Applicazioni Blockchain

A.Marchetti Spaccamela

Blockchain technology

- Bitcoin is history's first permanent, decentralized, global, trustless ledger of records. Since its invention, entrepreneurs in industries around the world have come to understand the implications of this development.
- The nature of blockchain technology has got imaginations running wild, because the idea can now be applied to any need for a trustworthy record. It is also putting the full power of cryptography in the hands of individuals, stopping digital relationships from requiring a transaction authority for what are considered 'pull transactions'.

Blockchain technology

- Networks connect participants
  - Customers, suppliers, banks, consumers
- Markets organize trades
  - Public and private markets
- Value comes from assets
  - Physical assets (house, car ...)
  - Virtual assets (bond, patent ...)
  - Services are also assets
- Transactions exchange assets

Distributed ledgers

- Ledger records all business activity as transactions
  - Databases
- Every market and network defines a ledger
- Ledger records asset transfers between participants
- Problem: (Too) many ledgers
  - Every market has its ledger
  - Every organization has its own ledger
- Every party keeps its own ledger and state
- Problems, incidents, faults
  - Diverging ledgers

Blockchain provides one ledger

- One common trusted ledger
- Today often implemented by a centralized intermediary
- Blockchain creates one single ledger for all parties
- Replicated and produced collaboratively
- Trust in ledger from
  - Cryptographic protection and Distributed validation

Four elements characterize Blockchain

Replicated ledger

- History of all transactions
- Append-only with immutable past
- Distributed and replicated

Consensus

- Decentralized protocol
- Shared control tolerating disruption
- Transactions validated

Cryptography

- Integrity of ledger
- Authenticity of transactions
- Privacy of transactions
- Identity of participants

Business logic

- Complex operations executed together with transactions
- From simple "coins" to self-enforcing "smart contracts"

Applications areas

Logistics

- Real-time visibility Improved efficiency transparency & verifiability
- Reduced cost

Property records

- Digital but unforgeable: fewer disputes
- Transparency & verifiability
- Lower transfer fees

Capital markets

- Faster settlement times Increased credit availability Transparency & verifiability No reconciliation cost

Key aspects: cryptography

- Cryptography is a key technology in the financial world: ATM security, smart cards, online banking ...
- Trust model of (financial) business has not changed – Trusted intermediary needed for exchange among non-trusting partners
- Today cryptography mostly secures point-to-point interactions
- Bitcoin introduces use of cryptography for a new trust model (= trust no entity)
- The promise of Blockchain – Reduce trust and replace it by technology
- Exploit advanced cryptographic techniques

Key aspects: Digital identity

- Cryptographic keys in the hands of individuals allow for new ownership rights and a basis to form interesting digital relationships.
- Blockchains provide an opportunity to establish a strong system for digital identity that is NOT based on accounts and permissions associated with accounts
- ownership of private keys is ownership of the digital asset,
- a new and secure way to manage identity in the digital world that avoids exposing users to sharing too much vulnerable personal information.

Key aspects: Data management

- Token: Items (transactions) are paired with a corresponding digital token.
- These digital tokens are useful for supply chain management, intellectual property, and anti-counterfeiting and fraud detection.
- blockchain technology represents a revolution in how information is gathered and collected. It is less about maintaining a database, more about managing a system of record.

Key aspects: Governments

Governments have an interest in blockchain technology.

- There is the ownership rights surrounding cryptographic key possession, revocation, generation, replacement, or loss.
- There is interest in who can act as part of a blockchain network.
- Governments often regulate transaction authorization through compliance regimes (eg stock market regulators authorize the format of market exchange trades).
- Bitcoin itself is an example of automated governance, or a DAO (decentralized autonomous organization). It, and other projects, remain experiments in governance, and much research is missing on this subject.

For this reason, regulatory compliance is seen as a business opportunity by many blockchain developers.

Key aspects: Data management

- Token: Items (transactions) are paired with a corresponding digital token.
- These digital tokens are useful for supply chain management, intellectual property, and anti-counterfeiting and fraud detection.
- blockchain technology represents a revolution in how information is gathered and collected. It is less about maintaining a database, more about managing a system of record.

Key aspects: smart contracts

Blockchains are where digital relationships are being formed and secured.

- Smart contracts: use information and documents stored in blockchains to support complex legal agreements.
- Ethereum: applying business logic on a blockchain, so that transactions of any complexity can be coded, then authorized (or denied) by the network running the code.
- Ethereum's primary purpose is to be a platform for smart contract code, comprising of programs controlling blockchain assets, executed by a blockchain protocol, and in this case running on the ethereum network.

Beyond Bitcoin

- Many proposals
- Permissioned vs permissionless
- Permissionless: everybody can be a node and a validator
- Permissioned: there are constraints
  - Everybody can read: Yes
  - Everybody can be a node: Yes/No
  - Everybody can be a validator: Yes/No
- Permissionless: all No (Bitcoin)
- Permissioned: various degree

Ethereum: smart contracts

- Ethereum is a Turing-complete contract processing and execution platform based on a blockchain ledger.
- It is not a clone of Bitcoin, but a completely independent design and implementation.
- Ethereum has a built-in currency, called ether, which is requiredin order to pay for contract execution.
- Ethereum's blockchain records contracts, which are expressed in a low-level, byte code–like, Turing-complete language.
- Essentially, a contract is a program that runs on every node in the Ethereum system.
- Ethereum contracts can store data, send and receive ether payments, store ether, and execute an infinite range (hence Turing-complete) of computable actions, acting as decentralized autonomous software agents.

Ethereum: smart contracts

- Smart contracts help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman.
- No smart contracts: you go to a lawyer or a notary, pay them, and wait while you get the document
- With smart contracts, you simply drop a bitcoin into ledger, and your escrow, driver's license, or whatever drops into your account.
- Smart contracts not only define the rules and penalties around an agreement in the same way that a traditional contract does, but also automatically enforce those obligations.

Ethereum: smart contracts

Example

- Suppose you rent an apartment from Bob. You can do this through the blockchain by paying in cryptocurrency.
- You get a receipt which is held in the virtual contract; Bob gives you the digital entry key which comes to you by a specified date.
- If the key doesn't come on time, the blockchain releases a refund. If Bob sends the key before the rental date, the function holds it releasing both the fee and key to you respectively when the date arrives.
- The system works on the If-Then premise and is witnessed by hundreds of people, so you can expect a faultless delivery.
- If Bob gives you the key, he is sure to be paid. If you pay certain you receive the key.

Ethereum: applications

There are many Ethereum-based applications that you can use today. Example:

- Gitcoin: a network of incentivized open-source developers
- Cent: a social network where you earn money by posting
- Veil: a trading platform that lets you place bets on real world events
- CryptoKitties: a game where you collect and breed digital collectible cats
- Adchan: A token curated publisher registry that optimizes digital advertising.

Ethereum: currency

- Ether is Ethereum's native currency. It is "digital money" that can be sent over the internet and also be used in Ethereum-based applications.
- In the Ethereum blockchain, instead of mining for bitcoin, miners work to earn Ether, a type of crypto token that fuels the network.
- Ether is a tradeable cryptocurrency, Ether is also used by application developers to pay for transaction fees and services on the Ethereum network.
- miners are also paid in Gas; Gas is a unit that measures the amount of computational effort that it will take to execute certain operations; every smart contract execution requires a certain amount of gas to be sent along with it to (paid by the people signing the contract)

Ethereum: conclusions

- Ethereum is a public, permissionless blockchain.
- In Ethereum ALL smart contracts are stored publicly on every node of the blockchain, which has costs.
- The downside is that performance issues arise in that every node is calculating all the smart contracts in real time, resulting in lower speeds and high transctions costs. · Dec 16 version improves efficiency
- Some groups, mostly industry consortia, have adapted Ethereum's open-source protocol to run their own permissioned, private instance of Ethereum.

Hyperledger project

- Popularity of Bitcoin, Ethereum motivate the interest in applying the blockchain technology - distributed ledger and distributed application platform - to more innovative *enterprise* use cases
- However, many enterprise use cases require performance characteristics that the permissionless blockchain technologies are unable (presently) to deliver.
- In addition, in many use cases, the identity of the participants is a hard requirement, such as in the case of financial transactions where Know-Your-Customer (KYC) and Anti-Money Laundering (AML) regulations must be followed.

Hyperledger project

Enterprise using blockchain technology are interested in the following requirements:

- Participants must be identified/identifiable
- Networks need to be *permissioned*
- High transaction throughput performance
- Low latency of transaction confirmation
- Privacy and confidentiality of transactions and data pertaining to business transactions

While many early blockchain platforms are currently being *adapted* for enterprise use, **Hyperledger Fabric** has been *designed* for enterprise use from the outset.

Hyperledger project: Fabric

- **modular** and **configurable** architecture, enabling innovation, versatility and optimization for a broad range of industry use cases including banking, finance, insurance, healthcare, human resources, supply chain and even digital music delivery.
- first distributed ledger platform to support **smart contracts authored in general-purpose programming languages** such as Java, Go and Node.js, rather than constrained domain-specific languages (DSL).
- This means that most enterprises already have the skill set needed to develop smart contracts, and no additional training to learn a new language or DSL is needed.

Hyperledger project: Fabric

- Bitcoin is permissionelss = everybody is anonymus ad can participate wthout asking permission
- Fabric is **permissioned**, meaning that, unlike with a public permissionless network, the participants are known to each other, rather than anonymous and therefore fully untrusted.
- This means that while the participants may not *fully* trust one another (they may, for example, be competitors in the same industry), a network can be operated under a governance model that is built off of what trust *does* exist between participants, such as a legal agreement or framework for handling disputes.

Hyperledger project : Fabric

- Open-source collaboration under Linux Foundation
- www.hyperledger.org
  – Hyperledger unites industry leaders to advance blockchain technology (Dec. '15)
  - 100 members in Jan. '17
- Develops enterprise-grade, open-source distributed ledger technology; permissioned
- Code contributions from several members
- Fabric is the IBM-started contribution – github.com/hyperledger/fabric/ – Security architecture and consensus protocols from IBM Research - Zurich

Hyperledger project: IBM

IBM

- supports the Linux Foundation Hyperledger
- delivers an enterprise-grade blockchain service underpinned by the industry's most secure Linux server
- has an easy to access, proven and incremental engagement model giving customers the confidence to get started NOW
- Fabric is the IBM-started contribution – github.com/hyperledger/fabric/ – Security architecture and consensus protocols from IBM Research - Zurich

Finance: cross border transactions

Infrastructure for cross-border transactions

- The digital revolution has ; web pages in the 1990s; mobile apps in the new millennium.
- But the digital revolution has not yet revolutionized cross-border transactions. Western Union remains a big name, running much the same business they always have. Banks continue to use a complex infrastructure for simple transactions, like sending money abroad.
- Digitization has meant we merely sort information into private databases much faster.
- Blockchain technology allows for financial institutions to create direct links between each other, avoiding correspondent banking.

Finance: digital property

Bitcoin created something unique: digital property.

- Before bitcoin, anything digital could be copied with the click of a button. (EXAMPLE: music industry and album sales)
- Bitcoin created **uncopyable** digital code.
- Now we can own something digital that couldn't be copied. This gave the digital code value: bitcoin's value is based on the capacity of its blockchain to prevent double-spending and the creation of counterfeit coins.
- This ability, however, extends beyond just recording transactions.
- Example: Nasdaqwas one of the first to build a platform enabling private companies to issue and trade shares using a blockchain.

Finance: other aspects

- **Regulations**: Blockchains can serve as a fully transparent and accessible system of record for regulators. For example, in US banks have obligations to report public agencies transaction of more than $10,000,
- **Clearing and Settlement:** With paper-world trading, the time reuired for clearing and settlement of a transaction is generally three days (for risk) . With blockchain technology usign digital asset and digital ownership riskis reduced
- **Accounting and auditing**: most databases are snapshots of a moment in time; blockchain databases are built from their own transaction history. The implications for auditing and accounting are profound.

Ripple

- Today the world sends more than $155 trillion $ across borders. Underlying infrastructure is old
- Ripple connects banks, payment providers and digital asset exchanges via RippleNet to provide one frictionless experience to send money globally.
- Banks join RippleNet to process cross-border payments in real time with end-to-end tracking and certainty.
- Banks can expand payments offerings into new markets that are otherwise too difficult or expensive to reach.
- Permissioned

Ripple

- Today the world sends more than $155 trillion $ across borders. Underlying infrastructure is old
- Ripple is a system, for currency exchange and remittance created in 2012 by Ripple Las, a US-based technology company.
- Ripple connects banks, payment providers and digital asset exchanges via RippleNet to provide one frictionless experience to send money globally.
- Banks join RippleNet to process cross-border payments in real time with end-to-end tracking and certainty.
- Banks can expand payments offerings into new markets that are otherwise too difficult or expensive to reach.
- Permissioned

Ripple

- The ledger employs the decentralized native cryptocurrency known as XRP, which as of September 2018 was the second largest coin by market capitalization (73 Billion US $) now 12.7 Billion US$
- Ripple relies on a common shared ledger, which is a distributed database storing information about all Ripple accounts.
- The network is "managed by a network of independent validating servers that constantly compare their transaction records." Servers could belong to anyone, including banks or market makers.
- Ripple validates accounts and balances instantly for payment transmission and delivers payment notification with very little latency (within a few seconds).
- A class-action lawsuit was filed against Ripple in May 2018 "alleging that it led a scheme to raise hundreds of millions of dollars through unregistered sales of its XRP tokens. [creating] billions of coins 'out of thin air' and then profited by selling them to the public in 'what is essentially a never-ending initial coin offering'.