Application Development for Ethereum

Getting Started

Mike McEwan

Contents

Abstract

While blockchain technology is poised to break into the mainstream, few in the mainstream are positioned to benefit from it. Those who are prepared will become the new giants of the global economy. Those who are not will have their kodak moment. There are numerous sources of information on blockchain – few of them give the uninitiated reader the guidance required to break into the inner circle and become a beneficiary of blockchain. This paper gives practical pointers, and aims to leave the reader standing on the first step of the path to business turnaround through blockchain, using Ethereum as the practical example.

Overview

The following outlines the technology behind blockchain, indicates the nature of the market for the use of blockchain, provides examples of who is (and shortly will be) succeeding and profiting from this market, then concludes with a description of the project lifecycle best-suited to delivery in this environment, and consequently, the nature of the team that needs to be assembled to do so. The particular focus of this is Ethereum, but the points apply to any similar implementation of blockchain or distributed ledger technology.

The Technology

In a sense, this is the easy part, and the most documented. Those who are familiar with the technology can skip the next two paragraphs – and if you choose to read anyway, please forgive the simplification.

Consider a simple ledger of accounts – a book that contains a listing of transactions. Now consider hundreds of copies of that ledger, distributed out to trusted individuals, along with a seamless process that passes a bundle of new transactions to each holder of the ledger, so that they can be applied to their copy. Those transactions can come in from any of the holders of the ledger. Part of that process is that everyone can check that a transaction is being applied to a valid copy of the ledger, because everyone can check that their ledger matches those held by all the others. If not valid, the local copy can be corrected by getting updates from the network. There is no practical way to corrupt the ledger, because it would only work if done simultaneously to every copy – and no one person actually knows where every copy is held. This is one of the key foundations to blockchain technology – the ledger is a database, a copy of which is held on every computer that participates within the network, a block is a bundle of transactions, and the process is the means of chaining each new block to the previous block with an incorruptible link that cannot be broken by the computation power available for the foreseeable future.

The other key foundation is the nature of the transactions. In a simple ledger, the transactions are debits and credits to accounts. The paper at https://github.com/ethereum/wiki/wiki/White-Paper introduces an alternative perspective – that each transaction represents a state change. This more generic perspective allows for the simple debit and credit, but opens the door to the wider possibilities provided by the Ethereum network, where transactions can involve a variety of operations on different types of data, and state changes can be implemented through smart contracts, written in the Solidity language, which is compiled to an intermediate code. This intermediate code is interpreted by the Ethereum Virtual Machine, running on nodes in the network. This presents limitless possibilities to address previously intractable business problems. Some of these are described at https://www.ethereum.org/ , which also provides more detail on the technology.

An additional consideration is the distinction between public and private blockchains. The former – like Ethereum itself – is open to all, while the latter can only be accessed by those with permission to do so. Key benefits of a private blockchain are improved security, execution efficiency, and resilience.

The Market

Simplistically, there are two main markets – simple ledgers and decentralised applications.

Simple Ledgers

Simple ledgers equate to the traditional paper ledgers, and provide secure and immutable records of transactions, such as balances of accounts for cryptocurrencies, or documentary letters of credit being issued. The inherent advantage of blockchain here is the "trustless trust" – there is no requirement to establish trust between parties, because the existence of the transaction on the blockchain is sufficient confirmation that it is valid. However, there is a very limited market for cryptocurrencies, because they have no inherent value of their own. Like most things, the price is determined by what the recipient is prepared to pay, and there are few differences in functionality between the cryptocurrencies currently on the market. The key differences lie in the marketing of the various offerings. Those where the marketing has been successful have seen incredibly high prices being paid, such as for Bitcoin. They have also seen just as incredible drops in prices, and there are no tangible assets which back them, so the price is driven by the market – that is, there is significant risk in holding such assets. There is development underway to change this and remove the volatility, coming from global players such as Facebook – although by far the most interesting and credible proposal is that of InitiativeQ (described later).

In addition, there is a significant market for private cryptocurrencies, used to support business operations between members of a defined group – conceptually, this would be the modern-day equivalent of the old European Currency Unit (ECU). An example of this is the Utility Settlement Coin (USC) to be provided by Fnality International (see link later).

Decentralised applications

The best source of information on these is at the Ethereum sites, in describing the smart contracts referenced above. To quote from one at https://docs.ethhub.io/ethereum-basics/what-isethereum/#what-are-smart-contracts-and-decentralized-applications

> "These can be used to create a wide range of Decentralized Applications (DApps) which can include games, digital collectibles, online-voting systems, financial products and many others."

The various Ethereum sites host enthusiastic papers and lively discussions about the range of possibilities now open with the current incarnation of Ethereum, and equally enthusiastic contributions to the specification and implementation of the next incarnation. Actual, real-world examples of Ethereum DApps being in use to solve live business problems are harder to find. To draw a historical analogy – Ethereum is currently at the stage equivalent to that of the initial introduction of the IBM PC running DOS, with speculation about the direction it would take, given the WIMP interface provided by the Apple alternative. In those early days, it was a solution greeted by the industry with public enthusiasm, but with businesses trying to understand what problems it solved.

But then this is the crux of the current opportunity – to find the problem for which blockchain can provide a step-change in the nature of the solution, much as Uber did for people wanting to get transport from point A to point B, or AirBnB did for people seeking temporary accommodation.

Who is making the money?

There are many people making small to large profits, and broadly speaking can be described as being in one of the 3 groups:

- Contributors
- Speculators
- Innovators

Contributors

This group consist of the vast array of global resource which helped to implement the Ethereum ecosystem, and is helping it to build and develop. There are 2 sub-groups, which for the purposes of this paper are described as soft and hard contributors (some individuals can be considered members of both sub-groups).

Soft Contributors

These are the people who sell the vision and present the possibilities. They have had a dramatic effect in encouraging wider interest and investment by companies, which has resulted in the creation of internal instances of the Ethereum network. They can often be found in Strategy or Architecture teams within large organisations, where their efforts have helped to shape the research investigations and prioritised dedicated funding for the local environments

Hard Contributors

These are the hands-on people, ranging from an individual using the graphics card in their home PC or laptop to mine as part of a pool, earning less than 1 ETH per month, to those developing and testing the designs and the code for the various components of the eco-system. As an indication of the reward to these contributors, as outlined at https://xena.exchange/blog/history-of-ethereumhard-forks-will-istanbul-support-eth-prices/ (which itself is a useful summary of the history of Ethereum), early stress testers were rewarded by a grant of 25,000 ETH – at the time of writing, that equates to US$4.65M at the current exchange rate. These are the technically-proficient people who are taking forward the development of the capabilities, but are very rarely the average members of development teams within large businesses.

Speculators

The speculators are those who are buying and selling large volumes of cryptocurrencies, and drive the publications by cryptocurrency analysts, who apply models to predict rises and falls. It is a matter of individual choice and risk appetite whether to invest in this way. The speculation has had the effect of driving up prices over the long-term, which in turn has indirectly funded the development of the industry (an example being those early stress testers, who presumably could move into full-time development). One notable difference between applying predictive models for cryptocurrencies, and doing so for the stock market, is that models for the latter can be validated to confirm – for example – that corn or CPUs are selling for the price expected and at the rate expected, so the stocks and shares of companies that depend on these sales are rising or falling in line with commodity values.

Innovators

These are the people who are coming up with the genuinely new ideas, and one useful perspective is that there are currently 3 generations of these:

- Originators
- Enablers
- Adopters

Originators

There is a very small group of people who have originated ideas in the blockchain world, and successfully sold the concept. Bitcoin was the first of these, successfully selling the concept and implementation to the world at large, and boosting the fortunes of those who were involved at the start. Similarly, a relatively small number of people own a significant proportion of ETH (Ether) – see https://www.bloomberg.com/news/articles/2019-05-15/just-376-people-found-to-own-a-third-ofall-ether-cryptocurrency

Their relevance now is that their knowledge makes them hugely influential on the future direction of development, while their wealth makes it possible for them to ensure implementation of that direction. This means that anyone involved in any blockchain-related work needs to keep up to date with their latest communications.

Enablers

This is the next generation, which can only exist when the Originators have created something. They provide additional capabilities that add value, or simplify access or use of blockchains. Examples are:

- Cryptocurrency wallets (both hardware such as Ledger Nano and software such as MyEtherWallet for a smartphone)
- User Interfaces containing wallet capability (such as Ethereum Wallet, which is a full node wallet)
- Blockchain browsers such as Etherscan.io
- Coin exchanges such as CEX.IO
- Service providers such as Fnality – see https://www.fnality.org/ : “Fnality International has been founded to create a network of decentralised Financial Market Infrastructures (dFMIs) to deliver the means of payment-on-chain in tomorrow’s wholesale banking markets”

Adopters

This is the current generation, who are adopting the available technology to support a business proposition, an example of which is InitiativeQ. This merits some attention as it is a current example of a business in the process of being built. InitiativeQ aims to provide a global currency for consumers. The marketing materials on their website give clues to the stages of the plan:

1) Build a huge global base of consumers who state an intention to buy using the Q cryptocurrency, which will be pegged to the US$, and can be bought or sold at the rate of 1 per US$
2) Sign up merchants who will accept the Q in payment for goods, on the strength of the massive consumer base

3) Get investors to fund the whole proposition with actual US$, on the strength of the size of the consumer and merchant base, and by offering a discount – for example, buying at 50% of the value

Step 1 is being achieved right now, by giving those who provide their email address with a small allocation (for example, 3000) of the future pool of Q, along with a further small allocation for each one of their contacts that they introduce this to, and who also provide their email address (up to a maximum number – initially, 5 – and in a limited time window of 1-2 weeks). Step 2 can be inferred from the website, while step 3 is more thoroughly described there, along with academic papers explaining how a currency can have more in circulation than is supported by the assets that back it up, along with information on addressing the credit risk for those using the Q instead of US$.

This is the type of radical business proposition made possible by the existing technology, and is a win-win scenario for all involved – consumers get some free money, merchants get more business with a fraction of the transaction cost for handling payments, investors get an asset with an instant profit, and the founders of the business will have their own pool of Q which will have an instant realworld value. As a (possibly unintended) side-effect, this will also result in the largest ever redistribution of wealth from the extremely rich to the wider population. Inevitably, someone has to lose – the losers will be those businesses seeking investment funds, which will no longer be available to them.

The 4th Group – Integrators

There is a 4th group notably missing at this stage, and is the one most-probably best described as Integrators – those who will take this technology, build on it, and integrate with other components to deliver full solutions to end-users and businesses. This is the group that is the main audience for this paper, and will be discussed next.

Business Proposals

To be credible, any business proposal needs a business case showing a return on investment (ROI), and a plan to show how and when that ROI can be achieved. These can be scrutinised and assessed against similar proposals seen previously. The difficulty for blockchain-based solutions is that there is little to compare against.

Business Case

The business cases which are currently attracting investment are those created by Innovators, and for the Enablers and Adopters. The Originators have already made their cases and received their investment, although there is always space for fundamentally new propositions. A part of the investment comes from the potential end-users of the technology – so for example, the various businesses that have funded Fnality. A key consideration is that Fnality intend to provide the infrastructure to host a solution – they are not providing the full solution. This means that the investors – to get the full return on their investment – need someone to develop the solution that will run on the infrastructure. At present, the information that supported the case can only have come from the Soft Contributors, by presenting the vision of what will be possible. If questioned on the availability of resource to implement, they can point to the global pool of Hard Contributors, demonstrating that – when the time comes – there will be people that can “cut the code”. The elements are all there to support a business proposal, and to make the case with some illustration of ROI.

Business Plan

To a point, business plans can be created. An example is International Cash Management (ICM) or Multi-Bank Cash Management (MBCM). These provide services to large companies to move funds between countries and banks. The customers are familiar with the sweeping, topping and pooling services that enable them to maximise credit interest and minimise debit interest. This is an obvious candidate for a blockchain-based solution – instead of using SWIFT messaging to transfer actual funds between accounts, secured tokens can be used to maintain each customer's total balance. These can be converted into currency at the point when required. A business plan can be created based on knowledge of previous ICM/MBCM plans. The development cost can be estimated from the cost of previous developments of cryptocurrencies, but this is the point at which a gap appears – there is no defined development methodology, and there appears to be an assumption that none is needed. Hard Contributors have already implemented their own pet projects; there are new cryptocurrencies already available that are defined to Ethereum in the ERC20 standard. Some have used existing methodologies for Agile development, some have simply copied other code and amended until they get the desired result. This will not be sufficient for the future developments, because of two fundamental ways in which the blockchain environment differs from other current computing environments.

Environment Implications

Physical Environment

The security inherent in the blockchain approach and the confidence that – once a transaction has been processed, including the deployment of a smart contract – it cannot be modified, means that the operating environment is analogous to deploying to Programmable Read Only Memory (PROM). Once written to PROM, code cannot be changed – any changes can only be applied to a new PROM. This means that – while an iterative approach to development can be done in test environments – it would be very difficult (although not impossible) to take an iterative approach to the delivery of business functionality into a production environment.

Logical Environment

As described earlier, transactions represent state changes, and knowledge of state transitions needs to be reflected in the smart contract code written in Solidity, which includes facilities for explicitly identifying code that does not change the state.

Development Methodology

The environment implications give pointers towards the methodology most applicable to blockchainbased projects, which is that used for embedded systems. There are many references available for a variety of methodologies, and it would be possible to investigate each and pick the most suitable. A more pragmatic approach would be to engage a team of Software Engineers who have delivered embedded real-time systems, and use their experience as input to estimating to contribute towards the business plan.

In the absence of such a team, an alternative would be to look back at the approach taken in the 1980s and 90s to delivering PROM-based systems, and use case-studies from that time as the basis for estimating.

In either case, the methodology must also cater for the logical environment considerations. In practice, this means the design work must include state machine design. An example from the 1980s would be Yourdon Analysis and Design, where the approach of creating State Transition Diagrams, Entity Relationship Diagrams and Data Flow Diagrams would be applicable. For more on this, see (for example) https://erlinwin.files.wordpress.com/2012/06/jesachpt13.pdf

Project Plan

Having an agreed methodology as above will then simplify the process of creating the project plan, regardless of whether the Development/Test approach is a Waterfall style or an Agile, iterative style. However, the project plan will only be realistic if it is delivered through a project team with the right resources.

Project Team

In principle, a Project Manager (PM) does not need to know the technical detail of the project. In practice, a degree of such knowledge is essential to be able to ask the right questions and assess the risks, assumptions, issues and dependencies. If the PM does not have any previous experience in blockchain-based solutions, look for a PM with previous experience in embedded systems, preferably deployed via PROM.

The person or team responsible for analysing the business problem and assessing the solution can come from existing business analysis/system analysis resources, augmented by training to understand the different concepts and environment offered by blockchain.

Those charged with designing the solution (with titles like architect, designer or solution manager) must have the skills appropriate to the development methodology, and must have practical experience of designing from the 3 perspectives of state transitions, entity relationships and data flow.

The build of the solution must include individuals with practical experience of implementing smart contracts written in Solidity, ideally demonstrated by live services that have already been deployed to the Ethereum live environment. If not available, the project plan has to allow some reasonable time (at least a month full time) for training and familiarisation.

Testing teams can be drawn from existing resources, but will require some additional training on the nature of the Ethereum environment, and the types of test cases that are unique to this, where – for example – an error in the contract can allow an attacker to acquire all the ETH owned by the contract.

Implementation teams can also be drawn from existing resources, but need to be aware that there is no concept of "backing out" or "forward fixing" a smart contract deployment, so the emphasis should be on the skills and experience for holding and driving multi-disciplinary Implementation Readiness reviews and Schedule of Events walkthroughs.

Conclusion

Blockchain technology, and Ethereum in particular, are at a key point in their use in the industry. There is enough available to deliver on the promises of efficient, reliable and low-cost services. However, this is all at an early stage, meaning businesses that want to provide such services to customers may find that their delivery projects are stalled, and struggling to find a way forward. However, there is a way forward, and it can be achieved by relying on some of the processes and people from the past.

Note

This paper is from the perspective of traditional project management, looking at what blockchain offers. To understand the practical problems, the author researched, designed, developed and implemented into the Ethereum production network a new cryptocurrency, the T-Coin. The contract for this is located at address 0xd557d29c6e45649142b7ef6e4a4f2d0c8b0ec4b0 and the transaction history can be viewed by entering this address at https://etherscan.io/ The Buy and Sell functions have been disabled so that the currency cannot be used for speculation, but small quantities of coins can be made available for anyone wanting to test. The only cost would be that charged by Ethereum to transfer them, which is generally the ETH equivalent of a few US cents, or less.

Acknowledgements

Thanks to are due to James McEwan and Paul McEwan for being sounding boards for this material, to David Hinley, Martin Johnson and Rebecca Welch for their comments and thoughts, to Olaf Ransome for his feedback on the first version, and to Dilyana Valcheva for her introduction to Olaf.