Blockchain: Bitcoin and Beyond

University of Pisa – P2P Systems and Blockchains

Pisa, May 17, 2019

Vincenzo Di Nicola, Conio Co-CEO

@vincenzo
It allows **to transfer** the property of a digital asset. 

**In an irrefutable way**  
**Without forgery**  
**Without intermediaries**
Blockchain, IT innovation that involves many sectors.

- **Economy** (Private global currency)
- **Finance** (IPO and Stock Exchange trading)
- **Politics** (Direct vote)
Seemingly impossible.

How to solve the following digital challenges?

No Double Spending
(Sequence of bits cannot be used more than once by the same person)

No Counterfeiting
(Legit sequence of bits cannot just be “printed out”)

Rest
(Sequence of bits can be “divided”)
Actually possible. A quick view:

Digitally sign a message.
Vincenzo gives 1 Denarius to Jeff.

Add a serial number to the message before.
Vincenzo gives 1 Denarius to Jeff with serial number 5429013.

Use a central entity.
1. Jeff verifies that Vincenzo really owns Denarius 5429013 and has not used it.
2. Jeff tells the central entity to update its records.

Decentralization. Everyone part of the “central” entity.
1. Jeff broadcasts the information to the whole network
2. If all is good, the network gives the ok and the information is updated on a publicly shared ledger (the Blockchain).
Effects on the economy.

International e-commerce (preventing fraudulent payments)

Know-how and jobs (technical skills that can be extended to other sectors)

Competition (greater discipline of national currencies)
THIRTY years from now, Americans, Japanese, Europeans, and people in many other rich countries, and some relatively poor ones will probably be paying for their shopping with the same currency. Prices will be quoted not in dollars, yen or D-marks but in, let’s say, the phoenix. The phoenix will be favoured by companies and shoppers because it will be more convenient than today’s national currencies, which by then will seem a quaint cause of much disruption to economic life in the last twentieth century.
07. The challenges of digital assets

The main problem of digital assets

Key challenges that Conio solves:

- Theft
- Forgetfulness
- Inheritance

The £625m lost forever - the phenomenon of disappearing Bitcoins

Immensely strong security means there's no hope of recovering Bitcoins if you lose the password - and it happens a lot more often than you'd imagine.
What's Bitcoin?
Bitcoin is accessible from a private key.
What’s Bitcoin

1E99423A4ED27608A1
5A2616A2B0E9E52CED
330AC530EDCC32C8F
FC6A526AEDD
Simplifying the private key: mnemonic.
12. What’s Bitcoin

Write down your recovery Bitcoin code
Write it on a piece of paper and keep it safe

Which is the word at position 1

Which is the word at position 1
13. Challenges

It’s **safe**. Isn’t it?

Technologically yes, in practice no.
14. Challenges

Physical theft

A CRYPTO NERD'S IMAGINATION:
His laptop's encrypted. Let's build a million-dollar cluster to crack it.

WHAT WOULD ACTUALLY HAPPEN:
His laptop's encrypted. Drug him and hit him with this $5 wrench until he tells us the password.

NO GOOD! IT'S 4096-BIT RSA!

BLAST! OUR EVIL PLAN IS FOILED!

GOT IT.
Forgetfulness
16. Challenges

Inheritance
With great power comes great responsibility.

Are you sure you know how to handle Bitcoin (or any digital asset) on your own?
An answer Made in Italy.

Making hard things trivial is the basis on which we started Conio. Now we are 16.

- Brought back talents in Italy
- Trained young people
- SDK/platform integration with Bank applications
- App awarded in San Francisco
SW solution:
2 pending patents

Iron age:
Physical device

Stone age:
Offline storage
And now banks are probing a new frontier

Custody, or the business of keeping financial assets safe and accounted for. Analysts say that if the banks get it right, providing services comparable to mainstream custody specialists like BNY Mellon or State Street, they could unlock billions of dollars of investment in crypto from funds required by law to keep assets with a qualified custodian. And hence a whole new world of fees.
21. Wall Street and digital asset custody

"We believe that a custody offering is a logical precursor to digital asset market making."

- Goldman Sachs
Conio solution: Keys divided into three parts.

- **01** Client key
- **02** Conio key
- **03** Backup key

**COMMON TRANSACTION**

**RECOVERY TRANSACTION**
Custody solution resilient to both internal and external attacks

A further divided key, unknown to anyone and manageable through a quorum.
Custody solution for all types of digital assets:

01 Cryptocurrencies
02 Digital coins
03 Security tokens
National Cryptocurrency?

There has been a lot of talking about it recently. How to make it happen?

Central institution takes fractions of Bitcoin

Communicate that it has a value

National currency is so "coined"

Or, even without a central institution:

Seigniorage distributed among each person who participates in the network
Central banks have to work quickly to establish digital cash for burgeoning networks of private financial transactions or risk their mushrooming into trading networks that were inherently unstable.

The advantage is clear. Your payment would be immediate, safe, cheap, and potentially semi-anonymous. And central banks would retain a sure footing in payments. In addition, they would offer a more level playing field for competition, and a platform for innovation.

- Christine Lagarde
Blockchain was born with Bitcoin. And it is evolving.

- **Smart contracts** (Immutable programs that follow precise rules: e.g. Ethereum, NEO, Tron)
- **Privacy** (Solutions that, unlike Bitcoin, enable anonymity: e.g. Monero, Zcash)
- **Public vs Private** (Everyone can participate vs access restricted: e.g. Hyperledger, Corda)
Smart contracts.
An insurance example:

**Contract**
(Code deployed on the Blockchain)

**Event**
(Train is late)

**Execution**
(Rules of the contract are automatically triggered)

**Result**
(Refund transaction)
Smart contracts *limitations*.

**Immutability**
(bug cannot be fixed)

**Real world vs Virtual world link**
(what is the source of truth in the real world?)

Smart contracts most potential in a 100% virtual environment. For example, Stock Exchange.
30. **Short-term opportunities**

**IPO and global stock exchange.**

Why not digitalize the companies themselves?

- Stocks registered on the Blockchain
- Augment external investment opportunities for SMEs
- Almost unlimited channel to finance innovation

A global Stock Exchange that:
- it is always open 24/7/365, attracts new investments for the economy and retires the old London and New York.
- Switzerland and Malta are already at work.
SIX (Switzerland’s Stock Exchange) is in a unique position in that it runs the entire securities and payments value chain for Switzerland already, and is ideally positioned to create the digital ecosystem for the future, allowing existing and new market participants to develop their business models for the opportunities available in this new environment. These are strengths that we can bring to the digital space and contribute meaningfully to what is one of the most innovative and dynamic environments of our time.”

- SIX CEO
32. Improvements to the Public Administration

Digital Vote?
33. Digital vote

Vote for the Prime Minister

<table>
<thead>
<tr>
<th>Candidate</th>
<th>Votes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cavour</td>
<td>1</td>
</tr>
<tr>
<td>Garibaldi</td>
<td>0</td>
</tr>
<tr>
<td>Mazzini</td>
<td>2</td>
</tr>
</tbody>
</table>

Vote
Seemingly trivial. But **how to:**

- **Guarantee only lawful people can vote?**
- **Ensure vote anonymity?**
- **Prevent visibility of voting trends?**
- **Hide real-time turnout (if required by law)?**

Digital identity and anonymous blockchains may be the answer.
Q&A

vincenzo@conio.com

@vincenzo