Digital Currencies

Transforming the Future of Money
WAAS & Future Capital Initiative Initiative
Dubrovnik, November 18-20, 2019

Georgios THEODOROPOULOS
Chair Professor
Dept. of Computer Science and Engineering
SUSTech, Shenzhen, China
Money

The money flower: a taxonomy of money

Adaptation from Bank for International Settlements (2017)

Transforming the Future of Money - Digital Currencies
Professor Georgios K. Theodoropoulos
Cryptocurrencies are virtual currencies, **digital representations of value**, not issued by a central bank, credit institution or e-money institution, which in some circumstances can be used as an **alternative to money**. Unregulated, digital money, which is issued and usually controlled by its **developers**, and used and accepted among the members of a **specific virtual community**.

Cryptocurrencies are a subset of virtual currencies which are **digital representations of value**, issued by **private developers** and denominated in their own unit of account.

Cryptocurrencies are **digital currencies** with following features:

- they are assets, the value of which is determined by supply and demand, similar in concept to commodities such as gold, yet with zero intrinsic value;

- **make use of distributed ledgers** to allow remote peer-to-peer exchanges of electronic value in the absence of trust between parties and **without the need for intermediaries**;

- they are **not operated by any specific individual or institution**.
Cryptocurrencies are **virtual currencies, digital representations of value** that are neither issued by a central bank or public authority nor **necessarily attached to a fiat currency** but are used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically.

Adopts EBA definition

Cryptocurrencies are a subset of digital currencies, **digital representations of value that are denominated in their own unit of account, distinct from e-money**, which is simply a digital payment mechanism, representing and denominated in fiat money.

Cryptocurrencies are **math-based, decentralized, convertible virtual currencies** that are protected by cryptography.
Blockchain

• It all started with a 2008 white paper sent by Satoshi Nakamoto to the Cryptography Mailing List.

Bitcoin P2P e-cash paper

Satoshi Nakamoto satoshi at vistomail.com
Fri Oct 31 14:10:00 EDT 2008

• Previous message: Fw: SHA-3 lounge
• Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

“We proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power”
• Bitcoin vs Altcoins: not based on Bitcoin’s open-source protocol
• There are approximately 2,950 cryptocurrencies being traded with a total market capitalisation of $221bn (as of October 8th 2019).
• The top 10 cryptocurrencies represent roughly 85% of the total market value

Source: Cryptocurrencies and blockchain, Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies, PE 619.024 - July 2018
Transforming the Future of Money - Digital Currencies
Professor Georgios K. Theodoropoulos
Blockchain Keywords

- **ledger** – the abstraction at the heart of blockchain systems: a log of transactions that take place between various parties; establishes which transactions happened and in which order. Ledgers are public accessible but tamper-proof.
- **Decentralised, distributed** – divided among many, in multiple locations;
- **mutual** – shared in common, or owned by a community;
- **mutual distributed ledger (MDL)** – a record of transactions shared in common and stored in multiple locations;
- **mutual distributed ledger technology** – a technology that provides an immutable record of transactions shared in common and stored in multiple locations
- **Token**: a unit of value issued by a private organization within blockchain system.
- **Public and Private Keys**
- **Cryptographic hash functions**
- **Consensus protocols (governance)**: Proof of Work, Proof of Stake, etc
Blockchain: How it works

1. A wants to send money to B
2. The transaction is represented online as a ‘block’
3. The block is broadcast to every party in the network
4. Those in the network approve the transaction is valid
5. The block then can be added to the chain, which provides an indelible and transparent record of transactions
6. The money moves from A to B

Source: “Technology: Banks seeks the key to blockchain”, by J. Wild, M. Arnold and P. Stafford, 1 November 2015, Financial Times
<table>
<thead>
<tr>
<th>5 key questions</th>
<th>Permissioned Blockchain</th>
<th>Permissionless Blockchain</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Who maintains it? (edit mode)</td>
<td>1 or a small group of pre-selected and permissioned entities</td>
<td>Anyone that wants</td>
</tr>
<tr>
<td>2) How are they incentivized to do it right?</td>
<td>Reputational risk</td>
<td>“Cryptoeconomics” Direct economic incentive, carrot &amp; stick (e.g. token reward &amp; fees vs power costs in PoW)</td>
</tr>
<tr>
<td>3) Who produces the underlying data? (can send their transactions)</td>
<td>Permissioned group of people (e.g. customers of a bank)</td>
<td>Anyone that wants</td>
</tr>
<tr>
<td>4) Who has access to that database? (read-only)</td>
<td>1 or a small group of pre-selected and permissioned entities (usually the ones that maintain it)</td>
<td>Anyone that wants</td>
</tr>
<tr>
<td>5) Where is it stored?</td>
<td>Central servers</td>
<td>Massively distributed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Features</th>
<th>Permissioned Blockchain</th>
<th>Permissionless Blockchain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need to trust central entity to secure it</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Transaction costs (direct function of cost of maintaining the ledger)</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>Speed</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>Censorship Resistance</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Need to use a token</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Examples</td>
<td>Hyperledger</td>
<td>Bitcoin, Ethereum</td>
</tr>
<tr>
<td>Name</td>
<td>Permissionless / Permissioned</td>
<td>Decentralized</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Bitcoin</td>
<td>Permissionless</td>
<td>✓</td>
</tr>
<tr>
<td>Ethereum</td>
<td>Permissionless</td>
<td>✓</td>
</tr>
<tr>
<td>Ripple</td>
<td>Permissioned</td>
<td>✓</td>
</tr>
<tr>
<td>Bitcoin Cash</td>
<td>Permissionless</td>
<td>✓</td>
</tr>
<tr>
<td>Litecoin</td>
<td>Permissionless</td>
<td>✓</td>
</tr>
<tr>
<td>Stellar</td>
<td>Permissionless</td>
<td>✓</td>
</tr>
<tr>
<td>Cardano</td>
<td>Permissioned / Permissionless</td>
<td>✓</td>
</tr>
<tr>
<td>IOTA</td>
<td>Permissionless</td>
<td>✓</td>
</tr>
<tr>
<td>NEO</td>
<td>Permissioned</td>
<td>✓</td>
</tr>
<tr>
<td>Monero</td>
<td>Permissionless</td>
<td>✓</td>
</tr>
<tr>
<td>Dash</td>
<td>Permissionless</td>
<td>✓</td>
</tr>
</tbody>
</table>

Legend:
- ✓ = Yes
- ✗ = No
- ★ = To a limited extent
- ✗ = No
The Fundamental Challenge: Consensus and Agreement
Consensus and Agreement: The Byzantine Generals Problem

• The systems actors must agree on a concerted strategy, but some of these actors are unreliable.
• The problem [Lamport 1982]
  – three or more (N) generals are to agree to attack or retreat
  – one (commander) issues the order
  – the others (lieutenants) decide
  – one or more (f) generals are treacherous (or faulty!)
    • propose attacking to one general, and retreating to another
    • either commander or lieutenants can be treacherous!
• In a synchronous system: impossibility with \( N \leq 3f \)
• In asynchronous system: impossibility with even one failure!!
Consensus protocols in Blockchain

- Blockchains are decentralized ledgers. Each node participating in the blockchain has an independent copy of the ledger.
- To confirm the validity of transactions attempting to be lodged on the ledger, a solution was needed to ensure that ‘traitors’ could not add their transactions onto the ledger.

*Source: blockgeeks.com*
Hashing, Keys and Signatures

- Hash function is math which takes in data and produces a single number
  - Irreversible
  - Unpredictable
  - Collision probability
- Public Key yields a message only holder can read
- Private Key yields a “digital signature” a message everyone can read but only the holder could have produced
Transactions and Ledgers

Transforming the Future of Money - Digital Currencies
Professor Georgios K. Theodoropoulos
Transaction Validation

Output of Previous Transaction iixj4...
- Hashed public key Aa123...
- Amount: 5 BTC
- Amount transferred to user with hashed public key Aa123
- Claim: Public key of Rob
- Signature
- Claim: Private Key of Rob
- Credentials for the input of unverified Transaction 32aab... The input is the transaction iixj4...

Validation script encapsulated in transaction iixj4...
- Hash Function
- Comparison
- Hash Function
- Comparison
- Decrypt

Transaction id: \textit{rx11}...
Rob \rightarrow Peter 5BTC
- Maria \rightarrow Jenni 2 BTC
- George \rightarrow Peter 3 BTC
- Rob \rightarrow Peter 5BTC

Rob' Wallet
- Public key
- Private key

Digitally signed transaction \textit{rr1xd}...

Digitally signed transaction \textit{rr1xd}...

Rob \rightarrow Peter 5 BTC
Transforming the Future of Money - Digital Currencies
Professor Georgios K. Theodoropoulos
Blockchain

Transforming the Future of Money - Digital Currencies
Professor Georgios K. Theodoropoulos
Blockchain

Start

New block

Hash Number

Is hash < target value?

yes

Problem is solved

Mining reward

no

Modify nonce and try again with a new hash

Header of the most recent block

Mining difficulty

Nonce

Mining difficulty
Blockchain

Smart Contracts

Option contract written as code into a blockchain.

Contract is part of the public blockchain.

Parties involved in the contract are anonymous.

Contract executes itself when the conditions are met.

Regulators use blockchain to keep an eye on contracts.

Happy Hustlin'

https://codebrahma.com
Blockchain

The mining difficulty is set every 2016 blocks (approximately two weeks)

More miners join the network

Block creation rate increases

Average mining time decreases

Block creation rate decreases

Average mining time goes back to normal

Mining difficulty increases
Three nodes solved simultaneously the mathematical problem.

Each node tries to build the next block.

All network node adopt the longest chain (i.e. the one containing B and B1).
Blockchain forks

Source: www.visualcapitalist.com
Perceived Pros

• Seismic shift in finance and business
  – Security and anonymity
  – Protection from fraud, identity theft and counterfeit products
  – Very low transaction fees: Instant, borderless, cost efficient payments and fund transfers
  – It offers e-commerce businesses and traders a lot of autonomy with no third-party interruptions

• Blockchain is viewed as a democracy tech
  – Blockchain ideal world is one in which all economic activity and human interactions are subject to libertarian decentralisation
  – Decentralisation to resist “authoritarianism and evil concentrations of power”
  – Blockchain-based governance
  – “Code is the law”
  – “Blockchain for good”
“Blockchain for good”: Universal Basic Income

- Simplify the welfare system, provide a stable income, replace the current system of social security, unemployment and pension payments, child support and tax spendings
- Several UBI Blockchain initiatives
  - SwiftDemand, Mannabase, Solidar, Circle, Manna, Grantcoin, Democracy Earth, Big Foundation, projectUBU
- Issue their own currency in the form of tokens: instead of recirculating existing money in the economy, they generate new value by minting a new currency.
- Minimum Viable Economy: build enough of an ecosystem around a token
  - Monetary Policy (incentives to accept and spend tokens, airdrops, etc),
  - Liquidity (exchange the token for another currency, stablecoins)
- Identity Verification & Anti-Fraud Challenges: voting and social trust
- Sustainability: align the developers’ interest with their users’ interests
“Blockchain for good”: Impact Investment

- “Impact Tokens”
  - Claim to represent a UN Sustainable Development Goal-related impact, usually in the form of a quantified, unit-based measurement metric, which is linked to its origin
  - Can be used to make performance-based payments, track impacts through supply chains or substantiate claims on supporting SDGs
- Blockchain supports tracking progress and verifying that milestones have been met.
  - **Trust**: automate and accelerate impact measurement and verification, enabling credible accounting of impacts
  - **Attribution of impact**: allocation of an impact-related claim to an investor, often risking the “double-counting” of claims. Impact tokens can be used to track the impact of an investment
  - **Impact monetisation** acceleration, transaction costs removed, transparency and open source to support a broad stakeholder base.
“Blockchain for good”: Impact Investment

- UN’s Principles for Responsible Investment initiative has listed a variety of areas, including energy trading systems, secure recording of educational certificates for local schools and storing and access to medical data.

- **SolarCoin** (SLR), one of the earliest impact tokens. Incentivize solar electricity by rewarding the generators of solar electricity to reduce the cost of electricity production. 1SLR/1MWh. “**Proof of impact**” verification protocol.

- **Sun Exchange** use of impact tokens to fund new solar projects in Africa.

- **ClimateChainCoalition** (UNFCCC Secretariat).

- **GainForest** project explores the conversion of high-resolution satellite data into carbon stock data and impact tokens. Smart contract architecture connects donors from private and public sector with caretakers.

- A blockchain pilot captures and verifies data from **greenhouse gas emission reduction projects** to make the resulting positive impact tangible at the moment it is physically achieved.

- **Building Blocks** platform by the **World Food Programme** to make payments to refugees. Blockchain technology provides unique digital identity to eligible beneficiaries and cut transaction costs for cash transfers.
Blockchain Technologies

- Gartner expects blockchain to become fully scalable technically and operationally by 2028
Blockchain Applications

Transforming the Future of Money - Digital Currencies
Professor Georgios K. Theodoropoulos
Transforming the Future of Money - Digital Currencies

Professor Georgios K. Theodoropoulos
Technological Support

- Tech industry already is a major hub for crypto and Blockchain applications.
- IBM
  - IBM Blockchain World Wire: 72 countries, with 47 currencies. 6 global banks to issue their own stablecoins on IBM Blockchain World Wire
- Google to introduce open source integrations for decentralized apps built with the blockchain platforms Hyperledger, Fabric and Ethereum in the Google Cloud Product marketplace
- Microsoft, Dell and Dish, which are now accepting cryptocurrencies as payment
- Facebook Libra: Permissioned. With 2.4 billion people using Facebook each month, Libra could be a financial game changer
Distributed Systems Cycle

- Centralisation: Mainframe and dump terminals
- Decentralisation: The advent of the PC - and client-server network
- Decentralisation: IoT and edge
- Centralisation: Grid, Cloud and thin clients
Banking

- Blockchain in several key areas in banking and investments services, primarily focused on permissioned ledgers.
- Bank of America holder of most blockchain technology patents
- Gartner sites banking as the most mature industry for Blockchain
  - “We also expect continued developments in the creation and acceptance of digital tokens. However considerable work needs to be completed in nontechnology-related activities such as standards, regulatory frameworks and organization structures for blockchain capabilities to reach the Plateau of Productivity – the point at which mainstream adoption takes off, in this industry.”
Regulation: G20

- G20 leaders issued a joint declaration in which they pledged support for the Financial Action Task Force’s (FATF) recommendations regarding the regulation of crypto assets.

“...while crypto-assets do not pose a threat to global financial stability ...we are closely monitoring developments and remain vigilant to existing and emerging risks. ... We welcome ongoing work by the Financial Stability Board (FSB) and other standard setting bodies and ask them to advise on additional multilateral responses as needed”.

Transforming the Future of Money - Digital Currencies
Professor Georgios K. Theodoropoulos
Regulation: US

- Regulatory frameworks proposed by:
  - The U.S. Internal Revenue Service (IRS)
  - The U.S. Commodity Futures Trading Commission
  - The U.S. Securities Exchange Commission (SEC)
  - The US Financial Industry Regulatory Authority (FINRA)

Donald J. Trump
@realDonaldTrump

I am not a fan of Bitcoin and other Cryptocurrencies, which are not money, and whose value is highly volatile and based on thin air. Unregulated Crypto Assets can facilitate unlawful behavior, including drug trade and other illegal activity....

8:15 AM · Jul 12, 2019 · Twitter for iPhone
Regulation: EU

- Feb 2018, Working Groups
  - Blockchain Policy and Framework Conditions
  - Use Cases and Transition Scenarios

- No specific legislation regarding cryptocurrencies at the EU Parliament level. Cryptocurrencies are broadly considered legal across the bloc, exchange regulations depend on individual member states.
- Single Supervisory Mechanism proposed
Regulation: China

• Blockchain technology strong (e.g. Shenzhen subway)
• 2017 ban on all ICOs, crypto trading, crypto exchanges etc
  – Making of new digital currency for existing cryptocurrencies continued
• October 2019 ban reversed. President Xi directed China to expedite issuing its own digital currency to beat the U.S.-based Facebook’s launch of Libra Coin
• Stock market frenzy followed. Nov 6 People’s Daily warns about the need to avoid speculative behavior in the blockchain sector.
Reality Check: Pitfalls and Fallacies

• Democratic?
  – It provides governments with an almost perfect means of tracking individual and business financial activity.
  – Hard forks can be authoritarian
  – Code is the law: trust?

• Not secure at all

• Immense energy consumption

• Massive centralisation of power among cryptocurrency “miners,” exchanges, developers
Double Spent Attack

- Transactions become more secure with time
- 51% attack. Jan 2019 CoinBase $1.1M

![Diagram showing a double spent attack in blockchain]

Someone pays Bob 2BTC (trans x)
Bob uses transaction x to pay the company (trans y)
Company sees trans y and ships the product
Bob makes a reverse payment z back to him and tries to create a longer chain

Time
Decentralised Autonomous Organisation Attack

```solidity
function withdraw(uint amount) {
    client = msg.sender;
    if (balance[client] >= amount) {
        if (client.call.sendMoney(amount)) {
            balance[client] -= amount;
        }
    }
}
```

Fig. 1. Pseudocode for DAO-like contract

```solidity
function sendMoney(uint amount) {
    victim = msg.sender;
    balance += amount;
    victim.withdraw(amount)
}
```

Fig. 2. Pseudocode for DAO-like exploit

- June 2016 within a few hours, 3.6 million ETH were stolen, the equivalent of $70 million
Energy

• Bitcoin is using around seven gigawatts of electricity, equal to 0.21% of the world's supply.
• That is as much power as would be generated by seven Dungeness nuclear power plants at once.
• Energy use is doubling every six months.
• Far more energy per transaction than all the world's banks put together, when considering the amount of energy used by data centres.
• £1M/day for Ethereum mining
Transforming the Future of Money - Digital Currencies
Professor Georgios K. Theodoropoulos
Hash Rate and Mining Distribution

Source: www.blockchain.com
Performance rests more on processing power and data

Explainability in AI

Large Scale Complex System
Thank You