Regtech Improving Governance Authenticating Identities, Authorization Signatures and Digital Content

Section 1: Summary

Use Case Summary			
Use Case ID:	GOV-005	**Use Case Type:**	Government and Public Sector
Use Case Title:	OriginalMy Blockchain	**Is Use Case supporting SDGs**	*Yes*
		Domain:	*List 1 Appendix 1*
Status of Case	Running/Production	**Sub-Domain**	*If necessary*
Contact information of person submitting/ managing the use-case	Full Name: Edilson Osorio Junior Job Title: CEO E-mail address: osoriojr@originalmy.com Telephone number: +372 5709-5771 Social media: https://www.linkedin.com/in/osoriojr/ Web site: **https://originalmy.com**		
Proposing Organization	OriginalMy Blockchain OÜ Registry Code: 14450907		
Short Description	A LegalTech engine platform that builds Trust in e-Governance seamlessly authenticating: identities, authorisation signatures, and digital content		
Long description	Founded in 2015, OriginalMy envisions a world in which individuals and entities have a balanced alignment of interests and are empowered to take necessary actions that build Trust in the e-Governance for the benefit of the entire organisation. The challenge to achieve that vision is building Trust and increase the overall governance process while providing compliance, risk management and cybersecurity tools that cannot be flawed, corruptible, temperable and non-verifiable - because of centralisation. The solution is presenting a trusted and immutable blockchain framework with: - The next generation of Digital Identity & storage of assets; - Seamlessly authentication with proof-of-authorship; - Single Sign-On, with control of delivering of personal data; - Authentic signed documents, contracts and transactions ; - Proof-of-authenticity for digital content; - Blockchain-enabled e-voting systems; This approach is trustful because it improves the overall e-Governance reducing costs and saving time, is flexible to address an array of risk and compliance needs, performs traceability of all digital acts performed and has the security provided by blockchain cryptography protocols.		

SDG in Focus (when applicable)	*Enter one or more number (1-17) and specific corresponding indicator/s as applicable* *See https://www.un.org/sustainabledevelopment/sustainable-development-goals/* Use your right to elect the leaders in your country and local community **Goal 16: Promote just, peaceful and inclusive societies** 16.3 Promote the rule of law at the national and international levels and ensure equal access to justice for all 16.4 By 2030, significantly reduce illicit financial and arms flows, strengthen the recovery and return of stolen assets and combat all forms of organized crime 16.5 Substantially reduce corruption and bribery in all their forms 16.6 Develop effective, accountable and transparent institutions at all levels 16.7 Ensure responsive, inclusive, participatory and representative decision-making at all levels 16.8 Broaden and strengthen the participation of developing countries in the institutions of global governance 16.9 By 2030, provide legal identity for all, including birth registration 16.10 Ensure public access to information and protect fundamental freedoms, in accordance with national legislation and international agreements 16.A Strengthen relevant national institutions, including through international cooperation, for building capacity at all levels, in particular in developing countries, to prevent violence and combat terrorism and crime 16.B Promote and enforce non-discriminatory laws and policies for sustainable development Call out sexist language and behaviour **Goal 5: Achieve gender equality and empower all women and girls** 5.1 End all forms of discrimination against all women and girls everywhere 5.2 Eliminate all forms of violence against all women and girls in the public and private spheres, including trafficking and sexual and other types of exploitation 5.B Enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of women 5.C Adopt and strengthen sound policies and enforceable legislation for the promotion of gender equality and the empowerment of all women and girls at all levels Raise your voice against discrimination **Goal 10: Reduce inequality within and among countries** 10.2 By 2030, empower and promote the social, economic and political inclusion of all, irrespective of age, sex, disability, race, ethnicity, origin,

	religion or economic or other status 10.3 Ensure equal opportunity and reduce inequalities of outcome, including by eliminating discriminatory laws, policies and practices and promoting appropriate legislation, policies and action in this regard 10.6 Ensure enhanced representation and voice for developing countries in decision-making in global international economic and financial institutions in order to deliver more effective, credible, accountable and legitimate institutions 10.7 Facilitate orderly, safe, regular and responsible migration and mobility of people, including through the implementation of planned and well-managed migration policies Partnership for the goals **Goal 17: Revitalize the global partnership for sustainable development** 17.7 Promote the development, transfer, dissemination and diffusion of environmentally sound technologies to developing countries on favourable terms, including on concessional and preferential terms, as mutually agreed 17.8 Fully operationalize the technology bank and science, technology and innovation capacity-building mechanism for least developed countries by 2017 and enhance the use of enabling technology, in particular information and communications technology		
Value Transfer:	It allows the tokenization of all of your own resources, assets and attributes carrying it on your identity, avoiding the needing of a third party to certify/comprove what belongs the to you. It reduces costs, bureaucracy, time and empower people.	**Number of Users:**	*30.000*
Types of Users:	natural person and entities		
Stakeholders	natural person, entities and government		
Data:	*What data are expected to be stored in distributed ledger in terms of types, record structure, privacy, etc.* *How DLT solution would interact with external data and other systems.* Stores the link between the document id and the blockchain id, mantaining history of changes. Stores the hashes of digital documents, the signatures made on documents and authorisations and, in the future, the reputational system. It don't store any personal data on the ledger. Thus, OriginalMy will use tokens to reward users who made tasks, like working on the decentralised network of validation being constructed.		
Identification:	Identity validation automatically or using own bureau. After the validation, the personal data is stored just with the user. There's no possibility of anonymous use.		

Predicted Outcomes:	

Overview of the Business Problem or Opportunity

Explanation of the business problem or opportunity.

The problem is the lack of trust on digital content and on who is performing the digital act or transaction, in situations where the authenticity, authorship or ownership is critical.
It opens a window for corruption, bureaucracy and expending of money and time.

Fines and compliancy divergences costs:

- **$300 billion post 2008 crisis regulatory fines**
  FT Research
- **492% volume of regulatory change between 2008 and 2015**
  Thomsom Reuters
- **45x increase of regulatory fines in 20 large US and EU banks**
  McKinsey
- **10-15% of total workforce dedicated to governance, risk and compliance**
  McKinsey
- **Proxy voting remains "noisy, imprecise and disturbingly opaque"**
  Barrons - about $60m P&G proxy fight costs

The opportunity:

- **$780 billion** per year regulatory divergence costs Thomson Reuters: Cost of Compliance 2018 Report
- **ROI of 600%** in regulatory software investment
  LPT Research: Strategic Analysis of RegTech - A $100b Opportunity
- **$118.7 billion** per year revenue stream by 2020
  LPT Research: Strategic Analysis of RegTech - A $100b Opportunity

On the Identity field, a McKinsey report identified that until 2030, countries will spend up to 13% of the GDP on Digital Identity and related services, to avoid identity and payroll fraud and improving the onboarding systems.

Why Distributed Ledger Technology?

How distributed ledger technology would improve the current solutions (if they exist) or enable new solutions which were previously unavailable.
Please also specify which DLT features are required (immutability, security, verifiability, resilience, transparency, etc.)

The full solution is only possible because of blockchain technologies.

- Allows the full decentralisation of the identity and being the future generation of digital identity (where the identity will store itself all of your resources, assets and attributes).
- Allows the transaction of personal data being tracked and rewarded.
- Allows the proof-of-authenticity of digital content and transactions
- Allows proof-of-authorship for authorisation signatures on documents, and contracts
- Single sign-on systems with delivering (transacting) of personal data with proof-of-agreement
- Improves trust on e-voting, where the main problem is the lack of trust just after casting the vote to the blinded ballot box and in the centralised tallying phase (see Hääl - the

worldwide first protocol for Secret E-Voting on Public Blockchains, with running PoC: https://github.com/eddieoz/haal)
- Allows decentralised reputation system and dispute resolution
- Security provided by many layers of strong cryptography
- Immutability and integrity of all data stored, as resilience and redundancy for contingence.
- Transparency and auditability of all data and transactions
- High availability of all network

Section 2: Current process

Current Solutions
If there are existing systems which automate the above business problem/opportunity. - OriginalMy: providing end-to-end digital governance And other systems who addresses part of the solutions: UPort: digital identity Civic: digital Identity Signatura: signing contracts and documents BlockNotary: notarisation of documents

Existing Flow (as-is): Signing documents and contracts		
Step	**User Actions**	**System Actions**
1.	Local authentication	User goes to a notary
2.	Sign a contract	User register the contract on a notary

Existing Flow (as-is): Signing public petitions		
Step	**User Actions**	**System Actions**
1.	Signature collecting	User signs a paper
2.	Validation	Impossible to validate
3.	Acceptability	Representative endorses the petition

Existing Flow (as-is): Proof-of-authenticity of web content + notarization (avoiding fake news dissemination, harassment and other on social media)		
Step	**User Actions**	**System Actions**

1.	Collecting the legal proof	User goes to a Notary Notary transcribe the page on a report The report can be attached to a case and sent to the justice

Existing Flow (as-is): Platform: Notarization of documents		
Step	**User Actions**	**System Actions**
1.	Authenticating documents	User goes to a Notary Notary makes a copy of the document Notary authenticates the copy of the document

Existing Flow (as-is): E-voting		
Step	**User Actions**	**System Actions**
1.	Voter casts the ballot	Send to a centralised platform Needs to Trust on the platform; Too much power on a centralised entity No transparency and verification in real-time Black-boxes of voting

Data and information (as-is)		
Data	**Type**	**Description**
1	*Documents*	In paper
2	*Web content*	Must go to a Notary
3	*Certificate of Signatures*	Must go to a Notary to verify the signatures
4	*Certificate of Authenticity*	Provided by a notary, in paper
5	*Notary Authentication*	Digitally stamped document issued by a notary
6	*Notary declaration*	Report issued by the notary, with the description of the service provided
8	*Collecting Signatures on Public petitions*	On paper

9	*Voting ballot*	On-paper on electronic by centralised trusted entity

Participants and their roles (as-is)		
Actor	**Type/Role**	**Description**
1	*Lawyers*	Collect evidence to attach to the process
2	*Bank*	Pre-authenticate documents to send to the notary
3	*Government*	Preserves the authenticity of your papers and documents
5	*Users*	Has the needs of authenticating documents, verifying theirselves or their signatures
6	*Notary*	Provides the service for authenticating documents and signatures

Other Notes
Any assumptions, issues

Section 3: Expected process

Existing Flow (to-be): Mobile app: Signing documents and contracts		
Step	**User Actions**	**System Actions**
1.	Local authentication	User uses local biometrics to validate him/herself
2.	Sign a contract	User proves the ownership of the document to be signed (using pin-code) System verifies on-chain if the user is allowed to sign and if the document is authentic System stores the digital signature and the blockchain id on the smart-contract, together to the other signatures of that document

Existing Flow (to-be): Mobile app: Authentication system with delivering of personal data		
Step	**User Actions**	**System Actions**
1.	Local Authentication	User uses local biometrics to validate him/herself
2.	Scans a QR-code	Opens a popup showing all the data that will be collected by the platform
3.	User agree on deliverying of the data	Authenticates user using cryptography challenges Sign the data to be transferred Transfer the data to the desired platform Registers the transaction The desired platform checks the authenticity of the data, as the reputation.

Existing Flow (to-be): Mobile app: Mudamos+ (created by ITS-Rio) internally using our engine for identity, signatures and authentication, for signing public petitions (+600k downloads, 2 laws approved)		
Step	**User Actions**	**System Actions**
1.	User selects the public petition	verifies the authenticity of public petition on-chain
2.	User decides signing	System uses the stored and previously validated Blockchain ID for signing the petition App does proof-of-work, generating a block to be accepted by the network (avoiding hacking, spam and brute-force on the network) Sends the block to network.

		If the block is valid, the network stores the block on a sidechain In the selected times, the system scan the sidechain, revalidates all user signatures, and generates and publish a new version of the PDF report with all signatures collected for all open public petitions System authenticates each generated new version of the report on blockchain
3.	User submits the signatures report to verify the authenticity	System verifies the authenticity of the report on-chain System validates each signature in the report: user validity and integrity of the user signature

Existing Flow (to-be): Chrome Plugin: Proof-of-authenticity of web content + notarization (avoiding fake news dissemination, harassment and other on social media)		
Step	**User Actions**	**System Actions**
1.	Click on Chrome Plugin	Scans the page Generates a report which contains the permalink, timestamp and the copy of the page Authenticates the report in blockchain Send the report to the notary Notary verifies the authenticity in on-chain Notary extracts the permalink, access the page, copies the page, authenticates the copy of the page and delivers back to the user

Existing Flow (to-be): Platform: Notarization of documents		
Step	**User Actions**	**System Actions**
1.	User submits a document	Extracts the hash Verify on-chain the authenticity of the document If document is already authenticated, returns the full information If the document is not authenticated yet, goes to the checkout
2.	User goes to the payment page	System detects if the user is staking the token ABC - Anti Bureaucracy Coin If yes, system recalculates the discount

3.	User makes the payment	System authenticates the hash of the document in on or more blockchains

Existing Flow (to-be): Platform: Registration of documents to be signed		
Step	**User Actions**	**System Actions**
1.	User submits a document	Extracts the hash Verify on-chain the authenticity of the document If document is already authenticated, returns the full information If the document is not authenticated yet, goes to the checkout
2.	User goes to the payment page	System detects if the user is staking the token ABC - Anti Bureaucracy Coin If yes, system recalculates the discount
3.	User makes the payment	System authenticates the hash of the document in on or more blockchains System opens a session on a smart-contract to start collecting the signatures System notifies all signatories Signatories make the signature System stores the signature together on the smart-contract After collecting all signatures, system generates a report and send to each signer.

Existing Flow (to-be): Platform and app: Public e-voting		
Step	**User Actions**	**System Actions**
1.	Voter submits the filled voting ballot for signing	Extracts the hash Register the ballot for signature by the selected BlockchainID on the smart-contract and wait for the signature
2.	Voter sign the ballot with BlockchainID	System stores the user signature on the smart-contract After confirmation, system provides a certificate of signature to the user
3.	User submit the ballot and the certificate to the voting	off-chain process

	administration for tallying purposes	

Expected Flow (to-be): Secret voting on public blockchain PoC and paper: https://github.com/eddieoz/haal		
Step	**User Actions**	**System Actions**
1.	User authenticates to voting session	Validate the user identity Open the voting session Unlink user identity Generates the stealth addresses for voting and register it on chain to be discovered
2.	User cast the vote through stealth wallet	System creates the zero-knowledge proof-of-vote Encrypts the ballot with homomorphic encryption Casts the encrypted ballot and store in blockchain Validates the zkProof-of-Vote on chain User verify own vote Closes the voting session
3	Voting administrator closes the election session	Smart-contract automatically the result Smart-contract publishes the result
4	Auditor retrieve all results to check	Decrypts all votes Calculates the final result Generates the proof-of-result Publish the proof-of-result on chain

Expected Flow (to-be): Decentralized network of validation		
Step	**User Actions**	**System Actions**
1.	User A collect the web-content proof and send to the platform	Opens a collecting proofs session System authenticates the proof on blockchain System asks for how many people must access and collect proofs System calculates how much ABCs must be deposited to reward the network for collecting proofs
2.	User A deposits the amount	System randomly notifies the network to collect proofs
3.	Users from network receive the notification and agrees on collecting proof from their device	System generates automatically the proof System asks for user to sign the proof with the Blockchain ID to prove it is a real person
4.	User from network agrees on signing	System sign the proof using the Blockchain ID System authenticates the generated proof on blockchain Stores the proof to the proofs repository
5.	User A collects the proofs collection	After aproval, rewards user from network Delivers all signed proofs to the User A Closes the collecting proofs session

Process scheme (to-be)

Participants and their roles		
Actor	**Type/Role**	**Description**
1	*Government/Institution*	Voting system administrator: Setup the voting infrastructure, open and closes the voting session
2	*Natural person*	Vote, request webcontent proofs participate on the decentralized network for collecting webcontent proofs.
3	*Lawyer*	Request webcontent proofs from decentralized network
4	*OriginalMy*	It is the first validator of user identity
5	*Auditor*	Audit the voting process in real time, compute the result and the proof-of-result to check if it matches with the automatically calculated by the smart-contract, count users, count open voting sessions, verify if user validation is correct
6	*Notary*	Executes a digital process of authenticating documents and signatures

Data and information		
Data	**Type**	**Description**
1	*Web Content*	Content collected on Web Browser
2	*Proof-of-Authenticity of Web Content*	PDF report that contains the permalink, timestamp and the copy of the web content.
3	*Ballot*	Ballot that contains all the races and candidates
4	*Encrypted Vote*	The ballot with each vote encrypted
5	*Proof-of-Vote*	Zero Knowledge proof-of-vote issued optionally after voting, used as vote receipt
6	*Proof-of-Result*	Zero-knowledge proof-of-result, proves the voting administrator decrypted all votes and calculated the result for auditing purposes
7	*Digital Document*	Any kind of digital media, to be authenticated
8	*Digital Signature*	Signature made using the private-keys owned by the user

9	*Digital Identity*	Digital certificate where the private-keys are located. It must be stored just with the user

Security and privacy
1. User validates the identity for using the BlockchainID 2. User casts the vote, unlinked to identity 3. No participant can see the content of the vote of another user 4. No possibility of double-voting 5. User can keep the (zk)proof-of-vote, to prove the vote without exposing the vote 6. Vote buying and vote coersion avoided if the voting session is open for many days and user have the possibility of changing vote anytime (Estonia example) 7. OriginalMy dont store user personal data, content or documents, for privacy purposes 8. User delivers own personal data, signing the data delivered. Destination platform has proof-of-agreement for all received data. 9. Decentralized identity and decentralized storage of personal data. No single point of failure

Main Success Scenario + expected time line
Actual Key Achievements The main key achievements are: - having blockchain proofs accepted in the Court of Appeals (Superior Court), - new laws created that started on our engines (through Mudamos+), - marriages and child born registrations, - used by presidential candidates to fight against fake-news dissemination, - shareholders e-voting on Brazilian Fintechs Association, - mentioned in books and academic papers, - Brazilians no longer need to go to the notary to authenticate documents, because of the first notary integration, - featured on a US documentary of Reason.tv: "3 Ways Bitcoin is Promoting Freedom in Latin America" - featured on a documentary of Globo, the second largest commercial TV: "Estonia has a pioneering project to end bureaucracy and facilitate citizens' lives" Awarded: - Google.org Social Impact Challenge in 2016 (through Mudamos+ by ITS-Rio - app for signing public petitions powered by our engine for identity, signatures and authentication), - Financial Personality of the Year in 2017 - Most Innovative Startup in 2018

Future Success Scenario

An anonymous electronic voting system on public blockchains with the transparency and auditability provided by a public blockchain like Ethereum to bring another level of trust and security because everything can be auditable during the voting process. The smart-contract starts the tally phase and verify it using distributed computing if needed. The voting privacy is granted by stealth wallets, homomorphic encryption, at the same time that zero-knowledge proofs grant the and the proof-of-vote and the proof-of-result.

We expected until the end of 2019 having a open capital company doing the shareholders proxy-voting through our platform

Conditions (pre- or post-)

For using Blockchain ID:

1. Download OriginalMy app

2. Validation of the identity of the user through automated or manual process

For authenticating documents

1. Create an account on the website

For authenticating web-proofs

1. Installing the Chrome Browser extension

Performance needs

What potential performance specs (frequency of use, transactions per second, confirmation time, sync time, etc.) are expected. What scalability, interoperability, reliability, accessibility needs exist.

- Improving the confirmation time for contract and signatures
- Improving the fee & gas of blockchain/smart-contracts
- Scale the identity validation
- Implement another public blockchains (Waves, Litecoin and others)
- Interoperability with x509 certificates
- reducing fee for using ABC token

Legal considerations

For each issue, please describe the name of the legal act containing the identified barrier, what is the negative impact and a proposal to overcome this negative impact.

1. Compliance with MP 2200-2/2001
2. Compliance with Civil Law Arts. 104-107, 219 and 220
3. Legal opinion for digital authentication with notaries

   No law barriers with negative impact, but laws expressly approving the format of authentication could be helpful, like the case of Wyioming https://www.forbes.com/sites/caitlinlong/2019/03/04/what-do-wyomings-new-blockchain-laws-mean/#2943280e5fde

Risks

Legal, business and technical risks related to use case

Risks of lobby by notaries, banks and congressmen

Lack of regulations in Brazil creating an insecure environment for crypto-startups

Tech risks:

- 0-day in Bitcoin, Ethereum or EDSA curves,
- 51% attack,
- expensive fee costs because of cryptocurrency prices

Special Requirements

No special requirements

External References and Miscellaneous

List of references for standards or well-defined mechanisms if any of requirements calls for the implementation of a standard or protocol or other well-defined mechanism. If the use case needs non-standard consensus mechanisms or cryptographic tools, such information should be included here. Also such section may be used to provide more information regarding the use case including links to any kind of related materials, terms and descriptions or any other related information.

Albrecht, Martin, et al. Homomorphic Encryption Standard. 21 Nov. 2018, http://homomorphicencryption.org/wp-content/uploads/2018/11/HomomorphicEncry ptionStandardv1.1.pdf.

A Next-Generation Smart Contract and Decentralized Application Platform. https://github.com/ethereum/wiki/wiki/White-Paper. Accessed 13 Jan. 2019.

Aztec Protocol Specification. https://github.com/AztecProtocol/AZTEC/blob/master/AZTEC.pdf. Accessed 13 Jan. 2019.

Baudron, Olivier, et al. "Practical Multi-Candidate Election System." Proceedings of the Twentieth Annual ACM Symposium on Principles of Distributed Computing - PODC '01, 2001, doi: 10.1145/383962.384044.

Bitcoin-Development | Stealth Addresses. https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2014-January/004020.html. Accessed 14 Jan. 2019.

Blum, Manuel, et al. "Noninteractive Zero-Knowledge." SIAM Journal on Computing, vol. 20, no. 6, 1991, pp. 1084–118.

Camenisch, Jan, et al. "Efficient Protocols for Set Membership and Range Proofs." Lecture Notes in Computer Science, 2008, pp. 234–52.

Dahlin, Taylor Fox, and daylighting society. "Paillier Zero-Knowledge Proof."

Https://paillier.daylightingsociety.org, 17 Dec. 2016,

https://paillier.daylightingsociety.org/Paillier_Zero_Knowledge_Proof.pdf. Damgård, Ivan. On Σ-Protocols.

http://www-cs.ccny.cuny.edu/~fazio/F15-csc85030/readings/Dam10.pdf. Accessed 13

Jan. 2019.Decentralised Applications.

https://github.com/ethereum/wiki/wiki/Decentralized-apps-(dapps).Developer Guide - Bitcoin | Blockchain.

https://bitcoin.org/en/developer-guide#block-chain. Accessed 14 Jan. 2019.

Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret

MacAlpine, J. Alex Halderman. Security Analysis of the Estonian Internet Voting

System. https://jhalderm.com/pub/papers/ivoting-ccs14.pdf. Accessed 13 Jan. 2019. Goldwasser, S., et al. "The Knowledge Complexity of Interactive Proof-Systems." Proceedings

of the Seventeenth Annual ACM Symposium on Theory of Computing - STOC '85, 1985,

doi:10.1145/22145.22178.

Goldwasser, Shafi, et al. The Knowledge Complexity of Interactive Proof Systems. Feb. 1989,

http://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/

The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf.

Heiberg, Sven, et al. "Improving the Verifiability of the Estonian Internet Voting Scheme."

Lecture Notes in Computer Science, 2017, pp. 92–107.Introduction – Homomorphic Encryption Standardization.

http://homomorphicencryption.org/introduction/. Accessed 14 Jan. 2019.

Lai, Wei-Jr, et al. "DATE: A Decentralized, Anonymous, and Transparent E-Voting System."

2018 1st IEEE International Conference on Hot Information-Centric Networking

(HotICN), 2018, doi:10.1109/hoticn.2018.8605994.

Racanelli, Vito J. "Proxy Voting Is Broken and Needs to Change." Barrons Online, Barrons, 7

July 2018, https://www.barrons.com/articles/proxy-voting-is-broken-and-needs-to-change-15309 24318.

Rivest, Ronald L. The ThreeBallot Voting System. 1 Oct. 2006, https://people.csail.mit.edu/rivest/Rivest-TheThreeBallotVotingSystem.pdf.

Tsang, Patrick P., and Victor K. Wei. "Short Linkable Ring Signatures for E-Voting, E-Cash and Attestation." Lecture Notes in Computer Science, 2005, pp. 48–60.

What Are Zk-SNARKs? https://z.cash/technology/zksnarks/. Accessed 14 Jan. 2019. Wu, Wei-Jr Lai Ja-Ling. An Efficient and Effective Decentralized Anonymous Voting

System. 18 Apr. 2018, http://arxiv.org/abs/1804.06674.

Yu, Bin, et al. "Platform-Independent Secure Blockchain-Based Voting System." Lecture

Notes in Computer Science, 2018, pp. 369–86.Zcash Protocol Specification.

https://github.com/zcash/zips/blob/master/protocol/protocol.pdf. Accessed 13 Jan. 2019.

Other Notes
Any assumptions, issues