The New Original Innovator

ETHEREUM CLASSIC

Marcus R. Brown

Blockchain Meetup (Phoenix, Arizona)

September 13th, 2016

Overview

1. **Why Ethereum Classic?**
    - Brief History of Ethereum
    - What Went Wrong
    - Paying Back The DAO Investors
    - What Really Went Wrong
    - Birth of Ethereum Classic

2. **Progress to Date**
    - Principles of Decentralisation
    - Minimizing Points of Failure
    - Technology
    - Community
    - Administration
    - Ecosystem Roadmap (WIP)

ETHEREUM
CLASSIC

Overview (cont'd)

3. **Ethereum Classic Core Development**
    - Core Development
    - Core Dev Focus Points
    - Difficulty Bomb
    - Mitigate Replay Attacks
    - Fix ETC Monetary Policy
    - Fix ETC Monetary Policy - Options
    - Develop Tools and Libraries

4. **Third Party Products and Development Services**
    - Data Feeds for ETC Development
    - Fundonomy Overview
    - Fundonomy Features
    - Tortuga Trading
    - Who Else?

ETHEREUM CLASSIC

Why Ethereum Classic?

“Welcome to Ethereum Classic, a blockchain community dedicated to the principles of openness, neutrality and immutability.”

- Arvicco, the Initiator of Ethereum Classic

Brief History Of Ethereum

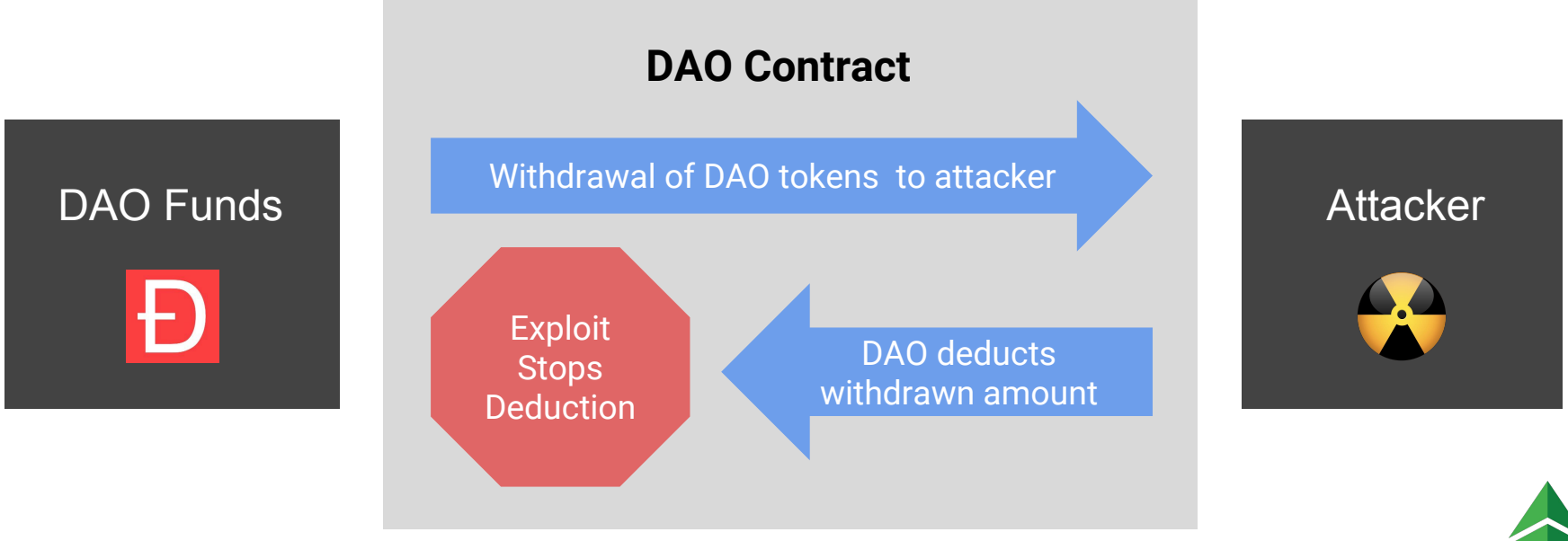
January 3rd, 2009	Satoshi Nakamoto created Bitcoin, the world's first decentralised digital currency, and introduced the concept of a blockchain.
July 30th, 2015	Vitalik Buterin created Ethereum, the world's first decentralised blockchain with turing-complete* smart contracts.
May 28th, 2016	The DAO investment fund is created using Ethereum's smart contract technology.
June 17th, 2016	The DAO is hacked, and 3.6 million ETH is misappropriated due to inadequate security. The Ethereum network itself remains unaffected.
June 17th, 2016	Ethereum Foundation members create various proposals to reclaim DAO investor funds. The community fragments and a month long debate ensues.
July 14th, 2016	Arvicco starts a movement to uphold the original social contract of decentralisation: openness, neutrality and immutability, many agree.
July 20th, 2016	At 13:20:39 UTC the hard fork is executed, refunding DAO, and splitting Ethereum across two networks.

ETHEREUM CLASSIC

*Turing completeness allows for programs to be written for and run on the Ethereum blockchain much as they would on a regular computer.

What Went Wrong

The DAO, a smart contract based fund raises ~$150million from more than 11,000 investors, and was hacked, with ~$70million** being “misappropriated”



*Weakness in smart contracts was due to a reentrancy issue
** Figures based on $20=1ETH market price at time of hack

ETHEREUM CLASSIC

What Went Wrong...

In everyday terms...

How ATM's Work:

- You have $50 in the bank and you want to withdraw that from an ATM.
- You insert your card, PIN and request $50.
- Before the ATM dispenses funds, it updates the balance to the proper amount, $0.
- Then, the ATM asks if you'd like to process another transaction
- You press yes but since the ATM has recorded the new balance of $0, no further funds will be dispensed.

What if:

- You have $50 in the bank and like before you withdraw $50 from an ATM.
- But now the ATM doesn't record your new balance until you end the session.
- You could keep requesting $50 again and again until ATM runs out of money

ETHEREUM CLASSIC

Paying Back The DAO Investors

The immutable ledger was reversed to pay back The DAO token holders

Hard Fork Approach

3.6 Million ETH Stolen

A small group presents various solutions

5% of Ethereum is pro-fork.*

1% of Ethereum is anti-fork.*

94% abstain from voting.*

Protocol level change results in hard fork due to miner centralization

Ethereum, and its value, splits across two chains

Redistribution of assets to victims on the Hard Fork chain

Legal Approach

3.6 Million ETH Stolen

Authorities notified

Assets frozen when discovered by end point users e.g. exchanges

Redistribution of assets to victims. No protocol level change or network split.

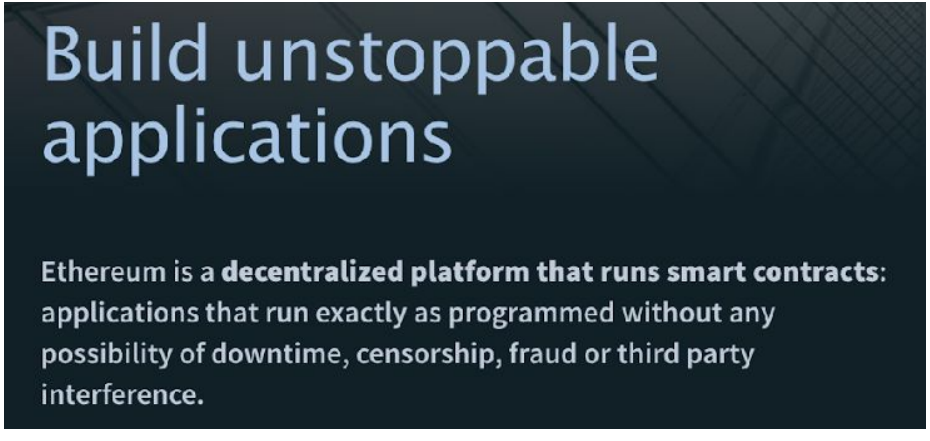
*Numbers taken from http://carbonvote.com/

ETHEREUM CLASSIC

What *Really* Went Wrong

The failure of the DAO was not just a program failure, but a failure in risk management; and it also exposed an even deeper failure of the underlying social contract: *Ethereum transaction/programs would never be changed by a third party*.

Ethereum Website



… until something goes wrong that impacts the interests of a centralized authority.

ETHEREUM CLASSIC

Birth of Ethereum Classic

Saying “Code is Law” implies infrastructure on which it runs is responsible for upholding the law… infrastructure is not responsible for greed, ignorance or malicious behaviour - same as in phone networks, internet and even on the road

- **“Code is Not Law”:** The infrastructure is not there to enforce and uphold law, it's only a protocol that allows execution of immutable transactions and programs
- **User Responsibility:** Developers and entrepreneurs need to understand and take responsibility for legal and regulatory requirements to protect customers
- **Legal Recourse:** If anything goes wrong the infrastructure can not be controlled into changing its state, recourse for financial crime and other illegal activities needs to take place through normal channels
- **Protocol Fixes and Updates:** Only changes to fix protocol level bugs and implement updates/upgrades are acceptable at the infrastructure level

ETHEREUM CLASSIC

Progress to Date

“Only those communities that clearly define their values and stick to them, come hell or high water, will be successful in the world of free and voluntary cooperation without coercion.”

- Arvicco

Principles of Decentralization

Unstoppable Applications can only be built through upholding key principles that ensure infrastructure can only be changed for upgrades, updates and bugs

- **Neutral:** Infrastructure should be neutral to applications being developed/operating on it; endorsements by a central team leads to conflict of interest that skew future evolution
- **Open:** Infrastructure should be openly accessible by anyone to ensure scalability and minimize possibilities of risks linked to centralization
- **Immutable** Infrastructure should be a truth machine that can not be changed no matter what the circumstances

ETHEREUM CLASSIC

Minimising Points of Failure

Decentralization of infrastructure is not sufficient; all key aspects of the ecosystem require a certain level of decentralization to minimize points of failure

Decentralized Infrastructure

Technology
- Core Dev/Support
- Operations
- R&D

Community
- Marketing
- Education
- Dapp Dev

Administration
- Governance
- Finance Management
- Risk Control

Decentralization of all aspects of ETC Ecosystem

ETHEREUM CLASSIC

Technology

A strong, globally distributed team of self motivated developers is set up and working to establish a robust foundation for the Ethereum Classic network.

1. Replay issue remediation strategy being developed so that transactions on Ethereum Classic are unaffected by Ethereum Hard Fork.
2. Go Ethereum (geth), Mist, EthereumJ, PyEthereum, and Parity have been ported to Ethereum Classic
3. A number of block explorers and network trackers live
4. Plans underway to remove the “difficulty bomb”, allowing for PoW to remain viable for miners.
5. New economic policy and hybrid PoW + PoS consensus mechanisms being discussed
6. New technologies being researched and developed to create tamper-resistant contracts (verified compilation, and provable smart contracts).

ETHEREUM CLASSIC

Community

Without a globally connected and energised community, there is no future for the network, no matter how exceptional the technology is.

1. Ethereum Classic social contract and principles defined and released on the Independence Block 2,050,000
2. Meetups set up in London, Zurich, Shanghai and Melbourne and more coming soon, which are being used to establish “ETC local hubs”
3. Globally distributed team coordinating consistent marketing
4. Framework to connect and scale community of Dapp developers being set up
5. Relationships with startups, universities and companies being established

ETHEREUM CLASSIC

Administration

Work is underway to instill principles of decentralization at the heart of the global Ethereum Classic ecosystem, which establishes a framework for sustainable growth.

1. Established a clear social contract and principles the community agrees to. *Completed*
2. In the process of defining a roadmap in-line with core principles. *In progress*
3. Define and deploy appropriate governance model to execute roadmap. *In discussion*
4. Define and deploy appropriate fundraising plan to execute roadmap. *In discussion*

ETHEREUM CLASSIC

Ecosystem Roadmap (WIP)

	2016	2017	2018
Technology	• Core ETC dev team being established • Multiple clients ported • Execute removal of difficulty bomb • Strategy/fix for transaction replay issue • Assess dev of ETC Mist-like client • Deploy independent blockchain nodes • Gain dev / R&D support from 3rd parties	• Align with Core ETH dev team to design, dev and test standard protocol updates • Research/test PoW/PoS mechanisms • Research/test maximally efficient monetary policy for consensus mechanism • Dev ETC focused Mist-like client • Assess path to state Sharding • Assess VM upgrades e.g. verified compiler	• Execute PoW, PoS or Hybrid cons mech • Execute appropriate monetary policy • Test/implement state sharding • Research/test VM improvements if deemed fit for implementation
Community	• Establishing communication channels for global coordination and consistency • Setup global meetups to begin deployment of decentralised community network • Define framework for Dapp developers	• Further outreach to miners • Extend meetups and conferences • Setup of overall Dev conference • Deployment of structured Dapp dev ecosystem and support framework e.g. hackathons and 3rd party funding	• TBD
Administration	• Defining core social contract • Defining community-driven roadmap • Define governance models for execution • Design/deploy funding mechanisms for key infrastructure (build/testing servers, ETC-testnet, web hosting)	• TBD	• TBD

ETHEREUM CLASSIC

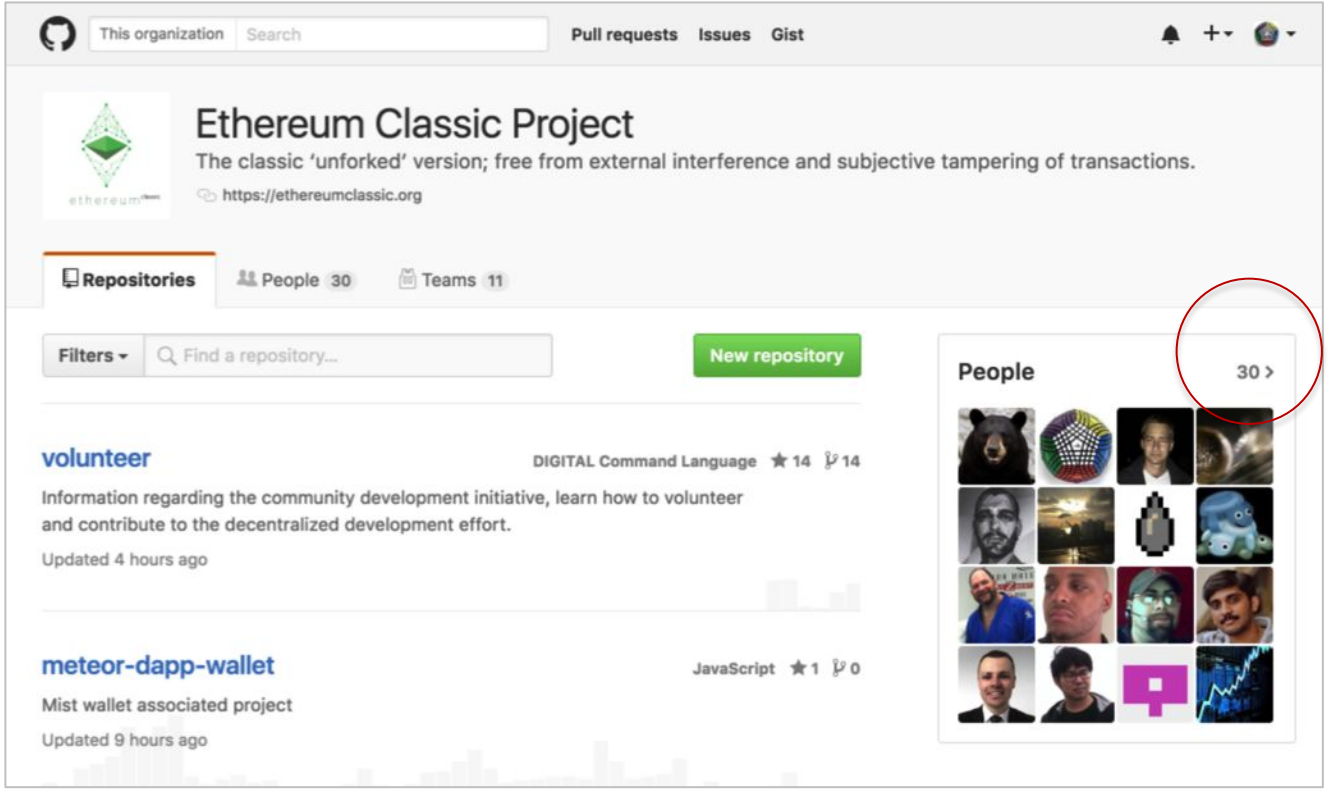
Ethereum Classic Core Development

“Necessity is the Mother of Invention”

- Plato’s Republic

Core Development

Growing ETC Development Team on github repository, which is currently being organized and structured for sustainable development of the core infrastructure



ETHEREUM CLASSIC

Core Dev Focus Points

1. Diffuse Difficulty Bomb
2. Mitigate Replay Attacks
3. Fix ETC Monetary Policy and Possible Options
4. Develop Tools and Libraries

ETHEREUM CLASSIC

Difficulty Bomb

Overview

- Difficulty Bomb - exponentially growing difficulty of Ethereum mining
- Time between mined blocks will become longer and longer
- Eventually, “final doom” occurs, when no more blocks can be mined at all
- Serves no useful purpose, other than to break PoW consensus and push users to PoS
- Will make PoW impractical by early 2017
- Diffusing diff bomb is in best interest of all ETC users and makes PoW viable for long-term
- Long-term decision of ETC consensus algo will be based on data in 2018, with possibilities such as PoW, PoS or a hybrid PoW/PoS

Plan

- Changes to: GO-Ethereum, Cpp-Ethereum, EthereumJ, PyEthereum, EthCore Parity
- Implementation needs to be ready and fully tested by November 2016
- Deployment by end of 2016
- 1-3 months to release
- Mostly part time, but a lot of testing
- Many people involved, pretty much every ETC project needs to update
- ECIP-1010 Proposal by splix

ETHEREUM CLASSIC

Mitigate Replay Attacks

Overview

- Transactions occurring on the forked Ethereum chain can be replayed on the Classic chain and vice versa
- This can lead to a loss of funds if the same address is used on both chains
- User loses ETC or ETH with no options for recovery
- Coinbase/GDAX vulnerable after the hard fork
- Ethereum Classic nonce can be modified in a future hard fork to a value incompatible with Ethereum
- No chance of replay attacks because transaction won't be valid on the opposite chain

Plan

- Changes to: GO-Ethereum, Cpp-Ethereum, EthereumJ, PyEthereum, EthCore Parity
- ECIP in progress by igetgames (me!)
- Implementation tested outside of and alongside the difficulty bomb extension
- Needs to activate at the same time as difficult bomb fix and any other protocol changes, to minimize disruption due to hard forks

ETHEREUM CLASSIC

Fix ETC Monetary Policy

Overview

- Platform token aligns economic incentives of users, miners and investors
- Current Ethereum monetary policy undefined (unlimited token inflation)
- ETH policy is supposed to change with a transition to PoS unpredictably
- Lack of token scarcity does not support long-term investor confidence
- ETC transition to a long-term PoW necessitates monetary policy decision
- ETC commitment to a specific monetary policy:
  1. provide certainty to the market
  2. boost investor confidence
  3. creates competitive differentiator to ETH with its undefined policies

Plan

- Review monetary policy models and assess pros and cons
- Review in parallel to ETC Diff-bomb fix, with target to implement when diff-bomb hard fork executed
- Any consensus parameters can be adjusted to comply to this policy
- Potentially gain research support from universities

ETHEREUM CLASSIC

Fix ETC Monetary Policy - Options

Keep unlimited token inflation forever, like current ETH

- **Pros:** keeps the status quo, encourages token spending
- **Cons:** long-term monetization uncertain, not a good store of value/investment

Fixed final supply with Bitcoin-like reward cut-offs (halvings)

- **Pros:** experimentally proven to work for BTC, sustainable token monetization due to scarcity
- **Cons:** changes existing inflationary parameters, disruptive “halving” events

Fixed final supply with exponential reward adjustments (per epoch)

- **Pros:** no disruptive “halvings”, sustainable token monetization due to scarcity
- **Cons:** changes existing inflationary parameters

ETHEREUM CLASSIC

Develop Tools and Libraries

Overview

- Dapp UI and web components that are not licensed under LGPL/GPL open up development to a wider community
- Preparation for any breaking points where ETC is no longer compatible with ETH at the protocol level
- Java frameworks for Fintech and Corporates, or large businesses where NodeJS development is not allowed
- Add features and ideas not used or promoted in the forked chain

Plan

- Build a new Dapp browser (Mist) built from the ground up, focused on speed and ease of use
- Build a minimalistic, native wallet Dapp to maintain balances and transactions
- Develop a robust Java-based ecosystem with testing, reporting, and integration into existing tools
- Continued maintenance and ports of libraries and tools that originate from the Ethereum Project

ETHEREUM CLASSIC

Third Party Products and Development Services

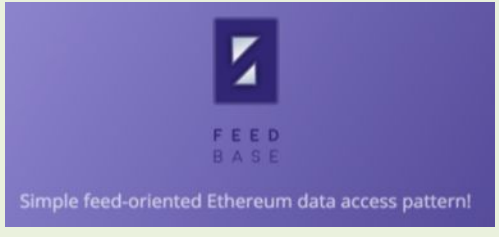
“If you Build It They Will Come”

- Field Of Dreams

Data Feeds for ETC Development

Getting API and other Web data securely, effectively and efficiently into the Blockchain is an important development consideration

Existing ETH Systems also Available for ETC



Planning Phase: Open Oracle Project
Project being planned for accessing api data from the web by paying small amount of ETC through an internal contract transaction without dependency on any centralized party acting as the data bridge from the web to the Blockchain

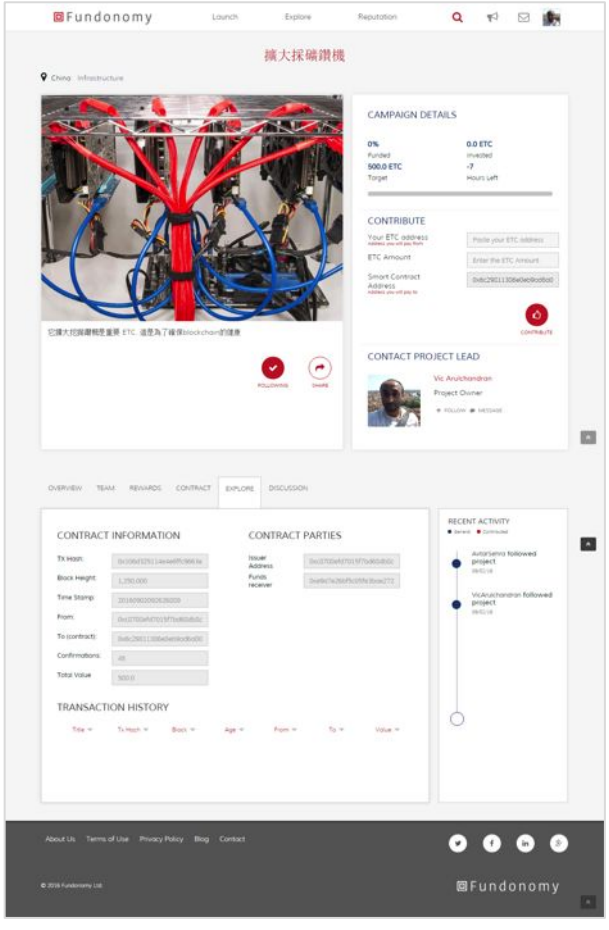
ETHEREUM CLASSIC

Fundonomy Overview

Fundonomy is a platform for ETC community to launch a project funding contract on the ETC Blockchain, with no technical experience required, and receive ETC funding from contributors. Contributors can also judge performance and use the platform to record scores in an open reputation utility contract

ETHEREUM CLASSIC

ETC is a Key Component in the Stack



Web Application Layer – Is about information sharing

- Powerful project marketing tools to spread messages across all social networks with a single user friendly interface
- Communications and group management tools to enables users to manage campaigns before, during and after they launch
- Allows users to build communities and relationships

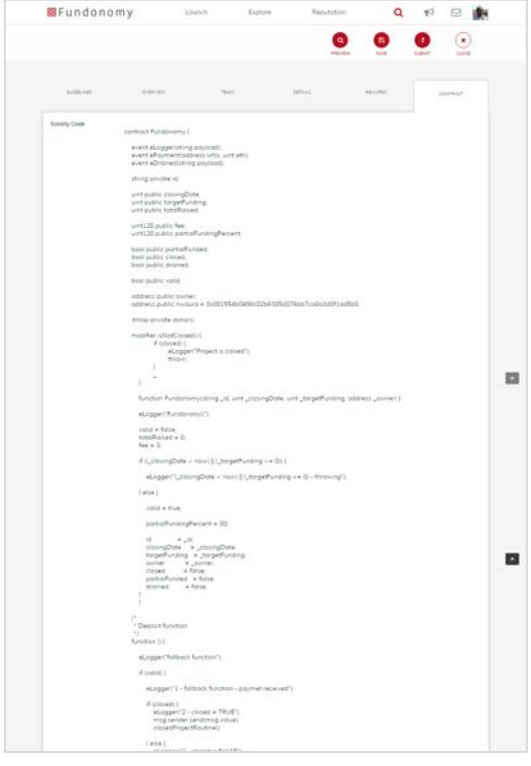
Blockchain Layer – Is about storing and managing value

- Collection of funds at little or no cost
- Holding of funds securely that release on key triggers e.g. dates, completion of milestones etc
- Reputation score becomes a source of value that should be independent of anyone party and can become a utility that can be tapped into for any funding contract on or off Fundonomy

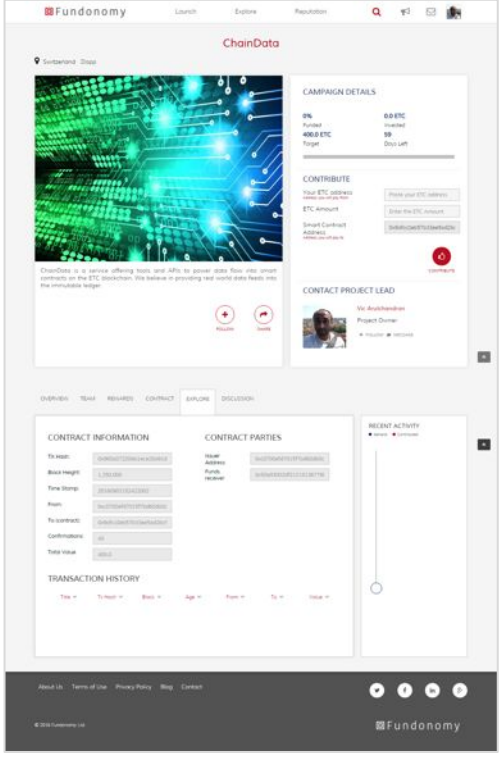
ETHEREUM CLASSIC

Deploy and Market Funding Contracts

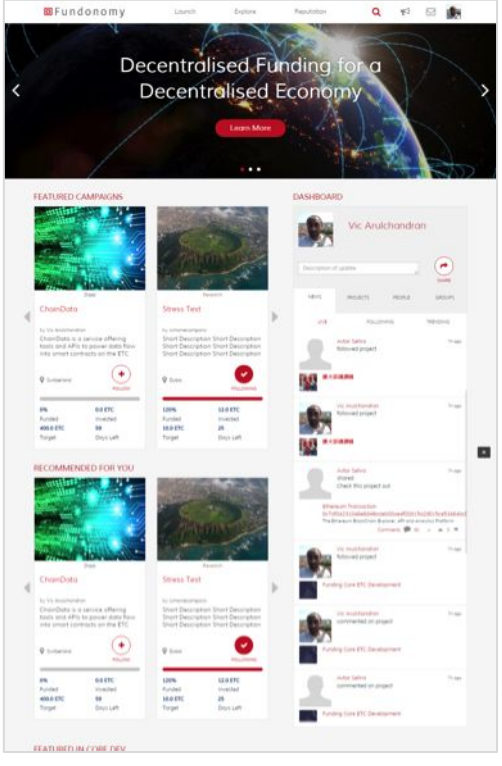
Construct and Deploy
Project Bounty Contracts



Market and Enable Users to
Discuss and Contribute



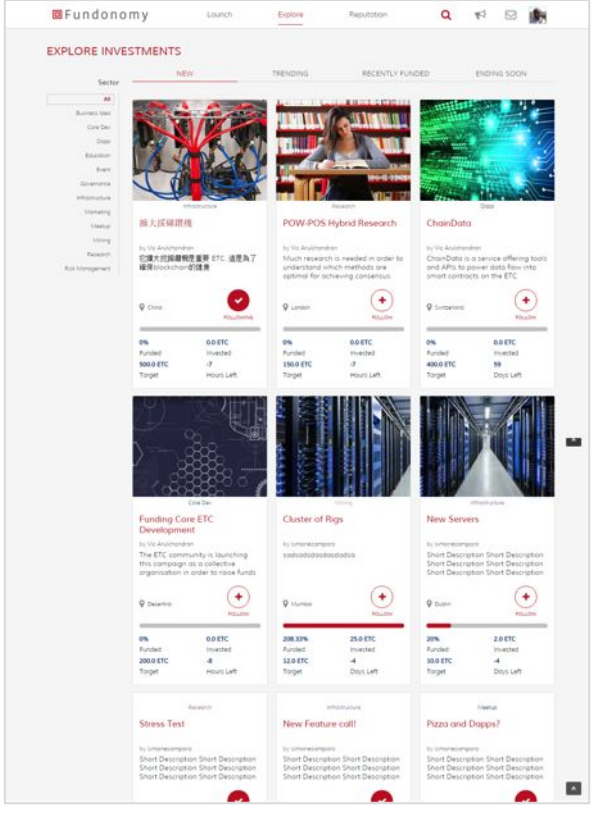
Create a Social Marketplace of
Project Bounties and Ideas



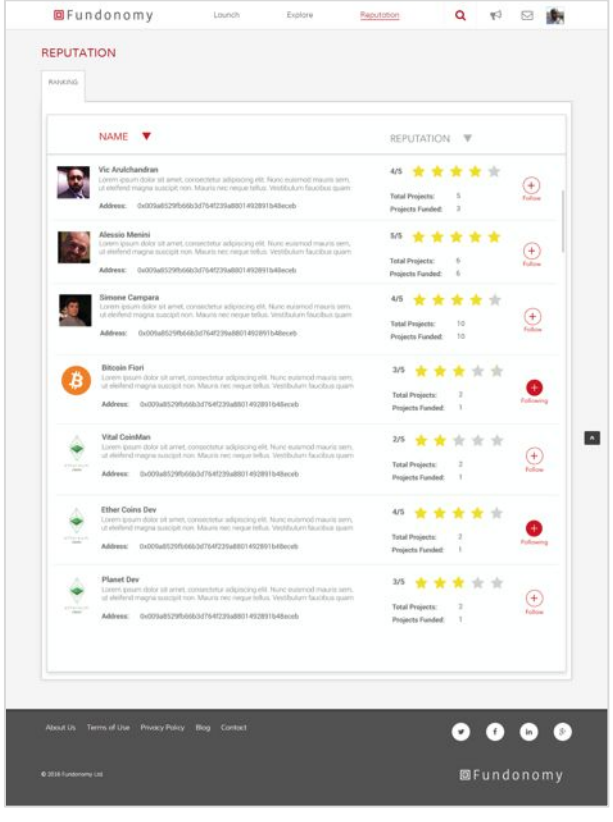
ETHEREUM
CLASSIC

Project Success Drives Reputation

Explore Project Bounties for
Contribution Based on Team Reputation



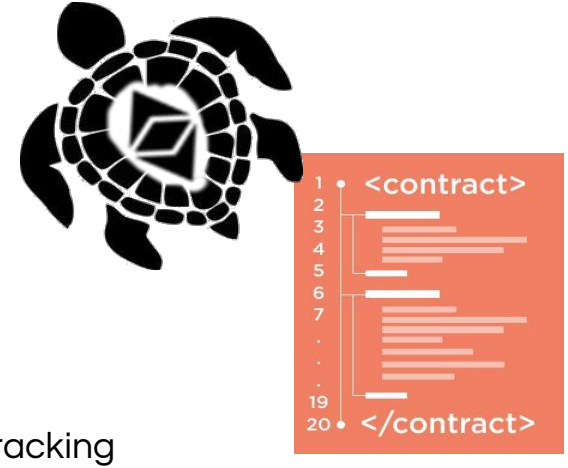
Team Members Build Reputation
Score Based on Contributor Feedback



ETHEREUM CLASSIC

Tortuga Trading

Tortuga Trading is a new Dapp in development with the mission: “Real world trading using smart contracts on the ETC blockchain”. It promises a “sneaker-net” trading platform built on top of Ethereum Classic. It will provide wallet management, one click contract deployment and voting, local trading maps, and tracking of all contracts deployed.



Web3 integration

Contracts without coding

Reputation tracking

Blockchain tracking

Map searching

Wallet creation and management

ETHEREUM CLASSIC

Tortuga Trading (cont'd)

"One of the main challenges to the widespread adoption of cryptocurrencies in general has been the lack of accessibility. ETC is currently traded online by users who have traded bitcoin through exchanges and other third party services. With the ability to record and manage contracts on the blockchain, Ethereum Classic has presented the framework to deploy the next generation of over-the-counter trading.

The goal of Tortuga Trading is to allow users to interact and trade ETC for goods and services in the real world. The service will initially offer user the ability to exchange ETC for fiat currencies with everyday people in their local neighborhoods with a convenient map locator interface. Users will enter into trade contracts on the block chain and transact in the real world.

All the mechanics of smart contract construction will be handled on the backend of the service and the user will be able to find and make trades without having to write a single line of code or understand advanced cryptographic systems. Point, click, trade.

With the full deployment of the Tortuga Trading platform, users will not only be able to trade their ETC for Fiat, but will have the ability to intuitively use premade contracts to trade anything they want using ETC. Buyers and sellers will be able to arrange trades, find willing parties, and transact on the blockchain without having to worry if the other party is trustworthy because all of their previous trades are available to the world for review. Price discovery will occur in real time. The reputation system will be the blockchain.

The third phase of Tortuga trading plans to open the world of derivatives contracts to the system. The concept of the fixed contract size and terms of trade lends itself well to a futures/forwards market which would provide for high transaction volume."

- Cody Burns, Creator of Tortuga Trading

ETHEREUM CLASSIC

Who Else?

- Solidarity: “Vault” for multi-signature online wallet with two-factor authentication
- Stampery.com
- Jaxx now supports ETC and splitting
- Any others?

ETHEREUM CLASSIC

Questions?

Contributors

Gravity	gravity@ethereumclassic.org
Igor Artamonov	splix@ethereumclassic.org
Marcus R. Brown	marcus@ethereumclassic.org
Elaine Ou	elaine@ethereumclassic.org
Arvicco	arvicco@ethereumclassic.org
Colibry	colibry545@ethereumclassic.org
Cody Burns	cody.w.burns@ethereumclassic.org
Eric Somdahl	eric.somdahl@ethereumclassic.org
Avtar Sehra	avtarsehra@ethereumclassic.org

ETHEREUM
CLASSIC

ETHEREUM CLASSIC

Web: ethereumclassic.org

Twitter: @eth_classic

Facebook: @EthereumClassicETC

Slack: ethereumclassic.herokuapp.com

Discord: https://discord.gg/xy777au