. Say everybody is working on **block 91**.

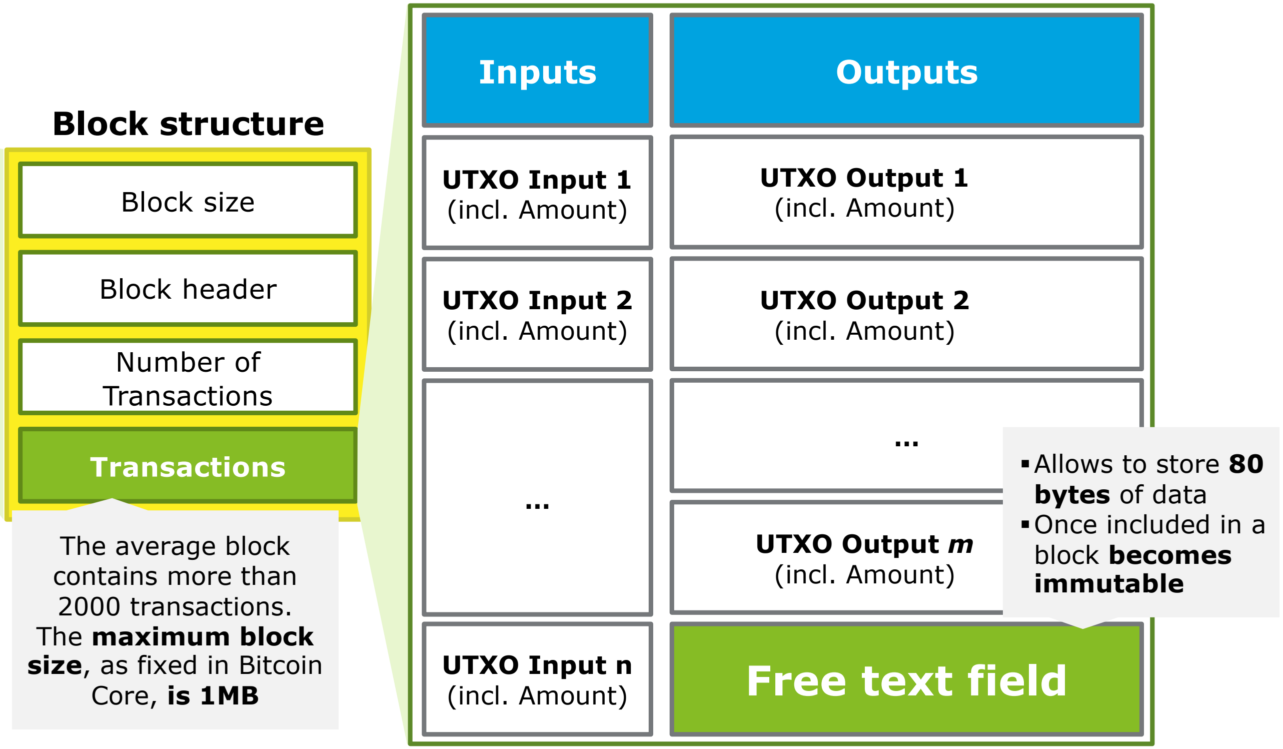
2. But one miner wants to alter a transaction in **block 74**.

3. He’d have to make his changes and redo all the computations for blocks 74–90 and do block 91. That’s **18 blocks of expensive computing**.

4. What’s worse, he’d have to do it all **before** everybody else in the Bitcoin network finished **just the one block (number 91)** that they’re working on.

Decentralized security is ‘inefficient’ by design !

Bitcoin mining operations alone ‘burn’ 332 megawatts/h, around the equivalent of 268,990 American homes



Block structure

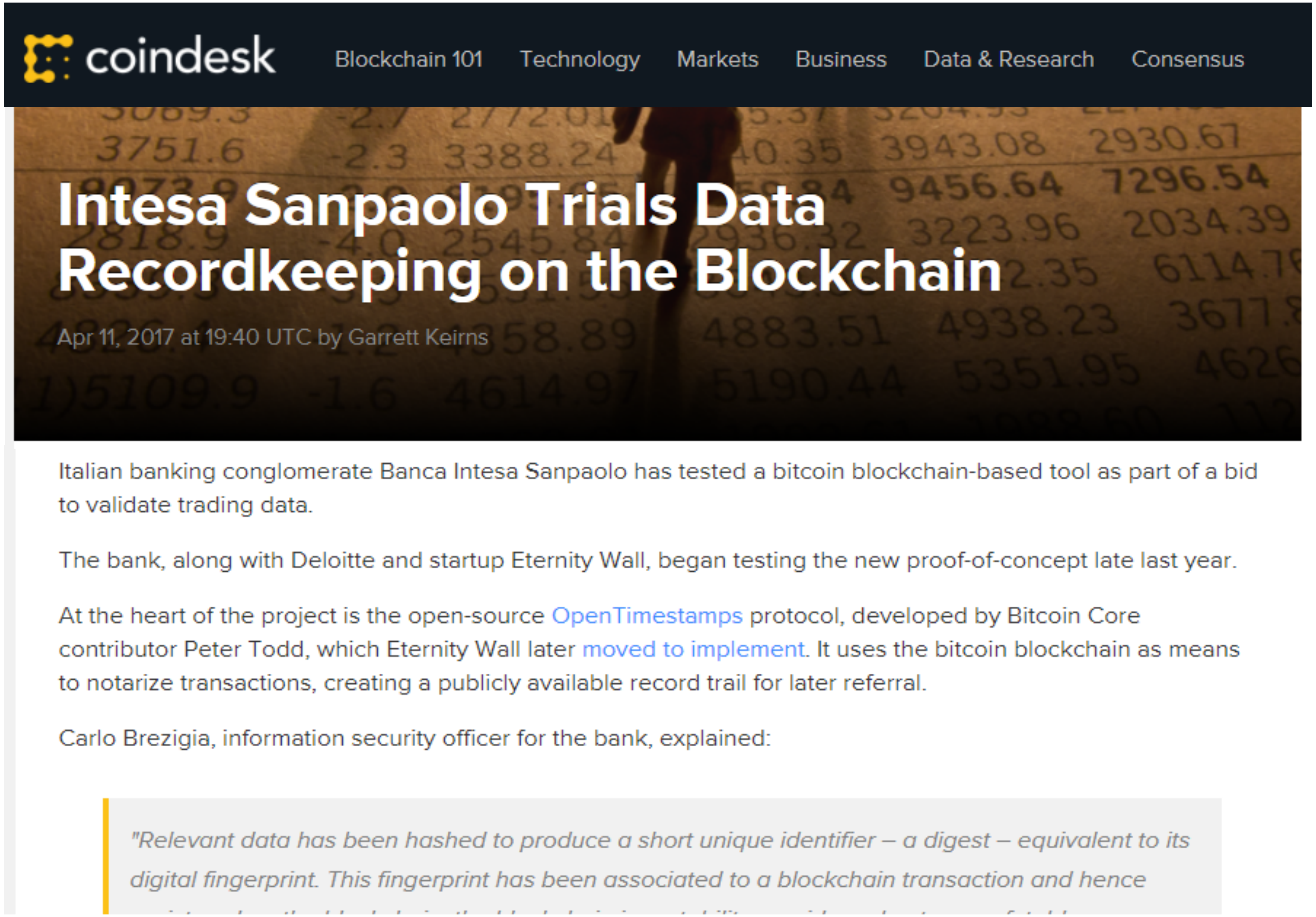
- Block size
- Block header
- Number of Transactions
- **Transactions**

The average block contains more than 2000 transactions. The **maximum block size**, as fixed in Bitcoin Core, **is 1MB**

Inputs	Outputs
UTXO Input 1 (incl. Amount)	**UTXO Output 1** (incl. Amount)
UTXO Input 2 (incl. Amount)	**UTXO Output 2** (incl. Amount)
…	…
	UTXO Output *m* (incl. Amount)
UTXO Input n (incl. Amount)	**Free text field**

- Allows to store **80 bytes** of data
- Once included in a block **becomes immutable**

What we’ve done so far



Intesa Sanpaolo Trials Data Recordkeeping on the Blockchain

Apr 11, 2017 at 19:40 UTC by Garrett Keirns

Italian banking conglomerate Banca Intesa Sanpaolo has tested a bitcoin blockchain-based tool as part of a bid to validate trading data.

The bank, along with Deloitte and startup Eternity Wall, began testing the new proof-of-concept late last year.

At the heart of the project is the open-source OpenTimestamps protocol, developed by Bitcoin Core contributor Peter Todd, which Eternity Wall later moved to implement. It uses the bitcoin blockchain as means to notarize transactions, creating a publicly available record trail for later referral.

Carlo Brezigia, information security officer for the bank, explained:

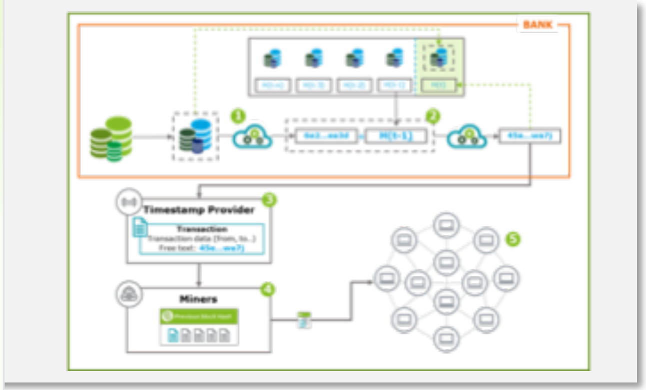
> *"Relevant data has been hashed to produce a short unique identifier – a digest – equivalent to its digital fingerprint. This fingerprint has been associated to a blockchain transaction and hence*

Timestamping at a glance

Hash creation process and verification process

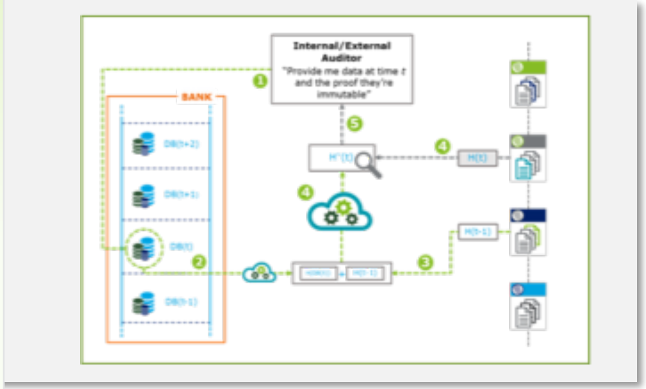
Timestamping Process

1. The Bank makes a back up of its database and, by mean of **hash functions**, **converts it into an alphanumerical string** (i.e. hash value).
2. The Bank **concatenates** this string with the **previous day hash H(t-1)** and calculates the resulting hash.
3. The output string **H(t)** is sent to an **external provider that includes it as metadata in a transaction.**
4. The transaction **is propagated over the network** and **reaches the miners** that include it in a **new block.** The first miner that adds this new block to the chain sends it to all other nodes.
5. **Every node adds this new block** to its local copy of the blockchain.



Verification Process

1. Any auditor may ask for the data **immutability proof** at a certain date/time.
2. The authority is granted with the **access to the database** archive, **restores the backup** of the relevant date (i.e. DB(t)) and processes it through the **hashing function** giving H(DB(t)).
3. The authority **recovers the last timestamped hash value** on the blockchain (i.e. H(t-1)).
4. By **concatenating H(DB(t)) and H(t-1)** and hashing the resulting string, the auditor will find **the exact H$^{\sim}$(t)** that matches the one published on the Blockchain for date *t*.
5. The **equivalence** between the published hash and the calculated one **ensures data integrity** for the specific date and any previous date.


Internal/External Auditor
"Provide me data at time t and the proof they're immutable"
1
BANK
DB(t+2)
DB(t+1)
DB(t)
DB(t-1)
2
H(DB(t))
H(t-1)
3
H(t-1)
4
H~(t)
H(t)
4
5

What’s in store?

Other sectors are testing PoW permissionless timestamping as a cheap and secure solution to data notarization

Private and pubic certification authorities

Postal Services

Governments

What’s in store ?

Edu-Chain: use timestamping to share education certificates in a transparent and secure manner

Private and pubic certification authorities

The prototype aims to simplify and **streamline the Minimum Competency Code** (MCC) process, leveraging on **blockchain technology**

The solution will be designed with the **Bank of Ireland** (employer) as well as the **Institute of Banking** (academia)

We are designing the blockchain solution based on **best in class technology** and build the **architecture on agile technology**

Digitizing Cash

Virtual money that will replace physical cash

Digital cash could address some key problems faced by the Italian Financial Services Industry …

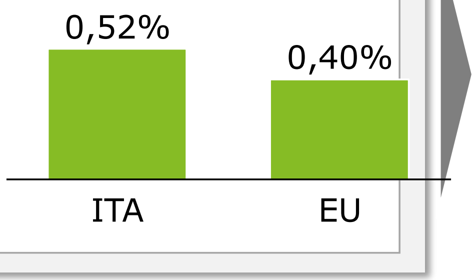
Issue | The Italian context | Benefits of digital cash

Social costs of cash

- Cash is the **main payment instrument in Italy** (83% of retail transactions)
- **Very high social costs for Italian system,** ~8 Mld € (divided by banks and infrastructures ~60% and companies and merchants ~40%)

Cash costs

(% GDP, 2009[1])



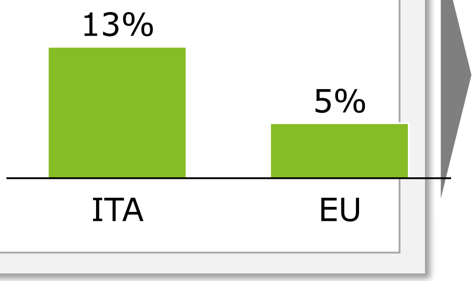
- Digital cash could be an **alternative to physical cash, reducing** social costs

Slow financial inclusion process

- Italy has one of **the highest percentage of unbanked money populations** in Europe
  - Strong regional differences (~27% South and Islands; ~7% Center; ~6% North)
  - Constant number of banked people in the last years (~1% CAGR$_{2010\text{-}2014}$)

Unbanked population

(% > 15 years, 2014)



- Digital cash **could introduce the unbaked** to different **payment instruments**

[1] Last available data, report 2012

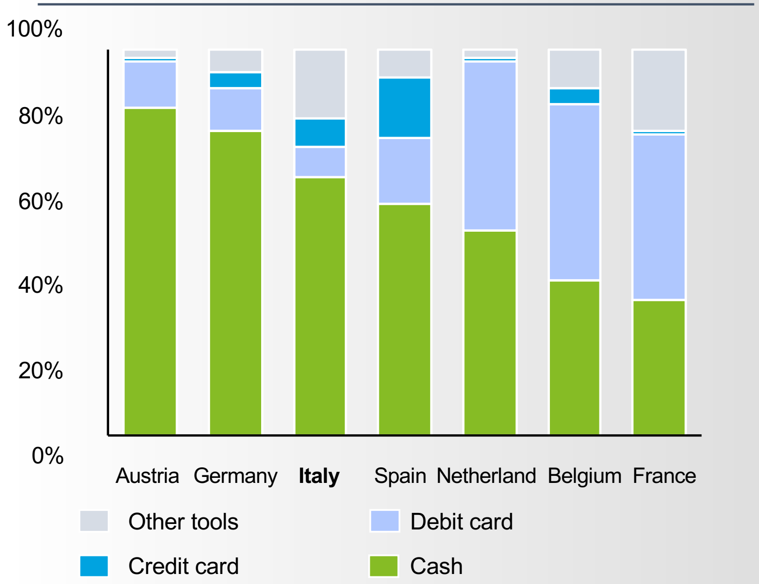
Source: data from ECB, Banca d'Italia, EIU, World Bank

…but no payment solutions have been developed that replicate the cash digitally yet, which is still the most widely used face-to-face tool

Cash still results as the most used payment instrument ….

Tools used for retail transactions in Europe

Percentage use for payment instruments



Sources: European Commission Survey on merchants

… there are examples of possible evolutionary scenarios to create a widely accepted digital equivalent

According to Yves Mersch, in order to create the real analog of cash in the digital world, it is essential to implement a solution that is "Value Based" and not "Account Based" (like all other digital money solutions). This solution must preserve the anonymity of the transactions.

*"**Cash is value based** and accounts are not involved. […] Anonymity towards the central bank can be achieved only with value-based."*

Yves Mersch

Member of the Executive Board
of the European Central Bank

The digitization of cash is the natural evolution of traditional payment systems

Main payment systems and digital cash[1]

Features	Credit Card	Debit Card	Mobile Wallets[2]	Online Wallets[3]	Cash	Digital cash
Bearer instrument	✗	~[4]	✗	✗	✓	✓
Available to unbanked	✗	~[4]	✗	✗	✓	✓
Privacy preserving	✗	~[4]	✗	✗	✓	✓
Proximity payments	✓	✓	✓	✗	✓	✓
Remote payments	✓	~[4]	✗	✓	✗	✓
Instant P2P payments	✗	✗	✓	✓	✓	✓

Our idea for Digital Cash

Digital currency	**Monetary credit** for instant payments, performed through **mobile wallets** and available to **every phone number holder**
Value Based	Presence of an **embedded value**
Collateralized	**Euro deposits** and **convertibility** at ***par value*** with Euro
Efficient	**No transaction fees. Low fees** apply for top-ups or withdrawals (i.e. during conversion between Euro and digital Euro and vice versa)
Partially traceable	Some **controls** can be enforced (trade off between controls and security to be studied)
DLT	**DLT Arrangement** underlying the technology

[1] Extract from a detailed analytical benchmark

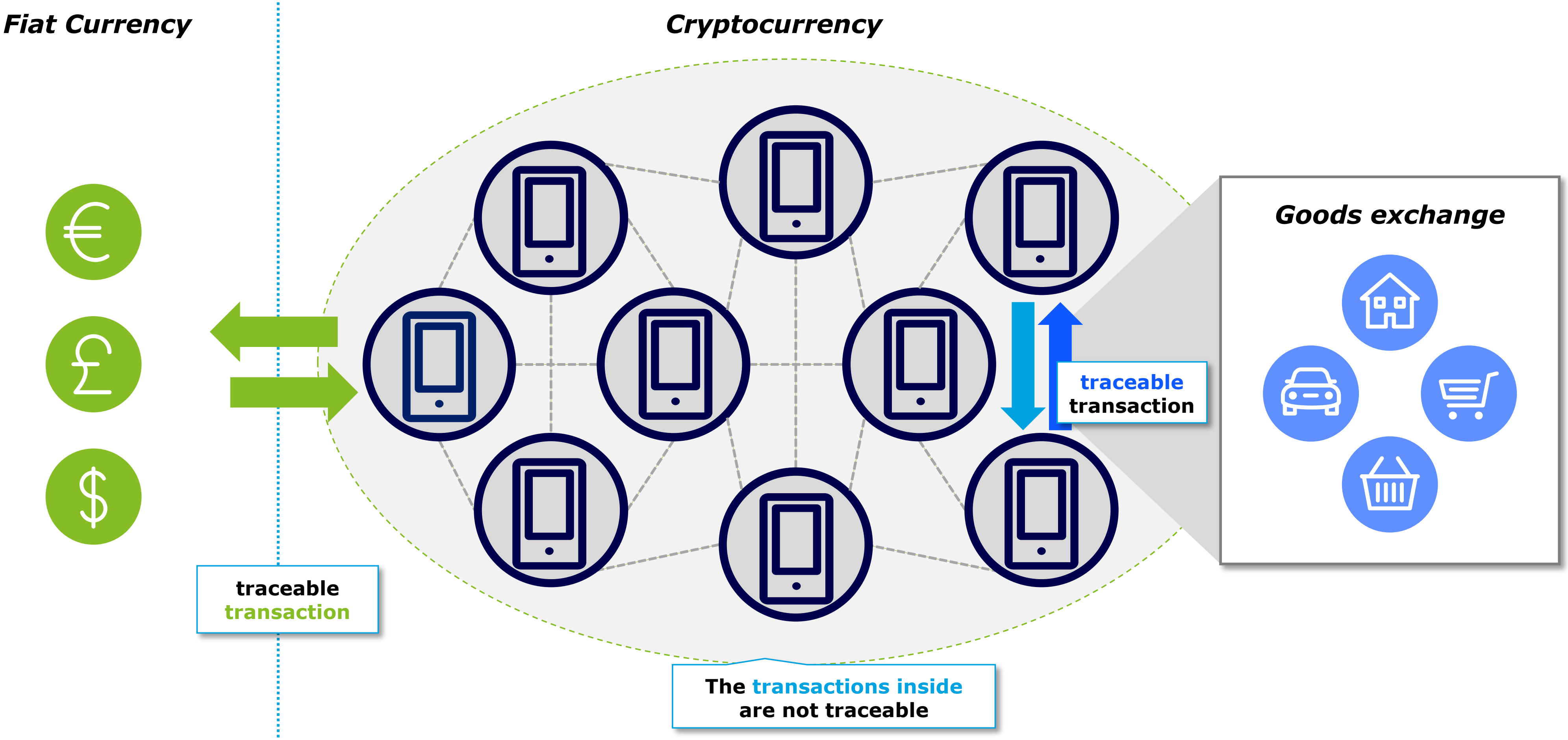
[2] E.g. Satispay

Sources: Benchmark payment instruments, Monitor Deloitte

[3] E.g. Paypal

[4] Possible with some cards (e.g. paysafecard)

What will always remain controllable is the point of contact between the world of cryptocurrencies and the real world



Fiat Currency

Cryptocurrency

Goods exchange

traceable transaction

traceable transaction

The transactions inside are not traceable

Initial Coin Offerings

At the frontier of fundraising

An Initial Coin Offering (ICO) is a new mean to raise funds by issuing new crypto-tokens

Objectives

- ✓ **Raise funds** to **launch** a new **product/ service**
- ✓ **Leverage** on **crypto-tokens** to **support** a **new operating model**

Main features

- **Start ups** launch an **ICO campaign** to attract **a community of investors,** leveraging on a **business plan**
- ICO processes generate a **new currency** or a **token** which gives access to certain **functionally** to the **future users** of the service/ product
- A **percentage** of the newly issued **token** is **sold** to **investors**, in exchange for **legal tender** or (more often) other **cryptocurrencies**
- **Tokens** are usually listed and **traded** on independent **exchange** platforms

ICOs are often compared and sometimes confused with IPOs, but they fundamentally different

IPO – Initial Public Offering

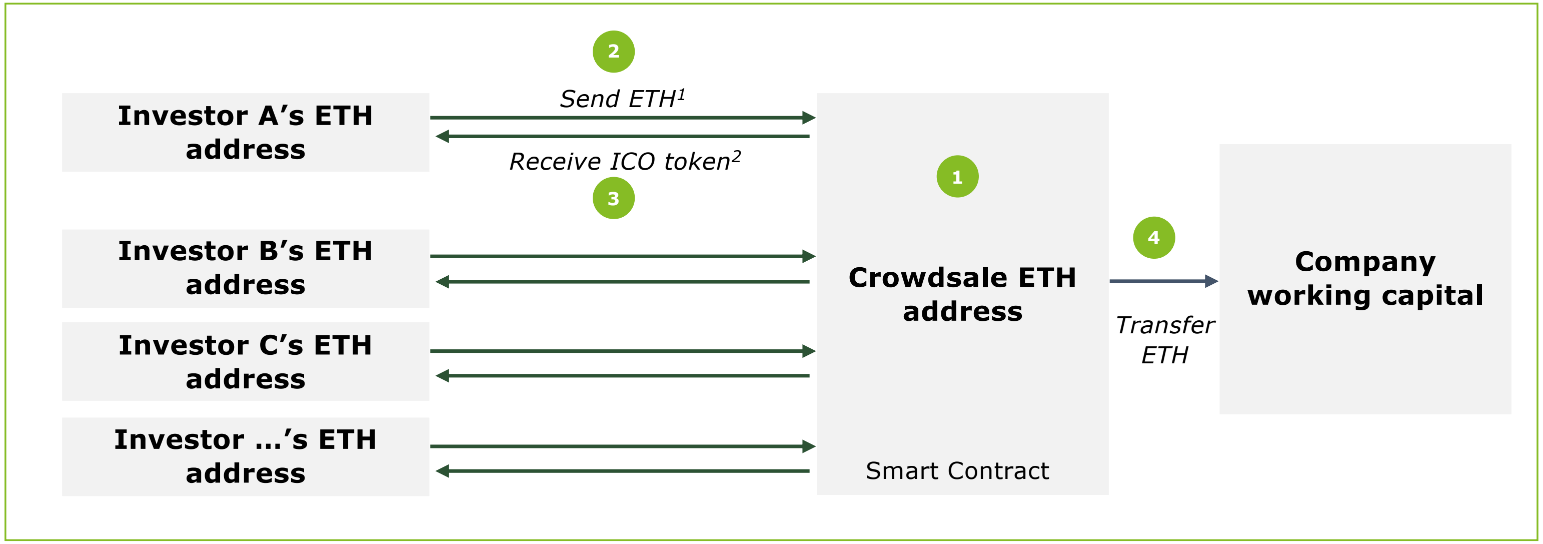
- The company sells its **ownership shares or equity percentage** in exchange for additional capital from investors
- Investors in the company **gain cash value** from the **share value** and **dividends** as the company grows
- The **stakeholders' equity** increase is reflected on the **balance sheet**
- Successful start ups receive **multiple rounds of funding** until the company can gain enough transaction for an IPO

vs

ICO – Initial Coin Offering

- The company has a **unique business value proposition** that relies on the **token** as a **core part** of its **future operating model**
- The token is sold as a way to incentivize **new product users**, participate with the **ecosystem** and **augment the utility** of their technology
- Stakeholders **gain product value**, not necessarily cash value, by being able to spend their purchased tokens

Ethereum is the most commonly used platform to launch ICOs



1 The project creates a **Smart Contract** which has an address for **receiving funds** and displays it on a web page. It is like opening a bank account and displaying it on a web page for people to send money

2 Investors **send ETH** to the published address

3 The company creates **the token[2] and the investor can control his tokens** with **his personal account. Once he receives** the tokens, the investor can **transfer them to any other ether addresses**

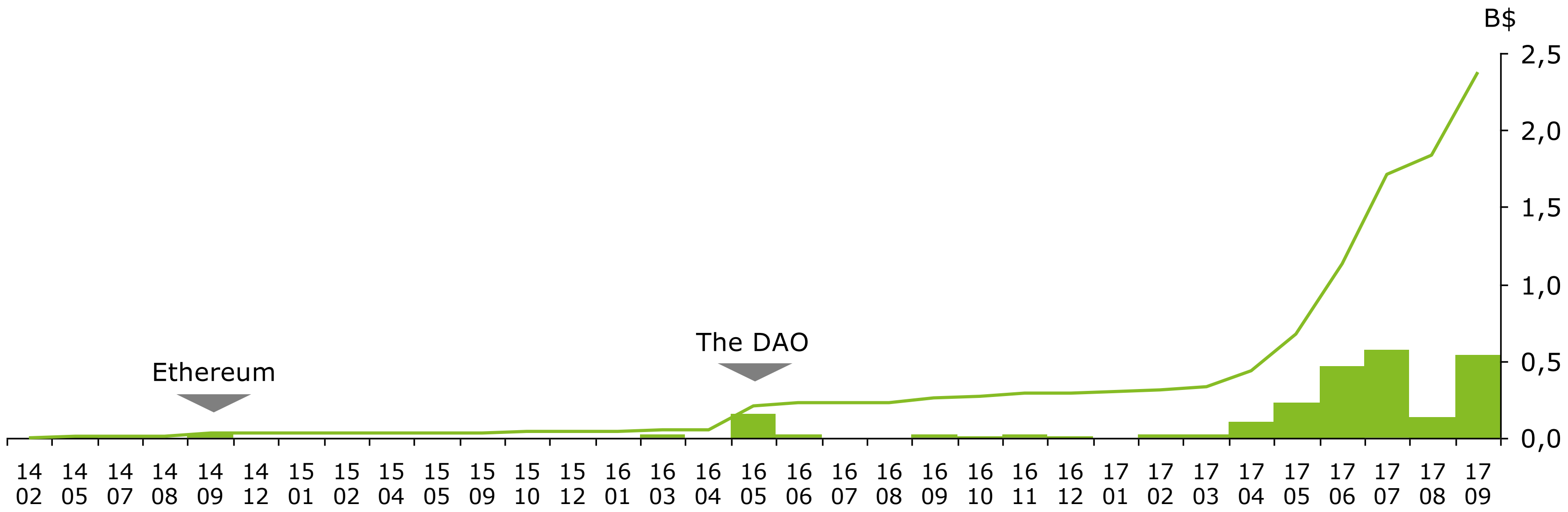
4 The company using the **ETH** to **pay staff/ providers** on the eco-system could **sell the token** for fiat currency on a cryptocurrency exchange to fund the project

[1] Process based on ETH blockchain

[2] The tokens issued by the project to investors are generally created and tracked in one of the following two ways:

- as the intrinsic token of an entirely new blockchain
- or as a token on top of an existing blockchain (e.g. smart contract on Ethereum blockchain)

The ICO market is growing fast with respect to the number of total launches and average funds raised, with a strong acceleration in 2017



Number of ICOs	3	3	4	2	5	3	9	9	2	8	5	13	20	31	35	16	35
Min size*	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0
Average size*	52	6	1	1	5	4	2	1	1	2	4	8	12	15	16	8	15
Max size*	152	16	1	1	11	8	9	2	2	5	15	23	53	153	232	26	262

50% of ICOs raised less than*	2,3	1,1	0,6	0,7	3,5	4,7	1,3	0,6	1,2	1,6	1,1	5,6	4,7	1,8	4,7	5,8	3,1
% ICOs that raised less than 2M	33	67	100	100	20	33	78	100	50	63	60	23	45	52	31	38	40

(*M$, rounded)

Several factors are crucial for a successful ICO

Driver	SILVERCOIN	WeTrust	Indorse	GNOSIS	civic	basicattentiontoken	KIN
1 Clearness of the solution	▮▯▯	▮▯▯	▮▮▯	▮▮▮	▮▮▮	▮▮▮	▮▮▮
2 Fact based business idea	✗	✗	✗	✗	✓	✓	✓
3 The token has value in the ecosystem	✗	✓	✓	✓	✓	✓	✓
4 Clearness of token function	▮▯▯	▮▯▯	▮▯▯	▮▮▯	▮▮▯	▮▮▮	▮▮▮
5 Pre-existing solution	✗	✗	✗	✗	✗	✓	✓
6 Strategic partnership	✗	✗	✓	✓	✓	✓	✓
7 Team knowledge and experience[1]	•	⬤	●	●	•	⬤	⬤
Fund raised	$0,2 Mln	$4,7 Mln	$7,9 Mln	$12 Mln	$33 Mln	$35 Mln	$100 Mln

Legend

▮▮▮ High ▮▮▯ Medium ▮▯▯ Low ⬤ High experience ● Standard experience • Low experience

Source: Deloitte Benchmark

At the same time, some external factors that have commonly caused ICO failures should be well monitored by start-ups

Common factors that can cause an ICO failure:

Regulation

- ✓ Tokens considered **securities** by **regulators** and exchange platforms delist them, avoiding legal issues
- ✓ Other **regulation issues** have impact on the **business model** and the **token role** within the **target operating model**

Reputation

- ✓ ICOs without a **strong reputation** and market confidence are often considered **scams** and delisted from exchange platforms

Hacking

- ✓ Possible **hacking** of smart contract **codes** and theft of tokens
- ✓ Possible **hacking** of **exchange platforms** and loss of tokens

Paolo Gianturco
Senior Partner

Fintech & FSI Tech Leader, EMEA Blockchain Lab co-leader

pgianturco@deloitte.it